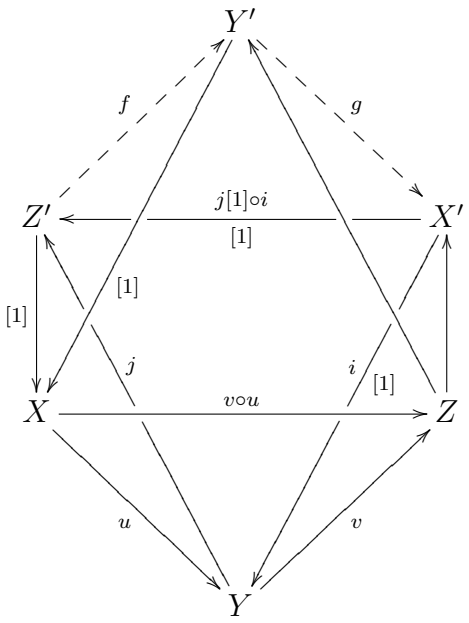
Serge Lang's

Algebra

Seminar notes, exercise solutions etc.

Gau Syu



Last Update: September 27, 2013

Preface

Roughly speaking, this book is an collection of solutions to Serge Lang's *Algebra* i.e.[Lang, 2002]. However, it doesn't cover solutions of all exercises, but some interesting topics. In addition to these exercises, I try to introduce some related concepts and conclusions. Since many concepts and notations have been given in Lang's textbook, I will follow it and omit detail explain.

Furthermore, this book is also a note for a inofficial seminar after school whose theme is to learn some systematic knowledge about algebra. The main reference material is of course Serge Lang's *Algebra*. Besides, some related books and articles given great help.

Thanks to all.

Gau Syu

Contents

List of Theorems

List of Exercises

Part I

The Basic Objects of Algebra

Chapter 1

Groups

1.1 Some Definitions

1.1 (Goursat's Lemma). *Let G, G' be groups, and let H be a subgroups of $G \times G'$ such that the two projections $p_1 \colon H \to G$ and $p_2 \colon H \to G'$ are surjective. Let $N = \ker p_2, N' = \ker p_1$.*

a) One can identify N as a normal subgroup of G, and N' as a normal subgroup of G'.

b) Show that the image of H in $G/N \times G'/N'$ is the graph of an isomorphism

$$G/N \cong G'/N'$$

Proof. We have the following diagram at first

$$\begin{array}{ccccc} & & N & & \\ & & \downarrow{\scriptstyle k_1} & & \\ N' & \xrightarrow{k_2} & H & \xrightarrow{p_1} & G \\ & & \downarrow{\scriptstyle p_2} & & \\ & & G' & & \end{array}$$

Notice that $N \cap N' = e$, we have

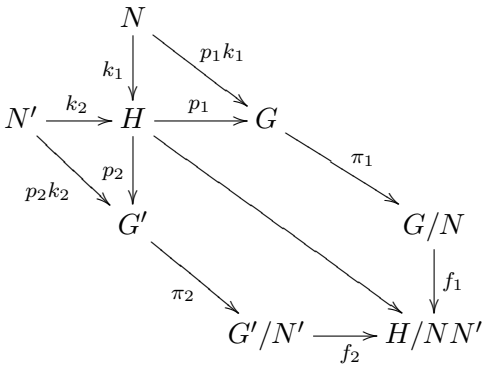
$$\begin{aligned} NN'/N' \trianglelefteq & H/N' \\ H/N' \cong & G \\ NN'/N' \cong & N/(N \cap N') \cong N \end{aligned}$$

thus $N \trianglelefteq G$ and $p_1 k_1$ is the inclusion from N to G, similarly, $N' \trianglelefteq G'$ with inclusion $p_2 k_2$.

Then

$$\begin{aligned}(H/N')/N \cong &(H/N')/(N/(N\cap N'))\\ \cong &(N/N')/(NN'/N') \cong H/NN'\end{aligned}$$

and so does $(H/N)/N'$. Hence we have the following diagram



The third isomorphism theorem tell us that it is commutative.

The image of H in $G/N\times G'/N'$ is $\{(f_1\pi_1p_1(h), f_2\pi_2p_2(h)) \mid h\in H\}$, and by the commutativity of the diagram, equal to the graph of the isomorphism $G/N\cong G'/N'$. □

Remark. The third isomorphism theorem tell us more than $(G/K)/(N/K)\cong G/N$, but also their short exact sequences are *commutative*, i.e. the following diagram is commutative

$$\begin{array}{ccccccccc}1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & G/N & \longrightarrow & 1\\ & & \downarrow & & \downarrow & & \vdots & & \\ 1 & \longrightarrow & N/K & \longrightarrow & G/K & \longrightarrow & (G/K)/(N/K) & \longrightarrow & 1\end{array}$$

Remark. In general, If we have the following diagram

$$\begin{array}{ccccccccc}1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G/H & \longrightarrow & 1\\ & & \downarrow & & \downarrow f & & \vdots\,\overline{f} & & \\ 1 & \longrightarrow & H' & \longrightarrow & G' & \xrightarrow{\pi} & G'/H' & \longrightarrow & 1\end{array}$$

where H is kernel of πf, then there exist a natural injective $\overline{f}$ such that the diagram is commutative. Moreover, f is surjective implies $\overline{f}$ is isomorphism.

1.1.1 Kernel and Cokernel

Essentially, we have a summary:

Theorem 1.1.1. *Let $f: G\to H$ be a homomorphism of groups, then*

a) There exist precisely one(by the meaning of isomorphic[1]) group K and

[1]Moreover, the isomorphism is unique.

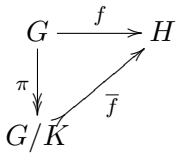
homomorphism $k\colon K \to G$ *such that*

1) $fk = \mathbf{0}$*(the zero means trivial homomorphism)*

2) *For any group* F *and homomorphism* $g\colon F \to G$ *such that* $fg = \mathbf{0}$*, there is a unique homomorphism* μ *such that* $k\mu = g$*.*

b) k *is injective.*

c) f *factor through the canonical map* $\pi\colon G \to G/K$*, which means the following diagram is commutative*



d) f *is surjective implies* $\overline{f}$ *is isomorphism.*

To prove it we need a lemma

Lemma 1.1.2. *Let* $f\colon G \to H$ *be a homomorphism of groups, then*

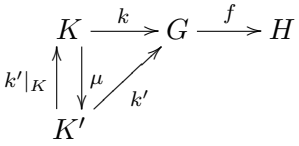
a) f *is injective if and only if for any homomorphisms* $X \underset{\beta}{\overset{\alpha}{\rightrightarrows}} G \xrightarrow{f} H$*,* $f\alpha = f\beta$ *implies* $\alpha = \beta$*.*

b) f *is surjective if and only if for any homomorphisms* $G \xrightarrow{f} H \underset{\beta}{\overset{\alpha}{\rightrightarrows}} X$*,* $\alpha f = \beta f$ *implies* $\alpha = \beta$*.*

Proof. f is injective $\Rightarrow G \cong f(G)$, whence the statement is true. On the contrary, let X be $\ker f$, α the inclusion and $\beta = \mathbf{0}$, then $f\alpha = \mathbf{0} = f\beta$ implies that $\ker f = 1$. The second property is very trick see [Jacobson, 1980]. □

We finish the proof of theorem 1.1.1 now.

Proof. First of all, we verify the kernel of f, written K, and inclusion $k\colon K \to G$ fit the properties in a). For any group F and homomorphism $g\colon F \to G$ such that $fg = \mathbf{0}$, it is clear the image of g is in K and therefore $g|_K$ is the required homomorphism, moreover, it is unique since k is injective. We only need to verify the uniqueness. If there is another group K' and homomorphism $k'\colon K' \to G$ fit these properties, then there must be a unique homomorphism μ such that the following diagram is commutative



Notice that k' is injective since the uniqueness in 2), we have

$$k \circ k'|_K \circ \mu = k' \circ \mu = k \Rightarrow k'|_K \circ \mu = 1_K$$
$$k' \circ \mu \circ k'|_K = k \circ k'|_K = k' \Rightarrow \mu \circ k'|_K = 1_{K'}$$

Hence $(\mu, k'|_K)$ is the unique isomorphism between K and K'.

c) and d) are just the first isomorphism theorem since K is just the kernel of f. □

Remark. The first statement in lemma 1.1.2 does not means that f has a left inverse, if it has, f is called a *split monomorphism*, and the left inverse is called *retraction*. Dually, a homomorphism f has a right inverse, names *section*, is called a *split epimorphism*. It is clear that any split monomorphism must be injective and any split epimorphism is surjective.

In any category with zero morphism, the unique morphism mentioned in the first property(if it exists) is called the *kernel* of f, written $\ker f$. One can think the kernel as the pair (k, K) instead of one of them. One can also consider the dual of theorem 1.1.1, and the unique morphism c mentioned in the first property(if it exists) is called the *cokernel* of f, written $\operatorname{coker} f$. Similarly, one can think the cokernel as a pair (c, C) instead of one of them. The kernel of the cokernel of f is called the *image* of f, written $\operatorname{im} f$, and the cokernel of the kernel of f is called the *coimage* of f, written $\operatorname{coim} f$.

The dual of theorem 1.1.1 is true

Theorem 1.1.3. *Let $f\colon G \to H$ be a homomorphism of groups, then*

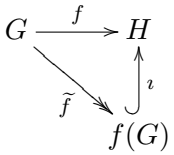
a) There exist precisely one(by the meaning of isomorphic) group C and homomorphism $c\colon H \to C$ such that

1) $cf = \mathbf{0}$(the zero means trivial homomorphism)

2) For any group F and homomorphism $g\colon H \to F$ such that $gf = \mathbf{0}$, there is a unique homomorphism μ such that $\mu c = g$.

b) c is surjective.

c) f factor through the inclusion map $\imath\colon f(G) \to H$,[2] which means the following diagram is commutative



d) f is injective implies $\widetilde{f}$ is isomorphism.

[2]Also factor through $\operatorname{im} f$, but may not an epi-mono factorization.

Proof. First of all, let N be the normal subgroup in H which is generated by $f(G)$, we verify H/N, written C, and canonical map $\pi\colon H \to C$ fit the properties in a). For any group F and homomorphism $g\colon H \to F$ such that $gf = \mathbf{0}$, it is clear that $f(G)$ is in $\ker g$. We define a map

$$\begin{aligned} \overline{g}\colon C &\longrightarrow F \\ xN &\longmapsto g(x) \end{aligned}$$

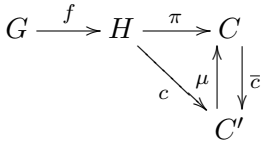
it is well-define homomorphism since if $xN = yN$, then $xy^{-1} \in N \subset \ker g$, therefore

$$xy^{-1} = h_1k_1h_1^{-1}\cdots h_nk_nh_n^{-1}, h_i \in H, k_i \in f(G)$$

hence

$$\begin{aligned} g(xy^{-1}) =& g(h_1k_1h_1^{-1}\cdots h_nk_nh_n^{-1}) \\ =& g(h_1)g(k_1)g(h_1^{-1})\cdots g(h_n)g(k_n)g(h_n^{-1}) \\ =& g(h_1)1g(h_1^{-1})\cdots g(h_n)1g(h_n^{-1}) = 1 \end{aligned}$$

Therefore $\overline{g}$ is the required homomorphism, moreover, it is unique since π is surjective. We only need to verify the uniqueness. If there is another group C' and homomorphism $c\colon H \to C'$ fit these properties, then there must be a unique homomorphism μ such that the following diagram is commutative



Notice that c is surjective since the uniqueness in 2), we have

$$\begin{aligned} \overline{c}\circ\mu\circ c = \overline{c}\circ\pi = c \Rightarrow \overline{c}\circ\mu = 1_{C'} \\ \mu\circ\overline{c}\circ\pi = \mu\circ c = \pi \Rightarrow \mu\circ\overline{c} = 1_C \end{aligned}$$

Hence $(\mu, \overline{c})$ is the unique isomorphism between C' and C.

c) and d) are trivial. □

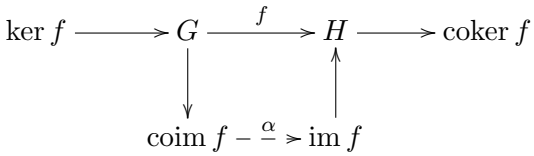
Corollary 1.1.4. *Let $f\colon G \to H$ be a homomorphism of groups, then*

a) $\operatorname{coim} f = G/\ker f$.

b) $\operatorname{im} f$ *is the normal subgroup generated by* $f(G)$.

c) $f(G) \cong \operatorname{coim} f$.

d) there exists a natural homomorphism $\alpha\colon \operatorname{coim} f \to \operatorname{im} f$ *such that the following diagram is commutative*



Remark. If $f(G)$ is normal in H, then it is clear to see that $\operatorname{im} f = f(G)$ and therefore α is isomorphism, but unfortunately, it may not be always true unless H is abelian. In fact, every morphism has kernel and cokernel, and its coimage isomorphic to its image are the axioms which make an additive category to be *abelian*. Therefore the category of groups (which is usually denoted by **Grp**) must not be abelian. But the category of abelian groups (which is usually denoted by **Ab**) is abelian.

1.1.2 Equalizer and Coequalizer

The kernel of a morphism is a special case of equalizer, we give a theorem as a example in group theory case.

Theorem 1.1.5. *Let* $G \underset{g}{\overset{f}{\rightrightarrows}} H$ *be two homomorphism of groups, then*

a) There exist precisely one(by the meaning of isomorphic) group E *and homomorphism* $e\colon E \to G$ *such that*

1) $fe = ge$

2) For any group F *and homomorphism* $h\colon F \to G$ *such that* $fh = gh$*, there is a unique homomorphism* μ *such that* $e\mu = h$*.*

b) e *is injective.*

Proof. One can verify that $\ker d(f,g)$ is the required pair of group and homomorphism, where $d(x) \overset{\text{def}}{=} f(x)(g(x))^{-1}$ is called the *difference* of f, g. □

In arbitrary category, a pair (E, e) of object and morphism fit the properties in above theorem is called the *equalizer* of f, g. Equalizer must be injective, but the converse may not holds. If it holds, the monomorphism is called *regular*. Moreover, if every monomorphism is regular, the category is called *regular*. For example the category of sets, the category of groups and all abelian categories are regular, the category of topological spaces **Top** is not regular.

The following proposition is true in any category and is easy to prove.

Proposition 1.1.6. *Let $e\colon E \to A$ be the equalizer of $f, g\colon A \to B$, then the following statements are equivalent:*

a) $f = g$.

b) e *is surjective.*

c) e *is an isomorphism.*

d) id_A *is the equalizer of* f, g.

The dual of equalizer is *coequalizer*, which is the generalization of cokernel, we also give a theorem as a example in group theory case, it is the dual of theorem 1.1.5.

Theorem 1.1.7. *Let* $G \underset{g}{\overset{f}{\rightrightarrows}} H$ *be two homomorphism of groups, then*

a) There exist precisely one(by the meaning of isomorphic) group Q *and homomorphism* $q\colon H \to Q$ *such that*

1) $qf = qg$

2) For any group F *and homomorphism* $h\colon H \to F$ *such that* $hf = hg$, *there is a unique homomorphism* μ *such that* $\mu q = h$.

b) q *is surjective.*

Proof. One can verify that $\operatorname{coker} d(f, g)$ is the required pair of group and homomorphism. □

The dual proposition of 1.1.6 is

Proposition 1.1.8. *Let $c\colon B \to C$ be the equalizer of $f, g\colon A \to B$, then the following statements are equivalent:*

a) $f = g$.

b) c *is injective.*

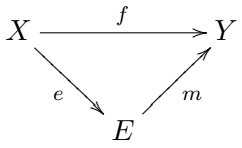
c) c *is an isomorphism.*

d) id_B *is the equalizer of* f, g.

In a regular category, the regular epimorphisms[3] and the monomorphisms form a *factorization system*: every morphism $f\colon X \to Y$ can be factorized

[3]Notice that not every epimorphism is regular.

by the following commutative diagram, where e is regular epimorphism and m is monomorphism



The factorization is unique in the sense that if $\xrightarrow{e'} E' \xrightarrow{m'}$ is another factorization, then there exists an isomorphism $h\colon E \to E'$ such that $he = e'$ and $m'h = m$. The monomorphism m is called the *image* of f.

1.2 Semidirect Product

1.2. *Let G be a finite group and let N be a normal subgroup such that N and G/N have relatively prime orders.*

a) Let H be a subgroup of G having the same order as G/N. Prove that $G = HN$.

b) Let g be an automorphism of G. Prove that $g(N) = N$.

Proof. a), It is clear that the only element in $N \cap H$ is 1 since its order must divide a pair of relatively prime $|H|$ and $|N|$. Therefore

$$|HN| = \frac{|H||N|}{|H \cap N|} = |G/N||N| = |G|$$

and $HN \subset G$, thus $G = HN$.

b), Let $k = |N|$. For any $\varphi \in \operatorname{Aut} G$ and $x \in N$, we assume $\varphi(x) = ng$, where $g \in G \setminus N$. Then $\varphi(x)^k = \varphi(x^k) = 1$, follow by

$$\begin{aligned}(ng)^k = 1 \Rightarrow & g(ng)^{k-1} = n^{-1} \in N \\ \Rightarrow & (ng)^{k-1}g = g^{-1}(g(ng)^{k-1})g \in N \\ \Rightarrow & (ng)^{k-2}g^2 \in N \\ & \cdots\cdots \\ \Rightarrow & g^k \in N\end{aligned}$$

hence $(gN)^k = N$, which conflict with $|G/N|$ relatively prime with $|N|$. Whence $\varphi(x) \in N$ as desired. □

a) tells us that G is the semidirect product of N and H. We also give a theorem to explain this concept.

Theorem 1.2.1. *Let G be a group, and $N \trianglelefteq G, H \leqslant G$. The following statements are equivalent:*

a) $G = NH$ and $N \cap H = 1$.

b) $G = HN$ and $N \cap H = 1$.

c) Every element of G can be written as a unique product of an element of N and an element of H.

d) Every element of G can be written as a unique product of an element of H and an element of N.

e) The composition of natural embedding $H \to G$ and natural projection $G \to G/N$ is an isomorphism.

f) There exists an retraction of the natural embedding and whose kernel is N.

In case one of these statements hold, we say G is a *semidirect product* of N and H, written $N \rtimes H$.

Proof. The equivalence of a) and b) is clear by $(nh)^{-1} = h^{-1}n^{-1}$. In case a) holds, and $nh = n'h'$ where $n, n' \in N, h, h' \in H$, then $nn'^{-1} = h'h^{-1}$, since the left is in N and the right is in H, therefore $n = n', h = h'$. Thus a)⇒c). Similarly, b)⇒d). c)⇔d) is clear. If d) holds, any $g \in G$ can be write as $hn, h \in H, n \in N$ uniquely, thus $hn \mapsto h$ is a well-defined epimorphism from G to H and whose kernel is N. Moreover, it is the retraction of the natural embedding, whence its induced map is the inverse of the composition in e). If f) holds, let φ be the retraction, then for any $g \in G$, $\varphi(g^{-1})g \in N$, thus $g = \varphi(g)\varphi(g^{-1})g$ is a decomposition of g, therefore $G = HN$. If $x \in H \cap N$, then $\varphi(x) = x$ since $x \in H$, but $\varphi(x) = 1$ since $x \in N$, thus $H \cap N = 1$. □

1.2.1 Characteristic Subgroup

The second statement in 1.2 tell us that N is *characteristic*, means $g(N) = N, \forall g \in \mathrm{Aut}(G)$. Characteristic is a strong property since it obviously implies normal. and moreover we have

Proposition 1.2.2. *Let $N \trianglelefteq G$, and H be a characteristic subgroup of N, then $H \trianglelefteq G$. Moreover, if N is characteristic in G, so is H.*

Proof. For any $g \in G$, $c_g(N) = N$ since $N \trianglelefteq G$, thus $c_g \in \mathrm{Aut}(N)$. Since H is characteristic in N, $c_g(H) = H$, thus $H \trianglelefteq G$. Moreover, if N is characteristic in G, then $\mathrm{Aut}(G) \subset \mathrm{Aut}(N) \subset \mathrm{Aut}(H)$, thus H is characteristic in G. □

1.3 Some Operations

1.3. *Let H be a proper subgroup of a finite group G. Show that G is not the union of all the conjugations of H.*

Proof. Conversely assume $G = \cup H^x$, and notice that the orbit containing H under the conjugate operation is its conjugation class and its stabilizer is the normalizer. Then

$$\begin{aligned} |G| =& 1 + |\bigcup_{x\in G} H^x\{e\}| \\ \leqslant& 1 + (G : H_G(H))(|H| - 1) \\ \leqslant& 1 + |G| - (G : N_G(H)) \end{aligned}$$

Hence $G = N_G(H)$, $H \trianglelefteq G$. Thus $\cup H^x = H \lneqq G$ which is a contradiction.□

Warning. This may not be true for infinite group, see Chapter 13.

1.4. *Let G be a finite group operation on a finite set S with $|S| \geqslant 2$. Assume that there is only one orbit. Prove that there exist an element $x \in G$ which has no fixed point.*

Proof. It's easy to prove this by using Burnside's lemma. But we can also use the conclusion given by the previous exercise instead of Burnside's lemma. Indeed, Let $S = \{s_1, \cdots, s_n\}$ and assume that every element of G has fixed point, then $G = \bigsqcup G_{s_i}$, where $G_{s_i} = \{g \in G \mid gs_i = s_i\}$. Since $G_{gs_i} = \{x \in G \mid xgs_i = gs_i\}$, G_{gs_i} is conjugated with G_{s_i}. But there is only one orbit and hence these G_{s_i} are all conjugated which contradict to 1.3. □

1.5 (Burnside's Lemma). *Let G be a finite group operation on a finite set S, then*

a) For each $s \in S$,

$$\sum_{t\in\mathcal{O}_s} \frac{1}{|\mathcal{O}_t|} = 1$$

b) Let N denote the number of orbits, then

$$N = \frac{1}{|G|}\sum_{x\in G} |\operatorname{Fix}(x)|$$

Proof. the right equal to

$$\sum_{\substack{s\in\operatorname{Fix}(x)\\ x\in G}} \frac{1}{|\mathcal{O}_s||G_s|}$$

Notice that the summation contain every s for $|G_s|$ times. Hence the above summation obviously equal to

$$\sum_{s\in S}|G_s|\frac{1}{|\mathcal{O}_s||G_s|}=\sum_{s\in S}\frac{1}{|\mathcal{O}_s|}=N \qquad \square$$

The following exercise is a useful property, here p is a prime number.

1.6. *Let P be a $p-$group. Let A be a normal subgroup of order p. Prove that A is contained in the center of P.*

Proof. Let the $p-$group act on A, then the number of fixed points of P is $\equiv |A| \mod p$.(a lemma in the text) But $|A|>0$ since e must be fixed, hence the number of fixed point is p, which means every element of A commute with P, i.e. is contained in the center of P. $\square$

1.3.1 Orbits, Stabilizers etc.

Definition 1.3.1. Here is some easily confused concepts about group action, assuming that G act on S

a) The *orbit* of a point s in S

$$Gs=\{gs \mid g\in G\}.$$

b) The *stabilizer* of a point s in S

$$G_s=\{g\in G \mid gs=s\}.$$

c) The set of *fixed points* of $g\in G$ is denoted

$$S^g=\{s\in S \mid gs=s\}.$$

d) A *$G-$invariant element* of S is $s\in S$ such that $gs=s$ for all $g\in G$. The set of all such s is denoted

$$S^G=\{s\in S \mid gs=s, \forall g\in G\}.$$

and called the *$G-$invariants* of S.

e) The set of all orbits of S under the action of G is written as S/G (or, less frequently: $G\backslash S$), and is called the *quotient* of the action. In geometric situations it may be called the *orbit space*, while in algebraic situations it may be called the space of *coinvariants*, and written S_G.

For orbits and stabilizers of a point s in S, we have

Theorem 1.3.2 (Orbit-stabilizer Theorem). *The image and coimage of map $g \mapsto gs$ is Gs and G/G_s.*

If T is a subset of S, we write GT for the set $\{gt \mid t \in T, g \in G\}$.

a) T is called *invariant* under G if $GT = T$ (or equivalently, $GT \subset T$).

b) T is called *fixed* under G if $gt = t$ for all $g \in G, t \in T$.

Remark. The coinvariants are a quotient while the invariants are a subset. These terminologies and notations are used particularly in group cohomology and group homology, which use the same superscript/subscript convention.

1.4 Explicit Determination of Groups

1.7. *Let G be a group of order p^3, where p is prime, and G is not abelian. Show that $|Z(G)| = p$.*

The key to prove this is the following lemma:

Lemma 1.4.1. *G is abelian if and only if $G/Z(G)$ is cyclic.*

Proof. Assume $G/Z(G)$ is not trivial, and its generator is a, then, for any $g \in G$, g can be write as $a^k z$ for some $k \in N, z \in Z(G)$, hence $ag = a^{k+1}z = a^k za = ga$, thus $a \in Z(G)$ which is a contradiction. □

1.8. *Show that every group of order < 60 is solvable.*

Since any tower has a simple refinement, we only need to show that every simple group of order < 60 is abelian. The following proof comes from [Rotman, 2002]. We introduce a lemma first.

Lemma 1.4.2. *There is no non-abelian simple group of order $p^n m$, where, p is prime and $p \nmid m, p^n \nmid (m-1)!$*

Proof. We claim that every $p-$group G of order$> p$ is not simple. Since $Z(G)$ is non-trivial, either $Z(G)$ is proper subgroup and G is not simple or $Z(G) - G$ and G is abelian.

Suppose that such a simple group G exists. By Sylow's theorem, G contains a subgroup P of order p^n, hence of index m. We may assume that $m > 1$, for non-abelian $p-$groups are never simple. By the theorem of representation on cosets, there exists a homomorphism $\phi\colon G \to S_m$ with $\ker\phi \leqslant P$. Since G is simple, however, it has no proper normal subgroups; hence $\ker\phi = 1$ and ϕ is an injection; that is, $G \cong \phi(G) \leqslant S_m$. By Lagrange's theorem, $p^n m \mid m!$, and so $p^n \mid (m-1)!$, contrary to the hypothesis. □

Where the theorem of representation on cosets is

Theorem 1.4.3 (Representation on Cosets). *Let G be a group, and let H be a subgroup of G having finite index n. Then there exists a homomorphism $\phi\colon G \to S_n$ with $\ker\phi \leqslant H$.*

The rest proof of 1.8 consider three cases in which the order of G not satisfy the lemma. The are $|G| = 30, 40$ and 56. We only show the proof in case $|G| = 30$, the others are similar.

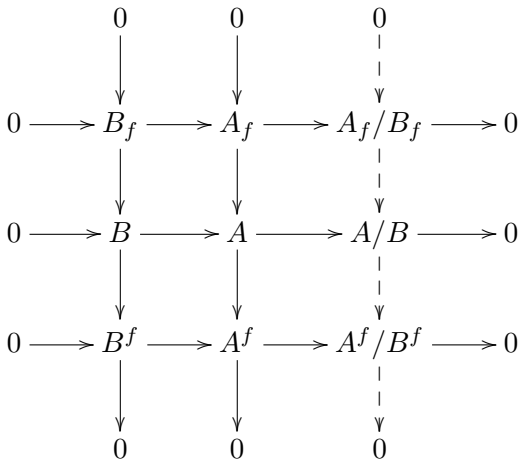
Proof. Let P be a Sylow $5-$subgroup of G, so that $|P| = 5$. The number r_5 of conjugates of P is a divisor of 30 and $r_5 \equiv 1 \mod 5$. Now $r_5 \neq 1$ lest $P \lhd G$, so that $r_5 = 6$. By Lagrange's theorem, the intersection of any

two of these is trivial. There are four nonidentity elements in each of these subgroups, and so there are $6 \times 4 = 24$ nonidentity elements in their union. Similarly, the number r_3 of Sylow 3−subgroups of G is 10 (for $r_3 \neq 1$, r_3 is a divisor of 30, and $r_3 \equiv 1 \mod 3$). There are two nonidentity elements in each of these subgroups, and so the union of these subgroups has 20 nonidentity elements. We have exceeded the number of elements in G, and so G cannot be simple. □

1.5 Abelian Groups

1.9. *Let $f\colon A \to A'$ be a homomorphism of abelian groups. Let B be a subgroup of A. Denote by A^f and A_f the image and kernel of f in A respectively, and similarly for B^f and B_f. Show that $(A : B) = (A^f : B^f)(A_f : B_f)$, in the sense that if two of these three indices are finite, so is the third, and the stated equality holds.*

Proof. Consider the following commutative diagram



By the 9−lemma, the third column is exact, $A^f/B^f \cong (A/B)/(A_f/B_f)$. Hence $(A : B) = (A^f : B^f)(A_f : B_f)$ as desired. □

1.5.1 Abelian Category

A general concept of abelian group is abelian category, which is a special case of preadditive category

Definition 1.5.1. A category $\mathcal{C}$ is called *preadditive*, if every morphism set $\mathrm{Hom}(A, B)$ is an abelian group, and for every $A, B, C \in \mathrm{ob}\,\mathcal{C}$,

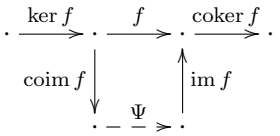
$$\begin{aligned} \mathrm{Hom}(A,B) \times \mathrm{Hom}(B,C) &\longrightarrow \mathrm{Hom}(A,C) \\ (f,g) &\longmapsto g \circ f \end{aligned}$$

is a homomorphism.

In any preadditive category, we can consider the kernel and cokernel of a morphism (even not every one has).

Definition 1.5.2. Let f be a morphism with kernel and cokernel, we call the kernel of $\mathrm{coker}\, f$ (if exists) the *image* of f, denoted by $\mathrm{im}\, f$, while the cokernel of $\ker f$ the *coimage* of f with notation $\mathrm{coim}\, f$. In such situation,

there exist a *natural morphism* Ψ such that the following diagram commutative:



The factorization $f = \operatorname{im} f \circ \Psi \circ \operatorname{coim} f$ is called *standard*.

Definition 1.5.3. Two adjacent morphisms

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

are called *exact* or *exact at* B, if $\operatorname{im} f \cong \ker g$.

It is natural to consider the initial object and the terminal object.

Proposition 1.5.4. *Let $\mathcal{C}$ be a preadditive category, and $A \in \operatorname{ob}\mathcal{C}$. Then the following statements are equivalent:*

a) A is the initial object.

b) A is the terminal object.

c) $1_A = 0$.

d) $\operatorname{Hom}(A, A)$ is trivial.

Such an object is called the *zero object* (and usually denoted by 0). By the universal property of initial object and terminal object, any preadditive category has at most one zero object, and the morphism set between zero object and others must be trivial. Moreover, any zero morphism $0\colon A \to B$ can be factor through two zero morphisms

$$A \longrightarrow 0 \longrightarrow B$$

We can also consider the product and coproduct in such category. Although may not every finite objects have product or coproduct, we still have some special properties in a preadditive category.

Proposition 1.5.5. *Let $\mathcal{C}$ be a preadditive category, and $A, B, C \in \operatorname{ob}\mathcal{C}$. Then the following statements are equivalent:*

a) C is the product of A and B.

b) C is the coproduct of A and B.

c) There exist morphisms $p_1 \colon C \to A, P_2 \colon C \to B, k_1 \colon A \to C, k_2 \colon B \to C$ *such that*

$$\begin{aligned} p_1 k_1 &= \mathrm{id}_A \\ p_2 k_2 &= \mathrm{id}_B \\ k_1 p_1 + k_2 p_2 &= \mathrm{id}_C \end{aligned}$$

This property shows that the finite product and coproduct in a preadditive category is the same thing, which is called a *biproduct*. The third statement can be thought as the definition of the biproduct of two objects A and B. We take $A \oplus B$ as the notation of it.

Warning. Notice that, although infinite direct sums make sense in some categories, like **Ab**, infinite biproducts do not make sense.

By adding some properties to preadditive category, we have a list kind of categories.

Definition 1.5.6. An *additive category* is a preadditive category with all finite biproducts. A *pre-abelian category* is an additive category with all kernels and cokernels. An *abelian category* is a pre-abelian category such that all natural morphism Ψ are isomorphisms.

During consider preadditive categories, a kind of functors between preadditive categories are very important.

Definition 1.5.7. A functor $\mathcal{F}$ between two preadditive categories $\mathcal{C}$ and $\mathcal{D}$ is called *additive*, if for any given objects A and B in $\mathcal{C}$, the correspondence from $\mathrm{Hom}(A, B)$ to $\mathrm{Hom}(\mathcal{F}(A), \mathcal{F}(B))$ is a homomorphism.

Proposition 1.5.8. *An additive functor maps zero object to zero object.*

1.5.2 Herbrand Quotient

[Serre and Greenberg, 1980]

1.10. *Let G be a finite cyclic group of order n, generated by an element σ. Assume that $f, g \colon A \to A$ be the endomorphisms of A given by*

$$\begin{aligned} f(x) &= \sigma x - x, \\ g(x) &= x + \sigma x + \cdots + \sigma^{n-1} x. \end{aligned}$$

Define the Herbrand quotient *by the expression $q(A) = (A_f : A^g)/(A_g : A^f)$, provided both indices are finite. Assume now that B is a subgroup of A such that $GB \subset B$,*

a) Define in a natural way an operation of G on A/B.

b) Prove that

$$q(A) = q(B)q(A/B)$$

in the sense that if two of these quotients are finite, so is the third, and the stated equality holds.

c) If A is finite, show that $q(A) = 1$.

We rewrite the statement of this problem to be

Proposition 1.5.9. *The Herbrand quotient is* multiplicative *on short exact sequences. In other words, if*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is exact, and any two of the quotients are defined, then so is the third and

$$q(B) = q(A)q(C)$$

Moreover, if A is finite then $q(A) = 1$.

To proof the property, we need some lammas.

