ALGEBRAIC THEORY OF ABELIAN GROUPS

N. P. STRICKLAND

Contents

1. Introduction

This document aims to give a self-contained account of the parts of abelian group theory that are most relevant for algebraic topology. It is almost purely expository, although there are some slightly unusual features in the treatment of tensor products, torsion products and Ext groups. The book [1] is a good reference for Sections 11 and 12. Earlier sections are more standard and can be found in very many sources.

2. Exactness and splittings

Definition 2.1. Consider a sequence $A_0 \xrightarrow{f_0} A_1 \to \cdots \xrightarrow{f_{r-1}} A_r$ of abelian groups and homomorphisms. We say that the sequence is *exact* at A_i if $\text{image}(f_{i-1}) = \ker(f_i) \leq A_i$ (which implies that $f_i \circ f_{i-1} = 0$). We say that the whole sequence is exact if it is exact at A_i for $0 < i < r$.

Next, we say that a sequence $A \xrightarrow{f} B \xrightarrow{g} C$ is *short exact* if it is exact, and also f is injective and g is surjective.

Remark 2.2. One can easily check the following facts.

(a) A sequence $A \xrightarrow{f} B \xrightarrow{0} C$ is exact iff f is surjective. In particular, a sequence $A \xrightarrow{f} B \to 0$ is exact iff f is surjective.
(b) A sequence $A \xrightarrow{0} B \xrightarrow{g} C$ is exact iff g is injective. In particular, a sequence $0 \to B \xrightarrow{g} C$ is exact iff g is injective.
(c) A sequence $A \xrightarrow{0} B \xrightarrow{g} C \xrightarrow{0} D$ is exact iff g is an isomorphism.
(d) A sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact iff $A \xrightarrow{f} B \xrightarrow{g} C$ is short exact.
(e) Suppose we have an exact sequence

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{k} E.$$

Date: March 16, 2023.

Then g induces a map from $\mathrm{cok}(f) = B/f(A)$ to C, and h can be regarded as a map from C to $\ker(k)$, and the resulting sequence

$$\mathrm{cok}(f) \xrightarrow{g} C \xrightarrow{h} \ker(k)$$

is short exact.

(f) If $A \xrightarrow{f} B \xrightarrow{g} C$ is short exact, then f induces an isomorphism $A \to f(A)$ and g induces an isomorphism $B/f(A) \to C$. Thus, if A, B and C are finite we have $|B| = |f(A)|.|B/f(A)| = |A||C|$. Similarly, if A and C are free abelian groups of ranks n and m, then B is a free abelian group of rank $n+m$.

Proposition 2.3 (The five lemma)**.** *Suppose we have a commutative diagram as follows, in which the rows are exact, and p_0, p_1, p_3 and p_4 are isomorphisms:*

$$\begin{tikzcd}
A_0 \arrow[r, "f_0"] \arrow[d, "p_0"', "\simeq"] & A_1 \arrow[r, "f_1"] \arrow[d, "p_1"', "\simeq"] & A_2 \arrow[r, "f_2"] \arrow[d, "p_2"'] & A_3 \arrow[r, "f_3"] \arrow[d, "p_3"', "\simeq"] & A_4 \arrow[d, "p_4"', "\simeq"] \\
B_0 \arrow[r, "g_0"'] & B_1 \arrow[r, "g_1"'] & B_2 \arrow[r, "g_2"'] & B_3 \arrow[r, "g_3"'] & B_4.
\end{tikzcd}$$

Then p_2 is also an isomorphism.

Proof. First suppose that $a_2 \in A_2$ and $p_2(a_2) = 0$. It follows that $p_3f_2(a_2) = g_2p_2(a_2) = g_2(0) = 0$, but p_3 is an isomorphism, so $f_2(a_2) = 0$, so $a_2 \in \ker(f_2)$. The top row is exact, so $\ker(f_2) = \mathrm{image}(f_1)$, so we can choose $a_1 \in A_1$ with $f_1(a_1) = a_2$. Put $b_1 = p_1(a_1) \in B_1$. We then have $g_1(b_1) = g_1p_1(a_1) = p_2f_1(a_1) = p_2(a_2) = 0$, so $b_1 \in \ker(g_1)$. The bottom row is exact, so $\ker(g_1) = \mathrm{image}(g_0)$, so we can choose $b_0 \in B_0$ with $g_0(b_0) = b_1$. As p_0 is an isomorphism, we can now put $a_0 = p_0^{-1}(b_0) \in A_0$. We then have $p_1f_0(a_0) = g_0p_0(a_0) = g_0(b_0) = b_1 = p_1(a_1)$. Here p_1 is an isomorphism, so it follows that $f_0(a_0) = a_1$. We now have $a_2 = f_1(a_1) = f_1f_0(a_0)$. However, as the top row is exact we have $f_1f_0 = 0$, so $a_2 = 0$. We conclude that p_2 is injective.

Now suppose instead that we start with an element $b_2 \in B_2$. Put $b_3 = g_2(b_2) \in B_3$ and $a_3 = p_3^{-1}(b_3) \in A_3$. We then have $p_4f_3(a_3) = g_3p_3(a_3) = g_3(b_3) = g_3g_2(b_2) = 0$ (because $g_3g_2 = 0$). As p_4 is an isomorphism, this means that $f_3(a_3) = 0$, so $a_3 \in \ker(f_3)$. As the top row is exact we have $\ker(f_3) = \mathrm{image}(f_2)$, so we can choose $a_2 \in A_2$ with $f_3(a_2) = a_3$. Put $b_2' = b_2 - p_2(a_2) \in B_2$. We have $g_2(b_2') = g_2(b_2) - g_2p_2(a_2) = b_3 - p_3f_2(a_2) = b_3 - p_3(a_3) = 0$, so $b_2' \in \ker(g_2) = \mathrm{image}(g_1)$. We can thus choose $b_1' \in B_1$ with $g_1(b_1') = b_2'$. Now put $a_1' = p_1^{-1}(b_1') \in A_1$ and $a_2' = f_1(a_1') \in A_2$. We find that $p_2(a_2') = p_2f_1(a_1') = g_1p_1(a_1') = g_1(b_1') = b_2' = b_2 - p_2(a_2)$, so $p_2(a_2 + a_2') = b_2$. This shows that p_2 is also surjective, and so is an isomorphism as claimed. ◻

Proposition 2.4. *Suppose we have a commutative diagram as follows, in which the rows are short exact sequences:*

$$\begin{tikzcd}
A \arrow[r, tail, "j"] \arrow[d, "f"'] & B \arrow[r, two heads, "q"] \arrow[d, "g"'] & C \arrow[d, "h"'] \\
A' \arrow[r, tail, "j'"'] & B' \arrow[r, two heads, "q'"'] & C'
\end{tikzcd}$$

Then there is a unique homomorphism $\delta\colon \ker(h) \to \mathrm{cok}(f)$ such that $\delta(q(b)) = a' + f(A)$ whenever $g(b) = j'(a')$. Moreover, this fits into an exact sequence

$$0 \to \ker(f) \xrightarrow{j} \ker(g) \xrightarrow{q} \ker(h) \xrightarrow{\delta} \mathrm{cok}(f) \xrightarrow{j} \mathrm{cok}(g) \xrightarrow{q} \mathrm{cok}(h) \to 0.$$

Proof. A *snake* for the above diagram is a list $(c, b, a', \overline{a})$ such that

(1) $c \in \ker(h) \leq C$
(2) $b \in B$ with $qb = c$
(3) $a' \in A'$ with $j'a' = gb \in B'$
(4) $\overline{a}$ is the image of a' in $\mathrm{cok}(f)$.

It is easy to see that the snakes form a subgroup of $\ker(h) \times B \times A' \times \mathrm{cok}(f)$. We claim that for all $c \in \ker(h)$, there exists a snake starting with c. Indeed, as q is surjective, we can choose $b \in B$ satisfying (2). Then

$q'g(b) = hq(b) = h(c) = 0$, so $g(b) \in \ker(q') = \operatorname{img}(j')$, so we can choose $a' \in A'$ satisfying (3). Finally, we can define $\overline{a}$ to be the image of a' in $\operatorname{cok}(f)$, so that (4) is satisfied: this gives a snake as required. Next, we claim that any two snakes starting with c have the same endpoint. By subtraction we reduce to the following claim: if $(0, b, a', \overline{a})$ is a snake, then $\overline{a} = 0$, or equivalently $a' \in \operatorname{img}(f)$. Indeed, condition (2) says that $b \in \ker(q) = \operatorname{img}(j)$, so we can find $a \in A$ with $b = ja$. Now $j'(fa - a') = j'fa - gb = gja - gb = gb - gb = 0$, and j' is injective, so $fa = a'$ as required. This allows us to construct a map $\delta\colon \ker(h) \to \operatorname{cok}(f)$ as follows: we define $\delta(c)$ to be the endpoint of any snake starting with c.

We now need to check exactness of the resulting sequence.

(1) As $j\colon A \to B$ is injective, it is clear that the restricted map $j\colon \ker(f) \to \ker(g)$ is also injective.
(2) As the composite $A \xrightarrow{j} B \xrightarrow{q} C$ is zero, the same is true of the restricted composite $\ker(f) \xrightarrow{j} \ker(g) \xrightarrow{q} \ker(h)$. Moreover, suppose we have $b \in \ker(g)$ with $qb = 0$. By the original exactness assumption we can find $a \in A$ with $ja = b$. Now $j'fa = gja = gb = 0$ but j' is injective so $fa = 0$ so $a \in \ker(f)$. Thus, b is in the image of the map $j\colon \ker(f) \to \ker(g)$.
(3) Suppose we have $b \in \ker(g)$. Then $(qb, b, 0, 0)$ is a snake starting with qb, showing that $\delta qb = 0$. Conversely, suppose that $c \in \ker(h)$ with $\delta c = 0$, so there exists a snake $(c, b, a', 0)$. By the last snake condition, we must have $a' \in \operatorname{img}(f)$, say $a' = fa$ for some $a \in A$. Put $b' = b - ja \in B$. Snake condition (2) gives $qb = c$ but also $qj = 0$ so $qb' = c$. On the other hand, snake condition (3) gives $gb = j'a' = j'fa = gja$ so $gb' = 0$. This means that c is in the image of the map $q\colon \ker(g) \to \ker(h)$.
(4) Suppose we have $c \in \ker(h)$ with $\delta(c) = \overline{a}$. This means that there is a snake $(c, b, a', \overline{a})$. We claim that the induced map $j'\colon \operatorname{cok}(f) \to \operatorname{cok}(g)$ sends $\overline{a}$ to 0, or equivalently that $j'a' \in \operatorname{img}(g)$. This is clear because $j'a' = gb$ by the snake axioms. Conversely, suppose that $\overline{a} \in \operatorname{cok}(f)$ and that $\overline{a}$ maps to 0 in $\operatorname{cok}(g)$. This means that we can find $a' \in A$ representing $\overline{a}$ and that ja' lies in the image of g, say $ja' = gb$ for some $b \in B$. If we put $c = qb \in C$ we find that $hc = hqb = q'gb = q'j'a' = 0$, so $c \in \ker(h)$. By construction we see that $(c, b, a', \overline{a})$ is a snake so $\overline{a} \in \operatorname{img}(\delta)$.
(5) As the composite $A' \xrightarrow{j'} B' \xrightarrow{q'} C'$ is zero, the same is clearly true for the induced maps $\operatorname{cok}(f) \to \operatorname{cok}(g) \to \operatorname{cok}(h)$. Conversely, suppose we have an element $\overline{b} \in \operatorname{cok}(g)$ that maps to zero in $\operatorname{cok}(h)$. We can choose $b' \in B'$ representing $\overline{b}$, and then $q'b'$ must lie in $\operatorname{img}(h)$, say $q'b' = hc$. As q is surjective we can choose $b \in B$ with $qb = c$. This gives $q'b' = hqb = q'gb$, so the element $b' - gb$ lies in $\ker(q')$, which is the same as $\operatorname{img}(j')$. We can therefore choose $a' \in A'$ with $b' = gb + j'a'$. If we let $\overline{a}$ denote the image of a' in $\operatorname{cok}(f)$, we find that $\overline{b} = j'\overline{a}$ in $\operatorname{cok}(g)$.
(6) Finally, suppose we have $\overline{c} \in \operatorname{cok}(h)$. We can then choose a representing element $c' \in C'$. As q' is surjective we can choose $b' \in B'$ with $q'b' = b$, then we can put $\overline{b} = [b'] \in \operatorname{cok}(g)$. We find that $q'\overline{b} = \overline{c}$. This shows that $q'\colon \operatorname{cok}(g) \to \operatorname{cok}(h)$ is surjective.

