ABSTRACT ALGEBRA

December 27, 2025

Contents

1. Basic Group theory

1.1. **Definitions.**

Definition 1.1.1 (Groups)**.** A *group* is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$ is a binary operation, subject to the following conditions:

1. (Associativity) For all $g, h, k \in G$ one has

$$(g \cdot h) \cdot k = g \cdot (h \cdot k).$$

2. (Identity element) There exists an element $e \in G$ such that for all $g \in G$,

$$e \cdot g = g \cdot e = g.$$

3. (Inverse element) For all $g \in G$ there exists an element $g^{-1} \in G$ such that

$$g \cdot g^{-1} = g^{-1} \cdot g = e.$$

The element e is called the *identity element of G*, and g^{-1} is called the *inverse of g*.

Equivalently, a group is a monoid (Definition A.2.2) with inverse elements.

A group $(G, \cdot)$ is often simply written as G, when the notation for the binary operation $\cdot$ is clear.

An *abelian group* or synonymously, a *commutative group*, is a group $(G, \cdot)$ whose binary operation $\cdot$ is *abelian* or *commutative* (Definition A.2.3), i.e. satisfies

$$g \cdot h = h \cdot g$$

for all $g, h \in G$.

An abelian group is equivalent to a $\mathbb{Z}$-module.

Remark 1.1.2. Given a set G and a binary operator $\cdot$ on it, the notation of $\cdot$ may often be omitted, especially when the binary operation is thought of as a "multiplication" (as opposed to, for example, "addition"); more precisely, one may write gh in place of $g \cdot h$ for $g, h \in G$.

Definition 1.1.3 (Group homomorphism)**.** Let $(G, \cdot)$ and $(H, *)$ be groups (Definition 1.1.1). A map $f : G \to H$ is called a *group homomorphism* if for all $g_1, g_2 \in G$ one has

$$f(g_1 \cdot g_2) = f(g_1) * f(g_2).$$

The collection of all groups with the group homomorphisms forms a locally small (Definition A.4.3) category (Definition A.4.1), called the *category of groups*.

If f is bijective (Definition A.1.3), then f is called a *group isomorphism*. .

Definition 1.1.4.

1. The *category of groups* is the locally small (Definition A.4.3) category (Definition A.4.1) whose objects are groups (Definition 1.1.1) and whose morphisms are group homomorphisms (Definition 1.1.3). It is often denoted by notations such as **Grp**.
2. The *category of abelian groups* is the locally small (Definition A.4.3) category (Definition A.4.1) whose objects are abelian groups (Definition 1.1.1) and whose morphisms are group homomorphisms (Definition 1.1.3). It is often denoted by notations such as **Ab**.

Definition 1.1.5. Let $(G, \cdot)$ be a group. A subset $H \subseteq G$ is called a *subgroup of G* if H, with the operation induced from G, is a group. That is, H is a subgroup if:

- $H \neq \emptyset$,
- For all $h_1, h_2 \in H$, the product $h_1 \cdot h_2 \in H$,
- For all $h \in H$, the inverse $h^{-1} \in H$.

We denote this relation by $H \leq G$, meaning "H is a subgroup of G".

Definition 1.1.6 (Conjugation)**.** Let $(G, \cdot)$ be a group (Definition 1.1.1).

1. For $g, h \in G$, the *conjugate of h by g* is the element $ghg^{-1} \in G$. Some may choose an opposite convention, letting the conjugate of h by g refer to the element $g^{-1}hg$ instead.
2. For $g \in G$ and a subgroup (Definition 1.1.5) $H \leq G$, the *conjugate of H by g* is the group

$$gHg^{-1} := \{ghg^{-1} \in G : h \in G.$$

It is a subgroup of G.

Some may choose an opposite convention, letting the conjugate of H by g to refer to the group $g^{-1}Hg$ instead.

Definition 1.1.7 (Cosets)**.** Let G be a group (Definition 1.1.1) and $H \leq G$ a subgroup (Definition 1.1.5). For each element $g \in G$, the *left coset of H in G determined by g* is

$$gH := \{gh \mid h \in H\},$$

and the *right coset of H in G determined by g* is

$$Hg := \{hg \mid h \in H\}.$$

Definition 1.1.8. Let G be a group (Definition 1.1.1) and let $H \leq G$ be a subgroup (Definition 1.1.5). The *index of H in G* is the cardinality (Definition A.1.11) of the set

$$\{gH : g \in G\}$$

of left cosets of H in G. This is equivalent to the cardinality of the set

$$\{Hg : g \in G\}$$

of right cosets of H in G.

Definition 1.1.9. Let $(G, \cdot)$ be a group (Definition 1.1.1). A subgroup (Definition 1.1.5) $N \leq G$ is called a *normal subgroup of G* if N is closed under conjugation (Definition 1.1.6) by elements of G, i.e. for all $g \in G$ and $n \in N$, one has

$$gng^{-1} \in N.$$

Equivalently, N is normal in G if every left coset of N in G is also a right coset of N in G (Definition 1.1.22). We denote this relation by $N \trianglelefteq G$, meaning "N is a normal subgroup of G".

Lemma 1.1.10. Every subgroup (Definition 1.1.5) of an abelian group (Definition 1.1.1) is a normal subgroup (Definition 1.1.9).

Definition 1.1.11. Let $\phi : G \to H$ be a group homomorphism (Definition 1.1.3).

1. The *kernel of ϕ*, denoted $\ker(\phi)$, is the set of elements in G that map to the identity element of H:
$$\ker(\phi) = \{g \in G \mid \phi(g) = e_H\}$$
where e_H is the identity element of H.
2. The *image of ϕ,* denoted $\operatorname{im}(\phi)$ or $\phi(G)$, is the set of elements in H that are the image of some element in G:
$$\operatorname{im}(\phi) = \{h \in H \mid \exists g \in G, \phi(g) = h\}$$

Proposition 1.1.12. Let $\phi : G \to H$ be a group homomorphism (Definition 1.1.3).

1. The kernel $\ker(\phi)$ (Definition 1.1.11) is a normal subgroup (Definition 1.1.9) of G.
2. The image (Definition 1.1.11) $\operatorname{im}(\phi)$ is a subgroup (Definition 1.1.5) of H.
3. The homomorphism ϕ is injective (Definition A.1.3) if and only if $\ker(\phi) = \{e_G\}$, where e_G is the identity element of G.
4. The homomorphism ϕ is surjective (Definition A.1.3) if and only if $\operatorname{im}(\phi) = H$.

Definition 1.1.13 (Quotient Group)**.** Let G be a group (Definition 1.1.1) and $N \trianglelefteq G$ a normal subgroup (Definition 1.1.9). The *quotient group of G by N*, denoted by G/N, is the set of all left (or equivalently, right) cosets (Definition 1.1.7) of N in G,

$$G/N := \{gN \mid g \in G\},$$

endowed with the operation defined by

$$(gN)(hN) := (gh)N \quad \text{for all } g, h \in G.$$

This operation is well-defined because N is normal in G, and under this operation G/N is a group with identity element N and inverse given by $(gN)^{-1} = g^{-1}N$.

There is (Theorem 1.1.15) a canonical surjective homomorphism $G \to G/N$ given by $g \mapsto gN$.

Note that any abelian group (Definition 1.1.1) has a quotient by any subgroup (Definition 1.1.5) as all subgroups of an abelian group are normal (Lemma 1.1.10).

Proposition 1.1.14. Let G be a group (Definition 1.1.1) and N a normal subgroup (Definition 1.1.9) of G. The binary operation of the quotient group G/N is well defined and G/N is indeed a group.

Theorem 1.1.15. The map $\pi : G \to G/N$ defined by $\pi(g) = gN$ is a surjective (Definition A.1.3) group homomorphism (Definition 1.1.3) with kernel (Definition 1.1.11) N. This map is called the *canonical projection* or *natural homomorphism*.

Theorem 1.1.16.

1. (First Isomorphism Theorem) Let $\phi : G \to H$ be a group homomorphism with kernel $K = \ker(\phi)$ and image $I = \operatorname{im}(\phi)$. Then K is a normal subgroup of G, I is a subgroup of H, and there is an isomorphism
$$G/K \cong I$$
given by the map $gK \mapsto \phi(g)$. This theorem implies that any homomorphic image of a group is isomorphic to a quotient of that group.
2. (Second Isomorphism Theorem, or Diamond Isomorphism Theorem) Let G be a group, H a subgroup of G, and N a normal subgroup of G. Then: 1. The product $HN = \{hn \mid h \in H, n \in N\}$ is a subgroup of G. 2. The intersection $H \cap N$ is a normal subgroup of H. 3. There is an isomorphism
$$H/(H \cap N) \cong (HN)/N$$
given by the map $h(H \cap N) \mapsto hN$.
3. (Third Isomorphism Theorem) Let G be a group and let N and K be normal subgroups of G with $N \subseteq K$. Then K/N is a normal subgroup of G/N, and there is an isomorphism
$$(G/N)/(K/N) \cong G/K$$
given by the map $(gN)(K/N) \mapsto gK$.
4. (Correspondence Theorem, or Lattice Isomorphism Theorem) Let G be a group and N be a normal subgroup of G. There is a one-to-one correspondence between the set of subgroups A of G containing N (i.e., $N \subseteq A \subseteq G$) and the set of subgroups of the quotient group G/N. This correspondence is given by $A \mapsto A/N$, and it preserves properties such as inclusion, indices, normality, and intersections.

1.1.1. *Some basic examples of groups.*

Definition 1.1.17. Let X be a set. The *symmetric group on X* or the *permutation group on X*, denoted by $\mathfrak{S}_X$, S_X, or Sym_X, is the group (Definition 1.1.1) whose elements are all bijections (Definition A.1.3) $\sigma : X \to X$, with the group operation being composition of maps:
$$(\sigma \circ \tau)(x) := \sigma(\tau(x)), \quad \sigma, \tau \in \mathfrak{S}_X,\ x \in X.$$
The identity element is the identity map id_X (Definition A.1.7), and the inverse of σ is its inverse function σ^{-1} (Definition A.1.3).

Elements of the symmetric group are called *permutations*.

A symmetric group on a finite set (Definition A.1.5) of n elements is typically denoted by $\mathfrak{S}_n$, S_n, or Sym_n. Any two symmetric groups on sets of equal cardinality are isomorphic (Definition 1.1.3).

Definition 1.1.18. Let $\mathfrak{S}_n$ denote the symmetric group (Definition 1.1.17) on $\{1, 2, \ldots, n\}$. For $\tau \in \mathfrak{S}_n$, the *parity of τ* is defined to be 0 if τ can be expressed as a product of an even number of transpositions, and 1 otherwise. The *signature of τ* or *sign of τ* is then denoted by $\mathrm{sgn}(\tau)$, defined by

$$\mathrm{sgn}(\tau) := (-1)^{\mathrm{parity}(\tau)} \in \{1, -1\}.$$

Let X be a finite set and $\mathfrak{S}_X$ its symmetric group. The *signature or sign of an element of $\mathfrak{S}_X$*, denoted by $\mathrm{sgn}(\sigma)$ for $\sigma \in \mathfrak{S}_X$, is defined by choosing any bijection $\phi : X \to \{1, 2, \ldots, n\}$, setting $\tau := \Phi_\phi(\sigma) \in \mathfrak{S}_n$, and then

$$\mathrm{sgn}(\sigma) := \mathrm{sgn}(\tau).$$

This definition is independent of the choice of ϕ, and thus $\mathrm{sgn} : \mathfrak{S}_X \to \{1, -1\}$ is a well-defined group homomorphism (Definition 1.1.3).

1.1.2. *Normalizer of a subgroup and centralizer of a subset of a group.*

Definition 1.1.19 (Normalizer)**.** Let $(G, \cdot)$ be a group (Definition 1.1.1) and let $H \subseteq G$ be a subgroup (Definition 1.1.5). The *normalizer of H in G* is defined as

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

Proposition 1.1.20. Let $(G, \cdot)$ be a group (Definition 1.1.1) and let $H \subseteq G$ be a subgroup (Definition 1.1.5). The group H is a normal subgroup (Definition 1.1.9) of the normalizer $N_G(H)$ (Definition 1.1.19).

Definition 1.1.21 (Centralizer)**.** Let $(G, \cdot)$ be a group (Definition 1.1.1) and let $S \subseteq G$ be a subset. The *centralizer of S in G* is defined as

$$C_G(S) = \{g \in G : gs = sg \text{ for all } s \in S\}.$$

1.1.3. *Group actions.*

Definition 1.1.22 (Left and Right Group Actions)**.** Let $(G, \cdot)$ be a group (Definition 1.1.1) and let X be a set.

1. A *left group action of G on X* is a function

   $$\varphi : G \times X \to X$$

   such that for all $g, h \in G$ and all $x \in X$,

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

   For $g \in G$ and $x \in X$, the element $\varphi(g, x)$ is called the *image of x under the action of g*. We often write $g \cdot x$ for $\varphi(g, x)$.

If G acts on X on the left via a function $\varphi : G \times X \to X$, we write

$$G \curvearrowright X.$$

2. A *right group action of G on X* is a function

$$\psi : X \times G \to X$$

such that for all $g, h \in G$ and all $x \in X$,

$$\psi(x, e) = x,$$
$$\psi(x, gh) = \psi(\psi(x, g), h).$$

For $x \in X$ and $g \in G$, the element $\psi(x, g)$ is called the *image of x under the right action of g*. We often write $x \cdot g$ for $\psi(x, g)$.

If G acts on X on the right via a function $\psi : X \times G \to X$, we write

$$X \curvearrowleft G.$$

Definition 1.1.23 (Orbit)**.** Let $(G, \cdot)$ be a group (Definition 1.1.1) acting on (Definition 1.1.22) a set X, with action denoted by $g \cdot x$. For $x \in X$, the *orbit of x* under the action of G is

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

Definition 1.1.24 (Stabilizer)**.** Let $(G, \cdot)$ be a group acting on a set X. For $x \in X$, the *stabilizer of x in G* is

$$\operatorname{Stab}_G(x) = \{g \in G : g \cdot x = x\}.$$

Definition 1.1.25 (Fixed Point Set)**.** Let $(G, \cdot)$ be a group acting on a set X. For $H \subseteq G$, the *fixed point set of H in X* is defined by

$$X^H = \{x \in X : h \cdot x = x \text{ for all } h \in H\}.$$

Proposition 1.1.26. Let $(G, \cdot)$ be a group (Definition 1.1.1) acting (Definition 1.1.22) (on the left) on a set X. Define a binary relation (Definition A.1.8) $\sim$ on X by

$$x \sim y \iff \exists g \in G : g \cdot x = y.$$

Then $\sim$ is an equivalence relation (Definition A.1.9) on X, and the equivalence classes (Definition A.1.10) are exactly the orbits (Definition 1.1.23) $\{G \cdot x : x \in X\}$.

Proposition 1.1.27. Let $(G, \cdot)$ be a group (Definition 1.1.1) acting (Definition 1.1.22) (on the left) on a set X. For all $x \in X$, the stabilizer (Definition 1.1.24)

$$\operatorname{Stab}_G(x) = \{g \in G : g \cdot x = x\}$$

is a subgroup (Definition 1.1.5) of G.

Proposition 1.1.28. Let $(G, \cdot)$ be a group (Definition 1.1.1) acting (Definition 1.1.22) (on the left) on a set X. For all $x \in X$, there is a bijection of sets

$$G/\operatorname{Stab}_G(x) \longleftrightarrow G \cdot x, \quad g \operatorname{Stab}_G(x) \mapsto g \cdot x.$$

In particular, if G is finite then

$$|G \cdot x| = [G : \operatorname{Stab}_G(x)] = \frac{|G|}{|\operatorname{Stab}_G(x)|}.$$

Proposition 1.1.29. Let $(G, \cdot)$ be a group (Definition 1.1.1) acting (Definition 1.1.22) (on the left) on a set X. For any subgroup $H \subseteq G$, the fixed point set (Definition 1.1.25)

$$X^H = \{x \in X : h \cdot x = x \text{ for all } h \in H\}$$

satisfies $X^H \subseteq X^{H'}$ whenever $H' \subseteq H$.

1.2. **Constructions of Groups from others.**

Definition 1.2.1 (Product of Groups)**.** Let $\{G_i\}_{i \in I}$ be a family of groups indexed by a (possibly infinite (Definition A.1.5) but small (Definition A.1.1)) set I, each with group operation denoted multiplicatively and identity element e_i. The *(direct) product of the family $\{G_i\}_{i \in I}$*, denoted by $\prod_{i \in I} G_i$, is defined as the set of all functions

$$\prod_{i \in I} G_i := \{(g_i)_{i \in I} \mid g_i \in G_i \text{ for all } i \in I\},$$

equipped with the binary operation defined componentwise by

$$(g_i)_{i \in I} \cdot (h_i)_{i \in I} := (g_i h_i)_{i \in I}$$

for all $(g_i)_{i \in I}, (h_i)_{i \in I} \in \prod_{i \in I} G_i$. Then $\prod_{i \in I} G_i$ is a group with the identity element $(e_i)_{i \in I}$ and inverses given by

$$(g_i)_{i \in I}^{-1} = (g_i^{-1})_{i \in I}.$$

The product $\prod_{i=1} G_i$ is the product (Definition A.4.21) of the objects G_i in the category of groups (Definition 1.1.3). As a set, note that $\prod_{i \in I} G_i$ coincides with the product $\prod_{i \in I} G_i$ (Definition A.1.4) of the G_i as sets.

A self product of a group G (indexed by a small set I), is often denoted by G^I. A finite self product of a group G taken n times is often denoted by G^n. In case that G is abelian, these may be written as $G^{\oplus I}$ and $G^{\oplus n}$ respectively.

The product of finitely many groups $G_1, \ldots, G_n$ is often denoted by $G_1 \times \cdots \times G_n$.

1.3. **Sylow theory.**

Definition 1.3.1. Let G be a finite (Definition A.1.5) group (Definition 1.1.1) and p be a prime number. A subgroup (Definition 1.1.5) H of G is called a *p-subgroup* if the order of H is a power of p.

Definition 1.3.2. Let G be a finite (Definition A.1.5) group (Definition 1.1.1) of order $p^n m$, where p is a prime number and p does not divide m. A *Sylow p-subgroup* of G is a subgroup (Definition 1.1.5) of order p^n.

The set of all Sylow p-subgroups of a group G is denoted by $\mathrm{Syl}_p(G)$. The number of Sylow p-subgroups is denoted by $n_p(G)$ or simply n_p.

Theorem 1.3.3. Let G be a finite (Definition A.1.5) group (Definition 1.1.1) and p be a prime number such that p divides the order of G.

1. (Sylow's first theorem) $\mathrm{Syl}_p(G)$ (Definition 1.3.2) is non-empty; that is, G contains at least one subgroup of order p^n, where p^n is the highest power of p dividing $|G|$.

2. (Sylow's second theorem) If P_1 and P_2 are Sylow p-subgroups of G (Definition 1.3.2), then they are conjugate (Definition 1.1.6) in G. That is, there exists an element $g \in G$ such that $gP_1g^{-1} = P_2$.
3. (Sylow's third theorem) Let G be a finite group of order $p^n m$ where $p \nmid m$. The number of Sylow p-subgroups, n_p (Definition 1.3.2), satisfies the following conditions:

$$n_p \equiv 1 \pmod p$$

$$n_p \mid m$$

   Furthermore, $n_p = [G : N_G(P)]$ for any Sylow p-subgroup P, where $N_G(P)$ is the normalizer (Definition 1.1.19) of P in G.

Corollary 1.3.4. Let G be a finite group and p a prime number. Every p-subgroup (Definition 1.3.1) of G is contained in some Sylow p-subgroup (Definition 1.3.2) of G.

1.4. **Short exact sequences of general groups.**

Definition 1.4.1.

1. A sequence of groups (Definition 1.1.1) and group homomorphisms (Definition 1.1.3)

$$\dots \xrightarrow{\phi_{i-1}} G_i \xrightarrow{\phi_i} G_{i+1} \xrightarrow{\phi_{i+1}} \dots$$

   is called *exact at G_i* if $\operatorname{im}(\phi_{i-1}) = \ker(\phi_i)$ (Definition 1.1.11). The sequence is called an *exact sequence* if it is exact at every group G_i.
2. A *short exact sequence of groups* is an exact sequence of the form

$$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1$$

   where 1 denotes the trivial group. Exactness implies that ι is injective (Definition A.1.3), π is surjective (Definition A.1.3), and $\operatorname{im}(\iota) = \ker(\pi)$.

Definition 1.4.2. Let $1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1$ be a short exact sequence of groups.

1. A *section* (or *splitting homomorphism)* of the short exact sequence is a group homomorphism (Definition 1.1.3) $s : H \to G$ such that $\pi \circ s = \mathrm{id}_H$.
2. The short exact sequence $1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1$ is said to *split* if there exists a section $s : H \to G$.

1.5. **Semidirect products.**

Definition 1.5.1. Let G be a group.

1. An *automorphism of G* is an isomorphism (Definition 1.1.3) $\phi : G \to G$.
2. The *automorphism group of a group G,* denoted $\mathrm{Aut}(G)$, is the set of all automorphisms of G equipped with the binary operation of function composition. For $\phi, \psi \in \mathrm{Aut}(G)$, the composition $\phi \circ \psi$ is defined by $(\phi \circ \psi)(g) = \phi(\psi(g))$ for all $g \in G$.

The automorphism group of a group G is the automorphism group (Definition A.4.2) of G as an object of the category of groups (Definition 1.1.4).

Proposition 1.5.2. Let $\mathcal{C}$ be a locally small category (Definition A.4.3) and X be an object of $\mathcal{C}$. The automorphism group (Definition A.4.2) $\mathrm{Aut}_{\mathcal{C}}(X)$ indeed forms a group (Definition 1.1.1) under composition. The identity element is the identity morphism id_X, and the inverse of an element f is its inverse morphism f^{-1}.

Definition 1.5.3.

1. Let N and H be groups (Definition 1.1.1), and let $\varphi : H \to \mathrm{Aut}(N)$ be a homomorphism (Definition 1.1.3), where $\mathrm{Aut}(N)$ is the group of automorphisms (Definition 1.5.1) of N. The *external semidirect product of N and H with respect to φ*, denoted $N \rtimes_\varphi H$, is the group defined on the set $N \times H$ with the binary operation:
$$(n_1, h_1)(n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)$$
for all $n_1, n_2 \in N$ and $h_1, h_2 \in H$.
2. Let G be a group. G is the *internal semidirect product of a subgroup N and a subgroup H* if the following conditions hold:
   (a) N is a normal subgroup (Definition 1.1.9) of G.
   (b) $G = NH$, meaning every element $g \in G$ can be written as $g = nh$ for some $n \in N$ and $h \in H$.
   (c) $N \cap H = \{1\}$, where 1 is the identity element of G.

Theorem 1.5.4. Let G be a group (Definition 1.1.1) with subgroups (Definition 1.1.5) N and H. The group G is the internal semidirect product (Definition 1.5.3) of N and H if and only if G is isomorphic (Definition 1.1.3) to the external semidirect product (Definition 1.5.3) $N \rtimes_\varphi H$, where the homomorphism $\varphi : H \to \mathrm{Aut}(N)$ is given by conjugation (Definition 1.1.6) within G:
$$\varphi(h)(n) = hnh^{-1}$$
for all $h \in H$ and $n \in N$. Under this isomorphism, the subgroups N and H of the internal product correspond to the subgroups $\{(n, 1) \mid n \in N\}$ and $\{(1, h) \mid h \in H\}$ of the external product, respectively.

Theorem 1.5.5. Let N and H be groups (Definition 1.1.1). A group G is isomorphic (Definition 1.1.3) to a semidirect product (Definition 1.5.3) of N by H if and only if there exists a short exact sequence (♠ TODO: short exact sequence of groups, splitting, section)
$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\iota"] & G \arrow[r, "\pi"] & H \arrow[r] & 1 \end{tikzcd}$$
that splits, meaning there exists a section $s : H \to G$, i.e. a group homomorphism (Definition 1.1.3) such that $\pi \circ s = \mathrm{id}_H$. In this case, $G \cong N \rtimes_\varphi H$ with $\varphi(h)(n) = s(h)ns(h)^{-1}$ (identifying N with its image $\iota(N)$).

2. Basic Ring theory

2.1. **Definitions.**

2.1.1. *Rings, division rings, and fields.*

Definition 2.1.1. A *ring* is a triple $(R, +, \cdot)$ where

1. $(R, +)$ is a commutative group (Definition 1.1.1), and

2. $(R, \cdot)$ is a monoid (Definition A.2.2).
3. $\cdot$ is distributive over $+$, i.e. for all $a, b, c \in R$, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Equivalently, a ring is a triple $(R, +, \cdot)$ where $+, \cdot : R \times R \to R$ are binary operations satisfying

1. $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$ for all $a, b, c \in R$
2. There exists an element $0 \in R$ such that $a + 0 = a = 0 + a$ for all $a \in R$.
3. For every $a \in R$, there exists an element $-a \in R$ such that $a + (-a) = 0 = (-a) + a$ for all $a \in R$.
4. There exists an element $1 \in R$ such that $a \cdot 1 = a = 1 \cdot a$ for all $a \in R$.
5. For all $a, b, c \in R$, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

The operation $+$ is often called *addition* and the operation $\cdot$ is often called *multiplication*. Accordingly, the identity element 0 of $+$ is often called the *additive identity* and the identity element 1 of $\cdot$ is often called the *multiplicative identity*.

Remark 2.1.2. Some writers might not require a ring to have a multiplicative identity element, i.e. would define a ring so that $(R, +)$ is a commutative group, $(R, \cdot)$ is a semigroup, and $\cdot$ is distributive over $+$. Such writers would call the notion of ring in Definition 2.1.1 a *unitary ring* to emphasize the existence of the multiplicative identity 1.

Definition 2.1.3 (Opposite ring)**.** Let $R = (R, +, \cdot, 0, 1)$ be a ring (Definition 2.1.1) with addition $+$, multiplication $\cdot$, additive identity 0, and multiplicative identity 1 (not necessarily commutative).

The *opposite ring of R*, denoted R^{op}, is the ring with the same underlying set R and the same addition $+$ and additive identity 0, but with multiplication defined by

$$r \star s := s \cdot r$$

for all $r, s \in R$.

That is, multiplication in R^{op} is the multiplication of R reversed in order.

If R is commutative (Definition 2.1.4), then R and R^{op} are naturally isomorphic to each other.

Definition 2.1.4. A *commutative (unital) ring* is a ring (Definition 2.1.1) $(R, +, \cdot)$ such that $\cdot$ is a commutative operation (Definition A.2.3), i.e. $a \cdot b = b \cdot a$.

For many writers (e.g. "commutative" algebraists or number theorists), a *ring* refers to a commutative ring as above.

Definition 2.1.5 (Center of a ring)**.** Let R be a (not necessarily commutative) ring (Definition 2.1.1). The *center of R*, denoted by $Z(R)$, is the subset of elements in R that commute with every element of R:

$$Z(R) := \{z \in R \mid zr = rz \text{ for all } r \in R\}.$$

The center $Z(R)$ is a commutative (Definition 2.1.4) subring (Definition 2.1.25) of R.

Definition 2.1.6. Any set with a single element equipped with the only possible binary operators $+$ and $\cdot$ is a commutative ring (Definition 2.1.4) whose multiplicative and identity elements are both the sole element. Any ring with a single element is called the *zero ring* or the *trivial ring*.

Definition 2.1.7. Let $(R, +, \cdot)$ be a not-necessarily commutative ring (Definition 2.1.1).

1. An element $a \in R$ is a *left zero-divisor* if there exists a nonzero $x \in R$ such that $ax = 0$. Otherwise, a is called *left regular* or *left cancellable*.
2. An element $a \in R$ is a *right zero-divisor* if there exists a nonzero $x \in R$ such that $xa = 0$. Otherwise, a is called *right regular* or *right cancellable*.
3. An element $a \in R$ is a *zero-divisor* if it is a left zero-divisor or a right zero-divsor.
4. An element $a \in R$ is a *two-sided zero-divisor* if it is both a left zero-divisor and a right zero-divsor.
5. An element $a \in R$ is *regular*, *cancellable*, or a *non-zero-divisor* if it is both left and right regular.

A zero-divisor of any kind that is not itself 0 is said to be a *nonzero zero divisor* or a *nontrivial zero divisor* of its kind.

A non-zero ring with no nontrivial zero divisors is called a *domain*. A domain that it also a commutative ring (Definition 2.1.4) is also called an *integral domain*.

Definition 2.1.8. Let $(R, +, \cdot)$ be a not-necessarily commutative ring (Definition 2.1.1). A *unit* or *invertible element of R* is an element $u \in R$ such that there exist an element $v \in R$ such that

$$uv = 1 = vu.$$

Such an element v is called the *multiplicative inverse of u* and is often denoted by u^{-1}. If it exists, then it is unique.

The set of units of R forms a group (Definition 1.1.1), often denoted by $R^\times$ or R^*, under the multiplication operation $\cdot$. It is called the *group of units* or *unit group* of R.

Definition 2.1.9. Let $(R, +, \cdot)$ be a not-necessarily commutative ring (Definition 2.1.1). It is called a *division ring*, a *skew field*, or an *sfield*, if it is a nontrivial ring (Definition 2.1.6) in which every nonzero element $a \in R$ is a unit (Definition 2.1.8).

Definition 2.1.10 (Field)**.** A *field* is commutative division (Definition 2.1.9) ring (Definition 2.1.4). In other words, a field is a commutative ring for which all nonzero elements have a multiplicative inverse (Definition 2.1.8).

Lemma 2.1.11. Let F be a field. Its unit group $F^\times$ (Definition 2.1.8) as a set equals $F - \{0\}$.