Lemma 1.5.10. *Consider the sequence with f injective and g surjective:*

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

The following statements are equivalent:

a) This sequence is exact.

b) A is the kernel of g.

c) C is the cokernel of f.

Proof. Notice that, the sequence is *exact* means $\operatorname{coim} f \cong \ker g$ in abelian category. f is injective implies $\operatorname{coim} f \cong A$, g is surjective implies $\operatorname{im} g \cong C$.□

We also need some diagram lemmas, see [Lane, 1998] or later section.

Consider the following *cochain complex* (which means the composition of any adjacent two morphisms is zero.):

$$\cdots \longleftarrow K^{2n+1}(A) \xleftarrow{f} K^{2n}(A) \xleftarrow{g} K^{2n-1}(A) \longleftarrow \cdots$$

where every $K^i(A) = A$.

One can verify that $K(-)$ is a well-defined functor from the category of abelian groups to the category of cochain complexes. Moreover $K(-)$ is an additive functor.

The quotient may be defined for a pair of endomorphisms of an Abelian group, f and g, which satisfy the condition $fg = gf = 0$. Their *Herbrand quotient* $q(f, g)$ is defined as

$$q(f, g) = (\ker f : \operatorname{im} g)/(\ker g : \operatorname{im} f)$$

In mathematics, the *Herbrand quotient* is a quotient of orders of cohomology groups of a cyclic group. It was invented by Jacques Herbrand. As a special case of the general theory of Euler characteristics, it has an important application in class field theory.

If G is a finite cyclic group acting on a $G-$module A, then the cohomology groups $H^n(G, A)$ have period 2 for $n \geqslant 1$; in other words

$$H^n(G, A) = H^{n+2}(G, A)$$

an isomorphism induced by cup product with a generator of $H^2(G, Z)$. (If instead we use the *Tate cohomology groups* then the periodicity extends down to $n = 0$.)

A *Herbrand module* is an A for which the cohomology groups are finite. In this case, the *Herbrand quotient* $h(G, A)$ is defined to be the quotient of the order of the even and odd cohomology groups, like

$$h(G, A) = \frac{|H^2(G, A)|}{|H^1(G, A)|}$$

The proof of 1.5.9 in fact is a proof to

Proposition 1.5.11. *The Herbrand quotient is* multiplicative *on short exact sequences. In other words, if*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is exact, and any two of the quotients are defined, then so is the third and

$$h(G, B) = h(G, A)h(G, C)$$

Moreover, if A is finite then $h(G, A) = 1$.

Corollary 1.5.12. *If there is a $G-$homomorphism $f\colon A \to B$ with finite kernel and cokernel. Then A and B have the same Herbrand quotient.*

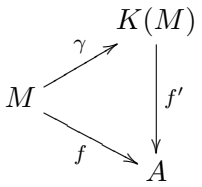
1.5.3 Grothendieck Group

Proposition 1.5.13. *Let M be an abelian monoid, written additively. There exists an abelian group $K(M)$ with a monoid-homomorphism*

$$\gamma\colon M \longrightarrow K(M)$$

having the following universal property:

If $f\colon M \longrightarrow A$ is a homomorphism into an abelian group A, then there exists a unique homomorphism $f'\colon K(M) \longrightarrow A$ making the following diagram commutative:



Proof. Let $F_{\mathrm{ab}}(M)$ be the free abelian group generated by M. We denote the generator of $F_{\mathrm{ab}}(M)$ corresponding to $x \in M$ by $[x]$. Let B be the subgroup generated by all elements of type

$$[x+y]-[x]-[y]$$

where $x, y \in M$. Let $K(M) = F_{\mathrm{ab}}(M)/B$, and let γ be the composition $M \hookrightarrow F_{\mathrm{ab}}(M) \twoheadrightarrow F_{\mathrm{ab}}(M)/B$. Then it is easy to check that $(K(M), \gamma)$ satisfying the universal property. □

The group $K(M)$ is called the *Grothendieck group* of M.

Proposition 1.5.14. *For any $x \in F_{\mathrm{ab}}(M)$, let $\overline{x}$ denote its image in $K(M)$. Then $\overline{[x]} = \overline{[y]}$ if and only if there exists a $t \in M$ such that $x + t = y + t$.*

Proof. Consider $M \times M/\sim$, where $(x, y) \sim (x', y')$ if there exists a $t \in M$ such that $x + y' + t = x' + y + t$. It is easy to check that $\sim$ is a equivalent relation and $M \times M/\sim$ is a group (the inverse of (x, y) is (y, x)). Define $\varphi\colon M \longrightarrow M \times M/\sim$ to be $\varphi(x) = (x, 0)$, then $(M \times M/\sim, \varphi)$ satisfying the universal property:

For any monoid-homomorphism $f\colon M \longrightarrow G$, define $f'\colon M \times M/\sim \longrightarrow G$ to be $f'((x, y)) = f(x) - f(y)$. It is easy to check that f' is the unique homomorphism make the diagram commutative. □

1.6 Inverse Limit and Completion

Definition 1.6.1. Let A be an additive abelian group[4]. Let $p_A \colon A \longrightarrow A$ denote multiplication by p. We say that A is *$p-$divisible* if p_A is surjective. By taking $A_n = A$ and $\phi_{n-1}^n = p_A$ for all n, (A, p_A) can be view as an inverse system. The inverse limit is denoted by $V_p(A)$. Let $T_p(A)$ be the subset of $V_p(A)$ consisting of whose corresponding sequences start with 0. Let $A[p^n]$ be the kernel of p_A^n. Then

$$T_p(A) = \varprojlim A[p^{n+1}]$$

The group $T_p(A)$ is called the *Tate group* associated with the $p-$divisible group A.

Definition 1.6.2. An inverse limit of an inverse system of finite groups is called a *profinite group*.

[4]or, in other words, a $\mathbb{Z}-$module

1.7 Appendix

1.7.1 Proof of Lemma 1.1.2

[Jacobson, 1980].

If f is surjective, it's clear that the statement is true. On the contrary, we consider two cases.

For case $f(G) \trianglelefteq H$, Let $X = H/f(G)$, and α be the canonical map, β be the trivial homomorphism, then $\alpha f = \beta f$, the statement assert $\alpha = \beta$, hence $f(G) = H$, i.e. f is surjective.

For case $f(G) \ntrianglelefteq H$, it implies that $[H : f(G)] > 2$. In this case, we will show that there exists two distinct homomorphisms α and β from H to S_H such that $\alpha f = \beta f$, which is a contradiction.

Let α be $h \mapsto l_h$, where l_h denote the left translation. We shall take β as form $h \mapsto p l_h p^{-1}$, and it does not equal to $h \mapsto l_h$, i.e. p does not commute with every l_h. Since the permutation commuting with all left translation must be right translation, and every translation $\neq 1$ has no fixed point, our condition will be satisfied if p is a permutation $\neq 1$ with a fixed point.

On the another hand, $\alpha f = \beta f$ requires that p commutes with every $g \in f(G)$. To construct a permutation satisfying all of our condition, we choose a permutation π of $f(G)\backslash H$ such that $\pi \neq 1$ and has a fixed point. This can be done since $|f(G)\backslash H| > 2$. Let I be the set of representatives of right cosets, Then, every element of H can be written in one and only one way as $gh, g \in f(G), h \in I$, and our map p is defined by $p(gh) = gh'$, where $\pi(f(G)h) = f(G)h'$. Then it is clear that p satisfies all of our condition and hence $\alpha f = \beta f$ but $\alpha \neq \beta$ as desired.

Chapter 2

Rings

Chapter 3

Modules

3.1 Some Definitions

3.1.1 Modules

Definition 3.1.1. Let R be a ring. A *left module* over R, or a left $R-$module M is an abelian group together with an left operation of R on M satisfies both left and right distributive laws.

Definition 3.1.2. Let R be an *entire* ring and let M be a $R-$module. The *torsion submodule* M_{tor} is the set of *torsion* elements in M.

Proposition 3.1.3. *Let ${}_R\mathfrak{I}$ be the ring of left ideals of R, then a $R-$module is also a ${}_R\mathfrak{I}-$module.*

Remark. We denote $\mathfrak{I}$ to be the ring of ideals of R, then the same proposition holds for $\mathfrak{I}$.

3.1.2 Algebras

Definition 3.1.4. By an *$R-$algebra*, we mean a $R-$module together with a bilinear map.

Definition 3.1.5. By an *algebra over A*, we mean a ring-homomorphism $f\colon A \longrightarrow B$ such that $f(A)$ is contained in the center of B. We say that the algebra is *finitely generated* if B is *finitely generated as a ring* over $f(A)$.

Remark. In this case, B can be view as an $A-$module by the operation

$$(a, b) \longmapsto f(a)b$$

More over, any $B-$module can be view as an $A-$module by the above operation.

3.2 Homomorphisms

In this section, we should assume R is commutative.

3.2.1 Exactness

Proposition 3.2.1. *The functor* $\mathrm{Hom}_R(-, N)$ *is* right exact. *Which means each sequence*

$$M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is exact, then the sequence

$$\mathrm{Hom}_R(M', N) \longleftarrow \mathrm{Hom}_R(M, N) \longleftarrow \mathrm{Hom}_R(M'', N) \longleftarrow 0$$

is exact.

Proposition 3.2.2. *The functor* $\mathrm{Hom}_R(M, -)$ *is* left exact. *Which means each sequence*

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N''$$

is exact, then the sequence

$$0 \longrightarrow \mathrm{Hom}_R(M, N') \longrightarrow \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M, N'')$$

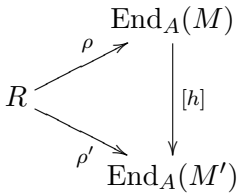
is exact.

3.2.2 Representation

Let M be an $A-$module, then $\mathrm{End}_A(M)$ is a ring and M is a module over $\mathrm{End}_A(M)$. Moreover, if A is commutative and $\rho\colon R \longrightarrow \mathrm{End}_A(M)$ is a ring homomorphism, then M is also a module over R.

Definition 3.2.3. Let R be a ring and let $\rho\colon R \longrightarrow \mathrm{End}_A(M)$ be a ring homomorphism. Then ρ is called a *representation* of R on M.

Definition 3.2.4. A *morphism* of representation $\rho\colon R \longrightarrow \mathrm{End}_A(M)$ into another $\rho'\colon R \longrightarrow \mathrm{End}_A(M')$ is an $A-$module homomorphism $h\colon M \longrightarrow M'$ such that the following diagram is commutative.



where $[h]$ is defined by $[h]f = h \circ g \circ h^{-1}$.

Definition 3.2.5. Let G be a *monoid*. By a *representation* of G on an $A-$module M, we mean a homomorphism $\rho\colon G \longrightarrow \mathrm{End}_A(M)^*$.

Remark. We may extend ρ to be a representation of $A[G]$ on $\mathrm{End}_A(M)$.

3.3 Category of Modules

Definition 3.3.1. A module M is said to be *finitely generated* or of *finite type*, or *finite* over R, if it has a finite number of generators.

Definition 3.3.2. An exact sequence of modules $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ is said to *split*, if it is *equivalent* to the canonical one: $0 \longrightarrow M' \xrightarrow{\imath} M' \oplus M'' \xrightarrow{p} M'' \longrightarrow 0$. That is there exist an isomorphism $M \longrightarrow M' \oplus M''$ make the following diagram commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \| & & \cong\downarrow & & \| & & \\ 0 & \longrightarrow & M' & \xrightarrow[\imath]{} & M' \oplus M'' & \xrightarrow[p]{} & M'' & \longrightarrow & 0 \end{array}$$

Proposition 3.3.3. *Let $0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ be an exact sequence of modules. Then the following statements are equivalent:*

1. *this sequence is split;*
2. *f is split monomorphism;*
3. *g is split epimorphism.*

Remark. Such a proposition is true in general abelian category.

Definition 3.3.4. In abelian category, a *kernel* of a morphism $f\colon A \longrightarrow B$, is a morphism $k\colon K \longrightarrow A$ such that for any object X, the following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(X, K) \longrightarrow \mathrm{Hom}(X, A) \longrightarrow \mathrm{Hom}(X, B) \longrightarrow 0$$

Similarly, we have

Definition 3.3.5. In abelian category, a *cokernel* of a morphism $f\colon A \longrightarrow B$, is a morphism $c\colon B \longrightarrow C$ such that for any object X, the following sequence is exact:

$$0 \longrightarrow \mathrm{Hom}(A, X) \longrightarrow \mathrm{Hom}(B, X) \longrightarrow \mathrm{Hom}(C, X) \longrightarrow 0$$

Remark. It is clear that these definitions are consist with the definitions in Chapter1.

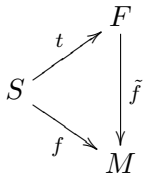
Theorem 3.3.6. *The category of modules over a ring is an abelian category.*

3.4 Free Module

Definition 3.4.1. A non-empty family of elements of M is called a *basis* of M if it is linearly independent and generates M. By a *free* module we mean a module admits a basis, or zero module.

Definition 3.4.2. Let S be a non-empty set, we define the *free* module over a ring R *generated by* S, denoted by $R\langle S\rangle$, to be the unique object in $\mathbf{Mod}_R$ satisfying the following universal property

> For any $R-$module M and any set-map $f\colon S \longrightarrow M$, there exist exact one $R-$homomorphism $\tilde{f}\colon F \longrightarrow M$ making the following diagram commutative



These two definitions are consist. If S is a non-empty set then it is consist with a diagram of type S (view as a discrete category) say $\{Rx_i\}_{i\in S}$. For any $R-$module M and any set-map $f\colon S \longrightarrow M$, (M, f) induces a nature cocone (M, ϕ_i) where ϕ_i is the composite of canonical maps

$$\begin{aligned} Rx_i \longrightarrow & R \longrightarrow M \\ rx_i \longmapsto & r \longmapsto ry_i \end{aligned}$$

where $y_i \in M$ is arbitrary. By such a translation, the solution of the above universal property is exact the colimit of $\{Rx_i\}_{i\in S}$ and hence is $\oplus Rx_i$.

Proposition 3.4.3. *If sets S and S' have same cardinality, then $R\langle S\rangle \cong R\langle S'\rangle$.*

Warning. The converse may not be true! If it is true, we say R has *invariant dimension property*. In this case, we define the *dimension* of a free module F to be the cardinality of a basis of F.

Example. Let F be a free $A-$module with countable infinite basis, then $R = \mathrm{End}_A(F)$ is a ring. And as $R-$modules $R \cong R \oplus R \oplus \cdots \oplus R$ for any finite number of summands.

The following propositions about invariant dimension property can be found in [Hungerford, 1974]. We just list them here.

Proposition 3.4.5. *Let F be a free $R-$module with infinite basis, then every basis of F has same cardinality.*

Proposition 3.4.6. *Fields have invariant dimension property.*

Proposition 3.4.7. *Let I be an ideal of R and F be a free $R-$module with basis X. $\pi\colon F \longrightarrow F/IF$ is the canonical map. Then F/IF is a free $R/I-$module with basis $\pi(X)$ and $|\pi(X)| = |X|$.*

Proposition 3.4.8. *If $f\colon R \longrightarrow A$ is an epimorphism where A has invariant dimension property, then so does R.*

Proof. Consider $I = \ker f$, then $A \cong R/I$, and the following comes from the above proposition. □

Proposition 3.4.9. *Commutative rings have invariant dimension property.*

Definition 3.4.10. A module M is called *principal* if there exists an element $x \in M$ such that $M = Ax$.

3.4.1 Vector Spaces

Proposition 3.4.11. *If any $A-$module is free, then A is a division ring.*

Remark. A ring over which every module is projective is called *semisimple*.

Theorem 3.4.12 (Kernel and Image). *If $f\colon V \longrightarrow W$ is a homomorphism of vector spaces over a field k, then*

$$\dim V = \dim \ker f + \dim \operatorname{im} f$$

3.1. *Let V be a vector spaces over a field k, and let U, W be subspaces. Show that*

$$\dim U + \dim W = \dim(U + W) + \dim(U \cap W)$$

Proof. Let $\{v_1, v_2, \cdots, v_k\}$ be a basis of $U \cap W$. One can extend it to a basis of U, say $\{v_1, v_2, \cdots, v_k, u_{k+1}, u_{k+2}, \cdots, u_n\}$. Similarly, we get a basis of W, say $\{v_1, v_2 \cdots, v_k, w_{k+1}, w_{k+2}, \cdots, w_m\}$. Then it is clear that $\{v_1, v_2, \cdots, v_k, u_{k+1}, u_{k+2}, \cdots, u_n, w_{k+1}, w_{k+2}, \cdots, w_m\}$ is a basis of $U + W$. Hence we get the formula. □

3.2. *Generalize the dimension statement of 3.4.6 to free modules over a commutative ring.*

Proof. Notice that $F/\mathfrak{m}F$ is a vector space over $A/\mathfrak{m}$. □

3.3. *Let R be an entire ring containing a field k as subring. Suppose that R is a finite dimensional vector space over k under the ring multiplication. Show that R is a field.*

Proof. Let $e^1, e^2, \cdots, e^n$ be a basis of R, and $e^i e^j = a_k^{ij} e^k$, then for any $\alpha = \alpha_i e^i, \beta = \beta_j e^j \neq 0$, the equations $\alpha X = \beta$ has a solution $X = \alpha^{-1}\beta$. Otherwise, $\det(\alpha_i a_k^{ij}) = 0$, hence $\alpha X = 0$ has a non-zero solution, which contradict to the entireness of R. □

3.5 Duality

Definition 3.5.1. Let E be a free module over a commutative ring A. By the *dual module* $E^\vee$ of E we mean the module $\mathrm{Hom}(E, A)$. Its elements will be called *functionals*.

Remark. If $x \in E, f \in E^\vee$, we sometimes denote $f(x)$ by $\langle x, f\rangle$. Keeping x fixed, we get a linear map on $E^\vee$, which is 0 if and only if $x = 0$. Hence we get an injection $E \longrightarrow E^{\vee\vee}$ which is not always a surjective. If it is, we call E is *reflexive*.

Proposition 3.5.2. *Let E ba a finite free module over the commutative ring A, of dimension n. Then $E^\vee$ is also free, and $\dim E^\vee = n$. If $\{x_1, \cdots, x_n\}$ is a basis for E, and f_i is the functional such that $f_i(x_j) = \delta_{ij}$, then $\{f_1, \cdots, f_n\}$ is a basis for $E^\vee$.*

We call such a basis $\{f_i\}$ the *dual basis* of $\{x_i\}$.

Corollary 3.5.3. *When E is of finite type, then the natural map $E \longrightarrow E^{\vee\vee}$ is an isomorphism.*

Definition 3.5.4. Let V, V' be two vector spaces over a field K. Given a bilinear map

$$\begin{aligned} V \times V' &\longrightarrow K \\ (x, x') &\longmapsto \langle x, x'\rangle \end{aligned}$$

An element $x \in V$ is said to be *orthogonal* to a subset s' of V' if $\langle x, x'\rangle = 0$ for all $x' \in S'$. We define the *kernel* of the bilinear map on the left to be the subspace of V which is orthogonal to V', and similarly for the kernel on the right.

Theorem 3.5.5. *Let $V \times V' \longrightarrow K$ be a bilinear map, let W, W' be its kernels on the left and right respectively, and assume that V'/W' is finite dimensional. Then the induced homomorphism $V'/W' \longrightarrow (V/W)^\vee$ is an iosmorphism.*

Remark. Let E be a module over a commutative ring A, then we may form two types of dual:

$E^\wedge = \mathrm{Hom}(E, \mathbb{Q}/\mathbb{Z})$, viewing E as an abelian group;

$E^\vee = \mathrm{Hom}_A(E, A)$, viewing E as an $A-$module.

Both are called dual. If we need to distinguish them, we call $E^\wedge$ the *Pontrjagin dual*.

3.6 Modules over Principal Rings

Throughout this section, we assume that R is a principal entire ring. All modules are over R unless otherwise specified.

Proposition 3.6.1. *Principal rings have invariant dimension property.*

Theorem 3.6.2. *Let F be a free module, and M a submodule. Then M is free, and its dimension is less than or equal to the dimension of F.*

Proof. Let $\{v_i\}_{i\in I}$ be a basis of F. For any subset J of I, we let F_J to be the free submodule generated by $\{v_j\}_{j\in J}$, and we let $M_J = F_J \cap M$. Let S be the set of all pairs (M_J, w) where J is a subset of I, and w is a basis of M_J indexed by a subset J' of J. For two such pairs $(M_J, w), (M_K, u)$, we define $(M_J, w) \prec (M_K, u)$ if $J \subset K$ and if the basis u of M_K is a extension of the basis w of M_J. Then we will use Zorn's lemma and the rest are easy to prove. □

Warning. This is not true in general case. For example, $\mathbb{Z}/6$ is a free $\mathbb{Z}/6-$module, but its submodule $\{0, 2, 4\}$ is not free.

Corollary 3.6.3. *Let E be a finitely generated module and E' a submodule. Then E' is finitely generated.*

Definition 3.6.4. A free $1-$dimensional module over R is called *infinite cyclic*.

Definition 3.6.5. Let E be a module. An element x of E is called a *torsion element* if there exists $a \in R, a \neq 0$ such that $ax = 0$. The *torsion submodule* E_{tor} is the set of torsion elements in E. We say that E is a *torsion module* if it consists of torsion elements. If $E_{\text{tor}} = 0$, we say that E is *torsion free*.

Theorem 3.6.6 (Structure Theorem of f.g.Modules over PID). *Let E be finitely generated. Then E/E_{tor} is free. There exists a free submodule F of E such that*

$$E = E_{\text{tor}} \oplus F$$

The dimension of such a submodule F is uniquely determined.

Proof. First prove that E/E_{tor} is torsion free, then use lemma 3.6.7 and lemma 3.6.8. □

Lemma 3.6.7. *A finitely generated torsion free module is free.*

Lemma 3.6.8. *Let E, E' be modules, and assume that E' is free. Let $f\colon E \longrightarrow E'$ be surjective. Then there exist a free submodule F of E such that $f|_F$ is an isomorphism, and such that*

$$E = F \oplus \ker f$$

Definition 3.6.9. The dimension of the free module F in Theorem 3.6.6 is called the *rank* of E.

Definition 3.6.10. Let E be a module over R. For $x \in E$, the map $a \mapsto ax$ is a homomorphism of R onto the submodule generated by x, and the kernel $\mathrm{ann}(x)$ is an ideal called the *annihilator* of x. We say that $m \in R$ is a *period* of x if $(m) = \mathrm{ann}(x)$. An element $c \in R, c \neq 0$ is said to be an *exponent* for E (resp. for x) if $cE = 0$ (resp. $cx = 0$).

Let p be a rime element. We denoted by $E(p)$ the submodule of E consisting of all elements having an exponent which is a power $p^r (r \geqslant 1)$. A *$p-$submodule* of E is a submodule contained in $E(p)$.

We select once and for all a system of representatives for the prime elements of R (modulo units).

Let $m \in R, m \neq 0$. We denoted by E_m the kernel of the map $x \mapsto mx$. It consists of all elements of E having exponent m.

A module E is said to be *cyclic* if it is isomorphic to $R/(a)$ for some element $a \in R$. Without loss of generality if $a \neq 0$, one may assume that a is a product of primes in our system of representatives, and then we could say that a is the *order* of the module.

Definition 3.6.11. Let $r_1, \cdots, r_s$ be integers $\geqslant 1$. A $p-$module E is said to be of *type*

$$(p^{r_1}, \cdots, p^{r_s})$$

if it is isomorphic to the product of cyclic modules $R/(p^{r_i})$ $(i = 1, \cdots, s)$. If p is fixed, then one could say that the module is of type $(r_1, \cdots, r_s)$ (relative to p).

Definition 3.6.12. Let $y_1, \cdots, y_m$ be elements of a module, we say that they are *independent* if whenever we have a relation

$$a_1 y_1 + \cdots + a_m y_m = 0$$

with $a_i \in R$, then we must have $a_i y_i = 0$ for all i.

Warning. Observe that *independent* does not mean *linearly independent*.

Lemma 3.6.13. *Let E be a torsion module of exponent $p^r (r \geqslant 1)$ for some prime element p. Let $x_1 \in E$ be an element of period p^r. Let $\overline{E} = E/(x_1)$. Let $\overline{y}_1, \cdots, \overline{y}_m$ be independent elements of $\overline{E}$. Then for each i there exists a representative $y_i \in E$ of $\overline{y}_i$, such that the period of y_i is the same as the period of $\overline{y}_i$. The elements $x_1, y_1, \cdots, y_m$ are independent.*

Theorem 3.6.14. *Let E be a finitely generated torsion module $\neq 0$. Then E is the direct sum*

$$E = \bigoplus_p E(p)$$

taken over all primes p such that $E(p) \neq 0$. Each $E(p)$ can be written as a direct sum

$$E(p) = R/(p^{r_1}) \oplus \cdots \oplus R/(p^{r_s})$$

with $1 \leqslant r_1 \leqslant \cdots \leqslant r_s$. The sequence $r_1, \cdots, r_s$ is uniquely determined.

Theorem 3.6.15. *Let E be a finitely generated torsion module $\neq 0$. Then E is isomorphic to a direct sum of non-zero factors*

$$R/(q_1) \oplus \cdots \oplus R/(q_r)$$

where $q_1, \cdots, q_r$ are non-zero elements of R, and $q_1 | q_2 | \cdots | q_r$. The sequence of ideals $(q_1), \cdots, (q_r)$ is uniquely determined by the above conditions.

Remark. The ideals $(q_1), \cdots, (q_r)$ are called the *invariants* of E.

Theorem 3.6.16 (Elementary Divisors). *Let F be a free module, and let M be a finitely generated submodule $\neq 0$. Then there exists a basis $\mathfrak{B}$ of F, elements $e_1, \cdots, e_m$ in this basis, and non-zero elements $a_1, \cdots, a_m \in R$ such that*

(i) The elements $a_1 e_1, \cdots, a_m e_m$ form a basis of M over R.

(ii) We have $a_i | a_{i+1}$ for $i = 1, \cdots, m-1$.

The sequence of ideals $(a_1), \cdots, (a_m)$ is uniquely determined by the preceding conditions.

Remark. We call the ideals $(a_1), \cdots, (a_m)$ the *invariants* of M in F.

Theorem 3.6.17. *Assume that the elementary matrices in $R^{n \times n}$ generate $\mathrm{GL}_n(R)$. Let (c_{ij}) be a non-zero matrix with components in R. Then with a finite number of row and column operations, it is possible to bring the matrix to the form*

$$\mathrm{diag}\{a_1, a_2, \cdots, a_m, 0, \cdots, 0\}$$

with $a_1 \cdots a_m \neq 0$ and $a_1 | a_2 | \cdots | a_m$.

3.6.1 Lattice

3.4. *Let A be an additive subgroup of Euclidean space $\mathbb{R}^n$, and assume that in every bounded region of space, there is only a finite number of elements of A. Show that A is a free abelian group on $\leqslant n$ generators.*

Proof. Induction on the maximal number of linearly independent elements of A over $\mathbb{R}$.

When this number is 1, since in every bounded region of space, there is only a finite number of elements of A, there must one $a \in A$, such that $d(a,0) = \min_{x \in A \setminus \{0\}} d(x,0)$. Then it is clear that $A = \mathbb{Z}a$.

Let $v_1, \cdots, v_m$ be a maximal set of linearly independent elements of A over $\mathbb{R}$, and let A_0 be the subgroup of A contained in $\mathbb{R}-$space generated by $v_1, \cdots, v_{m-1}$. By induction, one may assume that any element of A_0 is a linear integral combination of $v_1, \cdots, v_{m-1}$.

Let S be the subset of elements $v \in A$ of the form $v = a_1 v_1 + \cdots + a_m v_m$ with real coefficients a_i satisfying

$$\begin{aligned} &0 \leqslant a_i < 1 \quad \text{if } i = 1, \cdots, m-1 \\ &0 \leqslant a_m \leqslant 1 \end{aligned}$$

Since S is in a bounded region of space, there must be an element v'_m of S with the smallest $a_m \neq 0$. It is clear that $\{v_1, \cdots, v_{m-1}, v'_m\}$ is a basis of A over $\mathbb{Z}$. □

Remark. Such A is called a *lattice* in a Euclidean space. The above exercise is applied in algebraic number theory to show that the group of units in the ring of integers of a number field modulo torsion is isomorphic to a lattice in a Euclidean space. See.

3.5 (Artin-Tate). *Let G be a finite group operating on a finite set S. For $w \in S$, denote $1 \cdot w$ by $[w]$, so that we have the direct sum*

$$\mathbb{Z}\langle S \rangle = \sum_{w \in S} \mathbb{Z}[w]$$

Define an action of G on $\mathbb{Z}\langle S \rangle$ by defining $\sigma[w] = [\sigma w]$ (for $w \in S$), and extending σ to $\mathbb{Z}\langle S \rangle$ by linearity. Let M be a subgroup of $\mathbb{Z}\langle S \rangle$ of rank $\#[S]$. Show that M has a $\mathbb{Z}-$basis $\{y_w\}_{w \in S}$ such that $\sigma y_w = y_{\sigma w}$ for all $w \in S$.

Proof. First, we consider a Euclidean space E generated by S. Then M is a lattice of this space, hence there exists a real number $r > 0$ such that for any $X \in E$, there exist a $x \in M$ such that

$$\|X - x\| < r$$

For any integer n, we can find some $\{x_v\}_{v \in S} \subset M$ such that

$$\|n[v] - x_v\| < r$$

For any $w \in S$, define y_w as follow

$$y_w = \sum_{\substack{\sigma \in G \\ \sigma v = w}} \sigma x_v$$

Then it is clear that $\sigma y_w = y_{\sigma w}$. We will show that $\{y_w\}_{w\in S}$ is a $\mathbb{R}-$basis of M.

If not, then there exist some real numbers c_w, such that

$$\sum_{w\in S} c_w y_w = 0$$

Moreover, we can assume that, some $c_w = 1$.

Let $x_v = n[v] + b_v$, then

$$\begin{aligned} 0 &= \sum_{w\in S} c_w \sum_{\substack{\sigma\in G\\ \sigma v=w}} \sigma n[v] + b_v \\ &= \sum_{w\in S} \sum_{\substack{\sigma\in G\\ \sigma v=w}} c_w n[w] + b_v \end{aligned}$$

Hence

$$n \leqslant \left\| \sum_{w\in S} \sum_{\substack{\sigma\in G\\ \sigma v=w}} c_w n[w] \right\| = \left\| \sum_{w\in S} \sum_{\substack{\sigma\in G\\ \sigma v=w}} b_v \right\| < |S||G|r$$

However, n can be large enough to make this inequality fail to hold. Thence $\{y_w\}_{w\in S}$ is a $\mathbb{R}-$basis of M, and by multiply some rational numbers, we can get a $\mathbb{Z}-$basis of M satisfying the condition. □

3.6.2 Seminorm

3.6. *Let M be a finitely generated abelian group. By a* seminorm *on M we mean a real-valued function $v \mapsto |v|$ satisfying the following properties:*

1. $|v| \geqslant 0$ *for all* $v \in M$;
2. $|nv| = |n||v|$ *for* $n \in \mathbb{Z}$;
3. $|v + w| \leqslant |v| + |w|$ *for all* $v, w \in M$.

By the kernel *of seminorm we mean the subset of elements v such that $|v| = 0$.*

a) Let M_0 be the kernel. Show that M_0 is a subgroup. If $M_0 = \{0\}$, then the seminorm is called a norm.

b) Assume that M has rank r. Let $v_1, \cdots, v_r \in M$ be linearly independent over $\mathbb{Z}$ mod M_0. Prove that there exists a basis $\{w_1, \cdots, w_r\}$ of M/M_0 such that

$$|w_i| \leqslant \sum_{j=1}^{i} |v_j|$$

Proof. a) For $v \in M_0$, by *2*, $0, -v \in M_0$. For $u, v \in M_0$, by *3*, $u + v \in M_0$.

b) Without loss of generality, we can assume $M_0 = \{0\}$.

Let $M_1 = \langle v_1, \cdots, v_r \rangle$. Let d be the exponent of M/M_1. Then dM has a finite index in M_1 ($d \geqslant [M : dM] = [M : M_1][M_1 : dM]$).

Let $n_{j,j}$ be the smallest positive integer such that there exist integers $n_{j,1}, \cdots, n_{j,j-1}$ satisfying

$$n_{j,1}v_1 + \cdots + n_{j,j}v_j = dw_j$$

for some $w_j \in M$.

Without loss of generality, we may assume $0 \leqslant n_{j,k} \leqslant d - 1$. Then $w_1, \cdots, w_r$ form the desired basis:

First, $w_1, \cdots, w_r$ obversely form a $\mathbb{R}-$basis. We need to prove that it is also a $\mathbb{Z}-$basis. For any $a \in M$, we have $a = a_1w_1 + \cdots + a_rw_r$. Without loss of generality, we can assume $0 \leqslant a_j < 1$. Hence

$$\begin{aligned} da &= a_1dw_1 + \cdots + a_rdw_r \\ &= \sum_{j=1}^{r} a_j \sum_{i=1}^{j} n_{j,i}v_i \\ &= \sum_{i=1}^{r} \sum_{j=1}^{r} a_j n_{j,i} v_i \end{aligned}$$

Notice that $0 \leqslant a_r n_{r,r} < n_{r,r}$, by the minimum of $n_{r,r}$, a_r must be 0, and the equality become

$$da = \sum_{i=1}^{r-1} \sum_{j=1}^{r-1} a_j n_{j,i} v_i$$

Since $0 \leqslant a_j n_{j,j} < n_{j,j}$, we can get all $a_j = 0$ by induction. Hence $a = 0$, which means that $w_1, \cdots, w_r$ a $\mathbb{Z}-$basis.