□

Definition 2.5. A *split short exact sequence* is a diagram

$$\begin{tikzcd} A \arrow[r, bend left, "i"] & B \arrow[l, bend left, "r"] \arrow[r, bend left, "p"] & C \arrow[l, bend left, "s"] \end{tikzcd}$$

where

$$pi = 0 \qquad rs = 0 \qquad ri = 1_A \qquad ps = 1_C \qquad ir + sp = 1_B.$$

This can also be displayed as

$$\begin{tikzcd} A \arrow[rr, "0"] \arrow[dr, "i"] \arrow[dd, "1"'] & & C \\ & B \arrow[ur, "p"] \arrow[dl, "r"] & \\ A & & C \arrow[ll, "0"] \arrow[ul, "s"'] \arrow[uu, "1"'] \end{tikzcd}$$

Example 2.6. Given abelian groups A and C, there is a split short exact sequence

$$\begin{tikzcd} A \arrow[r, bend left, "i'"] & A \oplus C \arrow[l, bend left, "r'"] \arrow[r, bend left, "p'"] & C \arrow[l, bend left, "s'"] \end{tikzcd}$$

given by

$$\begin{aligned} i'(a) &= (a,0) & p'(a,c) &= c \\ s'(c) &= (0,c) & r'(a,c) &= a. \end{aligned}$$

The above example is essentially the only example, as we see from the following result:

Proposition 2.7. *Suppose we have a split short exact sequence*

$$\begin{tikzcd} A \arrow[r, bend left, "i"] & B \arrow[l, bend left, "r"] \arrow[r, bend left, "p"] & C \arrow[l, bend left, "s"] \end{tikzcd}$$

Then there is an isomorphism $f\colon B \to A\oplus C$ given by $f(b) = (r(b), p(b))$ with inverse $f^{-1}(a,c) = i(a)+s(c)$. Moreover, the diagram

$$\begin{tikzcd} A \arrow[r, bend left, "i"] \arrow[d, equal] & B \arrow[l, bend left, "r"] \arrow[r, bend left, "p"] \arrow[d, "f", "\simeq"'] & C \arrow[l, bend left, "s"] \arrow[d, equal] \\ A \arrow[r, bend left, "i'"] & A \oplus C \arrow[l, bend left, "r'"] \arrow[r, bend left, "p'"] & C \arrow[l, bend left, "s'"] \end{tikzcd}$$

commutes in the sense that

$$fi = i' \qquad fs = s' \qquad pf = p' \qquad rf = f'.$$

Proof. We can certainly define homomorphisms $B \xrightarrow{f} A \oplus C \xrightarrow{g} B$ by $f(b) = (r(b), p(b))$ and $g(a,c) = i(a) + s(c)$. We then have $gf(b) = (ir + sp)(b) = b$ and $fg(a,c) = (ri(a) + rs(c), pi(a) + ps(c)) = (a,c)$ so f and g are mutually inverse isomorphisms. We also have $fi(a) = (ri(a), pi(a)) = (a,0) = i'(a)$, and the equations $fs = s'$, $pf = p'$ and $rf = f'$ can be verified equally easily. $\square$

Our terminology is justified by the following observation:

Lemma 2.8. *If*

$$\begin{tikzcd} A \arrow[r, bend left, "i"] & B \arrow[l, bend left, "r"] \arrow[r, bend left, "p"] & C \arrow[l, bend left, "s"] \end{tikzcd}$$

is a split short exact sequence, then

$$A \xrightarrow{i} B \xrightarrow{p} C$$

is a short exact sequence.

Proof. Suppose that $i(a) = 0$. As $ri = 1_A$ we have $a = r(i(a)) = r(0) = 0$. This shows that $\ker(i) = 0$, so i is injective. Next, we have $ps = 1_C$, so for all $c \in C$ we have $c = p(s(c)) \in \mathrm{image}(p)$; so p is surjective. We also have $pi = 0$, so $\mathrm{image}(i) \leq \ker(p)$. Finally, we have $ir + sp = 1_B$, so for $b \in B$ we have $b = i(r(b)) + s(p(b))$. If $b \in \ker(p)$ this reduces to $b = i(r(b)) \in \mathrm{image}(i)$, so $\ker(p) \leq \mathrm{image}(i)$ as required. $\square$

Proposition 2.9. *Let $A \xrightarrow{i} B \xrightarrow{p} C$ be a short exact sequence.*

(a) *For any map $r\colon B \to A$ with $ri = 1_A$, there is a unique map $s\colon C \to B$ such that (i,p,r,s) gives a split short exact sequence.*
(b) *For any map $s\colon C \to B$ with $ps = 1_C$, there is a unique map $r\colon B \to A$ such that (i,p,r,s) gives a split short exact sequence.*

Proof. We will prove (a) and leave the similar proof of (b) to the reader. Define $f = 1 - ir\colon B \to B$. As $ri = 1$ we have $fi = i - i(ri) = 0$, so f vanishes on $\mathrm{image}(i)$, which is the same as $\ker(p)$. We therefore have a well-defined map $s\colon C \to B$ given by $s(c) = f(b)$ for any b with $p(b) = c$. This means that $sp = f = 1 - ir$, or in other words $1_B = ir + sp$. We also have $pi = 0$ so $psp = p(1 - ir) = p$, so $(ps - 1)p = 0$. As p is surjective this implies that $ps - 1 = 0$ or $ps = 1_C$. Finally, we have $ri = 1$ so $rsp = r(1 - ir) = r - (ri)r = 0$ but p is surjective so $rs = 0$. Thus, all the conditions for a split short exact sequence are verified. If $s' : C \to B$ is another map giving a split short exact sequence then we can subtract the equations $ir + sp = 1$ and $ir + s'p = 1$ to get $(s - s')p = 0$ but p is surjective so $s = s'$; this shows that s is unique. □

Proposition 2.10. *Let B be an abelian group, and let A and C be subgroups such that $B = A + C$ and $A \cap C = 0$. Let $i : A \to B$ and $s : C \to B$ be the inclusion maps. The there is a unique pair of homomorphisms $A \xleftarrow{r} B \xrightarrow{p} C$ giving a split short exact sequence.*

Proof. Consider an element $b \in B$. As $B = A + C$ we can find $(a, c) \in A \oplus C$ such that $b = a + c$. Suppose we have another pair $(a', c') \in A \oplus C$ with $b = a' + c'$. We put $x = a - a'$, and by rearranging the equation $a + c = a' + c'$ we see that $x = c' - c$. The first of these expressions shows that $x \in A$, and the second that $x \in C$. As $A \cap C = 0$ this means that $x = 0$, so $a = a'$ and $c = c'$. Thus, the pair (a, c) is unique, so we can define maps $A \xleftarrow{r} B \xrightarrow{p} C$ by $r(b) = a$ and $p(b) = c$. It is straightforward to check that these give a split short exact sequence. □

Proposition 2.11. *Let B be an abelian group, and let $e : B \to B$ be a homomorphism with $e^2 = e$. Then $\text{image}(e) = \ker(1 - e)$ and $\ker(e) = \text{image}(1 - e)$ and $B = \text{image}(e) \oplus \text{image}(1 - e)$.*

Proof. First, if $b \in \text{image}(e)$ then $b = e(a)$ for some a, so $(1 - e)(b) = e(a) - e^2(a) = 0$, so $b \in \ker(1 - e)$. Conversely, if $b \in \ker(1 - e)$ then $b - e(b) = 0$ so $b = e(b) \in \text{image}(e)$. This shows that $\text{image}(e) = \ker(1 - e)$ as claimed. Now put $f = 1 - e$. We then have $f^2 = 1 - 2e + e^2 = 1 - 2e + e = f$, so f is another idempotent endomorphism of B. We can thus apply the same logic to see that $\text{image}(f) = \ker(1 - f)$, or in other words $\text{image}(1 - e) = \ker(e)$.

Now consider an arbitary element $b \in B$. We can write b as $e(b) + (1 - e)(b)$, so $b \in \text{image}(e) + \text{image}(1 - e)$; this shows that $B = \text{image}(e) + \text{image}(1 - e)$. Now suppose that $b \in \text{image}(e) \cap \text{image}(1 - e) = \ker(1 - e) \cap \ker(e)$. This means that $(1 - e)(b) = e(b) = 0$, so $b = e(b) = 0$. This means that $\text{image}(e) \cap \text{image}(1 - e) = 0$, so the sum is direct. □

We now give a useful application of Proposition 2.7 to the theory of additive functors. We recall the definition:

Definition 2.12. A *covariant functor* from abelian groups to abelian groups is a construction that gives an abelian group $F(A)$ for each abelian group A, and a homomorphism $f_* : F(A) \to F(B)$ for each homomorphism $f : A \to B$, in such a way that:

(a) For identity maps we have $(1_A)_* = 1_{F(A)}$ for all A.
(b) For homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$ we have $(gf)_* = g_* f_* : F(A) \to F(C)$.

We say that F is a *additive* if $(f_0 + f_1)_* = (f_0)_* + (f_1)_*$ for all $f_0, f_1 : A \to B$.

Example 2.13. Fix an integer $n > 0$. We can then define an additive functor F by $F(A) = A[n] = \{a \in A \mid na = 0\}$, and another additive functor G by $G(A) = A/nA$. In both cases the homomorphisms f_* are just the obvious ones induced by f.

Proposition 2.14. *Let F be an additive covariant functor as above. Then for any abelian groups A and C we have an natural isomorphism $f : F(A \oplus C) \to F(A) \oplus F(C)$ given by $f(b) = (r'_*(b), p'_*(b))$ with inverse $f^{-1}(a, c) = i'_*(a) + s'_*(c)$.*

Proof. Put $B = A \oplus C$, and recall that $1_B = i'r' + s'p'$. As F is an additive functor we have

$$1_{F(B)} = (1_B)_* = (i'r')_* + (s'p')_* = i'_* r'_* + s'_* p'_*.$$

In the same way the equations $r'i' = 1$, $p's' = 1$, $p'i' = 0$ and $r's' = 0$ give $r'_* i'_* = 1$, $p'_* s'_* = 1$, $p'_* i'_* = 0$ and $r'_* s'_* = 0$, so we have a split short exact sequence

$$\begin{tikzcd} F(A) \arrow[r, bend left, "i'_*"] & F(B) \arrow[l, bend left, "r'_*"] \arrow[r, bend left, "p'_*"] & F(C) \arrow[l, bend left, "s'_*"] \end{tikzcd}$$

Thus, Proposition 2.7 gives us an isomorphism $F(A \oplus C) = F(B) \to F(A) \oplus F(C)$, and by unwinding the definitions we see that this is given by the stated formulae. $\square$

There is a similar statement for contravariant functors as follows.

Definition 2.15. A *contravariant functor* from abelian groups to abelian groups is a construction that gives an abelian group $F(A)$ for each abelian group A, and a homomorphism $f^*\colon F(B) \to F(A)$ for each homomorphism $f\colon A \to B$, in such a way that:

(a) For identity maps we have $(1_A)_* = 1_{F(A)}$ for all A.

(b) For homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$ we have $(gf)^* = f^*g^*\colon F(C) \to F(A)$.

We say that F is *additive* if $(f_0 + f_1)^* = f_0^* + f_1^*$ for all $f_0, f_1\colon A \to B$.

Proposition 2.16. *Let F be an additive contravariant functor as above. Then for any abelian groups A and C we have an natural isomorphism $f\colon F(A \oplus C) \to F(A) \oplus F(C)$ given by $f(b) = ((i')^*(b), (s')^*(b))$ with inverse $f^{-1}(a, c) = (r')^*(a) + (p')^*(c)$.*

Proof. Essentially the same as Proposition 2.14. $\square$

3. Products and coproducts

If we have a finite list of abelian groups $A_1, \dots, A_n$, we can form the product group $\prod_{i=1}^n A_i = A_1 \times \cdots \times A_n$, which is also denoted by $\bigoplus_{i=1}^n A_i = A_1 \oplus \cdots \oplus A_n$. This should be familiar. These constructions can be generalised to cover families of abelian groups A_i indexed by a set I that may be infinite, and need not be ordered in any natural way. This is a little more subtle, and in particular $\bigoplus_i A_i$ is not the same as $\prod_i A_i$ in this context. In this section we will briefly outline the relevant definitions and properties.

Definition 3.1. Let I be a set, and let $(A_i)_{i \in I}$ be a family of abelian groups indexed by I. The *product group* $\prod_{i \in I} A_i$ is the set of all systems $a = (a_i)_{i \in I}$ consisting of an element $a_i \in A_i$ for each $i \in I$. We make this into an abelian group by the obvious rule

$$(a_i)_{i \in I} \pm (b_i)_{i \in I} = (a_i \pm b_i)_{i \in I}.$$

For each $k \in I$ we define $\pi_k\colon \prod_{i \in I} A_i \to A_k$ by $\pi_k((a_i)_{i \in I}) = a_k$. This is clearly a homomorphism. We also define $\iota_k\colon A_k \to \prod_{i \in I} A_i$ by

$$\iota_k(a)_i = \begin{cases} a \in A_k & \text{if } i = k \\ 0 \in A_i & \text{if } i \neq k. \end{cases}$$

Example 3.2. If $I = \{1, 2, \dots, n\}$, then $\prod_{i \in I} A_i$ is just the set of n-tuples $(a_1, \dots, a_n)$ with $a_i \in A_i$, as before.

Example 3.3. Suppose we have a fixed group U, and we take $A_i = U$ for all i. Then $\prod_{i \in I} A_i$ is just the set $\mathrm{Map}(I, U)$ of all functions from I to U, considered as a group under pointwise addition.

Remark 3.4. It is easy to see that a homomorphism $f\colon U \to \prod_{i \in I} A_i$ is essentially the same thing as a family of homomorphisms $f_i\colon U \to A_i$, one for each $i \in I$. Indeed, given such a family we define $f\colon U \to \prod_{i \in I} A_i$ by $f(u) = (f_i(u))_{i \in I}$, and we can then recover the original homomorphisms f_i as the composites $\pi_i \circ f$. This means that $\prod_{i \in I} A_i$ is a product for the groups A_i in the general sense considered in category theory.