A prominent example of a field would be the field of fractions of an integral domain.

Definition 2.1.12. Let R be an integral domain (Definition 2.1.7), and consider the set $R \times (R \setminus \{0\})$ as above. Define a relation $\sim$ on $R \times (R \setminus \{0\})$ by declaring that

$$(a, b) \sim (c, d) \quad \text{if and only if} \quad ad = bc,$$

for $a, c \in R$ and $b, d \in R \setminus \{0\}$. This relation is an equivalence relation. Its equivalence classes are denoted by $\frac{a}{b}$.

The set of equivalence classes

$$\left\{ \tfrac{a}{b} \,\middle|\, a \in R,\, b \in R \setminus \{0\} \right\}$$

under the relation $\sim$ defined above is called the *field of fractions of R*, and is denoted by $\mathrm{Frac}(R)$.

The operations on $\mathrm{Frac}(R)$ are defined by

$$\begin{aligned} \tfrac{a}{b} + \tfrac{c}{d} &= \tfrac{ad+bc}{bd}, \\ \tfrac{a}{b} \cdot \tfrac{c}{d} &= \tfrac{ac}{bd}, \end{aligned}$$

for $a, c \in R$ and $b, d \in R \setminus \{0\}$. With these operations, $\mathrm{Frac}(R)$ is a field (Definition 2.1.10).

Equivalently, $\mathrm{Frac}(R)$ may be defined as the localization of R (Definition 2.2.37) by the multiplicative subset $R \setminus \{0\}$ (Definition 2.2.36).

Definition 2.1.13. Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be rings (Definition 2.1.1), not assumed to be commutative. A function $f : R \to S$ is called a *ring homomorphism* if for all $r_1, r_2 \in R$ the following properties hold:

1. $f(r_1 + r_2) = f(r_1) + f(r_2)$,
2. $f(r_1 r_2) = f(r_1) f(r_2)$,
3. $f(1_R) = 1_S$ where 1_R and 1_S denote the multiplicative identities in R and S, respectively.

A ring homomorphism is said to be a *ring isomorphism* if it is invertible as a map of sets.

An *R-ring* refers to a ring S equipped with a ring homomorphism $f : R \to S$.

We note that a ring homomorphism $f : R \to S$ yields a natural left R-module (Definition 2.2.1) structure on S and a natural right R-module structure on S respectively as follows for $r \in R$ and $s \in S$:

$$r \cdot s = f(r) \cdot s$$

$$s \cdot r = s \cdot f(r).$$

However, these left and right module structures need not yield a two-sided R–module structure.

Definition 2.1.14.

1. The *category of rings* is the locally small (Definition A.4.3) category (Definition A.4.1) whose objects are rings (Definition 2.1.1) R and whose morphisms $R \to S$ are ring homomorphisms (Definition 2.1.13). The category of rings over R is often denoted by notations such as **Ring**.
2. The *category of commutative rings* is the full subcategory (Definition A.4.10) of **Ring** consisting of the commutative rings (Definition 2.1.4). It is denoted by notations such as **CommRing** or **CRing**.

Definition 2.1.15.

1. Let R be a not necessarily commutative ring (Definition 2.1.1). The *category of rings over R* or the *category of R-rings* is the locally small (Definition A.4.3) category (Definition A.4.1) whose objects are R-rings (Definition 2.1.13) $(S,\ \varphi)$ and whose morphisms $(S_1, \varphi_1) \to (S_2, \varphi_2)$ are given by ring homomorhpisms $\psi : S_1 \to S_2$ such that $\varphi_2 = \psi \circ \varphi_1$.

$$\begin{tikzcd} & R \arrow[dl, "\varphi_1"'] \arrow[dr, "\varphi_2"] & \\ S_1 \arrow[rr, "\psi"'] & & S_2 \end{tikzcd}$$

   Equivalently, the category of R-rings is the category of objects under (Definition A.4.8) the object S in the category of rings (Definition 2.1.14). The category of rings over R is often denoted by notations such as $\mathbf{Ring}_R$.
2. The category of commutatative R-rings is the full subcategory of $\mathbf{Ring}_R$ consisting of the R-rings (A, φ) such that A is a commutative ring. It is denoted by notations such as $\mathbf{CommRing}_R$ or $\mathbf{CRing}_R$.

Lemma 2.1.16. The category of rings (Definition 2.1.14) is equivalent (Definition A.4.7) to the category of $\mathbb{Z}$-rings (Definition 2.1.15).

Lemma 2.1.17. Let R be a not necessarily commutative ring (Definition 2.1.1). The category $\mathbf{Ring}_R$ (Definition 2.1.15) of rings over R has an initial object (Definition A.4.9), namely R equipped with the identity morphism.

Definition 2.1.18. Let R be a (not-necessarily commutative) ring with unity (Definition 2.1.1). An *R-algebra* is a ring A together with a ring homomorphism (Definition 2.1.13)

$$\varphi : R \to A$$

into the center $Z(A)$ (Definition 2.1.5) of A (so that $\varphi(r)$ commutes with every element of A for all $r \in R$), such that $\varphi(1_R) = 1_A$. The ring homomorphism φ is called the *structure map* of the algebra.

Equivalently, an R-algebra consists of a ring A endowed with a two-sided R-module (Definition 2.2.1) structure for which the scalar multiplication satisfies

$$r \cdot (ab) = (r \cdot a)b = a(r \cdot b) \quad \text{for all } r \in R,\ a, b \in A.$$

In particular, any ring homomorphism between commutative rings (Definition 2.1.4) specifies an algebra structure.

Definition 2.1.19.

1. Let R be a not necessarily commutative ring (Definition 2.1.1). The *category of algebras over R* or the *category of R-algebras* is the locally small (Definition A.4.3) category (Definition A.4.1) whose objects are R-algebras (Definition 2.1.18) (A, φ) and whose morphisms $(A_1, \varphi_1) \to (A_2, \varphi_2)$ are given by ring homomorphisms $\psi : A_1 \to A_2$ such that $\varphi_2 = \psi \circ \varphi_1$.

$$\begin{tikzcd} & R \arrow[dl, "\varphi_1"'] \arrow[dr, "\varphi_2"] & \\ A_1 \arrow[rr, "\psi"'] & & A_2 \end{tikzcd}$$

In other words, the category of R-algebras is the full subcategory (Definition A.4.10) of the category of R-rings (Definition 2.1.15) whose objects are the R-algebras.

The category of algebras over R is often denoted by notations such as $\mathbf{Alg}_R$ or R-$\mathbf{Alg}$.

2. The *category of commutative R-algebras* is the full subcategory of $\mathbf{Alg}_R$ consisting of those R-algebras (A, φ) for which A is a commutative ring. It is often denoted by $\mathbf{CAlg}_R$ or $\mathbf{CommAlg}_R$.

Definition 2.1.20. Let R be a commutative ring (Definition 2.1.4) and let (A, φ) be an R-algebra (Definition 2.1.18). The algebra A is called a *central R-algebra* if the structure map $\varphi : R \to Z(A)$ induces an isomorphism (Definition 2.1.13) between R and the center of A (Definition 2.1.5). Specifically, this requires two conditions:

1. The map φ is surjective onto $Z(A)$, meaning $Z(A) = \varphi(R)$.
2. The map φ is injective (faithful), so $R \cong \varphi(R)$.

In other words, A is central if $Z(A) \cong R$ via the structure map.

Definition 2.1.21 (Subalgebra of an algebra over a ring)**.** Let R be a (not necessarily commutative) ring (Definition 2.1.1) and let A be an R-algebra (Definition 2.1.18).

A subset $B \subseteq A$ is an *R-subalgebra* if:

- B is a subring of A (Definition 2.1.25),
- B is closed under scalar multiplication by R, i.e., for all $r \in R$ and $b \in B$, we have $r \cdot b \in B$.

In particular, B inherits the structure of an R-algebra as a subobject of A.

Definition 2.1.22 (Subalgebra generated by a subset)**.** Let R be a (not necessarily commutative) ring (Definition 2.1.1) and let A be an R-algebra (Definition 2.1.18). Given a subset $S \subseteq A$, the *subalgebra of A generated by S*, denoted by notations such as $\langle S \rangle = \langle S \rangle_R$, is the smallest R-subalgebra (Definition 2.1.21) of A that contains S.

Explicitly, the *subalgebra generated by S* is the intersection

$$\langle S \rangle_R = \bigcap_{T \subseteq S \text{ subalgebra}} T$$

of all R-subalgebras of A containing S. Equivalently, it consists of all R-linear combinations of finite products of elements from S and from the multiplicative identity element 1_A.

In case that R and A are both commutative, the subalgebra generated by S may be denoted by notations such as $R[S]$.

Definition 2.1.23 (Free associative algebra over a ring)**.** Let R be a (not necessarily commutative) ring (Definition 2.1.1), and let $\{x_i\}_{i \in I}$ be a set of formal variables indexed by a set I.

The *free associative R-algebra on the variables* $\{x_i\}_{i \in I}$, denoted by notations such as $R\langle x_i \mid i \in I \rangle$ or $R\langle x_i \rangle_{i \in I}$, is defined as the R-algebra (Definition 2.1.18) whose underlying R-module is freely generated by all finite words in the letters x_i (including the empty word, which acts as the multiplicative unit), with multiplication given by concatenation of words extended R-linearly.

Equivalently, $R\langle x_i \mid i \in I\rangle$ is the noncommutative polynomial ring generated by the x_i over R, satisfying no relations other than those required by the ring and algebra axioms.

In the case that I is a finite set, and writing $y_1, \ldots, y_n$ for the variables x_i, it is customary to let $R\langle y_1, \ldots, y_n\rangle$ denote the free associative R-algebra.

Definition 2.1.24 (Polynomial ring over a commutative ring)**.** Let R be a commutative ring (Definition 2.1.4). For a set of variables $\{x_i\}_{i\in I}$, the *polynomial ring in variables $\{x_i\}$ over R*, denoted by notations such as $R[x_i \mid i \in I]$ or $R[x_i]_{i\in}$, is defined as the commutative R-algebra (Definition 2.1.18) whose elements are finite R-linear combinations of monomials in the variables x_i, where the variables commute with each other and with elements of R.

That is, $R[x_i \mid i \in I]$ is the free commutative R-algebra generated by the set $\{x_i\}$.

In the case that I is a finite set, and writing $y_1, \ldots, y_n$ for the variables x_i, it is customary to let $R[y_1, \ldots, y_n]$ denote the polynomial ring.

Definition 2.1.25 (Subring)**.** Let R be a not necessarily commutative ring (Definition 2.1.1). A subset $S \subseteq R$ is called a *subring of R* if:

- S is itself a ring with the same operations as R (addition and multiplication inherited from R),
- the multiplicative identity 1_R of R is contained in S,
- and the additive identity 0_R of R is contained in S.

Equivalently, $S \subseteq R$ is a subring if S is nonempty, closed under addition, multiplication, and additive inverses, and contains 1_R.

Definition 2.1.26. Let R be a not necessarily commutative ring (Definition 2.1.1). A *extension ring of R* is an R-algebra A such that the ring homomorphism $R \to A$ is an injection (Definition A.1.3). We also say that A/R is an *extension of rings*.

In this case, the image of $R \to A$ is a subring (Definition 2.1.25) of A isomorphic (Definition 2.1.13) to R; we often identify R with this image to consider R as a subring of A.

2.2. **Modules of a ring.**

Definition 2.2.1. Let R be a not-necessarily commutative ring (Definition 2.1.1).

1. A *left R-module* is an abelian group $(M, +)$ together with an operation $R \times M \to M$, denoted $(r, m) \mapsto rm$, such that for all $r, s \in R$ and $m, n \in M$:
    - $r(m + n) = rm + rn$,
    - $(r + s)m = rm + sm$,
    - $(rs)m = r(sm)$,
    - $1_R m = m$ where 1_R is the multiplicative identity of R.

2. A *right R-module* is defined similarly as an abelian group $(M, +)$ with an operation $M \times R \to M$, denoted $(m, r) \mapsto mr$, such that for all $r, s \in R$ and $m, n \in M$:
   - $(m + n)r = mr + nr$,
   - $m(r + s) = mr + ms$,
   - $m(rs) = (mr)s$,
   - $m1_R = m$.
3. Let R and S be (not necessarily commutative) rings (Definition 2.1.1).

   An *R-S-bimodule* (or an *R-S-module* or an (R, S)-module, etc.)is an abelian group (Definition 1.1.1) $(M, +)$ equipped with
   (a) a left action of R:
   $$R \times M \to M, \quad (r, m) \mapsto r \cdot m,$$
   making M a left R-module (Definition 2.2.1),
   (b) a right action of S:
   $$M \times S \to M, \quad (m, s) \mapsto m \cdot s,$$
   making M a right S-module,

   such that the left and right actions commute; that is, for all $r \in R$, $s \in S$, and $m \in M$,
   $$r \cdot (m \cdot s) = (r \cdot m) \cdot s.$$
4. A *two-sided R-module* (or *R-bimodule*) is an R-R-bimodule.

If R is a commutative ring (Definition 2.1.4), then a left/right R-module can automatically be regarded as a two-sided R-module. As such, we simply talk about *R-modules* in this case.

Any abelian group is equivalent to a two-sided $\mathbb{Z}$-module. Moreover, any left R-module is equivalent to an $R - \mathbb{Z}$-bimodule (Definition 2.2.1) and any right R-module is equivalent to an $\mathbb{Z} - R$-bimodule (Definition 2.2.1). Given a left/right/two-sided R-module, its *natural bimodule structure* will refer to its structure as a R-$\mathbb{Z}$/$\mathbb{Z}$-R/R-R bimodule. In this way, many definitions associated with the notions of left/right/two-sided R-modules can be defined as special cases for definitions for R-S-bimodules.

Definition 2.2.2. Let R, S be not-necessarily commutative rings (Definition 2.1.1).

1. Let M be an R-S-bimodule whose abelian group (Definition 1.1.1) structure is given by the operator $+$. An *R-S-submodule of M* is a subgroup (Definition 1.1.5) $N \subseteq (M, +)$ if for all $r \in R$, $s \in S$, and $n \in N$, we have $rn \in N$ and $ns \in N$; in this case, N inherits an R-S bimodule structure from M.
2. If M is a left/right/two-sided R-module, then a *left/right/two-sided R-submodule of M* is a submodule of the natural bimodule structure (Definition 2.2.1) of M.

A submodule of M is a categorical subobject (Definition A.4.24) of M in the appropriate category of modules.

Definition 2.2.3. Let R, S be (not-necessarily commutative) rings (Definition 2.1.1).

1. Let M and N be R-S-bimodules (Definition 2.2.1). A function $\varphi : M \to N$ is called an *R-S-bimodule homomorphism* or *R-S-linear* if it is a group homomorphism (Definition 1.1.3) of the underlying abelian groups of M and N and respects the scalar actions as follows: for all $m_1, m_2 \in M$, $r \in R$, and $s \in S$,

$$\begin{aligned} \varphi(r \cdot m_1) &= r \cdot \varphi(m_1), \\ \varphi(m_1 \cdot s) &= \varphi(m_1) \cdot s. \end{aligned}$$

2. Let M and N be left/right/two-sided R-modules (Definition 2.2.1). A function $\varphi : M \to N$ is called a *left/right/two-sided R-module homomorphism* if it is an bimodule homomorphism on the natural bimodule structures (Definition 2.2.1) of M and N. Such a function is also called *R-linear*.

Modules and homomorphisms of a fixed type (i.e. R-S-bimodules or left/righ/two-sided R-modules) form a locally small (Definition A.4.3) category (Definition A.4.1).

Definition 2.2.4. Let R and S be (not necessarily commutative) rings (Definition 2.1.1).

1. The *category of (R, S)-bimodules* (or R-S-bimodules), denoted by ${}_R\mathsf{Mod}_S$, is the category whose objects are (R, S)-bimodules (Definition 2.2.1) and whose R-S-bimodule homomorphisms (Definition 2.2.3).
2. The *category of left R-modules*, denoted by ${}_R\mathsf{Mod}$, is the category ${}_R\mathsf{Mod}_{\mathbb{Z}}$, i.e. the category whose objects are left R-modules (Definition 2.2.1) and whose morphisms are left R-linear maps (Definition 2.2.3).
3. The *category of right R-modules*, denoted by ${}_R\mathsf{Mod}$, is the category ${}_R\mathsf{Mod}_{\mathbb{Z}}$, i.e. the category whose objects are right R-modules (Definition 2.2.1) and whose morphisms are right R-linear maps (Definition 2.2.3).

The category of bimodules can be canonically identified with module categories over tensor product rings (Definition 2.2.40):

- ${}_R\mathsf{Mod}_S$ is isomorphic to the category of left modules over the ring $R \otimes_{\mathbb{Z}} S^{\mathrm{op}}$.
- ${}_R\mathsf{Mod}_S$ is isomorphic to the category of right modules over the ring $R^{\mathrm{op}} \otimes_{\mathbb{Z}} S$.

Consequently, standard module-theoretic concepts (such as projective objects, injective objects, and flat objects) in ${}_R\mathsf{Mod}_S$ correspond exactly to the respective concepts in ${}_{R \otimes S^{\mathrm{op}}}\mathsf{Mod}$.

Relation to One-Sided Modules. Note that there are canonical isomorphisms of categories:

$${}_R\mathsf{Mod} \cong {}_R\mathsf{Mod}_{\mathbb{Z}} \quad \text{and} \quad \mathsf{Mod}_S \cong {}_{\mathbb{Z}}\mathsf{Mod}_S.$$

That is, left R-modules are exactly $(R, \mathbb{Z})$-bimodules, and right S-modules are exactly $(\mathbb{Z}, S)$-bimodules.

2.2.1. *Linear combinations, spanning, and linear indepencence for modules over rings.*

Definition 2.2.5. Let R, S be (not-necessarily commutative) rings (Definition 2.1.1).

1. Let M be a R-S-bimodule (Definition 2.2.1). Given elements $x_1, \ldots, x_n \in M$, $r_1, \ldots, r_n \in R$, and $s_1, \ldots, s_n \in R$, an element of the form
$$\sum_{i=1}^{n} r_i x_i s_i \in M$$
is called a *(R-S-)linear combination of $x_1, \ldots, x_n$*. Given an arbitrary subset $\{m_i\}_{i \in I} \subseteq M$, a *(R-S-)linear combination of the m_i over R* refers to a linear combination of some finite subset of $\{m_i\}_{i \in I}$ over R.
2. Let M be a left/right/two-sided R-module (Definition 2.2.1). A *llinear combination of elements $\{m_i\}_{i \in I} \subseteq M$* refers to a linear combination of (a finite subset of) $\{m_i\}_{i \in I}$ for the natural bimodule structure (Definition 2.2.1) of M. In case that M is a left/right R-module, and given finitely many $m_1, \ldots, m_n \in M$, a linear combination of these m_i is equivalently an element of the form
$$r_1 x_1 + r_2 x_2 + \cdots + r_n x_n$$
$$x_1 r_1 + x_2 r_2 + \cdots + x_n r_n$$
for $r_1, \ldots, r_n \in R$ respectively.

Definition 2.2.6 (Submodule generated by elements in an (R, S)-bimodule)**.** Let R and S be (not necessarily commutative) rings (Definition 2.1.1).

1. Let M be an (R, S)-bimodule (Definition 2.2.1).

   Given a subset $X \subseteq M$, the *sub-bimodule of M generated by X* is the smallest (R, S)-sub-bimodule of M containing X. It is often denoted by notations such as $\langle X \rangle = \langle X \rangle_{R,S}$ and is more explicitly the intersection
$$\langle X \rangle_{R,S} = \bigcap_{X \subseteq T \subseteq M, T \text{ is a } (R,S)\text{-submodule of } M} T$$
of al (R, S)-submodules of M containing X.

   Equivalently, $\langle X \rangle_{R,S}$ consists of all linear combinations (Definition 2.2.5) of X.
2. If M is a left/right/two-sided R-module and given a subset $X \subseteq M$, the *submodule of M generated by X* is the submodule of the natural bimodule (Definition 2.2.1) of M generated by X. It is denoted by notations such as $\langle X \rangle = \langle X \rangle_R$.

Definition 2.2.7. Let R be a (not necessarily commutative) ring (Definition 2.1.1) and let M be an R-module (Definition 2.2.1).

1. If M is a left R-module (Definition 2.2.1), a finite subset $S = \{x_1, \ldots, x_n\} \subseteq M$ is said to be *linearly independent over R* if, whenever $r_1, \ldots, r_n \in R$ satisfy
$$r_1 x_1 + r_2 x_2 + \cdots + r_n x_n = 0,$$
it follows that each $r_i = 0$.
2. If M is a right R-module (Definition 2.2.1), a finite subset $S = \{x_1, \ldots, x_n\} \subseteq M$ is said to be *linearly independent over R* if, whenever $r_1, \ldots, r_n \in R$ satisfy
$$x_1 r_1 + x_2 r_2 + \cdots + x_n r_n = 0,$$
it follows that each $r_i = 0$.

3. If M is a two-sided R-module (Definition 2.2.1), a finite subset $S = \{x_1, \dots, x_n\} \subseteq M$ is said to be *linearly independent over R* if, whenever $r_1, \dots, r_n, s_1, \dots, s_n \in R$ satisfy

$$r_1 x_1 s_1 + r_2 x_2 s_2 + \cdots + r_n x_n s_n = 0,$$

   it follows that each $r_i s_i = 0$ in R. Equivalently, no nontrivial pair of coefficient actions on the x_i yields the zero element of M.

An arbitrary subset $S \subseteq M$ is *linearly independent over R* if every finite subset of S is linearly independent.

Definition 2.2.8. Let R and S be (not necessarily commutative) rings (Definition 2.1.1).

1. If M is an R-S-bidmodule (Definition 2.2.1), then a subset $\{m_i\}_{i \in I} \subseteq M$ is said to *span M (as an R-S-bimodule)* if every element $m \in M$ is a linear combination (Definition 2.2.5) of $\{m_i\}_{i \in I}$.
2. If M is a left/right/two-sided R-module, then a subset $\{m_i\}_{i \in I} \subseteq M$ is said to *span M (as a left/right/two-sided R-module)* if $\{m_i\}_{i \in}$ spans its natural bimodule structure (Definition 2.2.1).

In each case, such a set $\{m_i\}_{i \in I}$ is called a *generating set* or *spanning set of M over R*.

In each case, such a set S is called a *generating set* or *spanning set of M over R*.

Definition 2.2.9 (Finitely generated modules and bimodules)**.** Let R and S be (not necessarily commutative) rings (Definition 2.1.1).

1. An R-S-bimodule M is *finitely generated* if it has a finite spanning set (Definition 2.2.8).
2. A left/right/two-sided R-module is *finitely generated* if has a finite spanning set (Definition 2.2.8), or equivalently if its natural bimodule structure (Definition 2.2.1) is finitely generated.

2.2.2. *Categories of modules as abelian categories.*

Definition 2.2.10 (Additive category)**.** Let $\mathcal{A}$ be a locally small category (Definition A.4.3).

1. $\mathcal{A}$ is said to be a *preadditive category* if the following hold:
   - For any two objects A, B in $\mathcal{A}$, the set $\mathrm{Hom}_{\mathcal{A}}(A, B)$ is an abelian group (Definition 1.1.1), and composition of morphisms is bilinear.
   - There is a zero object (Definition A.4.9) 0 in $\mathcal{A}$.
2. If $\mathcal{A}$ is preadditive, then it is called *additive* if it additionally satisfies the following:
   - For any two objects A, B in $\mathcal{A}$, there exists a product object $A \times B$ (Definition A.4.21), often written $A \oplus B$, called the *direct sum of A and B*. In fact, $A \oplus B$ is not only a product but also a coproduct (Definition 2.2.17) of A and B (Lemma A.5.7).

   Given a finite collection $\{A_i\}_i$ of objects A_i in an additive category $\mathcal{A}$, we may more generally speak of the *direct sum* $\bigoplus_i A_i$; it has canonical injections from and projections to each A_i.

Definition 2.2.11 (Additive functor)**.**

1. Let $\mathcal{A}$ and $\mathcal{B}$ be pre-additive categories. A functor
$$F : \mathcal{A} \to \mathcal{B}$$
is an *additive functor* if for every pair of objects $A, A' \in \mathcal{A}$, the induced map
$$F_{A,A'} : \mathrm{Hom}_{\mathcal{A}}(A, A') \to \mathrm{Hom}_{\mathcal{B}}(F(A), F(A'))$$
is a group homomorphism of abelian groups, or equvialently if it is enriched over the category Ab of abelian groups.
2. Let $\mathcal{A}$ and $\mathcal{B}$ be additive categories. A functor
$$F : \mathcal{A} \to \mathcal{B}$$
is an *additive functor* if it an additive functor of pre-additive categories and satisfies the following:
   - F sends the zero object $0_{\mathcal{A}}$ of $\mathcal{A}$ to the zero object $0_{\mathcal{B}}$ of $\mathcal{B}$, i.e.,
$$F(0_{\mathcal{A}}) = 0_{\mathcal{B}}.$$
   - F preserves finite direct sums: For any finite family of objects $\{A_i\}_{i=1}^{n}$ in $\mathcal{A}$,
$$F\left(\bigoplus_{i=1}^{n} A_i\right) \cong \bigoplus_{i=1}^{n} F(A_i)$$
via the canonical isomorphism induced by F applied to the canonical injections and projections.

   In other words, F is a functor that is compatible with the additive structures on $\mathcal{A}$ and $\mathcal{B}$.

Definition 2.2.12 (Abelian category)**.** Let $\mathcal{A}$ be a category. The category $\mathcal{A}$ is an *abelian category* if:

- $\mathcal{A}$ is an additive category (Definition 2.2.10).
- Every morphism $f : A \to B$ has a kernel $\ker(f)$ and a cokernel $\mathrm{coker}(f)$ (Definition A.4.14).
- For every morphism $f : A \to B$, the canonical morphism $\mathrm{coim}(f) \to \mathrm{im}(f)$ is an isomorphism, where
$$\mathrm{coim}(f) = \mathrm{coker}(\ker(f) \to A), \quad \mathrm{im}(f) = \ker(B \to \mathrm{coker}(f)).$$
(♠ TODO: I think I need to re-check this defintion) (♠ TODO: coimage)

It is also worth considering Grothendieck's additional axioms for abelian categories (Definition 2.2.13).

Definition 2.2.13 (Grothendieck's axioms for abelian categories (Ab1–Ab5))**.** Let $\mathcal{A}$ be an abelian category (Definition 2.2.12).

Grothendieck introduced the following hierarchy of additional axioms to express stronger completeness and exactness properties in $\mathcal{A}$ — we note that Ab1, Ab2, and Ab2* are already satisfied for any abelian category:

- *Ab1*: Every morphism in $\mathcal{A}$ has a kernel and a cokernel (Definition A.4.14).

- *Ab2*: Every monic (Definition A.4.23) in $\mathcal{A}$ is the kernel of its cokernel.
- *Ab2**: Every epi in $\mathcal{A}$ is the cokernel of its kernel.
- *AB3*: The category $\mathcal{A}$ is cocomplete (Definition A.4.16).
  - Since $\mathcal{A}$ is abelian (hence has finite colimits), this is equivalent to requiring that $\mathcal{A}$ has all small coproducts (Definition A.4.21) (direct sums).
- *AB4*: The category $\mathcal{A}$ satisfies AB3, and coproducts are *exact*.
  - That is, the coproduct of a family of short exact sequences is a short exact sequence. Explicitly, for any family of short exact sequences $0 \to A_i \to B_i \to C_i \to 0$ indexed by a set I, the sequence

    $$0 \to \bigoplus_{i\in I} A_i \to \bigoplus_{i\in I} B_i \to \bigoplus_{i\in I} C_i \to 0$$

    is exact in $\mathcal{A}$.
- *AB5*: The category $\mathcal{A}$ satisfies AB3, and filtered colimits (Definition A.4.20) are *exact*.
  - Equivalently, for any filtered (Definition A.4.17) index category J and any directed system (Definition A.4.18) of short exact sequences $0 \to A_j \to B_j \to C_j \to 0$, the colimit sequence

    $$0 \to \varinjlim A_j \to \varinjlim B_j \to \varinjlim C_j \to 0$$

    is exact.
  - Note: AB5 implies AB4. An abelian category satisfying AB5 and having a generator (Definition 2.2.14) is called a *Grothendieck category*.
- *AB6*: The category $\mathcal{A}$ satisfies AB3, and for any object X and any family of filtered subobjects $\{F_i\}_{i\in I}$ of X (where each F_i is a filter of subobjects), the intersection commutes with the limit:

  $$\bigcap_{i\in I}(\varinjlim_{j\in F_i} U_{i,j}) = \varinjlim_{(j_i)\in\prod F_i} (\bigcap_{i\in I} U_{i,j_i}).$$

  (This axiom is less commonly cited but appears in Grothendieck's Tohoku paper).
- *AB3**: The category $\mathcal{A}$ is complete (Definition A.4.16) (i.e., has all small products).
- *AB4**: The category $\mathcal{A}$ satisfies AB3* and products are exact.
  - Note: This is rarely satisfied for module categories (e.g., it fails for Abelian groups), but it is satisfied for the category of sheaves on a space.
- *AB5**: The category $\mathcal{A}$ satisfies AB3* and filtered limits (inverse limits) are exact.

Notes:

- AB5 implies AB4, and AB4 implies AB3.
- AB5* implies AB4*, and AB4* implies AB3*.

Definition 2.2.14 (Generator of a category)**.** Let $\mathcal{C}$ be a category (Definition A.4.1).