The desired inequality comes from

$$\begin{aligned} |w_j| &= \frac{1}{d}|n_{j,1}v_1 + \cdots + n_{j,j}v_j| \\ &\leqslant \sum_{i=1}^{j} \frac{n_{j,i}}{d}|v_i| \leqslant \sum_{i=1}^{j} |v_i| \end{aligned}$$

□

3.7. *Consider the multiplicative group $\mathbb{Q}^*$ of non-zero rational numbers. For a non-zero rational number $x = a/b$ with $a, b \in \mathbb{Z}$ and $(a, b) = 1$, define the* height

$$h(x) = \log \max(|a|, |b|)$$

a) *Show that h defines a seminorm on $\mathbb{Q}^*$, whose kernel consists of ± 1 (the torsion group).*

b) *Let M_1 be a subgroup of $\mathbb{Q}^*$, generated by $x_1, \cdots, x_m$. Let M be the subgroup of $\mathbb{Q}^*$ consisting of those elements x such that $x^s \in M_1$ for some positive integer s. Show that M is finitely generated, and using Exercise 3.6, find a bound for the seminorm of a set of generators of M in terms of the seminorms of $x_1, \cdots, x_m$.*

Proof. a) *1* is clear. For $x = a/b, (a, b) = 1$, if $n > 0$, then $(a^n, b^n) = 1$, hence

$$h(x^n) = \log \max(|a^n|, |b^n|) = \log(\max(|a|, |b|))^n = nh(x)$$

if $n < 0$, then

$$h(x^n) = \log \max(|b^{|n|}|, |a^{|n|}|) = \log(\max(|b|, |a|))^{|n|} = |n|h(x)$$

if $n = 0$, then

$$h(x^0) = \log \max(1, 1) = 1 = h(1)$$

Which proves *2*.

Let $v = a/b, w = c/d, (a, b) = (c, d) = 1$, assume $(ac, bd) = e$, then

$$\begin{aligned} h(vw) &= \log \max(|ac/e|, |bd/e|) \\ &\leqslant \log \max(|ac|, |bd|) \\ &\leqslant \log \max(|a|, |b|) + \log \max(|c|, |d|) = h(v) + h(w) \end{aligned}$$

Which is *3*.

Hence $h(x)$ is a seminorm on $\mathbb{Q}^*$.

If $h(a/b) = 0$, then $\max(|a|, |b|) = 1$, hence $|a| = |b| = 1$. So the kernel consists of ± 1.

b) For $x_i = a_i/b_i$, let a_i and b_i be factorized into power of primes $p_{i,j}$ and $q_{i,j}$ respectively. Then For any $x = a/b \in M_1$, a (resp. b) must be a product of some power of $p_{i,j}$ (resp. $q_{i,j}$).

For $x = a/b \in M$, assume $x^s \in M_1$, then a^s (resp. b^s) must be a product of some power of $p_{i,j}$ (resp. $q_{i,j}$), and hence so do a and b. Whence M must be a subgroup of the subgroup of $\mathbb{Q}^*$ which is generated by those primes.

Moreover, since for any $x \in M$, there exist a s such that $x^s \in M_1$ and hence can be written by a product of $x_1, \cdots, x_m$. This fact shows that $x_1, \cdots, x_m$ is a maximal linear independent term in M. By Exercise 3.6, the generators of $y_1, \cdots, y_m$ of M must satisfying

$$h(y_i) \leqslant \sum_{j=1}^{i} h(x_j)$$

for $i = 1, \cdots, m$. Whence we get a bound of the set of generators of M, say $\sum_{i=1}^{m} h(x_i)$. $\square$

3.7 Localization

Throughout this section, we assume that A is a commutative ring. All modules are over A unless otherwise specified.

3.8. *Let A be a commutative ring and let M be an $A-$module. Let S be a multiplicative subset of A. Define $S^{-1}M$ in a manner analogous to the one we used to define $S^{-1}A$. Show that*

a) $S^{-1}M$ is an $S^{-1}A-$module.

b) the functor $M \mapsto S^{-1}M$ is exact.

Proof. a) We consider pairs (x, s) with $x \in M$ and $s \in S$. we define a relation

$$(x, s) \sim (x', s')$$

between such pairs, by the condition that there exists an element $s_1 \in S$ such that

$$s_1(s'x - sx') = 0$$

It is then trivially verified that this is an equivalence relation, and the equivalence class containing a pair (x, s) is denoted by x/s. The set of equivalence classes is denoted by $S^{-1}M$.

We define a $S^{-1}A-$module structure on $S^{-1}M$ by

$$(a/s)(x/s') = ax/ss'$$

It is trivially verified that this is well defined. For any $a/s_1, a'/s_1' \in S^{-1}A$ and $x/s_2, x'/s_2' \in S^{-1}M$, we have the left and right distributive laws:

$$\begin{aligned}
(\frac{a}{s_1} + \frac{a'}{s_1'})\frac{x}{s_2} &= \frac{s_1'a + s_1a'}{s_1s_1'}\frac{x}{s_2} = \frac{s_1'ax + s_1a'x}{s_1s_1's_2} \\
&= \frac{ax}{s_1s_2} + \frac{a'x}{s_1's_2} = \frac{a}{s_1}\frac{x}{s_2} + \frac{a'}{s_1'}\frac{x}{s_2} \\
\frac{a}{s_1}(\frac{x}{s_2} + \frac{x'}{s_2'}) &= \frac{a}{s_1}\frac{s_2'x + s_2x'}{s_2s_2'} = \frac{s_2'ax + s_2ax'}{s_1s_2s_2'} \\
&= \frac{ax}{s_1s_2} + \frac{ax'}{s_1s_2'} = \frac{a}{s_1}\frac{x}{s_2} + \frac{a}{s_1}\frac{x'}{s_2'}
\end{aligned}$$

b) For any $A-$homomorphism $f\colon M \longrightarrow M'$, we define $S^{-1}f\colon S^{-1}M \longrightarrow S^{-1}M'$ to be

$$S^{-1}f(x/s) = f(x)/s$$

It is trivially verified that this is a $S^{-1}A-$homomophism and the following diagram is commutative:

$$\begin{array}{ccc} M & \xrightarrow{\varphi_S} & S^{-1}M \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle S^{-1}f} \\ M' & \xrightarrow[\varphi_S]{} & S^{-1}M' \end{array}$$

where φ_S is the natural map $x \mapsto x/1$. Whence S^{-1} is a functor.

Given an arbitrary short exact sequence

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

We need to show the sequence

$$0 \longrightarrow S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M'' \longrightarrow 0$$

is exact.

1) $S^{-1}f$ *is injective:* For any $S^{-1}f(x'/s) = 0/1$, there exists a $s' \in S$ such that $s'f(x') = 0$. Hence $s'x' \in \ker f$. Since f is injective, hence $s'x' = 0$, which means $x'/s = 0/1$.
2) $S^{-1}g$ *is surjective:* For any $x''/s \in S^{-1}M''$, there exists a $x \in M$ such that $g(x) = x''$ since g is surjective. Hence $S^{-1}g(x/s) = x''/s$.
3) $\ker S^{-1}g = \operatorname{im} S^{-1}f$*:* Since $g \circ f = 0$ and S^{-1} is a functor, we have $S^{-1}g \circ S^{-1}f = 0$. The rest is to show that $\ker S^{-1}g \subset \operatorname{im} S^{-1}f$: For any $x/s \in \ker S^{-1}g$, there exists a $s' \in S$ such that $s'g(x) = 0$. Hence $s'x \in \ker g$. Since $\ker g = \operatorname{im} f$, there exist a $x' \in M'$ such that $f(x') = s'x$. Whence $S^{-1}f(x'/s's) = x/s$. □

Proposition 3.7.1. *If N, P are submodules of an $A-$module M, then*

(i) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$*;*

(ii) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$*;*

(iii) $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$*.*

Proof. (i) follows from definition. *(ii)* is easy to verify: if $x/s = y/t$ ($x \in N, y \in P, s, t \in S$), then there exist a $u \in S$ such that $u(tx - sy) = 0$. Hence $w = utx = usy \in N \cap P$ and $x/s = w/ust \in S^{-1}(N \cap P)$. Consequently, $S^{-1}N \cap S^{-1}P \subset S^{-1}(N \cap P)$, and the reverse inclusion is clear.

(iii). Apply the functor S^{-1} to the following exact sequence:

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$ □

Corollary 3.7.2. $S^{-1}(M \oplus N) = S^{-1}M \oplus S^{-1}N$.

3.9. *Let $\mathfrak{p}$ be a prime ideal, define $M_{\mathfrak{p}}$ in a manner analogous to the one we used to define $A_{\mathfrak{p}}$.*

a) Show that the natural map

$$M \longrightarrow \prod M_{\mathfrak{p}}$$

of a module M into the direct product of all localizations $M_{\mathfrak{p}}$ where $\mathfrak{p}$ ranges over all maximal *ideals, is injective.*

b) Show that a sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is exact if and only if the sequence

$$0 \longrightarrow M'_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow M''_{\mathfrak{p}} \longrightarrow 0$$

is exact for all primes $\mathfrak{p}$.

c) Let A be entire and let M be torsion-free. For each prime $\mathfrak{p}$ of A show that the natural map $M \longrightarrow M_{\mathfrak{p}}$ is injective.

Proof. a) Suppose the natural map is not injective, and x is a non-zero element in its kernel, let $\mathfrak{a} = \operatorname{ann}(x)$. It is an ideal $\neq (1)$, hence must be contained in some maximal ideal $\mathfrak{m}$. But by the natural map, there exists a $s \notin \mathfrak{m}$ such that $sx = 0$ which contradicts with $\mathfrak{a} \subset \mathfrak{m}$. Whence the natural map must be injective.

b) We leave the proof to proposition 3.7.7.

c) The condition implies that $\operatorname{ann}(x) = 0$ for any $x \neq 0$. Let x be in the kernel, then there exists a $s \notin \mathfrak{p}$ such that $sx = 0$, which can be true only when $x = 0$. □

3.7.1 Local Properties

See [Atiyah, 1994] and [Eisenbud, 1995].

Definition 3.7.3. A property $\mathcal{P}$ of A (or of an $A-$module M) is said to be a *local property* if the following is true:

> A (or M) has $\mathcal{P}$ if and only if $A_{\mathfrak{p}}$ (or $M_{\mathfrak{p}}$) has $\mathcal{P}$ for each prime ideal of A.

Proposition 3.7.4. *Let M be an $A-$module, and $x \in M$. Then the following are equivalent:*

1. *$x = 0$;*
2. *$x/1 = 0/1$ in $M_\mathfrak{p}$ for all prime ideals $\mathfrak{p}$ of A;*
3. *$x/1 = 0/1$ in $M_\mathfrak{m}$ for all maximal ideals $\mathfrak{m}$ of A.*

Proof. It is clear *1)⇒2)⇒3)*. Suppose *3)*, and $x \neq 0$. Let $\mathfrak{a} = \operatorname{ann}(x)$, it is an ideal $\neq (1)$, hence must be contained in some maximal ideal $\mathfrak{m}$. But $x/1 = 0/1$ in $M_\mathfrak{m}$, there exists a $s \notin \mathfrak{m}$ such that $sx = 0$ which contradicts with $\mathfrak{a} \subset \mathfrak{m}$. □

Corollary 3.7.5. *Let M be an $A-$module. Then the following are equivalent:*

1. *$M = 0$;*
2. *$M_\mathfrak{p} = 0$ for all prime ideals $\mathfrak{p}$ of A;*
3. *$M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ of A.*

Proposition 3.7.6. *Let $f\colon M \longrightarrow N$ be an $A-$homomorphism. Then the following are equivalent:*

1. *f is a monomorphism (resp. epimorphism, isomorphism);*
2. *$f_\mathfrak{p}\colon M_\mathfrak{p} \longrightarrow N_\mathfrak{p}$ is a monomorphism (resp. epimorphism, isomorphism) for each prime ideal $\mathfrak{p}$ of A;*
3. *$f_\mathfrak{m}\colon M_\mathfrak{m} \longrightarrow N_\mathfrak{m}$ is a monomorphism (resp. epimorphism, isomorphism) for each maximal ideal $\mathfrak{m}$ of A.*

Proof. We prove only the statements for monomorphisms:

1)⇒2). $0 \to M \to N$ is exact, hence $0 \to M_\mathfrak{p} \to N_\mathfrak{p}$ is exact, i.e. $f_\mathfrak{p}$ is a monomorphism.

2)⇒3) because a maximal ideal is prime.

3)⇒1). Let M' be the kernel of f, then $0 \to M' \to M \to N$ is exact, hence so is $0 \to M'_\mathfrak{m} \to M_\mathfrak{m} \to N_\mathfrak{m}$. Then $M'_\mathfrak{m} = 0$ because $f_\mathfrak{m}$ is injective. Hence $M = 0$ by 3.7.5. Which proved f is injective. □

Proposition 3.7.7. *Let $0 \to M' \to M \to M'' \to 0$ be a sequence of $A-$modules. Then the following are equivalent:*

1. *$0 \to M' \to M \to M'' \to 0$ is exact;*
2. *$0 \to M'_\mathfrak{p} \to M_\mathfrak{p} \to M''_\mathfrak{p} \to 0$ is exact for each prime ideal $\mathfrak{p}$ of A;*

3. $0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to M''_{\mathfrak{m}} \to 0$ *is exact for each maximal ideal* $\mathfrak{m}$ *of* A.

Proof. By the exactness of the functor S^{-1}, it is clear *1)⇒2)⇒3).*

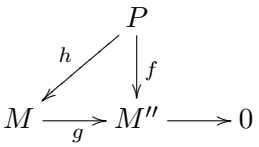
Denote $M' \longrightarrow M$ by f, and $M \longrightarrow M''$ by g.

3)⇒1). By proposition 3.7.6, we only need to prove that $\ker g = \operatorname{im} f$. It is clear that $\ker g_{\mathfrak{m}} = (\ker g)_{\mathfrak{m}}$ and $\operatorname{im} f_{\mathfrak{m}} = (\operatorname{im} f)_{\mathfrak{m}}$, hence $(\ker g)_{\mathfrak{m}} = (\operatorname{im} f)_{\mathfrak{m}}$. Hence $\ker g = \operatorname{im} f$ because the natural map $M \longrightarrow \prod M_{\mathfrak{m}}$ is injective. □

3.8 Projective Modules

Proposition 3.8.1. *Let P be a $R-$module, then the following are equivalent.*

P1 *Given a homomorphism $f\colon P \longrightarrow M''$ and surjective homomorphism $g\colon M \longrightarrow M''$, there exist a homomorphism $h\colon P \longrightarrow M$ make the following diagram commutative.*



P2 *Every exact sequence $0 \longrightarrow M' \longrightarrow M'' \longrightarrow P \longrightarrow 0$ splits.*

P3 *There exists a module M such that $P \oplus M$ is free, or in words, P is a direct summand of a free module.*

P4 *The functor $M \mapsto \mathrm{Hom}_R(P, M)$ is exact.*

Definition 3.8.2. A *projective module* is a module satisfying *P1*.

Proposition 3.8.3. *Direct sums and direct summands of projective modules are projective.*

Warning. Submodules of projective modules need not be projective; a ring R for which every submodule of a projective left module is projective is called left *hereditary*.

Proposition 3.8.4. *In principal domains or local rings, projective modules and free modules coincide.*

Proof. It is clear that projective is torsion-free, hence free over a principal domain by Theorem 3.6.6. The local ring case is a deep theorem by Irving Kaplansky, see [Kaplansky, 1958], but the finite generated case is just a corollary to Nakayama's lemma. □

Remark. There may be other rings over which the similar statement is true. For example, for polynomial rings over a field, any finite projective module is free. This is Quillen-Suslin theorem, see Chapter 21, Theorem 3.7.

Definition 3.8.5. A module is called locally free if its every localization is free.

Corollary 3.8.6. *Projective module is locally free.*

Proof. It is clear that a localization of a projective module is a projective module over a local ring, hence is free. □

Warning. The converse is not always true.

3.8.1 Grothendieck Group

Let A be a ring. Isomorphism classes of finite[1] projective modules form an abelian monoid. The addition is defined by

$$[P] + [Q] \stackrel{\text{def}}{=} [P \oplus Q]$$

The corresponding *Grothendieck group* is denoted by $K(A)$.

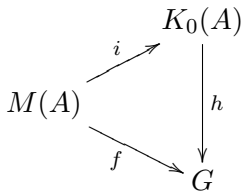
We define an equivalence relation (which is called *stably isomorphic*) $\sim$ as follow: $P \sim P'$ if there exist finite free modules F, F' such that $P \oplus F \cong P' \oplus F'$. Under this equivalence relation we obtain another group denoted by $K_0(A)$.

Proposition 3.8.7. $K(A) = K_0(A)$

Proof. It suffices to show that $K_0(A)$ satisfying the universal property of $K(A)$.

Let $M(A)$ be the monoid of isomorphism classes of finite projective modules. Let $i\colon M(A) \longrightarrow K_0(A)$ be $[M] \mapsto [[M]]$ where the $[[M]]$ denotes the equivalent class contains M. This map is well-defined since any isomorphic modules must be stably isomorphic.

Let G be an arbitrary abelian group, and f be a homomorphism from $M(A)$ to G. We need to show that there exists a unique homomorphism $h\colon K_0(A) \longrightarrow G$ satisfying the commutative diagram:



Uniqueness. Let h, h' be two homomorphisms satisfying the commutative diagram, then for any $[M] \in M(A)$, $h([[M]]) = h'([[M]])$. □

Warning. Since the monoid-homomorphism from an abelian monoid to its Grothendieck group may not be injective in general, two finite projective modules which are isomorphic may not be stably isomorphic.

A family of modules $\mathfrak{F}$ is called *exact* if for any short exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$, $M \in \mathfrak{F}$ if and only if $M', M'' \in \mathfrak{F}$.

Let $\mathcal{F}$ be the free abelian group generated by isomorphism classes of modules in $\mathfrak{F}$. Let Γ be the subgroup generated by all elements

$$[M'] - [M] + [M'']$$

[1] finitely generated

for which there exist an exact sequence $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$.

The factor group $\mathcal{F}/\Gamma$ is called the *Grothendieck group* $K(R)$.

More general, one can consider Grothendieck group of an exact category.

By an *exact category* $\mathcal{A}$, we mean an additive category together with a class of distinguished short sequences $A \longrightarrow B \longrightarrow C$ which are called "exact sequences".

It is defined in the same way as before as the abelian group with one generator $[M]$ for each isomorphism class of objects in the category and one relation

$$[A] - [B] + [C] = 0$$

for each exact sequence $A \longrightarrow B \longrightarrow C$.

3.8.2 Euler-Poincaré Maps

Definition 3.8.8. Let A be a ring and Γ is an abelian group. An *Euler-Poincaré mapping* is a corresponding φ from an exact family of $A-$modules, or a Serre subcategory of $\mathbf{Mod}_A$, to Γ such that: for any short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

we have

$$\varphi(M) = \varphi(M') + \varphi(M'')$$

Definition 3.8.9. If M is a module, then a sequence of submodules

$$M = M_1 \supset M_2 \supset \cdots \supset M_r = 0$$

is called a *finite filtration*, and r is called the *length* of the filtration.

Definition 3.8.10. A module M is said to be *simple* if $M \neq 0$ and if it does not contain any submodule other than 0 and M. A filtration is called *simple* if each M_i/M_{i+1} is simple.

Theorem 3.8.11 (Jordan-Hölder Theorem). *Two simple filtrations of a module are equivalent.*

Definition 3.8.12. A module M is said to be *of finite length* if it is 0 or if it admits a simple finite filtration. The length of such a simple filtration is called the *length* of the module.

Theorem 3.8.13. *Let φ be an rule which to each simple module associates an element of an abelian group Γ, and such that if $M \cong M'$ then*

$$\varphi(M) = \varphi(M')$$

Then φ has a unique extension to an Euler-Poincaré mapping defined on all modules of finite length.

Proof. Given a simple filtration

$$M = M_1 \supset M_2 \supset \cdots \supset M_r = 0$$

we define

$$\varphi(M) = \sum_{i=1}^{r-1} \varphi(M_i/M_{i+1}) \qquad \square$$

3.8.3 Projective Modules over Dedekind Rings

Let $\mathfrak{o}$ be a Dedekind ring and K its quotient field.

3.10. *Let M be a finitely generated torsion-free module over $\mathfrak{o}$. Prove that M is projective.*

Proof. Given a prime ideal $\mathfrak{p}$, the localized module $M_\mathfrak{p}$ is finitely generated torsion-free over $\mathfrak{o}_\mathfrak{p}$, which is principal. Then $M_\mathfrak{p}$ is projective, so if F is finite free over $\mathfrak{o}$, and $f\colon F \to M$ is a surjective homomorphism, then $f_\mathfrak{p}\colon F_\mathfrak{p} \to M_\mathfrak{p}$ has a splitting $g_\mathfrak{p}\colon M_\mathfrak{p} \to F_\mathfrak{p}$. There exists $c_\mathfrak{p} \in \mathfrak{o}$ such that $c_\mathfrak{p} \notin \mathfrak{p}$ and $c_\mathfrak{p} g_\mathfrak{p}(M) \subset F$ because $g_\mathfrak{p}(M)$ is finitely generated. The family $\{c_\mathfrak{p}\}$ generates the unit ideal $\mathfrak{o}$: if not then $\{c_\mathfrak{p}\}$ generates an proper ideal hence belongs to some maximal ideal $\mathfrak{m}$, but $c_\mathfrak{m} \notin \mathfrak{m}$ which is a contradiction. So there is a finite number of elements $c_{\mathfrak{p}_i}$ and elements $x_i \in \mathfrak{o}$ such that $\sum x_i c_{\mathfrak{p}_i} = 1$. Let

$$g = \sum x_i c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}$$

Then $g\colon M \to F$ is a homomorphism, and $f \circ g = f \circ (\sum x_i c_{\mathfrak{p}_i} g_{\mathfrak{p}_i}) = \sum x_i f \circ c_{\mathfrak{p}_i} g_{\mathfrak{p}_i} = \sum x_i c_{\mathfrak{p}_i} f_{\mathfrak{p}_i} \circ g_{\mathfrak{p}_i} = \sum x_i c_{\mathfrak{p}_i} \mathrm{id}_{\mathfrak{p}_i} = \mathrm{id}$. $\square$

3.11. *a) Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Show that there is an isomorphism:*

$$\mathfrak{a} \oplus \mathfrak{b} \xrightarrow{\cong} \mathfrak{o} \oplus \mathfrak{a}\mathfrak{b}$$

b) Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals, and let $f\colon \mathfrak{a} \to \mathfrak{b}$ be an isomorphism (as $\mathfrak{o}-$modules, of course). Then f has an extension to a $K-$linear map $f_K\colon K \to K$. Let $c = f_K(1)$. Show that $\mathfrak{b} = c\mathfrak{a}$ and that f is given by the mapping $m_c\colon x \mapsto cx$.

c) Let $\mathfrak{a}$ be a fractional ideal. For each $b \in \mathfrak{a}^{-1}$ the map $m_b\colon \mathfrak{a} \to \mathfrak{o}$ is an element of the dual $\mathfrak{a}^\vee$. Show that $\mathfrak{a}^{-1} = \mathfrak{a}^\vee$ under this map, and so $\mathfrak{a}^{\vee\vee} = \mathfrak{a}$.

Proof. a) Assume $\mathfrak{a}, \mathfrak{b}$ are relatively prime. Then $\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$ and $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$. Consider the canonical map from $\mathfrak{a} \oplus \mathfrak{b}$ to $\mathfrak{a} + \mathfrak{b}$, we get the following exact sequence:

$$0 \longrightarrow \mathfrak{a}\mathfrak{b} \longrightarrow \mathfrak{a} \oplus \mathfrak{b} \longrightarrow \mathfrak{o} \longrightarrow 0$$

Since $\mathfrak{o}$ is a free $\mathfrak{o}-$module, $\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{o} \oplus \mathfrak{ab}$.

As for the general case, thanks to Exercise 2.19, there exists a $c \in K$ such that $c\mathfrak{a}$ is relatively prime to $\mathfrak{b}$. Hence we have

$$\mathfrak{a} \oplus \mathfrak{b} \cong c\mathfrak{a} \oplus \mathfrak{b} \cong \mathfrak{o} \oplus c\mathfrak{ab} \cong \mathfrak{o} \oplus \mathfrak{ab}$$

b) For any $x \in \mathfrak{a}$, we have $c = f_K(1) = f_K(x^{-1}x) = x^{-1}f(x)$ since f_K is a $K-$linear map and an extension of f. Hence $f(x) = cx$, which proved the statements since f is an isomorphism.

c) The map $b \mapsto m_b$ is clearly injective and a $\mathfrak{o}-$homomorphism. It suffices to show that it is surjective. For any $f \in \mathfrak{a}^\vee$, by *b)*, there exists a $c \in K$ such that $f = m_c$ and $c\mathfrak{a} \subset \mathfrak{o}$. Since $\mathfrak{a}^{-1} = \{c \in K | c\mathfrak{a} \subset \mathfrak{o}\}$ (if $c\mathfrak{a} \subset \mathfrak{o}$, then $c\mathfrak{a}\mathfrak{a}^{-1} \subset \mathfrak{a}^{-1}$, hence $c \in \mathfrak{a}^{-1}$), we have $c \in \mathfrak{a}^{-1}$. □

3.12. *a) Let M be a projective finite module over the Dedekind ring $\mathfrak{o}$. Show that there exist free modules F and F' such that $F \supset M \supset F'$, and F, F' have the same rank, which is called the* rank *of M.*

b) Prove that there exists a basis $\{e_1, \cdots, e_n\}$ of F and ideals $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ such that $M = \mathfrak{a}_1 e_1 + \cdots + \mathfrak{a}_n e_n$, or in other words, $M = \bigoplus \mathfrak{a}_i$.

c) Prove that $M \cong \mathfrak{o}^{n-1} \oplus \mathfrak{a}$ for some ideal $\mathfrak{a}$, and that the association $M \mapsto \mathfrak{a}$ induces isomorphism of $K_0(\mathfrak{o})$ with the group of ideal classes $\mathrm{Pic}(\mathfrak{o})$.

Proof. a) Let $x_1, \cdots, x_n$ generated M, then there exists a maximal linear independent subterm, say $x_1, \cdots, x_k$, then $F' = \langle x_1, \cdots, x_k \rangle \subset M$. For any $x_i, k < i \leqslant n$, assume that $a_i x_i \in F'$, then there exists a $c \in K$ such that $x_i \in F = \langle cx_i, \cdots, cx_k \rangle$ for any $1 \leqslant i \leqslant n$. Hence $F' \subset M \subset F$ and $\mathrm{rank}(F) = \mathrm{rank}(F')$.

b) Let $p_i \colon F \to \mathfrak{o}$ be the projection from F to the $i-$th coefficient, then $p_i(M) = \mathfrak{a}_i$ is an ideal of $\mathfrak{o}$. It is then clear that $M = \mathfrak{a}_1 e_1 \cdots + \mathfrak{a}_n e_n$.

c) By Exercise 3.11, there exists an ideal $\mathfrak{a}$ such that $M \cong \mathfrak{o}^{n-1} \oplus \mathfrak{a}$, and the map $M \mapsto \mathfrak{a}$ is a homomorphism. Since every ideal is a projective module, the map is clearly surjective. It suffices to show that if $M \cong \mathfrak{o}^n \oplus \mathfrak{a}$, $N \cong \mathfrak{o}^m \oplus \mathfrak{b}$ and $[\mathfrak{a}] = [\mathfrak{b}]$ in $\mathrm{Pic}(\mathfrak{o})$, then $[M] = [N]$ in $K_0(\mathfrak{o})$.

$[\mathfrak{a}] = [\mathfrak{b}]$ means there exists a principal fractional ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{c}\mathfrak{a}$. Hence $N \cong \mathfrak{o}^m \oplus \mathfrak{c}\mathfrak{a} \cong \mathfrak{o}^{m-1} \oplus \mathfrak{c} \oplus \mathfrak{a}$. But $\mathfrak{c}$ is clearly a free module. Hence there exist free modules F and F' such that $M \oplus F \cong \mathfrak{o}^r \oplus \mathfrak{a} \cong N \oplus F'$, which means $[M] = [N]$ in $K_0(\mathfrak{o})$. □

3.9 Inverse Limits

Theorem 3.9.1. *Inverse limits exist in the category of groups., in the category of modules over a ring, and also in the category of rings.*

3.13. *Prove that the inverse limit of a system of simple groups in which the homomorphisms are surjective is either the trivial group, or a simple group.*

Proof. For any homomorphism ϕ in this system, since ϕ is surjective and its domisn is simple, ϕ must be isomorphism or trivial. If all homomorphisms are isomorphism, then it is clear that the limit is isomorphic to the groups in system, which are simple, or trivial. If not, there must be one trivial homomorphism whose codomain is trivial since it is surjective. Consider the commutative diagram below

$$\begin{array}{ccc} \varprojlim G & \longrightarrow & G_i \\ {\scriptstyle 1 \mid 0}\uparrow\downarrow & \searrow^{0} & \downarrow{\scriptstyle 0} \\ \varprojlim G & \xrightarrow[0]{} & G_j \end{array}$$

where 0 denote the trivial homomorphisms and 1 denote the isomorphism. By the universality of $\varprojlim G$, $1 = 0$, hence $\varprojlim G$ is trivial. □

Definition 3.9.2. Let A be a commutative ring and I a proper ideal. Define a *$I-$Cauchy sequence* $\{x_n\}$ to be a sequence of elements of A satisfying the following condition:

Given a positive integer k, there exists N such that for all $n, m \geqslant N$ we have $x_n - x_m \in I^k$.

Define a *null sequence* to be a sequence for which given k there exists N such that for all $n \geqslant N$ we have $x_n \in I^k$.

Proposition 3.9.3. *Define addition and multiplication of sequences termwise. Then the $I-$Cauchy sequences form a ring $\mathcal{C}$, the null sequences form an ideal $\mathcal{N}$.*

Definition 3.9.4. The factor ring $\mathcal{C}/\mathcal{N}$ is called the *$I-$adic completion* of A.

Proposition 3.9.5. *There is a natural isomorphism*

$$\mathcal{C}/\mathcal{N} \cong \varprojlim A/I^n$$

Definition 3.9.6. Let p be a prime number. For $n \geqslant m$ we have a canonical surjective ring homomorphism

$$\phi_m^n \colon \mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^m\mathbb{Z}$$

The projective limit is called the ring of $p-$adic integers, and denoted by $\mathbb{Z}_p$.

Warning. $\mathbb{Z}_p$ is not isomorphic to $\mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at (p). In fact, $\mathbb{Z}_p$ has the cardinality of the continuum! By the way, $\mathbb{Z}_p$ is the completion of $\mathbb{Z}_{(p)}$ at the unique maximal ideal $p\mathbb{Z}_{(p)}$.

3.14. *a) Let n range over the positive integers and let p be a prime number. Show that the abelian groups $A_n = \mathbb{Z}/p^n\mathbb{Z}$ form a projective system under the canonical homomorphisms. Let $\mathbb{Z}_p$ be its inverse limit. Show that $\mathbb{Z}_p$ maps surjectively on each $\mathbb{Z}/p^n\mathbb{Z}$; that $\mathbb{Z}_p$ has no divisors of 0, and has a unique maximal ideal generated by p. Show that $\mathbb{Z}_p$ is factorial, with only one prime, namely p itself.*

b) Next consider all ideals of $\mathbb{Z}$ as forming a directed system, by divisibility. Prove that

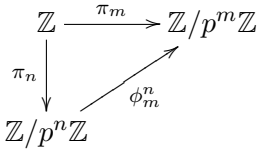
$$\varprojlim_{(a)} \mathbb{Z}/(a) = \prod_p \mathbb{Z}_p$$

where the limit is taken over all ideals (a), and the product is taken over all primes p.

Proof. a) We prove the statements one by one.

1). The abelian groups A_n form a projective system under the canonical homomorphisms.

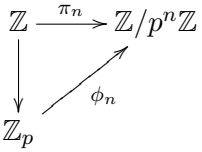
For $n \geqslant m$, ϕ_m^n is the quotient of π_m induced by π_n, where π_n is the canonical map from $\mathbb{Z}$ to $\mathbb{Z}/p^n\mathbb{Z}$.



By the uniqueness of quotient, $\phi_k^j \circ \phi_j^i = \phi_k^i$ for any $i \leqslant j \leqslant k$. Hence the abelian groups A_n form a projective system under the canonical homomorphisms.

2). $\mathbb{Z}_p$ maps surjectively on each A_n.

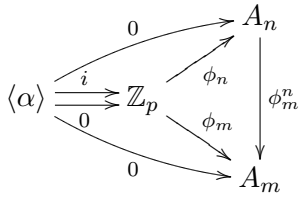
By the discuss above, $(\mathbb{Z}, \pi_n)$ is also a cone of (A_n, ϕ_m^n), hence there exists a unique morphism from $(\mathbb{Z}, \pi_n)$ to the inverse limit $(\mathbb{Z}_p, \phi_n)$. Consider an arbitrary commutative diagram in this morphism:



Since π_n is surjective, hence so is ϕ_n.

3). A $p-$adic integer α equals to 0 if and only if $\phi_n(\alpha) = 0$ for all n.

Let $\langle\alpha\rangle$ be the subring of $\mathbb{Z}_p$ generated by α. Then $(\langle\alpha\rangle, 0)$ is a cone of (A_n, ϕ_m^n), hence there exists a unique morohism from $(\langle\alpha\rangle, 0)$ to $(\mathbb{Z}_p, \phi_n)$. However, both 0 and the inclusion i satisfying the commutative diagrams, hence $i = 0$, i.e. $\alpha = 0$.



4). $\mathbb{Z}_p$ has no divisors of 0.

Let α, β be two non-zero $p-$adic integers, by the discuss above, when n is large enough, we have $\phi_n(\alpha) \neq 0$ and $\phi_n(\beta) \neq 0$. Taking l, m to be the largest integers such that p^l, p^m divide $\phi_n(\alpha)$ and $\phi_n(\beta)$ respectively. then for any $N \geqslant n$, the same statements hold for $\phi_N(\alpha)$ and $\phi_N(\beta)$. Therefore, we can assuming n is larger than $l + m$, and hence $\phi_n(\alpha)\phi_n(\beta) \neq 0$, which implies $\alpha\beta \neq 0$. That shows $\mathbb{Z}_p$ has no divisors of 0.