Definition 3.5. Given an element $a = (a_i)_{i \in I} \in \prod_{i \in I} A_i$, the *support* of a is the set

$$\mathrm{supp}(a) = \{i \in I \mid a_i \neq 0\} \subseteq I.$$

We put

$$\bigoplus_{i \in I} A_i = \{a \in \prod_{i \in I} A_i \mid \mathrm{supp}(a) \text{ is a finite set } \}.$$

It is easy to see that $\mathrm{supp}(a \pm b) \subseteq \mathrm{supp}(a) \cup \mathrm{supp}(b)$, and thus that $\bigoplus_{i \in I} A_i$ is a subgroup of $\prod_{i \in I} A_i$. We call it the *coproduct* of the family $(A_i)_{i \in I}$. We also note that $\mathrm{supp}(\iota_k(a)) \subseteq \{k\}$, so ι_k can be regarded as a homomorphism $A_k \to \bigoplus_{i \in I} A_i$.

Remark 3.6. If the index set I is finite then all supports are automatically finite and so the coproduct is the same as the product. In fact, we only need the set $I' = \{i \mid A_i \neq 0\}$ to be finite for this to hold.

Definition 3.5 is again compatible with the more general definition coming from category theory, as we see from the following result:

Proposition 3.7. *Suppose we have an abelian group V, and a system of homomorphisms $g_i \colon A_i \to V$ for all $i \in I$. Then there is a unique homomorphism $g \colon \bigoplus_{i \in I} A_i \to V$ such that $g \circ \iota_k = g_k$ for all $k \in I$.*

Proof. Given a point $a = (a_i)_{i \in I} \in \bigoplus_{i \in I} A_i$, we define

$$g(a) = \sum_{i \in \mathrm{supp}(a)} g_i(a_i) \in V.$$

The terms in the sum are meaningful because $a_i \in A_i$ and $g_i \colon A_i \to V$, and $\mathrm{supp}(a)$ is finite so there only finitely many terms so it is not a problem to add them up. If we replace $\mathrm{supp}(a)$ by some larger finite set $J \subseteq I$ then this gives us some extra terms but they are all zero so the sum is unchanged. After taking $J = \mathrm{supp}(a) \cup \mathrm{supp}(b)$ it becomes easy to see that $g(a + b) = g(a) + g(b)$, so g is a homomorphism. Using $\mathrm{supp}(\iota_k(a)) \subseteq \{k\}$ we see that $g \circ \iota_k = g_k$, as required. Let $g' \colon \bigoplus_{i \in I} A_i \to V$ be another homomorphism with $g' \circ \iota_k = g_k$ for all k. If we have an element a as before, we observe that $a = \sum_{i \in \mathrm{supp}(a)} \iota_i(a_i)$, and by applying g' to this we get

$$g'(a) = \sum_{i \in \mathrm{supp}(a)} g'(\iota_i(a_i)) = \sum_{i \in \mathrm{supp}(a)} g_i(a_i) = g(a),$$

so g is unique as claimed. $\square$

Remark 3.8. It would at worst be a tiny abuse of notation to say that $g(a) = \sum_{i \in I} g_i(a_i)$. This is a sum with infinitely many terms, which would not normally be meaningful, but only finitely many of the terms are nonzero, so the rest can be ignored.

Remark 3.9. Suppose we have an abelian group A, and a family of subgroups $(A_i)_{i \in I}$. There is then a unique homomorphism $\sigma \colon \bigoplus_{i \in I} A_i \to A$ such that $\sigma \circ \iota_k \colon A_k \to A$ is just the inclusion for all k. More explicitly, we just have $\sigma(a) = \sum_{i \in \mathrm{supp}(a)} a_i$. If this map σ is an isomorphism, we will say (with another slight abuse of notation) that $A = \bigoplus_{i \in I} A_i$.

4. Torsion groups

Definition 4.1. Let A be an abelian group.

(a) We say that an element $a \in A$ is a *torsion element* if $na = 0$ for some integer $n > 0$.
(b) We write $\mathrm{tors}(A)$ for the set of torsion elements of A. This is easily seen to be a subgroup, because if $na = 0$ and $mb = 0$ then $nm(a \pm b) = 0$.
(c) We say that A is a *torsion group* if every element is torsion, or equivalently $\mathrm{tors}(A) = A$. At the other extreme, we say that A is *torsion-free* if $\mathrm{tors}(A) = 0$.
(d) Now fix a prime p. We say that a is a *p-torsion element* if $p^k a = 0$ for some $k \geq 0$. We write $\mathrm{tors}_p(A)$ for the set of p-torsion elements, which is again a subgroup.
(e) We say that A is a *p-torsion group* if every element is p-torsion, or equivalently $\mathrm{tors}_p(A) = A$. At the other extreme, we say that A is *p-torsion free* if $\mathrm{tors}_p(A) = 0$.

Remark 4.2. We write $n.1_A$ for the endomorphism of A given by $a \mapsto na$. Then $\mathrm{tors}(A) = \bigcup_{n>0} \ker(n.1_A)$, and A is torsion-free if and only if the maps $n.1_A$ (for $n > 0$) are all injective.

Example 4.3. If A is a finite abelian group with $|A| = n$ then Lagrange's Theorem tells us that $na = 0$ for all $a \in A$, so A is a torsion group. For another instructive proof of the same fact, consider the element $z = \sum_{x \in A} x$. As x runs over A, the elements $a + x$ also run over A, so $z = \sum_{x \in A}(a + x) = na + z$, so $na = 0$. It is a curious fact, which we leave to the reader, that z itself is actually zero in all cases except when $|A| = 2$.

Example 4.4. It is clear that any free abelian group is torsion-free. The groups $\mathbb{Q}$ and $\mathbb{R}$ are torsion-free but not free.

Example 4.5. Consider the quotient group $A = \mathbb{Q}/\mathbb{Z}$. The subset

$$A_n = \{\mathbb{Z} = \tfrac{0}{n} + \mathbb{Z}, \tfrac{1}{n} + \mathbb{Z}, \dots, \tfrac{n-1}{n} + \mathbb{Z}\}$$

is a cyclic subgroup of order n. Any element $a \in \mathbb{Q}/\mathbb{Z}$ can be written as $a = m/n + \mathbb{Z}$ for some $m, n \in \mathbb{Z}$ with $n > 0$. We can also write m as $qn + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$ and observe that $a = m/n + \mathbb{Z} = r/n + q + \mathbb{Z} = r/n + \mathbb{Z} \in A_n$. This proves that A is the union of the subgroups A_n. As $na = 0$ for all $a \in A_n$, we see that A is a torsion group. One can also check that $A_n \leq A_m$ if and only if n divides m. In particular, for each prime p we have a chain of subgroups

$$A_p \leq A_{p^2} \leq A_{p^3} \leq \cdots \leq \bigcup_k A_{p^k} = \mathrm{tors}_p(A).$$

Example 4.6. Now consider instead the group $\mathbb{R}/\mathbb{Z}$. Suppose we have a torsion element $a = t + \mathbb{Z}$. This means that for some integer $n > 0$ we have $nt \in \mathbb{Z}$, which implies that t is rational. It follows that $\mathrm{tors}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$. A similar argument shows that $\mathbb{R}/\mathbb{Q}$ is torsion-free.

The following result is known as the Chinese Remainder Theorem.

Proposition 4.7. *Suppose we have positive integers $n_1, \dots, n_r$ any two of which are coprime, and we put $n = \prod_i n_i$. Define*

$$\phi\colon \mathbb{Z}/n \to (\mathbb{Z}/n_1) \times \cdots \times (\mathbb{Z}/n_r)$$

by

$$\phi(k + n\mathbb{Z}) = (k + n_1\mathbb{Z}, \dots, k + n_r\mathbb{Z}).$$

Then

(a) *There exist integers $e_1, \dots, e_r$ such that $\sum_i e_i = 1$ and $e_i = 1 \pmod{n_i}$ and $e_i = 0 \pmod{n/n_i}$.*
(b) *The map ϕ is an isomorphism.*

Proof. For $i \neq j$ we know that n_i and n_j are coprime, so we can choose integers a_{ij} and b_{ij} with $a_{ij}n_i + b_{ij}n_j = 1$. We then put $f_{ij} = b_{ij}n_j = 1 - a_{ij}n_i$, so $f_{ij} = 1 \pmod{n_i}$ and $f_{ij} = 0 \pmod{n_j}$. Now fix i, and let g_i be the product of the numbers f_{ij} as j runs over the remaining indices. We find that $g_i = 1 \pmod{n_i}$, but g_i is divisible by the product of all the n_j, or equivalently by n/n_i. Thus, the numbers g_i almost have property (a), but we will need a slight adjustment to make the sum equal to one. However, we are now ready to prove (b). Given any integers $m_1, \dots, m_r$, we have

$$\phi(\sum_i m_i g_i + n\mathbb{Z}) = (m_1 + n_1\mathbb{Z}, \dots, m_r + n_r\mathbb{Z}).$$

This proves that ϕ is surjective, and the domain and codomain of ϕ both have order n, so ϕ must actually be an isomorphism. By construction we have $\phi(\sum_i g_i + n\mathbb{Z}) = \phi(1 + n\mathbb{Z})$, and ϕ is injective, so $\sum_i g_i = 1 + nk$ for some k. We define $e_i = g_i$ for $i < r$, and $e_r = 1 - \sum_{i<r} g_i = g_r - nk$; these clearly satisfy (a). □

The following special case is often useful:

Corollary 4.8. *Suppose that the prime factorisation of n is $n = p_1^{v_1} \cdots p_r^{v_r}$, where the primes p_i are all distinct. Then there are integers $e_1, \dots, e_r$ such that $\sum_i e_i = 1$ and $e_i = 1 \pmod{p_i^{v_i}}$ and $e_i = 0 \pmod{n/p_i^{v_i}}$. Moreover, the natural map*

$$\mathbb{Z}/n \to (\mathbb{Z}/p_1^{v_1}) \times \cdots \times (\mathbb{Z}/p_r^{v_r})$$

is an isomorphism. □

Proposition 4.9. *For any abelian group A we have* $\mathrm{tors}(A) = \bigoplus_p \mathrm{tors}_p(A)$.

Proof. Suppose we have a torsion element $a \in A$, so $na = 0$ for some $n > 0$. We can factor this as $\prod_{i=1}^r p_i^{v_i}$ and then choose integers e_i as in Corollary 4.8. Now $e_i = 0 \pmod{n/p_i^{v_i}}$ so $p_i^{v_i} e_i$ is divisible by n, so $p_i^{v_i} e_i a = 0$, so $e_i a \in \mathrm{tors}_{p_i}(A)$. We also have $\sum_i e_i = 1$, so $a = \sum_i e_i a \in \sum_i \mathrm{tors}_{p_i}(A)$. This shows that $\mathrm{tors}(A) = \sum_p \mathrm{tors}_p(A)$.

To show that the sum is direct, suppose we have a finite list of distinct primes $p_1, \dots, p_r$, and elements $a_i \in \mathrm{tors}_{p_i}(A)$ with $\sum_i a_i = 0$; we must show that $a_i = 0$ for all i. As $a_i \in \mathrm{tors}_{p_i}(A)$ we have $p_i^{v_i} a_i = 0$ for some $v_i \geq 0$. We again choose numbers e_i as in Corollary 4.8. As $p_i^{v_i} a_i = 0$ and $e_i = 1 \pmod{p_i^{v_i}}$ we have

$e_i a_i = a_i$. On the other hand, for $j \neq i$ we have $e_i = 0 \pmod{p_j^{v_j}}$ and so $e_i a_j = 0$. We can thus multiply the relation $\sum_j a_j = 0$ by e_i to get $a_i = 0$ as required. □

Lemma 4.10. *The quotient group $A/\operatorname{tors}(A)$ is always torsion-free.*

Proof. Suppose we have a torsion element $a = x + \operatorname{tors}(A)$ in $A/\operatorname{tors}(A)$. This means that for some $n > 0$ we have $na = 0$ or equivalentlt $nx \in \operatorname{tors}(A)$. This in turn means that for some $m > 0$ we have $mnx = 0$, which shows that x itself is a torsion element in A. This means that the coset $a = x + \operatorname{tors}(A)$ is zero, as required. □

5. Finitely generated abelian groups

Let A be an abelian group, and let $a_1, \dots, a_r$ be elements of A. We then have a homomorphism $f\colon \mathbb{Z}^r \to A$ given by

$$f(n_1, \dots, n_r) = n_1 a_1 + \cdots + n_r a_r.$$

In particular, if e_i is the i'th standard basis vector in $\mathbb{Z}^r$ then $f(e_i) = a_i$. Conversely, if we start with a homomorphism $f\colon \mathbb{Z}^r \to A$ we can put $a_i = f(e_i) \in A$ and we find that

$$f(n_1, \dots, n_r) = f(\sum_i n_i e_i) = \sum_i n_i a_i,$$

so everything fits together as before. The image of f is the smallest subgroup of A containing all the elements a_i, or in other words the subgroup generated by $\{a_1, \dots, a_r\}$. This justifies the following definition:

Definition 5.1. We say that an abelian group A is *finitely generated* if there exists a surjective homomorphism $f\colon \mathbb{Z}^r \to A$ for some r.