1. An object $G \in \mathcal{C}$ is called a *generator* (or *separator*) if for every pair of distinct morphisms $f, g : X \to Y$ in $\mathcal{C}$, there exists a morphism $h : G \to X$ such that

   $$f \circ h \neq g \circ h.$$

In case that $\mathcal{C}$ is locally small (Definition A.4.3), this is equivalent to the condition that the representable functor

$$\mathrm{Hom}_{\mathcal{C}}(G, -) : \mathcal{C} \to \mathbf{Set}$$

is faithful (Definition A.4.26), which in turn is equivalent to the condition that for every object $X \in \mathcal{C}$, there exists an epimorphism

$$\bigoplus_{i \in I} G \twoheadrightarrow X$$

for some indexing set I, where $\bigoplus$ denotes the coproduct (Definition A.4.21) in $\mathcal{C}$.

2. A family $\{G_i\}_{i \in I}$ is called a *generating family* if for every pair of distinct morphisms $f, g : X \to Y$ in $\mathcal{C}$, there exists some index $i \in I$ and a morphism $h : G_i \to X$ such that

$$f \circ h \neq g \circ h.$$

In case $\mathcal{C}$ is locally small, this is equivalent to the condition that the collection of representable functors

$$\{\mathrm{Hom}_{\mathcal{C}}(G_i, -) : \mathcal{C} \to \mathbf{Set}\}_{i \in I}$$

is jointly faithful, which in turn is equivalent to the condition that for every object $X \in \mathcal{C}$, there exists a family of objects $\{G_i\}_{i \in J}$ from the generating set indexed by some set J, and an epimorphism

$$\bigoplus_{i \in J} G_i \twoheadrightarrow X.$$

Definition 2.2.15 (Hom of left/right/bi-modules)**.** Let R, S, T be (not necessarily commutative) rings (Definition 2.1.1).

1. Let M and N be left R-modules (Definition 2.2.1). The *homomorphism group of left R-modules from M to N* is the abelian group

$$\mathrm{Hom}(M, N) = \mathrm{Hom}_R(M, N) := \{f : M \to N \mid f \text{ is a left } R\text{-module homomorphism}\}.$$

(Definition 2.2.3)

2. Let M and N be right R-modules (Definition 2.2.1). The *homomorphism group of right R-modules from M to N* is the abelian group

$$\mathrm{Hom}(M, N) = \mathrm{Hom}_R(M, N) := \{f : M \to N \mid f \text{ is a right } R\text{-module homomorphism}\}.$$

3. Let S be a (not necessarily commutative ring) and let M and N be $R - S$-bimodules (Definition 2.2.1). The *homomorphism group of R-S-bimodules from M to N* is the abelian group

$$\mathrm{Hom}(M, N) = \mathrm{Hom}_{R-S}(M, N) \coloneqq \{f : M \to N | f \text{ is a } R - S\text{-bimodule homomorphism}\}$$

In each case, $\mathrm{Hom}(M, N)$ has a natural structure of an *abelian group* given by *pointwise addition*: for $f, g \in \mathrm{Hom}(M, N)$,

$$(f + g)(m) := f(m) + g(m),$$

and the zero morphism 0 given by $0(m) := 0_N$ acts as the identity element. The additive inverse $-f$ is defined by $(-f)(m) := -f(m)$. Moreover, depending on bi-module structures that M and N may be carrying, $\mathrm{Hom}(M, N)$ may itself carry additional module structures:

- In case that M is a $R - S$-bimodule and N is a $R - T$-bimodule, $\mathrm{Hom}_R(M, N)$, the group of left R-module homomorphisms, is an $S - T$-bimodule as follows:
$$(s \cdot f \cdot t)(m) = f(m \cdot s) \cdot t \quad f \in \mathrm{Hom}_R(M, N), s \in S, t \in T.$$
- Dually, in case that M is a $S - R$-bimodule and N is a $T - R$-bimodule, $\mathrm{Hom}_R(M, N)$, the group of right R-module homomorphisms, is an $S - T$-bimodule as follows:
$$(s \cdot f \cdot t)(m) = f(s \cdot m) \cdot t \quad f \in \mathrm{Hom}_R(M, N), s \in S, t \in T.$$

Some cases of interest may be when R, S, or T is in fact $\mathbb{Z}$ — these allow us to see module structures on $\mathrm{Hom}(M, N)$ even when M and N are one-sided modules.

(♠ TODO: state this as a theorem) We furthermore note that $\mathrm{Hom}_R(-, -)$ yields biadditive functors (Definition A.5.1)

$$\mathrm{Hom}_R(-, -) : {}_R\mathbf{Mod}_S^{\mathrm{op}} \times {}_R\mathbf{Mod}_T \to {}_S\mathbf{Mod}_T$$
$$\mathrm{Hom}_R(-, -) : {}_S\mathbf{Mod}_R^{\mathrm{op}} \times {}_T\mathbf{Mod}_R \to {}_S\mathbf{Mod}_T.$$

(Definition A.4.12) (Definition 2.2.4) (Theorem 2.2.21)

Definition 2.2.16 (Product of Modules)**.** Let R and S be (not necessarily commutative) rings (Definition 2.1.1), and let $\{M_i\}_{i \in I}$ be a (possibly infinite (Definition A.1.5) but small (Definition A.1.1)) family of (R, S)-bimodules (Definition 2.2.1).

left R-modules, of right R-modules, of two-sided R-modules (Definition 2.2.1), or of

The *(direct) product of the family* $\{M_i\}_{i \in I}$ is defined, as a group (Definition 1.1.1), as the product of sets (Definition 1.2.1):

$$\prod_{i \in I} M_i := \{(m_i)_{i \in I} \mid m_i \in M_i \text{ for all } i \in I\}.$$

$\prod_{i \in I} M_i$ inherits a natural R-S module structure defined componentwise by the following rules for all $(m_i)_{i \in I}, (n_i)_{i \in I} \in \prod_{i \in I} M_i$ and all scalars $r \in R$, $s \in S$:

$$(m_i)_{i \in I} + (n_i)_{i \in I} := (m_i + n_i)_{i \in I}, \qquad r \cdot (m_i)_{i \in I} \cdot s := (r \cdot m_i \cdot s)_{i \in I}.$$

The zero element of $\prod_{i \in I} M_i$ is the tuple $(0)_{i \in I}$, and additive inverses are given componentwise:

$$-(m_i)_{i \in I} := (-m_i)_{i \in I}.$$

Note that we can define the product of a family $\{M_i\}_{i \in I}$ of left/right/two-sided R-modules by taking the natural bimodule structure (Definition 2.2.1) of each module.

As usual (Definition 1.2.1), $\prod_{i \in I} M_i$ is the categorical product (Definition A.4.21) of the objects M_i in the appropriate category of modules (Definition 2.2.4). Moreover, the product of finitely many modules $M_1, \ldots, M_n$ is often written as $M_1 \times \cdots \times M_n$, which agrees with notation for the product of finitely many groups (Definition 1.2.1). We often write the self-product of a module M indexed by a (small) set I as M^I or by $M^{\oplus I}$. A finite self-product of a module M taken n times is often denoted by M^n or $M^{\oplus n}$; note that these all agree with the notations for abelian groups.

Definition 2.2.17 (Coproduct of Modules)**.** Let R and S be (not necessarily commutative) rings (Definition 2.1.1), and let $\{M_i\}_{i\in I}$ be a (possibly infinite but small) family of (R, S)-bimodules.

The *coproduct (direct sum) of the family* $\{M_i\}_{i\in I}$, denoted by $\bigoplus_{i\in I} M_i$, is constructed as

$$\bigoplus_{i\in I} M_i := \left\{ (m_i)_{i\in I} \in \prod_{i\in I} M_i \mid m_i = 0 \text{ for all but finitely many } i \in I \right\}$$

(Definition 2.2.16) consisting of all tuples with only finitely many nonzero entries.

Addition and scalar multiplication in $\bigoplus_{i\in I} M_i$ are defined componentwise as in the direct product (Definition 2.2.16):

$$(m_i)_{i\in I} + (n_i)_{i\in I} := (m_i + n_i)_{i\in I}, \qquad r \cdot (m_i)_{i\in I} \cdot s := (r \cdot m_i \cdot s)_{i\in I}, \qquad r \in R,\ s \in S.$$

In all cases, the zero element is $(0)_{i\in I}$, and additive inverses are given by $-(m_i)_{i\in I} := (-m_i)_{i\in I}$.

Note that we can define the coproduct of a family $\{M_i\}_{i\in I}$ of left/right/two-sided R-modules by taking the natural bimodule structure (Definition 2.2.1) of each module.

(♠ TODO: submodule) Note that $\bigoplus_{i\in I} M_i$ is a submodule of $\prod_{i\in I} M_i$. Moreover, $\bigoplus_{i\in I} M_i$ is the coproduct (Definition A.4.21) in the appropriate category of modules (Definition 2.2.4).

For finitely many modules $M_1, \ldots, M_n$, the direct sum $\bigoplus_{j=1}^{n} M_j$, which may also be written as $M_1 \oplus \cdots \oplus M_n$, is simply the usual Cartesian product $\prod_{j=1}^{n} M_j$ (Definition 2.2.16) of the modules, as every tuple automatically has only finitely many nonzero entries.

Definition 2.2.18. (♠ TODO: define coset, kernel of R-module homomorphism) Let R, S be (not necessarily commutative) rings (Definition 2.1.1).

1. Let M be an R-S-bimodule (Definition 2.2.1). Let $N \subseteq M$ be a submodule of M (Definition 2.2.2).

   The quotient group M/N (Definition 1.1.13), which is well defined as M is an abelian group (Definition 1.1.1) and hence N is a normal subgroup (Definition 1.1.9) (Proposition 1.1.20), has the structure of an R-S-bimodule — the (abelian) group structure is simply the group structure of M/N, whereas the R-S-bimodule structure is given as follows: for $m \in M$, $r \in R$, $s \in S$, we have

   $$r \cdot (m + N) \cdot s = r \cdot m \cdot s + N.$$

   This R-S-bidmodule structure on M/N is called the *quotient R-S-bidmodule of M by N* and is also denoted as M/N.

   The canonical projection map

   $$\pi : M \to M/N, \quad m \mapsto m + N,$$

is a surjective R-module homomorphism (Definition 2.2.3) with kernel N.

2. Let M be a left/right/two-sided R-module. Let $N \subseteq M$ be a submodule of M. The *quotient R-module* M/N is the quotient of M by N for their respective natural bimodule structures (Definition 2.2.1).

The quotient M/N is the categorical quotient object (Definition A.4.25) of M by the subobject (Definition A.4.24) N in the appropriate category of modules

Definition 2.2.19. Let R, S be (not-necessarily commutative) rings with unity (Definition 2.1.1), and let M, N be R-S-bimodules (Definition 2.2.1). Let

$$\varphi : M \to N$$

be a homomorphism of R-S-bimodules (Definition 2.2.3). We define:

1. The *kernel of φ* is the submodule of M (Definition 2.2.2) given by
$$\ker(\varphi) := \{m \in M \mid \varphi(m) = 0\} \subseteq M.$$
2. The *image of φ* is the submodule of N given by
$$\operatorname{im}(\varphi) := \{\varphi(m) \mid m \in M\} \subseteq N.$$
3. The *cokernel of φ* is the quotient module of N (Definition 2.2.18) defined by
$$\operatorname{coker}(\varphi) := N/\operatorname{im}(\varphi).$$
4. The *coimage of φ* is the quotient module of M (Definition 2.2.18) defined by
$$\operatorname{coim}(\varphi) := M/\ker(\varphi).$$

It is not difficult to see that each of these are indeed R-S bimodules. In case M and N are left/right/two-sided R-modules, the *kernel, image, cokernel, and coimage* of a module homomorphism $\varphi : M \to N$ are respectively defined to be the kernel, image, cokernel, and coimage for the natural bimodule structures (Definition 2.2.1) of M and N.

The kerel, cokernel, image, and coimage of f are respectively the categorical kernel, cokernel (Definition A.4.14), image, and coimage (Definition A.4.15) (Lemma 2.2.20).

Lemma 2.2.20. Let R, S be (not-necessarily commutative) rings with unity (Definition 2.1.1), let M, N be R-S-bimodules (Definition 2.2.1), and let $f : M \to N$ be a module homomorphism (Definition 2.2.3). The kerel, cokernel, image, and coimage (Definition 2.2.19) of f are respectively the categorical kernel, cokernel (Definition A.4.14), image, and coimage (Definition A.4.15).

Theorem 2.2.21. Let R, S be (not-necessarily commutative) rings with unity (Definition 2.1.1). The category of R-S-bimodules (Definition 2.2.1) is a Grothendieck abelian category (Definition 2.2.13).

Definition 2.2.22. Let $\mathcal{A}$ be an additive category (Definition 2.2.10). A sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

of moprhisms in $\mathcal{A}$ is called a *short exact sequence* if the morphisms satisfy:

- $f : A \to B$ is a monomorphism (Definition A.4.23) and is the kernel of g (Definition A.4.14),
- $g : B \to C$ is an epimorphism (Definition A.4.23) and is the cokernel of f (Definition A.4.14),
- the sequence is exact at B, meaning $\mathrm{Im}(f) = \mathrm{Ker}(g)$ (Definition A.4.15).

This means the sequence starts and ends with the zero object and is exact everywhere.

Definition 2.2.23. Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor (Definition 2.2.11) between abelian categories (Definition 2.2.12).

1. F is called *left exact* if it preserves all finite limits (Definition A.4.19), or equivalently it preserves kernels (Definition A.4.14) and any finite limit diagrams. Equivalently, for every left exact sequence in $\mathcal{A}$
$$0 \to A' \xrightarrow{f} A \xrightarrow{g} A''$$
the sequence
$$0 \to F(A') \xrightarrow{F(f)} F(A) \xrightarrow{F(g)} F(A'')$$
is exact at $F(A')$ and $F(A)$ (i.e., F preserves monomorphisms (Definition A.4.23) and exactness at the first two terms).
2. Dually, F is called *right exact* if it preserves all finite colimits (Definition A.4.19), or equivalently it preserves cokernels (Definition A.4.14) and any finite colimit diagrams. Equivalently, for every right exact sequence in $\mathcal{A}$
$$A' \xrightarrow{f} A \xrightarrow{g} A'' \to 0,$$
the sequence
$$F(A') \xrightarrow{F(f)} F(A) \xrightarrow{F(g)} F(A'') \to 0$$
is exact at $F(A)$ and $F(A'')$ (i.e., F preserves epimorphisms (Definition A.4.23) and exactness at the last two terms).
3. F is called *exact* if it is both left and right exact.

Definition 2.2.24 (Natural module structures induced by opposite rings)**.** Let R be a ring (not necessarily commutative) (Definition 2.1.1).

1. If M is a left R-module (Definition 2.2.1), then M naturally has a structure of a right R^{op} (Definition 2.1.3)-module defined by
$$m \cdot r := r \cdot m,$$
for all $m \in M$ and $r \in R$, where the multiplication on the right is the original left R-action on M but re-interpreted so elements of R^{op} act from the right.
2. Dually, if M is a right R-module, then M naturally has a structure of a left R^{op}-module defined by
$$r \cdot m := m \cdot r,$$
for all $m \in M$ and $r \in R$, where the multiplication on the left is the original right R-action on M but re-interpreted as a left action of R^{op}.

If R is a commutative ring, and given a left/right R-module M, recall that R^{op} is naturally isomorphic to R (Definition 2.1.3), so the right/left R^{op}-module structure on M is a right/left R-module structure. In fact, the left/right R-module and right/left R-module structures on M make M into an R-R-bimodule (Definition 2.2.1).

Remark 2.2.25. Given a general left/right R-module (Definition 2.2.1) M, the right/left R^{op} (Definition 2.1.3)-module structure does not necessarily make M into an R-R^{op}-bimodule (Definition 2.2.1).

2.2.3. *Simple modules.*

Definition 2.2.26. Let R be a not necessarily commutative ring (Definition 2.1.1). An R-module M is called *simple* if $M \neq 0$ and the only submodules of M (Definition 2.2.2) are $\{0\}$ and M itself.

Definition 2.2.27. A not necessarily commutative ring (Definition 2.1.1) R is called *simple* if $R \neq 0$ and the only two-sided ideals of R (Definition 2.2.28) are $\{0\}$ and R itself.

2.2.4. *Ideals of a ring.*

Definition 2.2.28. Let R be a (not necessarily commutative, possibly nonunital) ring (Definition 2.1.1). A *left ideal of R* is a subset $I \subseteq R$ such that

- $(I, +)$ is an additive subgroup (Definition 1.1.5) of $(R, +)$,
- $RI \subseteq I$, i.e., for all $r \in R$ and $x \in I$, one has $rx \in I$.

Similarly, a *right ideal of R* is a subset $I \subseteq R$ such that

- $(I, +)$ is an additive subgroup of $(R, +)$,
- $IR \subseteq I$, i.e., for all $r \in R$ and $x \in I$, one has $xr \in I$.

A *two-sided ideal* (or simply an *ideal*) of R is a subset $I \subseteq R$ which is both a left ideal and a right ideal of R. We denote by $I \trianglelefteq R$ the relation expressing that I is a two-sided ideal of R.

Equivalently, an left/right/two-sided ideal of R is a submodule (Definition 2.2.2) of R as an R-module (Definition 2.2.1).

A left/right/two-sided ideal is said to be *proper* if it is strictly contained in R.

Note that every left or right ideal of a commutative ring is a two-sided ideal.

Definition 2.2.29. Let R be a (not necessarily commutative) ring (Definition 2.1.1), and let $X \subseteq R$ be a subset (Definition A.1.2).

The *left ideal generated by X* is the smallest left ideal (Definition 2.2.28) of R containing X; it equals the set of all finite sums of elements of the form rx with $r \in R$ and $x \in X$.

Similarly, the *right ideal generated by X* is the smallest right ideal of R containing X; it equals the set of all finite sums of elements of the form xr with $x \in X$ and $r \in R$.

The *two-sided ideal generated by X* is the smallest two-sided ideal of R containing X; it equals the set of all finite sums of elements of the form rxs with $r, s \in R$ and $x \in X$.

A left/right/two-sided ideal I of R is said to be *finitely generated* if there exists some finite subset X of R such that I equals the left/right/two-sided ideal generated by X. Moreover, I is said to be *principal* if there exists some subset X of R of cardinality 1 such that I equals the left/right/two-sided ideal generated by X.

Definition 2.2.30. Let R be a ring, and let I, J be left ideals of R (Definition 2.2.28) (resp. right ideals, resp. two-sided ideals).

The *product ideal IJ* is the left (resp. right, resp. two-sided) ideal defined as the additive subgroup (Definition 1.1.5) of R generated by (Definition 2.2.29) all products xy where $x \in I$ and $y \in J$. In other words,

$$IJ = \left\{ \sum_{k=1}^{n} x_k y_k : n \geq 0, x_k \in I, y_k \in J \right\}.$$

More generally, we may speak of the product of finitely many ideals of R.

Definition 2.2.31. Let R be a not-necesarily commutative ring (Definition 2.1.1) and $I \subseteq R$ a two-sided ideal (Definition 2.2.28). The set

$$R/I = \{r + I : r \in R\}$$

is called the *quotient ring of R by I*, where $r + I = \{r + i : i \in I\}$ and the operations are defined by

$$(r + I) + (s + I) := (r + s) + I,$$

$$(r + I)(s + I) := rs + I.$$

With these operations, R/I is a ring and the canonical projection $R \to R/I$, $r \mapsto r + I$ is a surjective ring homomorphism (Definition 2.1.13).

Definition 2.2.32. Let R be a (not necessarily commutative) ring (Definition 2.1.1). A proper two-sided ideal $P \trianglelefteq R$ (Definition 2.2.28) is called a *prime ideal* if the following equivalent conditions holds:

1. If I, J are left ideals and $IJ \subset P$ (Definition 2.2.30), then $I \subset P$ or $J \subset P$.
2. If I, J are right ideals and $IJ \subset P$, then $I \subset P$ or $J \subset P$.
3. If I, J are two-sided idaels and $IJ \subset P$, then $I \subset P$ or $J \subset P$.
4. If $x, y \in R$ with $xRy \subset \mathfrak{p}$, then $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

A proper left/right/two-sided ideal $M \subsetneq R$ is called *maximal* if there exists no other left/right/two-sided ideal $J \trianglelefteq R$ such that $M \subsetneq J \subsetneq R$. Equivalently,

- a left/right ideal M of R is maximal if and only if the quotient module R/M (Definition 2.2.18) is a simple (Definition 2.2.26) left/right R-module.
- a two-sided ideal M of R is maximal if and only if the quotient ring R/M (Definition 2.2.31) is a simple ring (Definition 2.2.27).

Lemma 2.2.33. Let R be a commutative ring. An ideal $P \subseteq R$ is prime if and only if the following holds:

$$\text{For all } a, b \in R, \text{ if } ab \in P \text{ then } a \in P \text{ or } b \in P.$$

Definition 2.2.34. Let R be a ring (Definition 2.1.1), not assumed commutative. The *Jacobson radical of R*, denoted by $J(R)$, is the intersection of all maximal left ideals of R:

$$J(R) = \bigcap\{M \subseteq R : M \text{ is a maximal left ideal of } R\}.$$

Equivalently, $J(R)$ is also the intersection of all maximal right ideals of R. Thus, $J(R)$ is a two-sided ideal of R.

Definition 2.2.35. Let R be a ring (Definition 2.1.1) with unity, not necessarily commutative. The ring R is called a *local ring* if it has a unique maximal left ideal (Definition 2.2.32). In this case, R also has a unique maximal right ideal, and these coincide with the Jacobson radical $J(R)$ of R (Definition 2.2.34). The unique maximal left (and right) ideal of a local ring R may sometimes be denoted by $\mathfrak{m}_R$.

Definition 2.2.36. Let R be a not necessarily commutative ring (Definition 2.1.1). A subset $S \subseteq R$ is called a *multiplicative subset* if

- $1 \in S$ (assuming R has unity),
- For all $s, t \in S$, one has $st \in S$.

Definition 2.2.37. Let R be a commutative ring with unity (Definition 2.1.4) and let $S \subseteq R$ be a multiplicative subset (Definition 2.2.36). The *localization of R at S*, denoted by $S^{-1}R$, is the ring whose elements are equivalence classes of pairs $(r, s) \in R \times S$ under the equivalence relation

$$(r, s) \sim (r', s') \iff \exists u \in S \text{ such that } u(sr' - s'r) = 0.$$

Write $\frac{r}{s}$ for the equivalence class of (r, s). Addition and multiplication on representatives are defined by

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'},$$
$$\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}.$$

The map $r \mapsto \frac{r}{1}$ defines a ring homomorphism (Definition 2.1.13); therefore, $S^{-1}R$ is naturally an R-algebra (Definition 2.1.18).

Given an element $f \in R$, the localization of R at $S = \{f^n : n \geq 0\}$ is denoted by R_f.

If P is a prime ideal of R (Definition 2.2.32), then $R_P := S^{-1}R$ with $S = R \setminus P$ is called the *localization of R at P*. It is a local ring (Definition 2.2.35) whose maximal ideal (Definition 2.2.32) is given by

$$S^{-1}P = \{\frac{p}{s} \in R_P : p \in P\}.$$

Definition 2.2.38. Let $(R, \mathfrak{m}_R)$ and $(S, \mathfrak{m}_S)$ be local rings (Definition 2.2.35), not necessarily commutative. A ring homomorphism (Definition 2.1.13) $\varphi : R \to S$ is called a *local morphism* (or *local homomorphism*) if $\varphi(\mathfrak{m}_R) \subseteq \mathfrak{m}_S$.

2.2.5. *Tensor and Hom's of modules.*

Definition 2.2.39 (Tensor product of bimodules)**.** Let R, S, T be (not necessarily commutative) rings (Definition 2.1.1), let M be an R-S bimodule (Definition 2.2.1), and let N be an S-T bimodule. In the free abelian group $\mathbb{Z}[M \times N]$ generated by the Cartesian product $M \times N$ (Definition A.1.4), let U be the subgroup generated by elements of the form (♠ TODO: subgroup generated)

$$\begin{aligned}
&(m + m', n) - (m, n) - (m', n), \\
&(m, n + n') - (m, n) - (m, n'), \\
&(m \cdot s, n) - (m, s \cdot n),
\end{aligned}$$

for all $m, m' \in M$, $n, n' \in N$, and $s \in S$. The *tensor product of M and N over S* is the quotient (Definition 1.1.13) abelian group

$$M \otimes_S N := \mathbb{Z}[M \times N]/U.$$

The image of an element of the form $(m, n) \in M \times N$ in $M \otimes_S N$ is denoted $m \otimes n$ and called a *pure tensor*. In general, the elements of $M \otimes_S N$ are finite sums

$$\sum_{i=1}^{n} m_i \otimes n_i \quad m_i \in M, n_i \in N$$

of pure tensors. Thus, the pure tensors satisfy the following relations:

$$\begin{aligned}
(m + m') \otimes n &= m \otimes n + m' \otimes n \\
m \otimes (n + n') &= m \otimes n + m \otimes n' \\
(m \cdot s) \otimes n &= m \otimes (s \cdot n)
\end{aligned}$$

This tensor product becomes naturally an R-T bimodule with left action and right action defined by

$$\begin{aligned}
r \cdot (m \otimes n) &= (r \cdot m) \otimes n, \\
(m \otimes n) \cdot t &= m \otimes (n \cdot t),
\end{aligned}$$

for all $r \in R$, $t \in T$, $m \in M$, and $n \in N$.

Inductively, given rings $R_0, \ldots, R_k$ and $R_{i-1} - R_i$-bimodules M_i for $i = 1, \ldots, k$, we may speak of the tensor product

$$M_0 \otimes_{R_1} M_1 \otimes_{R_2} \cdots \otimes_{R_{k-1}} M_k;$$

tensor products are associative(♠ TODO:), so parentheses are not strictly needed to notate them. Its *pure tensors* are elements of the form $m_0 \otimes m_1 \otimes \cdots \otimes m_k$ for $m_i \in M_i$, and its general elements are finite sums

$$\sum_{j=1}^{n} m_{0j} \otimes m_{1j} \otimes \cdots m_{kj} \quad m_{ij} \in M_i.$$

of pure tensors. It also has a natural $R_0 - R_k$-bimodule structure.

In general, $(M_0, \dots, M_k) \mapsto M_0 \otimes_{R_1} M_1 \otimes_{R_2} \cdots \otimes_{R_{k-1}} M_k$ defines a $(k+1)$-ary additive functor (Definition A.5.1)

$$ {}_{R_0}\mathbf{Mod}_{R_1} \times \cdots \times {}_{R_{k-1}}\mathbf{Mod}_{R_k} \to {}_{R_0}\mathbf{Mod}_{R_k} $$

(Theorem 2.2.21).

Given a ring R and a two-sided R-module M, we may also speak of the *n-fold tensor product* $M^{\otimes n} = M^{\otimes_R n}$

Definition 2.2.40. Let k be a not necessarily commutative ring (Definition 2.1.1). Let R and S be k-rings (Definition 2.1.13) (not necessarily commutative). Assume that at least one of R or S is a k-algebra (Definition 2.1.18). The *tensor product ring* $R \otimes_k S$ is the k-module $R \otimes_k S$ (Definition 2.2.39) equipped with a multiplication defined on simple tensors by

$$ (r_1 \otimes s_1) \cdot (r_2 \otimes s_2) = (r_1 r_2) \otimes (s_1 s_2) $$

and extended by linearity. This multiplication is well-defined and makes $R \otimes_k S$ into a k-ring under the ring homomorphism

$$ k \to R \otimes_k S, \quad a \mapsto a \otimes 1 = 1 \otimes a. $$

The unit element is $1_R \otimes 1_S$.

In this ring, the subrings (Definition 2.1.25) $R \otimes 1$ and $1 \otimes S$ commute with each other; that is, for all $r \in R$ and $s \in S$,

$$ (r \otimes 1) \cdot (1 \otimes s) = r \otimes s = (1 \otimes s) \cdot (r \otimes 1). $$

If R and S are both k-algebras, then $R \otimes_k S$ is also a k-algebra.

2.2.6. *Restriction and extension of scalars.*

Definition 2.2.41. Let R and S be associative rings with identity (Definition 2.1.1), and let $\varphi : R \to S$ be a unital ring homomorphism (Definition 2.1.13). Let T be a ring.

1. Let $(M, +)$ be an abelian group (Definition 1.1.1) equipped with either the structure of a $S-T$-bimodule (Definition 2.2.1) $(M, +, \cdot_S)$ or the structure of a $T-S$-bimodule $(M, +, \cdot_S)$.

   The *restriction of scalars of M along φ* is the R-module structure on the same underlying abelian group $(M, +)$ defined as follows:
   - If M is a $S-T$-bimodule, the restriction of scalars of M along φ, often denoted by $\varphi_* M$ (or ${}_R M$), is the $R-T$-bimodule whose R-action $\cdot_R : R \times M \to M$ is given by
     $$ r \cdot_R m := \varphi(r) \cdot_S m $$
     for all $r \in R$ and $m \in M$.
   - If M is a $T-S$-bimodule, the restriction of scalars of M along φ, often denoted by $\varphi_* M$ (or M_R), is the $T-R$-bimodule whose R-action $\cdot_R : M \times R \to M$ is given by
     $$ m \cdot_R r := m \cdot_S \varphi(r) $$
     for all $r \in R$ and $m \in M$.

2. Let ${}_S\mathrm{Mod}_T$ and ${}_T\mathrm{Mod}_S$ be the categories of $S - T$ and $T - S$-bimodules (Definition 2.2.4), respectively, and similarly for R.

