Algebraic Structures 3 1998

2. Categories and functors

2.1. Definitions

2.1.1. Definition. A category $\mathcal{Q}$ consists of objects $\mathrm{Ob}(\mathcal{Q})$ and morphisms between objects: for every $Q, R \in \mathcal{Q}$ there is a set $\mathrm{Mor}(R, S)$ which is called the set of morphisms from R to S; for every three objects Q, R, S in $\mathcal{Q}$ there is a composition of morphisms, i.e. a map

$$\mathrm{Mor}(R, S) \times \mathrm{Mor}(Q, R) \to \mathrm{Mor}(Q, S), \quad (f, g) \to f \circ g.$$

The following axioms should be satisfied:

(1) The intersection of $\mathrm{Mor}(Q, R)$ and $\mathrm{Mor}(Q', R')$ is empty unless $Q = Q'$ and $R = R'$.

(2) For every Q of $\mathrm{Ob}(\mathcal{Q})$ there is a morphism $\mathrm{id}_Q \in \mathrm{Mor}(Q, Q)$ such that for every R in $\mathrm{Ob}(\mathcal{Q})$ and every $h \in \mathrm{Mor}(R, Q)$, $g \in \mathrm{Mor}(Q, R)$

$$\mathrm{id}_Q \circ h = h, g \circ \mathrm{id}_Q = g.$$

(unit axiom)

(3) For every Q, R, S, T in $\mathrm{Ob}(\mathcal{Q})$ and every $f \in \mathrm{Mor}(Q, R), g \in \mathrm{Mor}(R, S), h \in \mathrm{Mor}(S, T)$

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

(associativity of the composition of morphisms).

2.1.2. An element $f \in \mathrm{Mor}(Q, R)$ can be written as $f \colon Q \to R$.

2.2. Examples

2.2.1. The category Set has sets as objects, maps of sets as morphisms.

2.2.2. The category Gr has groups as objects, homomorphisms of groups as morphisms.

2.2.3. The category Rg consists of rings as objects, homomorphisms of rings as morphisms.

2.2.4. The category $A - mod$ consists of left modules over a (not necessarily commutative) ring A as objects, homomorphisms of rings as morphisms. Note that $\mathbb{Z} - mod$ coincides with the category Ab of abelian groups as objects, homomorphisms of groups as morphisms.

2.2.5. The category Fld consists of fields as objects, homomorphisms of rings as morphisms.

2.3. Definitions

2.3.1. Definition. A morphism $f: Q \to R$ is called an isomorphism if there is a morphism $g: R \to Q$ such that $f \circ g = \mathrm{id}_R$ and $g \circ f = \mathrm{id}_Q$. It is easy to show that if g exists, then g is unique. The objects Q and R are called isomorphic objects.

Isomorphisms in Set are bijections.

An isomorphism from Q to Q is called an automorphism of Q, the set of all automorphisms is denoted by $\mathrm{Aut}(Q)$. It is a group.

2.3.2. Morphisms from Q to Q are called endomorphisms. The set of all endomorphism of Q is denoted by $\mathrm{End}(Q)$.

2.3.3. A morphism $f: Q \to R$ is called a monomorphism if for every two morphisms $g_1, g_2: S \to Q$

$$f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2$$

(can cancel f on the left).

Monomorphisms of categories of 2.2.1-2.2.5 are injective maps. Every morphism of a category of 2.2.1-2.2.5 which is injective is a monomorphism.

2.3.4. A morhism $f: Q \to R$ is called an epimorphism if for every two morphisms $g_1, g_2: R \to S$

$$g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2$$

(can cancel f on the right).

Surjective morphisms of categories of 2.2.1-2.2.5 are epimorphisms.

Lemma. *A morphism of Set, $A - mod$ which is an epimorphism is surjective.*

Proof. If $f: Q \to R$ is not surjective for sets Q, R, then define $g_i: R \to \{0,1\}$ by $g_1(f(Q)) = 0$, $g_1(r) = 1$ for $r \in R \setminus f(Q)$ and $g_2(R) = 0$. Then $g_1 \circ f = g_2 \circ f$ and $g_1 \neq g_2$.

If $f: Q \to R$ is not surjective for modules Q, R, then let $g_1: R \to R/f(Q)$ be the canonical surjective homomorphism and $g_2: R \to R/f(Q)$ be the zero homomorphism. Then $g_1 \circ f = g_2 \circ f$ and $g_1 \neq g_2$.

However, in other categories there are epimorphisms which are not surjective: for example, the inclusion $f: \mathbb{Z} \to \mathbb{Q}$ is an epimorphism in Rg. Indeed, assume that $g_1: \mathbb{Q} \to A$ is a ring homomorphism, and $g_2: \mathbb{Q} \to A$ is a ring homomorphism such that $g_1 \circ f = g_2 \circ f$. If the kernel of g_1 is $\mathbb{Q}$, then its image is $\{0\}$. Then $\mathbb{Z} \subset \ker(g_2)$, so $\ker(g_2) = \mathbb{Q}$ and $g_1 = g_2$. If the kernel of g_1 is (0), then its image is an integral domain and so is the image of g_1 bu the preceding arguments. From $g_1(n) = g_2(n)$ for every integer n, we get $mg_1(n/m) = g_1(n) = g_2(n) = mg_2(n/m)$, so $g_1(n/m) = g_2(n/m)$ and $g_1 = g_2$.

Note that f isn't an isomorphism, though it is a monomorphism and epimorphism.

2.3.5. Definition. Let $\mathcal{Q}$ be a category. The opposite category $\mathcal{Q}^{op}$ has the same objects as $\mathcal{Q}$, for Q, R in $\mathrm{Ob}(\mathcal{Q}^{op})$ the set $\mathrm{Mor}_{\mathcal{Q}^{op}}(Q, R)$ is equal by the definition to the set $\mathrm{Mor}_{\mathcal{Q}}(R, Q)$; the composition

$$\mathrm{Mor}_{\mathcal{Q}^{op}}(R, S) \times \mathrm{Mor}_{\mathcal{Q}^{op}}(Q, R) \to \mathrm{Mor}_{\mathcal{Q}^{op}}(Q, S)$$

is defined as $(f, g) \to g \circ f \in \mathrm{Mor}_{\mathcal{Q}}(S, Q) = \mathrm{Mor}_{\mathcal{Q}^{op}}(Q, S)$.

Monomorphisms of $\mathcal{Q}$ are epimorphisms of $\mathcal{Q}^{op}$; epimorphisms of $\mathcal{Q}$ are monomorphisms of $\mathcal{Q}^{op}$.

2.3.6. Definition. An initial object of $\mathcal{Q}$ (if it exists) is an object I such that for every Q in $\mathrm{Ob}(\mathcal{Q})$ there is exactly one morphism from I to Q. A terminal object of $\mathcal{Q}$ (if it exists) is an object T such that for every Q in $\mathrm{Ob}(\mathcal{Q})$ there is exactly one morphism from Q to T.

All initial objects are isomorphic, and all terminal objects are isomorphic.

For example, the initial object of Set is the empty set; the terminal object of Set is any one-element set. The group consisting of one element is an initial and terminal object of Gr and Ab. The A-module $\{0\}$ is an initial and terminal object of $A - mod$.

2.3.7. Let Q in $CalQ$ and let $\mathcal{Q}_Q$ be a category whose objects are morphisms $f\colon R \to Q$, R in $\mathrm{Ob}(\mathcal{Q})$ and morhisms from $f\colon R \to Q$ to $g\colon S \to Q$ are morphisms $h\colon R \to S$ such that $g \circ h = f$.

2.3.8. Let $\mathcal{Q}$ be a category. Define a new category $\mathcal{M}(\mathcal{Q})$ whose objects are morphisms of $\mathcal{Q}$ and for two morphisms $f\colon Q \to R \in \mathrm{Ob}(\mathcal{M}(\mathcal{Q}))$ and $f'\colon Q' \to R' \in \mathrm{Ob}(\mathcal{M}(\mathcal{Q}))$ morphism of f to f' in $\mathcal{M}(\mathcal{Q})$ is the pair $(\phi\colon A \to A', \psi\colon B \to B')$ of morphisms of $\mathcal{Q}$ such that $\psi \circ f = f' \circ \phi$.

2.4. Products and coproducts

2.4.1. Definition. If Q_k, $k \in K$ is a set of objects in $\mathcal{Q}$, then a product $\prod_{k\in K} Q_k$ (if it exists) is an object of $\mathcal{Q}$ together with morphisms $\pi_k\colon \prod_{k\in K} Q_k \to Q_k$ such that for every Q in $\mathrm{Ob}(\mathcal{Q})$ and every set of morphisms $f_k\colon Q \to Q_k$ there is a unique morphism $f\colon Q \to \prod_{k\in K} Q_k$ such that

$$\pi_k \circ f = f_k \quad \text{for all } k \in K.$$

2.4.2. If a product exists it is unique up to an isomorphism.

If $K = \{1, 2\}$ we just write $Q_1 \times Q_2$ for the product of Q_1 and Q_2.

2.4.3. Product in category Set is the product of sets, in Ab is the product of groups, in Rg is the product of rings, in $A - mod$ is the product of modules, in Fld doesn't exist.

2.4.4. Definition. If Q_k, $k \in K$ is a set of objects in $\mathcal{Q}$, then a coproduct $\coprod_{k\in K} Q_k$ (if it exists) is an object of $\mathcal{Q}$ together with morphisms $i_k\colon Q_k \to \coprod_{k\in K} Q_k$ such that for every Q in $\mathrm{Ob}(\mathcal{Q})$ and every set of morphisms $f_k\colon Q_k \to Q$ there is a unique morphism $f\colon \coprod_{k\in K} Q_k \to Q$ such that

$$f \circ i_k = f_k \quad \text{for all } k \in K.$$

2.4.5. Coproduct in category Set is the disjoint union of sets, in Ab is the direct sum of groups, in $A - mod$ is the direct sum of modules, in Rg and Fld doesn't exist.

2.4.6. Coproduct in $\mathcal{Q}$ corresponds to product in $\mathcal{Q}^{op}$ and product in in $\mathcal{Q}$ corresponds to coproduct in $\mathcal{Q}^{op}$.

2.5. Functors of categories

2.5.1. Definition. A (covariant) functor $\mathcal{F}$ from a category $\mathcal{Q}$ to a category $\mathcal{R}$ is a rule which associates an object $\mathcal{F}(Q)$ of $\mathcal{R}$ to every object $Q \in \mathcal{Q}$, and a morphism $\mathcal{F}(f)\colon \mathcal{F}(Q) \to \mathcal{F}(R)$ to every morphism $f\colon Q \to R$ such that the following properties hold:

(1) $\mathcal{F}(\mathrm{id}_Q) = \mathrm{id}_{\mathcal{F}(Q)}$ for every Q in $\mathrm{Ob}(\mathcal{Q})$;

(2) $\mathcal{F}(f \circ g) = \mathcal{F}(f) \circ \mathcal{F}(g)$ for every $f \in \mathrm{Mor}(R, S), g \in \mathrm{Mor}(Q, R)$.

2.5.2. Example 1. The identity functor $\mathrm{id}_{\mathcal{Q}}$ associates Q to Q in $\mathrm{Ob}(\mathcal{Q})$ and f to $f \in \mathrm{Mor}(\mathcal{Q})$.

Example 2. A forgetful functor, for example from $A - mod$ to Ab (forget the A-module structure), or from Gr to Set (forget the group structure).

2.5.3. If $\mathcal{F}: \mathcal{Q} \to \mathcal{R}$ and $\mathcal{G}: \mathcal{R} \to \mathcal{S}$ are two functors, then $\mathcal{G} \circ \mathcal{F} : \mathcal{Q} \to \mathcal{S}$ is defined as $(\mathcal{G} \circ \mathcal{F})(Q) = \mathcal{G}(\mathcal{F}(Q))$ and $(\mathcal{G} \circ \mathcal{F})(f) = \mathcal{G}(\mathcal{F}(f))$.

Then $\mathrm{id}_{\mathcal{Q}} \circ \mathcal{F} = \mathcal{F} = \mathcal{F} \circ \mathrm{id}_{\mathcal{Q}}$.