Example 5.2. Suppose that A is actually finite, so we can choose a list $a_1, \dots, a_r$ that contains all the elements of A. The corresponding map $\mathbb{Z}^r \to A$ is certainly surjective, so A is finitely generated.

Our main aim in this section is to prove the following classification theorem:

Theorem 5.3. *Let A be a finitely generated abelian group. Then A can be decomposed the direct sum of a finite list of subgroups, each of which is isomorphic either to $\mathbb{Z}$, or to $\mathbb{Z}/p^v$ for some prime p and some $v > 0$. The number of subgroups of each type in the decomposition is uniquely determined, although the precise list of subgroups is not.*

Remark 5.4. Note that Proposition 4.7 gives a decomposition of the stated type for the cyclic group $\mathbb{Z}/n$.

The groups $\mathbb{Z}^r$ themselves are of course finitely generated. It is convenient to observe that no two of them are isomorphic:

Lemma 5.5. *If $\mathbb{Z}^r$ is isomorphic to $\mathbb{Z}^s$, then $r = s$.*

Proof. Any isomorphism $f\colon A \to B$ induces an isomorphism $A/2A \to B/2B$, so in particular $|A/2A| = |B/2B|$. We have $\mathbb{Z}^r/2\mathbb{Z}^r = (\mathbb{Z}/2)^r$, which has order 2^r, and the claim follows easily. □

This means that the term 'rank' in the following definition is well-defined:

Definition 5.6. We say that an abelian group A is *free of rank r* if it is isomorphic to $\mathbb{Z}^r$.

Lemma 5.7. *Let A be a subgroup of $\mathbb{Z}$. Then either $A = 0 \simeq \mathbb{Z}^0$ or $A = d\mathbb{Z} \simeq \mathbb{Z}$ for some (unique) $d > 0$.*

Proof. The case where $A = 0$ is trivial, so suppose that $A \neq 0$. As $A = -A$ we see that A must contain at least one strictly positive integer. Let d be the smallest strictly positive integer in A. It is than clear that $d\mathbb{Z} \subseteq A$. Conversely, suppose that $n \in A$. As $d > 0$ we see that n must lie between id and $(i+1)d$ for some $i \in \mathbb{Z}$, say $n = id + j$ with $0 \leq j < d$. Now $j = n - id \in A$ and $0 \leq j < d$, which contradicts the defining property of d unless $j = 0$. We thus have $n = di$, showing that $A = d\mathbb{Z}$ as claimed. □

Proposition 5.8. *Let A be a subgroup of $\mathbb{Z}^r$; then A is free of rank at most r.*

Proof. For $i \leq r$ we put

$$F_i = \{x \in \mathbb{Z}^r \mid x_{i+1} = \cdots = x_r = 0\} \simeq \mathbb{Z}^i.$$

We let $\pi_s \colon \mathbb{Z}^r \to \mathbb{Z}$ be the projection map $x \mapsto x_s$, and put

$$J = \{j \mid \pi_j(A \cap F_j) \neq 0\} = \{j \mid A \cap F_j > A \cap F_{j-1}\}.$$

We can list the elements of this set as $j_1 < \cdots < j_s$ for some $s \leq r$ (possibly $s = 0$). We see from Lemma 5.7 that $\pi_{j_p}(A \cap F_{j_p})$ must have the form $d_p\mathbb{Z}$ for some $d_p > 0$ say. We can thus choose $a_p \in A \cap F_{j_p}$ such that $\pi_{j_p}(a_p) = d_p$ for all p. We claim that the list $a_1, \ldots, a_s$ is a basis for A over $\mathbb{Z}$, so that A is a free abelian group as claimed. More precisely, we claim that $a_1, \ldots, a_p$ is always a basis for $A \cap F_{j_p}$. In the case $p = 0$ we have the empty list and the zero group so the claim is clear. When $p > 0$ we can inductively assume the statement for $p-1$. Consider an arbitrary element $u \in A \cap F_{j_p}$. By the definition of d_p, we have $\pi_{j_p}(u) = m_p d_p$ for some $m_p \in \mathbb{Z}$. The element $u' = u - m_p a_p$ then lies in $A \cap F_{j_p}$ and satisfies $\pi_{j_p}(u') = 0$ so in fact $u' \in A \cap F_{j_{p-1}}$. By the induction hypothesis there are unique integers $m_1, \ldots, m_{p-1}$ with $u' = m_1 a_1 + \cdots + m_{p-1} a_{p-1}$, and it follows that $u = u' + m_p a_p = m_1 a_1 + \cdots + m_p a_p$. This shows that u can be expressed as an integer combination of $a_1, \ldots, a_p$, and a similar argument shows that the expression is unique. This completes the induction step, and after s steps we see that A itself has a basis as claimed. $\square$

Remark 5.9. In the above proof, we can alter our choice of a_p by subtracting off suitable multiples of a_{p-1}, a_{p-2} and so on in turn to ensure that $0 \leq \pi_{j_q}(a_p) < d_q$ for $1 \leq q < p$. One can then check that the resulting basis satisfying this auxiliary condition is in fact unique.

Corollary 5.10. *If A is finitely generated and B is a subgroup of A then B and A/B are also finitely generated.*

Proof. Choose a surjective homomorphism $f \colon \mathbb{Z}^r \to A$. The composite $\mathbb{Z}^r \xrightarrow{f} A \xrightarrow{\pi} A/B$ is again surjective, so A/B is finitely generated. Now put $F = \{x \in \mathbb{Z}^r \mid f(x) \in B\}$, and let $g \colon F \to B$ be the restriction of f. For $b \in B \leq A$ we can choose $x \in \mathbb{Z}^r$ with $f(x) = b$ (because f is surjective). Then $x \in F$ be the definition of f, and $g(x) = f(x) = b$; this proves that g is surjective. Moreover, F is a subgroup of $\mathbb{Z}^r$, so it is isomorphic to $\mathbb{Z}^s$ for some $s \leq r$ by the proposition. It now follows that B is finitely generated. $\square$

Proposition 5.11. *Suppose that F is finitely generated and torsion free; then F is free.*

Proof. Choose a surjective homomorphism $f \colon \mathbb{Z}^r \to F$ with r as small as possible. Put $A = \ker(f)$; it will suffice to show that $A = 0$. If not, choose some nonzero element $a = (a_1, \ldots, a_r) \in \ker(f)$. Let d be the greatest common divisor of $a_1, \ldots, a_r$ (or equivalently, the number $d > 0$ such that $\sum_i a_i\mathbb{Z} = d\mathbb{Z}$, which exists by Lemma 5.7). We find that $a/d \in \mathbb{Z}^r$ and $d\,f(a/d) = f(a) = 0$ in F, so $f(a/d)$ is a torsion element, but F is assumed torsion free, so $f(a/d) = 0$. We may thus replace a by a/d and assume that $d = 1$, so $\sum_i a_i\mathbb{Z} = \mathbb{Z}$. We can thus choose integers $b_1, \ldots, b_r$ with $\sum_i a_i b_i = 1$. Now define $\beta \colon \mathbb{Z}^r \to \mathbb{Z}$ by $\beta(x) = \sum_i x_i b_i$ and put $U = \ker(\beta)$. As $\beta(a) = 1$ we find that $x - \beta(x)a \in U$ for all x, and it follows that $\mathbb{Z}^r = U \oplus \mathbb{Z}a$. Proposition 5.8 tells us that U is free, and using the splitting $\mathbb{Z}^r = U \oplus \mathbb{Z}a$ we see that U has rank $r - 1$. As $f(a) = 0$ we also see that $f(U) = f(U \oplus \mathbb{Z}a) = f(\mathbb{Z}^r) = F$, so f restricts to give a surjective homomorphism $U \to F$. This contradicts the assumed minimality of r, so we must have $A = 0$ after all, so $f \colon \mathbb{Z}^r \to F$ is an isomorphism. $\square$

Corollary 5.12. *Let A be a finitely generated abelian group. Then* $\operatorname{tors}(A)$ *is finite, and there exists a finitely generated free subgroup $F \leq A$ such that $A = \operatorname{tors}(A) \oplus F \simeq \operatorname{tors}(A) \oplus \mathbb{Z}^s$ for some s.*

Proof. Firstly, Corollary 5.10 tells us that $\operatorname{tors}(A)$ is finitely generated, so we can choose a finite list of generators, say $a_1, \ldots, a_r$. These must be torsion elements, so we can choose $n_i > 0$ with $n_i a_i = 0$. This means that the corresponding surjection $f \colon \mathbb{Z}^r \to \operatorname{tors}(A)$ factors through the finite quotient group $\prod_{i=1}^r (\mathbb{Z}/n_i)$, so $\operatorname{tors}(A)$ is finite as claimed. Next, the quotient group $A/\operatorname{tors}(A)$ is finitely generated (by Corollary 5.10) and torsion-free (by Lemma 4.10) so it is free of finite rank by Proposition 5.11. We can thus choose an isomorphism $\overline{g} \colon \mathbb{Z}^s \to A/\operatorname{tors}(A)$. Now choose an element $a_i \in A$ representing the coset $g(e_i)$ (for $i = 1, \ldots, s$) and define $g \colon \mathbb{Z}^s \to A$ by $g(x) = \sum_i x_i a_i$, and put $F = g(\mathbb{Z}^s)$. If we let q denote the quotient map $A \to A/\operatorname{tors}(A)$ we have $qg = \overline{g}$, which is an isomorphism. It follows that $g\colon \mathbb{Z}^s \to F$ is an isomorphism, so F is free as claimed. Next, let $h\colon A \to F$ be the composite

$$A \xrightarrow{q} A/\operatorname{tors}(A) \xrightarrow{\overline{g}^{-1}} \mathbb{Z}^s \xrightarrow{g} F.$$

We find that $qh = q$, so $q(a - h(a)) = 0$, so $a - h(a) \in \operatorname{tors}(A)$ for all a. This implies that $a = (a - h(a)) + h(a) \in \operatorname{tors}(A) + F$, so $A = \operatorname{tors}(A) + F$. Moreover, the intersection $\operatorname{tors}(A) \cap F$ is both torsion and torsion-free, so it must be zero, so the sum is direct. $\square$

This corollary allows us to focus on $\operatorname{tors}(A)$, which is a finite group, of order n say. Proposition 4.9 gives a splitting $\operatorname{tors}(A) = \bigoplus_p \operatorname{tors}_p(A)$, and it is clear that $\operatorname{tors}_p(A)$ can only be nonzero if p divides n. In that case, $\operatorname{tors}_p(A)$ will be a finite abelian group whose order is a power of p.

Lemma 5.13. *Let A be an abelian group of order p^v. Suppose we have an element c of order p^w, and that every other element has order dividing p^w, and that the subgroup $C = \mathbb{Z}c$ has nontrivial intersection with every nontrivial subgroup. Then $A = C$.*

Proof. Consider a nontrivial element $a \in A$. The order of $a + C$ in A/C will then be p^i for some $i \leq w$. We then have $p^i a = mc$ for some $m \in \mathbb{Z}$, and the assumption $(\mathbb{Z}a) \cap C \neq 0$ means that $mc \neq 0$. We can thus write $mc = up^j c$ for some $j < w$ and some u such that $u \neq 0 \pmod{p}$. It follows that the order of mc in A is p^{w-j}, and thus that the order of a in A is p^{w-j+i}. By assumption, this is at most p^w, so $i \leq j$. We can thus put $b = a - up^{j-i}c$, and observe that $p^i b = 0$. Now b is congruent to a mod C, so it again has order p^i in A/C, but $p^i b$ is already zero in A, so $(\mathbb{Z}b) \cap C = 0$. As C meets every nontrivial subgroup, we must have $\mathbb{Z}b = 0$, so $a = up^{j-i}c \in C$. This means that $A = C$ as claimed. $\square$

Corollary 5.14. *Let A be an abelian group of order p^v, and suppose that the largest order of any element of A is p^w. Then $A \simeq B \oplus (\mathbb{Z}/p^w)$ for some subgroup B of order p^{v-w}.*

Proof. Choose an element c of order p^w, and let C be the subgroup that it generates, so $C \simeq \mathbb{Z}/p^w$. Among the subgroups B with $B \cap C = 0$, choose one of maximal order. Then put $\overline{A} = A/B$, and let $\overline{C}$ be the image of C in $\overline{A}$, which is isomorphic to C because $B \cap C = 0$. It will suffice to prove that $A = B + C$, or equivalently that $\overline{A} = \overline{C}$. By the lemma, we need only check that $\overline{C}$ has nontrivial intersection with every nontrivial subgroup of $\overline{A}$. Consider a nonzero element $\overline{a} \in \overline{A}$, and choose a representing element $a \in A \setminus B$. Then $\mathbb{Z}a + B$ is strictly larger than B and must meet C nontrivially, so there exists $k \in \mathbb{Z}$ and $b \in B$ with $ka + b \in C \setminus \{0\}$. If $ka + b$ were in B it would give a nontrivial element of $B \cap C$, contrary to assumption. It follows that $k\overline{a}$ is nontrivial in $\overline{A}$ and lies in C, as required. $\square$

Corollary 5.15. *Let A be an abelian group of order p^v. Then A is isomorphic to $\bigoplus_{i=1}^r \mathbb{Z}/p^{w_i}$ for some list $w_1, \ldots, w_r$ of positive integers with $\sum_i w_i = v$.*

Proof. This follows by an evident induction from Corollary 5.14. $\square$

Definition 5.16. Let A be a finite abelian group. For any prime p and positive integer k, we put

$$F_p^k(A) = \{a \in p^{k-1}A \mid pa = 0\}.$$

This is a finite abelian group of exponent p, so it has order p^v for some v. We define $f_p^k(A)$ to be this v, and we also put $g_p^k(A) = f_p^k(A) - f_p^{k+1}(A)$.