   The *restriction of scalars functor for modules* is the covariant functor (Definition A.4.5) induced by φ, defined for both left and right modules:
   - For left S-modules, it is the functor $\varphi_* : {}_S\mathrm{Mod}_T \to {}_R\mathrm{Mod}_T$ defined as follows:
     (a) On objects: For any left S-module M, $\varphi_*(M)$ is the left R-module obtained by restriction of scalars along φ.
     (b) On morphisms: For any homomorphism (Definition 2.2.3) of left S-modules $h : M \to N$, the image $\varphi_*(h) : \varphi_*(M) \to \varphi_*(N)$ is the map h itself, viewed as a homomorphism of left R-modules.
   - For right S-modules, it is the functor $\varphi_* : {}_T\mathrm{Mod}_S \to {}_T\mathrm{Mod}_R$ defined as follows:
     (a) On objects: For any right S-module M, $\varphi_*(M)$ is the right R-module obtained by restriction of scalars along φ.
     (b) On morphisms: For any homomorphism of right S-modules $h : M \to N$, the image $\varphi_*(h) : \varphi_*(M) \to \varphi_*(N)$ is the map h itself, viewed as a homomorphism of right R-modules.

   In either context, if φ is an inclusion map (making R a subring of S), this functor is often called the *forgetful functor*.
3. Let Ring_S (or S/Ring) denote the category of S-rings (Definition 2.1.15). Let Ring_R be defined similarly.

   The *restriction of scalars functor for rings*, denoted by $\varphi_* : \mathsf{Ring}_S \to \mathsf{Ring}_R$ is the functor defined as follows:
   - On objects: Let (A, ψ) be an S-ring. Then $\varphi_*(A)$ is the R-ring $(A, \psi \circ \varphi)$, where the structure map is the composition $R \xrightarrow{\varphi} S \xrightarrow{\psi} A$.
   - On morphisms: For any morphism of S-rings $h : (A, \psi_A) \to (B, \psi_B)$, the image $\varphi_*(h)$ is the map h itself, which satisfies $h \circ (\psi_A \circ \varphi) = \psi_B \circ \varphi$ and is thus a morphism of R-rings.

   This functor simply pre-composes the structure map with φ, effectively "forgetting" the factorization through S.

   The restriction of scalars functor restricts to a functor $\varphi_* : \mathbf{Alg}_S \to \mathbf{Alg}_R$ (Definition 2.1.18).

Definition 2.2.42. Let R and S be rings (Definition 2.1.1) (not necessarily commutative), and let $f : R \to S$ be a ring homomorphism (Definition 2.1.13). This homomorphism gives S the structure of an (R, R)-bimodule (Definition 2.2.1) via restriction of scalars (Definition 2.2.41). Let T be a ring (Definition 2.1.1).

1. The *extension of scalars* (or *base change*) along f is defined separately for modules:
   - For an $(R-T)$-bimodule M, the extension of scalars of M along f is the $(S-T)$-bimodule $S \otimes_R M$ (Definition 2.2.39) where S is viewed as an (S, R)-bimodule. In particular, the action of $s' \in S$ on a simple tensor (Definition 2.2.39) $s \otimes m$ is given by $s' \cdot (s \otimes m) = (s's) \otimes m$.
   - For a $(T - R)$-bimodule M, the extension of scalars of M along f is the $(T - S)$-bimodule $M \otimes_R S$ where S is viewed as an (R, S)-bimodule. In particular, the action of $s' \in S$ on a simple tensor $m \otimes s$ is given by $(m \otimes s) \cdot s' = m \otimes (ss')$.

2. The *base change functor* (or *extension of scalars functor* or *induction functor*), denoted by f^*, $S \otimes_R -$, $- \otimes_R S$, or Ind_R^S, is given by:
   - For left R-modules:
   $$f^* : {}_R\mathsf{Mod}_T \to {}_S\mathsf{Mod}_T, \quad M \mapsto S \otimes_R M.$$
   (Definition 2.2.4) This is the left adjoint (Definition A.4.11) to the restriction of scalars (Definition 2.2.41) functor $f_* : {}_S\mathsf{Mod}_T \to {}_R\mathsf{Mod}_T$.
   - For right R-modules:
   $$f^* : {}_T\mathsf{Mod}_R \to {}_T\mathsf{Mod}_S, \quad M \mapsto M \otimes_R S.$$
   This is the left adjoint to the restriction of scalars functor $f_* : {}_T\mathsf{Mod}_S \to {}_T\mathsf{Mod}_R$.
3. Let A be an R-ring (Definition 2.1.13), i.e. a ring equipped with a ring homomorphism $R \to A$. Assume that S or A is an R-algebra (Definition 2.1.18).

   The *base change of the algebra A along f* is the S-ring defined as
   $$A_S := S \otimes_R A$$
   (Definition 2.2.40) equipped with the natural homomorphism $S \to S \otimes_R A$ given by $s \mapsto s \otimes 1_A$. As a ring, the multiplication in A_S is determined by $(s_1 \otimes a_1)(s_2 \otimes a_2) = (s_1 s_2) \otimes (a_1 a_2)$ for $s_1, s_2 \in S$ and $a_1, a_2 \in A$.
4. Then the base change construction induces functors in the following situations:
   (a) If S is only an R-ring, then base change induces a functor $f^* : \mathbf{Alg}_R \to \mathbf{Ring}_S$.
   (b) If S is an R-algebra, then base change induces a functor $f^* : \mathbf{Ring}_R \to \mathbf{Ring}_S$ which restricts to a functor $f^* : \mathbf{Alg}_R \to \mathbf{Alg}_S$

   In either case, the base change functor is defined as follows:
   - On objects: For any R-algebra (A, φ), $f^*(A)$ is the S-algebra $S \otimes_R A$ defined above.
   - On morphisms: For any homomorphism of R-algebras $h : A \to B$, the image $f^*(h)$ is the map $\mathrm{id}_S \otimes h : S \otimes_R A \to S \otimes_R B$, defined by $s \otimes a \mapsto s \otimes h(a)$.

   (♠ TODO: comment on adjunction)

Definition 2.2.43. Let R and S be rings (Definition 2.1.1) (not necessarily commutative), and let $f : R \to S$ be a ring homomorphism (Definition 2.1.13). The homomorphism f endows S with two bimodule structures — that of an (R, S)-bimodule and of an (S, R)-bimodule via restriction of scalars (Definition 2.2.41). Let T be a ring.

1. The *co-extension of scalars* (or simply *co-extension*) along f is defined separately for modules:
   - For an $R - T$-bimodule M, the co-extension of scalars of M along f is the $S - T$-bimodule $\mathrm{Hom}_R(S, M)$ (Definition 2.2.15) of left R-module homomorphisms from the $R - S$-bimodule S to M.
   - For a $T - R$-bimodule M, the co-extension of scalars of M along f is the $T - S$-bimodule $\mathrm{Hom}_R(S, M)$ of right R-module homomorphisms from the $S - R$-bimodule S to M.
2. The *co-extension of scalars functor* (or *coinduction functor*), denoted by $f^!$ or CoInd_R^S, is the functor given by:

- For left R-modules:

  $$f^! : {}_R\mathsf{Mod}_T \to {}_S\mathsf{Mod}_T, \quad M \mapsto \mathrm{Hom}_R(S, M).$$

  This functor is the right adjoint to the restriction of scalars functor $f_* : {}_S\mathsf{Mod} \to {}_R\mathsf{Mod}$.
- For right R-modules:

  $$f^! : {}_T\mathsf{Mod}_R \to {}_T\mathsf{Mod}_S, \quad M \mapsto \mathrm{Hom}_R(S, M).$$

  This functor is the right adjoint to the restriction of scalars functor $f_* : \mathsf{Mod}_S \to \mathsf{Mod}_R$.

Theorem 2.2.44 (Extension-Restriction and Restriction-Coextension adjunction for modules)**.** Let R and S be rings (Definition 2.1.1) (not necessarily commutative), and let $f : R \to S$ be a ring homomorphism (Definition 2.1.13). Let T be a ring.

1. **Extension-Restriction adjunction:**
   (a) **Restriction on the Left:** The extension of scalars functor (Definition 2.2.42)

   $$f^* = S \otimes_R - : {}_R\mathsf{Mod}_T \to {}_S\mathsf{Mod}_T$$

   (Definition 2.2.4) is left adjoint (Definition A.4.11) to the restriction of scalars functor (Definition 2.2.41)

   $$f_* : {}_S\mathsf{Mod}_T \to {}_R\mathsf{Mod}_T.$$

   Explicitly, for any $R-T$-bimodule M and any $S-T$-bimodule N, there is a natural isomorphism:

   $$\mathrm{Hom}_{S-T}(S \otimes_R M, N) \cong \mathrm{Hom}_{R-T}(M, f_*N).$$

   (b) **Restriction on the Right:** The extension of scalars functor

   $$f^* = - \otimes_R S : {}_T\mathsf{Mod}_R \to {}_T\mathsf{Mod}_S$$

   is left adjoint to the restriction of scalars functor

   $$f_* : {}_T\mathsf{Mod}_S \to {}_T\mathsf{Mod}_R.$$

   Explicitly, for any $T-R$-bimodule M and any $T-S$-bimodule N, there is a natural isomorphism:

   $$\mathrm{Hom}_{T-S}(M \otimes_R S, N) \cong \mathrm{Hom}_{T-R}(M, f_*N).$$
2. **Restriction-Coextension adjunction:**
   (a) **Restriction on the Left:** The co-extension of scalars functor (Definition 2.2.43)

   $$f^! = \mathrm{Hom}_R(S, -) : {}_R\mathsf{Mod}_T \to {}_S\mathsf{Mod}_T$$

   is right adjoint (Definition A.4.11) to the restriction of scalars functor

   $$f_* : {}_S\mathsf{Mod}_T \to {}_R\mathsf{Mod}_T.$$

   Explicitly, for any $S-T$-bimodule N and any $R-T$-bimodule M, there is a natural isomorphism:

   $$\mathrm{Hom}_{R-T}(f_*N, M) \cong \mathrm{Hom}_{S-T}(N, \mathrm{Hom}_R(S, M)).$$

(b) **Restriction on the Right:** The co-extension of scalars functor

$$f^! = \mathrm{Hom}_R(S, -) : {}_T\mathsf{Mod}_R \to {}_T\mathsf{Mod}_S$$

is right adjoint to the restriction of scalars functor

$$f_* : {}_T\mathsf{Mod}_S \to {}_T\mathsf{Mod}_R.$$

Explicitly, for any $T-S$-bimodule N and any $T-R$-bimodule M, there is a natural isomorphism:

$$\mathrm{Hom}_{T-R}(f_*N, M) \cong \mathrm{Hom}_{T-S}(N, \mathrm{Hom}_R(S, M))$$

where here $\mathrm{Hom}_R(S, M)$ uses the left R-module structure on S and the right R-module structure on M.

Theorem 2.2.45 (Adjunction for Rings)**.** (♠ TODO:) Let $f : R \to S$ be a homomorphism of rings. Let Ring_R and Ring_S denote the categories of R-rings (Definition 2.1.15) and S-rings, respectively.

There is an adjunction between these categories:

1. The *restriction of scalars functor*, $f_* : \mathsf{Ring}_S \to \mathsf{Ring}_R$, sends an S-ring $(B, \psi : S \to B)$ to the R-ring $(B, \psi \circ f)$.
2. The *extension of scalars functor*, $f^* : \mathsf{Ring}_R \to \mathsf{Ring}_S$, sends an R-ring $(A, \varphi : R \to A)$ to the *pushout* $S \amalg_R A$ in the category of rings (the free product of S and A with amalgamation over R).

Then f^* is left adjoint to f_*. For any R-ring A and any S-ring B, there is a natural bijection:

$$\mathrm{Hom}_{\mathsf{Ring}_S}(S \amalg_R A, B) \cong \mathrm{Hom}_{\mathsf{Ring}_R}(A, f_*B).$$

Special Case (Algebras): If R is commutative and we restrict to the full subcategory Alg_R of R-algebras (where the structure map maps to the center), and similarly for S (assuming S is an R-algebra), then the extension functor is given by the tensor product $S \otimes_R A$, and the adjunction becomes:

$$\mathrm{Hom}_{\mathsf{Alg}_S}(S \otimes_R A, B) \cong \mathrm{Hom}_{\mathsf{Alg}_R}(A, f_*B).$$

Proposition 2.2.46 (Universal Property of the Tensor Product of Bimodules)**.** Let R, S, T be (not necessarily commutative) rings (Definition 2.1.1). Let M be an R-S bimodule (Definition 2.2.1) and let N be an S-T bimodule. Let P be an R-T bimodule. Then for every R-T bilinear map (Definition 4.2.1)

$$\beta : M \times N \to P,$$

that is, a map satisfying

$$\begin{aligned}
\beta(m+m', n) &= \beta(m,n) + \beta(m', n), \\
\beta(m, n+n') &= \beta(m,n) + \beta(m, n'), \\
\beta(r \cdot m, n) &= r \cdot \beta(m,n), \\
\beta(m, n \cdot t) &= \beta(m,n) \cdot t, \\
\beta(m \cdot s, n) &= \beta(m, s \cdot n),
\end{aligned}$$

for all $m, m' \in M$, $n, n' \in N$, $r \in R$, $s \in S$, $t \in T$, there exists a unique R-T bimodule homomorphism

$$\widetilde{\beta} : M \otimes_S N \to P$$

such that $\widetilde{\beta}(m \otimes n) = \beta(m,n)$ for all $m \in M$, $n \in N$.

Theorem 2.2.47 (Tensor-Hom Adjunction for Bimodules)**.**

1. Let R, S, T be (not necessarily commutative) rings (Definition 2.1.1). Let M be an R-S bimodule (Definition 2.2.1), let N be an S-T bimodule, and let P be an R-T bimodule. Then there is a natural isomorphism of abelian groups

   $$\mathrm{Hom}_{R\text{-}T}(M \otimes_S N,\, P) \;\cong\; \mathrm{Hom}_{S\text{-}T}(N,\, \mathrm{Hom}_R(M, P))$$

   (Definition 2.2.39) (Definition 2.2.15). Note that $\mathrm{Hom}_{R\text{-}T}$ is the abelian group of R-T bimodule homomorphisms, $\mathrm{Hom}_{S\text{-}T}$ is the abelian group of S-T bimodule homomorphisms, and $\mathrm{Hom}_R(M, P)$ is endowed with the structure of an S-T bimodule via

   $$\begin{aligned}
   (s \cdot f)(m) &= f(m \cdot s), \\
   (f \cdot t)(m) &= f(m) \cdot t,
   \end{aligned}$$

   for all $s \in S$, $t \in T$, $f \in \mathrm{Hom}_R(M, P)$, $m \in M$. Intuitively, this expresses that $M \otimes_S -$ is left adjoint (Definition A.4.11) to $\mathrm{Hom}_R(M, -)$ in the category of bimodules.
2. Let R, S, T be (not necessarily commutative) rings (Definition 2.1.1). Let M be an R-S bimodule (Definition 2.2.1), let N be an S-T bimodule, and let P be an R-T bimodule. Then there is a natural isomorphism of abelian groups

   $$\mathrm{Hom}_{R\text{-}T}(M \otimes_S N,\, P) \;\cong\; \mathrm{Hom}_{R\text{-}S}(M,\, \mathrm{Hom}_T(N, P))$$

   (Definition 2.2.39) (Definition 2.2.15).

   Note that $\mathrm{Hom}_{R\text{-}T}$ is the abelian group of R-T bimodule homomorphisms, $\mathrm{Hom}_{R\text{-}S}$ is the abelian group of R-S bimodule homomorphisms, and $\mathrm{Hom}_T(N, P)$ is endowed with the structure of an R-S bimodule via

   $$\begin{aligned}
   (r \cdot f)(n) &= r \cdot f(n), \\
   (f \cdot s)(n) &= f(n \cdot s),
   \end{aligned}$$

   for all $r \in R$, $s \in S$, $f \in \mathrm{Hom}_T(N, P)$, and $n \in N$.

   Intuitively, this expresses that $-\otimes N$ is left adjoint (Definition A.4.11) to $\mathrm{Hom}_T(N, -)$ in the category of bimodules.

Proposition 2.2.48. Let $\mathcal{A}, \mathcal{B}$ be abelian categories (Definition 2.2.12) and let $F : \mathcal{A} \to \mathcal{B}$ and $G : \mathcal{B} \to \mathcal{A}$ be adjoint (Definition A.4.11) additive functors (Definition 2.2.11), say with $F \dashv G$ (i.e. F is left adjoint to G). The left adjoint functor F is right exact (Definition 2.2.23) and and the right adjoint functor G is left exact (Definition 2.2.23)

Proposition 2.2.49. Let R, S, T be (not necessarily commutative) rings (Definition 2.1.1). Recall that categories of modules are abelian (Definition 2.2.12) (Theorem 2.2.21).

1. Let M be an R-S-bimodule (Definition 2.2.1). The functor $M \otimes_S - : {}_S\mathbf{Mod}_T \to {}_R\mathbf{Mod}_T$ (Definition 2.2.39) is a right exact functor (Definition 2.2.23).
2. Let N be an S-T-bimodule. The functor $- \otimes_S N : {}_R\mathbf{Mod}_S \to {}_R\mathbf{Mod}_T$ is a right exact functor (Definition 2.2.23).
3. Let M be an R-S-bimodule. The functor

$$\mathrm{Hom}(M, -) : {}_R\mathbf{Mod}_T \to {}_S\mathbf{Mod}_T$$

(Definition 2.2.15) is a left exact functor (Definition 2.2.23).

Now let M be an S-R-bimodule. The functor

$$\mathrm{Hom}(M, -) : {}_T\mathbf{Mod}_R \to {}_S\mathbf{Mod}_T$$

is a left exact functor (Definition 2.2.23).

4. Let N be an R-T-bimodule. The functor

$$\mathrm{Hom}(-, N) : {}_R\mathbf{Mod}_S^{\mathrm{op}} \to {}_S\mathbf{Mod}_T$$

(Definition A.4.12) is a left exact functor (Definition 2.2.23).

Now let N be an T-R-bimodule. The functor

$$\mathrm{Hom}(-, N) : {}_S\mathbf{Mod}_R^{\mathrm{op}} \to {}_S\mathbf{Mod}_T$$

is a left exact functor (Definition 2.2.23).

Proof. The right exactness of the tensor functors and the left exactness of $\mathrm{Hom}(M, -)$ follow from Theorem 2.2.47 and Proposition 2.2.48. (♠ TODO: prove left exactness of $\mathrm{Hom}(-, N)$). □

Definition 2.2.50 (Flat module over a ring)**.** Let R be a (not necessarily commutative) ring (Definition 2.1.1).

1. Let M be a left R-module. The module M is said to be *flat (with respect to the left R-module structure)* if the functor

$$- \otimes_R M : \mathrm{Mod}_R \to \mathbf{Ab}$$

(Definition 2.2.39) from the category of right R-modules to abelian groups is exact; that is, for every exact sequence of right R-modules

$$0 \to N' \to N \to N'' \to 0,$$

the induced sequence

$$0 \to N' \otimes_R M \to N \otimes_R M \to N'' \otimes_R M \to 0$$

is exact.

(♠ TODO: tor) Equivalently, M is flat if $\mathrm{Tor}_1^R(-, M) = 0$.

2. Let M be a right R-module. The module M is said to be *flat (with respect to the right R-module structure)* if the functor

$$M \otimes_R - : {}_R\mathrm{Mod} \to \mathbf{Ab}$$

from the category of left R-modules to abelian groups is exact; that is, for every exact sequence of right R-modules

$$0 \to N' \to N \to N'' \to 0,$$

the induced sequence

$$0 \to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$$

is exact.

Equivalently in either case, M is flat if it is flat with respect to the biadditive functor

$$- \otimes_R - : \mathbf{Mod}_R \times {}_R\mathbf{Mod} \to \mathrm{Ab}\,.$$

(Definition A.5.2)

Definition 2.2.51 (Faithfully flat module)**.** Let R be a (not necessarily commutative) ring (Definition 2.2.52), and let M be a left/right R-module (Definition 2.2.1).

We say that M is a *faithfully flat left/right R-module* if:

1. M is flat (Definition 2.2.50) as a left/right R-module, i.e. the appropriate functor $- \otimes_R M : \mathbf{Mod}_R \to \mathrm{Ab}$ (Definition 2.2.39) or $M \otimes_R - : {}_R\mathbf{Mod} \to \mathrm{Ab}$ is exact.
2. The functor $- \otimes_R M : \mathbf{Mod}_R \to \mathrm{Ab}$ or $M \otimes_R - : {}_R\mathbf{Mod} \to \mathrm{Ab}$ is faithful (Definition A.4.26). Since the flatness of M means that the tensor functors are exact (Definition 2.2.23), the faithfulness of these functors is equivalent to saying that for any left/right R-module N, if $M \otimes_R N = 0$ or $N \otimes_R M = 0$ as appropriate, then $n = 0$.

Equivalently, the functor $M \otimes_R -$ or $- \otimes_R M$ as appropriate reflects (Definition A.4.27) exactness (Definition 2.2.22) and injectivity (Definition A.1.3), making M a generator (Definition 2.2.14) in the category of left/right R-modules.

Definition 2.2.52 (Flat ring homomorphism)**.** (♠ TODO: flat module) Let R and S be (not necessarily commutative) rings (Definition 2.1.1), and let $\varphi : R \to S$ be a ring homomorphism (Definition 2.1.13).

1. We may say that S is *flat as a left module* or that φ is *flat (as a left module)* if $- \otimes_R S : \mathrm{Mod}_R \to \mathrm{Mod}_S$ (Definition 2.2.39) is exact (Definition 2.2.23).
2. We may say that S is *flat as a right module* or that φ is *flat (as a right module)* if $S \otimes_R - : {}_R\mathrm{Mod}_R \to {}_S\mathrm{Mod}$ (Definition 2.2.39) is exact (Definition 2.2.23).

These two notions of flatness are different in general. However, if φ equips S with the structure of an R-algebra (Definition 2.1.18), then these two notions of flatness coincide. In this case, we may speak of the notion of *flatness of R-algebras* and say that S is *flat over R*.

If S is faithfully flat (Definition 2.2.51) as a left/right R-module, then we may say that φ is *faithfully flat (as a left/right R-module)*.

Definition 2.2.53 (Injective and Projective objects in a general category)**.** Let $\mathcal{C}$ be a category (Definition A.4.1)

- An object $I \in \mathcal{C}$ is called *injective* if for every monomorphism (Definition A.4.23) $m : A \to B$ in $\mathcal{C}$ and every morphism $f : A \to I$, there exists a morphism $\tilde{f} : B \to I$ such that the diagram

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, hook, "m"] & I \\
B \arrow[ru, dashed, "\tilde{f}"'] &
\end{tikzcd}$$

  commutes, i.e., $\tilde{f} \circ m = f$.
- Dually, an object $P \in \mathcal{C}$ is called *projective* if for every epimorphism (Definition A.4.23) $e : X \to Y$ in $\mathcal{C}$ and every morphism $g : P \to Y$, there exists a morphism $\tilde{g} : P \to X$ such that the diagram

$$\begin{tikzcd}
 & P \arrow[d, "g"] \arrow[ld, dashed, "\tilde{g}"'] \\
X \arrow[r, two heads, "e"] & Y
\end{tikzcd}$$

  commutes, i.e., $e \circ \tilde{g} = g$.

Definition 2.2.54. Let R and S be (not necessarily commutative) rings (Definition 2.1.1). A *projective R-S-bimodule* is an (R, S)-bimodule (Definition 2.2.1) P that satisfies any of the following equivalent conditions:

1. The functor
$$\mathrm{Hom}_{{}_R\mathsf{Mod}_S}(P, -) : {}_R\mathsf{Mod}_S \to \mathsf{Ab}$$
   is an exact functor (Definition 2.2.23) between the abelian categories ${}_R\mathsf{Mod}_S$ (Definition 2.2.4) and Ab (Definition 1.1.4).
2. P is a projective left module over the ring $R \otimes_{\mathbb{Z}} S^{\mathrm{op}}$ (Definition 2.2.40) (Definition 2.1.3).
3. P is a direct summand of a free (R, S)-bimodule. (A free (R, S)-bimodule is a direct sum of copies of the tensor product $R \otimes_{\mathbb{Z}} S$, equipped with the natural left R-action and right S-action).
4. P is a projective object (Definition 2.2.53) in the category ${}_R\mathsf{Mod}_S$. That is, for every surjective homomorphism of (R, S)-bimodules $f : M \to N$ and every homomorphism $g : P \to N$, there exists a homomorphism $h : P \to M$ such that $f \circ h = g$.

Being a projective bimodule is a strictly stronger condition than being projective as a left or right module.

- A bimodule ${}_RP_S$ may be projective as a left R-module (i.e., projective in ${}_R\mathsf{Mod}$) without being a projective bimodule.
- Similarly, it may be projective as a right S-module (i.e., projective in Mod_S) without being a projective bimodule.

- A bimodule that is projective on both sides is sometimes called *biprojective*, but this does not imply it is a projective object in ${}_R\mathsf{Mod}_S$. For example, if $R = S = \mathbb{Z}$, the bimodule $\mathbb{Z}$ is free (hence projective) on both sides, but it is *not* a projective $(\mathbb{Z}, \mathbb{Z})$-bimodule because $\mathbb{Z}$ is not a projective $\mathbb{Z}[\mathbb{Z}]$-module (the augmentation ideal is not projective).

Proposition 2.2.55. Let R and S be rings (Definition 2.1.1), and let $f : R \to S$ be a ring homomorphism (Definition 2.1.13). Let T be a ring.

The base change functor (Definition 2.2.42) (extension of scalars) for bimodules,

$$f^* = S \otimes_R - : {}_R\mathsf{Mod}_T \to {}_S\mathsf{Mod}_T,$$

(Definition 2.2.4) preserves projective objects. That is, if M is a projective $R-T$-bimodule, then $S \otimes_R M$ is a projective $S-T$-bimodule.

Similarly, the functor $f^* = - \otimes_R S : {}_T\mathsf{Mod}_R \to {}_T\mathsf{Mod}_S$ sends projective $T-R$-bimodules to projective $T-S$-bimodules.

2.3. **Properties of rings and ring homomorphisms.**

2.3.1. *Finitely generated, finitely presented, and finite algebras.*

Definition 2.3.1. Let R be a (not-necessarily commutative) ring (Definition 2.1.1) and let A be an R-algebra (Definition 2.1.18). We say that A is a *finitely generated R-algebra* or synoymously that the ring homomorphism (Definition 2.1.13) $R \to A$ is *of finite type* if there exists a finite subset $\{a_1, \ldots, a_n\} \subseteq A$ such that R-subalgebra of A generated by (Definition 2.1.22) $\{a_1, \ldots, a_n\}$ is equal to A. Equivalently, every element of A can be expressed, using a finite composition of ring operations and R-linear combinations, from the generators $\{a_1, \ldots, a_n\}$.

Definition 2.3.2 (Finitely presented algebra over a ring)**.** Let R be a (not necessarily commutative) ring (Definition 2.1.1). An R-algebra (Definition 2.1.18) A is said to be *finitely presented* if there exists an integer $n \geq 0$ and a surjective R-algebra homomorphism

$$\varphi : R\langle x_1, \ldots, x_n\rangle \twoheadrightarrow A$$

where $R\langle x_1, \ldots, x_n\rangle$ is the free R-algebra on n generators (Definition 2.1.23), such that the kernel $\ker(\varphi)$ is a finitely generated two-sided ideal (Definition 2.2.28) of $R\langle x_1, \ldots, x_n\rangle$.

In other words, A admits a presentation as

$$A \cong R\langle x_1, \ldots, x_n\rangle / I,$$

where I is a finitely generated (Definition 2.2.29) two-sided ideal.

If R and A are commutative rings, this recovers the usual definition of a finitely presented commutative R-algebra by replacing $R\langle x_1, \ldots, x_n\rangle$ with the polynomial ring $R[x_1, \ldots, x_n]$ and I a finitely generated ideal.

Definition 2.3.3. Let $B \to A$ be a B-algebra (Definition 2.1.18). We say that A is a *finite B-algebra* if A is finitely generated (Definition 2.3.1) as a B-module.

2.3.2. *Integral elements and morphisms of rings.*

Definition 2.3.4 (Integral element over a ring)**.** Let R be a commutative ring with unity (Definition 2.1.4).

1. Let A be an R-algebra (Definition 2.1.18). An element $a \in A$ is called *integral over R* if there exists a monic polynomial
$$p(x) = x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0$$
with coefficients $r_i \in R$ such that
$$p(a) = a^n + r_{n-1}a^{n-1} + \cdots + r_1 a + r_0 = 0 \quad \text{in } A.$$
2. Let A be an extension ring (Definition 2.1.26) of R. The ring extension A/R is called an *integral extension* if every element of A is integral over R.
3. Let A be an extension ring (Definition 2.1.26) of R. The *integral closure of R in A*, sometimes denoted by $\widetilde{A}$, is the subring
$$\widetilde{A} = \{a \in A : a \text{ is integral over } R\}.$$
We say that R is integrally closed in A if $\widetilde{A}$ coincides with A (considered as a subring of R (Definition 2.1.25)).
4. Let R be an integral domain with field of fractions $K = \operatorname{Frac}(R)$. We say that R is *integrally closed* if it is integrally closed as a subring of K.

2.3.3. *PID's and UFD's.*

Definition 2.3.5 (Principal ideal ring/domain (PID))**.** Let R be a commutative unital ring (Definition 2.1.4). Then R is a *principal ideal ring (PIR)* if every ideal of R is principal (Definition 2.2.29). If R is additionally an integral domain (Definition 2.1.7), then R is said to be a *principal ideal domain (PID)*

Definition 2.3.6 (Unique factorization domain (UFD) / Factorial ring)**.** (♠ TODO: define irreducible elements) An integral domain (Definition 2.1.7) R is called a *unique factorization domain (UFD)* or *factorial ring* if every nonzero nonunit element of R can be factored as a product of irreducible elements uniquely up to order and units (Definition 2.1.8).