5). Any $p-$adic integer can be uniquely determined by a sequence $x_n \in A_n$ such that

$$x_{n+1} \equiv x_n \mod p^n$$

For any $x_n \in A_n$, since $\mathbb{Z}_p$ maps surjectively on each A_n, there exist a $p-$adic integer α, such that $\phi_n(\alpha) = x_n$. To show that we can choose the same α satisfying $\phi_m(\alpha) = x_m$ for any m, it suffices to check that $\phi_m^n(x_n) = (x_m)$ for all m, n, which are nothing but the congruences above. The uniqueness comes from *3).*

6). A $p-$adic integer α, which is determined by a sequence $x_n \in A_n$, is unit if and only if $x_1 \not\equiv 0 \mod p$.

Let α be a unit, then there exists a $p-$adic integer β such that $\alpha\beta = 1$. Let β be determined by a sequence $y_n \in A_n$, then

$$x_n y_n \equiv 1 \mod p^n$$

In particular, $x_1 y_1 \equiv 1 \mod p$, hence $x_1 \not\equiv 0 \mod p$.

Conversely, let $x_1 \not\equiv 0 \mod p$, then it is easy to show that

$$x_n \equiv x_{n-1} \equiv \cdots \equiv x_1 \not\equiv 0 \mod p$$

Therefore, for any n we can find a y_n satisfying $x_n y_n \equiv 1 \mod p^n$. Since $x_{n+1} \equiv x_n \mod p^n$ and $x_{n+1} y_{n+1} \equiv x_n y_n \mod p^n$, then also $y_{n+1} \equiv y_n$

mod p^n. This means the sequence $y_n \in A_n$ determined a $p-$adic integer β, and by the congruences above, $\alpha\beta = 1$.

7). $\mathbb{Z}_p$ has a unique maximal ideal generated by p.

By *6)*, any $\alpha \notin p\mathbb{Z}_p$ is a unit, hence $p\mathbb{Z}_p$ is the unique maximal ideal.

8). $\mathbb{Z}_p$ is factorial, with only one prime, namely p itself.

Let α be an arbitrary non-zero $p-$adic integer, we need to show that α can be uniquely written in the form $p^m\varepsilon$, where ε is a unit.

If α is a unit, then the statement is true. Assume not, let α be determined by $x_n \in A_n$. Then, by *6)*, $x_1 \equiv 0 \mod p$. Since $\alpha \neq 0$, by *3)*, the congruences $x_n \equiv 0 \mod p^n$ can not hold for all n. Let $m+1$ be the smallest index for which

$$x_{m+1} \not\equiv 0 \mod p^{m+1}$$

Then, for $s > 0$

$$x_{m+s} \equiv x_m \mod p^m$$

and therefore $y_s = x_{m+s}/p^m$ is an integer. From the congruences

$$p^m y_{s+1} - p^m y_s = x_{m+s+1} - x_{m+s} \equiv 0 \mod p^{m+s}$$

it follows that

$$y_{s+1} \equiv y_s \mod p^s$$

for all $s > 0$. Thus the sequence y_s determine a $p-$adic integer ε. Since $y_1 = x_{m+1}/p^m \not\equiv 0 \mod p$, by *6)*, ε is a unit. Finally, from

$$p^m y_s = x_{m+s} \equiv x_s \mod p^s$$

it follows that $p^m\varepsilon = \alpha$ as desired.

We assume now α can be also written as $\alpha = p^k\eta$, where η is a unit. Let η be determined by $z_n \in A_n$, then

$$p^m y_s \equiv p^k z_s \mod p^s$$

for all $s > 0$, and by *6)*, p never divides y_s or z_s since ε, η are unit. From the congruence

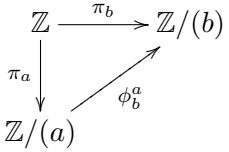
$$p^k z_{m+1} \equiv p^m y_{m+1} \not\equiv 0 \mod p^{m+1}$$

it follows that $k \leqslant m$. By symmetry, we have $m \leqslant k$, hence $k = m$. Therefore

$$p^m\varepsilon = \alpha = p^m\eta$$

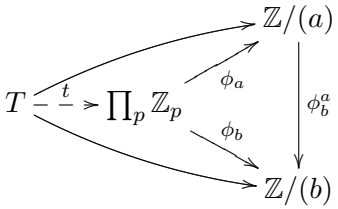
which implies $\varepsilon = \eta$ by *4)*.

b) First, we consider the structure of the inverse system of $\mathbb{Z}/(a)$. For any ideals $(a), (b)$ of $\mathbb{Z}$, there exist a homomorphism $\phi_b^a \colon \mathbb{Z}/(a) \longrightarrow \mathbb{Z}/(b)$ in this system if and only if it is induced from π_b by π_a:



if and only if $(a) \subset \ker \pi_b$, if and only if $b \mid a$.

To prove our statement, it suffices to check that $\prod_p \mathbb{Z}_p$ satisfying the universal property of $\varprojlim \mathbb{Z}/(a)$. Therefore, we need to show the existence and uniqueness of t for any T satisfying the following commutative diagram:

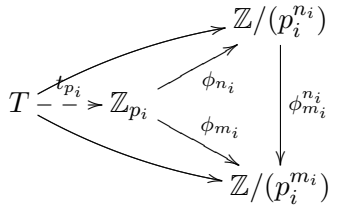


Let $a = p_1^{n_1} \cdots p_s^{n_s}, b = p_1^{m_1} \cdots p_s^{m_s}$ where $p_1, p_2, \cdots, p_s$ are distinct primes and $n_i \geqslant m_i$ for all $1 \leqslant i \leqslant s$. Then $(a) = \bigcap (p_i^{n_i})$ and $(b) = \bigcap (p_i^{m_i})$.

Hence, by the Chinese Remainder Theorem,

$$\mathbb{Z}/(a) = \prod_i \mathbb{Z}/(p_i^{n_i}) \qquad \mathbb{Z}/(b) = \prod_i \mathbb{Z}/(p_i^{m_i})$$

Hence the diagram above is just the product of the following commutative diagrams:



Hence t is the product of t_p, where each t_p uniquely exists and the product is taken over all primes p. Thus t uniquely exists. □

3.9.1 Mittag-Leffler Condition

Definition 3.9.7. A *morphism* between inverse system is just a natural transformation between them.

Definition 3.9.8. In an abelian category $\mathcal{C}$, a sequence of inverse systems indexed by the same index I

$$0 \longrightarrow (A_i) \longrightarrow (B_i) \longrightarrow (C_i) \longrightarrow 0$$

is said to be *exact* if the corresponding sequence of abelian groups is exact for each i.

Remark. $\mathcal{C}^I$ is also abelian, the definition for exact sequence of $I-$system coincide with concept of exact sequence in the abelian category $\mathcal{C}^I$.

Proposition 3.9.9. *Taking inverse limit is a left exact functor* $\mathcal{C}^I \longrightarrow \mathcal{C}$.

Proof. Draw a commutative diagram, then the it is trivial to verify. □

Warning. $\varprojlim$ is, in general case, not right exact, since you can't descent the limit cokernel to the termwise cokernels.

If I is ordered (not simply partially ordered) and countable, and $\mathcal{C}$ is the category **Ab** of abelian groups, the *Mittag-Leffler condition* is a condition on the transition morphisms ϕ_j^i that ensures the exactness of $\varprojlim$.

Specifically, Eilenberg constructed a functor

$$\varprojlim{}^1 \colon \mathbf{Ab}^I \longrightarrow \mathbf{Ab}$$

(pronounced "lim one") such that if (A_i), (B_i), and (C_i) are three projective systems of abelian groups, and

$$0 \longrightarrow (A_i) \longrightarrow (B_i) \longrightarrow (C_i) \longrightarrow 0$$

is a short exact sequence of inverse systems, then

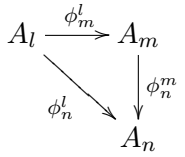
$$0 \longrightarrow \varprojlim A_i \longrightarrow \varprojlim B_i \longrightarrow \varprojlim C_i \longrightarrow \varprojlim{}^1 A_i$$

is an exact sequence in **Ab**.

Definition 3.9.10. If the ranges of the morphisms of the inverse system of sets (A_n, ϕ_n^m) are *stationary*, that is, for every n there exists $m \geqslant n$ such that for all $l \geqslant m$, $\operatorname{im} \phi_n^l = \operatorname{im} \phi_n^m$ one says that the system satisfies the *Mittag-Leffler condition* [2]. Denote **M. L.** to simplify the expressed.

[2] *Why the Mittag-Leffler condition is so named?* This condition comes from Bourbaki's Algebra [Bourbaki, 1998a], but the name first appear in Bourbaki's General Topology, Chapter II, section 3.5 [Bourbaki, 1998b]. The main theorem is attributed to Mittag-Leffler, and is concerned with inverse systems of "complete Hausdorff uniform spaces". The Mittag Leffler condition mentioned there says the functions in the system have dense image. The usual theorem about inverse limits is a corollary, for sets with the "discrete uniformity". Classical Mittag-Leffler is given as an example of the main theorem. The spaces there are essentially holomorphic functions on balls centred at 0, continuous on the boundary, with the uniform metric. — `http://mathoverflow.net/questions/14717/mittag-leffler-condition-whats-the-origin-of-its-name`

In fact, by the commutative diagram below, $(l \geqslant m \geqslant n)$



It is clear that $\operatorname{im}\phi_n^l \subset \operatorname{im}\phi_n^m$ is always true, hence form a *descending chain*:

$$A_n = \operatorname{im}\phi_n^n \supset \operatorname{im}\phi_n^{n+1} \supset \cdots \supset \operatorname{im}\phi_n^m \supset \cdots$$

Then **M. L.** says nothing but the chains are finite for all n.

Suppose (A_n) satisfying **M. L.** and each A_n is non-trivial. Let $A'_n = \bigcap_{m \geqslant n} \operatorname{im}\phi_n^m$. Then (A'_n) is also an inverse system with non-trivial terms and $\varprojlim A'_n \cong \varprojlim A_n$. Moreover, each $\phi_n^m \colon A'_m \longrightarrow A'_n$ is surjective. Hence $\varprojlim A'_n$ must be non-trivial.

Example. The following situations are examples satisfying **M. L.**:

- a system in which the morphisms ϕ_n^m are surjective.
- a system of finite-dimensional vector spaces.
- a system of finite-length $A-$modules.

Let's return to consider the inverse system of **abelian groups**, here is an important theorem:

Theorem 3.9.12. *If* (A_i) *satisfying* **M. L.**, *then* $\varprojlim{}^1 A_i = 0$.

Proof. Consider an arbitrary exact sequence:

$$0 \longrightarrow (A_i) \xrightarrow{f_i} (B_i) \xrightarrow{g_i} (C_i) \longrightarrow 0$$

It suffices to show that $\varprojlim g_i$ is surjective.

For any $c \in \varprojlim C_i$, let (c_i) be its corresponding sequence. By the short exact sequence of $i-$terms, each $D_i = g_i^{-1}(c_i)$ is non-trivial, moreover, a coset of A_i in B_i. Therefore (D_i) also form an inverse system (of sets) satisfying **M. L.**. Hence $\varprojlim D_i$ is non-trivial. But any element of $\varprojlim D_i$ lies in $\varprojlim B_i$ and is mapped to c, this proves $\varprojlim g_i$ is surjective as desired. □

Example. Taking I to be the non-negative integers, letting $A_i = p^i\mathbb{Z}, B_i = \mathbb{Z}$, and $C_i = \mathbb{Z}/p^i\mathbb{Z}$. Then

$$\varprojlim{}^1 A_i = \mathbb{Z}_p/\mathbb{Z}$$

This shows that $(p^i\mathbb{Z})$ dissatisfies **M. L.**, in fact, $\varprojlim p^i\mathbb{Z} = 0$.

Proposition 3.9.14. *If (A_i) satisfying* **M. L.**, *then we have an exact sequence*

$$0 \longrightarrow \varprojlim A_i \longrightarrow \prod A_i \xrightarrow{1-\phi} \prod A_i \longrightarrow 0$$

where the map ϕ is the product of ϕ_{i-1}^i.

Proof. For any N large enough, the sequence below is exact:

$$0 \longrightarrow \varprojlim_{1 \leqslant i \leqslant N} A_i \longrightarrow \prod_{i=1}^{N} A_i \xrightarrow{1-\phi} \prod_{i=1}^{N} A_i \longrightarrow 0$$

Moreover, the left terms satisfies **M. L.** since (A_i) satisfies. Hence the sequence in proposition is exact. □

3.15. *a) Let (A_n) be an inverse system of commutative rings, and let (M_n) be an inverse system of modules, each M_n is a module over A_n such that the following diagram is commutative:*

$$\begin{array}{ccccc} A_{n+1} & \times & M_{n+1} & \longrightarrow & M_{n+1} \\ \downarrow & & \downarrow & & \downarrow \\ A_n & \times & M_n & \longrightarrow & M_n \end{array}$$

Show that $\varprojlim M_n$ is a module over $\varprojlim A_n$.

b) Let M be a $p-$divisible group. Show that $T_p(M)$ is a module over $\mathbb{Z}_p$.

c) Let M, N be $p-$divisible groups. Show that $T_p(M \oplus N) = T_p(M) \oplus T_p(N)$, as modules over $\mathbb{Z}_p$.

Proof. a) It is clear.

b) $M[p^n]$ is a module over $\mathbb{Z}/p^n\mathbb{Z}$. Then by *a)*, $T_p(M) = \varprojlim M[p^n]$ is a module over $\mathbb{Z}_p$.

c) It is easy to check that $M \oplus N[p^n] = M[p^n] \oplus N[p^n]$. Then $T_p(M \oplus N) = T_p(M) \oplus T_p(N)$. □

3.10 Direct Limit

The direct limit of the direct system (A_i, ϕ_j^i) is can be constructed by the coproduct of the A_i modulo a certain subobject:

$$\varinjlim A_i = \coprod A_i \Big/ N$$

Here, N is generated by all x_j^i, $i \leqslant j$, defined below:

For any $x_i \in A_i$, $x_j^i = \imath(x_i) - \imath(\phi_j^i(x_i))$, where $\imath$ is the canonical injection $A_i \hookrightarrow \coprod A_i$.

Hence, if $x_i \in A_i$ and $x_j \in A_j$, then $\imath(x_i) = \imath(x_j)$ if there is some k such that $\phi_k^i(x_i) = \phi_k^j(x_j)$. Heuristically, two elements in the coproduct are equivalent if and only if they "eventually become equal" in the direct system.

3.16. *Let (A_i, ϕ_j^i) be a directed system of modules. Let $a_k \in A_k$ for some k, and suppose that the image of a_k in the direct limit A is 0. Show that there exists some index $j \geqslant k$ such that $\phi_j^k(a_k) = 0$.*

3.17. *Let I, J be two directed sets, and give the product $I \times J$ as the product of categories. Let A_{ij} be a $I \times J-$system of abelian groups. Show that the direct limits*

$$\varinjlim_i \varinjlim_j A_{ij} \qquad \textit{and} \qquad \varinjlim_j \varinjlim_i A_{ij}$$

are naturally isomorphic. State and prove the same result for inverse limits.

Proof. This follows immediately from Proposition A.3.32, i.e.

$$\mathbf{Ab}^{I \times J} \simeq (\mathbf{Ab}^J)^I \simeq (\mathbf{Ab}^I)^J$$ □

3.18. *The functor $\varinjlim\colon \mathbf{Mod}_R^I \longrightarrow \mathbf{Mod}_R$ is exact.*

Proof. Consider an arbitrary exact sequence:

$$0 \longrightarrow (M_i') \xrightarrow{f_i} (M_i) \xrightarrow{g_i} (M_i'') \longrightarrow 0$$

Only the injectivity of $f = \varinjlim f_i$ is non-trivial.

Assume $f(x) = 0$, we need to show $x = 0$. Let (x_i) be the corresponding sequence of x, Then, the image of $f_i(x_i)$ in $\varinjlim M_i$ is 0, by Exercise 3.16, there exists some index $j \geqslant i$ such that $\phi_j^i(f_i(x_i)) = 0$. Therefore $f_j(\phi_j^i(x_i)) = 0$. But f_j is injective, hence $\phi_j^i(x_i) = 0$. Therefore $\imath(x_i) = \imath(x_i) - \imath(\phi_j^i(x_i)) \in N$, which shows $x = 0$ as desired. □

3.19. *a) Let $\{M_i\}$ be a family of modules. For any module N show that*

$$\mathrm{Hom}(\bigoplus M_i, N) = \prod \mathrm{Hom}(M_i, N)$$

b) Show that

$$\mathrm{Hom}(N, \prod M_i) = \prod \mathrm{Hom}(N, M_i)$$

Proof. *a)* is a special case of Proposition A.5.18, while *b)* is a special case of Proposition A.5.19, here $\mathcal{J}$ is the discrete index set of $\{M_i\}$. □

3.20. *Let (M_i) be an inverse system of modules. For any module N show that*

$$\mathrm{Hom}(N, \varprojlim M_i) = \varprojlim \mathrm{Hom}(N, M_i)$$

Proof. This is again a special case of Proposition A.5.19, here $\mathcal{J}$ is the index set (which is a FPOS) of (M_i). □

3.21. *Show that any module is a direct limit of finitely generated submodules.*

Proof. The finitely generated submodules of a module M form a directed system under the order of containing. Then M induces a cocone of this system by the inclusions, hence there exist a unique homomorphism from M to the direct limit, say f.

f is injective: for $f(x) = 0$, there must be a finitely generated submodule N such that $x \in N$ and hence its image in the direct limit is 0. By Exercise 3.16, there exist a $N' \supset N$, such that $\phi^N_{N'}(x) = 0$, which means $x = 0$.

f is surjective: for any a in the direct limit, let x be it's preimage, then by the definitions, $f(x) = a$. □

Definition 3.10.1. A module M is called *finitely presented* if there is an exact sequence

$$F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

where F_0, F_1 are free with finite basis. The image of F_1 in F_0 is said to be the submodule of *relations*, among the free basis elements of F_0.

Remark. Any module is *presented*, in the sense that there is an exact sequence

$$F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

where F_0, F_1 are free.

First, for any module M is a quotient of a free module F_0, hence we have the an exact sequence

$$0 \longrightarrow R \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

Then R is also a quotient of a free module F_1, hence we get an epimorphism $F_1 \longrightarrow R$. By Lemma A.7.4, we obtain the require exact sequence.

Proposition 3.10.2. *A module M is finitely presented if and only if there is an exact sequence*

$$0 \longrightarrow R \longrightarrow F \longrightarrow M \longrightarrow 0$$

where F is free with finite basis, R is finitely generated.

3.22. *Show that any module is a direct limit of finitely presented modules (not necessarily submodules). In other words, given M, there exists a directed system (M_i) with M_i finitely presented for all i such that*

$$M \cong \varinjlim M_i$$

Proof. First, we have an exact sequence

$$0 \longrightarrow R \longrightarrow F \longrightarrow M \longrightarrow 0$$

By Exercise 3.21, R is the direct limit of its finitely generated submodules. Denote this directed system by (R_i), then it is clear that $R \longrightarrow F$ is injective. Let $M_i = F/R_i$, then we have a family of exact sequence

$$0 \longrightarrow R_i \longrightarrow F \longrightarrow M_i \longrightarrow 0$$

where each M_i is finitely presented. The connection homomorphisms in (R_i) naturally induce directed systems for F and $\{M_i\}$ of the same type with (R_i). Therefore we have an exact sequence

$$0 \longrightarrow (R_i) \longrightarrow (F) \longrightarrow (M_i) \longrightarrow 0$$

Since $\varinjlim$ is exact, we obtain an exact sequence of the limits:

$$0 \longrightarrow \varinjlim(R_i) \longrightarrow \varinjlim(F) \longrightarrow \varinjlim(M_i) \longrightarrow 0$$

where $\varinjlim(R_i) = R, \varinjlim(F) = F$. Compare it with the first exact sequence, we have $M = \varinjlim(M_i)$ as desired. □

3.23. *Let E be a module. Let (M_i) be a directed system of modules. If E is finitely generated, show that the natural homomorphism*

$$\varinjlim \mathrm{Hom}(E, M_i) \longrightarrow \mathrm{Hom}(E, \varinjlim M_i)$$

is injective. If E is finitely presented, show that this homomorphism is an isomorphism.

Proof. We finish the proof step by step.

1. Any connection homomorphism ϕ_j^i in (M_i) induces a homomorphism

$$\begin{aligned}\Phi_j^i\colon \operatorname{Hom}(E, M_i) &\longrightarrow \operatorname{Hom}(E, M_j)\\ f &\longmapsto \phi_j^i \circ f\end{aligned}$$

Thus $(\operatorname{Hom}(E, M_i), \Phi_j^i)$ form a directed system of the same type with (M_i).

Any homomorphism $\phi^i\colon M_i \longrightarrow \varinjlim M_i$ induces a homomorphism

$$\begin{aligned}\Phi^i\colon \operatorname{Hom}(E, M_i) &\longrightarrow \operatorname{Hom}(E, \varinjlim M_j)\\ f &\longmapsto \phi^i \circ f\end{aligned}$$

Then for any $\phi^i = \phi^j \circ \phi_j^i$, $\Phi^i = \Phi^j \circ \Phi_j^i$. Therefore $(\operatorname{Hom}(E, \varinjlim M_i), \Phi^i)$ is a cocone of $(\operatorname{Hom}(E, M_i), \Phi_j^i)$. Hence there exist a unique morphism

$$\varinjlim \operatorname{Hom}(E, M_i) \longrightarrow \operatorname{Hom}(E, \varinjlim M_i)$$

We denoted the natural homomorphism by Ψ.

Notice that for any $i, j \in I$, there exist $k \in I$ such that $i \leqslant k, j \leqslant k$,

2. *If E is free with finite basis, then Ψ is an isomorphism.*

Let $b_1, \cdots, b_n$ be a basis of E. We check that $\operatorname{Hom}(E, \varinjlim M_i)$ satisfies the universal property of $\varinjlim \operatorname{Hom}(E, M_i)$.

For any cocone (S, g_i), we need to show there exist a unique morphism $\operatorname{Hom}(E, \varinjlim M_i) \longrightarrow S$.

For any $f \in \operatorname{Hom}(E, \varinjlim M_i)$, consider the preimage $x_1, \cdots, x_n$ of $b_1, \cdots, b_n$ in M_i, then the map $b_j \mapsto x_j$ induces a unique homomorphism $E \longrightarrow M_i$. In this way, we get a map $\operatorname{Hom}(E, \varinjlim M_i) \longrightarrow \operatorname{Hom}(E, M_i)$ hence a map $\operatorname{Hom}(E, \varinjlim M_i) \longrightarrow S$. The commutativity is easy to check.

Assume there exist two morphisms

$$h_1, h_2\colon \operatorname{Hom}(E, \varinjlim M_i) \longrightarrow S$$

For any $f \in \operatorname{Hom}(E, \varinjlim M_i)$, we need to show $h_1(f) = h_2(f)$.

Consider $f_i \in g_i^{-1}(h_1(f))$, $f_i' \in g_i^{-1}(h_2(f))$. For $1 \leqslant j \leqslant n$, there exists $k_j \geqslant i$ such that $\phi_{k_j}^i(f_i(b_j)) = \phi_{k_j}^i(f_i'(b_j))$. Therefore there exists $k \geqslant i$ such that $\phi_k^i(f_i(b_j)) = \phi_k^i(f_i'(b_j))$ for any $1 \leqslant j \leqslant n$. But the map $b_j \mapsto \phi_k^i(f_i(b_j))$ induces a unique homomorphism $f_k \in \operatorname{Hom}(E, M_k)$, hence $h_1(f) = g_i(f_i) = g_k(f_k) = g_i(f_i') = h_2(f)$.

3. *If E is finitely presented by an exact sequence*

$$F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

then Ψ is an isomorphism.

Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \varinjlim \mathrm{Hom}(E, M_i) & \longrightarrow & \varinjlim \mathrm{Hom}(F_0, M_i) & \longrightarrow & \varinjlim \mathrm{Hom}(F_1, M_i) \\
 & & \Psi \downarrow & & \Psi_0 \downarrow & & \Psi_1 \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(E, \varinjlim M_i) & \longrightarrow & \mathrm{Hom}(F_0, \varinjlim M_i) & \longrightarrow & \mathrm{Hom}(F_1, \varinjlim M_i)
\end{array}$$

Here Ψ_0, Ψ_1 are isomorphisms by 2. Hence, by Five Lemma, Ψ is an isomorphism.

4. *If E is finitely generated by an epimorphism*

$$F \longrightarrow M \longrightarrow 0$$

then Ψ is injective.

Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccc}
0 & \longrightarrow & \varinjlim \mathrm{Hom}(E, M_i) & \longrightarrow & \varinjlim \mathrm{Hom}(F, M_i) \\
 & & \Psi \downarrow & & \Psi_0 \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(E, \varinjlim M_i) & \longrightarrow & \mathrm{Hom}(F, \varinjlim M_i)
\end{array}$$

Here Ψ_0 is an isomorphisms by 2. By $\triangle$ Lemma, Ψ is injective. $\square$

3.11 Graded Algebras

Definition 3.11.1. Let A be an algebra over a field k. By a *filtration* of A we mean a sequence of $k-$vector spaces $A_i (i = 0, 1, \cdots)$ such that

$$A_0 \subset A_1 \subset A_2 \subset \cdots \qquad \text{and} \qquad \bigcup A_i = A$$

and $A_i A_j \subset A_{i+j}$ for all $i, j \geqslant 0$, In particular, A is an A_0-algebra. We then call A a *filtered algebra*. Let R be an algebra. We say that R is *graded* if R is a direct sum $R = \bigoplus R_i$ of subspaces such that $R_i R_j \subset R_{i+j}$ for all $i, j \geqslant 0$.

3.24. *Let A be filtered algebra. Define R_i for $i \geqslant 0$ by $R_i = A_i/A_{i-1}$. By definition, $A_{-1} = \{0\}$. Let $R = \bigoplus R_i$, and $\mathrm{gr}_i(A) = R_i$. Define a natural product on R making R into a graded algebra, denoted by $\mathrm{gr}(A)$, and called the* associated graded algebra.

Proof. The multiplication $\mathrm{gr}(A) \times \mathrm{gr}(A) \longrightarrow \mathrm{gr}(A)$ is combined from the natural maps

$$\begin{aligned} A_i/A_{i-1} \times A_j/A_{j-1} &\longrightarrow A_{i+j}/A_{i+j-1} \\ (x + A_{i-1}, y + A_{j-1}) &\longmapsto xy + A_{i+j-1} \end{aligned}$$

The multiplication is well defined and endows $\mathrm{gr}(A)$ with the structure of a graded algebra, with gradation $\mathrm{gr}_i(A)$. □

3.25. *Let A, B be filtered algebras, $A = \bigcup A_i$ and $B = \bigcup B_i$. Let $L\colon A \longrightarrow B$ be an $(A_0, B_0)-$linear map preserving the filtration, that is $L(A_i) \subset B_i$ for all i, and $L(ca) = L(c)L(a)$ for $c \in A_0$ and $a \in A_i$ for all i.*

a) Show that L induces an $(A_0, B_0)-$linear map

$$\mathrm{gr}_i(L)\colon \mathrm{gr}_i(A) \longrightarrow \mathrm{gr}_i(B) \qquad \text{for all } i.$$

b) Suppose that $\mathrm{gr}_i(L)$ is an isomorphism for all i. Show that L is an $(A_0, B_0)-$isomorphism.

Proof. Consider the following $(A_0, B_0)-$linear map

$$A_i \xrightarrow{L} B_i \xrightarrow{\pi} B_i/B_{i-1}$$

its kernel contain A_{i-1} since $L(A_{i-1}) \subset B_{i-1}$, therefore it induces an quotient map $A_i/A_{i-1} \longrightarrow B_i/B_{i-1}$.

Consider the following commutative diagrams and using $5-$lemma, by induction on i, it is clear that if $\mathrm{gr}_i(L)$ are isomorphisms for all i, then L is an $(A_0, B_0)-$isomorphism.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{i-1} & \longrightarrow & A_i & \longrightarrow & \mathrm{gr}_i(A) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle L} & & \downarrow{\scriptstyle L} & & \downarrow{\scriptstyle \mathrm{gr}_i(L)} & & \\ 0 & \longrightarrow & B_{i-1} & \longrightarrow & B_i & \longrightarrow & \mathrm{gr}_i(B) & \longrightarrow & 0 \end{array}$$

□

3.26. *Suppose k has characteristic 0. Let $\mathfrak{n}$ be the set of all strictly upper triangular matrices of a given size $n \times n$ over k.*

a) For a given matrix $X \in \mathfrak{n}$, let $D_1(X), \cdots, D_n(X)$ be its diagonals, so $D_1 = D_1(X)$ is the main diagonal, and is 0 by the definition of $\mathfrak{n}$. Let $\mathfrak{n}_i$ be the subset of $\mathfrak{n}$ consisting of those matrices whose diagonals $D_1, \cdots, D_{n-i}$ are 0. Thus $\mathfrak{n}_0 = \{0\}$, $\mathfrak{n}_1$ consists of all matrices whose components are 0 except possibly for x_{1n}; $\mathfrak{n}_2$ consists of all matrices whose components are 0 except possibly those in the last two diagonals; and so forth. Show that each $\mathfrak{n}_i$ is an algebra, and its elements are nilpotent (in fact the $(i+1)-th$ power of its elements is 0).

b) Let U be the set of elements $I + X$ with $X \in \mathfrak{n}$. Show that U is a multiplicative group.

c) Let exp *be the exponential series defined as usual. Show that* exp *defines a polynomial function on $\mathfrak{n}$ (all but a finite number of terms are 0 when evaluated on a nilpotent matrix), and establishes a bijection*

$$\exp\colon \mathfrak{n} \longrightarrow U$$

Show that the inverse is given by the standard log *series.*

Proof. It is clear that $xy \in \mathfrak{n}_i$ for any $x, y \in \mathfrak{n}_i$, therefore $\mathfrak{n}_i$ is a subalgebra of $\mathfrak{n}$. Moreover, $xy \in \mathfrak{n}_{i-1}$, therefore the $(i+1)-$th power of $\mathfrak{n}_i$'s elements is 0.

The identity of U is I, for any $I + X \in U$, its inverse is $\sum(-X)^i$.

$$\exp(X) = \sum_{k=0}^{\infty} \frac{X^k}{k!}$$

$$\log(X) = -\sum_{k=1}^{\infty} \frac{(I-X)^k}{k}$$

□

3.12 Some Obvious Module Structure

Proposition 3.12.1. *Let R, S be rings, ${}_RA_S, {}_RB_S$ are double modules. Then*

1. $\mathrm{Hom}_R(A, -)$ *is a covatiant functor from* ${}_R\mathbf{Mod}$ *to* ${}_S\mathbf{Mod}$. *The left $S-$module structure is given by $(sf)a = f(as)$.*

2. $\mathrm{Hom}_R(-, B)$ *is a contravariant functor from* ${}_R\mathbf{Mod}$ *to* $\mathbf{Mod}_S$. *The right $S-$module structure is given by $(fs)a = (f(a))s$.*

Let A be a $R-$module, then $A \cong \mathrm{Hom}_R(R, A)$. $A^* \overset{\text{def}}{=} \mathrm{Hom}_R(A, R)$ is called the *dual module* of A. If $A \cong A^{**}$, then we say it is *reflexive*.

Proposition 3.12.2. *Let R, S be rings, ${}_SA_R, {}_RB_S$ are double modules. Then*

1. $A \otimes_R -$ *is a covatiant functor from* ${}_R\mathbf{Mod}$ *to* ${}_S\mathbf{Mod}$.

2. $- \otimes_R B$ *is a covariant functor from* $\mathbf{Mod}_R$ *to* $\mathbf{Mod}_S$.

Chapter 4

Polynomials

4.1 Basic Properties for Polynomials in One Variable

Part II

Algebraic Equations

Chapter 5

Algebraic Extensions

5.1 Finite and Algebraic Extensions

Example (Counterexample). Let α be an algebraic element over K, L is an extension of K, then $[L(\alpha) : L]$ integer divide $[K(\alpha) : K]$.

$\alpha = 2^{\frac{1}{3}}(-\frac{1}{2} + i\frac{\sqrt{3}}{2}), K = Q, L = Q(2^{\frac{1}{3}})$.

Chapter 6

Galois Theory

[Morandi, 1996]

6.1 Galois Extensions

Definition 6.1.1. Let K be a field and let G be a group of automorphisms of K. The subset of K consisting of all elements which is fixed under all $\sigma \in G$ is a field. It is called the *fixed field* of G, and denoted by K^G.

Definition 6.1.2. An algebraic extension K of a field k is called *Galois* if it is both normal and separable.

Definition 6.1.3. For an extension K/k, the group of automorphisms of K over k is denoted by $\mathrm{Aut}(K/k)$. When the extension is Galois, $\mathrm{Aut}(K/k)$ is called the *Galois group* of K over k, and is denoted by $\mathrm{Gal}(K/k)$ or $G(K/k)$.

The main theorem in this section is

Theorem 6.1.4 (Galois Connection). *Let K be a Galois extension of k, with Galois group G. Denote the set of intermediate field of K/k by $\mathrm{Int}(K/k)$, and the set of subgroups of G by $\mathrm{Sub}(G)$. Then there exists a bijection between them:*

$$\begin{aligned} \mathrm{Sub}(G) &\longrightarrow \mathrm{Int}(K/k) \\ H &\longmapsto E = K^H \end{aligned}$$

The field E is Galois if and only if H is normal in G. If that is the case, then the map $\sigma \mapsto \sigma|_E$ induces an isomorphism of G/H onto the Galois group of E over k.

Lang gives the proofs step by step.

Theorem 6.1.5. *Let K be a Galois extension of k, with Galois group G, then $k = K^G$. Denote the set of intermediate field of K/k by $\mathrm{Int}(K/k)$, and the set of subgroups of G by $\mathrm{Sub}(G)$. If $F \in \mathrm{Int}(K/k)$, then K is Galois over F. The map*

$$\begin{aligned} \mathrm{Int}(K/k) &\longrightarrow \mathrm{Sub}(G) \\ F &\longmapsto G(K/F) \end{aligned}$$

is injective.