Proposition 5.17. *Let A be a finite abelian group.*

(a) *If $A \simeq A'$, then $F_p^k(A) \simeq F_p^k(A')$ for all p and k, so $f_p^k(A) = f_p^k(A')$ and $g_p^k(A) = g_p^k(A')$.*
(b) *If $A = B \oplus C$ then $F_p^k(A) = F_p^k(B) \oplus F_p^k(C)$, so $f_p^k(A) = f_p^k(B) + f_p^k(C)$ and $g_p^k(A) = g_p^k(B) + g_p^k(C)$.*
(c) *If A has order not divisible by p, then $F_p^k(A) = 0$ and so $f_p^k(A) = g_p^k(A) = 0$.*
(d) *Suppose that A has a decomposition as a sum of subgroups $\mathbb{Z}/p_i^{v_i}$ (with $v_i > 0$). Then $g_p^k(A)$ is the number of times that $\mathbb{Z}/p^k$ occurs in the decomposition.*

Proof. Parts (a) to (c) are straightforward and are left to the reader. Given these, part (d) reduces to the claim that $g_p^k(\mathbb{Z}/p^j)$ is one when $j = k$, and zero otherwise. One can see from the definitions that $f_p^k(\mathbb{Z}/p^j)$ is one when $k \leq j$, and zero when $k > j$; the claim follows easily from this. $\square$

Proof of Theorem 5.3. Let A be a finitely generated abelian group. Corollary 5.12 and subsequent remarks show that $A \simeq \mathbb{Z}^s \oplus \bigoplus_{i=1}^m \operatorname{tors}_{p_i}(A)$ for some finite list of primes p_i. After applying Corollary 5.15 to each of the groups $\operatorname{tors}_{p_i}(A)$, we get the claimed splitting of A as a sum of copies of $\mathbb{Z}$ and $\mathbb{Z}/p_j^{w_j}$. The number s is the rank of the quotient group $A/\operatorname{tors}(A)$, which is well-defined by Lemma 5.5. We can also apply the last part of Proposition 5.17 to $\operatorname{tors}(A)$ to see that the number of summands of each type is independent of the choice of splitting. □

6. Free abelian groups and their subgroups

In various places we have already used the free abelian group $\mathbb{Z}[I]$ generated by a set I. We start with a more careful formulation of this construction. One approach is to define $\mathbb{Z}[I] = \bigoplus_{i \in I} \mathbb{Z}$ as in Definition 3.5. That is essentially what we will do, but we will spell out some details.

Definition 6.1. Let I be any set. We write $\operatorname{Map}(I, \mathbb{Z})$ for the set of all maps $u\colon I \to \mathbb{Z}$. These form an abelian group under pointwise addition. For any map $u\colon I \to \mathbb{Z}$, the *support* is the set

$$\operatorname{supp}(u) = \{i \in I \mid u(i) \neq 0\} \subseteq I.$$

We put

$$\operatorname{Map}_0(I, \mathbb{Z}) = \{u\colon I \to \mathbb{Z} \mid \operatorname{supp}(u) \text{ is finite }\}.$$

It is easy to see that $\operatorname{supp}(u \pm v) \subseteq \operatorname{supp}(u) \cup \operatorname{supp}(v)$, and thus that $\operatorname{Map}_0(I, \mathbb{Z})$ is a subgroup of $\operatorname{Map}(I, \mathbb{Z})$.

Next, for any $i \in I$ we define $\delta_i\colon I \to \mathbb{Z}$ by

$$\delta_i(j) = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{if } j \neq i. \end{cases}$$

Note that $\operatorname{supp}(\delta_i) = \{i\}$ so $\delta_i \in \operatorname{Map}_0(I, \mathbb{Z})$.

Remark 6.2. If I is a finite set with n elements then we see that $\operatorname{Map}_0(I, \mathbb{Z}) = \operatorname{Map}(I, \mathbb{Z}) \simeq \mathbb{Z}^n$. The situation is a little more subtle when I is infinite.

The following lemma shows that $\operatorname{Map}_0(I, \mathbb{Z})$ is generated freely, in a certain sense, by the elements δ_i.

Lemma 6.3. *Let A be an abelian group. Then for any function $f\colon I \to A$ there is a unique homomorphism $\overline{f}\colon \operatorname{Map}_0(I, \mathbb{Z}) \to A$ such that $\overline{f}(\delta_i) = f(i)$ for all $i \in I$.*

Proof. We put

$$\overline{f}(u) = \sum_{i \in \operatorname{supp}(u)} u(i)\, f(i).$$

The terms are meaningful, because each $u(i)$ is in $\mathbb{Z}$ and each $f(i)$ is in A so we can multiply to get an element of A. The sum is meaningful because $u \in \operatorname{Map}_0(I, \mathbb{Z})$, so $\operatorname{supp}(u)$ is finite, so there are only finitely many terms to add. More explicitly, if $\operatorname{supp}(u) = \{i_1, \dots, i_r\}$ and $u(i_t) = n_t \in \mathbb{Z}$ for all t then

$$\overline{f}(u) = n_1 f(i_1) + \cdots + n_r f(i_r) \in A.$$

Note that it would be harmless to replace $\operatorname{supp}(u)$ by any finite set J with $\operatorname{supp}(u) \subseteq J \subseteq I$; this would introduce some extra terms, but they would all be zero. After taking $J = \operatorname{supp}(u) \cup \operatorname{supp}(v)$ we can check that $\overline{f}(u + v) = \overline{f}(u) + \overline{f}(v)$, so $\overline{f}$ is a homomorphism. From the definitions it is clear that $\overline{f}(\delta_i) = f(i)$. Now let $\alpha\colon \operatorname{Map}_0(I, \mathbb{Z}) \to A$ be another homomorphism with $\alpha(\delta_i) = f(i)$. Put $\beta = \alpha - \overline{f}$, so $\beta(\delta_i) = 0$ for all i. It is not hard to see that a general element u as above can be expressed in the form

$$u = n_1 \delta_{i_1} + \cdots + n_r \delta_{i_r}.$$

It follows that

$$\beta(u) = n_1 \beta(\delta_{i_1}) + \cdots + n_r \beta(\delta_{i_r}) = n_1.0 + \cdots + n_r.0 = 0.$$

This shows that $\beta = 0$, so $\alpha = \overline{f}$ as required. □

The notation used so far is convenient for giving the definition, and the proof of the above freeness property, but not for the applications. We thus introduce the following alternative:

Definition 6.4. We write $\mathbb{Z}[I]$ for $\mathrm{Map}_0(I,\mathbb{Z})$, and $[i]$ for δ_i. We say that an abelian group A is *free* if it is isomorphic to $\mathbb{Z}[I]$ for some I.

The freeness property now takes the following form:

Lemma 6.5. *Let A be an abelian group. Then for any function $f\colon I \to A$ there is a unique homomorphism $\overline{f}\colon \mathbb{Z}[I] \to A$ such that $\overline{f}([i]) = f(i)$ for all $i \in I$.*

One key result is as follows:

Theorem 6.6. *If A is a free abelian group, then every subgroup of A is also free.*

This is a generalisation of Proposition 5.8, which covered the case where A is finitely generated. Below we will state and prove some more refined statements. To prove Theorem 6.6 itself, we can use Remark 6.14 and the case $k = \top$ of Lemma 6.16 (in the notation of Definition 6.13).

To extend the proof of Proposition 5.8 to cover infinitely generated groups, we need two ingredients. Firstly, we need to modify the inductive argument so that it works for a suitable class of infinite ordered sets. Next, we need to show that any set can be ordered in the required way. The precise structure that we need is as follows:

Definition 6.7. A *well-ordering* on a set I is a relation on I (denoted by $i \leq j$) such that

(a) For all $i \in I$ we have $i \leq i$.
(b) For all $i, j \in I$ we have either $i \leq j$ or $j \leq i$, and if both hold then $i = j$.
(c) For all $i, j, k \in I$, if $i \leq j$ and $j \leq k$ then $i \leq k$.
(d) For any nonempty subset $J \subseteq I$ there is an element $j_0 \in J$ such that $j_0 \leq j$ for all $j \in J$. (In other words, j_0 is smallest in J.)

Remark 6.8. We have stated the axioms in a form that is conceptually natural but inefficient. Axiom (a) follows from (d) by taking $J = \{i\}$, the first half of (b) follows from (d) by taking $J = \{i, j\}$, and with a little more argument one can deduce (c) by taking $J = \{i, j, k\}$ and appealing to the second half of (b). Thus, we really only need (d) together with the second half of (b).

Example 6.9. The obvious ordering of $\mathbb{N}$ is a well-ordering, as is the obvious ordering on $\mathbb{N} \cup \{\infty\}$. The obvious ordering on $\mathbb{Z}$ is not a well-ordering, because the whole set does not have a smallest element. We can choose a bijection $f\colon \mathbb{N} \to \mathbb{Z}$ (for example, by setting $f(2n) = n$ and $f(2n+1) = -n-1$) and use this to transfer the standard ordering of $\mathbb{N}$ to a nonstandard ordering of $\mathbb{Z}$ that is a well-ordering. Alternatively, we can specify a well-ordering on $\mathbb{Z}$ by the rules

$$0 < 1 < 2 < 3 < 4 < \cdots < -1 < -2 < -3 < \cdots .$$

By constructions such as these, one can give explicit well-orderings of most naturally occurring countable sets.

Remark 6.10. Let I be a well-ordered set. If I is nonempty then it must have a smallest element, which we denote by $\perp_I$ or just $\perp$. Now suppose that $i \in I$ and i is not maximal, so the set $I_{>i} = \{j \in I \mid j > i\}$ is nonempty. Then $I_{>i}$ must have a smallest element. We denote this by $s(i)$, and call it the *successor* of i. We say that an element $j \in I$ *is a successor* if $j = s(i)$ for some i. For example, in $\mathbb{N} \cup \{\infty\}$ the elements 0 and ∞ are not successors, but all other elements are successors.

Theorem 6.11. *Every set admits a well-ordering.*

The proof will be given after some preliminaries.

There is no known well-ordering of $\mathbb{R}$, and indeed it is probably not possible to specify a well-ordering concretely, although the author does not know of any precise theorems to that effect. Similarly, there is no known well-ordering of the set of subsets of $\mathbb{N}$, or of most other naturally occurring uncountable sets. The problem is that one needs to make an infinite number of arbitrary choices, which cannot be done explicitly. However, we shall assume the Axiom of Choice, a standard principle of Set Theory, which says that such choices are nonetheless possible. More precisely, we shall assume that every set has a choice function, in the following sense:

Definition 6.12. Let I be a set, and let $P'(I)$ denote the set of nonempty subsets of I. A *choice function* for I is a function $c\colon P'(I) \to I$ such that $c(J) \in J$ for all $J \in P'(I)$. (In other words, $c(J)$ is a "chosen" element of J.)

If I is well-ordered, we can define a choice function by taking $c(J)$ to be the smallest element of J. Conversely, if we are given a choice function then we can use it to construct a well-ordering, as we now explain. In the literature it is more common to do this by proving Zorn's Lemma as an intermediate step, but here we have chosen to bypass that.

Proof of Theorem 6.11. Let I be a set, and let c be a choice function for I. Let $P(I)$ be the set of all subsets of I, and put $P^*(I) = P(I) \setminus \{I\}$. Define $d\colon P^*(I) \to I$ by $d(J) = c(I \setminus J)$, and then define $e\colon P(I) \to P(I)$ by

$$e(J) = \begin{cases} J \cup \{d(J)\} & \text{if } J \neq I \\ I & \text{if } J = I. \end{cases}$$

We call this the *expander* function. Clearly we have $J \subseteq e(J)$ for all J, with equality iff $J = I$. Now say that a subset $\mathcal{A} \subseteq P(I)$ is *saturated* if

(a) Whenever $J \in \mathcal{A}$, we also have $e(J) \in \mathcal{A}$.
(b) For any family of sets in $\mathcal{A}$, the union of that family is also in $\mathcal{A}$.