3. Field Theory

4. Basic Linear algebra

4.1. **Definitions.**

Definition 4.1.1 (Vector space over a field)**.** Let $(k, +, \cdot)$ be a field (Definition 2.1.10). A *vector space over k* or a *k-vector space* is a triple $(V, +, \cdot)$[1] where

1. $(V, +)$ is an abelian group, and

[1] Note that $+$ and $\cdot$ are abuse of notation here as these are already used for the addition and multiplication of $\cdot$

2. $\cdot$ is a map $k \times V \to V$, called *scalar multiplication*

such that the following axioms hold for all $a, b \in k$ and all $u, v \in V$:

1. (Compatibility with field multiplication)
$$(ab) \cdot v = a \cdot (b \cdot v).$$

2. (Identity scalar)
$$1 \cdot v = v.$$

3. (Distributivity over vector addition)
$$a \cdot (u + v) = a \cdot u + a \cdot v.$$

4. (Distributivity over scalar addition)
$$(a + b) \cdot v = a \cdot v + b \cdot v.$$

Definition 4.1.2. Let F be a field (Definition 2.1.10), and let V be an F-vector space (Definition 4.1.1). A subset $B \subseteq V$ is called a *basis of V* if: (i) B is linearly independent (Definition 2.2.7) over F, and (ii) B spans (Definition 2.2.8) V.

If B is a basis, we define the *dimension of V over F* (or *rank of V over F*), denoted by
$$\dim_F(V),$$
(♠ TODO: cardinality) to be the cardinality of B. This value is uniquely determined by V and F.

Definition 4.1.3. Let F be a field (Definition 2.1.10), and let V and W be F-vector spaces (Definition 4.1.1). A function $T : V \to W$ is called a *(homo)morphism of vector spaces over F*, or an *F-linear map*, if for all $u, v \in V$ and all $a, b \in F$, we have
$$T(au + bv) = aT(u) + bT(v).$$
The set of all such morphisms from V to W is denoted by
$$\operatorname{Hom}_F(V, W).$$

Definition 4.1.4. Let R be a (not necessarily commutative) ring (Definition 2.1.1). Depending on the module structure of M, we define its dual module as follows:

1. If M is a left R-module (Definition 2.2.1), then the *(right) dual module of M* is
$$M^* = M^\vee := \operatorname{Hom}_R(M, R).$$
(Definition 2.2.15) Note that it is a right R-module, as M is a $R - \mathbb{Z}$-bimodule and R is an $R - R$-bimodule.
2. If M is a right R-module (Definition 2.2.1), then the *(left) dual module of M* is
$${}^*M = {}^\vee M := \operatorname{Hom}_R(M, R).$$
(Definition 2.2.15) Note that it is a left R-module, as M is a $\mathbb{Z} - R$-bimodule and R is an $R - R$-bimodule.

3. If M is a two-sided R-module, then the *dual of M* usually refers to either the right or the left dual as above.

In any case, the functor $M \mapsto M^\vee$ is a contravariant functor (Definition A.4.5) from the appropriate category of modules (Definition 2.2.4) to itself.

If R is a field (Definition 2.1.10) F and V is an F-vector space (Definition 4.1.1), then the dual module

$$V^* = V^\vee := \mathrm{Hom}_F(V, F)$$

is called the *dual vector space of V*.

Definition 4.1.5. Let R be a (not necessarily commutative) ring (Definition 2.1.1), and let $m, n \in \mathbb{N}$. The set of all $m \times n$ arrays with entries in R is denoted by

$$M_{m,n}(R) = \{(a_{ij}) \mid a_{ij} \in R \text{ for all } i, j\}.$$

Elements of $M_{m,n}(R)$ are called *matrices over R* of size $m \times n$. Matrix addition $A + B$ and multiplication AB are defined by the usual componentwise and summation formulas. More precisely, if $A, B \in M_{m,n}(R)$, then

$$(A + B)_{ij} = a_{ij} + b_{ij},$$

and if $A \in M_{m,n}(R)$ and $B \in M_{n,p}(R)$, then

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \quad 1 \leq i \leq m, 1 \leq j \leq p.$$

4.2. **Multilinear maps.**

Definition 4.2.1. 1. Let $R_0, \ldots, R_k$ be (not necessarily commutative) rings (Definition 2.1.1). Let M_i be a $R_{i-1} - R_i$-bimodule (Definition 2.2.1) for $i = 1, \ldots, k$, and let N be an $R_0 - R_k$-bimodule. A function $\Phi : M_1 \times \cdots \times M_k \to N$ is called a *multilinear map* (or *$R_0 - R_k$-multilinear*) if

- for each $j = 1, \ldots, k$ and fixed $m_i \in M_i$ for $i \neq j$, the map $M_j \to N$ given by $m_j \mapsto \Phi(m_1, \ldots, m_j, \ldots, m_k)$ is a group homomorphism (Definition 1.1.3) and
- for all $m_i \in M_i$ for $i = 1, \ldots, k$ and $r_j \in R_j$ where $j \in \{1, \ldots, k-1\}$, we have

$$\Phi(m_1, \ldots, m_j r_j, m_{j+1}, \ldots, m_k) = \Phi(m_1, \ldots, m_j r_j, r_j m_{j+1}, \ldots, m_k).$$

- Φ is left R_0-linear (Definition 2.2.3) in the first argument and right R_k-linear in the kth argument, i.e. for all $r_0 \in R_0$ and $r_k \in r_k$ we have

$$\Phi(r_0 m_1, m_2, \ldots, m_{k-1}, m_k r_k) = r_0 \cdot \Phi(m_1, \ldots, m_k) \cdot r_k.$$

2. Let R be a (not necessarily commutative) ring and let M be a two-sided R-module (Definition 2.2.3). A *multilinear form* is a multilinear map $M^r \to R$ (where M^r here is the set theoretic Cartesian product (Definition A.1.4), rather than a product of groups or modules) for some $r \geq 0$.

In particular, when R be a commutative ring (Definition 2.1.4), and M_i for $i = 1, \ldots, k$ and N are R-modules, we may speak of a multilinear map $\Phi : M_1 \times \cdots \times M_k \to N$. We may thus also speak of multilinear maps $M^r \to R$ for $r \geq 0$

Additionally, we may speak of *bilinear maps/forms*, *trilinear maps/forms*, etc.

Definition 4.2.2. Let R be a (not necessarily commutative) ring (Definition 2.1.1), M an two-sided R-module (Definition 2.2.3), $k \in \mathbb{N}$ and $\Phi : M^k \to R$ a multilinear form (Definition 4.2.1)

1. Φ is *symmetric* if for every permutation (Definition 1.1.17) $\sigma \in S_k$ and all $x_1, \ldots, x_k \in M$,
$$\Phi(x_1, ..., x_k) = \Phi(x_{\sigma(1)}, ..., x_{\sigma(k)}).$$
2. Φ is *antisymmetric* if for all $\sigma \in S_k$ and all $x_1, \ldots, x_k \in M$,
$$\Phi(x_{\sigma(1)}, ..., x_{\sigma(k)}) = \operatorname{sgn}(\sigma)\Phi(x_1, ..., x_k),$$
where $\operatorname{sgn}(\sigma)$ is the sign (Definition 1.1.18) of the permutation σ.
3. Φ is *alternating* if whenever $x_i = x_j$ for some $i \neq j$, $\Phi(x_1, ..., x_k) = 0$. Every alternating form is antisymmetric, since if $x_i = x_j$ and we swap coordinates, both terms are zero.

For $k = 2$, these definitions specialize to *bilinear forms*; in particular:

- Φ is symmetric if $\Phi(x, y) = \Phi(y, x)$.
- Φ is antisymmetric if $\Phi(x, y) = -\Phi(y, x)$.
- Φ is alternating if $\Phi(x, x) = 0$ for all x.

Definition 4.2.3. Let $n \in \mathbb{N}$. The symmetric group (Definition 1.1.17) on n letters is denoted by $\mathfrak{S}_n$. For a two-sided module (Definition 2.2.1) M over a (not necessarily commutative) ring (Definition 2.1.1), this group acts (on the right) (Definition 1.1.22) on the tensor power $M^{\otimes_R n}$ (Definition 2.2.39) by permutation of the tensor factors: on the pure tensors, the action is given by
$$(x_1 \otimes \cdots \otimes x_n) \cdot \sigma := x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}, \quad \sigma \in \mathfrak{S}_n,\ x_i \in M$$
and the action is extended linearly.

Definition 4.2.4. Let R be a (not necessarily commutative) ring (Definition 2.1.1), and let M an two-sided R-module (Definition 2.2.1).

1. The *symmetric power of M of degree n*, denoted by $S^n_R(M)$ or $\operatorname{Sym}^n(M) = \operatorname{Sym}^n_R(M)$, is the quotient two-sided module (Definition 2.2.18)
$$S^n_R(M) := M^{\otimes_R n}/I_{\text{sym}},$$
(Definition 2.2.39) where I_{sym} is the two-sided (Definition 2.2.1) submodule (Definition 2.2.2) of $M^{\otimes_R n}$ generated by (Definition 2.2.6) all elements of the form
$$x_1 \otimes \cdots \otimes x_n - (x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}), \qquad x_i \in M,\ \sigma \in \mathfrak{S}_n.$$
(Definition 1.1.17) (Definition 4.2.3)
2. The *exterior power of M of degree n*, denoted by $\Lambda^n_R(M)$, is the quotient two-sided module (Definition 2.2.18)
$$\Lambda^n_R(M) := M^{\otimes_R n}/I_{\text{alt}},$$

where I_{alt} is two-sided submodule (Definition 2.2.2) of $M^{\otimes_R n}$ generated by (Definition 2.2.6) all elements of the form

$$x_1 \otimes \cdots \otimes x_n - \operatorname{sgn}(\sigma)\,(x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(n)}), \qquad x_i \in M,\ \sigma \in \mathfrak{S}_n.$$

(Definition 1.1.17) (Definition 1.1.18)

In particular, we often speak of symmetric powers of exterior powers of modules over commutative rings (Definition 2.1.4) and even vector spaces (Definition 4.1.1) over fields (Definition 2.1.10).

4.3. **Sesquilinear and Hermitian forms.**

Definition 4.3.1. Let $\mathcal{C}$ be a category. An *involution on an object $X \in \mathrm{Ob}(\mathcal{C})$* is an endomorphism $i : X \to X$ such that $i \circ i = \mathrm{id}_X$.

Definition 4.3.2. Let R be a unital associative ring. An *involution on R* is a ring homomorphism (Definition 2.1.13) that is an involution (Definition 4.3.1), i.e. a map $\sigma : R \to R$ satisfying the following conditions for all $a, b \in R$:

1. $\sigma(a + b) = \sigma(a) + \sigma(b)$;
2. $\sigma(ab) = \sigma(b)\sigma(a)$ (anti-homomorphism property);
3. $\sigma(1) = 1$;
4. $\sigma(\sigma(a)) = a$.

In many contexts, an involution may simply be notated by $\cdot \mapsto \bar{\cdot}$ A *ring with involution* is a ring eqiupped with an involution.

Definition 4.3.3. Let (R, σ) be a ring with involution (Definition 4.3.2). Let M be a left R-module. A *σ-sesquilinear form* (or simply *sesquilinear form*) on M is a map $\phi : M \times M \to R$ such that for all $u, v, w \in M$ and $a \in R$:

1. $\phi(u + v, w) = \phi(u, w) + \phi(v, w)$ and $\phi(u, v + w) = \phi(u, v) + \phi(u, w)$;
2. $\phi(au, v) = a\phi(u, v)$ (linear in the first variable);
3. $\phi(u, av) = \phi(u, v)\sigma(a)$ (conjugate-linear in the second variable).

Definition 4.3.4. Let (R, σ) be a ring with involution (Definition 4.3.2) and M a left R-module (Definition 2.2.1). A *hermitian form on M* is a σ-sesquilinear form (Definition 4.3.3) $\phi : M \times M \to R$ satisfying the symmetry condition:

$$\phi(v, u) = \sigma(\phi(u, v))$$

for all $u, v \in M$. The pair (M, ϕ) is often called a *hermitian module*.

Definition 4.3.5. Let (R, σ) be a ring with involution (Definition 4.3.2). Let N be a left R-module (Definition 2.2.1). The *twisted dual module*, denoted $N^\vee$ or $\mathrm{Hom}_R(N, R)_\sigma$, is the set of all R-linear maps (Definition 2.2.3) $f : N \to R$, equipped with the left R-module structure given by

$$(r \cdot f)(n) = f(n)\sigma(r)$$

for all $r \in R$, $f \in N^\vee$, $n \in N$.

Definition 4.3.6. Let (R, σ) be a ring with involution (Definition 4.3.2) and M a left R-module (Definition 2.2.1) equipped with a sesquilinear form (Definition 4.3.3) $\phi : M \times M \to R$. The form ϕ is *nondegenerate* if the induced adjoint map

$$\hat{\phi} : M \to M^\vee, \quad u \mapsto (v \mapsto \phi(v, u))$$

is injective.

Definition 4.3.7. Let (R, σ) be a ring with involution and M a left R-module equipped with a sesquilinear form $\phi : M \times M \to R$. The *adjoint map of ϕ* is the morphism of R-modules

$$\hat{\phi} : M \to M^\vee, \quad u \mapsto (v \mapsto \phi(v, u))$$

where $M^\vee = \mathrm{Hom}_R(M, R)_\sigma$ is the twisted dual module (Definition 4.3.5).

4.4. **Quadratic forms.**

Definition 4.4.1 (Quadratic form over a ring with involution)**.** Let R be a ring with involution (Definition 4.3.2).

1. A quadratic form *on a right R-module M* is a map $q : M \to R$ such that:
   (a) $q(rm) = rq(m)\bar{r}$ for all $r \in R$, $m \in M$;
   (b) The map $B_q : M \times M \to R$ defined by $B_q(x, y) = q(x + y) - q(x) - q(y)$ is Hermitian.
2. A quadratic form *on a left R-module N* is a map $q : N \to R$ such that:
   (a) $q(rn) = \bar{r}q(n)r$ for all $r \in R$, $n \in N$;
   (b) The map $B_q : N \times N \to R$ defined by $B_q(x, y) = q(x + y) - q(x) - q(y)$ is Hermitian.

In either case, the form B_q is called the polarization *of q* or the *associated Hermitian form*, which may also be denoted by $\langle x, y \rangle_R = B_q(x, y)$.

A *quadratic module* refers to a module equipped with a quadratic form.

Definition 4.4.2 (Isometry of quadratic modules)**.** Let R be a ring with involution (Definition 4.3.2) and (M, q), (M', q') quadratic modules (Definition 4.4.1) over R (right or left modules consistently).

An *isometry* $\phi : M \to M'$ is an R-module isomorphism (Definition 2.2.3) such that $q'(\phi(m)) = q(m)$ for all $m \in M$.

Two quadratic modules (M, q) and (M', q') are isometric, written $(M, q) \cong (M', q')$, if there exists an isometry $\phi : M \to M'$.

Definition 4.4.3 (Non-degenerate quadratic form)**.** Let R be a ring with involution (Definition 4.3.2). Let $q : M \to R$ be a quadratic form (Definition 4.4.1). The quadratic form $q : M \to R$ is non-degenerate if for every $x \in M$, the map $y \mapsto \langle x, y \rangle_R$ is zero only if $x = 0$.

Definition 4.4.4 (Quadratic form on a module over a commutative ring)**.** Let R be a commutative ring (Definition 2.1.4). A quadratic form *on a R-module M* is a map $q : M \to R$ satisfying:

1. $q(rm) = r^2 q(m)$ for all $r \in R$, $m \in M$;
2. The map $b_q : M \times M \to R$ given by $b_q(x,y) = q(x+y) - q(x) - q(y)$ is R-bilinear (Definition 4.2.1).

The associated bilinear form b_q is called the polarization *of* q. It is also often written as B_q. One also often write $\langle x, y \rangle = B_q(x,y)$. Equivalently, a quadratic form on an R-module M for a commutative (unital) ring R is equivalent to a quadratic form (Definition 4.4.1) on M where R is considered as an involution ring (Definition 4.3.2) under the identity map.

A *quadratic module* refers to a module equipped with a quaratic form.

Definition 4.4.5. Let R be a commutative ring (Definition 2.1.4), and let M be a quadratic module (Definition 4.4.4).

An *isometry* $\phi : M \to M'$ is an R-module isomorphism such that $q'(\phi(m)) = q(m)$ for all $m \in M$.

Two quadratic modules (M, q) and (M', q') are *isometric*, written $(M,q) \cong (M', q')$, if there exists an isometry $\phi : M \to M'$.

Equivalently, these notions can be defiend via Definition 4.4.2 where R is considered as an involution ring with the identity morphism.

Definition 4.4.6 (Isotropic and hyperbolic)**.** Let R be a commutative ring (Definition 2.1.4). Let $q : M \to R$ be a quadratic form (Definition 4.4.4) on a module (Definition 2.2.1) over R.

1. An element $x \in M$ is isotropic if $q(x) = 0$.
2. A subspace $L \subset M$ is isotropic if $q(L) = 0$.
3. The quadratic form q is anisotropic if it has no non-zero isotropic vectors, i.e., $q(x) = 0$ implies $x = 0$.

Definition 4.4.7. Let R be a commutative ring (Definition 2.1.4). Let $q : M \to R$ be a quadratic form (Definition 4.4.4) on a module (Definition 2.2.1) over R.

The quadratic form q is called non-degenerate if $B_q(x, -) = 0$ implies $x = 0$. Equivalently, q is nondegenerate if it is nondegenerate (Definition 4.4.3) when considered as a quadratic form (Definition 4.4.1) on the module M where R is considered as an involution ring with the identity map.

Definition 4.4.8. Let R be a commutative ring (Definition 2.1.4). A *hyperbolic plane* is a quadratic module (Definition 4.4.4) isometric (Definition 4.4.5) to R^2 (Definition 2.2.16) eqiupped with the quadratic form given by $q(x,y) = xy$.

Lemma 4.4.9 (Properties of the hyperbolic plane)**.** Let (H, q_H) be a hyperbolic plane (Definition 4.4.8) over a commutative ring (Definition 2.1.4) R. Then:

1. The polarization (Definition 4.4.4) is $B_{q_H}((x_1, y_1), (x_2, y_2)) = x_1 y_2 + y_1 x_2$.
2. The vectors $e_1 = (1, 0)$ and $e_2 = (0, 1)$ satisfy $q_H(e_1) = q_H(e_2) = 0$ and $B_{q_H}(e_1, e_2) = 1$. (♠ TODO: symplectic basis)
3. H admits a symplectic basis $\{e_1, e_2\}$ where $B_{q_H}(e_i, e_j) = \delta_{i,3-j}$.

Proposition 4.4.10 (Isomorphism criterion)**.** Let R be a commutative ring (Definition 2.1.4), M a module (Definition 2.2.1) of R, $H \cong R^2$ a submodule (Definition 2.2.2) of M, and $q : M \to R$ a quadratic form (Definition 4.4.4). Then $(H, q|_H)$ is a hyperbolic plane (Definition 4.4.8) if and only if $q|_H \cong q_H$ as quadratic forms via some basis of H.

Proposition 4.4.11 (Witt cancellation)**.** Let R be a field (Definition 2.1.10) and $q : M \to R$, $q' : M' \to R$ quadratic forms (Definition 4.4.4) such that $(M, q) \cong (M', q') \oplus (H, q_H)$ as quadratic modules, where (H, q_H) is a hyperbolic plane (Definition 4.4.8). Then $(M, q) \cong (M', q')$ (Definition 4.4.5).

Theorem 4.4.12 (Witt decomposition theorem)**.** Let R be a field (Definition 2.1.10) and $q : M \to R$ a non-degenerate (Definition 4.4.7) quadratic form (Definition 4.4.4). Then there exists a unique (up to isomorphism) decomposition $M \cong M_a \oplus H^k$ where M_a is anisotropic (Definition 4.4.6) and H^k is a direct sum of k hyperbolic planes (Definition 4.4.8). (♠ TODO: direct sum of quadratic modules)

The integer k is called the Witt index *of* q.

Corollary 4.4.13 (Dimension formula)**.** Let R be a field (Definition 2.1.10) and $q : M \to R$ a non-degenerate (Definition 4.4.7) quadratic form (Definition 4.4.4). We have $\dim M \equiv \dim M_a \pmod 2$.

5. More group theory

5.1. Topological groups.

Definition 5.1.1 (Topological groups)**.** (♠ TODO: Product topology) A *topological group* is a group (Definition 1.1.1) $(G, \cdot)$ together with a topology (Definition A.3.1) $\mathcal{T}$ on G such that the maps

$$\begin{aligned} \mu : G \times G &\to G, & (g, h) &\mapsto g \cdot h, \\ \iota : G &\to G, & g &\mapsto g^{-1}, \end{aligned}$$

are continuous (Definition A.3.2) with respect to the product topology on $G \times G$ and the topology $\mathcal{T}$ on G.

Definition 5.1.2 (Topological rings)**.** (♠ TODO: Product topology) A *topological ring* is a (not necessarily commutative) ring (Definition 2.1.1) $(R, +, \cdot)$ together with a topology (Definition A.3.1) $\mathcal{T}$ on R such that the maps

$$\begin{aligned} + : R \times R \to R \quad & (a, b) \mapsto a + b \\ \cdot : R \times R \to R \quad & (a, b) \mapsto a \cdot b \\ - : R \to R \quad & a \mapsto -a \end{aligned}$$

are continuous (Definition A.3.2) with respect to the product topology on $R \times R$ and the topology $\mathcal{T}$ on R. Equivalently, a topological ring is a ring whose addition structure forms a topological group (Definition 5.1.1) and whose multiplication structure is also continuous.

Definition 5.1.3 (Topological fields)**.** (♠ TODO: Product topology) A *topological field* is a field (Definition 2.1.10) $(F, +, \cdot)$ together with a topology (Definition A.3.1) $\mathcal{T}$ on F such that the maps

$$\begin{aligned} + &: F \times F \to F \quad (a, b) \mapsto a + b \\ \cdot &: F \times F \to F \quad (a, b) \mapsto a \cdot b \\ - &: F \to F \quad a \mapsto -a \\ \cdot^{-1} &: F^\times \to F^\times \quad a \mapsto a^{-1} \end{aligned}$$

are continuous (Definition A.3.2) with respect to the product topology on $F \times F$, the topology $\mathcal{T}$ on F, and the subset topology on the unit group $F^\times = F - \{0\}$ (Definition 2.1.8). Equivalently, a topological field is a field with a topology which becomes a topological ring (Definition 5.1.2) under the ring structure and whose multiplicative inverse is also continuous.

Definition 5.1.4 (Topological fields)**.** (♠ TODO: Product topology) Let $(F, +, \cdot)$ be a topological field (Definition 5.1.3). A *topological vector space over F* or an *F-topological vector space* is an F-vector space $(V, +, \cdot)$ together with a topology (Definition A.3.1) $\mathcal{T}_V$ on V such that the maps

$$\begin{aligned} + &: V \times V \to V \quad (v, w) \mapsto v + w \\ \cdot &: F \times V \to V \quad (a, v) \mapsto a \cdot v \\ - &: V \to V \quad v \mapsto -v \end{aligned}$$

are continuous (Definition A.3.2) with respect to the product topologies on $V \times V$ and $F \times V$ and the topology $\mathcal{T}_V$ on V. Equivalently, a topological vector space is a vector space over a topological field with a topology which becomes a topological group (Definition 5.1.1) under the additive structure and whose scalar multiplication map is continuous.

5.2. **Profinite groups.**

Definition 5.2.1 (Profinite groups)**.** A *profinite group* is a topological group (Definition 5.1.1) that is compact (Definition A.3.3), Hausdorff, and totally disconnected. (♠ TODO: describe the topology)

Equivalently, a profinite group is the inverse limit of an inverse system of finite groups equipped with the discrete topology. That is,

$$G \cong \varprojlim_{i \in I} G_i,$$

(♠ TODO: define basis of a topology, rougher topologies,) where each G_i is a finite group and the connecting maps are group homomorphisms. The topology on G is called the *profinite topology* and is the roughest topology making the projection maps $G \to G_i$ continuous (Definition A.3.2); equivalently, the preimages of singletons under the projection maps $G \to G_i$ form a basis of open subsets (and in fact a basis of clopen subsets).

Appendix A. Miscellaneous definitions

A.1. **Set Theory.**

Definition A.1.1 (Small Set)**.** A *small set* refers to a set; the adjective of *small* is used to emphasize that the set is a set, rather than a proper class.

Alternatively, a *small set* is any object that belongs to a fixed universe of sets $\mathcal{U}$, called the *universe of small sets*. In other words, a set A is said to be *small* if and only if $A \in \mathcal{U}$. Elements of $\mathcal{U}$ may themselves be sets, but $\mathcal{U}$ is not assumed to be a set; it may be a proper class.

Definition A.1.2 (Subset)**.** Let A and B be sets. The set A is said to be a *subset of B*, written as $A \subseteq B$ or $A \subset B$, if every element of A is also an element of B, that is,

$$A \subseteq B \iff \forall x\,(x \in A \Rightarrow x \in B).$$

If $A \subseteq B$ and $A \neq B$, then A is called a *proper subset of B*; this is commonly denoted by $A \subsetneq B$.

Definition A.1.3. Let X and Y be sets and let $f : X \to Y$ be a function.

- The function f is said to be *injective* (or *one-to-one*) if for all $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$.
- The function f is said to be *surjective* (or *onto*) if for every $y \in Y$ there exists $x \in X$ such that $f(x) = y$.
- The map f is *bijective* if it is both injective and surjective. In this case, there exists a unique *inverse map* $f^{-1} : Y \to X$ such that for all $x \in X$ and $y \in Y$,

$$f^{-1}(f(x)) = x \text{ and } f(f^{-1}(y)) = y.$$

Definition A.1.4 (Product of Sets)**.** Let I be a (possibly infinite (Definition A.1.5) but small (Definition A.1.1)) index set and let $\{A_i\}_{i\in I}$ be a family of sets indexed by I. The *Cartesian product of the family $\{A_i\}_{i\in I}$*, denoted by $\prod_{i\in I} A_i$, is defined as the set of all tuples/functions (Definition A.1.6)

$$\prod_{i\in I} A_i := \{(a_i)_{i\in I} \mid a_i \in A_i \text{ for all } i \in I\},$$

where $(a_i)_{i\in I}$ denotes a function from I to $\bigcup_{i\in I} A_i$ such that $(a_i)_{i\in I}(i) = a_i \in A_i$ for each $i \in I$.

The self product of a set A indexed by I is often denoted by A^I. Note that elements of A^I can be identified with functions (Definition A.1.6) $I \to A$. The finite self product of A taken n times is often denoted by A^n. For finitely many sets $A_1, \ldots, A_n$, their Cartesian product is denoted by $A_1 \times \cdots \times A_n$. Elements of such a finite product may be written as $(a_1, \ldots, a_n)$.

Definition A.1.5. Let A be a set.

- The set A is said to be *countably infinite* (or simply *countable*) if there exists a bijection $f : \mathbb{N} \to A$.

- The set A is said to be *finite* if there exists some $n \in \mathbb{N}$ and a bijection $g : \{1, 2, \ldots, n\} \to A$.
- The set A is said to be *at most countable* if it is either finite or countably infinite.
- The set A is said to be *uncountable* if it is not at most countable.

Definition A.1.6. Let X and Y be sets. A *map* (or *function*) from X to Y is a rule f assigning to each element $x \in X$ exactly one element $f(x) \in Y$. We write $f : X \to Y$.

We say that X is the *domain* and that Y is the *codomain of f*.

Definition A.1.7. Let X be a set. The *identity function on X*, denoted by id_X, is the function (Definition A.1.6) $\mathrm{id}_X : X \to X$ defined by

$$\mathrm{id}_X(x) = x \quad \text{for all } x \in X.$$

It is the unique function on X satisfying $f \circ \mathrm{id}_X = f = \mathrm{id}_X \circ f$ for every function $f : X \to Y$ and every function $f : Y \to X$.

Definition A.1.8. Let n be a positive integer. Let $X_1, X_2, \ldots, X_n$ be sets. An *n-ary relation* on these sets is a subset $R \subseteq X_1 \times X_2 \times \cdots \times X_n$. The integer n is called the *arity* (or *degree*) of the relation. The sets $X_1, \ldots, X_n$ are called the *domains of the relation*.

If $(x_1, x_2, \ldots, x_n) \in R$, we say that the elements $x_1, \ldots, x_n$ are *related* by R.

In the special case where $X_1 = X_2 = \cdots = X_n = X$, we say that R is an *n-ary relation on the set X*. In this case, $R \subseteq X^n$.

Specific arities have standard names:

- A *unary relation* on X is a subset of X (arity $n = 1$).
- A *binary relation* from X to Y is a subset of $X \times Y$ (arity $n = 2$).
- A *ternary relation* is a subset of $X \times Y \times Z$ (arity $n = 3$).

Definition A.1.9. An *equivalence relation on a set X* is a binary relation (Definition A.1.8) on X that is reflexive, symmetric, and transitive.

Definition A.1.10. If $\sim$ is an equivalence relation on a set X and $x \in X$, the *equivalence class of x*, denoted by $[x]$ or $[x]_\sim$, is the set defined by

$$[x] = \{y \in X \mid x \sim y\}.$$

The set of all equivalence classes is called the *quotient set of X by $\sim$*, denoted by $X/{\sim}$.

Definition A.1.11. An ordinal number κ is a *cardinal number* (or simply a *cardinal*) if for every ordinal $\alpha < \kappa$, there is no bijection (Definition A.1.3) between α and κ. Equivalently, a cardinal is an initial ordinal—an ordinal that is not equinumerous with any smaller ordinal.