Definition 6.1.6. We say a subgroup H of G *belongs* to an intermediate field F if $H = G(K/F)$.

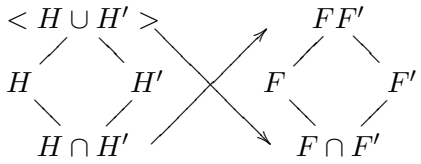
Corollary 6.1.7. *Let K/k be Galois with group G. Let F, F' be two intermediate fields, and let H, H' be the subgroups of G belonging to F, F' respectively. Then*

a) $H \cap H'$ belongs to FF';

b) The fixed field of the smallest subgroup of G containing H, H' is $F \cap F'$;

c) $F \subset F'$ if and only if $H' \subset H$.

Such results can be represented by the corresponding between the following two *Hasse diagrams*



Corollary 6.1.8. *Let E be a finite separable extension of a field k. Let K be the smallest normal extension of k containing E. Then K is finite Galois over k, and $\mathrm{Int}(E/k)$ is finite.*

Lemma 6.1.9. *Let E be an algebraic separable extension of k. Assume that there is an integer $n \geqslant 1$ such that every element of E is of degree $\leqslant n$ over k. Then $[E : k] \leqslant n$.*

Now, we have $K^{G(K/F)} = F$, but how about $G(K/K^H)$.

Theorem 6.1.10 (Artin). *Let K be a field and let G be a finite group of automorphisms of K, of order n. Let $k = K^G$ be the fixed field. Then K is a finite Galois extension of k, and its Galois group is G. We have $[K : k] = n$.*

Corollary 6.1.11. *Let K be a finite Galois extension of k and let G be its Galois group. Then every subgroup of G belongs to some $F \in \mathrm{Int}(K/k)$.*

Warning. This statement is not true when K is an infinite Galois extension of k.

Lemma 6.1.12. *Let K be a Galois extension of k. Let*

$$\lambda\colon K \longrightarrow \lambda K$$

be an isomorphism, then

$$G(\lambda K/\lambda k)^{\lambda} = G(K/k)$$

i.e.

$$G(\lambda K/\lambda k) = \lambda G(K/k)\lambda^{-1}$$

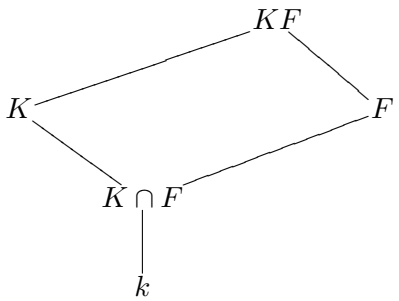
Theorem 6.1.13. *Let K be a Galois extension of k with group G. Let $F \in \mathrm{Int}(K/k)$, and let $H = G(K/F)$. Then F is normal over k if and only if H is normal in G. If that is the case, then the map $\sigma \mapsto \sigma|_E$ induces a homomorphism of G onto the Galois group of F over k, whose kernel is H.*

Definition 6.1.14. A Galois extension is said to be *abelian* (resp. *cyclic*) if its Galois group is *abelian* (resp. *cyclic*).

Corollary 6.1.15. *Let K/k be abelian (resp. cyclic). If $F \in \mathrm{Int}(K/k)$, then F/k is also abelian (resp. cyclic).*

Theorem 6.1.16. *Let K/k be Galois, F/k be an arbitrary extension, then $KF/F, K/(K \cap F)$ are Galois. Moreover, we have an isomorphism*

$$\mathrm{Gal}(KF/F) \cong \mathrm{Gal}(K/(K \cap F))$$
$$\sigma \leftrightarrow \sigma|_K$$



Corollary 6.1.17. *Let K/k be finite Galois, F/k be an arbitrary extension. Then $[KF : F]$ divides $[K : k]$.*

Warning. The assertion of above corollary is not usually valid if K/k is not Galois.

Indeed, let

$$\alpha = 2^{\frac{1}{3}} \quad \zeta = \frac{-1+\sqrt{-3}}{2} \quad \beta = \alpha\zeta$$

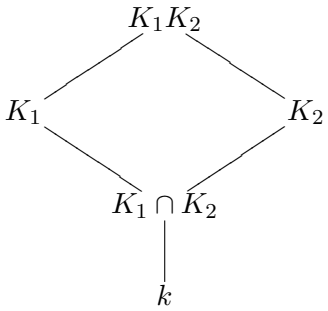
and $k = \mathbb{Q}, K = \mathbb{Q}(\beta), F = \mathbb{Q}(\alpha)$. Then

$$[KF : F] = 2 \quad [K : k] = 3$$

Theorem 6.1.18. *Let* $\mathrm{Gal}(K_1/k) = G_1, \mathrm{Gal}(K_2/k) = G_2$, *then* K_1K_2/k *is Galois. Let* G *be its Galois group, then*

$$\begin{aligned} G &\longrightarrow G_1 \times G_2 \\ \sigma &\longmapsto (\sigma|_{K_1}, \sigma|_{K_2}) \end{aligned}$$

is injective. If $K_1 \cap K_2 = k$, *then it is an isomorphism.*



Corollary 6.1.19. *Let* $K_1, \cdots, K_n$ *be Galois extensions of* k *with Galois groups* $G_1, \cdots, G_n$. *Assume* $K_{i+1} \cap (K_1 \cdots K_i) = k$, *then*

$$\mathrm{Gal}(K_1 \cdots K_n/k) \cong G_1 \times \cdots \times G_n$$

Corollary 6.1.20. *Let* K *be finite Galois over* k *with group* G, *and assume* $G = G_1 \times \cdots \times G_n$, *let* K_i *be the fixed field of*

$$G_1 \times \cdots \times 1 \times \cdots \times G_n$$

then K_i *is Galois over* k *and* $K_{i+1} \cap (K_1 \cdots K_i) = k, K = K_1 \cdots K_n$.

Theorem 6.1.21. *Assume all fields contained in some common field.*

(i) If K, L *are abelian over* k, *then so is* KL;

(ii) If K/k *is abelian and* F/k *is arbitrary, then* KF/F *is abelian;*

(iii) IF K/k *is abelian and* $F \in \mathrm{Int}(K/k)$, *then* $K/F, F/k$ *are abelian.*

Warning. The converse of last statement may not be true.

Definition 6.1.22. The composite of all abelian extensions of k in k^{a} is called the *abelian closure* of k and denoted by k^{ab}.

6.2 Examples and Applications

6.3 Norm and Trace

Let E/k be finite, $[E:k]_s = r$, $\alpha \in E$. We define the *norm* and *trace* of α to be

$$N_{E/k} = N_k^E(\alpha) = \prod_{v=1}^{r} \sigma_v \alpha^{[E:k]_i} = \left(\prod_{v=1}^{r} \sigma_v \alpha \right)^{[E:k]_i}$$

$$\mathrm{Tr}_{E/k} = \mathrm{Tr}_k^E(\alpha) = [E:k]_i \sum_{v=1}^{r} \sigma_v \alpha$$

If E/k is separable, then

$$N_k^E(\alpha) = \prod_{\sigma} \sigma\alpha$$

$$\mathrm{Tr}_k^E(\alpha) = \sum_{\sigma} \sigma\alpha$$

Theorem 6.3.1. *Let E/k be finite, then*

(i) $N_k^E(\alpha)$ is a multiplicative homomorphism of E^* into k^* and $\mathrm{Tr}_k^E(\alpha)$ is an additive homomorphism of E into k.

(ii) If $E \supset F \supset k$ is a tower, then

$$N_k^E = N_k^F \circ N_F^E \quad \text{and} \quad \mathrm{Tr}_k^E = \mathrm{Tr}_k^F \circ \mathrm{Tr}_F^E$$

(iii) If $E = k(\alpha)$, and $f(X) = \mathrm{Irr}(\alpha, k, X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, then

$$N_k^{k(\alpha)}(\alpha) = (-1)^n a_0 \qquad \mathrm{Tr}_k^{k(\alpha)}(\alpha) = -a_{n-1}$$

Theorem 6.3.2. *Let E/k be finite separable. Then Tr_k^E is a nonzero functional. The map*

$$E \times E \longrightarrow k$$
$$(x, y) \longmapsto \mathrm{Tr}(xy)$$

is bilinear, and identifies E with its dual space $E^\vee$.

Corollary 6.3.3. *Let $\omega_1, \cdots, \omega_n$ be a basis of E/k. Then there exists a basis $\omega_1', \cdots, \omega_n'$ of E/k such that $\mathrm{Tr}(\omega_i \omega_j') = \delta_{ij}$.*

Corollary 6.3.4. *Let E/k be finite separable, and let $\sigma_1, \cdots, \sigma_n$ be the distinct embeddings. Let $w_1, \cdots, w_n$ be elements of E. Then the vectors*

$$\xi_1 = (\sigma_1 w_1, \cdots, \sigma_1 w_n)$$
$$\cdots$$
$$\xi_n = (\sigma_n w_1, \cdots, \sigma_n w_n)$$

are linearly independent over E if $w_1, \cdots, w_n$ form a basis of E/k.

Remark. In characteristic 0, one sees much more trivially that the trace is not identically 0. Indeed, if $c \in k$ and $c \neq 0$, then $\mathrm{Tr}(c) = nc$ where $n = [E; k]$, and $n \neq 0$. This argument also holds in characteristic p where n is prime to p.

Proposition 6.3.5. *Let $E = k(\alpha)$ be separable. Let*

$$f(X) = \mathrm{Irr}(\alpha, k, X)$$

and let $f'(X)$ be its derivative. Let

$$\frac{f(X)}{(X - \alpha)} = \beta_0 + \beta_1 X + \cdots + \beta_{n-1} X^{n-1}$$

with $\beta_i \in E$. Then the dual basis of $1, \alpha, \cdots, \alpha^{n-1}$ is

$$\frac{\beta_0}{f'(\alpha)}, \cdots, \frac{\beta_{n-1}}{f'(\alpha)}$$

Define

$$\begin{aligned} m_\alpha \colon E &\longrightarrow E \\ x &\longmapsto \alpha x \end{aligned}$$

Proposition 6.3.6. *Let E/k be finite and let $\alpha \in E$. Then*

$$\det(m_\alpha) = N_{E/k}(\alpha) \quad \textit{and} \quad \mathrm{Tr}(m_\alpha) = \mathrm{Tr}_{E/k}(\alpha)$$

6.4 Cyclic Extensions

Theorem 6.4.1 (Hilbert's Theorem 90). *Let K/k be cyclic of degree n with Galois group G. Let σ be a generator of G. Let $\beta \in K$. The norm $N(\beta) = 1$ if and only if there exists an element $\alpha \neq 0$ in K such that $\beta = \alpha/\sigma\alpha$.*

Theorem 6.4.2. *Let k be a field, n an integer > 0 prime to the characteristic of k, and assume that there is a primitive $n-$th root of unity in k.*

(i) Let K be a cyclic extension of degree n. Then there exists $\alpha \in K$ such that $K = k(\alpha)$, and α satisfies an equation $X^n - a = 0$ for some $a \in k$.

(ii) Conversely, let $a \in k$. Let α be a root of $X^n - a$. Then $k(\alpha)$ is cyclic over k, of degree d, $d \mid n$, and α^d is an element of k.

Theorem 6.4.3 (Hilbert's Theorem 90, Additive Form). *Let K/k be cyclic of degree n with Galois group G. Let σ be a generator of G. Let $\beta \in K$. The trace $\mathrm{Tr}(\beta) = 0$ if and only if there exists an element $\alpha \neq 0$ in K such that $\beta = \alpha - \sigma\alpha$.*

Theorem 6.4.4 (Artin-Schreier). *Let k be a field of characteristic p.*

(i) Let K ba a cyclic extension of k of degree p. Then there exists $\alpha \in K$ such that $K = k(\alpha)$ and α satisfies an equation $X^p - X - a = 0$ with some $a \in k$.

(ii) Conversely, given $a \in k$, the polynomial $f(X) = X^p - X - a$ either has one root in k, in which case all its roots are in k, or it is irreducible. In this latter case, if α is a root then $k(\alpha)$ is cyclic of degree p over k.

6.5 Solvable and Radical Extensions

Definition 6.5.1. A Galois extension is called *solvable* if its Galois group is solvable. A finite extension E/k is said to be *solvable* if the smallest Galois extension K of k containing E is solvable.

Remark. This is equivalent to saying that there exist a solvable Galois extension L of k containing E.

Proposition 6.5.2. *Solvable extension form a distinguished class.*

Definition 6.5.3. A simple extension $k(\alpha)/k$ is called *solvable by radicals* if it is one of the following type:

1. It is obtained by adjoining a root of unity.
2. It is obtained by adjoining a root of a polynomial $X^n - a$ with $a \in k$ and n prime to the characteristic.
3. It is obtained by adjoining a root of an equation $X^p - X - a$ with $a \in k$, if p is the character > 0.

A finite extension F/k is said to be *solvable by radicals* if it is separable and if there exists a finite extension E/k containing F, and admitting a tower

$$k = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_m = E$$

such that each step is a simple extension solvable by radicals.

Proposition 6.5.4. *The class of extensions which are solvable by radical is distinguished.*

Proof. Using lifting. □

Theorem 6.5.5. *Let E/k be separable, then E is solvable by radical if and only if E/k is solvable.*

Definition 6.5.6. A polynomial $f \in k[X]$ is said to be *solvable by radicals* if its splitting field is solvable by radicals.

Definition 6.5.7. Let k be a field. The general polynomial of degree n over k is defined to be

$$f(X) = X^n - t_1 X^{n-1} + t_2 X^{n-2} + \cdots + (-1)^n t_n \in k(t_1, t_2, \cdots, t_n)[X]$$

where $t_1, t_2, \cdots, t_n$ are algebraic independent over k.

Corollary 6.5.8. *The general polynomial of degree n is solvable by radicals only if $n \leqslant 4$.*

6.6 Abelian Kummer Theory

Definition 6.6.1. A Galois extension K/k with group G is said to be of *exponent* m if $\sigma^m = 1$ for all $\sigma \in G$.

Let m be prime to the characteristic of k. We assume k contains a primitive $m-$th root of unity.

Let $a \in k$, and α be an $m-$th root of a. The field $k(\alpha)$ is independent of the choice of α and hence denoted by $k(a^{1/m})$.

We denote by k^{*m} the image of k^* under the homomorphism $x \mapsto x^m$.

Let $k^{*m} \subset B < k^*$. We denoted by $k(B^{1/m})$ or K_B the composite of all fields $k(a^{1/m})$ with $a \in B$.

K_B/k is Galois, let G be its Galois group. Let $\sigma \in G$. Then $\sigma\alpha = \omega_\sigma \alpha$ for some $m-$th root of unity $\omega_\sigma \in \boldsymbol{\mu}_m \subset k^*$.

There is a homomorphism:

$$\begin{aligned} G &\longrightarrow \boldsymbol{\mu}_m \\ \sigma &\longmapsto \omega_\sigma \end{aligned}$$

We may write $\omega_\sigma = \sigma\alpha/\alpha$, but it is independent of the choice of α.

We denote ω_σ by $\langle \sigma, \alpha \rangle$. The map

$$\begin{aligned} G \times B &\longrightarrow \boldsymbol{\mu}_m \\ (\sigma, a) &\longmapsto \langle \sigma, a \rangle \end{aligned}$$

is bilinear.

Theorem 6.6.2. *Let k be a field, m an integer > 0 prime to the characteristic of k, and assume that a primitive $m-$root of unity lies in k.*

(i) Let $k^{*m} \subset B < k^*$, $K_B = k(B^{1/m})$, then K_B/k is Galois and abelian of exponent m.

(ii) Consider the bilinear map

$$\begin{aligned} G \times B &\longrightarrow \boldsymbol{\mu}_m \\ (\sigma, a) &\longmapsto \langle \sigma, a \rangle \end{aligned}$$

The kernel of left is 1, and the kernel of right is k^{*m}.

(iii) K_B/k is finite if and only if $(B : k^{*m})$ is finite. If that is the case, then

$$B/k^{*m} \cong G^\wedge$$

and

$$[K_B : k] = (B : k^{*m})$$

Theorem 6.6.3. *There is a* $1-1$ *corresponding:*

$$\begin{aligned}\mathrm{Sub}(k^*; k^{*m}) &\cong \{\textit{abelian extension of } k \textit{ of exponent } m\}\\ B &\leftrightarrow K_B\end{aligned}$$

Theorem 6.6.4. *Let* k *be a field with characteristic* p*, we define the operator* $\wp$ *by*

$$\wp(x) = x^p - x$$

Then $\wp$ *is an additive automorphism of* k*.*
For $\wp(k) \subset B \subset k$*, Let* $K_B = k(\wp^{-1}B)$*.*

(i) There is a $1-1$ *corresponding*

$$\begin{aligned}\mathrm{Sub}(k : \wp(k)) &\cong \{\textit{abelian extension of } k \textit{ of exponent } p\}\\ B &\leftrightarrow K_B\end{aligned}$$

(ii) For $\sigma \in G, a \in B$ *and* $\alpha \in K_B$ *such that* $\wp\alpha = a$*. Let* $\langle \sigma, a\rangle = \sigma\alpha - \alpha$*. There is a bilinear map*

$$\begin{aligned}G \times B &\longrightarrow \mathbb{Z}/p\\ (\sigma, a) &\longmapsto \langle \sigma, a\rangle\end{aligned}$$

The kernel of left is 1*, and the kernel of right is* $\wp(k)$*.*

(iii) K_B/k *is finite if and only if* $(B : \wp(k))$ *is finite. If that is the case, then*

$$[K_B : k] = (B : \wp(k))$$

6.7 The Equation $X^n - a = 0$

In this section, the roots of unity are not in the ground field.

Theorem 6.7.1. *Let k be a field and n an integer $\geqslant 2$. Let $a \in k, a \neq 0$. Assume that for all $p \mid n$, we have $a \in k^p$, and if $4 \mid n$ then $a \notin -4k^4$. Then $X^n - a$ is irreducible in $k[X]$.*

Corollary 6.7.2. *$a \in k^*$, and $a \notin k^p$ for some p. If p is equal to the characteristic of k or p is odd, then for all $r \geqslant 1$, the polynomial $X^{p^r} - a$ is irreducible over k.*

Corollary 6.7.3. *If k^{a}/k is finite of degree > 1, then $k^{\mathrm{a}} = k(i)$ and its characteristic is 0.*

Example. Let k be a field with characteristic not dividing n. Let $a \in k^*$ and K be the splitting field of $X^n - a$. Let α be a root of $X^n - a$ and let ζ be a primitive $n-$th root of unity. Then

$$K = k(\alpha, \zeta) = k(\alpha, \boldsymbol{\mu}_n)$$

Let $\sigma \in G_{K/k}$. Then there exists some integer $b(\sigma)$ uniquely determined mod n, such that

$$\sigma(\alpha) = \alpha \zeta^{b(\sigma)}$$

There exists an integer $d(\sigma)$ uniquely determined mod n, such that

$$\sigma(\zeta) = \zeta^{d(\sigma)}$$

Let $G(n)$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n)$ consisting of all matrices

$$M = \begin{pmatrix} 1 & 0 \\ b & d \end{pmatrix}$$

where $b \in \mathbb{Z}/n, d \in (\mathbb{Z}/n)^*$.

Observe that $|G(n)| = n\varphi(n)$, and we obtain an injective map:

$$\begin{aligned} G_{K/k} &\longrightarrow G(n) \\ \sigma &\longmapsto M(\sigma) \end{aligned}$$

Theorem 6.7.5. *Let k be a field. Let n be an odd integer prime to the characteristic, and assume that $[k(\boldsymbol{\mu}_n) : k] = \varphi(n)$. Let $a \in k$, and $a \notin k^p$ for all prime $p \mid n$. Let K be the splitting field of $X^n - a$ over k.*

Then the above homomorphism $\sigma \mapsto M(\sigma)$ is an isomorphism. The commutator group is $\mathrm{Gal}(K/k(\boldsymbol{\mu}_n))$, so $k(\boldsymbol{\mu}_n)$ is the maximal abelian subextension of K.

Warning. When n is even, there are some complications.

Part

Appendix

Appendix A

Category Theory

A.1 Categories

Definition A.1.1. A *category* $\mathcal{C}$ consists of

- a class $\operatorname{ob}\mathcal{C}$ of *objects*.
- a class $\hom\mathcal{C}$ of *morphisms*, or *arrows*, or *maps*, between the objects.

  Each morphism f has a unique source object A and target object B where A and B are in $\operatorname{ob}\mathcal{C}$.

  We write $f\colon A \longrightarrow B$, and we say "$f$ is a morphism from A to B".

  We write $\operatorname{Hom}(A, B)$ (or $\operatorname{Hom}_{\mathcal{C}}(A, B)$ when there may be confusion about to which category $\operatorname{Hom}(A, B)$ refers) to denote the hom-class of all morphisms from A to B. (Some authors write $\operatorname{Mor}(A, B)$ or simply $\mathcal{C}(A, B)$ instead.)
- for every three objects A, B and C, a binary operation

  $$\operatorname{Hom}(A, B) \times \operatorname{Hom}(B, C) \longrightarrow \operatorname{Hom}(A, C)$$

  called *composition of morphisms*.

  The composition of $f\colon A \longrightarrow B$ and $g\colon B \longrightarrow C$ is written as $g \circ f$ or simply gf. (Some authors use "diagrammatic order", writing $f; g$ or fg.)

such that the following axioms hold:

associativity if $f\colon A \longrightarrow B, g\colon B \longrightarrow C$ and $h\colon C \longrightarrow D$ then

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

identity for every object A, there exists a morphism $1_A \colon A \longrightarrow A$ (sometimes write id_A) called the *identity morphism* for A, such that for every morphism $f \colon A \longrightarrow B$, we have $1_B \circ f = f = f \circ 1_A$.

From these axioms, one can prove that there is exactly one identity morphism for every object. Some authors use a slight variation of the definition in which each object is identified with the corresponding identity morphism.

Definition A.1.2. A category $\mathcal{C}$ is called *small* if both $\mathrm{ob}\,\mathcal{C}$ and $\mathrm{hom}\,\mathcal{C}$ are actually sets, and *large* otherwise. A *locally small category* is a category such that for all objects A and B, the hom-class $\mathrm{Hom}(A, B)$ is a set, called a hom-set. Many important categories in mathematics (such as the category of sets), although not small, are at least locally small.

Definition A.1.3. Any category $\mathcal{C}$ can itself be considered as a new category in a different way: the objects are the same as those in the original category but the arrows are those of the original category reversed. This is called the *dual* or *opposite category* and is denoted $\mathcal{C}^{\mathrm{op}}$.

Definition A.1.4. The *product category* $\mathcal{C} \times \mathcal{D}$ consists of:

- *objects:* pairs of objects (A, B), where A is an object of $\mathcal{C}$ and B of $\mathcal{D}$;
- *arrows from* (A, B_1) *to* (A_2, B_2)*:* pairs of arrows (f, g), where $f \colon A_1 \longrightarrow A_2$ is an arrow of $\mathcal{C}$ and $g \colon B_1 \longrightarrow B_2$ is an arrow of $\mathcal{D}$;
- *compositions:* component-wise composition from the contributing categories:
$$(f_2, g_2) \circ (f_1, g_1) = (f_2 \circ f_1, g_2 \circ g_1);$$
- *identities:* pairs of identities from the contributing categories:
$$1_{(A,B)} = (1_A, 1_B).$$

A.1.1 Subcategories

Definition A.1.5. Let $\mathcal{C}$ be a category. A *subcategory* $\mathcal{S}$ of $\mathcal{C}$ is given by

- a subcollection of objects of $\mathcal{C}$, denoted $\mathrm{ob}\,\mathcal{S}$,
- a subcollection of morphisms of $\mathcal{C}$, denoted $\mathrm{hom}\,\mathcal{S}$.

such that

1. for every X in $\mathrm{ob}\,\mathcal{S}$, the identity morphism id_X is in $\mathrm{hom}\,\mathcal{S}$,
2. for every morphism $f \colon X \longrightarrow Y$ in $\mathrm{hom}\,\mathcal{S}$, both the source X and the target Y are in $\mathrm{ob}\,\mathcal{S}$,

3. for every pair of morphisms f and g in $\hom \mathcal{S}$ the composite $f \circ g$ is in $\hom \mathcal{S}$ whenever it is defined.

Remark. These conditions ensure that $\mathcal{S}$ is a category in its own right: the collection of objects is $\operatorname{ob} \mathcal{S}$, the collection of morphisms is $\hom \mathcal{S}$, and the identities and composition are as in $\mathcal{C}$. There is an obvious faithful functor $I \colon \mathcal{S} \longrightarrow \mathcal{C}$, called the *inclusion functor* which takes objects and morphisms to themselves.

Definition A.1.6. Let $\mathcal{S}$ be a subcategory of a category $\mathcal{C}$. We say that $\mathcal{S}$ is a *full subcategory* of $\mathcal{C}$ if the inclusion functor is fully faithful.

Definition A.1.7. A subcategory $\mathcal{S}$ of $\mathcal{C}$ is said to be *isomorphism-closed* or *replete* if every isomorphism $k \colon X \longrightarrow Y$ in $\mathcal{C}$ such that Y is in $\mathcal{S}$ also belongs to $\mathcal{S}$. A isomorphism-closed full subcategory is said to be *strictly full*.

Definition A.1.8. A subcategory of $\mathcal{C}$ is said to be *wide* or *lluf* if it contains all the objects of $\mathcal{C}$.

A.1.2 Reflective Subcategory

A.1.3 Comma Categories

Definition A.1.9. Suppose that $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ are categories, and S and T (for source and target) are functors

$$\mathcal{A} \xrightarrow{S} \mathcal{C} \xleftarrow{T} \mathcal{B}$$

We can form the *comma category* $(S \downarrow T)$ as follows:

- The objects are all triples (α, β, f) with α an object in $\mathcal{A}$, β an object in $\mathcal{B}$, and $f \colon S(\alpha) \longrightarrow T(\beta)$ a morphism in $\mathcal{C}$.
- The morphisms from (α, β, f) to (α', β', f') are all pairs (g, h) where $g \colon \alpha \longrightarrow \alpha'$ and $h \colon \beta \longrightarrow \beta'$ are morphisms in $\mathcal{A}$ and $\mathcal{B}$ respectively, such that the following diagram commutes:

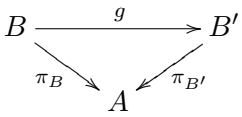
$$\begin{array}{ccc} S(\alpha) & \xrightarrow{S(g)} & S(\alpha') \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ T(\beta) & \xrightarrow[T(h)]{} & T(\beta') \end{array}$$

- Morphisms are composed by taking $(g, h) \circ (g', h')$ to be $(g \circ g', h \circ h')$, whenever the latter expression is defined.

- The identity morphism on an object (α, β, f) is $(\mathrm{id}_\alpha, \mathrm{id}_\beta)$.

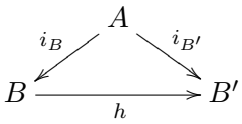
Example. Slice category.

When $\mathcal{A} = \mathcal{C}$, S is the identity functor, and $\mathcal{B} = \mathbf{1}$ (the category with one object $*$ and one morphism). Then $T(*) = A$ for some object A in $\mathcal{C}$. In this case, the comma category is written $(\mathcal{C} \downarrow A)$, and is often called the *slice category* over A or the category of *objects over A*. The objects $(\alpha, *, f)$ can be simplified to pairs (α, f), where $f\colon \alpha \longrightarrow A$. Sometimes, f is denoted π_α. A morphism from (B, π_B) to $(B', \pi_{B'})$ in the slice category is then an arrow $g\colon B \longrightarrow B'$ making the following diagram commute:



Example. Coslice category.

The dual concept to a slice category is a coslice category. Here, S has domain $\mathbf{1}$ and T is an identity functor. In this case, the comma category is often written $(A \downarrow \mathcal{C})$, where A is the object of $\mathcal{C}$ selected by S. It is called the *coslice category* with respect to A, or the category of *objects under A*. The objects are pairs (B, i_B) with $i_B\colon A \longrightarrow B$. Given (B, i_B) and $(B', i_{B'})$, a morphism in the coslice category is a map $h\colon B \longrightarrow B'$ making the following diagram commute:



Example. Arrow category.

S and T are identity functors on $\mathcal{C}$ (so $\mathcal{A} = \mathcal{B} = \mathcal{C}$). In this case, the comma category is the *arrow category* $\mathcal{C}^{\to}$. Its objects are the morphisms of $\mathcal{C}$, and its morphisms are commuting squares in $\mathcal{C}$.

Example. In the case of the slice or coslice category, the identity functor may be replaced with some other functor; this yields a family of categories particularly useful in the study of adjoint functors. Let s, t be given object in $\mathcal{C}$. An object of $(s \downarrow T)$ is called a *morphism from s to T* or a *$T-$structured arrow* with domain s in. An object of $(S \downarrow t)$ is called a *morphism from S to t* or a *$S-$costructured arrow* with codomain s in.

Proposition A.1.14. *For each comma category there are forgetful functors from it.*

- domain functor, $(S \downarrow T) \longrightarrow \mathcal{A}$, *which maps:*
  - *objects:* $(\alpha, \beta, f) \mapsto \alpha$;

  - *morphisms:* $(g, h) \mapsto g$;

- codomain functor, $(S \downarrow T) \longrightarrow \mathcal{B}$, *which maps:*
  - *objects:* $(\alpha, \beta, f) \mapsto \beta$;
  - *morphisms:* $(g, h) \mapsto h$;

Example. The category of **pointed sets** is a comma category $(\bullet \downarrow \mathbf{Set})$, with $\bullet$ being (a functor selecting) any singleton set, and **Set** (the identity functor of) the category of sets. Each object of this category is a set, together with a function selecting some element of the set: the "**basepoint**". Morphisms are functions on sets which map basepoints to basepoints. In a similar fashion one can form the category of **pointed spaces** $(\bullet \downarrow \mathrm{Top})$.

Example. The category of **graphs** is $(\mathbf{Set} \downarrow D)$, with $D\colon \mathbf{Set} \longrightarrow \mathbf{Set}$ the functor taking a set s to $s \times s$. The objects (a, b, f) then consist of two sets and a function; a is an **indexing set**, b is a set of **nodes**, and $f\colon a \longrightarrow (b \times b)$ chooses pairs of elements of b for each input from a. That is, f picks out certain edges from the set $b \times b$ of possible edges. A morphism in this category is made up of two functions, one on the indexing set and one on the node set. They must "agree" according to the general definition above, meaning that $(g, h)\colon (a, b, f) \longrightarrow (a', b', f')$ must satisfy $f' \circ g = D(h) \circ f$. In other words, the edge corresponding to a certain element of the indexing set, when translated, must be the same as the edge for the translated index.

Example. Colimits in comma categories may be "inherited". If $\mathcal{A}$ and $\mathcal{B}$ are cocomplete, $S\colon \mathcal{A} \longrightarrow \mathcal{C}$ is a cocontinuous functor, and $T\colon \mathcal{B} \longrightarrow \mathcal{C}$ another functor (not necessarily cocontinuous), then the comma category $(S \downarrow T)$ produced will also be cocomplete.

If $\mathcal{A}$ and $\mathcal{B}$ are complete, and both $S\colon \mathcal{A} \longrightarrow \mathcal{C}$ and $T\colon \mathcal{B} \longrightarrow \mathcal{C}$ are continuous functors, then the comma category $(S \downarrow T)$ is also complete, and the projection functors $(S \downarrow T) \longrightarrow \mathcal{A}$ and $(S \downarrow T) \longrightarrow \mathcal{B}$ are limit preserving.

Example. Adjunctions.

Lawvere showed that the functors $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ and $G\colon \mathcal{D} \longrightarrow \mathcal{C}$ are adjoint if and only if the comma categories $(F \downarrow \mathrm{id}_{\mathcal{D}})$ and $(\mathrm{id}_{\mathcal{C}} \downarrow G)$, with $\mathrm{id}_{\mathcal{D}}$ and $\mathrm{id}_{\mathcal{C}}$ the identity functors on $\mathcal{D}$ and $\mathcal{C}$ respectively, are isomorphic, and equivalent elements in the comma category can be projected onto the same element of $\mathcal{C} \times \mathcal{D}$. This allows adjunctions to be described without involving sets, and was in fact the original motivation for introducing comma categories.

Example. Natural transformations.

A natural transformation $\eta\colon S \longrightarrow T$, with $S, T\colon \mathcal{A} \longrightarrow \mathcal{C}$, corresponds to a functor $\mathcal{A} \longrightarrow (S \downarrow T)$ which maps each object α to $(\alpha, \alpha, \eta_\alpha)$ and maps each morphism g to (g, g). This is a bijective correspondence between natural transformations $S \longrightarrow T$ and functors $\mathcal{A} \longrightarrow (S \downarrow T)$ which are sections of both forgetful functors from $(S \downarrow T)$.

A.2 Morphisms

A.2.1 Monomorphisms, Epimorphisms and Zero Morphisms

Definition A.2.1. A morphism f is called a *monomorphism*, or *monoic*, if for any morphisms $\cdot \underset{\beta}{\overset{\alpha}{\rightrightarrows}} \cdot \xrightarrow{f} \cdot$, $f\alpha = f\beta$ implies $\alpha = \beta$. Dually, f is called an *epimorphism*, or *epi*, if for any morphisms $\cdot \xrightarrow{f} \cdot \underset{\beta}{\overset{\alpha}{\rightrightarrows}} \cdot$, $\alpha f = \beta f$ implies $\alpha = \beta$. If f is both a monomorphism and an epimorphism, then we say it is a *bimorphism*.

Definition A.2.2. A morphism f is called a *split monomorphism*, if it has a left inverse, names *retraction*. Dually, a morphism f is called a *split epimorphism*, if it has a right inverse, names *section*. If f is both a split monomorphism and a split epimorphism, then we say it is an *isomorphism*.

Remark. It is clear that any split monomorphism must be monoic and any split epimorphism is epi, hence any isomorphism is a bimorphism. However, the converse is not true in general case.