We say that a set J is *compulsory* if it lies in every saturated family. For example, by applying (b) to the empty family we see that the set $J_0 = \emptyset$ is compulsory. It follows using (a) that the sets $J_n = e^n(\emptyset)$ are compulsory for all n. Axiom (b) then tells us that the set $J_\omega = \bigcup_{n=0}^\infty J_n$ is compulsory, as is the set $J_{\omega+1} = e(J_\omega)$. If we had developed the theory of infinite ordinals, we could use transfinite recursion to define compulsory sets J_α for all ordinals α. As we have not discussed that theory, we will instead use an approach that avoids it. We let $\mathcal{C}$ denote the family of all compulsory sets. This is clearly itself a saturated family. We say that a set $J \in \mathcal{C}$ is *comparable* if for all other $K \in \mathcal{C}$ we have either $J \subseteq K$ or $K \subseteq J$. Let $\mathcal{D} \subseteq \mathcal{C}$ be the set of all comparable sets; we will show that this is saturated, and thus equal to $\mathcal{C}$. Consider a family of comparable sets J_α, with union J say, and another set $K \in \mathcal{C}$. For each α we have $J_\alpha \subseteq K$ or $K \subseteq J_\alpha$, because J_α is comparable. If $J_\alpha \subseteq K$ for all K then clearly $J \subseteq K$. Otherwise we must have $K \subseteq J_\alpha$ for some α but $J_\alpha \subseteq J$ so $K \subseteq J$. This shows that J is comparable, so $\mathcal{D}$ is closed under unions. Now consider a comparable set J; we claim that $e(J)$ is also comparable. To see this, put

$$\mathcal{E}_J = \{K \mid e(J) \subseteq K \text{ or } K \subseteq J\}.$$

By a similar argument to the previous paragraph, this is closed under unions. Suppose that $K \in \mathcal{E}_J$.

(a) If $e(J) \subseteq K$ then clearly $e(J) \subset e(K)$, so $e(K) \in \mathcal{E}_J$.
(b) If $K = J$ then $e(J) = e(K)$, so $e(K) \in \mathcal{E}_J$.
(c) Suppose instead that $K \subset J$. As $K \in \mathcal{C}$ we also have $e(K) \in \mathcal{C}$, and J is comparable so either $e(K) \subseteq J$ or $J \subset e(K)$. In the latter case we have $K \subset J \subset e(K)$, so $|e(K) \setminus K| \geq 2$, but $|e(K) \setminus K| \leq 1$ by construction, so this is impossible. We therefore have $e(K) \subseteq J$, so again $e(K) \in \mathcal{J}$.

We now see that $\mathcal{E}_J$ is a saturated subset of $\mathcal{C}$, so it must be all of $\mathcal{C}$. It follows easily from this that $e(J)$ is comparable. This means that $\mathcal{D}$ is a saturated subset of $\mathcal{C}$, so it must be all of $\mathcal{C}$, so all compulsory sets are comparable, or in other words $\mathcal{C}$ is totally ordered by inclusion.

We now claim that $\mathcal{C}$ is in fact well-ordered by inclusion. To see this, consider a nonempty family of compulsory sets K_α. Let J be the union of all compulsory sets that are contained in $\bigcap_\alpha K_\alpha$. As $\mathcal{C}$ is closed under unions, we see that J is actually the largest compulsory set that is contained in $\bigcap_\alpha K_\alpha$. In particular, the larger set $e(J)$ cannot be contained in $\bigcap_\alpha J_\alpha$, so for some α we have $e(J) \not\subseteq K_\alpha$. Now $K_\alpha \in \mathcal{C}$ and we have seen that $\mathcal{C} = \mathcal{E}_J$ and using this we see that $K_\alpha \subseteq J$. From this it follows easily that K_α is the smallest set in the family, as required.

Next, put $\mathcal{C}^* = \mathcal{C} \setminus \{I\}$, which is again well-ordered by inclusion. For $i \in I$ we let $p(i)$ be the union of all compulsory sets that do not contain i. As $\mathcal{C}$ is closed under unions this defines a map $p\colon I \to \mathcal{C}^*$. We can also restrict d to get a map $d\colon \mathcal{C}^* \to I$ in the opposite direction. Note that $e(p(i)) = p(i) \cup \{d(p(i))\}$ is a compulsory set not contained in $p(i)$, so we must have $i \in e(p(i))$, but $i \notin p(i)$ by construction, so we must have $d(p(i)) = i$. In the opposite direction, suppose we start with a compulsory set $J \in \mathcal{C}^*$, and put $i = d(J)$, so $e(J) = J \amalg \{i\}$. Now $p(i) \in \mathcal{C}$ and we have seen that $\mathcal{C} = \mathcal{E}_J$ so either $e(J) \subseteq p(i)$ or $p(i) \subseteq J$. The first of these would imply that $i \in p(i)$, contradicting the definition of $p(i)$, so we must instead have $p(i) \subseteq J$. On the other hand, J is one of the sets in the union that defines $p(i)$, so $J \subseteq p(i)$, so $J = p(i) = p(d(J))$. This proves that the maps $I \xrightarrow{p} \mathcal{C}^* \xrightarrow{d} I$ are mutually inverse bijections. We can thus introduce a well-ordering of I by declaring that $i \leq j$ iff $p(i) \subseteq p(j)$. □

We can now start to prove as promised that subgroups of free abelian groups are free. It will be enough to prove that every subgroup of $\mathbb{Z}[I]$ is free, and by Theorem 6.11 we may assume that I is well-ordered. We will need some auxiliary definitions.

Definition 6.13. Let I be a well-ordered set, and let A be a subgroup of $\mathbb{Z}[I]$. We put $I_\top = I \amalg \{\top\}$, ordered so that $i \leq \top$ for all $i \in I$ (which is again a well-ordering). Put $I_{<j} = \{i \in I \mid i < j\}$ and $A_{<j} = A \cap \mathbb{Z}[I_{<j}]$, and similarly for $I_{\leq j}$ and $A_{\leq j}$. Let $\pi_j \colon \mathbb{Z}[I] \to \mathbb{Z}$ be the j'th projection, which is characterised by the fact that $\pi_j([j]) = 1$ and $\pi_j([i]) = 0$ for all $i \neq j$. Put

$$J = \{j \in I \mid \pi_j(A_{\leq j}) \neq 0\} = \{j \in I \mid A_{<j} < A_{\leq j}\},$$

and $J_{<k} = \{j \in J \mid j < k\}$, and similarly for $J_{\leq k}$. For $j \in J$, we let d_j be the positive integer such that $\pi_j(A_{\leq j}) = d_j\mathbb{Z}$. We put

$$B_j = \{x \in A_{\leq j} \mid x_j = d_j\} \subseteq A,$$

which is nonempty by the definition of d_j. For any $k \in I_\top$, we define an *adapted basis for* $A_{<k}$ to be a map $a \colon J_{<k} \to A$ such that for all $j \in J_{<k}$ we have $a(j) \in B_j$. We also put

$$T_k = \{u \in \mathbb{Z}[I_{<k}] \mid 0 \leq u_j < d_j \text{ for all } j \in J_{<k}\}.$$

Note that this contains zero but is not a subgroup (unless $d_j = 1$ for all $j \in J$).

Remark 6.14. As each $B(j)$ is nonempty, we see that there exist adapted bases. Implicitly we are using the Axiom of Choice here: there exists a choice function c for A, and then we can take $a(j) = c(B(j))$ for all j. However, we will prove as Proposition 6.20 that there is a *unique* adapted basis satisfying a certain normalisation condition, which enables us to avoid this use of choice.

Remark 6.15. Let a be an adapted basis for $A_{<k}$. We then have a unique homomorphism

$$f_k \colon \mathbb{Z}[J_{<k}] \to A_{<k}$$

such that $f_k([j]) = a(j)$ for all $j \in J_{<k}$. If $m < k$ then $a|_{J_{<m}}$ is easily seen to be an adapted basis for $A_{<m}$. It therefore gives rise to a homomorphism $f_m \colon \mathbb{Z}[J_{<m}] \to A_{<m}$, which is just the restriction of the map $f_k \colon \mathbb{Z}[J_{<k}] \to A_{<k}$.

We can also define functions $g_m \colon \mathbb{Z}[J_{<m}] \times T_m \to \mathbb{Z}[I_{<m}]$ by $g_m(x, y) = f_m(x) + y$.

The terminology is justified by the following result:

Lemma 6.16. *Let a be an adapted basis for $A_{<k}$. Then the corresponding map $f_k \colon \mathbb{Z}[J_{<k}] \to A_{<k}$ is an isomorphism, and the map $g_k \colon \mathbb{Z}[J_{<k}] \times T_k \to \mathbb{Z}[I_{<k}]$ is a bijection. In particular, the group $A_{<k}$ is free.*

We will deduce it from the following auxiliary result:

Lemma 6.17. *Let a be an adapted basis for $A_{<k}$, and suppose that for all $m < k$ the maps f_m and g_m are bijective. Then f_k and g_k are also bijective.*

Proof. There are three cases to consider:

(a) k is not a successor.
(b) $k = s(m)$ for some $m \notin J$.
(c) $k = s(m)$ for some $m \in J$.

Suppose that case (a) holds. Then for $m < k$ we have $s(m) < k$ and so $f_{s(m)} \colon \mathbb{Z}[J_{<s(m)}] \to A_{<s(m)}$ is an isomorphism. Now $J_{<k}$ is easily seen to be the union of these sets $J_{<s(m)}$, and $A_{<k}$ is the union of the groups $A_{<s(m)}$. It therefore follows that f_k is also an isomorphism $\mathbb{Z}[J_{<k}] \to A_{<k}$, as required. Essentially the same argument proves that g_k is a bijection.

Next, in case (b) we see from the definition of J that $A_{<k} = A_{\leq m} = A_{<m}$ and similarly $J_{<k} = J_{<m}$ so $f_k = f_m$ and this is an isomorphism as required. We also have $T_k = T_m \times \mathbb{Z}.[m]$ and $\mathbb{Z}[I_{<k}] = \mathbb{Z}[I_{<m}] \times \mathbb{Z}.[m]$ so the bijectivity of g_k follows from that of g_m.

Finally, in case (c), we know that f_m and g_m are bijective by assumption. Suppose that $u \in \mathbb{Z}[I_{<k}]$. We then have $u_m = r\,d_m + s$ for some s with $0 \leq s < d_m$. Put $u' = u - r\,a_m - s\,[m]$, so $u'_m = 0$, so $u' \in \mathbb{Z}[I_{<m}]$. As g_m is a bijection we see that there is a unique pair $(x', y') \in \mathbb{Z}[J_{<m}] \times T_m$ with $u' = f_m(x') + y'$. If we put $x = x' + r\,[m] \in \mathbb{Z}[J_{<k}]$ and $y = y' + s\,[m] \in T_k$ we find that (x, y) is the unique pair with $g_k(x, y) = u$. It follows that g_k is a bijection. In the case where $u \in A_{<k}$ we must have $u_m \in d_m\mathbb{Z}$ so $s = 0$ and $u' = u - r\,a_m \in A_{<m}$ so $y' = 0$; using this we see that f_k is also an isomorphism. □

Proof of Lemma 6.16. We actually claim that more generally, the restricted maps $f_n \colon \mathbb{Z}[J_{<n}] \to A_{<n}$ are isomorphisms for all $n \leq k$. If not, as $I_{\leq k}$ is well-ordered, there must be a smallest n for which f_n is not an isomorphism. This means that f_m is an isomorphism for $m < n$, so we can apply Lemma 6.17 to $a|_{J_{<n}}$ to see that f_n is an isomorphism, which is a contradiction. The claim follows. □

Remark 6.18. The method that we used to deduce Lemma 6.16 from 6.17 is called *transfinite induction*; it is evidently an extension of the usual kind of induction over the natural numbers. We will use transfinite induction again below without spelling it out so explicitly.

As we remarked previously, Theorem 6.6 follows from Theorem 6.11, Lemma 6.16 and Remark 6.14. Because we need Theorem 6.11, the proof is unavoidably nonconstructive. Nonetheless, we can remove one set of arbitrary choices by pinning down a specific adapted basis, as we now explain.

Definition 6.19. Let a be an adapted basis for $A_{<k}$. We say that a is *normalised* if for all $i, j \in J_{<k}$ with $i < j$ we have $0 \leq a(j)_i < d_i$.

Proposition 6.20. *There is a unique normalised adapted basis for A.*

This follows by transfinite induction from the following lemma:

Lemma 6.21. *Suppose that for all $m < \top$ there is a unique normalised basis for $A_{<m}$. Then there is a unique normalised basis for A.*

Proof. We must again separate three cases:

(a) $\top$ is not a successor.
(b) $\top = s(m)$ for some $m \notin J$.
(c) $\top = s(m)$ for some $m \in J$.

We first consider case (a). For each $m < \top$ we see that $s(m) < \top$, so by the inductive assumption we have a unique normalised adapted basis $a_m \colon J_{<s(m)} \to A_{<s(m)}$. Now for $n < m$ we see that $a_m|_{J_{<s(n)}}$ is an adapted basis for $A_{<s(n)}$ so it must be the same as a_n. It follows that there is a unique map $a \colon J = J_{<\top} \to A$ such that $a|_{J_{<s(m)}} = a_m$ for all m. (Explicitly, it is given by $a(m) = a_m(m)$ for all $m < \top$.) It is straightforward to check that this is a normalised adapted basis for A, and that it is the unique one.

Now consider instead case (b). Here we have $A_{<\top} = A_{<m}$ and $J_{<\top} = J_{<m}$ so everything is trivial.