The *cardinality of an arbitrary set X*, denoted by $|X|$, $\mathrm{card}(X)$, or $\#X$, is the unique cardinal number κ such that there exists a bijection between X and κ. (The existence of such a κ for every set requires the Axiom of Choice).

A.2. **Algebraic definitions.**

Definition A.2.1 (Semigroup)**.** A *semigroup* is a pair $(M, \cdot)$ where M is a set and $\cdot : M \times M \to M$ is a binary operation satisfying the associativity law:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{for all } a, b, c \in M.$$

A semigroup is said to be *commutative* if the binary operation also satisfies the commutativity law:

$$a \cdot b \quad \text{for all}a, b \in M.$$

Definition A.2.2 (Monoid)**.** A *monoid* is a semigroup (Definition A.2.1) $(M, \cdot)$ such that there exists an element $e \in M$, called the *identity element*, with the property:

$$e \cdot a = a \cdot e = a \quad \text{for all } a \in M.$$

Definition A.2.3. Let G be a set and let $\cdot : G \times G \to G$ be a binary operation. The operation $\cdot$ is called *abelian* or *commutative* if for all $g, h \in G$, we have

$$g \cdot h = h \cdot g.$$

A.3. **Topological definitions.**

Definition A.3.1 (Topology)**.** Let X be a set. A *topology on X* is a collection $\mathcal{T}$ of subsets of X such that:

1. $\emptyset \in \mathcal{T}$ and $X \in \mathcal{T}$,
2. For any collection $\{U_i\}_{i \in I} \subseteq \mathcal{T}$ (with I arbitrary), the union $\bigcup_{i \in I} U_i \in \mathcal{T}$,
3. For any finite collection $\{U_1, \ldots, U_n\} \subseteq \mathcal{T}$, the intersection $U_1 \cap \cdots \cap U_n \in \mathcal{T}$.

If $\mathcal{T}$ is a topology on X, the pair $(X, \mathcal{T})$ is called a *topological space*. Members of $\mathcal{T}$ are called *open sets*.

A subset $C \subseteq X$ is *closed* if its complement $X \setminus C$ is an open set in $\mathcal{T}$

One very often refers to X as a topological spcae, omitting the notation of the topology $\mathcal{T}$.

The collection of all topologies on a set X may be denoted by notations such as $\mathrm{Top}(X)$, $\mathbf{Top}(X)$, or $\mathsf{Top}(X)$.

Definition A.3.2. Let $U \subseteq \mathbb{R}^n$ and $V \subseteq \mathbb{R}^m$ be open subsets, and let $k \in \mathbb{N}_0 \cup \{\infty\}$. A *continuous morphism* (or a *continuous map* or simply a *map between topological spaces*) from U to V is a function $f : U \to V$ that satisfies one of the following equivalent characterizations:

1. f is a continuous map from U to V as topological spaces.
2. for every point $x \in U$, for every open neighborhood W of $f(x)$ in V, there exists an open neighborhood O of x in U satisfying

$$f(O) \subseteq W.$$

We write $C(U, V) = C^0(U, V)$ for the set of continuous maps $U \to V$.

Definition A.3.3 (Compact topological space)**.** A topological space $(X, \mathcal{T})$ is *compact* if every open cover of X admits a finite subcover; that is, for every collection $\{U_i\}_{i \in I}$ of open sets in $\mathcal{T}$ such that $X = \bigcup_{i \in I} U_i$, there exists a finite subcollection $\{U_{i_j}\}_{j=1}^{n}$ such that $X = \bigcup_{j=1}^{n} U_{i_j}$.

Some mathematicians, e.g. algebraic geometers, would refer to this property as *quasi-compactness*.

A.4. **Categorical definitions.**

Definition A.4.1 (Category)**.** A *category* *category* $\mathcal{C}$ consists of the following data:

- A class of *objects* denoted $\mathrm{Ob}(\mathcal{C})$.
- For each pair of objects $X, Y \in \mathrm{Ob}(\mathcal{C})$, a class

$$\mathrm{Hom}_{\mathcal{C}}(X, Y)$$

  of *morphisms* (also called *arrows* or *homs*). If the category $\mathcal{C}$ is clear, then this *hom-class* is also denoted by $\mathrm{Hom}(X, Y)$. It may also be denoted by $\mathrm{hom}_{\mathcal{C}}(X, Y)$ or $\mathrm{hom}(X, Y)$, especially to distinguish from other types of hom's (e.g. internal hom's)
- For each triple of objects X, Y, Z, a composition law

$$\circ : \mathrm{Hom}_{\mathcal{C}}(Y, Z) \times \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, Z),$$

  denoted $(g, f) \mapsto g \circ f$.
- For each object X, an *identity morphism*

$$\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X, X).$$

These data satisfy the following axioms:

- (Associativity) For all morphisms $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$, and $h \in \mathrm{Hom}_{\mathcal{C}}(Z, W)$,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

- (Identity) For all $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$,

$$\mathrm{id}_Y \circ f = f = f \circ \mathrm{id}_X.$$

One often writes $X \in \mathcal{C}$ synonymously with $X \in \mathrm{Ob}(\mathcal{C})$, i.e. to denote that X is an object of of $\mathcal{C}$.

We may call a category as above an *ordinary category* to distinguish this notion from the notions of *categories enriched in monoidal categories* or higher/n-categories. (♠ TODO: TODO: define n-categories)

A category as defined above may be called called a *large category* or a *class category* to emphasize that the hom-classes may be proper classes rather than sets (note, however, that the possibility that hom-classes are sets is not excluded for large categories). Accordingly, a *category* may often refer to a locally small category (Definition A.4.3), which is a category whose hom-classes are all sets.

Definition A.4.2. Let $\mathcal{C}$ be a category (Definition A.4.1) and X be an object of $\mathcal{C}$.

1. An *automorphism of X* is a morphism $f : X \to X$ that is an isomorphism. That is, there exists a morphism $g : X \to X$ such that $f \circ g = \mathrm{id}_X$ and $g \circ f = \mathrm{id}_X$.
2. Assume that $\mathcal{C}$ is a locally small category (Definition A.4.3). The *automorphism group of X*, denoted $\mathrm{Aut}_{\mathcal{C}}(X)$, is the set of all automorphisms of X. It is indeed a group (Definition 1.1.1) (Proposition 1.5.2) and the group operation is the composition of morphisms in $\mathcal{C}$.

Definition A.4.3 (Locally small category)**.** A (large) category (Definition A.4.1) $\mathcal{C}$ is called a *locally small category* if for every pair of objects $X, Y \in \mathrm{Ob}(\mathcal{C})$, the collection $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ of morphisms between them is a (small (Definition A.1.1)) *set* (as opposed to a proper class). In other words, each hom-class is a set and may even be called a *hom-set*.

In some contexts, a locally small category may simply be called a *category*, especially when genuinely large categories are not considered.

A category $\mathcal{C}$ is called a *small category* if it is a locally small category and the class $\mathrm{Ob}(\mathcal{C})$ of objects is a set.

Remark A.4.4. Many "concrete" categories considered in "classical mathematics" or outside of more "abstract" category theory tend to be locally small. For example, the categories of sets, groups, R-modules, vector spaces, topological spaces, schemes, manifolds, sheaves on "small enough" sites are all locally small.

Definition A.4.5. Let $\mathcal{C}$ and $\mathcal{D}$ be (large) categories (Definition A.4.1).

1. A *functor $F : \mathcal{C} \to \mathcal{D}$ (from $\mathcal{C}$ to $\mathcal{D}$)* consists of :
   - For each object X in $\mathcal{C}$, an object $F(X)$ in $\mathcal{D}$.
   - For each morphism $f : X \to Y$ in $\mathcal{C}$, a morphism $F(f) : F(X) \to F(Y)$ in $\mathcal{D}$,

   such that:
   $$\begin{aligned} F(\mathrm{id}_X) &= \mathrm{id}_{F(X)} \quad \text{for all objects } X \text{ in } \mathcal{C}, \\ F(g \circ f) &= F(g) \circ F(f) \quad \text{for all } X, Y, Z \in \mathrm{Ob}(\mathcal{C}) \text{ and all } f : X \to Y, g : Y \to Z \text{ in } \mathcal{C}. \end{aligned}$$

   Functors as defined above are also referred to as *covariant functors* to distinguish them from contravariant functors
2. A *contravariant functor from $\mathcal{C}$ to $\mathcal{D}$* refers to a covariant functor $F : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$. Equivalently, such a functor consists of
   - For each object X in $\mathcal{C}$, an object $F(X)$ in $\mathcal{D}$.
   - For each morphism $f : X \to Y$ in $\mathcal{C}$, a morphism $F(f) : F(Y) \to F(X)$ in $\mathcal{D}$,

   such that:
   $$\begin{aligned} F(\mathrm{id}_X) &= \mathrm{id}_{F(X)} \quad \text{for all objects } X \text{ in } \mathcal{C}, \\ F(g \circ f) &= F(f) \circ F(g) \quad \text{for all } X, Y, Z \in \mathrm{Ob}(\mathcal{C}) \text{ and all } f : X \to Y, g : Y \to Z \text{ in } \mathcal{C}. \end{aligned}$$

Note that declarations such as "Let $F : \mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ be a contravariant functor" can be common; such declarations usually mean "Let F be a contravariant functor from $\mathcal{C}$ to $\mathcal{D}$" as opposed to "Let F be a contravariant functor from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{D}$". further note that a contravariant functor from $\mathcal{C}$ to $\mathcal{D}$ is equivalent to a covariant functor from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{D}$.

Definition A.4.6. Let $\mathcal{C}$ and $\mathcal{D}$ be (large) categories (Definition A.4.1). Let $F, G : \mathcal{C} \to \mathcal{D}$ be functors (Definition A.4.5).

A *natural transformation η between F and G* is a family of morphisms $\eta_X : F(X) \to G(X)$ in $\mathcal{D}$, one for each object X in $\mathcal{C}$, such that for every morphism $f : X \to Y$ in $\mathcal{C}$,

$$G(f) \circ \eta_X = \eta_Y \circ F(f)$$

in $\mathcal{D}$. In other words, the following diagram commutes:

$$\begin{tikzcd}
F(X) \arrow[r, "F(f)"] \arrow[d, "\eta_X"'] & F(Y) \arrow[d, "\eta_Y"] \\
G(X) \arrow[r, "G(f)"'] & G(Y)
\end{tikzcd}$$

We write such a natural transformation by $\eta : F \Rightarrow G$.

If η_X is an isomorphism for all objects X of $\mathcal{C}$, then η is said to be a *natural isomorphism*.

Definition A.4.7. An *equivalence of categories* between two (large) categories (Definition A.4.1) $\mathcal{C}$ and $\mathcal{D}$ consists of a pair of functors (Definition A.4.5)

$$F : \mathcal{C} \to \mathcal{D} \quad \text{and} \quad G : \mathcal{D} \to \mathcal{C}$$

together with natural isomorphisms (Definition A.4.6)

$$\eta : \mathrm{Id}_{\mathcal{C}} \xrightarrow{\sim} G \circ F \quad \text{and} \quad \epsilon : F \circ G \xrightarrow{\sim} \mathrm{Id}_{\mathcal{D}}.$$

Such functors F and G may be called *(natural) inverses of each other*.

When $\mathcal{C}$ and $\mathcal{D}$ are locally small categories (Definition A.4.3), F is an equivalence of categories if and only if F is fully faithful (Definition A.4.26) and essentially surjective

Definition A.4.8 (Category of objects over a fixed object)**.** Let $\mathcal{C}$ be a category (Definition A.4.1) and let $X \in \mathrm{Ob}(\mathcal{C})$ be a fixed object.

1. The *category of objects over X* (or synonymously the *slice category of X in $\mathcal{C}$* or the *over category of X in $\mathcal{C}$*), commonly denoted $\mathcal{C}/X$ or $\mathcal{C}_{/X}$, is the category defined as follows:
   - An object of $\mathcal{C}/X$ is a morphism $f\colon A \to X$ in $\mathcal{C}$, where $A \in \mathrm{Ob}(\mathcal{C})$.
   - A morphism from $f\colon A \to X$ to $g\colon B \to X$ in $\mathcal{C}/X$ is a morphism $h\colon A \to B$ in $\mathcal{C}$ such that the following diagram commutes:

     $$\begin{tikzcd}
     A \arrow[r, "h"] \arrow[dr, "f"'] & B \arrow[d, "g"] \\
     & X
     \end{tikzcd}$$

     i.e. such that $g \circ h = f$.
   - The identity morphisms and composition in $\mathcal{C}/X$ are inherited from $\mathcal{C}$.

2. The *category of objects under X* (or synonymously the *coslice category of X in $\mathcal{C}$* or the *under category of X in $\mathcal{C}$*), commonly denoted $X/\mathcal{C}$, $X\backslash\mathcal{C}$ or $\mathcal{C}_{X/}$, is the category defined as follows:
   - An object of $X/\mathcal{C}$ is a morphism $f\colon X \to A$ in $\mathcal{C}$, where $A \in \mathrm{Ob}(\mathcal{C})$.
   - A morphism from $f\colon X \to A$ to $g\colon X \to B$ in $X/\mathcal{C}$ is a morphism $h\colon A \to B$ in $\mathcal{C}$ such that the following diagram commutes:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "g"'] & A \arrow[d, "h"] \\ & B \end{tikzcd}$$

     i.e. such that $h \circ f = g$.
   - The identity morphisms and composition in $X/\mathcal{C}$ are inherited from $\mathcal{C}$.

Definition A.4.9. Let $\mathcal{C}$ be a (large) category (Definition A.4.1).

1. An object $I \in \mathcal{C}$ is called an *initial object* if for every object $X \in \mathcal{C}$ there exists a unique morphism
$$I \to X.$$
Equivalently, an initial object is a limit (Definition A.4.19) of the empty diagram, if such a limit exists.
2. An object $F \in \mathcal{C}$ is called a *final object* (or *terminal object*) if for every object $X \in \mathcal{C}$ there exists a unique morphism
$$X \to F.$$
Equivalently, a final object is a colimit (Definition A.4.19) of the empty diagram, if such a colimit exists.
3. An object $Z \in \mathcal{C}$ is called a *zero object* if Z is both initial and final in $\mathcal{C}$. In particular, for every object $X \in \mathcal{C}$ there exist unique morphisms
$$Z \to X \quad \text{and} \quad X \to Z.$$

In particular, if initial/final/zero objects exist in a cateogry, then they are unique up to unique isomorphism.

Definition A.4.10 (Full subcategory)**.** Let $\mathcal{C}$ be a (large) category (Definition A.4.1). A *full subcategory* $\mathcal{D}$ of $\mathcal{C}$ is a subcategory such that for every pair of objects $X, Y \in \mathrm{Ob}(\mathcal{D})$, the morphism classes coincide:
$$\mathrm{Hom}_{\mathcal{D}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y).$$

In other words, a full subcategory includes all morphisms between its objects that exist in the ambient category $\mathcal{C}$.

Definition A.4.11. (♠ TODO: make it soe that the for excerpts using this, the categories involved are locally small) Let $\mathcal{C}$ and $\mathcal{D}$ be locally small (Definition A.4.3) categories (or U-locally small categories if a universe U is available).

Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be functors. F is a *left adjoint to G* and G is a *right adjoint to F* (written $F \dashv G$) if for every object A in $\mathcal{C}$ and B in $\mathcal{D}$ there is a natural isomorphism (Definition A.4.6)

$$\mathrm{Hom}_{\mathcal{D}}(F(A), B) \cong \mathrm{Hom}_{\mathcal{C}}(A, G(B))$$

that is natural in both A and B.

Definition A.4.12 (Opposite category)**.** Let $\mathcal{C}$ be a (large) category (Definition A.4.1). The *opposite category* of $\mathcal{C}$, denoted $\mathcal{C}^{\mathrm{op}}$, is defined as follows:

- The objects of $\mathcal{C}^{\mathrm{op}}$ are the same as those of $\mathcal{C}$.
- For any pair of objects $X, Y \in \mathcal{C}$, the morphisms from X to Y in $\mathcal{C}^{\mathrm{op}}$ are given by the morphisms from Y to X in $\mathcal{C}$:

$$\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X, Y) := \mathrm{Hom}_{\mathcal{C}}(Y, X).$$

- Composition in $\mathcal{C}^{\mathrm{op}}$ is defined by reversing the order of composition in $\mathcal{C}$. That is, for morphisms $f \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(X, Y)$ and $g \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(Y, Z)$, their composition is

$$g \circ_{\mathcal{C}^{\mathrm{op}}} f := f \circ_{\mathcal{C}} g.$$

Intuitively, the category $\mathcal{C}^{\mathrm{op}}$ thus "reverses" the direction of all morphisms in $\mathcal{C}$.

Definition A.4.13. Let $\mathcal{C}$ be a (large) category (Definition A.4.1), and let $c_1, c_2, \ldots, c_n \in \mathrm{Ob}(\mathcal{C})$ be objects.

A *product of* $c_1, c_2, \ldots, c_n$ in $\mathcal{C}$ is a tuple

$$\big(c_1 \times c_2 \times \cdots \times c_n,\ p_1 : c_1 \times \cdots \times c_n \to c_1,\ \ldots,\ p_n : c_1 \times \cdots \times c_n \to c_n\big)$$

such that for every object $d \in \mathrm{Ob}(\mathcal{C})$ and every family of morphisms

$$(f_1 : d \to c_1,\ f_2 : d \to c_2,\ \ldots,\ f_n : d \to c_n),$$

there exists a unique morphism

$$\langle f_1, f_2, \ldots, f_n \rangle : d \to c_1 \times c_2 \times \cdots \times c_n$$

satisfying

$$p_i \circ \langle f_1, f_2, \ldots, f_n \rangle = f_i \quad \text{for all } 1 \leq i \leq n.$$

The morphisms p_i are called the *projection morphisms*, and the morphism $\langle f_1, f_2, \ldots, f_n \rangle$ is called the *product morphism*. The product $c_1 \times \cdots \times c_n$ is also denoted by $\prod_{i=1}^n c_i$, $c_1 \oplus \cdots \oplus c_n$, or $\bigoplus_{i=1}^n c_i$.

When $n = 0$, the product is defined to be a terminal object (Definition A.4.9) of $\mathcal{C}$, if one exists. When $n = 2$, we simply speak of the *binary product* or *biproduct* of c_1 and c_2.

Definition A.4.14. Let $\mathcal{C}$ be a (large) (Definition A.4.1) pointed category, i.e. a category with a zero object (Definition A.4.9) 0. Let $X, Y \in \mathrm{Ob}(\mathcal{C})$ be an object and let $f : X \to Y$ be a morphism.

1. A morphism $i : K \to X$ is called the *kernel of f* if:
   (a) $f \circ i = 0$, where 0 is the zero morphism $K \to Y$,

   (b) for any morphism $g : Z \to X$ such that $f \circ g = 0$, there exists a unique morphism $u : Z \to K$ such that $g = i \circ u$.

   The kernel, if it exists, is unique up to unique isomorphism. $\ker(f)$ denotes the object K determined (up to isomorphism) by a kernel of f.

2. a morphism $p : Y \to Q$ is called the *cokernel of f* if:
   (a) $p \circ f = 0$, where 0 is the zero morphism (Definition A.4.9) $X \to Q$,
   (b) for any morphism $g : Y \to Z$ such that $g \circ f = 0$, there exists a unique morphism $v : Q \to Z$ such that $g = v \circ p$.

   The cokernel, if it exists, is unique up to unique isomorphism. $\operatorname{coker}(f)$ denotes the object Q determined (up to isomorphism) by a cokernel of f.

Definition A.4.15. Let $\mathcal{C}$ be a category (Definition A.4.1), and let $f : A \to B$ be a morphism in $\mathcal{C}$.

1. An *image of f* consists of an object $I \in \mathrm{Ob}(\mathcal{C})$ together with a factorization of f into two morphisms

$$A \xrightarrow{e} I \xrightarrow{m} B,$$

   where e is an epimorphism (Definition A.4.23) and m is a monomorphism (Definition A.4.23), such that for any other factorization

$$A \xrightarrow{e'} I' \xrightarrow{m'} B$$

   with e' epi and m' mono, there exists a unique isomorphism $\varphi : I \simeq I'$ satisfying $m = m'\varphi$ and $\varphi e = e'$.

$$\begin{tikzcd}
& I \arrow[dr, hook, "m"] \arrow[dd, dashed, "\exists!\varphi", "\wr"'] & \\
A \arrow[ur, two heads, "e"] \arrow[dr, two heads, "e'"'] & & B \\
& I' \arrow[ur, hook, "m'"'] &
\end{tikzcd}$$

   The monomorphism $m : I \to B$ (or equivalently its subobject class) is called the *image of f in* $\mathcal{C}$.

2. Let $\mathcal{C}$ be a category (Definition A.4.1), and let $f : A \to B$ be a morphism in $\mathcal{C}$. A *coimage of f* consists of an object $C \in \mathrm{Ob}(\mathcal{C})$ together with a factorization of f into two morphisms

$$A \xrightarrow{e} C \xrightarrow{m} B,$$

   where e is an epimorphism and m is a monomorphism, such that for any other factorization

$$A \xrightarrow{e'} C' \xrightarrow{m'} B$$

   with e' epi and m' mono, there exists a unique isomorphism $\varphi : C \simeq C'$ satisfying $m = m'\varphi$ and $\varphi e = e'$.

$$\begin{tikzcd}
 & C \arrow[dr, hook, "m"] \arrow[dd, dashed, "\exists!\varphi", "\wr"'] & \\
A \arrow[ur, two heads, "e"] \arrow[dr, two heads, "e'"'] & & B \\
 & C' \arrow[ur, hook, "m'"'] &
\end{tikzcd}$$

The epimorphism $e : A \to C$ (or equivalently its quotient class) is called the *coimage of f in $\mathcal{C}$*.

Definition A.4.16 (Complete and Cocomplete Category)**.** Let $\mathcal{C}$ be a category (Definition A.4.1).

- The category $\mathcal{C}$ is called *complete* (resp. *finitely complete*) if all small limits (Definition A.4.22) (resp. finite limits) exist in $\mathcal{C}$; that is, for every small diagram $D : J \to \mathcal{C}$ (with J a small category), the limit $\lim D$ exists and is an object of $\mathcal{C}$.
- The category $\mathcal{C}$ is called *cocomplete* (resp. *finitely cocomplete*) if all small colimits (Definition A.4.22) (resp. finite colimits) exist in $\mathcal{C}$; that is, for every small diagram $D : J \to \mathcal{C}$, the colimit colim D exists and is an object of $\mathcal{C}$.

Definition A.4.17 (Filtered category)**.** 1. A *filtered category* is a (nonempty, large) category $\mathcal{I}$ satisfying the following conditions:

- For every finite collection of objects $i_1, i_2, \ldots, i_n$ in $\mathcal{I}$, there exists an object j and morphisms
$$\phi_k : i_k \to j, \quad \text{for each } k = 1, \ldots, n.$$
- For every pair of morphisms $f, g : i \to j$ in $\mathcal{I}$, there exists an object k and a morphism
$$h : j \to k$$
(♠ TODO: equalizer) that is an equalizer of f and g, i.e. satisfies
$$h \circ f = h \circ g.$$

$$\begin{tikzcd}
i_1 \arrow[dr, dashed, "\phi_1"] & \\
 & j \\
i_2 \arrow[ur, dashed, "\phi_2"'] &
\end{tikzcd}$$

Figure 1. *
Condition 1: Upper Bound

$$\begin{tikzcd}
i \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & j \arrow[r, dashed, "h"] & k
\end{tikzcd}$$

Figure 2. *
Condition 2: Equalizer

In other words, $\mathcal{I}$ is nonempty, any finite diagram of objects admits a cocone (Definition A.4.19), and any pair of parallel morphisms become equal after post-composition with an appropriate morphism.

2. Dually, a *Cofiltered category* is a category whose opposite category (Definition A.4.12) is filtered. More explicitly, A cofiltered category is a (nonempty, large) category $\mathcal{I}$ satisfying the following conditions:
   - For every finite collection of objects $i_1, i_2, \ldots, i_n$ in $\mathcal{I}$, there exists an object j and morphisms
   $$\phi_k : j \to i_k, \quad \text{for each } k = 1, \ldots, n.$$
   - For every pair of morphisms $f, g : j \to i$ in $\mathcal{I}$, there exists an object k and a morphism
   $$h : k \to j$$
   that is a coequalizer of f and g, i.e. satisfies
   $$f \circ h = g \circ h.$$

$$\begin{tikzcd}
i_1 & \\
& j \arrow[ul, dashed, "\phi_1"] \arrow[dl, dashed, "\phi_2"'] \\
i_2 &
\end{tikzcd}$$

FIGURE 3. *
Condition 1: Lower Bound

$$\begin{tikzcd}
k \arrow[r, dashed, "h"] & j \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & i
\end{tikzcd}$$

FIGURE 4. *
Condition 2: Equalizer

In other words, $\mathcal{I}$ is nonempty, any finite diagram of objects admits a cone, and any pair of parallel morphisms become equal after pre-composition with an appropriate morphism.

Definition A.4.18 (Systems in a category)**.** Let $\mathcal{C}$ be a (large) category. Let I be a (large) category.

1. A diagram/system $I \to C$ is called *filtered* (resp. *cofiltered*) if I is a filtered (Definition A.4.17) (resp. cofiltered (Definition A.4.17)) category.
2. A diagram/system $I \to C$ is called *directed* (resp. *codirected* if I is small and thing, i.e. is regardable/comes from a directed (resp. codirected) partially ordered set. A *direct system* or *inductive system* is synonymous for a directed system and a *inverse system* or *projective system* is synonymous for a codirected system.

One might also speak of a *filtered direct/inductive system* synonymously for a filtered system to emphasize that the indexing caetgory is a general filtered category, rather than a directed poset.

Definition A.4.19 (Cones, limits and colimits in a category)**.** Let $\mathcal{C}$ be a (large) category (Definition A.4.1), let I be a (large) category, and let $D : I \to \mathcal{C}$ be a diagram.

1. A *cone to the diagram D* is an object $L \in \mathcal{C}$ together with a family of morphisms

$$\{\pi_i : L \to D(i)\}_{i \in I}$$

such that for every morphism $f : i \to j$ in I, the diagram

$$\begin{tikzcd}
& L \arrow[ld, "\pi_i"'] \arrow[rd, "\pi_j"] & \\
D(i) \arrow[rr, "D(f)"] & & D(j)
\end{tikzcd}$$

commutes, i.e. $D(f) \circ \pi_i = \pi_j$.

2. A cone $(L, \{\pi_i\})$ is called a *limit of D* if it satisfies the following "universal property": for any cone $(C, \{f_i\})$ over D, there exists a *unique* morphism $u : C \to L$ such that

$$\pi_i \circ u = f_i \quad \text{for all } i \in I.$$

Visually, the following diagrams commute every morphism $f : i \to j$ in I:

$$\begin{tikzcd}
& C \arrow[d, dashed, "\exists! u"] \arrow[ldd, bend right, "f_i"'] \arrow[rdd, bend left, "f_j"] & \\
& L \arrow[ld, "\pi_i"'] \arrow[rd, "\pi_j"] & \\
D(i) \arrow[rr, "D(f)"] & & D(j).
\end{tikzcd}$$

If such a cone exists, then the object L is necessarily unique up to unique isomorphism by the universal property. In this case, L is denoted by $\lim_{i \in I} D$ or $\lim D$.

3. A *cocone from the diagram D* is an object $C \in \mathcal{C}$ together with a family of morphisms

$$\{\iota_i : D(i) \to C\}_{i \in I}$$

such that for every morphism $f : i \to j$ in I, the diagram

$$\begin{tikzcd}
D(i) \arrow[rr, "D(f)"] \arrow[rd, "\iota_i"'] & & D(j) \arrow[ld, "\iota_j"] \\
& C &
\end{tikzcd}$$

commutes, i.e. $\iota_j \circ D(f) = \iota_i$.

4. A cocone $(L, \{\iota_i\})$ is called a *colimit of D* if it satisfies the following "universal property": for any cocone $(C, \{g_i\})$ under D, there exists a *unique* morphism $u : L \to C$ such that

$$u \circ \iota_i = g_i \quad \text{for all } i \in I.$$

Visually, the following diagrams commute every morphism $f : i \to j$ in I:

$$\begin{tikzcd}
D(i) \arrow[rr, "D(f)"] \arrow[dr, "\iota_i"] \arrow[ddr, bend right, "g_i"'] & & D(j) \arrow[dl, "\iota_j"'] \arrow[ddl, bend left, "g_j"] \\
& L \arrow[d, dashed, "\exists! u"] & \\
& C & .
\end{tikzcd}$$

If such a cocone exists, then the object L is necessarily unique up to unique isomorphism by the universal property. In this case, L is denoted by $\operatorname{colim}_{i \in I} D$ or $\operatorname{colim} D$.

A limit/colimit is called *finite* (resp. *small*) if the diagram category I is finite (resp. small).

Some authors use the terms *projective limit* or *inverse limit* to refer to what is defined here as a limit, Similarly, the terms *inductive limit* or *direct limit* are sometimes used to mean a colimit. However, these phrases can have more specific meanings to other authors: a *projective* or *inverse limit* may refer to a limit over a diagram indexed by a codirected poset. Likewise, an *inductive* or *direct limit* may refer to a colimit over a directed poset (see Definition A.4.20) .

Thus, while the terms are sometimes used interchangeably with "limit" and "colimit," they may also emphasize particular indexing shapes and directions, distinguishing them from general limits and colimits taken over arbitrary small categories.