2.5.4. A contravariant functor $\mathcal{F}: \mathcal{Q} \to \mathcal{R}$ is a (covariant) functor $\mathcal{F}: \mathcal{Q} \to \mathcal{R}^{op}$, i.e. a rule which associates an object $\mathcal{F}(Q)$ of $\mathcal{R}$ to every object Q in $\mathrm{Ob}(\mathcal{Q})$, and a morphism $\mathcal{F}(f): \mathcal{F}(R) \to \mathcal{F}(Q)$ to every morphism $f: Q \to R$ such that the following properties hold:

(1) $\mathcal{F}(\mathrm{id}_Q) = \mathrm{id}_{\mathcal{F}(Q)}$ for every Q in $\mathrm{Ob}(\mathcal{Q})$;

(2) $\mathcal{F}(f \circ g) = \mathcal{F}(g) \circ \mathcal{F}(f)$ for every $f \in \mathrm{Mor}(R, S), g \in \mathrm{Mor}(Q, R)$.

2.5.5. Example 3. Let Q in $\mathrm{Ob}(\mathcal{Q})$. Define a functor $\mathcal{H}om(Q, \cdot): \mathcal{Q} \to Set$ by

$$\mathcal{H}om(Q, \cdot)(R) = \mathrm{Mor}(Q, R) \quad \text{and} \quad (\mathcal{H}om(Q, \cdot)(f))(g) = f \circ g$$

for every $g \in \mathrm{Mor}(Q, R)$ for a morphism $f: R \to S$, so $\mathcal{H}om(Q, \cdot)(f): \mathrm{Mor}(Q, R) \to \mathrm{Mor}(Q, S)$. If $\mathcal{Q} = mod - A$, then $\mathcal{H}om(Q, \cdot): \mathcal{Q} \to \mathcal{Q}$, $Hom(Q, \cdot)(R) = \mathrm{Hom}(Q, R)$.

Define a contravariant functor $\mathcal{H}om(\cdot, Q): \mathcal{Q} \to Set$ by

$$\mathcal{H}om(\cdot, Q)(R) = \mathrm{Mor}(R, Q) \quad \text{and} \quad (\mathcal{H}om(\cdot, Q)(f))(g) = g \circ f$$

for every $g \in \mathrm{Mor}(R, Q)$ for a morphism $f: S \to R$, so $\mathcal{H}om(\cdot, Q)(f): \mathrm{Mor}(R, Q) \to \mathrm{Mor}(S, Q)$. If $\mathcal{Q} = mod - A$, then $\mathcal{H}om(\cdot, Q): \mathcal{Q} \to \mathcal{Q}$.

2.5.6. Definition. Suppose that for every two morphisms $f, g: Q \to R$ in $\mathcal{Q}$ there is their sum $f + g: Q \to R$ and it is a morphism of $\mathcal{Q}$. A functor $\mathcal{F}: \mathcal{Q} \to \mathcal{Q}$ is called additive if $\mathcal{F}(f + g) = \mathcal{F}(f) + \mathcal{F}(g)$ for every two morphisms $f, g: Q \to R$ in $\mathcal{Q}$.

Lemma. *If $\mathcal{F}$ is an additive functor, then $\mathcal{F}(Q_1 \times Q_2)$ is a product of $\mathcal{F}(Q_1)$ and $\mathcal{F}(Q_2)$.*

Proof. First, let Q_1, Q_2, Q be objects of $\mathcal{Q}$. Suppose there are morphisms

$$i_1: Q_1 \to Q, \quad i_2: Q_2 \to Q, \quad p_1: Q \to Q_1, \quad p_2: Q \to Q_2$$

such that

$$p_1 \circ i_1 = \mathrm{id}_{Q_1}, \quad p_2 \circ i_2 = \mathrm{id}_{Q_2}, \quad p_1 \circ i_2 = 0, \quad p_2 \circ i_1 = 0, \quad i_1 \circ p_1 + i_2 \circ p_2 = \mathrm{id}_Q .$$

Let R be an object of $\mathcal{Q}$ and let $f_k: R \to Q_k$ be morphisms. Define $f: R \to Q$ as $f = i_1 \circ f_1 + i_2 \circ f_2$. Then $p_k \circ f = p_k \circ (i_1 \circ f_1 + i_2 \circ f_2) = f_k$. If $g: R \to Q$ satisfies $p_k \circ g = f_k$, then $p_k \circ (f - g) = 0$ and $f - g = (i_1 \circ p_1 + i_2 \circ p_2) \circ (f - g) = 0$, i.e. $f = g$. Thus, Q together with morphisms $p_k: Q \to Q_k$ is a product of Q_1 and Q_2.

Conversely, if Q is a product of Q_1 and Q_2, then there morphisms $i_k, p_k = \pi_k$ satisfy the listed relations.

Thus the property of Q to be a product of Q_1 and Q_2 can be reformulated in terms of morphisms. Then their images with respect to $\mathcal{F}$ satisfy the same relations, and thus, $\mathcal{F}(Q_1 \times Q_2)$ is a product of $\mathcal{F}(Q_1)$ and $\mathcal{F}(Q_2)$.

2.6. Complexes, commutative diagrams and exact sequences

Let $\mathcal{Q}$ be $A - mod$. We write groups additively. Denote by 0 the zero A-module. It is an initial and terminal object of $\mathcal{Q}$.

Every morphism in $\mathcal{Q}$ has its kernel (as a homomorphism in this case) and image.

2.6.1. Definition. A sequence of objects and morphisms in $\mathcal{Q}$

$$\dots \longrightarrow Q_{n+1} \xrightarrow{f_{n+1}} Q_n \xrightarrow{f_n} Q_{n-1} \longrightarrow \dots$$

is called exact if the kernel of f_n is equal to the image of f_{n+1} for every $n \in \mathbb{Z}$.

Example. A short sequence is

$$0 \longrightarrow Q \xrightarrow{f} R \xrightarrow{g} S \longrightarrow 0$$

and its exactness means that f is a injective, g is surjective and the kernel of g coincides with the image of f, so if we identify Q with its image in R, then S is isomorphic to R/Q.

2.6.2. Definition. A diagram of objects and morphisms is called commutative if the result of compositions of morphisms doesn't depend on the route chosen. For instance, the diagram

$$\begin{tikzcd}
\dots \arrow[r] & Q_{n.m} \arrow[r, "f_{n,m}"] \arrow[d, "g_{n,m}"'] & Q_{n,m-1} \arrow[r] \arrow[d, "g_{n,m-1}"'] & \dots \\
\dots \arrow[r] & Q_{n-1,m} \arrow[r, "f_{n-1,m}"] & Q_{n-1,m-1} \arrow[r] & \dots
\end{tikzcd}$$

of objects $Q_{n,m}$ of $\mathcal{Q}$ and morphisms $f_{n,m}: Q_{n,m} \to Q_{n,m-1}$, $g_{n,m}: Q_{n,m} \to Q_{n-1,m}$ is commutative if $f_{n-1,m} \circ g_{n,m} = g_{n,m-1} \circ f_{n,m}$ for every $n, m \in \mathbb{Z}$.

Note that a functor sends a commutative diagram into a commutative diagram, since $\mathcal{F}(f \circ \dots \circ g) = \mathcal{F}(f) \circ \dots \circ \mathcal{F}(g)$.

2.6.3. Definition. A chain complex $\mathbf{C}$ is a sequence C_n of objects of $\mathcal{Q}$, $n \in \mathbb{Z}$ such that there are morphisms $d_n: C_n \to C_{n-1}$ such that $d_n \circ d_{n+1}$ is the zero morphism $C_{n+1} \to C_{n-1}$. Note that every exact sequence is a chain complex.

We write

$$\dots \longrightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \dots$$

The morphisms d_n are called differentials of $\mathbf{C}$. The kernel of d_n which is an object of $\mathcal{Q}$ consists of so called n-cycles and is denoted by $Z_n(\mathbf{C})$. The image of d_{n+1} which is an object of $\mathcal{Q}$ consists of n-boundaries and is denoted by $B_n(\mathbf{C})$. Since $d_n \circ d_{n+1} = 0$ we get $0 \subset B_n(\mathbf{C}) \subset Z_n(\mathbf{C}) \subset C_n$ for all n. The quotient $Z_n(\mathbf{C})/B_n(\mathbf{C})$ is called the nth homology of $\mathbf{C}$ and is denoted by $H_n(\mathbf{C})$.

A complex $\mathbf{C}$ is called exact if sequence

$$\dots \longrightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \dots$$

is exact, i.e. $H_n(\mathbf{C}) = 0$ for all $n \in \mathbb{Z}$.

2.6.4. Definition. A cochain complex $\mathbf{C}$ is a sequence C^n of objects of $\mathcal{Q}$, $n \in \mathbb{Z}$ such that there are morphisms $d^n: C^n \to C^{n+1}$ such that $d^n \circ d^{n-1}$ is the zero morphism $C^{n-1} \to C^{n+1}$. We write

$$\dots \longrightarrow C^{n-1} \xrightarrow{d^{n-1}} C^n \xrightarrow{d^n} C^{n+1} \longrightarrow \dots$$

The morphisms d^n are called differentials of $\mathbf{C}$. The kernel of d^n which is an object of $\mathcal{Q}$ consists of n-cocycles and is denoted by $Z^n(\mathbf{C})$. The image of d^{n-1} which is an object of $\mathcal{Q}$ consists of n-coboundaries and is denoted by $B^n(\mathbf{C})$. Since $d^n \circ d^{n-1} = 0$ we get $0 \subset B^n(\mathbf{C}) \subset Z^n(\mathbf{C}) \subset C^n$ for all n. The quotient $Z^n(\mathbf{C})/B^n(\mathbf{C})$ is called the nth cohomology of $\mathbf{C}$ and is denoted by $H^n(\mathbf{C})$.

2.6.5. Definition. For two chain complexes

$$\ldots \longrightarrow C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \longrightarrow \ldots$$

and

$$\ldots \longrightarrow C'_{n+1} \xrightarrow{d'_{n+1}} C'_n \xrightarrow{d'_n} C'_{n-1} \longrightarrow \ldots$$

a morphism $u: \mathbf{C} \to \mathbf{C}'$ is a sequence of of morphisms $u_n: C_n \to C'_n$ such that

$$u_{n-1} \circ d_n = d_{n-1} \circ u_n$$

for every n. In other words, the diagram

$$\begin{tikzcd}
\ldots \arrow[r] & C_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "u_{n+1}"'] & C_n \arrow[r, "d_n"] \arrow[d, "u_n"'] & C_{n-1} \arrow[r] \arrow[d, "u_{n-1}"'] & \ldots \\
\ldots \arrow[r] & C'_{n+1} \arrow[r, "d'_{n+1}"] & C'_n \arrow[r, "d'_n"] & C'_{n-1} \arrow[r] & \ldots
\end{tikzcd}$$

is commutative.

Definition. A category $Ch(\mathcal{Q})$ of chain complexes over $\mathcal{Q}$ has chain complexes as objects and morphisms of chain complexes as morphisms.

The morphism $u: \mathbf{C} \to \mathbf{C}'$ induces morphisms $H_n(\mathbf{C}) \to H_n(\mathbf{C}')$ for all n.

2.6.6. Definition. A sequence of chain complexes $\mathbf{C}^{(n)}$ and morphisms $u^{(n)}: \mathbf{C}^{(n)} \to \mathbf{C}^{(n-1)}$ is called exact if for every $m \in \mathbb{Z}$ the sequence $C_m^{(n+1)} \xrightarrow{u_m^{(n+1)}} C_m^{(n)} \xrightarrow{u_m^{(n)}} C_m^{(n-1)}$ for every n.

2.6.7. Note that a functor send a chain complex into a chain complex, since $0 = \mathcal{F}(0) = \mathcal{F}(d_n \circ d_{n+1}) = \mathcal{F}(d_n) \circ \mathcal{F}(d_{n+1})$.

2.7. Long sequence of homologies

Let $\mathcal{Q}$ be $A - mod$.

2.7.1. Let $f: Q \to R$ be a morphism of $\mathcal{Q}$. Then we have an exact sequence

$$0 \longrightarrow \ker(f) \longrightarrow Q \xrightarrow{f} R \longrightarrow \operatorname{coker}(f) \longrightarrow 0.$$

Here $\ker(f)$ is the kernel of f and $\operatorname{coker}(f) = R/f(Q)$ is the cokernel of f.

2.7.2. Snake Lemma. *For a commutative diagram*

$$\begin{tikzcd}
 & A \arrow[r] \arrow[d, "f"'] & B \arrow[r, "p"] \arrow[d, "g"'] & C \arrow[r] \arrow[d, "h"'] & 0 \\
0 \arrow[r] & A' \arrow[r, "i"] & B' \arrow[r] & C' &
\end{tikzcd}$$

with exact rows there is an exact sequence

$$\ker(f) \longrightarrow \ker(g) \longrightarrow \ker(h) \xrightarrow{\delta} \operatorname{coker}(f) \longrightarrow \operatorname{coker}(g) \longrightarrow \operatorname{coker}(h)$$

with δ defined by the formula $\delta(c) = i^{-1}gp^{-1}(c) \mod \operatorname{coker}(f)$ for $c \in \ker(h)$. Moreover, if $A \to B$ is a monomorphism, then so is $\ker(f) \to \ker(g)$ and if $B' \to C'$ is an epimorphism, then so is $\operatorname{coker}(g) \to \operatorname{coker}(h)$.