A bijective morphism may fail to be an isomorphism:

Example. In **Top**, the map from the half-open interval $[0, 1)$ to the unit circle S^1 (thought of as a subspace of the complex plane) which sends x to e^{2ix} is continuous and bijective but not a *homeomorphism* since the inverse map is not continuous at 1.

Remark. This counterexample also shows why the concept of *subobject* does not correspond subspace in **Top**.

An epimorphism may fail to be surjective:

Example. In the category of rings, **Ring**, the inclusion map $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is a non-surjective epimorphism; to see this, note that any ring homomorphism on $\mathbb{Q}$ is determined entirely by its action on $\mathbb{Z}$. A similar argument shows that the natural ring homomorphism from any commutative ring R to any one of its localizations is an epimorphism.

Remark. This is also a counterexample shows that a quotient object may not be a quotient.

Definition A.2.5. A morphism f is called a *constant morphism* (or sometimes *left zero morphism*) if for any morphisms $\cdot \underset{\beta}{\overset{\alpha}{\rightrightarrows}} \cdot \xrightarrow{f} \cdot$, $f\alpha = f\beta$.

Dually, f is called a *coconstant morphism* (or sometimes *right zero morphism*) if for any morphisms $\cdot \xrightarrow{f} \cdot \underset{\beta}{\overset{\alpha}{\rightrightarrows}} \cdot$, $\alpha f = \beta f$. A *zero morphism* is one that is both a constant morphism and a coconstant morphism.

Definition A.2.6. A *category with zero morphisms* is one where, for every two objects A and B in $\mathcal{C}$, there is a fixed morphism $0_{AB}\colon A \longrightarrow B$ such that for all objects X, Y, Z in C and all morphisms $f\colon X \longrightarrow Y, g\colon Y \longrightarrow Z$, the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{0_{XY}} & Y \\ {\scriptstyle f}\downarrow & \searrow^{0_{XZ}} & \downarrow{\scriptstyle g} \\ Y & \xrightarrow[0_{YZ}]{} & Z \end{array}$$

Remark. The morphisms 0_{XY} necessarily are zero morphisms and form a *compatible system* of zero morphisms. If $\mathcal{C}$ is a category with zero morphisms, then the collection of 0_{XY} is unique.

Remark. If a category has zero morphisms, then one can define the notions of *kernel* and *cokernel* for any morphism in that category.

A.2.2 Factorization

[Freyd and Kelly, 1972]

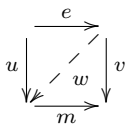
Definition A.2.7. If a morphism $f\colon X \longrightarrow Y$ can be written as a composition $f = g \circ h$ with $g\colon Z \longrightarrow Y$ and $h\colon X \longrightarrow Z$, then f is said to *factor through* any (and all) of Z, g, and h. We also say f is *factorized* as h followed by g.

Definition A.2.8. A *factorization system* (E, M) for a category $\mathcal{C}$ consists of two classes of morphisms E and M of $\mathcal{C}$ such that:

1. E and M both contain all isomorphisms of $\mathcal{C}$ and are closed under composition.
2. Every morphism f of $\mathcal{C}$ can be factored as $f = m \circ e$ for some morphisms $e \in E$ and $m \in M$.
3. The factorization is *functorial*: if u and v are two morphisms such that $vme = m'e'u$ for some morphisms $e, e' \in E$ and $m, m' \in M$, then there exists a unique morphism w making the following diagram commute:

$$\begin{array}{ccc} \cdot & \xrightarrow{e} & \cdot \\ {\scriptstyle u}\downarrow & \overset{w}{\swarrow} & \downarrow{\scriptstyle v} \\ \cdot & \xrightarrow[e']{} & \cdot \end{array} \qquad \begin{array}{ccc} \cdot & \xrightarrow{m} & \cdot \\ & \swarrow & \downarrow \\ \cdot & \xrightarrow[m']{} & \cdot \end{array}$$

Definition A.2.9. Two morphisms e and m are said to be *orthogonal*, if for every pair of morphisms u and v such that $ve = mu$ there is a unique morphism w such that the diagram



commutes. If so, denote by $e \downarrow m$,

This notion can be extended to define the orthogonals of sets of morphisms by

$$H^{\uparrow} \stackrel{\text{def}}{=} \{e \mid \forall h \in H, e \downarrow h\}$$

and

$$H^{\downarrow} \stackrel{\text{def}}{=} \{m \mid \forall h \in H, h \downarrow m\}$$

Since in a factorization system $E \cap M$ contains all the isomorphisms, the condition 3. of the definition is equivalent to 3':

$$E \subset M^{\uparrow} \qquad M \subset E^{\downarrow}$$

Proposition A.2.10. *The pair (E, M) of classes of morphisms of $\mathcal{C}$ is a factorization system if and only if it satisfies the following conditions:*

1. *Every morphism f of $\mathcal{C}$ can be factored as $f = m \circ e$ for some morphisms $e \in E$ and $m \in M$.*
2. *$E \subset M^{\uparrow}$ and $M \subset E^{\downarrow}$.*

A.2.3 Endomorphisms

[Balmer and Schlichting, 2001]

Definition A.2.11. An *endomorphism* is a morphism whose domain and co-domain coincide. An *automorphism* is a morphism that is both an endomorphism and an isomorphism.

Definition A.2.12. An *idempotent* e is an endomorphism such that $e \circ e = e$. An endomorphism e is said to *split* if it is idempotent, and if there are two morphisms f, g such that $e = gf$ and $\mathrm{id} = fg$.

Definition A.2.13. A category is called *idempotent complete*, if every idempotent splits.

Definition A.2.14. Let $\mathcal{C}$ be a category, the *Karoubi envelope* of $\mathcal{C}$, sometimes written $\mathbf{Split}(\mathcal{C})$, is the category whose objects are pairs of the form

(A, e) where A is an object of $\mathcal{C}$ and $e\colon A \longrightarrow A$ is an idempotent of $\mathcal{C}$, and whose morphisms are triples of the form

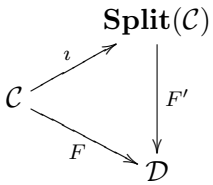
$$(e, f, e')\colon (A, e) \longrightarrow (A', e')$$

where $f\colon A \longrightarrow A'$ is a morphism of $\mathcal{C}$ satisfying $e' \circ f = f = f \circ e$ (or equivalently $f = e' \circ f \circ e$).

Composition in $\mathbf{Split}(\mathcal{C})$ is as in $\mathcal{C}$, but the identity morphism on (A, e) in $\mathbf{Split}(\mathcal{C})$ is (e, e, e), rather than the identity on A.

Proposition A.2.15. *The Karoubi envelope* $\mathbf{Split}(\mathcal{C})$ *of* $\mathcal{C}$ *is the* idempotent completion *of* $\mathcal{C}$*, which means that* $\mathcal{C}$ *can be fully faithfully embedded into* $\mathbf{Split}(\mathcal{C})$*, and the embedding* $\imath\colon \mathcal{C} \longrightarrow \mathbf{Split}(\mathcal{C})$ *satisfying the following universal property:*

> *For any functor* $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ *with* $\mathcal{D}$ *is idempotent complete, there is a unique functor* $F'\colon \mathbf{Split}(\mathcal{C}) \longrightarrow \mathcal{D}$ *such that the following diagram commutes:*



A.2.4 Initial and Terminal Morphisms

Definition A.2.16. Suppose that $U\colon \mathcal{D} \longrightarrow \mathcal{C}$ is a functor from a category $\mathcal{D}$ to a category $\mathcal{C}$, and let X be an object of $\mathcal{C}$. An *initial morphism* from X to U is an initial object in the category $(X \downarrow U)$ of morphisms from X to U. A *terminal morphism* from U to X is a terminal object in the comma category $(U \downarrow X)$ of morphisms from U to X.

Remark. The term *universal morphism* refers either to an initial morphism or a terminal morphism.

Proposition A.2.17. *Given a functor* U *and an object* X *as above, there may or may not exist an initial morphism from* X *to* U*. However, if an initial morphism does exist then it is unique up to a unique isomorphism.*

Proposition A.2.18. *Let* U *be a functor from* $\mathcal{D}$ *to* $\mathcal{C}$*, and let* X *be an object of* $\mathcal{C}$*. Then the following statements are equivalent:*

a. (A, ϕ) *is an initial morphism from* X *to* U*;*

b. (A, ϕ) *is an initial object of the comma category* $(X \downarrow U)$*;*

c. (A, ϕ) *is a representation of* $\mathrm{Hom}_{\mathcal{C}}(X, U(-))$.

The dual statements are also equivalent:

a'. (A, ϕ) *is a terminal morphism from* U *to* X*;*

b'. (A, ϕ) *is a terminal object of the comma category* $(U \downarrow X)$*;*

c'. (A, ϕ) *is a representation of* $\mathrm{Hom}_{\mathcal{C}}(U(-), X)$.

Suppose (A_1, ϕ_1) is an initial morphism from X_1 to U and (A_2, ϕ_2) is an initial morphism from X_2 to U. By the initial property, given any morphism $h\colon X_1 \longrightarrow X_2$ there exists a unique morphism $g\colon A_1 \longrightarrow A_2$ such that the following diagram commutes:

$$\begin{array}{ccc} X_1 & \xrightarrow{\phi_1} & U(A_1) \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle U(g)} \\ X_2 & \xrightarrow[\phi_2]{} & U(A_2) \end{array} \qquad \begin{array}{c} A_1 \\ \downarrow{\scriptstyle g} \\ A_2 \end{array}$$

If every object X_i of $\mathcal{C}$ admits an initial morphism to U, then the assignment $X_i \mapsto A_i$ and $h \mapsto g$ defines a functor V from $\mathcal{C}$ to $\mathcal{D}$. The maps ϕ_i then define a natural transformation from $\mathrm{id}_{\mathcal{C}}$ to UV. The functors (V, U) are then a pair of adjoint functors, with V left-adjoint to U and U right-adjoint to V.

Similar statements apply to the dual situation of terminal morphisms from U. If such morphisms exist for every X in $\mathcal{C}$ one obtains a functor $V\colon \mathcal{C} \longrightarrow \mathcal{D}$ which is right-adjoint to U (so U is left-adjoint to V).

Indeed, all pairs of adjoint functors arise from *universal constructions* in this manner. Let F and G be a pair of adjoint functors with unit η and co-unit ε. Then we have a universal morphism for each object in $\mathcal{C}$ and $\mathcal{D}$:

- For each object X in $\mathcal{C}$, $(F(X), \eta_X)$ is an initial morphism from X to G. That is, for all $f\colon X \longrightarrow G(Y)$ there exists a unique $g\colon F(X) \longrightarrow Y$ for which the following diagrams commute.

- For each object Y in $\mathcal{D}$, $(G(Y), \varepsilon_Y)$ is a terminal morphism from F to Y. That is, for all $g\colon F(X) \longrightarrow Y$ there exists a unique $f\colon X \longrightarrow G(Y)$ for which the following diagrams commute.

$$\begin{array}{ccc} X & \xrightarrow{\eta_X} & GF(X) \\ & {\scriptstyle f}\searrow & \downarrow{\scriptstyle G(g)} \\ & & G(Y) \end{array} \qquad \begin{array}{ccc} F(X) & & \\ \downarrow{\scriptstyle F(f)} & \searrow{\scriptstyle g} & \\ FG(Y) & \xrightarrow[\varepsilon_Y]{} & Y \end{array}$$

Universal constructions are more general than adjoint functor pairs: a universal construction is like an optimization problem; it gives rise to an adjoint pair if and only if this problem has a solution for every object of $\mathcal{C}$ (equivalently, every object of $\mathcal{D}$).

A.3 Functors

Definition A.3.1. Let $\mathcal{C}, \mathcal{D}$ be two categories, a *functor* $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ is a corresponding from $\operatorname{ob}\mathcal{C}$ into $\operatorname{ob}\mathcal{D}$ and $\hom\mathcal{C}$ into $\hom\mathcal{D}$ such that

(i) $F(1_X) = 1_{F(X)}$ for every object X;

(ii) $F(g \circ f) = F(g) \circ F(f)$ for all morphisms $f\colon A \longrightarrow B, g\colon B \longrightarrow C$.

Definition A.3.2. Let $\mathcal{C}, \mathcal{D}$ be two categories, a *contravariant functor* is a functor from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{D}$.

Ordinary functors are also called *covariant functor* in order to distinguish them from *contravariant* ones.

Definition A.3.3. Every functor $F\colon \mathcal{C} \longrightarrow \mathcal{D}$ induces the *opposite functor* $F^{\mathrm{op}}\colon \mathcal{C}^{\mathrm{op}} \longrightarrow \mathcal{D}^{\mathrm{op}}$ maps objects and morphisms identically to F.

Definition A.3.4. A *bifunctor* is a functor whose domain is a product category.

Example. Consider $S_2 \longrightarrow S_3 \longrightarrow S_2$ in **Grp**, it is not difficult to show that there is no functor **Grp** $\longrightarrow$ **Ab** sending each group to its center.

Example. The functor $\mathcal{C} \longrightarrow \mathcal{D}$ which maps every object of $\mathcal{C}$ to a fixed object X in $\mathcal{D}$ and every morphism in $\mathcal{C}$ to the identity morphism on X. Such a functor is called a *constant* or *selection functor*.

Example. The *diagonal functor* is defined as the functor from $\mathcal{D}$ to the functor category $[\mathcal{C}, \mathcal{D}]$ which sends each object in $\mathcal{D}$ to the constant functor at that object.

Definition A.3.8. A Functor $F\colon \mathcal{C} \to \mathcal{D}$ is said to be

a) *faithful* (resp. *full*, resp. *fully faithful*) if for any $X, Y \in \operatorname{ob}\mathcal{C}$, the map $\mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y))$ is injective (resp. surjective, resp. bijective).

b) *essentially surjective* if for each $Y \in \operatorname{ob}\mathcal{D}$, there exists $X \in \operatorname{ob}\mathcal{C}$ and an isomorphism $F(X) \cong Y$.

c) *conservative* if any morphism $f\colon X \to Y$ in $\mathcal{C}$ is an isomorphism as soon as $F(f)$ is an isomorphism.

Warning. A faithful functor need not be injective on objects or morphisms. That is, two objects X and X' may map to the same object in $\mathcal{D}$ (which is why the range of a fully faithful functor is not necessarily equivalent to

$\mathcal{C}$), and two morphisms $f\colon X \longrightarrow Y$ and $f'\colon X' \longrightarrow Y'$ (with different domains/codomains) may map to the same morphism in $\mathcal{D}$.

Likewise, a full functor need not be surjective on objects or morphisms. There may be objects in $\mathcal{D}$ not of the form $F(X)$ for some X in $\mathcal{C}$. Morphisms between such objects clearly cannot come from morphisms in $\mathcal{C}$.

Proposition A.3.9. *1) Let $F\colon \mathcal{C} \to \mathcal{D}$ be a faithful functor and let f be a morphism in $\mathcal{C}$. Then if $F(f)$ is a monomorphism (resp. an epimorphism), then f is a monomorphism (resp. an epimorphism).*

2) Moreover, assume that F is fully faithful. Then if $F(f)$ is an isomorphism, then f is an isomorphism. In other words, fully faithful functors are conservative.

Proof. For any $T \overset{\alpha}{\underset{\beta}{\rightrightarrows}} X \xrightarrow{f} T$ in $\mathcal{C}$ such that $f\alpha = f\beta$, then $F(f)F(\alpha) = F(f)F(\beta)$. Since $F(f)$ is injective, $F(\alpha) = F(\beta)$. Since F is faithful, $\alpha = \beta$. Hence f is also a monomorphism. The epimorphism case is similar.

Let φ be the inverse morphism of $F(f)\colon F(X) \to F(Y)$, since F is fully faithful, there exist a $g \in \mathrm{Hom}_{\mathcal{C}}(Y, X)$ such that $F(g) = \varphi$, moreover, it is the inverse morphism of f. □

Corollary A.3.10. *A fully faithful functor is necessarily injective on objects up to isomorphism.*

A.3.1 Natural Transformations and Functor categories

Definition A.3.11. Let F, G be two functors from $\mathcal{C}$ to $\mathcal{D}$. A morphism (or *natural transformation*) of functors $\pi\colon F \to G$ is the data for all $X \in \mathrm{ob}\,\mathcal{C}$ of a morphism $\pi(X)\colon F(X) \to G(X)$ such that for all $f\colon X \to Y$ in $\mathcal{C}$, the following diagram commutes:

$$\begin{array}{ccc} F(X) & \xrightarrow{\pi_X} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{\pi_Y} & G(Y) \end{array}$$

Hence, by considering the family of functors from $\mathcal{C}$ to $\mathcal{D}$ and the morphisms of such functors, we get a new category, denoted by $\mathbf{Fct}(\mathcal{C}, \mathcal{D})$ or simply $[\mathcal{C}, \mathcal{D}]$, or $\mathcal{D}^{\mathcal{C}}$.

Remark. If $\mathcal{C}$ and $\mathcal{D}$ are both *preadditive* categories, then we can consider the category of all additive functors from $\mathcal{C}$ to $\mathcal{D}$, denoted by $\mathbf{Add}(\mathcal{C}, \mathcal{D})$.

Example. Any ring R can be considered as a one-object preadditive category; the category of left modules over R is the same as the additive functor category $\mathbf{Add}(R, \mathbf{Ab})$, and the category of right $R-$modules is $\mathbf{Add}(R^{\mathrm{op}}, \mathbf{Ab})$. Because of this example, for any preadditive category $\mathcal{C}$, the category $\mathbf{Add}(\mathcal{C}, \mathbf{Ab})$ is sometimes called the "category of *left modules* over $\mathcal{C}$" and $\mathbf{Add}(\mathcal{C}^{\mathrm{op}}, \mathbf{Ab})$ is the category of *right modules* over $\mathcal{C}$.

Most constructions that can be carried out in $\mathcal{D}$ can also be carried out in $[\mathcal{C}, \mathcal{D}]$ by performing them "componentwise", separately for each object in $\mathcal{C}$.

For instance, if any two objects X and Y in $\mathcal{D}$ have a product $X \times Y$, then any two functors F and G in $[\mathcal{C}, \mathcal{D}]$ have a product $F \times G$, defined by $(F \times G)(c) = F(c) \times G(c)$ for every object c in $\mathcal{C}$.

Similarly, if $\eta_c \colon F(c) \longrightarrow G(c)$ is a natural transformation and each η_c has a kernel K_c in the category $\mathcal{D}$, then the kernel of η in the functor category $[\mathcal{C}, \mathcal{D}]$ is the functor K with $K(c) = K_c$ for every object c in $\mathcal{C}$.

As a consequence we have the general rule of thumb that the functor category $[\mathcal{C}, \mathcal{D}]$ shares most of the "nice" properties of $\mathcal{D}$:

- if $\mathcal{D}$ is complete (or cocomplete), then so is $[\mathcal{C}, \mathcal{D}]$;
- if $\mathcal{D}$ is an abelian category, then so is $[\mathcal{C}, \mathcal{D}]$;
- if $\mathcal{C}$ is any small category, then the category $[\mathcal{C}, \mathbf{Set}]$ of presheaves is a *topos*.

Proposition A.3.13. *the categories of directed graphs, $G-$sets and presheaves on a topological space X are all complete and cocomplete topoi, and that the categories of representations of G, modules over the ring R, and presheaves of abelian groups on a topological space X are all abelian, complete and cocomplete.*

Proposition A.3.14. *Every natural transformation $\pi \colon F \longrightarrow G$ defines a function which sends each arrow $f \colon A \longrightarrow B$ of $\mathcal{C}$ to an arrow $\pi_f \colon F(A) \longrightarrow G(B)$ of $\mathcal{D}$ in such a way that*

$$G(g) \circ \pi_f = \pi_{gf} = \pi_g \circ F(f)$$

for each composable pair g, f. Conversely, every such function π comes from a unique natural transformation with $\pi_X = \pi_{1_X}$.

Remark. This gives an arrows only description of a natural transformation.

Definition A.3.15. An *infranatural transformation* η from F to G is simply a family of morphisms $\eta_X \colon F(X) \longrightarrow G(X)$. Thus a natural transformation is an infranatural transformation for which $\eta_Y \circ F(f) = G(f) \circ \eta_X$ for every morphism $f \colon X \longrightarrow Y$. The *naturalizer* of η, $\mathrm{nat}(\eta)$, is the largest subcategory of $\mathcal{C}$ containing all the objects of $\mathcal{C}$ on which η restricts to a natural transformation.

Definition A.3.16. If, for every object X in $\mathcal{C}$, the morphism η_X is an isomorphism in $\mathcal{D}$, then η is said to be a *natural isomorphism*. Two functors F and G are said to be *naturally isomorphic* if there exists a natural isomorphism from F to G.

Example. Statements such as

> "Every group is *naturally isomorphic* to its opposite group"

abound in modern mathematics.

The content of the above statement is:

> "The identity functor $\mathrm{Id}\colon \mathbf{Grp} \longrightarrow \mathbf{Grp}$ is *naturally isomorphic* to the opposite functor $\mathrm{op}\colon \mathbf{Grp} \longrightarrow \mathbf{Grp}$."

Example. If K is a field, then for every vector space V over K we have a "natural" injective linear map $V \longrightarrow V^{**}$ from the vector space into its double dual. These maps are "natural" in the following sense: the double dual operation is a functor, and the maps are the components of a natural transformation from the identity functor to the double dual functor.

Definition A.3.19. A particular map between particular objects may be called an *unnatural isomorphism* (or "this isomorphism is not natural") if the map cannot be extended to a natural transformation on the entire category.

Remark. Some authors distinguish notationally, using $\cong$ for a natural isomorphism and $\approx$ for an unnatural isomorphism, reserving $=$ for equality (usually equality of maps).

Example. In group theory or module theory, a given decomposition of an object into a direct sum is "not natural", or rather "not unique", as automorphisms exist that do not preserve the direct sum decomposition

Example. fundamental group of torus

As an example of the distinction between the *functorial statement* and *individual objects*, consider homotopy groups of a product space, specifically the fundamental group of the torus.

> The homotopy groups of a product space are *naturally* the product of the homotopy groups of the components,
>
> $$\pi_n((X, x_0) \times (Y, y_0)) \cong \pi_n(X, x_0) \times \pi_n(Y, y_0)$$
>
> with the isomorphism given by projection onto the two factors, fundamentally because maps into a product space are exactly products of maps into the components.
>
> *This is a functorial statement.*

However, given the torus, which is abstractly a product of two circles, and thus has fundamental group isomorphic to $\mathbb{Z}^2$, but the splitting $\pi_1(T, t_0) \approx \mathbb{Z} \times \mathbb{Z}$ is not natural. Note the use of $\approx$, $\cong$, and $=$:

$$\pi_1(T, t_0) \approx \pi_1(S^1, x_0) \times \pi_1(S^1, y_0) \cong \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$$

This abstract isomorphism with a product *is not natural*, as some isomorphisms of T do not preserve the product: the self-homeomorphism of T (thought of as the quotient space $\mathbb{R}^2/\mathbb{Z}^2$) given by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ (geometrically a *Dehn twist* about one of the generating curves) acts as this matrix on $\mathbb{Z}^2$ (it's in the general linear group $\mathrm{GL}(\mathbb{Z}, 2)$ of invertible integer matrices), which does not preserve the decomposition as a product because it is not diagonal.

However, if one is given the torus as a product — equivalently, given a decomposition of the space — then the splitting of the group follows from the general statement earlier.

In categorical terms, the relevant category (preserving the structure of a product space) is "maps of product spaces, namely a pair of maps between the respective components".

Naturality is a categorical notion, and requires being very precise about exactly what data is given — the torus as a space that happens to be a product (in the category of spaces and continuous maps) is different from the torus presented as a product (in the category of products of two spaces and continuous maps between the respective components).

Example. dual of a finite-dimensional vector space

Every finite-dimensional vector space is isomorphic to its dual space, but this isomorphism relies on an arbitrary choice of isomorphism (for example, via choosing a basis and then taking the isomorphism sending this basis to the corresponding dual basis). There is in general no natural isomorphism between a finite-dimensional vector space and its dual space.

However, related categories (with additional structure and restrictions on the maps) do have a natural isomorphism.

In this category (finite-dimensional vector spaces with a *nondegenerate bilinear form*, maps linear transforms that respect the bilinear form), the dual of a map between vector spaces can be identified as a transpose.

Often for reasons of geometric interest this is specialized to a subcategory, by requiring that the nondegenerate bilinear forms have additional properties, such as being *symmetric* (*orthogonal matrices*), *symmetric* and *positive definite* (*inner product space*), *symmetric sesquilinear* (*Hermitian spaces*), *skew-symmetric* and *totally isotropic* (*symplectic vector space*), etc. — in all these categories a vector space is naturally identified with its dual, by the nondegenerate bilinear form.

Definition A.3.23. A functor $F\colon \mathcal{C} \to \mathcal{D}$ is an *equivalence* of categories if there exists $G\colon \mathcal{D} \to \mathcal{C}$ such that:

$$G \circ F \cong \mathrm{id}_{\mathcal{C}}$$
$$F \circ G \cong \mathrm{id}_{\mathcal{D}}$$

If such a functor exist, say $\mathcal{C}$ and $\mathcal{D}$ are *equivalent*, denoted by $\mathcal{C} \simeq \mathcal{D}$.

Remark. If two categories are equivalent, all results and concepts in one of them have their counterparts in the other one. This is why this notion of equivalence of categories plays an important role in Mathematics.

The following properties are easy to check

Theorem A.3.24. *The functor $F\colon \mathcal{C} \to \mathcal{D}$ is an equivalence of categories if and only if F is fully faithful and essentially surjective.*

Proposition A.3.25. *For any categories $\mathcal{C}, \mathcal{D}, \mathcal{E}$,*

1) $[\mathcal{C}, \mathcal{D}]^{\mathrm{op}} \simeq [\mathcal{C}^{\mathrm{op}}, \mathcal{D}^{\mathrm{op}}]$

2) $[\mathcal{C} \times \mathcal{D}, \mathcal{E}] \simeq [\mathcal{D}, [\mathcal{C}, \mathcal{E}]] \simeq [\mathcal{C}, [\mathcal{D}, \mathcal{E}]]$

A.3.2 Category of All Categories

Given functors and natural transformations:

$$\mathcal{C} \underset{G}{\overset{F}{\Downarrow \pi}} \mathcal{B} \underset{G'}{\overset{F'}{\Downarrow \tau}} \mathcal{A}$$

we first have the composite functors $F'F$ and $G'G$ and a commutative square

$$\begin{array}{ccc} F'F(X) & \xrightarrow{F'(\pi_X)} & F'G(X) \\ {\scriptstyle \tau_{F(X)}}\downarrow & & \downarrow{\scriptstyle \tau_{G(X)}} \\ G'F(X) & \xrightarrow{G'(\pi_X)} & G'G(X) \end{array}$$

Now define $(\tau \circ \pi)_X$ to be the diagonal of this square. Then $\tau \circ \pi$ is also a natural transformation. (Which will not be confused with the original composition of natural transformations: first, they are compositions in different categories; second, we will always use different nations. Indeed, we will use $\tau\pi$ to denote the original one.)

It is easy to check that all functors[1] form a category **Cat** under this composition (the horizontal composition). Moreover, for any functor $F\colon \mathcal{C} \longrightarrow \mathcal{D}$, the identity at F in **Cat** coincide with in $[\mathcal{C}, \mathcal{D}]$.

[1] Of course, we need a restriction. For instance, the functors between small categories.

Apart from this, For any functors and natural transformations:

$$\mathcal{C} \underset{\tau}{\overset{\pi}{\rightrightarrows}} \mathcal{B} \underset{\tau'}{\overset{\pi'}{\rightrightarrows}} \mathcal{A}$$

there is a identity (*interchange law*):

$$(\tau'\pi') \circ (\tau\pi) = (\tau' \circ \tau)(\pi' \circ \pi)$$

Conclusively, we have

Theorem A.3.26. Cat *has two compositions satisfying the interchange law and share the same identities.*

Corollary A.3.27. *The horizontal composition $\circ$ is a functor*

$$\circ \colon \mathcal{A}^{\mathcal{B}} \times \mathcal{B}^{\mathcal{C}} \longrightarrow \mathcal{A}^{\mathcal{C}}$$

More general, we define *double category* to be a category with two compositions satisfying interchange law. Further, a *2−category* is a double category which the two compositions share the same identities.

Example. Let G be a topological group with identity element e, while $\sigma, \sigma', \tau, \tau'$ are continuous loops in G at e. Define $\tau \circ \sigma$ to be the path σ followed by the path τ. Define $\tau\sigma$ to be the pointwise product of τ and σ. Then they form a 2−category.

Theorem A.3.29 (Hilton-Eckmann). *Let S be a set with two binary operations*

$$\cdot \colon S \times S \longrightarrow S \qquad \circ \colon S \times S \longrightarrow S$$

which both have the same unit element e and satisfying the interchange law. Then $\cdot$ and $\circ$ are equal, and each is commutative.

Corollary A.3.30. *The fundamental group of a topological group is abelian.*

Proposition A.3.31. *The functor category $\mathcal{D}^{\mathcal{C}} = [\mathcal{C}, \mathcal{D}]$ is itself a bijective $\mathbf{Cat}^{\mathrm{op}} \times \mathbf{Cat} \longrightarrow \mathbf{Cat}$. The arrow function sends a pair of functors $F \colon \mathcal{D} \longrightarrow \mathcal{D}'$ and $G \colon \mathcal{C}' \longrightarrow \mathcal{C}$ to the functor*

$$F^G \colon \mathcal{D}^{\mathcal{C}} \longrightarrow \mathcal{D}'^{\mathcal{C}'}$$

which defined on objects $S \in \mathcal{D}^{\mathcal{C}}$ as $F^G(S) = F \circ S \circ G$ and on arrows $\tau \colon S \longrightarrow T$ in $\mathcal{D}^{\mathcal{C}}$ as $F^G(\tau) = F \circ \tau \circ G$.

$$\mathcal{C}' \xrightarrow{G} \mathcal{C} \underset{T}{\overset{S}{\rightrightarrows}} \mathcal{D} \xrightarrow{F} \mathcal{D}'$$

Proposition A.3.32. *For categories $\mathcal{A}, \mathcal{B}, \mathcal{C}$ establish natural isomorphisms:*

$$(\mathcal{A} \times \mathcal{B})^{\mathcal{C}} \simeq \mathcal{A}^{\mathcal{C}} \times \mathcal{B}^{\mathcal{C}} \qquad \mathcal{C}^{\mathcal{A}\times\mathcal{B}} \simeq (\mathcal{C}^{\mathcal{B}})^{\mathcal{A}} \simeq (\mathcal{C}^{\mathcal{A}})^{\mathcal{B}}$$

A.3.3 Yoneda Lemma

Definition A.3.33. For a category $\mathcal{C}$, one can define two categories:

$$\mathcal{C}^\wedge \stackrel{\text{def}}{=} [\mathcal{C}^{\text{op}}, \mathbf{Set}]$$
$$\mathcal{C}^\vee \stackrel{\text{def}}{=} [\mathcal{C}, \mathbf{Set}]^{\text{op}}$$

and two functors:

$$\begin{aligned} \mathcal{M}^* \colon \mathcal{C} &\longrightarrow \mathcal{C}^\wedge & \qquad \mathcal{M}_* \colon \mathcal{C} &\longrightarrow \mathcal{C}^\vee \\ X &\longmapsto \mathcal{M}^X & \qquad X &\longmapsto \mathcal{M}_X \end{aligned}$$

where **Set** denoted the category of sets, $\mathcal{M}^X$ denoted the functor from $\mathcal{C}$ to **Set** which maps $Y \in \text{ob}\,\mathcal{C}$ to the set $\text{Hom}(Y, X)$, and $\mathcal{M}_X$ is similar.

Theorem A.3.34 (Yoneda Lemma). *For $F \in \text{ob}\,\mathcal{C}^\wedge$ and $X \in \text{ob}\,\mathcal{C}$, there is an isomorphism*

$$\text{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, F) \cong F(X)$$

which, moreover, is natural in both F and X.

Proof. For any $\alpha \in \text{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, F)$, let $\Phi(\alpha)$ be $\alpha_X(\text{id}_X)$. Which defined a map to $F(X)$. Conversely, for any $a \in F(X)$, let $\Psi(a)$ be a natural transformation such that for any $Y \in \text{ob}\,\mathcal{C}$ and morphism $f \colon Y \to X$, $\Psi(a)_Y(f) = F(f)(a)$.

To show that $\Psi(a)$ is natural, consider the following diagram for each $f \colon Y \to X$

$$\begin{array}{ccc} \mathcal{M}^X(X) & \xrightarrow{\Psi(a)_X} & F(X) \\ {\scriptstyle \mathcal{M}^X(f)}\downarrow & & \downarrow{\scriptstyle F(f)} \\ \mathcal{M}^X(Y) & \xrightarrow{\Psi(a)_Y} & F(Y) \end{array}$$

Let$g \in \mathcal{M}^X(X)$, then

$$\begin{aligned} F(f)\Psi(a)_X(g) &= F(f)F(g)(a) \\ &= F(gf)(a) \\ &= \Psi(a)_Y(gf) \\ &= \Psi(a)_Y(\mathcal{M}^X(f)(g)) \end{aligned}$$

Hence the diagram commutes and $\Psi(a)$ is natural.

For each $\alpha \in \text{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, F)$, consider the commutative diagram below

$$\begin{array}{ccc} \mathcal{M}^X(X) & \xrightarrow{\alpha_X} & F(X) \\ {\scriptstyle \mathcal{M}^X(f)}\downarrow & & \downarrow{\scriptstyle F(f)} \\ \mathcal{M}^X(Y) & \xrightarrow{\alpha_Y} & F(Y) \end{array}$$

It tells us that

$$\begin{aligned}\Psi(\Phi(\alpha))_Y(f) &= F(f)(\Phi(\alpha)) \\ &= F(f)(\alpha_X(\mathrm{id}_X)) \\ &= \alpha_Y(\mathcal{M}^X(f)(\mathrm{id}_X)) \\ &= \alpha_Y(f)\end{aligned}$$

Thus $\Psi(\Phi(\alpha)) = \alpha$. Hence $\Psi \circ \Phi = \mathrm{id}_{\mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, F)}$.

$$\begin{aligned}\Phi(\Psi(a)) &= \Psi(a)_X(\mathrm{id}_X) \\ &= F(\mathrm{id}_X)(a) \\ &= \mathrm{id}_{F(X)}(a) = a\end{aligned}$$

Hence $\Phi \circ \Psi = \mathrm{id}_{F(X)}$. Then, Φ is isomorphism.