Finally, consider case (c). Let $a \colon J_{<m} \to A_{<m}$ be the unique normalised adapted basis for $A_{<m}$. By the definition of d_m, we can choose $b \in A$ with $b_m = d_m$. Put $b' = b - d_m\,[m] \in \mathbb{Z}[I_{<m}]$. As $g_m \colon \mathbb{Z}[J_{<m}] \times T_m \to \mathbb{Z}[I_{<m}]$ is a bijection, there is a unique pair (x, y) with $f_k(x) + y = b'$. We put $a(m) = b - f_k(x) = y + d_m\,[m]$. The description $a(m) = b - f_k(x)$ shows that $a(m) \in A$, and the description $a(m) = y + d_m\,[m]$ shows that $a(m)$ satisfies the conditions for a normalised adapted basis. Now suppose we have another normalised adapted basis for A, say a'. Then $a|_{J_{<m}}$ and $a'|_{J_{<m}}$ are both normalised adapted bases for $A_{<m}$, so they are the same by the induction hypothesis, so $a(j) = a'(j)$ for all $j < m$. We also have $a(m)_m = d_m = a'(m)_m$, so the element $u = a'(m) - a(m)$ lies in $A_{<m}$, so $u = f_m(t)$ for some $t \in \mathbb{Z}[J_{<m}]$. If t is nonzero, then there are only finitely many indices j with $t_j \neq 0$, so we can let k be the largest one. We then find that $u_k = a'(m)_k - a(m)_k = t_k d_k$, so $a'(m)_k = a(m)_k \pmod{d_k}$. On the other hand, the normalisation condition means that $0 \leq a'(m)_k, a(m)_k < d_k$, and this can only be consistent if $a'(m)_k = a(m)_k$, so $t_k = 0$, contradicting the choice of k. Thus t must actually be zero, showing that $a = a'$ as required. □

7. Tensor and torsion products

Definition 7.1. Let A be an abelian group. We make the free abelian group $\mathbb{Z}[A]$ into a commutative ring by the rule

$$(\sum_i n_i[a_i]).(\sum_j m_j[b_j]) = \sum_{i,j} n_i m_j [a_i + b_j]$$

(so in particular $[a][b] = [a+b]$). We define a ring homomorphism $\epsilon\colon \mathbb{Z}[A] \to \mathbb{Z}$ by $\epsilon(\sum_i n_i[a_i]) = \sum_i n_i$, and we define I_A to be the kernel of ϵ. We write I_A^2 for the ideal generated by all products xy with $x, y \in I_A$. We also define a group homomorphism $q\colon \mathbb{Z}[A] \to A$ by $q(\sum_i n_i[a_i]) = \sum_i n_i a_i$.

Proposition 7.2. (a) *The abelian groups I_A and I_A^2 are both free.*

(b) *More specifically, the elements $\langle a\rangle = [a] - [0]$ for $a \in A \setminus 0$ form a basis for I_A.*

(c) *Put*

$$\langle a, b\rangle = \langle a\rangle\langle b\rangle = [a+b] - [a] - [b] + [0] = \langle a+b\rangle - \langle a\rangle - \langle b\rangle.$$

Then the set of all elements of this form generates I_A^2 as an abelian group.

(d) *There is a natural short exact sequence $I_A^2 \xrightarrow{j} I_A \xrightarrow{q} A$ (where j is just the inclusion).*

Proof. (a) Both I_A and I_A^2 are subgroups of $\mathbb{Z}[A]$, so they are free by Theorem 6.6.

(b) In the case of I_A it is easy to be more concrete. Suppose we have an element $x = \sum_i n_i[a_i] \in I_A$. Then $\sum_i n_i = 0$, so x can also be written as $\sum_i n_i([a_i] - [0])$, and it is clearly harmless to omit any terms where $a_i = 0$, so we see that x is in the subgroup generated by the elements $[a] - [0]$ with $a \neq 0$. It is easy to see that all such elements lie in I_A and that they are independent over $\mathbb{Z}$, so they form a basis for I_A as claimed.

(c) Let M be the subgroup of I_A generated by all elements of the form $\langle a, b\rangle$. As the elements $[a] - [0]$ generate I_A as an ideal, it is clear from the description $\langle a, b\rangle = \langle a\rangle\langle b\rangle$ that M generates I_A^2 as an ideal, so it will be enough to check that M itself is already an ideal. This follows easily from the identity $[x]\langle a, b\rangle = \langle a, b+x\rangle - \langle a, x\rangle$, which can be verified directly from the definitions.

(d) It is clear from the definitions that $q(\langle a, b\rangle) = a + b - a - b + 0 = 0$, so $qj = 0$ by part (c), so we have an induced map $\overline{q}\colon I_A/I_A^2 \to A$. In the opposite direction, we can define $s\colon A \to I_A/I_A^2$ by $s(a) = [a] - [0] + I_A^2$. We have

$$s(a+b) - s(a) - s(b) = [a+b] - [a] - [b] + [0] + I_A^2 = \langle a, b\rangle + I_A^2 = I_A^2,$$

which means that s is a homomorphism. It is visible that $\overline{q}s = 1_A$, so s is injective and $\overline{q}$ is surjective. It is also clear from (b) that $s(A)$ generates I_A/I_A^2 but s is a homomorphism so $s(A)$ is already a subgroup of I_A/I_A^2, so s is surjective. This means that s is an isomorphism, with inverse $\overline{q}$. As $\overline{q}$ is an isomorphism we see that $I_A^2 \xrightarrow{j} I_A \xrightarrow{q} A$ is exact.

∎

Definition 7.3. Let A and B be abelian groups. We regard A and B as subgroups of $A \times B$ in the obvious way. In $\mathbb{Z}[A \times B]$ we let J be the ideal generated by all elements $\langle a\rangle$ with $a \in A$, and we let K be the ideal generated by all elements $\langle b\rangle$ with $b \in B$. We then put $A \otimes B = JK/(J^2K + JK^2)$, and write $a \otimes b$ for the coset $\langle a, b\rangle + J^2K + JK^2 \in A \otimes B$. We also write $\mathrm{Tor}(A, B) = (J^2K \cap JK^2)/(J^2K^2)$.

Remark 7.4. Note that $A \otimes B$ is generated by elements of the form $a \otimes b$. Moreover, because

$$\langle a + a', b\rangle - \langle a, b\rangle - \langle a', b\rangle = \langle a\rangle\langle a'\rangle\langle b\rangle \in J^2K$$
$$\langle a, b + b'\rangle - \langle a, b\rangle - \langle a, b'\rangle = \langle a\rangle\langle b\rangle\langle b'\rangle \in JK^2$$

we see that these satisfy

$$a \otimes (b + b') = (a \otimes b) + (a \otimes b')$$
$$(a + a') \otimes b = (a \otimes b) + (a' \otimes b).$$

It follows easily that $a \otimes 0 = 0$ for all $a \in A$, and $0 \otimes b = 0$ for all $b \in B$, and $(na) \otimes (mb) = nm(a \otimes b)$ for all $n, m \in \mathbb{Z}$. In fact, $A \otimes B$ can be defined more loosely as the abelian group generated by symbols $a \otimes b$ subject only to the relations $a \otimes (b + b') = (a \otimes b) + (a \otimes b')$ and $(a + a') \otimes b = (a \otimes b) + (a' \otimes b)$.

Remark 7.5. Suppose we have homomorphisms $f\colon A \to A'$ and $g\colon B \to B'$. These give a homomorphism $f \times g\colon A \times B \to A' \times B'$, which induces a ring map $(f \times g)_\bullet\colon \mathbb{Z}[A \times B] \to \mathbb{Z}[A' \times B']$. This sends the ideals J and K to the coresponding ideals in $\mathbb{Z}[A' \times B']$ and so induces a homomorphism $A \otimes B \to A' \otimes B'$, which we denote by $f \otimes g$. By construction we have $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$. It is not hard to see that this construction is functorial, in the sense that $1_A \otimes 1_B = 1_{A\otimes B}$ and that $(f' \otimes g')(f \otimes g) = (f'f) \otimes (g'g)$ for all $f'\colon A' \to A''$ and $g'\colon B' \to B''$. It is also bilinear in the following sense: if $f_0, f_1\colon A \to A'$ and $g_0, g_1\colon B \to B'$ then

$$(f_0 + f_1) \otimes (g_0 + g_1) = (f_0 \otimes g_0) + (f_0 \otimes g_1) + (f_1 \otimes g_0) + (f_1 \otimes g_1)$$

as homomorphisms from $A \otimes B$ to $A' \otimes B'$.

Remark 7.6. As in Proposition 7.2, one can check that

(a) J is freely generated as an abelian group by the elements $\langle a\rangle[b] = [a + b] - [b]$ with $a \in A \setminus \{0\}$ and $b \in B$.
(b) K is freely generated as an abelian group by the elements $[a]\langle b\rangle = [a + b] - [a]$ with $a \in A$ and $b \in B \setminus 0$.
(c) JK is freely generated as an abelian group by the elements $\langle a, b\rangle$ with $a \in A \setminus 0$ and $b \in B \setminus 0$.
(d) J^2K is generated as an abelian group by the elements $\langle a\rangle\langle a'\rangle\langle b\rangle$ with $a, a' \in A$ and $b \in B$.
(e) JK^2 is generated as an abelian group by the elements $\langle a\rangle\langle b\rangle\langle b'\rangle$ with $a \in A$ and $b, b' \in B$.

We can generalise the identities in Remark 7.4 as follows:

Definition 7.7. Let A, B and V be abelian groups. We say that a function $f\colon A \times B \to V$ is *bilinear* if for all $a, a' \in A$ and all $b, b' \in B$ we have

$$f(a, b + b') = f(a, b) + f(a, b')$$
$$f(a + a', b) = f(a, b) + f(a', b).$$

More generally, we say that a map $g\colon A_1 \times \cdots \times A_n \to V$ is *multilinear* (or more specifically *n-linear*) if for each k and each $a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n$, the map

$$x \mapsto g(a_1, \ldots, a_{k-1}, x, a_{k+1}, \ldots, a_n)$$

is a homomorphism from A_k to V.

Example 7.8.

(a) Matrix multiplication defines a bilinear map $\mu\colon M_n(\mathbb{Z}) \times M_n(\mathbb{Z}) \to M_n(\mathbb{Z})$ by $\mu(M, N) = MN$.
(b) The dot product defines a bilinear map $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$, the cross product defines a bilinear map $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$, and the triple product $(u, v, w) \mapsto u.(v \times w)$ defines a trilinear map $\mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$.
(c) By construction, we have a bilinear map $\omega\colon A \times B \to A \otimes B$ defined by $\omega(a, b) = a \otimes b$.

Example (c) above is in a sense the universal example, as explained by the following result:

Proposition 7.9. *Let $f\colon A\times B \to V$ be a bilinear map. Then there is a unique homomorphism $\overline{f}\colon A\otimes B \to V$ such that $\overline{f}(a \otimes b) = f(a, b)$ for all $a \in A$ and $b \in B$ (or equivalently $\overline{f} \circ \omega = f$).*

Proof. As $A \otimes B$ is generated by the elements $a \otimes b$, it is clear that $\overline{f}$ will be unique if it exists.

By Lemma 6.5, there is a unique homomorphism $f_0\colon \mathbb{Z}[A \times B] \to V$ such that $f_0([a, b]) = f(a, b)$ for all a and b. Note that for $a \in A$ we have $f_0([a]) = f_0([a, 0]) = f(a, 0) = 0$, and similarly $f_0([b]) = 0$ for $b \in B$, so

$$f_0(\langle a, b\rangle) = f_0([a, b]) - f_0([a, 0]) - f_0([0, b]) + f_0([0, 0]) = f(a, b).$$

Note also that

$$f_0(\langle a\rangle\langle a'\rangle\langle b\rangle) = f_0(\langle a + a', b\rangle) - f_0(\langle a, b\rangle) - f_0(\langle a', b\rangle) = f(a + a', b) - f(a, b) - f(a', b) = 0,$$

so (using Remark 7.6(d)) we see that $f_0(J^2K) = 0$. Similarly, we have $f_0(JK^2) = 0$, so f_0 induces a homomorphism

$$\overline{f}\colon A \otimes B = \frac{JK}{J^2K + JK^2} \to V$$

with

$$\overline{f}(a \otimes b) = \overline{f}(\langle a, b\rangle + J^2K + JK^2) = f_0(\langle a, b\rangle) = f(a, b)$$

as required. □

Remark 7.10. For example, we have a bilinear map $\mu\colon M_n(\mathbb{Z})\times M_n(\mathbb{Z}) \to M_n(\mathbb{Z})$ given by $\mu(M,N) = MN$, so there is a unique homomorphism $\overline{\mu}\colon M_n(\mathbb{Z}) \otimes M_n(\mathbb{Z}) \to M_n(\mathbb{Z})$ such that $\overline{\mu}(M \otimes N) = MN$. Rather than spelling this out explicitly, we will usually just say that $\overline{\mu}\colon M_n(\mathbb{Z}) \otimes M_n(\mathbb{Z}) \to M_n(\mathbb{Z})$ is defined by $\overline{\mu}(M \otimes N) = MN$.

It will be convenient to reformulate Proposition 7.9 in a different way. We write $\mathrm{Hom}(A,B)$ for the set of homomorphisms from A to B, considered as a group under pointwise addition. Similarly, we write $\mathrm{Bilin}(A,B;V)$ for the group of bilinear maps from $A \times B$ to V.