Proof. Diagram chase.

2.7.3. Theorem. *Let*

$$0 \longrightarrow \mathbf{A} \xrightarrow{f} \mathbf{B} \xrightarrow{g} \mathbf{C} \longrightarrow 0$$

be a short exact sequence of chain complexes. Then there are morphisms $\delta_n\colon H_n(\mathbf{C}) \to H_{n-1}(\mathbf{A})$ called connecting morphisms such that

$$\dots \xrightarrow{g_{n+1}} H_{n+1}(\mathbf{C}) \xrightarrow{\delta_{n+1}} H_n(\mathbf{A}) \xrightarrow{f_n} H_n(\mathbf{B}) \xrightarrow{g_n} H_n(\mathbf{C}) \xrightarrow{\delta_n} H_{n-1}(\mathbf{A}) \longrightarrow \dots$$

is an exact sequence.

Similarly, if

$$0 \longrightarrow \mathbf{A} \xrightarrow{f} \mathbf{B} \xrightarrow{g} \mathbf{C} \longrightarrow 0$$

is a short exact sequence of cochain complexes, then there are morphisms $\delta^n\colon H^n(\mathbf{C}) \to H^{n+1}(\mathbf{A})$ called connecting morphisms such that

$$\dots \xrightarrow{g^{n-1}} H^{n-1}(\mathbf{C}) \xrightarrow{\delta^{n-1}} H^n(\mathbf{A}) \xrightarrow{f^n} H^n(\mathbf{B}) \xrightarrow{g^n} H^n(\mathbf{C}) \xrightarrow{\delta^n} H^{n+1}(\mathbf{A}) \longrightarrow \dots$$

is an exact sequence.

Proof. From the diagram

$$\begin{tikzcd}
0 \arrow[r] & A_n \arrow[r] \arrow[d, "d_n^A"'] & B_n \arrow[r] \arrow[d, "d_n^B"'] & C_n \arrow[r] \arrow[d, "d_n^C"'] & 0 \\
0 \arrow[r] & A_{n-1} \arrow[r] & B_{n-1} \arrow[r] & C_{n-1} \arrow[r] & 0
\end{tikzcd}$$

and the Snake Lemma we get exact sequences

$$0 \longrightarrow Z_n(\mathbf{A}) \longrightarrow Z_n(\mathbf{B}) \longrightarrow Z_n(\mathbf{C})$$

and

$$A_n/d_{n+1}^A(A_{n+1}) \longrightarrow B_n/d_{n+1}^B(B_{n+1}) \longrightarrow C_n/d_{n+1}^C(C_{n+1}) \longrightarrow 0.$$

Define morphism $\overline{d}_n^A\colon A_n/d_{n+1}^A(A_{n+1}) \to Z_{n-1}(\mathbf{A})$ as induced by d_n^A. Now we get the commutative diagram

$$\begin{tikzcd}
 & A_n/d_{n+1}^A(A_{n+1}) \arrow[r] \arrow[d, "\overline{d}_n^A"'] & B_n/d_{n+1}^B(B_{n+1}) \arrow[r] \arrow[d, "\overline{d}_n^B"'] & C_n/d_{n+1}^C(C_{n+1}) \arrow[r] \arrow[d, "\overline{d}_n^C"'] & 0 \\
0 \arrow[r] & Z_{n-1}(\mathbf{A}) \arrow[r] & Z_{n-1}(\mathbf{B}) \arrow[r] & Z_{n-1}(\mathbf{C}) &
\end{tikzcd}$$

The kernels of the vertical morphisms is $H_n(\mathbf{A})$, $H_n(\mathbf{B})$, $H_n(\mathbf{C})$ and their cokernels are $H_{n-1}(\mathbf{A})$, $H_{n-1}(\mathbf{B})$, $H_{n-1}(\mathbf{C})$. By the Snake Lemma we deduce an exact sequence

$$H_n(\mathbf{A}) \longrightarrow H_n(\mathbf{B}) \longrightarrow H_n(\mathbf{C}) \longrightarrow H_{n-1}(\mathbf{A}) \longrightarrow H_{n-1}(\mathbf{B}) \longrightarrow H_{n-1}(\mathbf{C}).$$

Pasting together these sequences we get the long exact sequence.

2.7.4. Remark. If

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{A} \arrow[r] \arrow[d] & \mathbf{B} \arrow[r] \arrow[d] & \mathbf{C} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & 'A \arrow[r] & \mathbf{B}' \arrow[r] & \mathbf{C}' \arrow[r] & 0
\end{tikzcd}$$

is a commutative diagram with short exact sequences of chain complexes, then the diagram

$$\begin{tikzcd}
\dots \arrow[r] & H_n(\mathbf{B}) \arrow[r] \arrow[d] & H_n(\mathbf{C}) \arrow[r] \arrow[d] & H_{n+1}(\mathbf{A}) \arrow[r] \arrow[d] & \dots \\
\dots \arrow[r] & H_n(\mathbf{B}) \arrow[r] & H_n(\mathbf{C}) \arrow[r] & H_{n+1}(\mathbf{A}) \arrow[r] & \dots
\end{tikzcd}$$

is commutative.

The proof follows from the explicit description of the morphism $\delta_n\colon H_n(\mathbf{C}) \to H_{n-1}(\mathbf{A})$: δ_n transforms an n-cycle $x \in C_n$ to $f_{n-1}^{-1} d_n^B g_n^{-1}(x) \mod d_{n-1}A_{n-1}$.

3. Free, projective and injective modules

Let $\mathcal{Q}$ be $A - mod$.

3.1. Free objects

3.1.1. Let X be a set. Consider a category $Map(X, \mathcal{Q})$ objects of which are maps $f: X \to Q$, $Q \in \mathcal{Q}$, and a morphism from an object $f: X \to Q$ to an object $g: X \to R$ is a morphism $\varphi: Q \to R$ in $\mathrm{Mor}(Q, R)$ such that $g = \varphi \circ f$.

3.1.2. Definition. An object F of $\mathcal{Q}$ together with a map $f: X \to F$ is called a X-free (free) object of $\mathcal{Q}$ if $f: X \to F$ is an initial object of the category $Map(X, \mathcal{Q})$. In other words, for every object Q of $\mathcal{Q}$ and a map $g: X \to Q$ there is a unique morphism $\psi: F \to Q$ in $\mathcal{Q}$ such that

$$\psi \circ f = g.$$

Or, equivalently, for every set $\{q_x \in Q : x \in X\}$ there is a unique morphism $\psi: F \to Q$ such that $\psi(f(x)) = q_x$ for all $x \in X$.

Example. If X consists of one element x, then A, $x \to 1$ is a X-free object in $A - mod$.

3.1.3. Lemma *For every set X there exists a X-free object of $\mathcal{Q}$. Every two X-free objects are isomorphic.*

Proof. Let $F = \coprod_{x \in X} A_x = \oplus_{x \in X} A_x$ in $\mathcal{Q}$ where $A_x = A$. Let the map $f: X \to F$ be defined by $x \to 1$ of the xth component. It is a X-free object of $\mathcal{Q}$: for an object Q of $\mathcal{Q}$ and a map $g: X \to Q$ define $\psi : F \to Q$ by $\psi(\oplus a_x) = \sum_{x \in X} a_x g(x)$. Then $\psi \circ f = g$. If $\psi' \circ f = g$, then $\psi' = \psi$.

Since F is a X-free object, there is a unique morphism $\psi_0: F \to F$ such that $\psi_0 \circ f = f$. We deduce that $\psi_0 = \mathrm{id}_F$.

If F', $f': X \to F'$ is another X-free object, then there is a unique morphism $\psi: F \to F'$ such that $f' = \psi \circ f$ and a unique morphism $\psi': F' \to F$ such that $f = \psi' \circ f'$. Then $f = \psi' \circ \psi \circ f$, so by the previous paragraph $\psi' \circ \psi = \mathrm{id}_F$ and similarly $\psi \circ \psi' = \mathrm{id}_{F'}$, so F and F' are isomorphic.

3.1.4. Lemma. *The coproduct of free objects is free.*

Proof. Let F_k be X_k-free (with $f_k: X_k \to F_k$), $k \in K$. Let $i_k: F_k \to \coprod_{k \in K} F_k$ be as in the definition of a coproduct in 2.4.4. Define $\rho_k: X_k \xrightarrow{f_k} F_k \xrightarrow{i_k} \coprod_{k \in K} F_k$. By the definition of a coproduct there is a map $f: \coprod_{k \in K} X_k \to \coprod_{k \in K} F_k$ such that the composition of $j_k: X_k \to \coprod_{k \in K} X_k$ and f coincides with ρ_k for all $k \in K$.

For a map $g: \coprod_{k \in K} X_k \to Q$ put $g_k = g \circ j_k$, $k \in K$. Then there are morphisms $\psi_k: F_k \to Q$ such that $\psi_k \circ f_k = g_k$ for all $k \in K$. From the definition of a coproduct we deduce there is a morphism $\psi: \coprod_{k \in K} F_k \to Q$ such that $\psi \circ i_k = \psi_k$. Then

$$\psi \circ f \circ j_k = \psi \circ \rho_k = \psi \circ i_k \circ f_k = \psi \circ i_k \circ f_k = \psi_k \circ f_k = g_k = g \circ j_k$$

for every $k \in K$. Then from the definition of a coproduct in 2.4.4 we conclude that $\psi \circ f = g$.

If $\psi' \circ f = g$, then

$$\psi' \circ f \circ j_k = \psi' \circ \rho_k = \psi' \circ i_k \circ f_k = g \circ j_k = g_k = \psi_k \circ f_k,$$

so $\psi' \circ i_k = \psi_k$ and then $\psi' = \psi$.

3.1.5. Lemma. *Every object of $\mathcal{Q}$ is a quotient of a free object.*

Proof. For an object Q put $X = Q$ and let $g\colon X \to Q$ be the identity map. Then there is a X-free object F with $f\colon X \to F$ such that there is a morphism $\psi\colon F \to Q$ satisfying $\psi \circ f = g$. Since g is surjective, ψ is an epimorphism and Q is a quotient of F.

3.2. Projective objects

3.2.1. Definition. An object P is called a summand of an object Q of $\mathcal{Q}$ if there are morphisms $\pi\colon Q \to P$ and $i\colon P \to Q$ such that $\pi \circ i = \mathrm{id}_P$.

Then the kernel if i and the cokernel of π are zero.

3.2.2. Examples.

1) P is a summand of P, just take i and π as the identity morphisms.

2) Define $i\colon P \to P \oplus R, \pi\colon P \oplus R \to P$ by $i_P(p) = (p, 0), \pi_P(p, r) = p$. Then P is a summand of $P \oplus R$.

3) Let P_k be a summand of Q_k, $k = 1, 2$. Then $P_1 \oplus P_2$ is a summand of $Q_1 \oplus Q_2$, just take $\pi = (\pi_1, \pi_2)$ and $i = (i_1, i_2)$.

3.2.3. Definition. A short exact sequence

$$0 \longrightarrow R \xrightarrow{u} Q \xrightarrow{v} S \longrightarrow 0$$

splits if there is a morphism $w\colon S \to Q$ such that $v \circ w = \mathrm{id}_S$.

Then S is a summand of Q. Conversely, if S is a summand of Q, then the sequence

$$0 \longrightarrow R \longrightarrow Q \xrightarrow{\pi} S \longrightarrow 0,$$

where $R = \ker \pi$, splits: $\pi \circ i = \mathrm{id}_S$.

Define a morphism $\rho\colon R \oplus S \to Q$ by $\rho((r, s)) = u(r) + w(s)$. If $\rho((r, s)) = 0$, then $0 = v(\rho((r, s))) = s$ and then $u(r) = 0$, so $r = 0$. Hence ρ is a injective. Since $v(q - wv(q)) = v(q) - v(q) = 0$, $q - wv(q) = u(r)$ for some $r \in R$. Then $q = \rho((r, v(q)))$. Therefore, ρ is an isomorphism and Q is a direct sum of R and S.