To show this isomorphism is natural in F, consider the diagram below for any natural transformation $\pi\colon F \to G$

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, F) & \xrightarrow{\Phi} & F(X) \\ {\scriptstyle \mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, \pi)}\downarrow & & \downarrow{\scriptstyle \pi_X} \\ \mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, G) & \xrightarrow{\Phi} & G(X) \end{array}$$

For any $\alpha \in \mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, F)$, we have

$$\begin{aligned}\pi_X \Phi(\alpha) &= \pi_X \alpha_X(\mathrm{id}_X) \\ &= (\pi\alpha)_X(\mathrm{id}_X) \\ &= \Phi(\pi\alpha) \\ &= \Phi\,\mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, \pi)(\alpha)\end{aligned}$$

Thus the diagram commutes and Φ is natural in F.

Similar, for each $f\colon Y \to X$, consider the diagram below

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, F) & \xrightarrow{\Phi} & F(X) \\ {\scriptstyle \mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^f, F)}\downarrow & & \downarrow{\scriptstyle F(f)} \\ \mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^Y, F) & \xrightarrow{\Phi} & F(Y) \end{array}$$

For any $\alpha \in \mathrm{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, F)$, we have

$$\begin{aligned}F(f)\Phi(\alpha) &= F(f)\alpha_X(\mathrm{id}_X) \\ &= \alpha_Y \mathcal{M}^X(f)(\mathrm{id}_X) \\ &= \alpha_Y(\mathrm{id}_X\, f) \\ &= \alpha_Y(f)\end{aligned}$$

On the other hand

$$\begin{aligned}\Phi \operatorname{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^f, F)(\alpha) &= \Phi(\alpha \mathcal{M}^f) \\ &= (\alpha \mathcal{M}^f)_Y(\mathrm{id}_Y) \\ &= \alpha_Y \mathcal{M}^f_Y(\mathrm{id}_Y) \\ &= \alpha_Y(f \,\mathrm{id}_Y) \\ &= \alpha_Y(f)\end{aligned}$$

Thus the diagram commutes and Φ is natural in X. □

Corollary A.3.35. *The functor $\mathcal{M}^*$ is fully faithful.*

Proof. For any $X, Y \in \operatorname{ob}\mathcal{C}$, we have

$$\begin{aligned}\operatorname{Hom}_{\mathcal{C}^\wedge}(\mathcal{M}^X, \mathcal{M}^Y) &\cong \mathcal{M}^Y(X) \\ &= \operatorname{Hom}_{\mathcal{C}}(X, Y)\end{aligned}$$

□

Remark. One calls $\mathcal{M}^*$ the *Yoneda embedding*, sometimes denoted by $Y_{\mathcal{C}}$. Hence, one may consider $\mathcal{C}$ as a full subcategory of $\mathcal{C}^\wedge$. In particular, for $X \in \operatorname{ob}\mathcal{C}$, $\mathcal{M}^X$ determines X up to unique isomorphism, that is, an isomorphism $\mathcal{M}^X \cong \mathcal{M}^Y$ determines a unique isomorphism $X \cong Y$.

Remark. Some authors define an *embedding* to be a fully faithful functor. Such a functor is necessarily injective on objects up-to-isomorphism. For instance, the Yoneda embedding is an embedding in this sense.

Example. If $\mathcal{C}$ has products and coproducts, then there is a canonical isomorphism

$$(A \times B) + (A \times C) \cong A \times (B + C).$$

To prove this, by the remark above, it is enough to prove

$$\operatorname{Hom}(X, (A \times B) + (A \times C)) \cong \operatorname{Hom}(X, A \times (B + C))$$

for each $X \in \operatorname{ob}\mathcal{C}$ and this isomorphism is natural in X. Which is easy to check.

Corollary A.3.37. *Let $\mathcal{C}$ be a category and let $f\colon X \to Y$ be a morphism in $\mathcal{C}$.*

1) *Assume that for any $Z \in \mathcal{C}$, the map $\operatorname{Hom}_{\mathcal{C}}(Z, X) \xrightarrow{f\circ} \operatorname{Hom}_{\mathcal{C}}(Z, Y)$ is bijective. Then f is an isomorphism.*

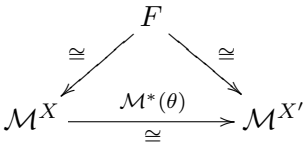
2) *Assume that for any $Z \in \mathcal{C}$, the map $\operatorname{Hom}_{\mathcal{C}}(X, Z) \xrightarrow{\circ f} \operatorname{Hom}_{\mathcal{C}}(Y, Z)$ is bijective. Then f is an isomorphism.*

Remark. If $\mathcal{C}$ is a preadditive category, then the Yoneda's lemma yields a full embedding of $\mathcal{C}$ into the functor category $\mathbf{Add}(\mathcal{C}^{\mathrm{op}}, \mathbf{Ab})$. So $\mathcal{C}$ naturally sits inside an abelian category.

A.3.4 Representable Functors

Definition A.3.38. One says that a functor $F\colon \mathrm{op}\,\mathcal{C} \to \mathbf{Set}$ is *representable* if there exists $X \in \mathrm{ob}\,\mathcal{C}$ such that $F(Y) \cong \mathrm{Hom}_{\mathcal{C}}(Y, X)$ functorially in $Y \in \mathcal{C}$. In other words, $F \cong \mathcal{M}^X$ in $\mathcal{C}^\wedge$. Such an object X is called a *representative* of F. Similarly, a functor $G\colon \mathcal{C} \to \mathbf{Set}$ is *representable* if there exists $X \in \mathrm{ob}\,\mathcal{C}$ such that $G(Y) \cong \mathrm{Hom}_{\mathcal{C}}(X, Y)$ functorially in $Y \in \mathcal{C}$.

Remark. It is important to notice that the isomorphisms above determine X up to unique isomorphism. More precisely, given two isomorphisms $F \xrightarrow{\cong} \mathcal{M}^X$ and $F \xrightarrow{\cong} \mathcal{M}^{X'}$ there exists a unique isomorphism $\theta : X \xrightarrow{\cong} X'$ making the following diagram commutative:



Definition A.3.39. Let $\mathcal{V}$ be a category. A $\mathcal{V}-$valued presheaf $\mathscr{F}$ on a category $\mathcal{C}$ is a functor $\mathscr{F}\colon \mathcal{C}^{\mathrm{op}} \longrightarrow \mathcal{V}$. Often presheaf is defined to be a $\mathbf{Set}-$valued presheaf. A morphism of presheaves is defined to be a natural transformation of functors. This makes the collection of all presheaves into a category, often written $\widehat{\mathcal{C}}$. A functor into $\widehat{\mathcal{C}}$ is sometimes called a *profunctor*.

Proposition A.3.40. *A locally small category $\mathcal{C}$ embeds fully and faithfully into the category $\widehat{\mathcal{C}}$ of $\mathbf{Set}-$valued presheaves via the Yoneda embedding $Y_{\mathcal{C}}$ which to every object A of $\mathcal{C}$ associates the hom-set $\mathrm{Hom}_{\mathcal{C}}(-, A)$.*

Proposition A.3.41. *The presheaf category $\widehat{\mathcal{C}}$ is (up to equivalence of categories) the free colimit completion of the category $\mathcal{C}$.*

A.4 Objects

A.4.1 Initial and Terminal Objects

Definition A.4.1. Let $\mathcal{C}$ be a category. An *initial object* of $\mathcal{C}$ is an object I in $\mathcal{C}$ such that for every object X in $\mathcal{C}$, there exists precisely one morphism $I \to X$. Dually, an object T is *terminal object* if for every object X in $\mathcal{C}$, there exists a single morphism $X \to T$. If an object is both initial and terminal, it is called a *zero object* or *null object*.

Remark. It is easy to see that the initial object and terminal object are unique up to isomorphism. Such universal properties will be detail in the limit theory later.

Remark. If $\mathcal{C}$ has a zero object 0, then given two objects X and Y in $\mathcal{C}$, there are canonical morphisms $f\colon 0 \longrightarrow X$ and $g\colon Y \longrightarrow 0$. Then, $f \circ g$ is a zero morphism in $\mathrm{Hom}_{\mathcal{C}}(Y, X)$. Thus, every category with a zero object is also a category with zero morphisms given by the composition $0_{XY}\colon X \longrightarrow 0 \longrightarrow Y$.

Not every category has terminal objects, for example:

Example. The category of infinite groups do not have a terminal object: given any infinite group G there are infinitely many morphisms $\mathbb{Z} \to G$, so G cannot be terminal.

A.4.2 Subobjects and Quotient Objects

Definition A.4.3. Let $A, B \in$ be objects in $\mathcal{C}$. If there exist a monomorphism $f\colon A \to B$, then we call (A, f) a *subobject* of B. If there exist an epimorphism $f\colon B \to A$, then we call (A, f) a *quotient object* of B.

Warning. Notice that the notation of subobject and quotient object may not be suitable abstract of sub- and quotient in usual sense. For example, Consider **Top**, the subobjects of an object are not just the subspaces, this concept mixes others. The same story happened in quotient objects.

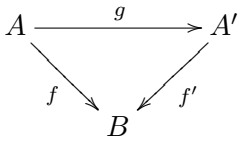
Example. In **Top**, every epimorphism is surjective. However, a quotient object may still not be a quotient space. In fact, for every topological space, the identity map from itself to the trivial topological space on the same underlying set is epimorphism.

Definition A.4.5. An *extremal monomorphism* is a monomorphism that cannot be nontrivially factored through an epimorphism. In another word, if $m = g \circ e$ with e an epimorphism, then e is an isomorphism. A subobject composed by an object with an extremal monomorphism is called an *extremal subobject*.

Example. The extremal subobject in **Top** is just the subspace with its inclusion map.

Remark. Notice that, in category theory, when we use the word "is", is actually under the meaning of "up to isomorphism". However, a bijective morphism may not be isomorphism. Which makes lots trouble, especially in epi- case: the concept of quotient object in the category of rings and topological spaces totally lose shape. Even consider special type of quotient objects like extremal ones may not work. The epimorphisms may be very mysterious.

Remark. Given two subobjects $(A, f), (A', f')$ of B, the morphism g from (A, f) to (A', f') is the morphism g (in fact, it is unique) in $\mathcal{C}$ such that the following diagram commutes:



Thus we get a category $\mathrm{Sub}_{\mathcal{C}}(B)$. Similar, we get $\mathrm{Qout}_{\mathcal{C}}(B)$.

A.4.3 Free Objects and Generators

Definition A.4.7. A *concrete category* $(\mathcal{C}, U)$ is a category $\mathcal{C}$ together with a faithful functor $U\colon \mathcal{C} \to \mathbf{Set}$, named *forgetful functor*. A category $\mathcal{C}$ is called *concretizable* if there exists such a forgetful functor.

Unlike the literal meaning, a concrete category may be very abstract. In fact, we have

Example. Let $\mathcal{C}$ be any small category, then there exists a faithful functor

$$\begin{aligned} P\colon \mathcal{C}^{\wedge} &\longrightarrow \mathbf{Set} \\ X &\longmapsto \coprod_{c \in \mathrm{ob}C} X(c) \end{aligned}$$

By composing this with the Yoneda embedding $\mathcal{M}^*\colon \mathcal{C} \to \mathcal{C}^{\wedge}$, one obtains a faithful functor $\mathcal{C} \to \mathbf{Set}$.

Not every category, whose objects are based on sets, are concretizable. For example

Example. The homotopy category of topological spaces **hTop**, which has same objects as **Top** but its morphisms are homotopy classes of continuous functions, is an example of a category that is not concretizable. The fact that there does not exist any faithful functor from **hTop** to **Set** was first proven

by Peter Freyd, see [Freyd, 1970]. In the same article, Freyd cites an earlier result that the category of "small categories and natural equivalence-classes of functors" also fails to be concretizable.

A category $\mathcal{C}$ may admit several faithful functors into **Set**. Hence there may be several concrete categories $(\mathcal{C}, U)$ all corresponding to the same category $\mathcal{C}$.

Example. For technical reasons, the category $\mathbf{Ban}_1$ of Banach spaces and linear contractions is often equipped not with the "obvious" forgetful functor but the functor $U_1 \colon \mathbf{Ban}_1 \to \mathbf{Set}$ which maps a Banach space to its (closed) unit ball.

Notice that, the forgetful functor may map different objects to the same set and, if this occurs, it will also map different morphisms to the same function, which is not contradictory to faithful.

Example. A set X can be equipped different topologies, hence become different objects in **Top**, and their identity maps are different morphisms. However, the usual forgetful functor maps them to the same set X and their identity maps to one id_X.

Definition A.4.12. A left adjoint functor F of a forgetful functor U is called the *free functor*. Let S be a set, then $F(S)$ is called the *free object* generated by S.

Remark. Since F is the adjoint functor of U, there must be a natural transformation $\eta \colon \mathrm{id}_{\mathbf{Set}} \to U \circ F$. More explicitly, F is, up to isomorphisms in $\mathcal{C}$, characterized by the following universal property:

> Whenever $T \in \mathrm{ob}\,\mathcal{C}$, and $f \colon S \to U(T)$ is a function, then there is a unique $\mathcal{C}-$morphism $g \colon F(S) \to T$ such that $U(g) \circ \eta(S) = f$.

Since the last section of Chapter I of Lang's textbook has discussed the free functor of **Grp** in detail, we will not repeat them here.

A related but different concept is the generator

Definition A.4.13. A *generator* (or *separator*) of a category $\mathcal{C}$ is an object G, such that for any two different morphisms $f, g \colon X \to Y$, there exist one morphism $h \colon G \to H$ such that $f \circ h \neq g \circ h$.

Example. $\mathbb{Z}$ is a generator in **Ab**. Similarly, the one-point set is a generator for **Set**.

A.5 Limit Theory

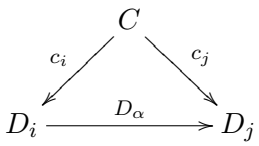
A.5.1 Cones and Limits

Definition A.5.1. Let $\mathcal{J}$ and $\mathcal{C}$ be categories. A *diagram of type* $\mathcal{J}$ or a $\mathcal{J}-$*diagram* in $\mathcal{C}$ is a functor $D\colon \mathcal{J} \to \mathcal{C}$. The category $\mathcal{J}$ is called the *index category* or the *scheme* of the diagram D. For j in the index category, we will write $D(j)$ in the form D_j.

A *cone* to a diagram D consists of an object C in $\mathcal{C}$ and a family of arrows in $\mathcal{C}$,

$$c_j\colon C \longrightarrow D_j, \forall j \in \operatorname{ob}\mathcal{J}$$

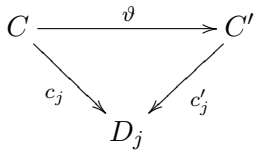
such that for each arrow $\alpha\colon i \to j$ in $\mathcal{J}$, the following triangle commutes.



A morphism of cones

$$\vartheta\colon (C, c_j) \longrightarrow (C', c'_j)$$

is an arrow ϑ in $\mathcal{C}$, making each triangle



commute.

Finally, cones to D with morphisms between them form a category $\mathbf{Cone}(D)$ (or denote $\Delta \downarrow D$).

Definition A.5.2. A *limit* for a diagram $D\colon \mathcal{J} \to \mathcal{C}$ is a terminal object in $\mathbf{Cone}(D)$. In particular, a finite limit is a limit for a diagram on a finite index category $\mathcal{J}$.

Remark. One often denote a limit in the form

$$p_i\colon \varprojlim_j D_j \longrightarrow D_i$$

When $\{p_i\}$ are obvious, one may simply call the object as the limit.

Example. Let $\mathbf{0}$ be the empty category, then in any category $\mathcal{C}$, there is only one diagram of type $\mathbf{0}$: the empty one. A cone to the empty diagram is essentially just an object of $\mathcal{C}$. The limit of the empty diagram is just the *terminal* object in $\mathcal{C}$.

Example. Let $\mathcal{C}$ be a small category, $\mathrm{id}_{\mathcal{C}} \colon \mathcal{C} \to \mathcal{C}$ is the identity functor. If $\mathcal{C}$ has initial object I, then I is the limit of $\mathrm{id}_{\mathcal{C}}$. Conversely, if $\{p_B \colon A \to B \mid B \in \mathrm{ob}\,\mathcal{C}\}$ is the limit of $\mathrm{id}_{\mathcal{C}}$, then its easy to see that it is the *initial* object in $\mathcal{C}$.

Example. Take $\mathcal{J} = \{1, 2\}$ the discrete category with two objects and no nonidentity arrows. A diagram $D \colon \mathcal{J} \to \mathcal{C}$ hence is a pair of objects $D_1, D_2 \in \mathcal{C}$. A cone to D is an object C equipped with arrows

$$D_1 \xleftarrow{c_1} C \xrightarrow{c_2} D_2$$

The limit of D is just the *product* of D_1 and D_2 in $\mathcal{C}$.

Example. Take $\mathcal{J}$ to be the following category:

$$1 \underset{\beta}{\overset{\alpha}{\rightrightarrows}} 2$$

Hence a diagram D of type $\mathcal{J}$ looks like

$$D_1 \underset{D_\beta}{\overset{D_\alpha}{\rightrightarrows}} D_2$$

The limit of D is the *equalizer* of D_α, D_β.

Example. Let $(I, \leqslant)$ be a *filtered partially ordered set* (FPOS), which means that for each two elements i, j, there exist an element $k \in I$ such that $k \leqslant i, k \leqslant j$. Treat I as a category, in any category $\mathcal{C}$, a diagram $D \colon I \to \mathcal{C}$ satisfy that for any $i \leqslant j \leqslant k$ in I, $D_{j \leqslant k} D_{i \leqslant j} = D_{i \leqslant k}$ is called an *inverse system* and its limit is called an *inverse limit*, or *projective limit*.

The limit of a diagram sometimes works like monomorphism, although each arrow in the cone may not be injective.

Proposition A.5.8. *Let $\{p_j \colon A \to D_j \mid j \in \mathrm{ob}\,\mathcal{J}\}$ be the limit of diagram $D \colon \mathcal{J} \to \mathcal{C}$. For any $f, g \colon B \to A$, if $p_j f = p_j g, \forall j \in \mathrm{ob}\,\mathcal{J}$, then $f = g$.*

Example. Let $\{(A_i, f_i) \mid i \in I\}$ be a family of subobject of A in $\mathcal{C}$. Treat $\{f_i \colon A_i \to A \mid i \in I\}$ as a subcategory of $\mathcal{C}$. hence its inclusion functor is a diagram in $\mathcal{C}$. If such a diagram has limit C, then then arrow from C to A can be determined by each arrow α_i from C to A_i. Use the proposition above, it is easy to check that $f_i \alpha_i \colon C \to A$ is injective, hence $(C, f_i \alpha_i)$ is also a subobject of A, called the *intersection* of $\{(A_i, f_i) \mid i \in I\}$.

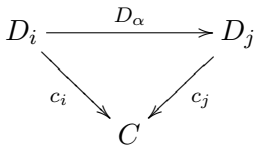
A.5.2 Co-cones and Colimits

Dually, we have corresponding concepts

Definition A.5.10. A *co-cone* to a diagram D consists of an object C in $\mathcal{C}$ and a family of arrows in $\mathcal{C}$,

$$c_j \colon D_j \longrightarrow C, \forall j \in \operatorname{ob} \mathcal{J}$$

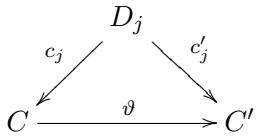
such that for each arrow $\alpha \colon i \to j$ in $\mathcal{J}$, the following triangle commutes.



A morphism of co-cones

$$\vartheta \colon (C, c_j) \longrightarrow (C', c'_j)$$

is an arrow ϑ in $\mathcal{C}$, making each triangle



commute.

Finally, co-cones to D with morphisms between them form a category $\mathbf{Cocone}(D)$ (or denote $D \downarrow \Delta$).

Definition A.5.11. A *colimit* for a diagram $D \colon \mathcal{J} \to \mathcal{C}$ is a initial object in $\mathbf{Cocone}(D)$. In particular, a finite colimit is a colimit for a diagram on a finite index category $\mathcal{J}$.

Remark. One often denote a colimit in the form

$$k_i \colon \varinjlim_j D_j \longleftarrow D_i$$

When $\{k_i\}$ are obvious, one may simply call the object as the colimit.

Example. Let $\mathcal{C}$ be a small category, the colimit of the identity functor is just the *terminal* object in $\mathcal{C}$.

Example. Take $\mathcal{J} = \{1, 2\}$ the discrete category with two objects and no nonidentity arrows. A diagram $D \colon \mathcal{J} \to \mathcal{C}$ hence is a pair of objects $D_1, D_2 \in \mathcal{C}$. A co-cone to D is an object C equipped with arrows

$$D_1 \xrightarrow{c_1} C \xleftarrow{c_2} D_2$$

The colimit of D is just the *coproduct* of D_1 and D_2 in $\mathcal{C}$.

Example. Take noations as in A.5.6, the colimit of D is the *coequalizer* of D_α, D_β.

Example. Let $(I, \leqslant)$ be a *directed partially ordered set* (DPOS), which means that for each two elements i, j, there exist an element $k \in I$ such that $i \leqslant k, j \leqslant k$. Treat I as a category, in any category $\mathcal{C}$, a diagram $D\colon I \to \mathcal{C}$ satisfy that for any $i \leqslant j \leqslant k$ in I, $D_{j\leqslant k} D_{i\leqslant j} = D_{i\leqslant k}$ is called an *direct system* and its colimit is called an *direct limit*, or *inductive limit*.

The colimit of a diagram sometimes works like epimorphism, although each arrow in the cone may not be surjective.

Proposition A.5.16. *Let $\{k_j\colon D_j \to A \mid j \in \operatorname{ob}\mathcal{J}\}$ be the limit of diagram $D\colon \mathcal{J} \to \mathcal{C}$. For any $f, g\colon A \to B$, if $fk_j = gk_j, \forall j \in \operatorname{ob}\mathcal{J}$, then $f = g$.*

Example. Let $\{(A_i, f_i) \mid i \in I\}$ be a family of quotient object of A in $\mathcal{C}$. Treat $\{f_i\colon A \to A_i \mid i \in I\}$ as a subcategory of $\mathcal{C}$. hence its inclusion functor is a diagram in $\mathcal{C}$. If such a diagram has colimit C, then then arrow from A to C can be determined by each arrow α_i from A_i to C. Use the proposition above, it is easy to check that $\alpha_i f_i\colon A \to C$ is surjective, hence $(C, f_i\alpha_i)$ is also a quotient object of A, called the *cointersection* of $\{(A_i, f_i) \mid i \in I\}$.

Proposition A.5.18. *Colimits are linked to limits via*

$$\operatorname{Hom}(\varinjlim_{\mathcal{J}} X_i, Y) = \varprojlim_{\mathcal{J}^{\mathrm{op}}} \operatorname{Hom}(X_i, Y)$$

Proof. For any connection morphism $\phi_j^i\colon X_i \longrightarrow X_j$ in (X_i), the corresponding connection map in $(\operatorname{Hom}(X_i, Y))$ is

$$\begin{aligned} \operatorname{Hom}(X_j, Y) &\longrightarrow \operatorname{Hom}(X_i, Y) \\ f &\longmapsto f \circ \phi_j^i \end{aligned}$$

Use this corresponding, the statement is easy to verify. □

A similar proposition is

Proposition A.5.19.

$$\operatorname{Hom}(X, \varprojlim_{\mathcal{J}} Y_i) = \varprojlim_{\mathcal{J}} \operatorname{Hom}(X, Y_i)$$

Proof. For any connection morphism $\phi_j^i\colon Y_i \longrightarrow Y_j$ in (Y_i), the corresponding connection map in $(\operatorname{Hom}(X, Y_i))$ is

$$\begin{aligned} \operatorname{Hom}(X, Y_i) &\longrightarrow \operatorname{Hom}(X, Y_j) \\ f &\longmapsto \phi_j^i \circ f \end{aligned}$$

Use this corresponding, the statement is easy to verify. □

A.5.3 Kernels and Cokernels

Definition A.5.20. Let $\{f_i\}$ be a family of parallel morphisms, which can be view as a diagram. the *equalizer* is the limit of the diagram. Dually, the *coequalizer* is the colimit.

Remark. The correct diagram for the degenerate case with *no morphisms* is slightly subtle: one might initially draw the diagram as consisting of the two objects X, Y and no morphisms. This is incorrect, however, since the limit of such a diagram is the product of these two objects, rather than the equalizer. (And indeed products and equalizers are different concepts: the set-theoretic definition of them are different.)

Instead, the appropriate insight is that every equalizer diagram is fundamentally concerned with the X, including Y only because Y is the codomain of morphisms which appear in the diagram.

With this view, we see that if there are no morphisms involved, Y does not make an appearance and the equalizer diagram consists of X alone. The limit of this diagram is then any isomorphism to X.

Similarly, the correct coequalizer diagram of *no morphisms* consists of the codomain alone.

Definition A.5.21. An equalizer of exactly two morphisms is sometimes called the *difference kernel* of them.

Proposition A.5.22. *Any equalizer is a monomorphism. Dually, any coequalizer is an epimorphism.*

Remark. A monomorphism is said to be *regular* if it is an equalizer of some set of morphisms. Dually, an epimorphism is said to be *regular* if it is a coequalizer of some set of morphisms.

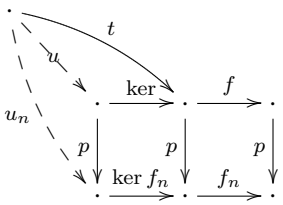
Definition A.5.23. The *kernel* of a morphism f is the equaliser of f and the parallel zero morphism. Dually, The *cokernel* is the coequalizer of f and the parallel zero morphism.

Definition A.5.24. A monomorphism is called *norm*, if it is a kernel of some morphism. Dually, an epimorphism is called *norm*, if it is a cokernel of some morphism.

Example. Coequalisers can be large: There are exactly two functors from the category **1** having one object and one identity arrow, to the category **2** with two objects and exactly one non-identity arrow going between them. The coequaliser of these two functors is the monoid of natural numbers under addition, considered as a one-object category. In particular, this shows that while every coequalising arrow is epic, it is not necessarily surjective.

Proposition A.5.26. *The kernel of the limit is also the limit of the kernels. Dually, the cokernel of the colimit is also the colimit of the cokernels.*

Proof. We start with a commutative diagram:



Here, f is the limit of f_n, and ker is the limit of the kernels, we want to show that it is also the kernel of f.

First, by the collective injectivity of limit (ref. A.5.8), the composition of f and ker is equal to 0.

Then, for any t such that $f \circ t = 0$, we have $f_n \circ p \circ t = 0$, hence there exist a unique morphism u_n such that $\ker f_n \circ u_n = p \circ t$. By the definition of limit, there exist a unique morphism u such that $u_n = p \circ u$. Hence $p \circ \ker \circ u = p \circ t$. By the collective injectivity again, $\ker \circ u = t$, which proves ker is the kernel of f. □

A.5.4 Products and Coproducts

Definition A.5.27. Consider a diagram of type $\mathcal{J}$, where $\mathcal{J}$ is a discrete category. It looks like a family of objects without arrows between them. The limit of such a diagram is called the *product* of these objects. Dually, the colimit of such a diagram is called the *coproduct* of these objects.

Remark. We often denote the product and the coproduct of a family of objects $\{A_i\}_{i \in I}$ as $\prod A_i$ and $\coprod A_i$.

Example. Since the nullary discrete category is the empty category, the *nullary product* is just the terminal object. Similar, the *unary product* of any object is itself. Dually, we get *nullary coproduct* and *unary coproduct*.

Proposition A.5.29. *A category has finite products, which means that each family of finite objects has product, if and only if it has binary product and terminal object.*

Proof. For $n \geqslant 2$, it is clear that $(\cdots((A_1 \times A_2) \times A_3) \cdots \times A_n)$ is the $n-$ary product of $A_1, A_2 \cdots, A_n$. Notice that the word "finite" include the nullary case, so we still need the existence of terminal object. □

Definition A.5.30. Let $\{f_i\colon A_i \to B_i\}_{i\in I}$ be family of morphisms in a category has products, the product of them is the only morphism $\Pi f_i\colon \Pi A_i \to \Pi B_i$ make the following diagram commutative

$$\begin{array}{ccc} \Pi A_i & \xrightarrow{\Pi f_i} & \Pi B_i \\ \downarrow & & \downarrow \\ A_j & \xrightarrow{f_j} & B_j \end{array}$$

Proposition A.5.31. *Product is a functor from $[I, \mathcal{C}]$ to $\mathcal{C}$.*

Proof. It's easy to check by definition. □

Remark. Similar, we can define coproduct of morphisms and check coproduct is a functor. More general, limit and colimit are functors.

Proposition A.5.32. *Monomorphisms are stable under product, which means the product of a family of monomorphisms is also a monomorphism.*

Proposition A.5.33. *In a category has products, for any $i \in I$, let (E_i, e_i) be the equalizer of $f_i, g_i\colon A_i \to B_i$, then, $(\Pi E_i, \Pi e_i)$ is the equalizer of $\Pi f_i, \Pi g_i\colon \Pi A_i \to \Pi B_i$.*

Proposition A.5.34. *Regular monomorphisms are stable under product, and so are isomorphisms.*

Dually, we have similar propositions for coproduct.

A.5.5 Pullback and Pushout

Definition A.5.35. Let $\mathcal{J}$ be

$$\cdot \longrightarrow \cdot \longleftarrow \cdot$$

a limit for a $\mathcal{J}-$diagram is of the form

$$A \xrightarrow{f} C \xleftarrow{g} B$$

which can be view as a commutative square in $\mathcal{C}$:

$$\begin{array}{ccc} P & \xrightarrow{\overline{f}} & B \\ {\scriptstyle \overline{g}}\downarrow & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array}$$

we call it a *pullback square* or *cartesian diagram*, and say $\overline{g}$ is the *pullback* of g through f, $\overline{f}$ is the *pullback* of f through g. We also call this limit the *fibre product* of A and B over C, and denoted by $A \times_C B$.

Sometime, we consider such kind of category, in which every pullback exist, we call it a *category with pullbacks* or say it *has* pullbacks.

Proposition A.5.36. *Let* $A \xrightarrow{f} C \xleftarrow{g} B$ *be a pair of morphisms in* $\mathcal{C}$*, and* $A \xleftarrow{p_A} A \times B \xrightarrow{p_B} B$ *be the product of* A *and* B*,* $e\colon E \to A \times B$ *is the equalizer of* fp_A *and* gp_B*. Then the following diagram is cartesian:*

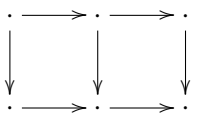
$$\begin{array}{ccc} E & \xrightarrow{p_B e} & B \\ {\scriptstyle p_A e}\downarrow & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array}$$

Proposition A.5.37. *Monomorphisms are* stable *under pullback, which means that the pullback of a monomorphism is also a monomorphism. Moreover, regular monomorphisms are also stable, and so are isomorphisms.*

Warning. Epimorphisms may not be stable under pullback in any category with pullbacks.

The following proportion is a good exercise for diagram chase:

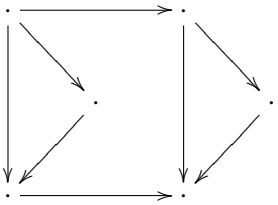
Proposition A.5.38 (Two-pullbacks). *Consider a commutative diagram in a category with pullbacks as below:*



1) If the two small squares are pullbacks, so is the outer rectangle.

2) If the right square and the outer rectangle are pullbacks, so is the left square.

Corollary A.5.39. *The pullback of a commutative triangle is a commutative triangle.*



The dual concept of pullback is pushout.

Definition A.5.40. Let $\mathcal{J}'$ be

a limit for a $\mathcal{J}'-$diagram is of the form

$$B \xleftarrow{g} C \xrightarrow{f} A$$

which can be view as a commutative square in $\mathcal{C}$:

$$\begin{array}{ccc} C & \xrightarrow{f} & A \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle \overline{g}} \\ B & \xrightarrow{\overline{f}} & P \end{array}$$

we call it a *pushout square* or *cocartesian diagram*, and say $\overline{g}$ is the *pushout* of g through f, $\overline{f}$ is the *pushout* of f through g. We also call this limit the *fibre coproduct* of A and B over C, and denoted by $A \amalg_C B$.

By the duality principle, the duality of the properties of pullback are also true.

Definition A.5.41. Let $\overline{f}$ be the pullback of f through g, it is called *descendable* if f is also the pushout of $\overline{f}$ through g.

Proposition A.5.42. *Let $\mathcal{C}$ be a category with pullbacks (resp, pushouts), then taking pullback (resp. pushout) is a functor from $[\mathcal{J},\mathcal{C}]$ to $[\mathcal{J}',\mathcal{C}]$ (resp. from $[\mathcal{J}',\mathcal{C}]$ to $[\mathcal{J},\mathcal{C}]$).*

A.5.6 Complete Categories

Definition A.5.43. A category is said to be *complete*, if every diagram in it has a limit. Similar, a *finite complete category* is such a category, in which every finite diagram has a limit. Dually, we have concepts of *cocomplete category* and *finite cocomplete category*.

Theorem A.5.44. *Let $\mathcal{C}$ be a category, the following statements are equivalent:*

a) C is finite complete.

b) C has finite products and equalizers.

c) C has pullbacks and terminal object.