Definition A.4.20 (Special cases of limits)**.** Let $\mathcal{C}$ be a (large) category. Let I be a (large) category. Let $I \to \mathcal{C}$ be a diagram/system.

- Suppose that the system is a cofiltered system (Definition A.4.18), i.e. I is a cofiltered category. A limit (Definition A.4.19) of this diagram is often denoted by

  $$\varprojlim_{i \in I} D(i)$$

  and may be called a *cofiltered (inverse/projective) limit*. In case that the system is more specifically an inverse/projective system (Definition A.4.18), i.e. I is a cofiltered poset, the preferred term for such a limit is *inverse/projective limit.*
- Suppose that the system is a filtered system, i.e. I is a filtered category. A colimit of this diagram is often denoted by

  $$\varinjlim_{i \in I} D(i)$$

  and may be called a *filtered colimit* or a *direct/inductive/injective limit*. In case that the system is more specifically a direct/inductive system, i.e. I is a filtered poset, the preferred term for such a limit is *direct/inductive limit.*

Definition A.4.21 (Product in a category)**.** Let $\mathcal{C}$ be a category and let $\{X_i\}_{i \in I}$ be a family of objects in $\mathcal{C}$ indexed by a class I.

1. A *product of the family* $\{X_i\}$ is an object P of $\mathcal{C}$ together with a "universal" family of morphisms
$$\pi_i : P \to X_i, \quad \text{for each } i \in I.$$
More precisely, for any object Y and any family of morphisms $\{f_i : Y \to X_i\}_{i\in I}$, there exists a unique morphism
$$f : Y \to P$$
making the following diagram commute for all $i \in I$, i.e. $\pi_i \circ f = f_i$:
$$\begin{tikzcd} Y \arrow[d, dashed, "\exists! f"] \arrow[dr, "f_i"] & \\ \prod X_i \arrow[r, "\pi_i"'] & X_i \end{tikzcd}$$
Such a product is often denoted by $\prod_{i\in I} X_i$. If $\prod_{i\in I} X_i$ exists in $\mathcal{C}$, then it is unique up to unique isomorphism by the universal property described above.

   Equivalently, the product $\prod_{i\in I} X_i$ is the limit (Definition A.4.19) of the diagram $I \to \mathcal{C}, i \mapsto X_i$, where I is made into a category whose objects are the members of I and whose morphisms are just the identity morphisms.
2. A *coproduct* (or synonymously *direct sum*) of the family $\{X_i\}$ is an object C of $\mathcal{C}$ together with a "universal" family of morphisms
$$\iota_i : X_i \to C, \quad \text{for each } i \in I.$$
More precisely, for any object Y and any family of morphisms $\{g_i : X_i \to Y\}_{i\in I}$, there exists a unique morphism
$$g : C \to Y$$
making the following diagram commute for all $i \in I$, i.e. $g \circ \iota_i = g_i$:
$$\begin{tikzcd} X_i \arrow[r, "\iota_i"] \arrow[dr, "g_i"'] & \coprod X_i \arrow[d, dashed, "\exists! g"] \\ & Y \end{tikzcd}$$
Such a coproduct is often denoted by $\coprod_{i\in I} X_i$ or $\oplus_{i\in I} X_i$. If $\coprod_{i\in I} X_i$ exists in $\mathcal{C}$, then it is unique up to unique isomorphism by the universal property described above.

   Equivalently, the coproduct $\coprod_{i\in I} X_i$ is the colimit (Definition A.4.19) of the diagram $I \to \mathcal{C}, i \mapsto X_i$, where I is made into a category whose objects are the members of I and whose morphisms are just the identity morphisms.

Definition A.4.22. Let $\mathcal{C}$ be a (large) category (Definition A.4.1), let I be a small category (Definition A.4.3), and let $D : I \to \mathcal{C}$ be a diagram.

A limit or colimit (Definition A.4.19) is called *finite* (resp. *small*) if the indexing category I has finitely many objects and morphisms (resp. if I is a small category (Definition A.4.3)).

Definition A.4.23 (Monomorphism and Epimorphism in Categories)**.** Let $\mathcal{C}$ be a category (Definition A.4.1). For objects $A, B \in \mathcal{C}$, let $f : A \to B$ be a morphism in $\mathcal{C}$.

- The morphism f is called a *monomorphism* (or a *monic morphism*) if for every object X and every pair of morphisms $g_1, g_2 : X \to A$, the equality $f \circ g_1 = f \circ g_2$ implies $g_1 = g_2$.
- The morphism f is called an *epimorphism* (or an *epic morphism*) if for every object Y and every pair of morphisms $h_1, h_2 : B \to Y$, the equality $h_1 \circ f = h_2 \circ f$ implies $h_1 = h_2$.

Definition A.4.24. Let $\mathcal{C}$ be an additive category (Definition 2.2.10). Let $X \in \mathrm{Ob}(\mathcal{C})$ be an object. A *subobject of X* refers to a monomorphism (Definition A.4.23) $i : Y \hookrightarrow X$ in $\mathcal{C}$. We regard two subobjects (Y, i) and (Y', i') of X as isomorphic if there exists an isomorphism $f : Y \to Y'$ such that $i = i' \circ f$. One often leaves the monomorphism i implicit, suprressing it from the notation.

Definition A.4.25. Let $\mathcal{C}$ be an abelian category (Definition 2.2.12). Let $X \in \mathrm{Ob}(\mathcal{C})$ be an object. Let $i : A \hookrightarrow X$ be a subobject (Definition A.4.24). The cokernel (Definition A.4.14) $\pi : X \twoheadrightarrow X/A := \mathrm{coker}(i)$ is called the *quotient object of X by A*. The object X/A is determined up to canonical isomorphism.

Definition A.4.26. Let $\mathcal{C}$ and $\mathcal{D}$ be locally small categories (Definition A.4.3). Let $F : \mathcal{C} \to \mathcal{D}$ be a functor (Definition A.4.5).

1. F is called *full* if for every pair of objects $x, y \in \mathrm{Ob}(\mathcal{C})$, the induced map on Hom-sets
$$F_{x,y} : \mathrm{Hom}_{\mathcal{C}}(x, y) \to \mathrm{Hom}_{\mathcal{D}}(F(x), F(y))$$
is *surjective.*
2. F is called *faithful* if for every pair of objects $x, y \in \mathrm{Ob}(\mathcal{C})$, the induced map on Hom-sets
$$F_{x,y} : \mathrm{Hom}_{\mathcal{C}}(x, y) \to \mathrm{Hom}_{\mathcal{D}}(F(x), F(y))$$
is *injective.*
3. F is called *fully faithful* if it is both full and faithful.

Definition A.4.27 (Reflecting a type of morphism)**.** Let $F : \mathcal{C} \to \mathcal{D}$ be a functor between (large) categories (Definition A.4.5), and let $\mathcal{P}$ be a property of morphisms (or more generally a property of sequences or families of morphisms) that is stable under isomorphism (e.g. monomorphism, epimorphism (Definition A.4.23), isomorphism, etc.). We say that F *reflects $\mathcal{P}$-morphisms* if for every morphism $f : x \to y$ in $\mathcal{C}$, whenever $F(f)$ has property $\mathcal{P}$ in $\mathcal{D}$, it follows that f has property $\mathcal{P}$ in $\mathcal{C}$.

Lemma A.4.28. Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor (Definition 2.2.11) between additive categories (Definition 2.2.10). The functor F is faithful (Definition A.4.26) if and only if for any morphism f in $\mathcal{A}$, we have $F(f) = 0$ exactly when $f = 0$.

Proof. To say that F is faithful means that for every pair of objects X and Y in $\mathcal{A}$, the induced abelian group (Definition 1.1.1) homomorphism (Definition 1.1.3)
$$F_{X,Y} : \mathrm{Hom}_{\mathcal{A}}(X, Y) \to \mathrm{Hom}_{\mathcal{B}}(F(X), F(Y))$$
on the Hom-sets is injective (Definition A.1.3). Equivalently, this means that for every morphism $f : X \to Y$ in $\mathcal{A}$, we have $F(f) = 0$ if and only if $f = 0$. □

Proposition A.4.29 (Reflection of morphism properties by full or faithful functors)**.** Let $F : \mathcal{C} \to \mathcal{D}$ be a functor (Definition A.4.5) between locally small categories (Definition A.4.3).

(1) If F is faithful (Definition A.4.26), then F reflects (Definition A.4.27) monomorphisms and epimorphisms (Definition A.4.23). That is, if $f : x \to y$ in $\mathcal{C}$ is such that $F(f)$ is a monomorphism (resp. epimorphism) in $\mathcal{D}$, then f is a monomorphism (resp. epimorphism) in $\mathcal{C}$.

(♠ TODO: define split monos and epis) (2) If F is fully faithful, then F reflects isomorphisms, split monomorphisms, and split epimorphisms. That is, if $f : x \to y$ in $\mathcal{C}$ is such that $F(f)$ is an isomorphism in $\mathcal{D}$, then f is an isomorphism in $\mathcal{C}$.

Proposition A.4.30. Let $F : \mathcal{A} \to \mathcal{B}$ be an exact functor (Definition 2.2.23) between abelian categories (Definition 2.2.12). The functor F is faithful (Definition A.4.26) if and only if it reflects (Definition A.4.27) short exact sequences (Definition 2.2.22).

Proof. Suppose F is faithful. Let

$$A_1 \xrightarrow{f} A_2 \xrightarrow{g} A_3$$

be a sequence in $\mathcal{A}$ such that

$$F(A_1) \xrightarrow{F(f)} F(A_2) \xrightarrow{F(g)} F(A_3)$$

is exact in $\mathcal{B}$. Because F is exact, it preserves kernels and images, so

$$F(\ker(g)) = \ker(F(g)), \quad F(\operatorname{im}(f)) = \operatorname{im}(F(f)).$$

Exactness in $\mathcal{B}$ gives

$$\ker(F(g)) = \operatorname{im}(F(f)),$$

so

$$F(\ker(g)) = F(\operatorname{im}(f)).$$

Since F is faithful, it reflects (Definition A.4.27) monomorphisms and epimorphisms (Definition A.4.23) (Proposition A.4.29), and morphisms that become equal via F must be equal in $\mathcal{A}$. Hence,

$$\ker(g) = \operatorname{im}(f).$$

Therefore, the sequence

$$A_1 \xrightarrow{f} A_2 \xrightarrow{g} A_3$$

is exact in $\mathcal{A}$, i.e., F reflects short exact sequences.

Conversely, suppose F reflects short exact sequences. Let $f : A \to B$ be a morphism in $\mathcal{A}$ such that

$$F(f) = 0.$$

Consider the sequence

$$0 \to A \xrightarrow{f} B.$$

Since $F(f) = 0$, we have the sequence

$$0 \to F(A) \xrightarrow{F(f)} F(B)$$

is exact at $F(A)$. Because F reflects short exact sequences, the original sequence must be exact at A, so f is a monomorphism with zero image, hence $f = 0$. Thus F is faithful by Lemma A.4.28. □

A.5. **Homological algebra.**

Definition A.5.1 (n-ary Additive Functor)**.** Let I be a finite set with $|I| = n$. Let $\{\mathcal{A}_i\}_{i \in I}$ be additive categories (Definition 2.2.10) and let $\mathcal{B}$ be an additive category. An *n-ary additive functor* (or *multilinear functor*)

$$F : \prod_{i \in I} \mathcal{A}_i \to \mathcal{B}$$

is a functor such that for each fixed collection of all but one variable, the resulting functor in the remaining variable is additive (Definition 2.2.11). Equivalently, for every $j \in I$ and objects $(A_i)_{i \in I}$ and morphisms $f_1, f_2 : A_j \to A'_j$ in $\mathcal{A}_j$, we have

$$\begin{aligned} &F(A_1, \dots, A_{j-1}, f_1 + f_2, A_{j+1}, \dots, A_n) \\ =&F(A_1, \dots, A_{j-1}, f_1, A_{j+1}, \dots, A_n) \\ &+ F(A_1, \dots, A_{j-1}, f_2, A_{j+1}, \dots, A_n), \end{aligned}$$

and F preserves zero morphisms componentwise:

$$F(A_1, \dots, 0_{A_j, A'_j}, \dots, A_n) = 0_{F(A_1, \dots), F(A'_1, \dots)}.$$

A bifunctor that satisfies this property for $n = 2$ is simply called a *biadditive functor*.

Definition A.5.2 (Flat object with respect to a tensor (monoidal) product)**.** Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be abelian categories (Definition 2.2.12), and let $F : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ be a biadditive functor (Definition A.5.1) (in practice, the following definitions are usually considered when F is some kind of "tensor product" $\otimes$ and is right exact (Definition 2.2.23) in each variable).

1. An object $X \in \mathcal{A}$ is called *flat (with respect to F on the left)* if the functor $F(X, -) : \mathcal{B} \to \mathcal{C}$ if exact (Definition 2.2.23).
2. An object $Y \in \mathcal{B}$ is called *flat (with respect to F on the right)* if the functor $F(-, Y) : \mathcal{A} \to \mathcal{C}$ if exact (Definition 2.2.23).

If $\mathcal{A} = \mathcal{B} = \mathcal{C}$ and F makes $\mathcal{A}$ into a symmetric monoidal category, then certainly $F(X, -)$ is exact if and only if $F(-, Y)$ is exact, i.e. flatness is equivalent on the two sides of $\otimes$.

Lemma A.5.3. Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be abelian categories (Definition 2.2.12), and let $\otimes : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ be a biadditive functor (Definition A.5.1) that is right exact (Definition 2.2.23) in each variable.

1. Say that $\mathcal{B}$ has enough projectives and let $\mathrm{Tor}_n(A, B)$ be the Tor object computed as the left derived functor of $A \otimes -$ applied to B. If A is flat (Definition A.5.2), then $\mathrm{Tor}_n(A, B) = 0$ for all $n \neq 0$ and all B.
2. Say that $\mathcal{A}$ has enough projectives and let $\mathrm{Tor}_n(A, B)$ be the Tor object computed as the left derived functor of $- \otimes B$ applied to A. If B is flat (Definition A.5.2), then $\mathrm{Tor}_n(A, B) = 0$ for all $n \neq 0$ and all A.

3. Say that $\mathcal{B}$ has enough flats $F_\bullet \to B$ and let $\mathrm{Tor}_n(A, B)$ be the Tor object computed as $H_n(A \otimes F_\bullet)$. If A is flat (Definition A.5.2), then $\mathrm{Tor}_n(A, B) = 0$ for all $n \neq 0$ and all B.
4. Say that $\mathcal{A}$ has enough flats $F_\bullet \to A$ and let $\mathrm{Tor}_n(A, B)$ be the Tor object computed as $H_n(F_\bullet \otimes B)$. If B is flat (Definition A.5.2), then $\mathrm{Tor}_n(A, B) = 0$ for all $n \neq 0$ and all A.

Proof. We prove the first part. The other parts hold similarly.

If A is flat, then for any $B \in \mathcal{B}$, letting $P_\bullet \to B$ be some projective resolution, the exactness of $A \otimes -$ implies that $\mathrm{Tor}_n(A, B) = H_n(A \otimes P_\bullet) = 0$ for all $n \neq 0$. □

Lemma A.5.4 (Dimension shifting, cf. [Wei94, Exercise 2.4.3])**.** Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor (Definition 2.2.11) between abelian categories (Definition 2.2.12). Let A be an object of $\mathcal{A}$.

1. Suppose that F is right exact (Definition 2.2.23).
   (a) Suppose that $0 \to M \to C \to A \to 0$ is an exact sequence in $\mathcal{A}$ where C is F-acyclic, and that A and M have projective resolutions. We have $L_iF(A) \cong L_{i-1}F(M)$ for $i \geq 2$ and $L_1F(A) \cong \ker(F(M) \to F(C))$.
   (b) Suppose that $\mathcal{A}$ has enough projectives. Let
   $$0 \to M_m \to C_m \to C_{m-1} \to \cdots \to C_0 \to A \to 0$$
   be an acyclic complex with the C_i F-acyclic. We have
      (i) $L_iF(A) \cong L_{i-m-1}F(M_m)$ for $i \geq m+2$ and
      (ii) $L_{m+1}F(A) \cong \ker(F(M_m) \to F(C_m))$.
2. (♠ TODO: dual statement)

Proof. 1. Suppose that F is right exact
   (a) Since C is F-acyclic, the long exact sequence of derived functors associated to $0 \to M \to C \to A \to 0$ yields an exact sequence
   $$0 \to L_1F(A) \to F(M) \to F(C) \to F(A) \to 0$$
   along with isomorphisms $L_iF(A) \cong L_{i-1}F(M)$ for $i \geq 2$. In particular, $L_1F(A) = \ker(F(M) \to F(C))$.
   (b) We now proceed by induction. The above proves the base case of $m = 0$. Associated to the acyclic complex
   $$0 \to M_m \to C_m \to C_{m-1} \to \cdots \to C_0 \to A \to 0$$
   is a short exact sequence
   $$0 \to M_m \to C_m \to M_{m-1} \to 0$$
   where $M_{m-1} = \mathrm{coker}(M_m \to C_m)$ and an acyclic complex
   $$0 \to M_{m-1} \to C_{m-1} \to \cdots \to C_0 \to A \to 0.$$
   The derived functor long exact sequence of the short exact sequence yields isomorphisms
   $$L_iF(M_{m-1}) \cong L_{i-1}F(M_m)$$

for all $i \geq 1$. By induction, we also have $L_iF(A) \cong L_{i-(m-1)-1}F(M_{m-1}) = L_{i-m}F(M_{m-1})$ for $i \geq m+1$, so we in fact have

$$L_iF(A) \cong L_{i-m}F(M_{m-1}) \cong L_{i-m-1}F(M_m)$$

for all $i \geq m+1$. Moreover, the derived functor long exact sequence also includes

$$0 \to L_1F(M_{m-1}) \to F(M_m) \to F(C_m) \to F(M_{m-1}) \to 0,$$

so $L_1F(M_{m-1}) \cong \ker(F(M_m) \to F(C_m))$. We found that $L_1F(M_{m-1}) \cong L_{m+1}F(A)$, so $L_{m+1}F(A)$ is the kernel of $F(M_m) \to F(C_m)$ as desired.

2. These hold dually.

□

Corollary A.5.5. Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be abelian categories (Definition 2.2.12), and let $\otimes : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ be a biadditive functor (Definition A.5.1) that is right exact (Definition 2.2.23) in each variable. Suppose that $\mathcal{A}$ and $\mathcal{B}$ have enough projectives and flats. Further suppose that (small) filtered colimits which exist in $\mathcal{C}$ are exact (e.g. which holds if $\mathcal{C}$ satisfies Ab5 (Definition 2.2.13)).

For any objects $A \in \mathcal{A}$ and $B \in \mathcal{B}$, all notions of $\mathrm{Tor}_n(A, B)$ as defined in Definition A.5.13 naturally agree with one another.

Proof. This follows from Theorem A.5.12 and Lemma A.5.6. □

Lemma A.5.6 (cf. [Wei94, Flat Resolution Lemma 3.2.8])**.** Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be abelian categories (Definition 2.2.12), and let $\otimes : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ be a biadditive functor (Definition A.5.1) that is right exact (Definition 2.2.23) in each variable. Let $A \in \mathcal{A}$ and $B \in \mathcal{B}$ be objects.

1. Suppose that $\mathcal{A}$ has enough projective objects. Suppose that A has some flat resolution. The Tor objects (Definition A.5.13)
$$\mathrm{Tor}_n(A, B) \in \mathcal{C}$$
obtained via a projective resolution of A and via a flat resolution of A are naturally isomorphic. In particular, either notion of Tor_n is well defined.
2. Suppose that $\mathcal{B}$ has enough projective objects. Suppose that B has some flat resolution. The Tor objects
$$\mathrm{Tor}_n(A, B) \in \mathcal{C}$$
obtained via a projective resolution of B and via a flat resolution of B are naturally isomorphic. In particular, either notion of Tor_n is well defined.

Proof. We show 1. Write $\mathrm{Tor}_n(A, B)$ for the tor object obtained via a projective resolution of A. Write $H_n(F_\bullet \otimes B)$ for the tor object obtained via a flat resolution $F_\bullet \to A$ of A. We argue by induction. For $n = 0$, we have $\mathrm{Tor}_0(A, B) \cong H_0(F_\bullet \otimes B)$ because $- \otimes B$ is right exact by assumption.

Let K be such that $0 \to K \to F_0 \to A$ is exact. write $E_\bullet = (\cdots \to F_2 \to F_1)$ so that $E_\bullet \to K$ is a resolution of K by flat objects (**??**). Since $\mathcal{A}$ has enough projectives, further note that all flat objects are acyclic for the functor $- \otimes B$ by Lemma A.5.3.

By Lemma A.5.4, we have

$$\mathrm{Tor}_1(A,B) = \ker(K \otimes B \to F_0 \otimes B) = \ker \left\{ \frac{F_1 \otimes B}{\mathrm{im}(F_2 \otimes B) \to F_0 \otimes B} = H_1(F \otimes B) \right\},$$

thus establishing the desired isomorphism for $n = 1$. For $n \geq 2$, use induction to see that

$$\mathrm{Tor}_n(A,B) \cong \mathrm{Tor}_{n-1}(K,B) \cong H_{n-1}(E_\bullet \otimes B) = H_n(F \otimes B).$$

□

Lemma A.5.7. Let $\mathcal{A}$ be a preadditive category (Definition 2.2.10). Finite products (Definition A.4.21) in $\mathcal{A}$ coincide with finite coproducts (Definition A.4.21). More precisely, if $\{A_i\}_{i=1}^n$ is a finite collection of objects of $\mathcal{A}$, then

1. if $\prod_{i=1}^n A_i$ exists, then so does $\coprod_{i=1}^n A_i$ and these are naturally isomorphic.
2. if $\coprod_{i=1}^n A_i$, then so does $\prod_{i=1}^n A_i$ and these are naturally isomorphic.

Proof. (♠ TODO:) □

Lemma A.5.8. Let C be a double complex of objects in an additive category (Definition 2.2.10) $\mathcal{A}$. If C is locally bounded along diagonals, then the complexes $\mathrm{Tot}^{\bigoplus}(A)$ and $\mathrm{Tot}^{\prod}(A)$ are naturally isomorphic.

Proof. Since C is locally bounded along diagonals, the degreee n components

$$\left(\mathrm{Tot}^{\oplus}\right)^n(A) = \bigoplus_{p+q=n} A^{p,q},$$
$$\left(\mathrm{Tot}^{\Pi}\right)^n(A) = \prod_{p+q=n} A^{p,q}.$$

are finite direct sums and finite products respectively and hence are naturally isomorphic (Lemma A.5.7). The differential maps of the two total complexes also naturally coincide. □

Lemma A.5.9 (cf. [Wei94, Acyclic Assembly Lemma 2.7.3])**.** (♠ TODO: It may be the case that this is generalizable beyond first quadrant double complexes, but I don't have a slick way to show this. See the commented out code for the statements; also, it may be necessary to assume something like AB4$*$ for such statements) Let $\mathcal{A}$ be an abelian category (Definition 2.2.12) for which (small) filtered colimits which exist are exact (e.g. which holds if $\mathcal{A}$ satisfies Ab5 (Definition 2.2.13)). Let C be a double complex in $\mathcal{A}$.

If C has exact columns or has exact rows and C is a bounded below or bounded above double complex, then $\mathrm{Tot}^{\Pi}(C)$ is an acyclic chain complex.

Proof. We show that if C has exact columns and C is bounded below, then $\mathrm{Tot}^{\Pi}(C)$ is an acyclic chain complex; it can then be argued symmetrically that if C has exact columns and C is bounded above, then $\mathrm{Tot}^{\Pi}(C)$ is acyclic. Moreover, the case of exact rows can be deduced by reflecting the rows and columns of double complexes.

Note that since C is assumed to be bounded below and hence is locally bounded along diagonals, $\mathrm{Tot}^{\Pi}(C)$ and $\mathrm{Tot}^{\oplus}(C)$ exist, are constructed by finite products (which are also finite coproducts), and are naturally isomorphic by Lemma A.5.8. Further recall that finite coproducts in an abelian category are exact.

Define the sub-double complexes F^kC of C by

$$(F^kC)^{p,q} = \begin{cases} C^{p,q} & \text{if } p \leq k \\ 0 & \text{otherwise} \end{cases}.$$

This yields a filtration

$$\cdots \subseteq F^{k-1}C \subseteq F^kC \subseteq F^{k+1} \subseteq \cdots \subseteq C.$$

Moreover, for each n,

$$\left(\mathrm{Tot}^{\Pi}(F^kC)\right)^n = \prod_{p \leq k, p+q=n} C^{p,q}.$$

For each n, the above stabilizes as $k \to \infty$ to $\mathrm{Tot}^{\Pi}(C)^n$. Now let

$$D^k = F^kC/F^{k-1}C = \begin{cases} C^{p,q} & \text{if } p = k \\ 0 & \text{otherwise.} \end{cases}$$

Since each column $C^{k,*}$ is exact by assumption, the total complex $\mathrm{Tot}^{\Pi}(D^k)$ is acyclic. Note that we have short exact sequences

$$0 \to F^{k-1}C \to F^kC \to D^k \to 0$$

of double complexes. The totalization functor $\mathrm{Tot}^{\Pi}(-)$ in this case is exact because all of the double complexes are locally bounded along diagonals. We hence have a short exact sequence

$$0 \to \mathrm{Tot}^{\Pi}(F^{k-1}C) \to \mathrm{Tot}^{\Pi}(F^kC) \to \mathrm{Tot}^{\Pi}(D^k) \to 0.$$

Since $\mathrm{Tot}^{\Pi}(D^k)$ is acyclic, the long exact cohomology sequences yield isomorphisms

$$H^n(\mathrm{Tot}^{\Pi}(F^{k-1}C)) \cong H^n(\mathrm{Tot}^{\Pi}(F^kC)).$$

Since C is assumed to be bounded, the subcomplex F^kC is zero for sufficiently negative k, in which case $\mathrm{Tot}^{\Pi}(F^kC)$ is acyclic. By induction on k, $\mathrm{Tot}^{\Pi}(F^kC)$ remains acyclic for all k. Moroever, the filtered colimit $\varinjlim_k \mathrm{Tot}^{\Pi}(F^kC)$ is $\mathrm{Tot}^{\Pi}(C)$. The assumed exactness of filtered colimits in $\mathcal{A}$ concludes that $\mathrm{Tot}^{\Pi}(C)$ is acyclic.

By symmetry, if C instead has exact rows, then $\mathrm{Tot}^{\Pi}(C)$ is an acyclic chain complex. □

Lemma A.5.10. Let $F : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ be a biadditive functor (Definition A.5.1) of abelian categories (Definition 2.2.12). Assume that (small) filtered colimits which exist in $\mathcal{C}$ are exact (e.g. which holds if $\mathcal{C}$ satisfies Ab5 (Definition 2.2.13)).

Let $A \in \mathcal{A}$ and $B \in \mathcal{B}$ be objects.

1. Suppose that left resolutions $P_{A,\bullet} \to A$ and $P_{B,\bullet} \to B$ exist such that $P_{A,i}$ and $P_{B,i}$ are flat (Definition A.5.2) with respect to F on the left and right respectively, i.e. $F(P_{A,i}, -) : \mathcal{B} \to \mathcal{C}$ and $F(-, P_{B,i}) : \mathcal{A} \to \mathcal{C}$ are exact for all i.

   The complexes $F(P_{A,\bullet}, B)$ and $F(A, P_{B,\bullet})$ are quasi-isomorphic to the complex $\mathrm{Tot}(F(P_{A,\bullet}, P_{B,\bullet}))$.

2. Suppose that right resolutions $A \to I^{A,\bullet}$ and $B \to I^{B,\bullet}$ exist such that $I^{A,i}$ and $I^{B,i}$ are flat (Definition A.5.2) with respect to F on the left and right respectively, $F(I^{A,i},-) : \mathcal{B} \to \mathcal{C}$ and $F(-, I^{B,i}) : \mathcal{A} \to \mathcal{C}$ are exact for all i.

   The complexes $F(I^{A,\bullet}, B)$ and $F(A, I^{B,\bullet})$ are quasi-isomorphic to the complex $\mathrm{Tot}(F(I^{A,\bullet}, I^{B,\bullet}))$.

Proof. We prove 1. The other part is the dual statement.

Choose resolutions $P_{A,\bullet} \xrightarrow{\varepsilon} A$ and $P_{B,\bullet} \xrightarrow{\eta} B$ such that $F(P_{A,i},-) : \mathcal{B} \to \mathcal{C}$ and $F(-,P_{B,i}) : \mathcal{A} \to \mathcal{C}$ are exact for all i. Identifying A and B with complexes concentrated in degree 0, we can form the three double complexes $F(P_{A,\bullet}, P_{B,\bullet})$, $F(A, P_{B,\bullet})$, and $F(P_{A,\bullet}, B)$. Note that the augmentation morphisms ε and η induce morphisms $P_{A,\bullet} \otimes P_{B,\bullet} \to A \otimes P_{B,\bullet}, P_{A,\bullet} \otimes B$.

Let C be the double complex of objects in $\mathcal{C}$ obtained from $F(P_{A,\bullet}, P_{B,\bullet})$ by adding $F(A, P_{B,\bullet}[-1])$ in the column $p = -1$. One can show that the translate $\mathrm{Tot}(C)[1]$ is the mapping cone of the map

$$\mathrm{Tot}(F(P_{A,\bullet}, P_{B,\bullet})) \xrightarrow{\varepsilon\otimes\mathrm{id}} \mathrm{Tot}(F(A, P_{B,\bullet})) = F(A, P_{B,\bullet}).$$

Moreover, since each $F(-,P_{B,i})$ is an exact functor, every row of C is exact, so $\mathrm{Tot}(C)$ is exact by Lemma A.5.9. Therefore, $F(\varepsilon, \mathrm{id})$ is a quasi-isomorphism and hence

$$H_*(\mathrm{Tot}(F(P_{A,\bullet}, P_{B,\bullet}))) \xrightarrow{H_*(F(\varepsilon, P_{B,\bullet}))} H_*(F(A, P_{B,\bullet}))$$

is a natural isomorphism.