Similarly one can show that Q is isomorphic to $R \oplus S$ iff there is a morphism $z\colon Q \to R$ such that $z \circ u = \mathrm{id}_R$.

Thus, S is a summand of Q iff there is a short exact split sequence

$$0 \longrightarrow R \xrightarrow{u} Q \xrightarrow{v} S \longrightarrow 0,$$

iff Q is a direct sum of S and R iff there is a morphism $z\colon Q \to R$ such that $z \circ u = \mathrm{id}_R$.

3.2.4. Definition. An object P is called projective if it is a summand of a free object.

Examples.

1) Every free object is a summand of itself, therefore every free object is projective.

2) Let $A = \mathbb{Z}/6\mathbb{Z}$. By the Chinese remainder theorem A is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, so $\mathbb{Z}/2\mathbb{Z}$ is a projective $\mathbb{Z}/6\mathbb{Z}$-module. However, it isn't a free $\mathbb{Z}/6\mathbb{Z}$-module, since every finite free $\mathbb{Z}/6\mathbb{Z}$-module has cardinality divisible by 6.

3.2.5. Lemma. *For objects P_1, P_2 the direct sum $P_1 \oplus P_2$ is projective iff P_1, P_2 are projective.*

Proof. Let $p_{P_k}: P_1 \oplus P_2 \to P_k$, $i_{P_k}: P_k \to P_1 \oplus P_2$, $k = 1, 2$, be morphisms introduced in example 2) above. If $P_1 \oplus P_2$ is a summand of a free object F with morphisms i, π, then P_k is a summand of F with morphisms $\pi_{P_k} \circ \pi$ and $i \circ i_{P_k}$.

If P_1, P_2 are summands of F_1, F_2, then by example 3) above $P_1 \oplus P_2$ is a summand of $F_1 \oplus F_2$ which is a free object by 3.1.4.

3.2.6. Proposition. *An object P is projective iff for every two objects R, Q, a morphism $\beta: P \to Q$ and an epimorphism $\alpha: R \to Q$*

$$\begin{tikzcd} & P \arrow[d, "\beta"'] & \\ R \arrow[r, "\alpha"] & Q \arrow[r] & 0 \end{tikzcd}$$

there is a morphism $\gamma: P \to R$ such that $\beta = \alpha \circ \gamma$.

Proof. First let's check that if P is a X-free object with $f: X \to P$, then it satisfies the property of the proposition. Denote $g = \beta \circ f$ and $q_x = g(x)$ for $x \in X$. Since α is surjective, $q_x = \alpha(r_x)$ for some $r_x \in R$. According to the definition of a X-free object, there is a morphism $\gamma: P \to R$ such that $\gamma(f(x)) = r_x$ for all $x \in X$. Then $\alpha \circ \gamma(f(x)) = \beta(f(x))$. Morphisms $\alpha \circ \gamma$ and β satisfy $\alpha \circ \gamma \circ f = g = \beta \circ f$, so $\alpha \circ \gamma = \beta$.

Now let P be projective, so there is a free object F and morphisms $\pi: F \to P$ and $i: P \to F$ such that $\pi \circ i = \mathrm{id}_P$. Then we get a morphism $\beta' = \beta \circ \pi: F \to Q$ and from the first paragraph there is a morphism $\gamma': F \to R$ such that $\alpha \circ \gamma' = \beta'$. Then for $\gamma = \gamma' \circ i: P \to R$ we get $\alpha \circ \gamma = \beta' \circ i = \beta \circ \pi \circ i = \beta$, so P satisfied the property of the proposition.

Conversely, assume P satisfies the property of the proposition. Let F be a free object such that P is its quotient, i.e. there is an epimorphism $\alpha: F \to P$. Then there is a morhism $\gamma: P \to F$ such that $\alpha \circ \gamma = \mathrm{id}_P$. Thus, P is a summand of F.

3.2.7. Corollary 1. *Let P be projective. Then for every three objects S, R, Q and a diagram*

$$\begin{tikzcd} & P \arrow[d, "\beta"'] & \\ S \arrow[r, "\delta"] & R \arrow[r, "\alpha"] & Q \end{tikzcd}$$

with exact row and $\alpha \circ \beta = 0$ there is a morphism $\varepsilon: P \to S$ such that

$$\beta = \delta \circ \varepsilon.$$

Proof. Since $\alpha \circ \beta = 0$, we deduce that $\mathrm{im}(\beta) \subset \ker(\alpha) = \delta(S)$. Consider the epimorphism $\delta': S \to \delta(S)$. From the proposition we deduce that there is a morphism $\varepsilon: P \to S$ such that $\beta = \delta' \circ \varepsilon$. Then $\beta = \delta \circ \varepsilon$.

3.2.8. Corollary 2. *P is projective iff every short exact sequence*

$$0 \longrightarrow R \longrightarrow Q \xrightarrow{v} P \longrightarrow 0$$

splits.

Proof. If P is projective, then by the proposition there is a morphism $\gamma: P \to Q$ such that $v \circ \gamma = \mathrm{id}_P$, so the sequence splits.

Let

$$0 \longrightarrow R \longrightarrow F \xrightarrow{v} P \longrightarrow 0$$

be an exact sequence where F is free. Then it splits, so P is a summand of F, and therefore P is projective.

Example 3.) Let $A = \mathbb{Z}/4\mathbb{Z}$. The sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

(the morphism $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is defined as $n \mod 4 \to n \mod 2$) doesn't split, because otherwise $\mathbb{Z}/4\mathbb{Z}$ were isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and wouldn't have an element $1 \mod 4$ of order 4. Thus, $\mathbb{Z}/2\mathbb{Z}$ isn't a projective object in the category $\mathbb{Z}/4\mathbb{Z} - mod$.

3.2.9. Definition. A functor $\mathcal{F}\colon \mathcal{Q} \to \mathcal{Q}$ is called exact (left exact, right exact) if for every short exact sequence

$$0 \longrightarrow R \longrightarrow Q \longrightarrow S \longrightarrow 0$$

the sequence

$$0 \longrightarrow \mathcal{F}(R) \longrightarrow \mathcal{F}(Q) \longrightarrow \mathcal{F}(S) \longrightarrow 0$$

is exact (exact everywhere with exception of $\mathcal{F}(S)$, exact everywhere with exception of $\mathcal{F}(R)$).

Lemma. *The functor $\mathcal{H}om(T, \cdot)\colon \mathcal{Q} \to \mathcal{Q}$ defined in 2.5.5 is left exact.*

Proof. Let

$$0 \to R \xrightarrow{u} Q \xrightarrow{v} S \longrightarrow 0$$

be an exact sequence. If $f\colon T \to R$ and $u \circ f\colon T \to Q$ is the zero morphism, then $f(T) = 0$ and so f is the zero morphism.

For $f\colon T \to R$ clearly $v \circ u \circ f\colon T \to S$ is the zero morphism. If $g\colon T \to S$ is such that $v \circ g\colon T \to S$ is the zero morphism, then for every $t \in T$ $g(t) = u(r_t)$ for a uniquely determined $r_t \in R$. Define $f\colon T \to R$ by $f(t) = r_t$. It is a morphism and $g = u \circ f$.

Similarly one can show that the contravariant functor $\mathcal{H}om(\cdot, T)\colon \mathcal{Q} \to \mathcal{Q}$ is left exact, i.e. for an exact sequence

$$0 \longrightarrow R \longrightarrow Q \longrightarrow S \longrightarrow 0$$

the sequence

$$0 \longrightarrow \mathrm{Hom}(S, T) \longrightarrow \mathrm{Hom}(Q, T) \longrightarrow \mathrm{Hom}(R, T)$$

is exact.

3.2.10. Corollary 3. *P is projective iff the functor $\mathcal{H}om(P, \cdot)\colon \mathcal{Q} \to \mathcal{Q}$ is exact.*

Proof. Let P be projective. Let

$$0 \longrightarrow R \longrightarrow Q \xrightarrow{v} S \longrightarrow 0$$

be an exact sequence. For every morphism $g\colon P \to S$ there is a morphism $f\colon P \to Q$ such that $g = v \circ f$. Thus, the morphism $\mathrm{Hom}(P, Q) \to \mathrm{Hom}(P, S)$ is surjective.

Let the functor $\mathcal{H}om(P, \cdot)$ be exact. Then for every epimorphism $v\colon Q \to S$ and a morphism $g\colon P \to S$ there is a morphism $f\colon P \to Q$ such that $g = v \circ f$. Hence by the propostion P is projective.

3.2.11. Remarks.

1) Projective modules over PID are free.

2) Projective modules over local rings are free.

3.3. Injective objects

3.3.1. Definition. An object J is called injective if it is a projective object in $\mathcal{Q}^{op}$. In other words, for every two objects R, Q, a morphism $\beta: R \to J$ and an monomorphism $\alpha: R \to Q$

$$\begin{array}{ccccc} 0 & \longrightarrow & R & \xrightarrow{\alpha} & Q \\ & & {\scriptstyle\beta}\big\downarrow & & \\ & & J & & \end{array}$$

there is a morphism $\gamma: Q \to J$ such that

$$\beta = \gamma \circ \alpha.$$

Note that there is not characterization of injective objects in terms of free objects.

3.3.2. Here are properties of injective objects similar to those of projective.

1) The product of objects is injective iff each object is injective.

2) If J is injective, then for every three objects S, R, Q and a diagram

$$\begin{array}{ccccc} Q & \xrightarrow{\delta} & R & \xrightarrow{\alpha} & S \\ & & {\scriptstyle\beta}\big\downarrow & & \\ & & J & & \end{array}$$

with exact row and $\beta \circ \delta = 0$ there is a morphism $\varepsilon: S \to J$ such that $\beta = \varepsilon \circ \alpha$.

3) J is injective iff the functor $\mathcal{H}om(\cdot, J): \mathcal{Q} \to \mathcal{Q}$ is exact.

4) J is injective $\Rightarrow$ every short exact sequence

$$0 \longrightarrow J \longrightarrow Q \longrightarrow R \longrightarrow 0$$

splits.

3.3.3. For every object Q there is an injective object J and a monomorphism $Q \to J$. The proof is a little tricky and is omitted.

Using this result one can replace $\Rightarrow$ in 4) by $\Leftrightarrow$.

3.3.4. Definition. An A-module Q is called divisible if for every $q \in Q$ and $a \in A$ which isn't a zero divisor there is $q' \in Q$ such that $q = aq'$.

For example, $\mathbb{Q}$ is a divisible $\mathbb{Z}$-modules.

One can prove that 1) $\mathbb{Z}$-module Q is injective iff Q is divisible and 2) if Q is an A-module, then the A-module $\mathrm{Hom}_{\mathbb{Z}}(A, Q)$ of all additive homomorphisms from A to Q is a divisible A-module.

3.4. Projective and injective resolutions

3.4.1 Lemma. *Every object Q of $\mathcal{Q}$ possesses a projective resolution, i.e. there is an exact sequence*

$$\ldots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \ldots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow Q \longrightarrow 0$$

in which P_i are projective objects of $\mathcal{Q}$.

Proof. By 3.1.5 there is an exact sequence

$$0 \longrightarrow K_0 \longrightarrow P_0 \longrightarrow Q \longrightarrow 0$$

in which P_0 is a projective object (even free). For K_0 there is an exact sequence

$$0 \longrightarrow K_1 \longrightarrow P_1 \longrightarrow K_0 \longrightarrow 0$$

in which P_1 is a projective object. Similarly define K_n, P_n, so we get an exact sequence

$$0 \longrightarrow K_n \longrightarrow P_n \longrightarrow K_{n-1} \longrightarrow 0.$$

Define $f_n: P_n \to P_{n-1}$ as the composition of $P_n \longrightarrow K_{n-1} \longrightarrow P_{n-1}$. Then $\ker(f_n)$ coincides with the kernel of $P_n \longrightarrow K_{n-1}$ which is equal to K_n and $\mathrm{im}(f_{n+1})$ coincides with the image of $K_n \longrightarrow P_n$ which is equal to K_n, so $\ker(f_n) = \mathrm{im}(f_{n+1})$.

3.4.2. Lemma. *Let $f: Q \to Q'$ be a morphism in $\mathcal{Q}$ and let*

$$\begin{gathered} \ldots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \ldots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow Q \longrightarrow 0 \\ \ldots \longrightarrow P'_n \longrightarrow P'_{n-1} \longrightarrow \ldots \longrightarrow P'_1 \longrightarrow P'_0 \longrightarrow Q' \longrightarrow 0 \end{gathered}$$

be projective resolutions of Q and Q'. Then there are morphism $f_n: P_n \to P'_n$ such that the diagram

$$\begin{tikzcd} \ldots \arrow[r] & P_1 \arrow[r] \arrow[d, "f_1"'] & P_0 \arrow[r] \arrow[d, "f_0"'] & Q \arrow[r] \arrow[d, "f"'] & 0 \\ \ldots \arrow[r] & P'_1 \arrow[r] & P'_0 \arrow[r] & Q' \arrow[r] & 0 \end{tikzcd}$$

is commutative.