A.6 Exactness

A.6.1 Exact Categories

Definition A.6.1. An *exact category* $\mathcal{E}$ is an additive category possessing a class $\mathfrak{E}$ of "short exact sequences": triples of objects connected by arrows

$$M' \longrightarrow M \longrightarrow M''$$

satisfying the following axioms inspired by the properties of short exact sequences in an abelian category:

1. $\mathcal{E}$ is closed under isomorphisms and contains the split exact sequences:

$$M' \longrightarrow M' \oplus M'' \longrightarrow M''$$

2. Suppose $M \to M''$ occurs as the second arrow of a sequence in $\mathfrak{E}$ (it is called an *admissible epimorphism*) and $N \to M''$ is any arrow in $\mathcal{E}$. Then their *pullback* exists and its *projection* to N is also an admissible epimorphism.

   Dually, if $M' \to M$ occurs as the first arrow of a sequence in $\mathfrak{E}$ (it is called an *admissible monomorphism*) and $M' \to N$ is any arrow, then their *pushout* exists and its *coprojection* from N is also an admissible monomorphism.

   In other words, the admissible epimorphisms are "stable under pullback", resp. the admissible monomorphisms are "stable under pushout".

3. Admissible monomorphisms are *kernels* of their corresponding admissible epimorphisms, and dually. The composition of two admissible monomorphisms is admissible (likewise admissible epimorphisms);

4. Suppose $M \to M''$ is a map in $\mathcal{E}$ which admits a kernel in $\mathcal{E}$, and suppose $N \to M$ is any map such that the composition $N \to M \to M''$ is an admissible epimorphism. Then so is $M \to M''$.

   Dually, if $M' \to M$ admits a cokernel and $M \to N$ is such that $M' \to M \to N$ is an admissible monomorphism, then so is $M' \to M$.

Remark. Admissible monomorphisms are generally denoted $\rightarrowtail$ and admissible epimorphisms are denoted $\twoheadrightarrow$. These axioms are not minimal; in fact, the last one has been shown by Bernhard Keller [Keller, 1990] to be redundant.

Definition A.6.2. An *exact functor* F from an exact category $\mathcal{D}$ to another one $\mathcal{E}$ is an additive functor such that if

$$M' \rightarrowtail M \twoheadrightarrow M''$$

is exact in $\mathcal{D}$, then

$$F(M') \rightarrowtail F(M) \twoheadrightarrow F(M'')$$

is exact in $\mathcal{E}$.

Definition A.6.3. A subcategory $\mathcal{D}$ of $\mathcal{E}$ is called an *exact subcategory* if the inclusion functor is fully faithful and exact.

Definition A.6.4. A *Serre subcategory* is a non-empty full subcategory $\mathcal{S}$ of an abelian category $\mathcal{A}$ such that for all short exact sequences

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

in $\mathcal{A}$, M belongs to $\mathcal{S}$ if and only if both M' and M'' do. This notion arises from Serre's C-theory.

Example. Exact categories come from abelian categories in the following way. Suppose $\mathcal{A}$ is abelian and let $\mathcal{S}$ be any Serre subcategory. We can take the class $\mathfrak{E}$ to be simply the sequences in $\mathcal{S}$ which are exact in $\mathcal{A}$; that is,

$$M' \longrightarrow M \longrightarrow M''$$

is in $\mathfrak{E}$ iff

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is exact in $\mathcal{A}$. Then $\mathcal{S}$ is an exact category.

Remark. The condition Serre subcategory can be weakened to be a strictly full additive subcategory which is closed under taking *extensions* in the sense that given an exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

in $\mathcal{A}$, then if M', M'' are in E, so is M.

Example. The category $\mathbf{Ab}_{\text{tf}}$ of torsion-free abelian groups is exact.

Example. The category $\mathbf{Ab}_{\text{tor}}$ of abelian groups with torsion (and also the zero group) is exact.

A.6.2 Exact Functors

Definition A.6.8. Let $\mathcal{A}, \mathcal{B}$ be two abelian categories, $F\colon \mathcal{A} \longrightarrow \mathcal{B}$ is an additive functor. Let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a short exact sequence in $\mathcal{A}$. We say that F is

- *half exact* if $F(A) \longrightarrow F(B) \longrightarrow F(C)$ is exact.
- *left exact* if $0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C)$ is exact.
- *right exact* if $F(A) \longrightarrow F(B) \longrightarrow F(C) \longrightarrow 0$ is exact.
- *exact* if $0 \longrightarrow F(A) \longrightarrow F(B) \longrightarrow F(C) \longrightarrow 0$ is exact.

For contravariant functor, the definition is similar.

Proposition A.6.9. *A covariant (not necessarily additive) functor is left exact if and only if it turns finite limits into limits; a covariant functor is right exact if and only if it turns finite colimits into colimits; a contravariant functor is left exact if and only if it turns finite colimits into limits; a contravariant functor is right exact if and only if it turns finite limits into colimits. A functor is exact if and only if it is both left exact and right exact.*

Proposition A.6.10. *If the functor F is left adjoint to G, then F is right exact and G is left exact.*

The degree to which a left exact functor fails to be exact can be measured with its right derived functors; the degree to which a right exact functor fails to be exact can be measured with its left derived functors.

A.7 Diagram Lammas in Abelian Categories

Throughout of this section, the category is assumed to be abelian unless otherwise specified.

A.7.1 Abelian Category

The concept of abelian category has been introduced in Chapter 1. We discuss some properties of abelian categories.

Proposition A.7.1. *A morphism $f\colon A \longrightarrow B$ is monoic (resp. epi) if and only if $\ker f = 0$ (resp. $\operatorname{coker} f = 0$) if and only if $\operatorname{coim} f = 1_A$ (resp. $\operatorname{im} f = 1_B$) if and only if $f = \operatorname{im} f$ (resp. $f = \operatorname{coim} f$).*

Proof. We prove the monoic case only, the epi case is dual to it.

($\text{monoic} \Longrightarrow \ker f = 0$.) We have $f \circ \ker f = 0 = f \circ 0$, since$f$ is monoic, $\ker f = 0$.

($\ker f = 0 \Longrightarrow \operatorname{coim} f = 1_A$.) It is easy to check that 1_A satisfying the universal property of $\operatorname{coim} f$.

($\operatorname{coim} f = 1_A \Longrightarrow f = \operatorname{im} f$.) By the natural isomorphism Ψ.

($f = \operatorname{im} f \Longrightarrow$ monoic.) A kernel is always monoic. □

Proposition A.7.2. *Any bimorphism must be a isomorphism.*

Proof. Suppose $f\colon A \longrightarrow B$ is a bimorphism, which means that f is both monoic and epi, hence $\operatorname{coim} f = 1_A$ and $\operatorname{im} f = 1_B$ by Proposition A.7.1. Whence the standard factorization become $f = \Psi$ which is a isomorphism in an abelian category. □

Corollary A.7.3. *Every morphism f can be uniquely factorized as an epimorphism e followed by a monomorphism m. Moreover, $e = \operatorname{coim} f$, $m = \operatorname{im} f$.*

Lemma A.7.4. *Let f be factorized as h followed by g, then*

(i) If g is monoic, then $\ker f = \ker h$;

(ii) If h is epi, then $\operatorname{coker} f = \operatorname{coker} g$.

Proof. By check the definition, the statements are clearly true and hold in any category where related concepts make sense. □

Definition A.7.5. A monomorphism is called *norm*, if it is a kernel of some morphism. Dually, an epimorphism is called *norm*, if it is a cokernel of some morphism.

We now introduce some equivalent conditions of abelian category.

Proposition A.7.6. *A pre-abelian category becomes abelian if and only if all monomorphisms and epimorphisms are normal.*

Proof. The "only if" comes from Proposition A.7.1.

Conversely, if all monomorphisms and epimorphisms are normal, then for every morphism f, □

A.7.2 Cartesian Diagrams

Lemma A.7.7. *Consider the following diagram:*

$$\begin{array}{ccc} E & \xrightarrow{f'} & B \\ {\scriptstyle g'}\downarrow & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & C \end{array}$$

(i) The diagram is commutative if and only if the composition

$$E \xrightarrow{\langle f',g'\rangle} A \oplus B \xrightarrow{\langle f,-g\rangle} C$$

is equal to 0. *Where* $\langle f', g'\rangle$ *is the unique morphism such that* $f' = p_2\langle f', g'\rangle$ *and* $g' = p_1\langle f', g'\rangle$, $\langle f, -g\rangle$ *is the unique morphism such that* $f = \langle f, -g\rangle i_1$ *and* $-g = \langle f, -g\rangle i_2$.

(ii) This diagram is cartesian if and only if $\langle f', g'\rangle = \ker\langle f, -g\rangle$.

(iii) This diagram is cocartesian if and only if $\langle f, -g\rangle = \operatorname{coker}\langle f', g'\rangle$.

Proof. (i) By the definition, we have

$$fg' - gf' = \langle f, -g\rangle i_1 p_1\langle f', g'\rangle + \langle f, -g\rangle i_2 p_2\langle f', g'\rangle = \langle f, -g\rangle\langle f', g'\rangle$$

Hence $fg' = gf'$ if and only if $\langle f, -g\rangle\langle f', g'\rangle = 0$.

(ii) It follows from Proposition A.5.36.

(iii) It is the dual of *(ii)*. □

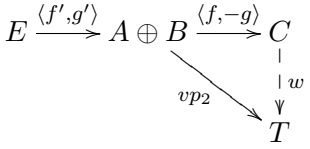
Proposition A.7.8. *In a cartesian diagram, if* f *is an epimorphism, then so is* f'*, and the diagram is also cocartesian.*

Proof. If f is epimorphism, then so is $\langle f, -g\rangle$: let $u\colon C \longrightarrow T$ be an arbitrary morphism such that $u\langle f, -g\rangle = 0$, then $uf = u\langle f, -g\rangle i_1 = 0$, which implies $u = 0$. Thus we get an exact sequence:

$$0 \longrightarrow E \xrightarrow{\langle f',g'\rangle} A \oplus B \xrightarrow{\langle f,-g\rangle} C \longrightarrow 0$$

Hence $\langle f, -g\rangle = \operatorname{coker}\langle f', g'\rangle$, and the diagram is cocartesian.

Let $v\colon B \longrightarrow T$ be an arbitrary morphism such that $vf' = 0$, then $vp_2\langle f', g'\rangle = 0$, hence there exists a morphism $w\colon C \longrightarrow T$ such that $vp_2 = w\langle f, -g\rangle$.



We then have (notice that $p_2 i_1 = 0$)

$$0 = vp_2 i_1 = w\langle f, -g\rangle i_1 = wf$$

hence $w = 0$ and therefore $v = 0$. □

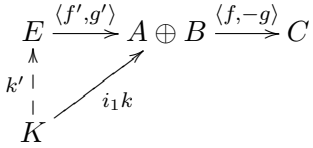
Proposition A.7.9. *In a cartesian diagram, let $k\colon K \longrightarrow A$ be the kernel of f. Then k can be factor as $k = g'k'$ where k' is a kernel of f'.*

Proof. First, we show that k can be factor as $k = g'k'$: Since $\langle f', g'\rangle = \ker\langle f, -g\rangle$ and

$$\langle f, -g\rangle i_1 k = fk = 0$$

there exist a unique morphism $k'\colon K \longrightarrow E$ such that

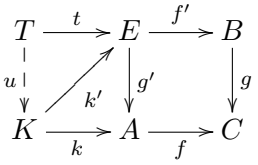
$$\langle f', g'\rangle k' = i_1 k$$



Hence

$$g'k' = p_1\langle f', g'\rangle k' = p_1 i_1 k = k$$

We now prove that k' is a kernel of f': Let $t\colon T \longrightarrow E$ be an arbitrary morphism such that $f't = 0$. Then $fg't = gf't = 0$, hence there exists a unique morphism u such that $ku = g't$.



Notice that

$$f'k'u = p_2\langle f', g'\rangle k'u = p_2 i_1 ku = 0 = f't$$

and $g'k'u = ku = g't$. Hence $k'u = t$. Which proved k' is a kernel of f'. □

A.7.3 Snake Lemma

When we drawing diagrams contain many kernels and cokernels, to simplify the notation, we denoted the domain of the kernel of f by $\ker f$ *while the codomain of the cokernel by* $\operatorname{coker} f$*.* $\operatorname{im} f$ *and* $\operatorname{coim} f$ *are similar. This will not make ambiguity since they are just be used as notations of objects in this situation.*

Theorem A.7.10 (Weak Snake Lemma). *The short exact sequences of morphisms α, β, γ, which means a commutative diagram like below*

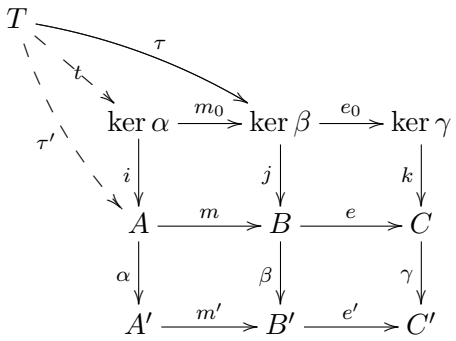
$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C'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

induces an exact sequence relating kernels and cokernels

$$0 \longrightarrow \ker\alpha \longrightarrow \ker\beta \longrightarrow \ker\gamma \xrightarrow{\delta} \operatorname{coker}\alpha \longrightarrow \operatorname{coker}\beta \longrightarrow \operatorname{coker}\gamma \longrightarrow 0$$

Proof. We proceed in steps:

1. The morphisms between kers are clearly given by the efinition and the commutative of diagram. By chasing the diagram and use the definition, one can verify that the sequence of kers is exact. For the cokers, the argument is similar. Let's proof that $m_0\colon \ker\alpha \longrightarrow \ker\beta$ is the kernel of $e_0\colon \ker\beta \longrightarrow \ker\gamma$ as an example:



   By choosing any object T with morphism τ such that $e_0\tau = 0$, we have $ke_0\tau = 0$, hence $ej\tau = 0$. Since m is the kernel of e, there exist a unique $\tau'\colon T \longrightarrow A$ such that $j\tau = m\tau'$.

   We have

$$m'\alpha\tau' = \beta m\tau' = \beta j\tau = 0$$

   Which implies $\alpha\tau' = 0$ since m' is monoic. Hence there exist a unique $t\colon T \longrightarrow \ker\alpha$ such that $it = \tau'$, hence

$$jm_0t = mit = m\tau' = j\tau$$

Which implies $m_0 t = \tau$ since j is monoic. Which shows that m_0 is a kernel of e_0 and the sequence is exact by lemma 1.5.10.

2. The morphism δ can be obtained by this way:

   Consider the following diagram

$$\begin{array}{ccccc}
A & \overset{s}{\twoheadrightarrow} & D & \xrightarrow{u} & \ker\gamma \\
\| & & \downarrow{\scriptstyle k'} & & \downarrow{\scriptstyle k} \\
A & \xrightarrow{m} & B & \xrightarrow{e} & C \\
\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\
A' & \xrightarrow{m'} & B' & \xrightarrow{e'} & C' \\
\downarrow{\scriptstyle c} & & \downarrow{\scriptstyle c'} & & \| \\
\operatorname{coker}\alpha & \xrightarrow[v]{} & D' & \overset{t}{\twoheadrightarrow} & C'
\end{array}$$

   where the upper-right square is cartesian and the lower-left square is cocartesian. Since e is epi, then u is epi and $u = \operatorname{coker} s$. Similarly, v is a monoic and $v = \ker t$.

   By the commutativity, $tc'\beta k' = \gamma k u = 0$, hence there exists a unique morphism $d\colon D \longrightarrow \operatorname{coker}\alpha$ such that

$$vd = c'\beta k'$$

   Similarly, $vds = c'\beta k's = vc\alpha = 0$. Then $ds = 0$ because v is monoic. Hence there exists a unique morphism

$$\delta\colon \ker\gamma \longrightarrow \operatorname{coker}\alpha$$

   such that $\delta u = d$. Moreover,

$$v\delta u = c'\beta k'$$

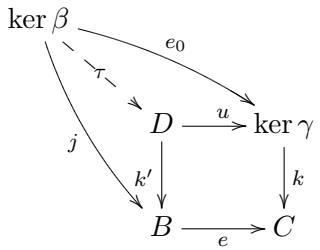
3. We now prove that the sequence

$$\ker\beta \xrightarrow{e_0} \ker\gamma \xrightarrow{\delta} \operatorname{coker}\alpha \xrightarrow{m_1} \operatorname{coker}\beta$$

   is exact, we prove the exactness at $\ker\gamma$ only, the case at $\operatorname{coker}\alpha$ is dual to this.

   Let $x\colon \ker\delta \longrightarrow \ker\gamma$ be the kernel of δ, and $t\colon \operatorname{im} e_0 \longrightarrow \ker\gamma$ be the image of e_0. We need to show the are equivalent. Since both x and t are monoic, it suffices to show that they can factor through each other.

(*1*) First, we prove that $e_0\delta = 0$.

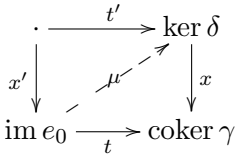


Since $ej = ke_0$ there exist a unique $\tau\colon \ker\beta \longrightarrow D$ such that $u\tau = e_0$ and $k'\tau = j$. Therefore

$$v\delta e_0 = v\delta u\tau = c'\beta k'\tau = c'\beta j = 0$$

Which implies $\delta e_0 = 0$ since v is monoic.

(*2*) Therefore t can factor through x by a unique morphism μ. To get a factorization of x through t, we pullback t through x and obtain a monomorphism t':



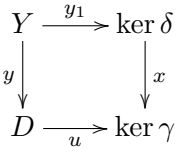
If t' is an isomorphism, then it is clearly that $x = tx't'^{-1}$. To prove this, it suffices to show t' is epi.

(*3*) Consider the diagram in 2. Since $e/\beta k' = \gamma ku = 0$, there exist a unique $f\colon D \longrightarrow A'$ such that $m'f = \beta k'$. We have

$$vcf = c'm'f = c'\beta k' = v\delta u$$

which implies $cf = \delta u$ because v is monoic.

Pullback x through u:



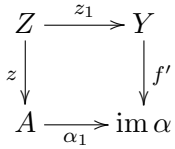
We have

$$cfy = \delta uy = \delta xy_1 = 0$$

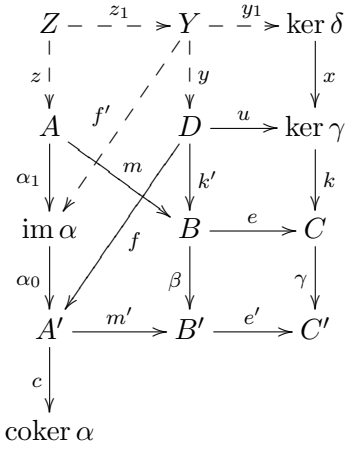
Hence there exist a unique $f'\colon Y \longrightarrow \operatorname{im}\alpha = \ker c$ such that

$$\alpha_0 f' = fy$$

We pullback through the f' the epimorphism α_1:



In order to see more clearly, we put these morphisms in the following diagram which may not commutative at the upper-left square:



(*4*) To measure the non-commutativity, define

$$\Delta = k'yz_1 - mz$$

Since

$$\beta k'yz_1 = m'fyz_1 = m'\alpha_0 f'z_1 = m'\alpha_0\alpha_1 z = \beta mz$$

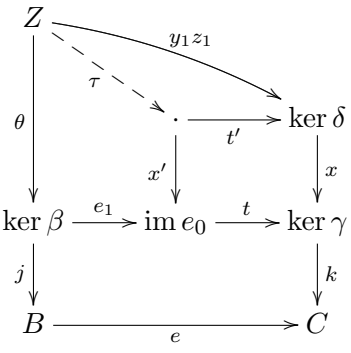
We have $\beta\Delta = 0$ and hence there exist a unique $\theta\colon Z \longrightarrow \ker\beta$ such that $j\theta = \Delta$.

On the other hand,

$$e\Delta = ek'yz_1 - emz = ek'yz_1 - 0 = kxy_1z_1$$

Hence $ej\theta = kxy_1z_1$.

Consider the diagram below:



We have

$$kte_1\theta = ke_0\theta = ej\theta = kxy_1z_1$$

which implies $te_1\theta = xy_1z_1$ because k is monoic.

By the universality of pullback, there exist a unique morphism τ, such that $t'\tau = y_1z_1$ which is an epimorphism, hence so is t'. □

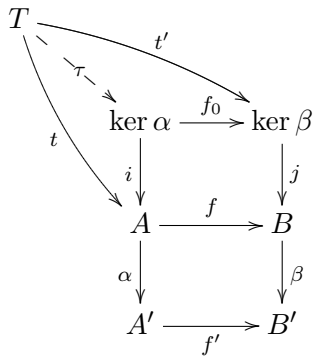
Theorem A.7.11 (Snake Lemma). *The following commutative diagram of exact sequences*

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

induces an exact sequence relating kernels and cokernels

$$\ker\alpha \longrightarrow \ker\beta \longrightarrow \ker\gamma \xrightarrow{\delta} \operatorname{coker}\alpha \longrightarrow \operatorname{coker}\beta \longrightarrow \operatorname{coker}\gamma$$

Proof. First, we prove that the kernel of α is a pullback of the kernel of β through f:



Let T be an arbitrary object with morphisms t, t' such that $ft = jt'$. Then

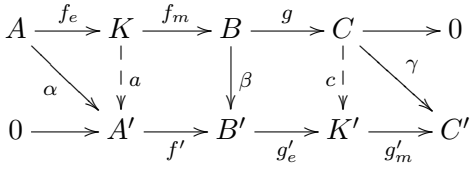
$$f'\alpha t = \beta f t = \beta j t' = 0$$

which implies $\alpha t = 0$ because f' is monoic. Hence there exist a unique $\tau\colon T \longrightarrow \ker\alpha$ such that $i\tau = t$. Then

$$jf_0\tau = fi\tau = ft = jt'$$

which implies $f_0\tau = t'$ because j is monoic. Hence i is the pullback of j through f.

Let $f_m\colon K \longrightarrow B$ be the kernel of g and $g'_e\colon B' \longrightarrow K'$ cokernel of f'. Then we get a commutative diagram



where $(f_e, f_m), (g'_e, g'_m)$ are the *epi-mono factorizations*[2] of f and g respectively, and a, c determined uniquely by the fact that $A' = \ker g'$ and $C = \operatorname{coker} f$.

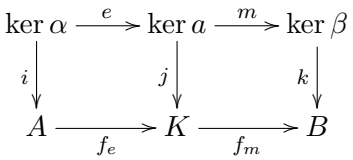
Then By the Weak Snake Lemma (A.7.10), the diagram induces an exact sequence:

$$0 \longrightarrow \ker a \longrightarrow \ker \beta \longrightarrow \ker c \xrightarrow{\delta} \operatorname{coker} a \longrightarrow \operatorname{coker} \beta \longrightarrow \operatorname{coker} c \longrightarrow 0$$

Since f_e is epi, by Lemma A.7.4, the cokernel of a and α coincide. Dually, the kernel of c and γ coincide.

Hence it suffices to show that $\ker a \longrightarrow \ker \beta$ is the image of $\ker \alpha \longrightarrow \ker \beta$, and the cokernel case is dual to this.

Consider the following diagram, where e exists and make the diagram commutative since $af_ei = fi = 0$.



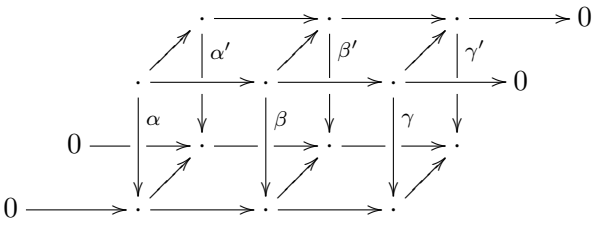
By the universal property of kernel, me is the morphism $\ker \alpha \longrightarrow \ker \beta$ we discussed above.

By the statements we proved at first, the right square and the outer rectangle are pullbacks, so is the left square by Proposition A.5.38. Therefore e is a pullback of f_e and hence epi. By the uniqueness of epi-mono factorization (A.7.3), m is the image of $\ker \alpha \longrightarrow \ker \beta$. □

Remark. The morphism δ is called *connection morphism*, while the long exact sequence is called *snake sequence*.

[2]Notice that the sequence is exact in B means that $\operatorname{im} f = \ker g$ and, dually, $\operatorname{coker} f = \operatorname{coim} g$. Hence we get the epi-mono factorization.

Proposition A.7.12. *The the snake sequence is* natural *in the sense that if*



is a commutative diagram with exact rows, then the snake lemma can be applied twice, to the "front" and to the "back", yielding two snake sequences; these are related by a commutative diagram of the form:

$$\begin{array}{ccccccccccc} & & \ker\alpha' & \longrightarrow & \ker\beta' & \longrightarrow & \ker\gamma' & \xrightarrow{\delta'} & \operatorname{coker}\alpha' & \twoheadrightarrow & \operatorname{coker}\beta' \twoheadrightarrow \operatorname{coker}\gamma' \\ & \nearrow & & \nearrow & & \nearrow & & \nearrow & & \nearrow & \nearrow \\ \ker\alpha & \longrightarrow & \ker\beta & \longrightarrow & \ker\gamma & \xrightarrow{\delta} & \operatorname{coker}\alpha & \twoheadrightarrow & \operatorname{coker}\beta & \twoheadrightarrow & \operatorname{coker}\gamma \end{array}$$

Proof. The commutativity of between kers (resp. cokers) are clear. It suffices to check commutativity at the connection morphisms.

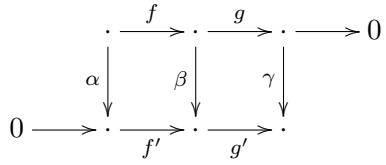
For α', β', γ', we have the same diagrams as α, β, γ in the construction of connection morphism. Without causing ambiguity, we can use the same labels and denote the morphisms from the "front" to the "back" by σ.

Since taking pullback and pushout are functors (A.5.42), we have

$$v\delta'\sigma u = v\delta' u\sigma = c'\beta' k'\sigma = \cdots = \sigma c'\beta k' = \sigma v\delta u = v\sigma\delta u$$

Hence $\delta'\sigma = \sigma\delta$. □

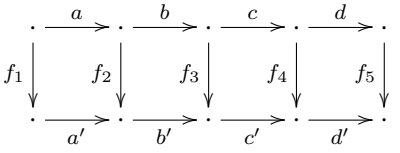
Theorem A.7.13 (Short Five Lemma). *Consider the following commutative diagram of exact sequences:*



Then, if α, γ are monoic (resp. epi), then so is β. Moreover, assume f is monoic and g' is epi, then any two of α, β, γ are isomorphisms implies so is the third.

Proof. Check the snake sequence, then the statements are obvious. □

Theorem A.7.14 (Five Lemma). *Consider the following exact sequences of five morphisms:*



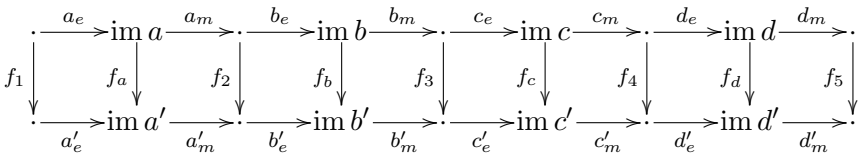
Then

a) If f_1 is epi and f_2, f_4 are monoic, then f_3 is monoic;

b) If f_5 is monoic and f_2, f_4 are epi, then f_3 is epi;

c) If f_1, f_2, f_4, f_5 are isomorphisms, then so is f_3.

Proof. First of all, notice that any exact sequence of morphisms can be factored into short exact sequences. For example, our exact sequence above can be factored as



We prove only *a)* as a example:

Since $a'_e f_1$ is epi, so is f_a. Consider the short exact sequence of f_a, f_2, f_b, by snake lemma, we have the snake sequence:

$$\ker f_a \longrightarrow \ker f_2 \longrightarrow \ker f_b \xrightarrow{\delta} \operatorname{coker} f_a \longrightarrow \operatorname{coker} f_2 \longrightarrow \operatorname{coker} f_b$$

Since f_2 is monoic and f_a is epi, the exact sequence at $\ker f_b$ become

$$0 \longrightarrow \ker f_b \xrightarrow{\delta} 0$$

Hence f_b is monoic.

Since $f_4 c_m$ is monoic, so is f_c. By the *short five lemma*, f_3 is monoic as desired. □

A.8 Appendix: Some Counterexamples

About Category Theory

In this chapter, I try to introduce some concepts in "category theory".

Nowadays, there are numerous books introducing category theory, like [Lawvere and Schanuel, 1997] and [Awodey, 2010] which are easily readable books. Of course, The standard textbook is [Lane, 1998]. Unless otherwise specified, most of the contents in this chapter comes from them. One can also find them in a modern homological algebra textbook.

Bibliography

[Atiyah, 1994] Atiyah, M. (1994). *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Westview Press.

[Awodey, 2010] Awodey, S. (2010). *Category Theory*. Oxford Logic Guides. OUP Oxford.

[Balmer and Schlichting, 2001] Balmer, P. and Schlichting, M. (2001). Idempotent completion of triangulated categories. *Journal of Algebra*, 236(2):819–834.

[Bourbaki, 1998a] Bourbaki, N. (1998a). *Algebra I: Chapters 1-3*. Springer.

[Bourbaki, 1998b] Bourbaki, N. (1998b). *General Topology: Chapters 1-4*. Elements of mathematics / Nicolas Bourbaki. Springer.

[Eisenbud, 1995] Eisenbud, D. (1995). *Commutative Algebra: With a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer.

[Freyd, 1970] Freyd, P. (1970). Homotopy is not concrete. In *Lecture Notes in Math. 168*, pages 25–34.

[Freyd and Kelly, 1972] Freyd, P. J. and Kelly, G. M. (1972). Categories of continuous functors, i. *Journal of pure and applied algebra*, 2(3):169–191.

[Hungerford, 1974] Hungerford, T. (1974). *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer.

[Jacobson, 1980] Jacobson, N. (1980). *Basic algebra*, volume 2. Freeman.

[Kaplansky, 1958] Kaplansky, I. (1958). Projective modules. *The Annals of Mathematics*, 68(2):372–377.

[Keller, 1990] Keller, B. (1990). Chain complexes and stable categories. *manuscripta mathematica*, 67(1):379–417.

[Lane, 1998] Lane, S. (1998). *Categories for the Working Mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer.

[Lang, 2002] Lang, S. (2002). *Algebra*, volume 211 of *Graduate Texts in Mathematic*. Springer.

[Lawvere and Schanuel, 1997] Lawvere, F. and Schanuel, S. (1997). *Conceptual Mathematics: A First Introduction to Categories*. Cambridge University Press.

[Morandi, 1996] Morandi, P. (1996). *Field and Galois Theory*, volume 167 of *Graduate Texts in Mathematics*. Springer.

[Rotman, 2002] Rotman, J. (2002). *Advanced Modern Algebra*. Prentice Hall.

[Serre and Greenberg, 1980] Serre, J. and Greenberg, M. (1980). *Local Fields*, volume 67 of *Graduate Texts in Mathematics*. Springer.

Index

Notations

$(\mathcal{C} \downarrow A)$	the slice category over A
$(A \downarrow \mathcal{C})$	the coslice category with respect to A
$(S \downarrow T)$	the comma category from S to T
$1_A, \mathrm{id}_A$	the identity over A
$[\mathcal{C}, \mathcal{D}], \mathcal{D}^{\mathcal{C}}$	the category of functors from $\mathcal{C}$ to $\mathcal{D}$
$\mathbf{Ab}$	the category of abelian groups
$\mathbf{Ab}_{\mathrm{tf}}$	the category of torsion-free abelian groups
$\mathbf{Cat}$	the category of all (small) categories
$\mathcal{C}^{\to}$	the arrow category of $\mathcal{C}$
$A^{\vee}$	the codual group of A
$E^{\vee}$	the dual module of E
$\coprod A_i$	the coproduct of $\{A_i\}_{i \in I}$
$A^{\wedge}$	the dual group of A
$E^{\wedge}$	the Pontrjagin dual of E
$\mathbf{Grp}$	the category of groups
$\mathrm{Hom}_{\mathcal{C}}(A, B)$	the set of morphisms from A to B in $\mathcal{C}$
$\mathbf{0}$	the zero object, zero morphism or empty category, which depends on context
$\mathbf{Ban}_1$	the category of Banach spaces and linear contractions
$\mathbf{Cocone}(D)$	the category of co-cones to D
$\mathbf{Cone}(D)$	the category of cones to D
$\mathbf{hTop}$	the category of topological spaces and homotopy classes
$\mathbf{Ring}$	the category of rings
$\mathcal{C} \simeq \mathcal{D}$	$\mathcal{C}$ and $\mathcal{D}$ are equivalent
$\mathcal{M}^*, \mathcal{M}_*$	the Yoneda embedding
$\varprojlim D_j$	the limit for D
$\varinjlim D_j$	the colimit for D
$\mathbf{Mod}_A$	the category of $A-$modules
$\mathbf{1}$	the category with one object $*$ and one morphism
$\prod A_i$	the product of $\{A_i\}_{i \in I}$
$\mathrm{Qout}_{\mathcal{C}}(B)$	the category of quotient objects of B in $\mathcal{C}$

Set	the category of sets
$\mathrm{Sub}_{\mathcal{C}}(B)$	the category of subobjects of B in $\mathcal{C}$
Top	the category of topological spaces
$A \amalg_C B$	the fibre coproduct of A and B over C
$A \oplus B$	the biproduct of A and B
$A \times_C B$	the fibre product of A and B over C
$d(f, g)$	the difference of f, g
f^*	the pullback functor induced by f
f_*	the pushout functor induced by f
G_s	the stabilizer of a point s in S
Gs	the orbit of a point s in S
$K(A), K_0(A)$	the Grothedieck group of A
M_{tor}	the set of torsion elements in M
$N \rtimes H$	the semidirect product of N and H
S/G	the orbit space of S under the action of G
S^1	the unit circle
S^G	the set of all $G-$invariant element
S^g	the set of fixed points of $g \in G$
S_G	the space of $G-$coinvariants
$Z(G)$	the center of G