By symmetry, there is a natural isomorphism $H_*(\mathrm{Tot}(F(P_{A,\bullet} P_{B,\bullet}))) \to H_*(F(P_{A,\bullet}, B))$. □

Theorem A.5.11. Let $F : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ be a biadditive functor (Definition A.5.1) of abelian categories (Definition 2.2.12). Assume that (small) filtered colimits which exist in $\mathcal{C}$ are exact (e.g. which holds if $\mathcal{C}$ satisfies Ab5 (Definition 2.2.13)).

Let $A \in \mathcal{A}$ and $B \in \mathcal{B}$ be objects.

1. Suppose that left resolutions $P_{A,\bullet} \to A$ and $P_{B,\bullet} \to B$ exist such that $F(P_{A,i},-) : \mathcal{B} \to \mathcal{C}$ and $F(-,P_{B,i}) : \mathcal{A} \to \mathcal{C}$ are exact for all i.
   (a) The objects $L^I_n F(A,B)$ and $L^{II}_n F(A,B)$ are naturally isomorphic.
   (b) The objects $L^I_n F(A,B)$ and $L^{II}_n F(A,B)$ are well defined (up to natural isomorphism), i.e. do not depend on the choice of left resolutions of A and B respectively.
2. Suppose that right resolutions $A \to I^{A,\bullet}$ and $B \to I^{B,\bullet}$ exist such that $F(I^{A,i},-) : \mathcal{B} \to \mathcal{C}$ and $F(-,I^{B,i}) : \mathcal{A} \to \mathcal{C}$ are exact for all i.
   (a) The objects $R^n_I F(A,B)$ and $R^n_{II} F(A,B)$ are naturally isomorphic.
   (b) The objects $R^n_I F(A,B)$ and $R^n_{II} F(A,B)$ are well defined (up to natural isomorphism), i.e. do not depend on the choice of left resolutions of A and B respectively.

Proof. We prove 1. The other part is the dual statement.

Choose resolutions $P_{A,\bullet} \xrightarrow{\varepsilon} A$ and $P_{B,\bullet} \xrightarrow{\eta} B$ such that $F(P_{A,i},-) : \mathcal{B} \to \mathcal{C}$ and $F(-,P_{B,i}) : \mathcal{A} \to \mathcal{C}$ are exact for all i. As per Lemma A.5.10, $F(\varepsilon, \mathrm{id})$ is a quasi-isomorphism and hence $H_*(\mathrm{Tot}(F(P_{A,\bullet}, P_{B,\bullet}))) \xrightarrow{H_*(F(\varepsilon, P_{B,\bullet}))} H_*(F(A, P_{B,\bullet}))$ is a natural isomorphism. By symmetry, there is a natural isomorphism $H_*(\mathrm{Tot}(F(P_{A,\bullet} P_{B,\bullet}))) \to H_*(F(P_{A,\bullet}, B))$. Therefore,

$L^I_n(A,B)$ and $L^{II}_n(A,B)$ are naturally isomorphic as claimed. In particular, $L^I_n(A,B)$ and $L^{II}_n(A,B)$ are independent of the choice of resolution of A and B respectively.

□

Theorem A.5.12 (Balancing of Tor, cf. [Wei94, Theorem 2.7.2])**.** Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be abelian categories (Definition 2.2.12), and let $\otimes : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ be a biadditive functor (Definition A.5.1) that is right exact (Definition 2.2.23) in each variable. Assume that (small) filtered colimits which exist in $\mathcal{C}$ are exact (e.g. which holds if $\mathcal{C}$ satisfies Ab5 (Definition 2.2.13)).

Given $A \in \mathcal{A}$ and $B \in \mathcal{B}$ for which flat resolutions exist, let $\mathrm{Tor}^I_n(A,B)$ and $\mathrm{Tor}^{II}_n(A,B)$ respectively be the Tor objects $\mathrm{Tor}^{\mathcal{A}}_n(A,B)$ (Definition A.5.13) computed via flat resolutions of A in $\mathcal{A}$ and of B in $\mathcal{B}$.

1. $\mathrm{Tor}^I_n(A,B)$ and $\mathrm{Tor}^{II}_n(A,B)$ are naturally isomorphic.
2. $\mathrm{Tor}^I_n(A,B)$ and $\mathrm{Tor}^{II}_n(A,B)$ are independent of the choice of flat resolution of A and B respectively.

In particular, we may identify the objects $\mathrm{Tor}^I_n(A,B)$ and $\mathrm{Tor}^{II}_n(A,B)$ and simply write $\mathrm{Tor}_n(A,B)$ for either.

Proof. This follows from Theorem A.5.11.

□

Definition A.5.13 (General circumstances for the existence of Tor functors)**.** Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be abelian categories (Definition 2.2.12), and let $\otimes : \mathcal{A} \times \mathcal{B} \to \mathcal{C}$ be a biadditive functor (Definition A.5.1) that is right exact (Definition 2.2.23) in each variable.

(♠ TODO: Do notation for tor in two categories, one category, modules over rings)

For objects $A \in \mathcal{A}$ and $B \in \mathcal{B}$, the *Tor objects*

$$\mathrm{Tor}_n(A,B) = \mathrm{Tor}^{\mathcal{A},\mathcal{B}}_n(A,B)$$

may be defined in one of several not-necessarily-equivalent ways:

1. as the left derived functors of $A \otimes -$ computed via projective resolutions of B in $\mathcal{B}$, assuming that such a projective resolution exists.
2. as the left derived functors of $- \otimes B$ computed via projective resolutions of B in $\mathcal{A}$, assuming that such a projective resolution exists.
3. as the "left derived functors" of $A \otimes -$ computed via flat resolutions of B in $\mathcal{B}$, assuming that such a flat resolution exists. More precisely, $\mathrm{Tor}_n(A,B) = H_n(A \otimes F_\bullet)$ in this case where $F_\bullet \to B$ is a flat resolution. A priori, this might depend on the choice of flat resolution.
4. as the "left derived functors" of $- \otimes B$ computed via flat resolutions of A in $\mathcal{A}$. More precisely, $\mathrm{Tor}_n(A,B) = H_n(F_\bullet \otimes B)$ in this case where $F_\bullet \to A$ is a flat resolution. A priori, this might depend on the choice of flat resolution.

See Theorem A.5.12 and Lemma A.5.6, which describe sufficient conditions under which the Tor functors defined via flat resolutions are independent of the choice of flat resolution. In particular Corollary A.5.5 shows that all of the above notions are in natural agreement if $\mathcal{A}$ and $\mathcal{B}$ have enough projectives and have enough flats and filtered direct limits that exist in $\mathcal{C}$ are exact.

For any of the above notions of Tor_n, note that

1. for fixed $A \in \mathcal{A}$, if $\mathrm{Tor}_n(A, B)$ exists and is well defined for any $B \in \mathcal{B}$, then $\mathrm{Tor}_n(A, -)$ is an additive functor $\mathcal{B} \to \mathcal{C}$.
2. for fixed $B \in \mathcal{B}$, if $\mathrm{Tor}_n(A, B)$ exists and is well defined for any $A \in \mathcal{A}$, then $\mathrm{Tor}_n(A, -)$ is an additive functor $\mathcal{A} \to \mathcal{C}$.
3. if $\mathrm{Tor}_n(A, B)$ exists and is well defined for any $A \in \mathcal{A}$ and $B \in \mathcal{B}$, then $\mathrm{Tor}_n(-, -)$ is an biadditive $\mathcal{A} \times \mathcal{B} \to \mathcal{C}$.

In the case that $\mathcal{A}$ is the category of $R - S$-modules, $\mathcal{B}$ is the category of $S - T$-modules, $\mathcal{C}$ is the category of $R - T$-modules for some (not necessarily commutative) rings R, S, T (Definition 2.1.1), and $\otimes$ is the usual tensor product between $R - S$-modules and $S - T$-modules producing $R - T$-modules, then the Tor functors may be denoted by

$$\mathrm{Tor}_n^S(A, B)$$

for $A \in \mathcal{A}$ and $B \in \mathcal{B}$.

Appendix B. Sesquilinear and Hermitian forms on sheaves of ring modules over sheaves of rings

Definition B.0.1. Let $(\mathcal{S}, \tau)$ be a site. Let $\mathcal{O}$ be a sheaf of rings on $\mathcal{S}$. An *involution on $\mathcal{O}$* is a morphism of sheaves of rings $\sigma : \mathcal{O} \to \mathcal{O}^{\mathrm{op}}$ such that $\sigma \circ \sigma = \mathrm{id}_{\mathcal{O}}$, i.e. an involution (Definition 4.3.1) in the category of sheaves of rings on $\mathcal{S}$.

Proposition B.0.2. Let (R, σ) be a ring with involution (Definition 4.3.2) and $\phi : M \times M \to R$ a sesquilinear form (Definition 4.3.3). If M is a finitely generated (Definition 2.2.9) projective (Definition 2.2.54) R-module, then the adjoint map $\hat{\phi} : M \to \mathrm{Hom}_R(M, R)_\sigma$ is an isomorphism if and only if ϕ is non-degenerate (Definition 4.3.6).

Definition B.0.3. Let $(\mathcal{S}, \tau)$ be a site. Let $(\mathcal{O}, \sigma)$ be a sheaf of rings on $\mathcal{S}$ with involution (Definition B.0.1) $\sigma : \mathcal{O} \to \mathcal{O}$. Let $\mathcal{E}$ be a sheaf of left $\mathcal{O}$-modules on $\mathcal{S}$.

A *sesquilinear form on $\mathcal{E}$* is a morphism of sheaves of abelian groups

$$\phi : \mathcal{E} \times \mathcal{E} \to \mathcal{O}$$

such that for every object $U \in \mathcal{S}$, the induced map on sections

$$\phi_U : \mathcal{E}(U) \times \mathcal{E}(U) \to \mathcal{O}(U)$$

is a σ_U-sesquilinear form (Definition 4.3.3) on the $\mathcal{O}(U)$-module $\mathcal{E}(U)$, where $\sigma_U : \mathcal{O}(U) \to \mathcal{O}(U)$ is the involution (Definition 4.3.2) on global sections.

Definition B.0.4. Let $(\mathcal{O}, \sigma)$ be a sheaf of rings with involution (Definition B.0.1) on a site $\mathcal{S}$. Let $\mathcal{E}$ be a sheaf of left $\mathcal{O}$-modules.

A *hermitian form on $\mathcal{E}$* is a morphism of sheaves of sets

$$\phi : \mathcal{E} \times \mathcal{E} \to \mathcal{O}$$

such that for every object U in $\mathcal{S}$, the map on sections

$$\phi_U : \mathcal{E}(U) \times \mathcal{E}(U) \to \mathcal{O}(U)$$

is a hermitian form (Definition 4.3.4) on the $\mathcal{O}(U)$-module $\mathcal{E}(U)$ with respect to the involution (Definition 4.3.2) $\sigma_U : \mathcal{O}(U) \to \mathcal{O}(U)$.

References

[AP07] Jeffrey D. Achter and Rachel Pries. The integral monodromy of hyperelliptic and trielliptic curves. *Mathematische Annalen*, 338(1):187–206, 2007.

[Arm92] Brumer Armand. The average rank of elliptic curves i. *Inventiones mathematicae*, 109(1):445–472, 1992.

[Ayo23] Joseph Ayoub. Counterexamples to F. Morel's conjecture on $\pi_0^{\partial^1}$. *Comptes Rendus. Mathématique*, 361:1087–1090, 2023.

[Bal04] Paul Balmer. The spectrum of prime ideals in tensor triangulated categories, 2004.

[BBD82] Alexander A. Beilinson, Joseph Berstein, and Pierre Deligne. Analyse et topologie sur les espaces singuliers (i). *Astérisque*, 100, 1982.

[BBDG18] Alexander A. Beilinson, Joseph Berstein, Pierre Deligne, and Ofer Gabber. *Faisceaux pervers*, volume 4. Société mathématique de France Paris, 2018.

[BBK$^+$23] Barinder S. Banwait, Armand Brumer, Hyun Jong Kim, Zev Klagsbrun, Jacob Mayle, Padmavathi Srinivasan, and Isabel Vogt. Computing nonsurjective primes associated to galois representations of genus 2 curves. *LuCaNT: LMFDB, Computation, and Number Theory*, 796:129, 2023.

[BC19] Tilman Bauer and Magnus Carlson. Tensor products of affine and formal abelian groups. *Documenta Mathematica*, 24:2525–2582, 2019.

[BFK$^+$17] Valentin Blomer, Étienne Fouvry, Emmanuel Kowalski, Philippe Michel, and Djordje Milićević. Some applications of smooth bilinear forms with kloosterman sums. *Proceedings of the Steklov Institute of Mathematics*, 296:18–29, 2017.

[BGI71] Pierre Berthelot, Alexander Grothendieck, and Luc Illusie. *Théorie des Intersections et Théorème de Riemann-Roch (SGA6)*, volume 225 of *Lecture Notes in Mathematics*. Springer-Verlag, 1971.

[BH12] Salman Baig and Chris Hall. Experimental data for goldfeld's conjecture over function fields. *Experimental Mathematics*, 21(4):362–374, 2012.

[BLGHT11] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of Calabi–Yau varieties and potential automorphy ii. *Publications of the Research Institute for Mathematical Sciences*, 47(1):29–98, 2011.

[Bor12] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer New York, 2012.

[BS15a] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Annals of Mathematics*, pages 191–242, 2015.

[BS15b] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Annals of Mathematics*, pages 587–621, 2015.

[BS15c] Bhargav Bhatt and Peter Scholze. The pro-étale topology for schemes. *Astérisque*, 360:99–201, 2015.

[BSD65] Bryan John Birch and Peter Francis Swinnerton-Dyer. Notes on elliptic curves. ii. *Journal für die reine und angewandte Mathematik*, 218:79–108, 1965.

[BSS18] Bhargav Bhatt, Christian Schnell, and Peter Scholze. Vanishing theorems for perverse sheaves on abelian varieties, revisited. *Selecta Mathematica*, 24:63–84, 2018.

[Cho08] Utsav Choudhury. Homotopy theory of schemes and a^1-fundamental groups. Master's thesis, Università degli Studi di Padova, 2008.

[CHT08] Laurent Clozel, Michael Harris, and Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l galois representations. *Publications mathématiques*, 108:1–181, 2008.

[DA73] Pierre Deligne and Michael Artin. *Théorie des Topos et Cohomologies Étale des Schémas. Séminaire de Géométrie Algébrique due Bois-Marie 1963-1964 (SGA 4)*. Lecture Notes in Mathematics. Springer Berlin, 1973.

[DBG$^+$77] Pierre Deligne, Jean-François Boutot, Alexander Grothendieck, Luc Illusie, and Jean-Louis Verdier. *Étale Cohomology. Séminaire de Géométrie Algébrique due Bois-Marie 1963-1964 (SGA 4 1/2)*. Lecture Notes in Mathematics. Springer-Verlag, 1977.

[Del80] Pierre Deligne. La conjecture de Weil : II. *Publications Mathématiques de l'IHÉS*, 52:137–252, 1980.

[Del89] Pierre Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois Groups over Q: Proceedings of a Workshop Held March 23–27, 1987*, pages 79–297. Springer, 1989.

[Die02] Luis V. Dieulefait. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4):503–512 (2003), 2002.

[DR04] Luis V. Dieulefait and Victor Rotger. The arithmetic of qm-abelian surfaces through their galois representations. *Journal of Algebra*, 281:124–143, 2004.

[Dri89] Vladimir Gershonovich Drinfeld. Cohomology of compactified manifolds of modules of f-sheaves. *Journal of Soviet Mathematics*, 46(2):1789–1821, 1989.

[Dru22] Anderi Eduardovich Druzhinin. Stable $\mathbb{A}^1$-connectivity over a base. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2022(792):61–91, 2022.

[DZ19] Alexander Dunn and Alexandru Zaharescu. Sums of Kloosterman sums over primes in an arithmetic progression. *The Quaterly Journal of Mathematics*, 70(1):319–342, 2019.

[Eke07] Torsten Ekedahl. *On The Adic Formalism*, pages 197–218. Birkhäuser Boston, Boston, MA, 2007.

[ELS20] Jordan S. Ellenberg, Wanlin Li, and Mark Shusterman. Nonvanishing of hyperelliptic zeta functions over finite fields. *Algebra & Number Theory*, 14(7):1895–1909, 8 2020.

[EVW16] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland. Homology stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields. *Annals of Mathematics*, 183:729–786, 2016.

[FFK25] Arthur Forey, Javier Fresán, and Emmanuel Kowalski. Arithmetic fourier transforms over finite fields: generic vanishing, convolution, and equidistribution, 2025.

[FK12] Sergey Finashin and Viatcheslav Kharlamov. Abundance of Real Lines on Real Projective Hypersurfaces. *International Mathematics Research Notices*, 2013(16):3639–3646, 06 2012.

[FLR23] Tony Feng, Aaron Landesman, and Eric M. Rains. The geometric distribution of Selmer groups of elliptic curves over function fields. *Mathematische Annalen*, 387:615–687, 2023.

[Fu15] Lei Fu. *Etale Cohomology Theory*, volume 14 of *Nankai Tracts in Mathematics*. World Scientific, 2015.

[FvdG04] Carel Faber and Gerard van der Geer. Complete subvarieties of moduli spaces and the Prym map. *Journal für die reine und angewandte Mathematik*, 2004(573):117–137, 2004.

[GL96] Ofer Gabber and François Loeser. Faisceaux pervers ℓ-adiques sur un tore. *Duke Math J.*, 83(3):501–606, 1996.

[Gol06] Dorian Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number Theory Carbondale 1979: Proceedings of the Southern Illinois Number Theory Conference Carbondale, March 30 and 31, 1979*, pages 108–118. Springer, 2006.

[GR04] Alexander Grothendieck and Michèle Raynaud. Revêtements étales et groupe fondamental (SGA 1). eprint arXiv matyh/0206203, 2004. Updated edition of the book of the same title published by Springer-Verlag in 1971 as volume 224 of the series Lecture Notes in Mathematics.

[Gro77] Alexander Grothendieck. *Cohomologie l-adique et fonctions L Séminaire de Géométrie Algébrique due Bois-Marie 1965-1966 (SGA 5)*, volume 589 of *Springer Lecture Notes*. Springer-Verlag, 1977. Avec la collaboration de I. Bucur, C. Houzel, L. Illusie, J.-P. Jouanolou, et J.-P. Serre.

[GV72] Alexander Grothendieck and Jean-Louis Verdier. *Theorie des Topos et Cohomologie Etale des Schemas. Seminaire de Geometrie Algebrique du Bois-Marie 1963-1964 (SGA 4)*. Lecture Notes in mathematics. Springer-Verlag Berlin Heidelberg, 1 edition, 1972.

[HB04] David Heath-Brown. The average analytic rank of elliptic curves. *Duke Math. J.*, 122:591–623, 2004.

[HK25] Chris Hall and Hyun Jong Kim. Independence of ℓ (title to be determined). In progress, 2025.

[HM73] Dale Husemoller and John Milnor. *Symmetric Bilinear Forms*, volume 73 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge*. Springer Berlin Heidelberg, 1973.

[HSBT05] Michael Harris, Nick Shepherd-Barron, and Richard Taylor. Ihara's lemma and potential automorphy, 2005.

[Hub97] Annette Huber. Mixed perverse sheaves for schemes over number fields. *Compositio Mathematica*, 108:107–121, 1997.

[Ibu22] Tomoyoshi Ibukiyama. Supersingular loci of low dimensions and parahoric subgroups. *Osaka Journal of Mathematics*, 59:703–726, 2022.

[Jor05] Andrei Jorza. The birch and swinnerton-dyer conjecture for abelian varieties over number fields, 2005.

[Joy02] André Joyal. Quasi-categories and kan complexes. *Journal of Pure and Applied Algebra*, 175(1-3):207–222, 2002.

[Kat90] Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, 1990.

[Kat96] Nicholas M. Katz. *Rigid Local Systems*, volume 139 of *annals of Mathematics Studies*. Princeton University Press, 1996.

[Kat98] Nicholas M. Katz. *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, 1998.

[Kat12] Nicholas M. Katz. *Convolution and Equidistribution Sato-Tate Theorems for Finite-Field Mellin Transforms*, volume 180 of *Annals of Mathematics Studies*. Princeton University Press, 2012.

[Kim23] Hyun Jong Kim. `trouver`, 2023. GitHub repository: https://github.com/hyunjongkimmath/trouver.

[Kim24] Hyun Jong Kim. *Cohen-Lenstra heuristics and vanishing of zeta functions for superelliptic curves over finite fields*. PhD thesis, University of Wisconsin-Madison, 2024.

[KL85] Nicholas M. Katz and Gérard Laumon. Transformation de fourier et majoration de sommes exponentielles. *Publications Mathématiques de l'IHÉS*, 62:145–202, 1985.

[KLSW23] Jesse Leo Kass, Marc Levine, Jake P. Solomon, and Kirsten Wickelgren. A quadratically enriched count of rational curves. arXiv 2307.01936, 2023.

[KM23] Seoyoung Kim and M. Ram Murty. From the Birch and Swinnerton-Dyer conjecture to Nagao's conjecture. *Mathematics of Computation*, 92(339):385–408, 2023.

[KMS17] Emmanuel Kowalski, Philippe Michel, and Will Sawin. Bilinear forms with Kloosterman sums and applciations. *Annals of Mathematics*, 186:413–500, 2017.

[KP24] Hyun Jong Kim and Sun Woo Park. Global $\mathbb{A}^1$ degrees of covering maps between modular curves, 2024.

[Krä14] Thomas Krämer. Perverse sheaves on semiabelian varieties. *Rendiconti del Seminario Matematico della Università di Padova*, 132:83–102, 2014.

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45. American Mathematical Society, 1999.

[KS22] Timo Keller and Michael Stoll. Exact verification of the strong bsd conjecture for some absolutely simple abelian surfaces. *Comptes Rendus Mathématique*, 360:483–489, 2022.

[KW13] Reinhardt Kiehl and Rainer Weissauer. *Weil Conjectures, Perverse Sheaves and ℓ'adic Fourier Transform*, volume 42 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics*. Springer Berlin, Heidelberg, 2013.

[KW15] Thomas Krämer and Rainer Weissauer. Vanishing theorems for constructible sheaves on abelian varieties. *J. Algebraic Geometry*, 24:531–568, 2015.

[KW19] Jesse Leo Kass and Kirsten Wickelgren. The class of Eisenbud-Khimshiashvili-Levine is the local $\mathbb{A}^1 -$ Brouwer degree. *Duke Mathematical Journal*, 168(3):429–469, 2019.

[KW21] Jesse Leo Kass and Kirsten Wickelgren. An arithmetic count of the lines on a smooth cubic surface. *Compositio Mathematica*, 157(4):677–709, 2021.

[Laf02] Laurent Lafforgue. Chtoucas de Drinfeld et correspondance de Langlands. *Inventiones mathematicae*, 147:1–241, 2002.

[Lom17] Davide Lombardo. Galois representations attached to abelian varieties of cm type. *Bulletin de la Société mathématique de France*, 145(3):469–501, 2017.

[Lur09] Jacob Lurie. *Higher topos theory*. Princeton University Press, 2009.

[May99] Jon Peter May. *A Concise Course in Algebraic Topology*. Chicago Lectures in Mathematics. University of Chicago Press, 1999.

[Mil80] James S. Milne. *Etale cohomology*. Number 33 in Princeton Mathematical Series. Princeton university press, 1980.

[Mil07] James S. Milne. Quotients of Tannakian categories. *Theory and Applications of Categories*, 18(21):654–664, 2007.

[Mil13] James S. Milne. Lie algebras, algebraic groups, and lie groups, 2013. Available at www.jmilne.org/math/.

[Mil17] James S. Milne. *Algebraic Groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2017.

[Mit14] Howard H. Mitchell. The subgroups of the quaternary abelian linear group. *Trans. Amer. Math. Soc.*, 15(4):379–396, 1914.

[Mor06] Fabien Morel. A1-algebraic topology. In *International Congress of Mathematicians*, volume 2, pages 1035–1059, 2006.

[Mor12] Fabien Morel. *A1-Algebraic Topology over a field*. Lecture Notes in Mathematics. Springer Berlin, Heidelberg, 2012.

[MV99] Fabien Morel and Vladimir Voevodsky. A1-homotopy theory of schemes. *Publications Mathématiques de l'IHÉS*, 90:45–143, 1999.

[Nag97] Koh-ichi Nagao. Q(t)-rank of elliptic curves and certain limit coming from the local points. *Manuscripta mathematica*, 92(1):13–32, 1997.

[nLa25a] nLab authors. geometric morphism. `https://ncatlab.org/nlab/show/geometric+morphism`, July 2025. Revision 61.

[nLa25b] nLab authors. homotopy group of a spectrum. `https://ncatlab.org/nlab/show/homotopy+group+of+a+spectrum`, June 2025. Revision 7.

[nLa25c] nLab authors. Introduction to Stable homotopy theory – 1-1. `https://ncatlab.org/nlab/show/Introduction+to+Stable+homotopy+theory+--+1-1`, June 2025. Revision 43.

[nLa25d] nLab authors. model structure on topological sequential spectra. `https://ncatlab.org/nlab/show/model+structure+on+topological+sequential+spectra`, June 2025. Revision 61.

[nLa25e] nLab authors. point of a topos. `https://ncatlab.org/nlab/show/point+of+a+topos`, July 2025. Revision 53.

[nLa25f] nLab authors. sheafification. `https://ncatlab.org/nlab/show/sheafification`, September 2025. Revision 40.

[nLa25g] nLab authors. stable homotopy category. `https://ncatlab.org/nlab/show/stable+homotopy+category`, June 2025. Revision 31.

[OT14] Christian Okonek and Andrei Teleman. Intrinsic signs and lower bounds in real algebraic geometry. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2014(688):219–241, 2014.

[Poo18] Bjorn Poonen. Heuristics for the arithmetic of elliptic curves. In *Proceedings of the International Congress of Mathematicians: Rio de Janeiro 2018*, pages 399–414. World Scientific, 2018.

[PR12] BJORN POONEN and ERIC RAINS. Random maximal isotropic subspaces and selmer groups. *Journal of the American Mathematical Society*, 25(1):245–269, 2012.

[Pri24] Rachel Pries. The torelli locus and newton polygons, 2 2024. Lecture Notes for the 2024 Arizona Winter School.

[Pri25] Rachel Pries. Some cases of oort's conjecture about newton polygons of curves. *Nagoya Mathematical Journal*, 257:93–103, 2025.

[PW21] Sabrina Pauli and Kirsten Wickelgren. Applications to $\mathbb{A}^1$-enumerative geometry of the $\mathbb{A}^1$-degree. *Research in the Mathematical Sciences*, 8(24):24–29, 2021.

[Ros02] Michael Rosen. *Number Theory in Function Fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2002.

[RS98] Michael Rosen and Joseph H. Silverman. On the rank of an elliptic surface. *Inventiones mathematicae*, 133:43–67, 1998.

[Rud87] Walter Rudin. *Real and Complex Analysis*. Mathematics Series. McGraw-Hill Book Company, 3 edition, 1987.

[Saw24] Will Sawin. General multiple dirichlet series from perverse sheaves. *Journal of Number Theory*, 262:408–453, 2024.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math*, 15:259–331, 1972.

[Ser00] Jean-Pierre Serre. Lettre à marie-france vignéras du 10/2/1986. *Oeuvres–Collected Papers*, 4:38–55, 2000.

[SFFK23] Will Sawin, Arthur Forey, Javier Fresán, and Emmanuel Kowalski. Quantitative sheaf theory. *Journal of the American Mathematical Society*, 36(3):653–726, 2023.

[Sil89] Joseph H. Silverman. Elliptic curves of bounded degree and height. *Proceedings of the American Mathematical Society*, 105(3):540–545, 1989.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 2 edition, 2009.

[ST21] Will Sawin and Jacob Tsimerman. Bounds for the stalks of perverse sheaves in characteristic p and a conjecture of shende and tsimerman. *Inventiones mathematicae*, 224(1):1–32, 2021.

[Sta25] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2025.

[Tat65] John T. Tate. Algebraic cycles and poles of zeta functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 93–110. Harper & Row, 1965. Also in Collected works of John Tate (2 vols.), Amer. Math. Soc. (2016), vol. 2.

[Tat66] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki : années 1964/65 1965/66, exposés 277-312*, number 9 in Astérisque, pages 415–440. Société mathématique de France, 1966. talk:306.

[Tay08] Richard Taylor. Automorphy for some l-adic lifts of automorphic mod l galois representations. ii. *Publications mathématiques*, 108:183–239, 2008.

[Voe98] Vladimir Voevodsky. A1-homotopy theory. In *Proceedings of the international congress of mathematicians*, volume 1, pages 579–604. Berlin, 1998.

[Wei94] Charles A. Weibel. *An Introduction to Homological Algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1994. First paperback edition 1995 Reprinted 1997.

[Wik25] Wikipedia contributors. Frobenius endomorphisms#frobenius for schemes — Wikipedia, the free encyclopedia, 2025. [Online; accessed 08-July-2025].

[You06] Matthew Young. Low-lying zeros of families of elliptic curves. *Journal of the American Mathematical Society*, 19(1):205–250, 2006.

[Yu97] Jiu-Kang Yu. Toward a proof of the Cohen-Lenstra conjecture in the function field case. preprint, 1997.