Proof. The morphism f_0 exists since P_0 is projective. The composition of the morphism $P_1 \to P_0 \to P'_0$ and the morphism $P'_0 \to Q'$ is zero, so by 3.2.7 there is a morphism $f_1: P_1 \to P'_1$ such that the composition of it with $P'_1 \to P'_0$ coincides with $P_1 \to P_0 \to P'_0$. Similarly one constructs morphisms f_n.

3.4.3. Lemma. *Let*

$$0 \longrightarrow R \longrightarrow Q \longrightarrow S \longrightarrow 0$$

be an exact sequence and let

$$\begin{gathered} \ldots \longrightarrow P'_1 \longrightarrow P'_0 \longrightarrow R \longrightarrow 0 \\ \ldots \longrightarrow P''_1 \longrightarrow P''_0 \longrightarrow S \longrightarrow 0 \end{gathered}$$

be projective resolutions. Denote $P_n = P'_n \oplus P''_n$ and let $i'_n: P'_n \to P_n$, $\pi''_n: P_n \to P''_n$ be morphisms associated to P_n as a product and coproduct of P'_n and P''_n.

Then there are morphisms α_i such that P_n form a projective resolution of Q and there is a *commutative diagram*

$$
\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\dots \arrow[r] & P_1' \arrow[r] \arrow[d, "i_1'"'] & P_0' \arrow[r, "\alpha_0'"] \arrow[d, "i_0'"'] & R \arrow[r] \arrow[d] & 0 \\
\dots \arrow[r] & P_1 \arrow[r, "\alpha_1"] \arrow[d, "\pi_1''"'] & P_0 \arrow[r, "\alpha_0"] \arrow[d, "\pi_0''"'] & Q \arrow[r] \arrow[d] & 0 \\
\dots \arrow[r] & P_1'' \arrow[r] \arrow[d] & P_0'' \arrow[r, "\alpha_0''"] \arrow[d] & S \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}
$$

Proof. Since P_0'' is projective, there is a morphism $w_0\colon P_0'' \to Q$ whose composition with $Q \longrightarrow S$ is equal to $P_0'' \longrightarrow S$. Due to the definition of the coproduct for the morphisms $P_0'' \longrightarrow Q$ and $v_0\colon P_0' \longrightarrow R \longrightarrow Q$ there is a morphism $\alpha_0\colon P_0 \to Q$ such that $\alpha_0 \circ i_0' = v_0$ and $w_0 \circ \pi_0'' = \alpha_0$. Therefore two left squares of the diagram are commutative.

For the Snake Lemma applied to the commutative diagram

$$
\begin{tikzcd}
0 \arrow[r] & P_0' \arrow[r, "i_0'"] \arrow[d, "\alpha_0'"'] & P_0 \arrow[r, "\pi_0'"] \arrow[d, "\alpha_0"'] & P_0'' \arrow[r] \arrow[d, "\alpha_0''"'] & 0 \\
0 \arrow[r] & R \arrow[r] & Q \arrow[r] & S \arrow[r] & 0
\end{tikzcd}
$$

with exact rows we get an exact sequence

$$0 \longrightarrow \ker(\alpha_0') \longrightarrow \ker(\alpha_0) \longrightarrow \ker(\alpha_0'') \longrightarrow \operatorname{coker}(\alpha_0') \longrightarrow \operatorname{coker}(\alpha_0) \longrightarrow \operatorname{coker}(\alpha_0'').$$

Since α_0' and α_0'' are surjective, we deduce that α_0 is surjective.

Consider the diagram

$$
\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & \\
P_1' \arrow[r] \arrow[d, "i_1'"'] & \ker(\alpha_0') \arrow[r] \arrow[d] & 0 \\
P_1 \arrow[d, "\pi_1''"'] & \ker(\alpha_0) \arrow[r] \arrow[d] & 0 \\
P_1'' \arrow[r] \arrow[d] & \ker(\alpha_0'') \arrow[r] \arrow[d] & 0 \\
0 & 0 &
\end{tikzcd}
$$

and define similarly a morphism $P_1 \to \ker(\alpha_0)$ which gives a morphism $\alpha_1\colon P_1 \to P_0$. Define further α_n by induction.

3.4.4. Similarly one can show that every object Q of $\mathcal{Q}$ possesses an injective resolution, i.e. there is an exact sequence

$$0 \longrightarrow Q \longrightarrow J_0 \longrightarrow J_1 \longrightarrow \dots \longrightarrow J_{n-1} \longrightarrow J_n \longrightarrow \dots$$

in which J_i are injective objects of $\mathcal{Q}$.

3.5. Left and right derived functors. Functors Ext and Tor

3.5.1. Definition. Let $\mathcal{F}\colon \mathcal{Q} \to \mathcal{Q}$ be a functor. For an object Q of $\mathcal{Q}$ let

$$\dots \longrightarrow P_n \xrightarrow{v_n} P_{n-1} \longrightarrow \dots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow Q \longrightarrow 0$$

be its projective resolution. Let d_0 be the zero morphism from $\mathcal{F}(P_0)$ to 0. Let $d_n = \mathcal{F}(v_n)$ for $n > 0$. Then

$$\mathbf{C}_Q \quad \dots \longrightarrow \mathcal{F}(P_n) \xrightarrow{d_n} \mathcal{F}(P_{n-1}) \longrightarrow \dots \longrightarrow \mathcal{F}(P_1) \xrightarrow{d_1} \mathcal{F}(P_0) \xrightarrow{d_0} 0$$

is a chain complex. Put

$$(L_n\mathcal{F})(Q) = H_n(\mathbf{C}_Q).$$

For a morphism $f\colon Q \to Q'$ consider their projective resolutions and the commutative diagram

$$\begin{tikzcd}
\dots \arrow[r] & P_1 \arrow[r] \arrow[d, "f_1"'] & P_0 \arrow[r] \arrow[d, "f_0"'] & Q \arrow[r] \arrow[d, "f"'] & 0 \\
\dots \arrow[r] & P_1' \arrow[r] & P_0' \arrow[r] & Q' \arrow[r] & 0
\end{tikzcd}$$

which exists by 3.4.2. Then we get a commutative diagram

$$\begin{tikzcd}
\dots \arrow[r] & \mathcal{F}(P_1) \arrow[r] \arrow[d, "\mathcal{F}(f_1)"'] & \mathcal{F}(P_0) \arrow[r] \arrow[d, "\mathcal{F}(f_0)"'] & 0 \\
\dots \arrow[r] & \mathcal{F}(P_1') \arrow[r] & \mathcal{F}(P_0') \arrow[r] & 0
\end{tikzcd}$$

Define $(L_n\mathcal{F})(f)\colon (L_n\mathcal{F})(Q) \to (L_n\mathcal{F})(Q')$ as $H_n(\mathbf{C}_Q) \to H_n(\mathbf{C}_{Q'})$ which is induced by the morphism of complexes $(\mathcal{F}(f_n))\colon \mathbf{C}_Q \to \mathbf{C}_{Q'}$ where the latter chain complex is associated to the the projective resolution of Q'.

Thus defined functor $L_n\mathcal{F}\colon \mathcal{Q} \to \mathcal{Q}$ is called the nth left derived functor of $\mathcal{F}$.

For example, $L_0\mathcal{F}(Q) = H_0(\mathbf{C}_Q)$ is the cokernel of d_1 which is $= \mathcal{F}(P_0)/d_1(\mathcal{F}(P_1))$.

Similarly one defines the nth right derived (contravariant) functor $R^n\mathcal{F}\colon \mathcal{Q} \to \mathcal{Q}$ of a (covariant) functor $\mathcal{F}$ using injective resolutions and cohomologies instead. For example, $R^0\mathcal{F}(Q) = H^0(\mathbf{C}_Q)$ is the kernel of $d^0\colon \mathcal{F}(J_0) \to \mathcal{F}(J_1)$.

Similarly one defines derived functors of contravariant functors.

3.5.2. We prove correctness of the definition of $L_n\mathcal{F}$, namely that $(L_n\mathcal{F})(Q)$ doesn't depend on the choice of a projective resolution and $(L_n\mathcal{F})(f)$ doesn't depend on the choice of (f_n) given by Lemma 3.4.2.

By Lemma 3.4.2 for projective resolutions

$$\mathbf{C} \quad \dots \longrightarrow P_n \xrightarrow{\alpha_n} P_{n-1} \longrightarrow \dots \longrightarrow P_1 \xrightarrow{\alpha_1} P_0 \xrightarrow{\alpha_0} Q \longrightarrow 0,$$

$$\mathbf{C}' \quad \dots \longrightarrow P_n' \xrightarrow{\alpha_n'} P_{n-1}' \longrightarrow \dots \longrightarrow P_1' \xrightarrow{\alpha_1'} P_0' \xrightarrow{\alpha_0'} Q' \longrightarrow 0$$

and a morphism $f\colon Q \to Q'$ in $\mathcal{Q}$ there is a commutative diagram

$$\begin{array}{ccccccccc}
\dots & \longrightarrow & P_1 & \xrightarrow{\alpha_1} & P_0 & \xrightarrow{\alpha_0} & Q & \longrightarrow & 0 \\
& & {\scriptstyle f_1}\Big\downarrow & & {\scriptstyle f_0}\Big\downarrow & & {\scriptstyle f}\Big\downarrow & & \\
\dots & \longrightarrow & P_1' & \xrightarrow{\alpha_1'} & P_0' & \xrightarrow{\alpha_0'} & Q' & \longrightarrow & 0
\end{array}$$

with morphisms $f_n\colon P_n \to P_n'$. Suppose that morphisms $g_n\colon P_n \to P_n'$, $n \geq 0$ satisfy the same property of Lemma 3.4.2.

Denote $P_{-1} = Q$, $P_{-2} = 0$, $P_{-1}' = Q'$. Put $\alpha_{-1} = 0$, $g_{-1} = f_{-1} = f$.

We claim that then there are morphisms $s_n\colon P_n \to P_{n+1}'$, $n \geq -2$ such that

$$g_n - f_n = \alpha_{n+1}' \circ s_n + s_{n-1} \circ \alpha_n, \quad n \geq -1.$$

Indeed, define $s_{-2} = 0, s_{-1} = 0$. For inductive step assume that $g_n - f_n = \alpha_{n+1}' \circ s_n + s_{n-1} \circ \alpha_n$. Calculate the composition of $h = g_{n+1} - f_{n+1} - s_n \circ \alpha_{n+1}$ and α_{n+1}' using the expression for $\alpha_{n+1}' \circ s_n$ given by the induction assumption:

$$\begin{aligned}
\alpha_{n+1}' \circ h &= \alpha_{n+1}' \circ (g_{n+1} - f_{n+1}) - (g_n - f_n - s_{n-1} \circ \alpha_n) \circ \alpha_{n+1} \\
&= \alpha_{n+1}' \circ (g_{n+1} - f_{n+1}) - (g_n - f_n) \circ \alpha_{n+1} = 0.
\end{aligned}$$

Now 3.2.7 implies that there is a morphism $s_{n+1}\colon P_{n+1} \to P_{n+2}'$ such that $\alpha_{n+2}' \circ s_{n+1} = h = g_{n+1} - f_{n+1} - s_n \circ \alpha_{n+1}$, so $g_{n+1} - f_{n+1} = \alpha_{n+2}' \circ s_{n+1} + s_n \circ \alpha_{n+1}$.

Now put $d_n = \mathcal{F}(\alpha_n)$, $d_n' = \mathcal{F}(\alpha_n')$ for $n > 0$ and $d_0 = d_0' = 0$; $r_n = \mathcal{F}(s_n)$ for $n \geq 0$. Let $r_{-1} = 0$. Then

$$\mathcal{F}(g_n) - \mathcal{F}(f_n) = d_{n+1}' \circ r_n + r_{n-1} \circ d_n \quad \text{for } n \geq 0.$$

If x is an n-cycle of $\mathbf{C}$ (i.e. $x \in \ker(d_n)$), then the difference

$$\mathcal{F}(g_n)(x) - \mathcal{F}(f_n)(x) = d_{n+1}' \circ r_n(x) + r_{n-1} \circ d_n(x) = d_{n+1}' \circ r_n(x)$$

belongs to the image of d_{n+1}', i.e. it is an n-boundary in $\mathbf{C}'$. Thus, the morphism $H_n(\mathbf{C}) \to H_n(\mathbf{C}')$ induced by f_n coincides with the morphism induced by g_n.

This shows that $(L_n\mathcal{F})(f)$ is well defined.

If

$$\begin{array}{ll}
\mathbf{C} & \dots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \dots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow Q \longrightarrow 0, \\
\mathbf{C}' & \dots \longrightarrow P_n' \longrightarrow P_{n-1}' \longrightarrow \dots \longrightarrow P_1' \longrightarrow P_0' \longrightarrow Q \longrightarrow 0
\end{array}$$

are two projective resolutions of Q, then by the previous results we have morphisms $H_n(\mathbf{C}) \to H_n(\mathbf{C}')$ and $H_n(\mathbf{C}') \to H_n(\mathbf{C})$ both induced by the identity morphism of Q. The composition $H_n(\mathbf{C}) \to H_n(\mathbf{C}') \to H_n(\mathbf{C})$ should coincide with the identity morphism $H_n(\mathbf{C}) \to H_n(\mathbf{C})$ due to the previous arguments. Similarly the composition $H_n(\mathbf{C}') \to H_n(\mathbf{C}) \to H_n(\mathbf{C}')$ should coincide with the identity morphism of $H_n(\mathbf{C}')$. Hence $H_n(\mathbf{C})$ is isomorphic to $H_n(\mathbf{C}')$. Thus, $L_n\mathcal{F}(Q)$ doesn't depend on the choice of a projective resolution of Q.

3.5.3. Two important examples.

1) If $\mathcal{F}$ is the functor $\mathcal{H}om(T,\cdot)$ defined in 2.5.5, the nth right derived functor R^n of the functor $\mathcal{H}om(T,\cdot)$ defined in 2.5.5 is called the nth Ext-functor and denoted by $\mathrm{Ext}^n(T,\cdot)$ or, to specify the ring A, by $\mathrm{Ext}^n_A(T,\cdot)$.

By 3.2.9 the covariant functor $\mathcal{H}om(T,\cdot)$ is left exact, so if

$$0 \longrightarrow Q \longrightarrow J_0 \longrightarrow J_1 \longrightarrow \dots$$

is an injective resolution, then the sequence

$$0 \longrightarrow \mathrm{Hom}(T, Q) \longrightarrow \mathrm{Hom}(T, J_0) \longrightarrow \mathrm{Hom}(T, J_1) \longrightarrow \dots$$

is exact and thus $H^0(\mathbf{C}_Q)$ which is equal to the kernel of

$$d^0 \colon \mathcal{F}(J_0) = \mathrm{Hom}(T, J_0) \to \mathrm{Hom}(T, J_1) = \mathcal{F}(J_1)$$

is isomorphic to $\mathrm{Hom}(T, Q)$. Thus,

$$\mathrm{Ext}^0(T, Q) \simeq \mathrm{Hom}(T, Q).$$

The nth right derived fuctor R^n of the (contravariant) functor $\mathcal{H}om(\cdot, T)$ gives nothing new: using double cochain complexes one can prove that

$$R^n \mathcal{H}om(T, \cdot)(Q) = R^n \mathcal{H}om(\cdot, Q)(T).$$

2) For an object T define a functor $(T\otimes, \cdot) \colon mod - A \to mod - A$ by $Q \to T \otimes Q$ and for a morphism $f \colon Q \to R$ put $(T\otimes, \cdot)(f) \colon T \otimes Q \to T \otimes R$ as the module homomorphism induced by f. The nth left derived functor L_n of $(T\otimes, \cdot)$ is called the nth Tor-functor and denoted $\mathrm{Tor}_n(T, \cdot)$ or $\mathrm{Tor}_n^A(T, \cdot)$ One can check that $\mathrm{Tor}_0(T, Q) = T \otimes Q$ and

$$L_n(T\otimes, \cdot)(Q) \simeq L_n(\cdot, \otimes Q)(T).$$

3.5.4. Theorem. *Let*

$$0 \longrightarrow T \longrightarrow Q \longrightarrow S \longrightarrow 0$$

be a short exact sequence. Let $\mathcal{F} \colon \mathcal{Q} \to \mathcal{Q}$ be an additive functor, which means that it transforms the sum of morphisms into the sum of the images. Then there are long exact sequences

$$\begin{gathered} \dots \longrightarrow L_n\mathcal{F}(T) \longrightarrow L_n\mathcal{F}(Q) \longrightarrow L_n\mathcal{F}(S) \longrightarrow L_{n-1}\mathcal{F}(T) \longrightarrow L_{n-1}\mathcal{F}(Q) \\ \longrightarrow L_{n-1}\mathcal{F}(S) \longrightarrow \dots \longrightarrow L_0\mathcal{F}(T) \longrightarrow L_0\mathcal{F}(Q) \longrightarrow L_0\mathcal{F}(S) \end{gathered}$$

and

$$\begin{gathered} R^0\mathcal{F}(T) \longrightarrow R^0\mathcal{F}(Q) \longrightarrow R^0\mathcal{F}(S) \longrightarrow R^1\mathcal{F}(T) \longrightarrow R^1\mathcal{F}(Q) \\ \longrightarrow R^1\mathcal{F}(S) \longrightarrow \dots \longrightarrow R^n\mathcal{F}(T) \longrightarrow R^n\mathcal{F}(Q) \longrightarrow R^n\mathcal{F}(S) \longrightarrow \dots \end{gathered}$$

Proof. By Lemma 3.4.3 there are projective resolutions

$$\begin{gathered} \dots \longrightarrow P_1' \longrightarrow P_0' \longrightarrow T \longrightarrow 0, \\ \dots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow Q \longrightarrow 0, \\ \dots \longrightarrow P_1'' \longrightarrow P_0'' \longrightarrow S \longrightarrow 0 \end{gathered}$$

which form a commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & P_1' & \longrightarrow & P_0' & \longrightarrow & T & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & Q & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & P_1'' & \longrightarrow & P_0'' & \longrightarrow & S & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

By 2.5.6 and 3.2.7 we know that the sequence

$$0 \longrightarrow \mathcal{F}(P_n') \to \mathcal{F}(P_n) \longrightarrow \mathcal{F}(P_n'') \longrightarrow 0$$

is exact.

The diagram

$$\begin{array}{cccccccc}
 & & & 0 & & 0 & & \\
 & & & \downarrow & & \downarrow & & \\
\mathbf{A} & \dots & \longrightarrow & \mathcal{F}(P_1') & \longrightarrow & \mathcal{F}(P_0') & \longrightarrow & 0 \\
 & & & \downarrow & & \downarrow & & \\
\mathbf{B} & \dots & \longrightarrow & \mathcal{F}(P_1) & \longrightarrow & \mathcal{F}(P_0) & \longrightarrow & 0 \\
 & & & \downarrow & & \downarrow & & \\
\mathbf{C} & \dots & \longrightarrow & \mathcal{F}(P_1'') & \longrightarrow & \mathcal{F}(P_0'') & \longrightarrow & 0 \\
 & & & \downarrow & & \downarrow & & \\
 & & & 0 & & 0 & &
\end{array}$$

is commutative and every column is exact, so the sequence of complexes

$$0 \longrightarrow \mathbf{A} \longrightarrow \mathbf{B} \longrightarrow \mathbf{C} \longrightarrow 0$$

is exact.

By Theorem 2.7.3 we get now the first long sequence of this theorem.

3.5.5. Examples.

1) For an exact sequence $0 \longrightarrow R \longrightarrow Q \longrightarrow S \longrightarrow 0$ the sequences

$$0 \to \mathrm{Hom}(T, R) \to \mathrm{Hom}(T, Q) \to \mathrm{Hom}(T, S) \to \mathrm{Ext}^1(T, R) \to \mathrm{Ext}^1(T, Q) \to \dots$$

and

$$0 \to \mathrm{Hom}(R, T) \to \mathrm{Hom}(Q, T) \to \mathrm{Hom}(S, T) \to \mathrm{Ext}^1(R, T) \to \mathrm{Ext}^1(Q, T) \to \dots$$

are exact (the exactness in the first term follows from left exactness of $\mathcal{H}om(T, \cdot)$ and $\mathcal{H}om(\cdot, T)$).

So Ext^1 measures how far $\mathcal{H}om(\cdot, T)$ is from an exact functor.

From 3.2.10 we deduce that T is projective iff $\mathrm{Ext}^1(T, R) = 0$ for all objects R.

2) For an exact sequence $0 \longrightarrow R \longrightarrow Q \longrightarrow S \longrightarrow 0$ the sequence

$$\ldots \longrightarrow \mathrm{Tor}_1(T,R) \longrightarrow \mathrm{Tor}_1(T,Q) \longrightarrow \mathrm{Tor}_1(T,S) \to T \otimes R \longrightarrow T \otimes Q \longrightarrow t \otimes S \to 0$$

is exact (the exactness in the last term follows from right exactness of $(T\otimes, \cdot)$).

So Tor_1 measures how far $(T\otimes, \cdot)$ is from an exact functor.

4. Group cohomologies

4.1. Category $fGr-mod$

4.1.1. Let G be a finite group. The group ring $\mathbb{Z}[G]$ by definition consists of $\sum_{g\in G} a_g g$ with $a_g \in \mathbb{Z}$ with operations

$$\sum a_g g + \sum b_g g = \sum (a_g + b_g) g, \quad (\sum a_g g)(\sum b_g g) = \sum a_g b_{g'} g g' = \sum c_g g$$

where $c_g = \sum_h a_h b_{h^{-1}g}$.

An abelian group A is called a G-module if A is a left $\mathbb{Z}[G]$-module. It means there is an operation $G \times A \to A$, $(g,a) \to ga$ such that $g(a+b) = ga + gb$, $(gh)a = g(ha)$.

A morphism $f\colon A \to B$ of $\mathbb{Z}[G]$-modules is called a morphism of G-modules.

An abelian group A is called a trivial G-module if $ga = a$ for every $a \in A$. For example, $\mathbb{Z}$ is a trivial G-module.

4.1.2. Define a category $fGr-mod$ whose objects are couples (G,A) where A is a G-module, G is a finite group and whose morphisms are couples $(\varphi,\psi)\colon (G,A) \to (G',A')$ where $\varphi\colon G' \to G$ and $\psi\colon A \to A'$ are group homomorphisms and $\psi(\varphi(g)a) = g\psi(a)$ for all $a \in A, g \in G'$.

In particular, if H is a subgroup of G we have a morphism called restriction

$$\mathrm{res} = (\mathrm{inc}, \mathrm{id})\colon (G,A) \to (H,A)$$

where $\mathrm{inc}\colon H \to G$ is the inclusion of groups.

If $f\colon A \to B$ is a homomorphism of G-modules, we have a morphism $(\mathrm{id}, f)\colon (G,A) \to (G,B)$ in $fGr-mod$.

4.2. Complexes $\mathbf{D}(G,A)$ and $\mathbf{C}(G,A)$

4.2.1. For a G-module A and $n \geq 0$ define abelian groups

$$D^n(G,A) = \{\text{maps } \alpha\colon \underbrace{G \times \cdots \times G}_{n+1 \text{ times}} \to A$$
$$\text{such that } \alpha(gg_0,\dots,gg_{n+1}) = g\alpha(g_0,\dots,g_{n+1}) \text{ for all } g \in G\}.$$

The addition is given by the sum of maps.

Note that there is an isomorphism of abelian groups $u^0\colon D^0(G,A) \to A$ given by $\alpha \to \alpha(1)$. The inverse isomorphism $v^0\colon A \to D^0(G,A)$ is given by $a \to \alpha$, $\alpha(g) = ga$.

Define $d^n = d^n_{\mathcal{D}}\colon D^n(G,A) \to D^{n+1}(G,A)$ for $n \geq 0$ by

$$d^n(\alpha)(g_0,\dots,g_{n+1}) = \sum_{i=0}^{n+1} (-1)^i \alpha(g_0,\dots,\hat{g}_i,\dots,g_{n+1})$$

where $\hat{g}_i$ means g_i is excluded. Then indeed

$$(d^n\alpha)(gg_0,\dots,gg_{n+1}) = g(d^n\alpha)(g_0,\dots,g_{n+1}).$$

We get $d^n \circ d^{n-1} = 0$ for $n \geq 1$, since

$$(d^n \circ d^{n-1}(\alpha))(g_0, \dots, g_{n+1}) \\ = \sum_{0 \leq i < j \leq n+1} ((-1)^{i+j} + (-1)^{i+j-1})\alpha(g_0, \dots, \hat{g}_i, \dots, \hat{g}_j, \dots, g_{n+1}) = 0.$$

We get a cochain complex

$$0 \longrightarrow D^0(G,A) \xrightarrow{d^0} D^1(G,A) \xrightarrow{d^1} D^1(G,A) \longrightarrow \dots \longrightarrow D^n(G,A) \xrightarrow{d^n} D^{n+1}(G,A) \longrightarrow \dots$$

which we denote by $\mathbf{D}(G,A)$.

4.2.2. Definition. The nth cohomology group $H^n(G,A)$ of the G-module A is $H^n(\mathbf{D}(G,A))$.

4.2.3. For a G-module A and $n > 0$ define abelian groups

$$C^n(G,A) = \{\text{maps } \beta: \underbrace{G \times \dots \times G}_{n \text{ times}} \to A\}.$$

Put $C^0(G,A) = A$.

Define $u^n: D^n(G,A) \to C^n(G,A)$ for $n > 0$ by $u^n(\alpha) = \beta$ where

$$\beta(g_1, \dots, g_n) = \alpha(1, g_1, g_1 g_2, \dots, g_1 g_2 \dots g_n).$$

Define $v^n: C^n(G,A) \to D^n(G,A)$ by $v^n(\beta) = \alpha$ where

$$\alpha(g_0, \dots, g_n) = g_0 \beta(g_0^{-1} g_1, g_1^{-1} g_2, \dots, g_{n-1}^{-1} g_n).$$

Note that indeed $g\alpha(g_0, \dots, g_n) = \alpha(gg_0, \dots, gg_n)$ since
$gg_0\beta(g_0^{-1}g_1, \dots, g_{n-1}^{-1}g_n) = gg_0\beta((gg_0)^{-1}(gg_1), \dots, (gg_{n-1})^{-1}gg_n)$.

Then $u^n \circ v^n$ and $v^n \circ u^n$ are identity maps for $n > 1$:

$$u^n \circ v^n(\beta)(g_1, \dots, g_n) = v^n(\beta)(1, g_1, g_1 g_2, \dots, g_1 \dots g_n) = 1\beta(g_1, \dots, g_n) = \beta(g_1, \dots, g_n),$$

and $v^n \circ u^n(\alpha)(g_0, \dots, g_n) = g_0 u^n(\alpha)(g_0^{-1}g_1, \dots, g_{n-1}^{-1}g_n) = g_0\alpha(1, g_0^{-1}g_1, \dots, g_0^{-1}g_n)$
$= \alpha(g_0, \dots, g_n)$.

Thus, $C^n(G,A)$ is isomorphic to $D^n(G,A)$ for $n \geq 0$ (use u^0, v^0 from 4.2.1).

Define $d^n_{\mathcal{C}}: C^n(G,A) \to C^{n+1}(G,A)$ as the composition $u^{n+1} \circ d^n_{\mathcal{D}} \circ v^n$, then

$$0 \longrightarrow C^0(G,A) \xrightarrow{d^0_{\mathcal{C}}} C^1(G,A) \longrightarrow \dots \longrightarrow C^n(G,A) \xrightarrow{d^n_{\mathcal{C}}} C^{n+1}(G,A) \longrightarrow \dots$$

is a cochain complex $\mathbf{C}(G,A)$ isomorphic to the complex $\mathbf{D}(G,A)$ and so

$$H^n(G,A) = H^n(\mathbf{C}(G,A)).$$

Explicitly, $d^0_{\mathcal{C}}(a)(g) = ga - a$ for all $g \in G$ and for $n \geq 1$

$$d^n_{\mathcal{C}}(\beta)(g_1, \dots, g_{n+1}) \\ = g_1\beta(g_2, \dots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i \beta(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) + (-1)^{n+1}\beta(g_1, \dots, g_n)$$

and $d^n_{\mathcal{C}} = 0$ for $n < 0$. Indeed,

$$d^0_{\mathcal{C}}\alpha(1, g_1) = \alpha(g_1) - \alpha(1) = g_1\alpha(1) - \alpha(1)$$

and

$$
\begin{aligned}
& d^n\alpha(1, g_1, g_1g_2, \ldots, g_1\ldots g_{n+1}) = \alpha(g_1, g_1g_2, \ldots, g_1\ldots g_{n+1}) \\
& + \sum_{i=1}^{n}(-1)^i \alpha(1, g_1, \ldots, g_1\ldots g_{i-1}, g_1\ldots g_i g_{i+1}, \ldots, g_1\ldots g_{n+1}) \\
& + (-1)^{n+1}\alpha(1, g_1, \ldots, g_1\ldots g_n).
\end{aligned}
$$

4.2.4. A morphism $(\varphi, \psi) \colon (G, A) \to (G', A')$ in $fGr - mod$ induces a morphism $\mathbf{D}(G, A) \to \mathbf{D}(G', A')$ and hence a morphism $H^n(G, A) \to H^n(G', A')$. In particular, a morphism of G-modules $f \colon A \to B$ induces a morphism $\tilde{f} \colon \mathbf{D}(G, A) \to \mathbf{D}(G, B)$, $\alpha \in D^n(G, A) \to f \circ \alpha \in D^n(G, B)$.

4.3. Small cohomology groups

4.3.1. $H^0(G, A) = \ker d^0$ consists of maps $\alpha \colon G \to A$ such that $\alpha(g_0) = \alpha(g_1)$ for all $g_0, g_1 \in G$ and $g\alpha(g_1) = \alpha(gg_1)$. So $\alpha(g_1) = a \in A$ for all $g_1 \in G$ and $ga = a$ for all $g \in G$, i.e. a belongs to the subgroup A^G of A consisting of fixed elements under the action of G. Thus, $H^0(G, A) = A^G$.

4.3.2. $H^1(G, A)$ coincides with $\ker(d^1_C)/\operatorname{im}(d^0_C)$. The "numerator" consists of maps $\beta \colon G \to A$ such that $g_1\beta(g_2) - \beta(g_1g_2) + \beta(g_1) = 0$, i.e.

$$\beta(g_1g_2) = g_1\beta(g_2) + \beta(g_1),$$

such β are called crossed homomorphisms (1-cocycles). If G acts trivially on A, then cross homomorphisms are just homomorphisms. The "denominator" consists of maps $\beta \colon G \to A$ such that for some $a \in A$

$$\beta(g) = ga - a \quad \text{for all } g \in G$$

called principal crossed homomorphisms (1-coborders). Thus $H^1(G, A)$ measures "how many" crossed homomorphisms are not principal.

4.4. Long sequence of cohomology groups

4.4.1. Let

$$0 \longrightarrow A \xrightarrow{k} B \xrightarrow{l} C \longrightarrow 0$$

be a short exact sequence of G-modules. Then the sequence of complexes

$$0 \longrightarrow \mathbf{C}(G, A) \xrightarrow{\tilde{k}} \mathbf{C}(G, B) \xrightarrow{\tilde{l}} \mathbf{C}(G, C) \longrightarrow 0$$

is exact. So by the theorem 2.7.3 we get a long exact sequence of groups

$$\ldots \xrightarrow{\delta^{n-1}} H^n(G, A) \xrightarrow{k^n} H^n(G, B) \xrightarrow{l^n} H^n(G, C) \xrightarrow{\delta^n} H^{n+1}(G, A) \longrightarrow \ldots$$

the first terms of which are

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) \longrightarrow \ldots$$

(exactness at A^G follows from injectivity of $A \to B$).

4.4.2. Consider the functor $\mathcal{F}^G\colon \mathbb{Z}[G]{-}mod \to \mathbb{Z}[G]{-}mod$: $\mathcal{F}^G(A) = A^G$, $\mathcal{F}^G(f) = f\colon A^G \to B^G$ for $f\colon A \to B$.

If $0 \longrightarrow A \longrightarrow J_0 \longrightarrow J_1 \longrightarrow \dots$ is an injective resolution of A, then the sequence $0 \longrightarrow A^G \longrightarrow J_0^G \leq J_1^G$ is exact, so from 3.5 we deduce that $\mathcal{F}^G = R^0(\mathcal{F}^G)$. Now from 4.4.1 one can deduce that $H^n(G,\cdot)$ is the nth right derived functor of the functor $\mathcal{F}^G$.

Remark. Using the properties of $\mathrm{Ext}^n(Q,T)$ from 3.5.3 and 3.5.5 and the equality

$$\mathrm{Ext}^0_{\mathbb{Z}[G]}(\mathbb{Z}, A) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) = A^G = H^0(G, A)$$

one can show that

$$H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

The nth homology group $H_n(G, A)$ of the G-module A is defined as $\mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A)$.

4.4.3. If

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0, \quad 0 \longrightarrow A' \longrightarrow B' \longrightarrow C' \longrightarrow 0$$

are exact sequences, then from 2.7.4 we deduce that the diagram

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & \longrightarrow & H^1(G,A) & \longrightarrow & H^1(G,B) & \longrightarrow & \dots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A'^G & \longrightarrow & B'^G & \longrightarrow & C'^G & \longrightarrow & H^1(G,A') & \longrightarrow & H^1(G,B') & \longrightarrow & \dots
\end{array}$$

is commutative.

4.5. Cohomologies of a group and its subgroup

4.5.1. Let H be a subgroup of a finite group G. Let A be an H-module. Then the set

$$M_G^H(A) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)$$

of all H-morphisms from $\mathbb{Z}[G]$ to A, i.e. all maps $\alpha\colon G \to A$ satisfying

$$\alpha(hg) = h\alpha(g) \quad \text{for all } h \in H$$

is a G-module with respect to the action $G \times M_G^H(A) \to M_G^H(A)$: $\alpha \to g\alpha$, $(g\alpha)(g') = \alpha(g'g)$.

A morphism $f\colon A \to B$ induces a morphism $\tilde{f}\colon M_G^H(A) \to M_G^H(B)$.

4.5.2. Lemma. *Let A be an abelian group. For $\alpha \in M_G^{\{1\}}(A)$ and $h \in H$, $g \in G$ define $(l(\alpha)(g))(h) = \alpha(hg)$. Then $l(\alpha)$ belongs to $M_G^H(M_H^{\{1\}}A$ and we get a map*

$$l\colon M_G^{\{1\}}(A) \to M_G^H(M_H^{\{1\}}A).$$

Moreover, l is an isomorphism of G-modules $M_G^{\{1\}}(A)$ and $M_G^H(M_H^{\{1\}}A)$.

Proof. First, $l(\alpha)$ belongs to $M_G^H(M_H^{\{1\}}A)$, i.e. $h'(l(\alpha)(g)) = l(\alpha)(h'g)$ for $h' \in H$. Indeed, $(h'(l(\alpha)(g)))(h) = (l(\alpha)(g))(hh') = \alpha(hh'g) = (l(\alpha)(h'g))(h)$.

Furthermore, l is a homomorphism of G-modules: since $(l(g'\alpha)(g))(h) = g'\alpha(hg) = \alpha(hgg') = (l(\alpha)(gg'))(h)$, we get $l(g'\alpha)(g) = l(\alpha)(gg')$ and $l(g'\alpha) = g'l(\alpha)$ for $g' \in G$.

Now define a map

$$m\colon M_G^H(M_H^{\{1\}}A) \to M_G^{\{1\}}(A)$$

by $m(\beta)(g) = (\beta(g))(1)$ for $\beta \in M_G^H(M_H^{\{1\}}A)$, $g \in G$. Then $(m \circ l)(\alpha)(g) = (l(\alpha)(g))(1) = \alpha(g)$ and

$$(l \circ m)(\beta)(g)(h) = m(\beta)(hg) = (\beta(hg))(1) = (h\beta(g))(1) = \beta(g)(h)$$

since $\beta \in M_G^H(M_H^{\{1\}}A)$. Thus, m and l are isomorphisms of G-modules.

4.5.3. Define $c: M_G^H(A) \to A$ by the formula $c(\alpha) = \alpha(1)$. Then $c(h\alpha) = (h\alpha)(1) = \alpha(h) = h\alpha(1) = hc(\alpha)$, so according to the definition of the category $fGr - mod$ given at 4.1.2, the inclusion $H \subset G$ and the homomorphism c induce a map $(G, M_G^H(A)) \to (H, A)$ in the category $fGr - mod$. So we get a homomorphism $H^n(G, M_G^H(A)) \to H^n(H, A)$.

4.5.4. Lemma. *Let $0 \longrightarrow A \xrightarrow{\mu} B \xrightarrow{\rho} C \longrightarrow 0$ be an exact sequence of H-modules, then*

$$0 \to M_G^H(A) \xrightarrow{\tilde{\mu}} M_G^H(B) \xrightarrow{\tilde{\rho}} M_G^H(C) \to 0$$

is an exact sequence of G-modules.

Proof. We get a sequence of G-modules

$$0 \longrightarrow M_G^H(A) \xrightarrow{\tilde{\mu}} M_G^H(B) \xrightarrow{\tilde{\rho}} M_G^H(C) \longrightarrow 0.$$

Exactness at $M_G^H(A)$ is easy to check.

Check exactness at $M_G^H(C)$. Let $\gamma \in M_G^H(C)$. Write G as a disjoint union of right cosets Hg_i. Then $\gamma(g_i) = \rho(b_i)$ for some $b_i \in B$. Define a map $\beta: G \to B$ by $hg_i \to hb_i$. Then $\beta \in M_G^H(B)$ and $\gamma = \tilde{\rho}(\beta)$.

Check exactness in the middle term. First $\tilde{\rho} \circ \tilde{\mu} = 0$. Second, if $\tilde{\rho}(\beta) = 0$, then for every $g \in G$ $\rho(\beta(g)) = 0$, so $\beta(g) = \mu(a_g)$ for a uniquely determined $a_g \in A$. Define $\alpha: G \to A$ by $g \to a_g$. Then $\alpha \in M_G^H(A)$: $\mu(h\alpha(g)) = \mu(ha_g) = h\mu(a_g) = h\mu(\alpha(g)) = h\beta(g) = \beta(hg) = \mu(\alpha(hg))$, so from injectivity of μ we deduce that $h\alpha(g) = \alpha(hg)$. Thus $\alpha \in M_G^H(A)$ and $\beta = \tilde{\mu}(\alpha)$.

4.5.5. Lemma. $H^n(G, M_G^{\{1\}}(A)) = 0$ *for* $n > 0$.

Proof. Define a map $s^n: C^n(G, M_G^{\{1\}}(A)) \to C^{n-1}(G, M_G^{\{1\}}(A))$ by

$$s^n(\alpha)(g_1, \ldots, g_{n-1})(g) = \alpha(g, g_1, \ldots, g_{n-1})(1).$$

Now

$$\begin{aligned}
&d^{n-1}s^n(\alpha)(g_1, \ldots, g_n)(g) = g_1 s^n(\alpha)(g_2, \ldots, g_n)(g) \\
&+ \sum_{i=1}^{n-1}(-1)^i s^n(\alpha)(g_1, \ldots, g_i g_{i+1}, \ldots, g_n)(g) + (-1)^n s^n(\alpha)(g_1, \ldots, g_{n-1})(g) = \\
&s^n(\alpha)(g_2, \ldots, g_n)(gg_1) + \sum_{i=1}^{n-1}(-1)^i s^n(\alpha)(g_1, \ldots, g_i g_{i+1}, \ldots, g_n)(g) \\
&+ (-1)^n s^n(\alpha)(g_1, \ldots, g_{n-1})(g) \\
&= \alpha(gg_1, g_2, \ldots, g_n)(1) + \sum_{i=1}^{n-1}(-1)^i \alpha(g, g_1, \ldots, g_i g_{i+1}, \ldots, g_n)(1) \\
&+ (-1)^n \alpha(g, g_1, \ldots, g_{n-1})(1)
\end{aligned}$$

and

$$s^{n+1}d^n(\alpha)(g_1,\dots,g_n)(g) = d^n\alpha(g,g_1,\dots,g_n)(1) = g\alpha(g_1,\dots,g_n)(1)$$
$$-\alpha(gg_1,g_2,\dots,g_n)(1) + \sum_{i=2}^{n}(-1)^i\alpha(g,\dots,g_{i-1}g_i,\dots,g_n)(1)$$
$$+(-1)^{n+1}\alpha(g,g_1,\dots,g_{n-1})(1) = \alpha(g_1,\dots,g_n)(g) - \alpha(gg_1,g_2,\dots,g_n)(1)$$
$$+\sum_{i=2}^{n}(-1)^i\alpha(g,\dots,g_{i-1}g_i,\dots,g_n)(1) + (-1)^{n+1}\alpha(g,g_1,\dots,g_{n-1})(1).$$

Thus $d^{n-1}\circ s^n + s^{n+1}\circ d^n$ is the identity map of $C^n(G, M_G^{\{1\}}(A))$. Hence if $d^n(\alpha)=0$, then α belongs to the image of d^{n-1}, thus $H^n(G, M_G^{\{1\}}(A)) = 0$.

4.5.6. Theorem. *Let H be a subgroup of a finite group G. Let A be an H-module. Then the homomorphism*

$$H^n(G, M_G^H(A)) \to H^n(H, A)$$

is an isomorphism.

Proof. First check the theorem for $n=0$. From 4.5.3 we get the homomorphism

$$c' \colon M_G^H(A)^G \to A, \quad c'(\alpha) = \alpha(1).$$

If $\alpha \in M_G^H(A)^G$, then $\alpha(hg) = h\alpha(g)$ for all $h\in H$ and $\alpha(g') = g\alpha(g') = \alpha(g'g)$ for all $g\in G$. So $\alpha\colon G\to A$ is a constant map. We deduce that $h\alpha(1) = \alpha(h) = \alpha(1)$, i.e. $c'(\alpha)\in A^H$. So $c'(M_G^H(A))\subset A^H$.

Define a homomorphism $b\colon A^H \to M_G^H(A)^G$ by $a\to\alpha$, $\alpha(g)=a$ for all $g\in G$.

Then c' and b are inverse to each other, and so are isomorphisms. That proves the case $n=0$.

Now argue by induction on n.

There is a homomorhism of H-modules $A\to M_H^{\{1\}}(A)$, $a\to\alpha$, $\alpha(h)=a$ for all $h\in H$. It is injective, so we have an exact sequence of H-modules

$$0 \longrightarrow A \longrightarrow M_H^{\{1\}}(A) \longrightarrow X \to 0.$$

Apply Lemma 4.5.4 and get an exact sequence

$$0 \longrightarrow M_G^H(A) \longrightarrow M_G^H(M_H^{\{1\}}(A)) \longrightarrow M_G^H(X) \longrightarrow 0$$

of G-modules. The middle term is isomorphic to $M_G^{\{1\}}(A)$ according to Lemma 4.5.2.

Now we get a long sequence of cohomological groups and the commutative diagram

$$\begin{array}{ccccccccc}
\dots & \longrightarrow & H^n(G, M_G^H(X)) & \longrightarrow & H^{n+1}(G, M_G^H(A)) & \longrightarrow & H^{n+1}(G, M_G^{\{1\}}(A)) & \longrightarrow & \dots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\dots & \longrightarrow & H^n(H,X) & \longrightarrow & H^{n+1}(H,A) & \longrightarrow & H^{n+1}(H, M_H^{\{1\}}(A)) & \longrightarrow & \dots .
\end{array}$$

The left vertical arrow is an isomorphism by the inductional assumption. The right vertical arrow is an isomorphism, since both groups are zero by Lemma 4.5.5. Thus, by the Snake Lemma the central vertical arrow is an isomorphism.

4.5.7. Remark. The theorem implies that if Y is defined from the exact sequence

$$0 \longrightarrow A \longrightarrow M_G^{\{1\}}(A) \longrightarrow Y \to 0,$$

then

$$H^{n+1}(G,A) \simeq H^n(G,Y).$$

This can be used to define group cohomologies by induction in n

4.5.8. For a G-module A the restriction map $\mathrm{res} = (\mathrm{inc}, \mathrm{id})\colon (G, A) \to (H, A)$ from 4.1.2 induces a homomorphism $\mathrm{res}^n\colon H^n(G, A) \to H^n(H, A)$ which is called a restriction.

For example, $\mathrm{res}^0\colon A^G \to A^H$ is the inclusion $A^G \subset A^H$.

Define a map $x\colon A \to M_G^H(A)$ by $x(a) = \alpha_a$, $\alpha_a(g) = ga$. It is a homomorphism of G-modules, since

$$x(g_1a)(g) = gg_1a = \alpha_a(gg_1) = g_1x(a)(g).$$

So we get a morphism $(G, A) \to (G, M_G^H(A))$ in $fGr - mod$.

The composition $H^n(G, A) \to H^n(G, M_G^H(A)) \to H^n(H, A)$ which uses the isomorphism of Theorem 4.5.6 corresponds to the morphism $(G, A) \to (G, M_G^H(A)) \to (H, A)$ in $fGr - mod$ which is explicitly desribed as the map $c \circ x\colon a \to \alpha_a(1) = a$ on A and the inclusion $H \subset G$. Thus, the restriction res^n coincides with the composition

$$H^n(G, A) \to H^n(G, M_G^H(A)) \to H^n(H, A).$$

4.5.9. Define a map $y\colon M_G^H(A) \to A$ by

$$y(\alpha) = \sum_{g \in S} g(\alpha(g^{-1}))$$

where $g \in S$ runs through any set of elements of G such that G is a disjoint union of gH. If $\{g' \in S'\}$ form another set with this property, then for every $g' \in S'$ there is a unique $g \in S$ such that $g'H = gH$, i.e. $g' = gh, h \in H$. Then

$$g'(\alpha({g'}^{-1})) = gh(\alpha(h^{-1}g^{-1})) = g(\alpha(hh^{-1}g^{-1})) = g(\alpha(g^{-1})),$$

so the map y doesn't depend on the choice of S.

The map y is a homomorphism of G-modules:

$$\begin{aligned} y(g_1\alpha) &= \sum_{g \in S} g((g_1\alpha)(g^{-1})) = \sum_{g \in S} g((\alpha)(g^{-1}g_1)) \\ &= \sum_{g \in S} g_1g_1^{-1}g((\alpha)((g_1^{-1}g)^{-1})) = \sum_{g' \in S' = g_1^{-1}S} g_1g'((\alpha)({g'}^{-1})) = g_1y(\alpha), \end{aligned}$$

since G is the disjoint union of $g_1^{-1}gH$ where g runs over all elements of S.

So we get a morphism $(\mathrm{id}, y)\colon (G, M_G^H(A)) \to (G, A)$ in $fGr - mod$ and there is a homomorphism $H^n(G, M_G^H(A)) \to H^n(G, A)$. Using the isomorphism of Theorem 4.5.6 we get a homomorphism

$$\mathrm{cor}^n\colon H^n(H, A) \to H^n(G, M_G^H(A)) \to H^n(G, A)$$

which is called a corestriction.

For example, $\mathrm{cor}^0\colon A^H \to A^G$ is defined as $\mathrm{cor}^0(a) = \sum_{g \in S} ga$.

4.5.10. Since the composition $A \xrightarrow{x} M_G^H(A) \xrightarrow{y} A$ is equal to

$$a \to \alpha_a \to \sum_{g \in S} g(\alpha_a(g^{-1})) = \sum_{g \in S} gg^{-1}a = |G : H|a,$$

we conclude from 4.5.8 and 4.5.9 that the composition

$$H^n(G, A) \xrightarrow{\mathrm{res}^n} H^n(H, A) \xrightarrow{\mathrm{cor}^n} H^n(G, A)$$

is equal to multiplication by the index $|G : H|$.

Alternatively we can look at $n = 0$ where it is obvious that $\mathrm{cor} \circ \mathrm{res} = |G : H|$ and then use Remark 4.5.7 and the commutative diagram

$$\begin{array}{ccc}
H^n(G,Y) & \longrightarrow & H^{n+1}(G,A) \\
{\scriptstyle \mathrm{res}^n}\big\downarrow & & {\scriptstyle \mathrm{res}^{n+1}}\big\downarrow \\
H^n(H,Y) & \longrightarrow & H^{n+1}(H,A) \\
{\scriptstyle \mathrm{cor}^n}\big\downarrow & & {\scriptstyle \mathrm{cor}^{n+1}}\big\downarrow \\
H^n(G,Y) & \longrightarrow & H^{n+1}(G,A)
\end{array}$$

to prove the result in the previous paragraph by induction on n.

Since for $n = 0$ the composition $\mathrm{res}^0 \circ \mathrm{cor}^0 \colon A^H \to A^H$ is equal to $a \to \sum_{g \in S} ga$ we can deduce in the same way as above that

$$H^n(H,A) \xrightarrow{\mathrm{cor}} H^n(G,A) \xrightarrow{\mathrm{res}} H^n(H,A)$$

is equal to $f \to \sum_{g \in S} gf$ for $f \in H^n(H,A)$.