Proposition 7.11. *For any abelian groups A, B and V, there are natural isomorphisms*

$$\mathrm{Hom}(A\otimes B,V) \simeq \mathrm{Bilin}(A,B;V) \simeq \mathrm{Hom}(A,\mathrm{Hom}(B,V)) \simeq \mathrm{Hom}(B,\mathrm{Hom}(A,V)).$$

More specifically, if we have elements

$$f_0 \in \mathrm{Hom}(A\otimes B,V) \qquad f_1 \in \mathrm{Bilin}(A,B;V) \qquad f_2 \in \mathrm{Hom}(A,\mathrm{Hom}(B,V)) \qquad f_3 \in \mathrm{Hom}(B,\mathrm{Hom}(A,V))$$

then they are related by the above isomorphisms if and only if for all $a \in A$ and $b \in B$ we have

$$f_0(a\otimes b) = f_1(a,b) = f_2(a)(b) = f_3(b)(a).$$

Proof. This is mostly trivial. For any map $f_1\colon A \times B \to V$, we can define a map $f_2\colon A \to \mathrm{Map}(B,V)$ by $f_2(a)(b) = f_1(a,b)$. If f_1 satisfies the right-linearity condition $f_1(a,b+b')$ we see that $f_2(a)(b+b') = f_2(a)(b) + f_2(a)(b')$, so $f_2(a)$ is a homomorphism from B to V, or in other words f_2 is a map from A to $\mathrm{Hom}(B,V)$. If f_1 also satisfies the left linearity condition $f_1(a+a',b) = f_1(a,b) + f_1(a',b)$ then we see that $f_2(a+a')$ is the sum of the homomorphisms $f_2(a)$ and $f_2(a')$, so f_2 itself is a homomorphism, or in other words $f_2 \in \mathrm{Hom}(A,\mathrm{Hom}(B,V))$. All of this is reversible, so we have an isomorphism $\mathrm{Bilin}(A,B;V) \simeq \mathrm{Hom}(A,\mathrm{Hom}(B,V))$. We can define $f_3(b)(a) = f_1(a,b)$ to obtain a similar isomorphism $\mathrm{Bilin}(A,B;V) \simeq \mathrm{Hom}(B,\mathrm{Hom}(A,V))$. Finally, Proposition 7.9 gives an isomorphism $\mathrm{Bilin}(A,B;V) \simeq \mathrm{Hom}(A\otimes B,V)$. $\square$

Proposition 7.12. *There are natural isomorphisms as follows:*

$$\begin{aligned} \eta_A\colon \mathbb{Z}\otimes A &\to A & \eta_A(n\otimes a) &= na \\ \tau_{AB}\colon A\otimes B &\to B\otimes A & \tau_{AB}(a\otimes b) &= b\otimes a \\ \alpha_{ABC}\colon A\otimes(B\otimes C) &\to (A\otimes B)\otimes C & \alpha_{ABC}(a\otimes(b\otimes c)) &= (a\otimes b)\otimes c. \end{aligned}$$

In other words, the operation $(-)\otimes(-)$ is commutative, associative and unital up to natural isomorphism.

Proof. First, we certainly have a bilinear map $\eta'_A\colon \mathbb{Z}\times A \to A$ given by $\eta'_A(n,a) = na$, and by Proposition 7.9 this gives a homomorphism $\eta_A\colon \mathbb{Z}\otimes A \to A$ as indicated. We can also define a homomorphism $\zeta_A\colon A \to \mathbb{Z}\otimes A$ by $\zeta_A(a) = 1\otimes a$, and it is clear that $\eta_A\zeta_A = 1_A$. In the opposite direction, we must show that the map

$$\xi = 1_{\mathbb{Z}\otimes A} - \zeta_A\eta_A\colon \mathbb{Z}\otimes A \to \mathbb{Z}\otimes A$$

is zero. By Proposition 7.11, it will suffice to show that the corresponding homomorphism $\xi'\colon \mathbb{Z} \to \mathrm{Hom}(A,\mathbb{Z}\otimes A)$ is zero. This is given by

$$\xi'(n)(a) = (n\otimes a) - (1\otimes na)$$

so visibly $\xi'(1) = 0$ but ξ' is a homomorphism so $\xi'(n) = n.\xi'(1) = 0$ for all n as required.

Next, Lemma 6.5 tells us that there is a unique homomorphism $\tau'_{AB}\colon \mathbb{Z}[A\times B] \to \mathbb{Z}[B\times A]$ with $\tau'_{AB}[a,b] = [b,a]$. It is visible that this is an isomorphism (with inverse τ'_{BA}) and that $\tau'_{AB}(R_{AB}) = R_{BA}$ so there is an induced isomorphism $\tau_{AB}\colon A\otimes B \to B\otimes A$, with inverse τ_{BA}.

Now fix $a \in A$, and define $\alpha''(a)\colon B\times C \to (A\otimes B)\otimes C$ by $\alpha''(a)(b,c) = (a\otimes b)\otimes c$. This is bilinear, and moreover $\alpha''(a+a') = \alpha''(a) + \alpha''(a')$, so we have a homomorphism

$$\alpha''\colon A \to \mathrm{Bilin}(B,C;(A\otimes B)\otimes C).$$

We also have an isomorphism

$$\mathrm{Bilin}(B,C;(A\otimes B)\otimes C) \simeq \mathrm{Hom}(B\otimes C,(A\otimes B)\otimes C)$$

and using that we obtain a homomorphism

$$\alpha'\colon A \to \mathrm{Hom}(B\otimes C;(A\otimes B)\otimes C).$$

characterised by $\alpha'(a)(b\otimes c) = (a\otimes b)\otimes c$. As in Proposition 7.11 this corresponds to a homomorphism $\alpha\colon A\otimes(B\otimes C)\to(A\otimes B)\otimes C$, given by

$$\alpha(a\otimes(b\otimes c)) = \alpha'(a)(b\otimes c) = (a\otimes b)\otimes c.$$

In the same way, we can construct $\beta\colon (A\otimes B)\otimes C\to A\otimes(B\otimes C)$ with $\beta((a\otimes b)\otimes c) = a\otimes(b\otimes c)$. This means that $\beta\alpha(x) = x$ whenever x has the form $a\otimes(b\otimes c)$, but elements of that form generate $A\otimes(B\otimes C)$, so $\beta\alpha = 1$. A similar argument shows that $\alpha\beta = 1$, so α is an isomorphism as required. □

Proposition 7.13. *For any families of abelian groups $(A_i)_{i\in I}$ and $(B_j)_{j\in J}$ there is a natural isomorphism*

$$\left(\bigoplus_{i\in I} A_i\right)\otimes\left(\bigoplus_{j\in J} B_j\right)\simeq\bigoplus_{(i,j)\in I\times J}(A_i\otimes B_j).$$

In particular, for any A, B and C we have $A\otimes(B\oplus C)\simeq(A\otimes B)\oplus(A\otimes C)$.

Proof. For brevity, let L and R be the left and right hand sides of the claimed isomorphism. For each i and j we can define a bilinear map $g'_{ij}\colon A_i\times B_j\to L$ by $g'_{ij}(a,b) = \iota_i(a)\otimes\iota_j(b)$. This gives a homomorphism $g_{ij}\colon A_i\otimes B_j\to L$, and Proposition 3.7 tells us that there is a unique $g\colon R\to L$ with $g\circ\iota_{ij} = g_{ij}$ for all i and j. In the opposite direction, we can define a bilinear map $f'\colon(\bigoplus A_i)\times(\bigoplus B_j)\to R$ by

$$f'(a,b) = \sum_{i\in\mathrm{supp}(a)}\sum_{j\in\mathrm{supp}(b)}\iota_{ij}(a_i\otimes b_j).$$

This corresponds in the usual way to a homomorphism $f\colon L\to R$. We leave it to the reader to check that $fg = 1_R$ and $gf = 1_L$. □

Corollary 7.14. *Given sets I and J and an abelian group B, we have natural isomorphisms $\mathbb{Z}[I]\otimes B\simeq\bigoplus_{i\in I}B$ and $\mathbb{Z}[I]\otimes\mathbb{Z}[J]\simeq\mathbb{Z}[I\times J]$. In particular, this gives $\mathbb{Z}^r\otimes B\simeq B^r$ and $\mathbb{Z}^r\otimes\mathbb{Z}^s\simeq\mathbb{Z}^{rs}$.*

Proof. By applying the Proposition to the family $\{\mathbb{Z}\}_{i\in I}$ and the family consisting of the single group B, we obtain $\mathbb{Z}[I]\otimes B\simeq\bigoplus_{i\in I}B$. If instead we use the family $\{\mathbb{Z}\}_{j\in J}$ on the right hand side, we obtain $\mathbb{Z}[I]\otimes\mathbb{Z}[J]\simeq\mathbb{Z}[I\times J]$. □

Another straightforward example is as follows:

Proposition 7.15. *For any integer n and any abelian group A there is a natural isomorphism $(\mathbb{Z}/n)\otimes A\simeq A/nA$. In particular, we have $(\mathbb{Z}/n)\otimes(\mathbb{Z}/m) = \mathbb{Z}/(n,m)$, where (n,m) denotes the greatest common divisor of n and m.*

Proof. We can define a bilinear map $f'\colon(\mathbb{Z}/n)\otimes A\to A/nA$ by $f'(k+n\mathbb{Z},a) = ka+nA$, and this induces a homomorphism $f\colon(\mathbb{Z}/n)\otimes A\to A/nA$. In the opposite direction, we can define $g\colon A/nA\to(\mathbb{Z}/n)\otimes A$ by $g(a+nA) = (1+n\mathbb{Z})\otimes a$. We leave it to the reader to check that these are well-defined and that fg and gf are identity maps. In particular, this gives $(\mathbb{Z}/n)\otimes(\mathbb{Z}/m) = \mathbb{Z}/(n\mathbb{Z}+m\mathbb{Z})$, but it is standard that $n\mathbb{Z}+m\mathbb{Z} = (n,m)\mathbb{Z}$. □

We saw in Section 5 that every finitely generated abelian group is a direct sum of groups of the form $\mathbb{Z}$ or $\mathbb{Z}/p^v$. We can thus use Proposition 7.13, Corollary 7.14 and Proposition 7.15 to understand the tensor product of any two finitely generated abelian groups.

We next consider the interaction between tensor products and exactness.

Proposition 7.16. *Let A, B, C and U be abelian groups.*

(a) *If we have an exact sequence*

$$A\xrightarrow{j}B\xrightarrow{q}C\to 0,$$

then the resulting sequence

$$U\otimes A\xrightarrow{1\otimes j}U\otimes B\xrightarrow{1\otimes q}U\otimes C\to 0$$

is also exact. (In other words, tensoring is right exact*.)*

(b) *If we have an injective map $j\colon A\to B$ and U is torsion-free, then $1\otimes j\colon U\otimes A\to U\otimes B$ is also injective.*

(c) *If we have a short exact sequence*

$$0 \to A \xrightarrow{j} B \xrightarrow{q} C \to 0,$$

and U is torsion-free, then the resulting sequence

$$0 \to U \otimes A \xrightarrow{1 \otimes j} U \otimes B \xrightarrow{1 \otimes q} U \otimes C \to 0$$

is also short exact.

For the first part, we will use the following criterion:

Lemma 7.17. *A sequence $A \xrightarrow{j} B \xrightarrow{q} C \to 0$ is exact iff for every abelian group V, the resulting sequence $0 \to \mathrm{Hom}(C,V) \xrightarrow{q^*} \mathrm{Hom}(B,V) \xrightarrow{j^*} \mathrm{Hom}(A,V)$ is exact.*

Remark 7.18. The evident analogous statement with short exact sequences is not valid. We will investigate this in more detail later.

Proof. Let $\mathcal{S}$ denote the first sequence, and write $\mathrm{Hom}(\mathcal{S},V)$ for the second one.

Suppose that $\mathcal{S}$ is exact, so q is surjective and $\ker(q) = \mathrm{image}(j)$. Suppose that $f \in \ker(q^*)$, so $f : C \to V$ and $fq = 0 : B \to V$. This means that $f(q(b)) = 0$ for all $b \in B$, but q is surjective, so $f(c) = 0$ for all $c \in C$, so $f = 0$. This proves that $\ker(q^*) = 0$, so q^* is injective. Now suppose that $g \in \ker(j^*)$, so $g : B \to V$ and $gj = 0$, or equivalently $g(\mathrm{image}(j)) = 0$, or equivalently $g(\ker(q)) = 0$. We thus have a well-defined map $f : C \to V$ given by $f(c) = g(b)$ for any b with $q(b) = c$. Now $f \in \mathrm{Hom}(C,V)$ and $q^*(f) = fq = g$, so $g \in \mathrm{image}(q^*)$. This proves that $\ker(j^*) = \mathrm{image}(q^*)$, so $\mathrm{Hom}(\mathcal{S},V)$ is exact.

Conversely, suppose that $\mathrm{Hom}(\mathcal{S},V)$ is exact for all V. Take $V = \mathrm{cok}(q) = C/q(B)$ and let $f : C \to V$ be the evident projection (which is surjective). By construction we have $q^*(f) = 0$ but q^* is assumed to be injective so f is zero as well as being surjective. This implies that $C/q(B) = 0$ so q is surjective.

Now instead take $V = C$. As $\mathrm{Hom}(\mathcal{S},C)$ is exact, we certainly have $j^*q^* = 0 : \mathrm{Hom}(C,C) \to \mathrm{Hom}(A,C)$. In particular, we see that $j^*q^*(1) = 0$ in $\mathrm{Hom}(A,C)$, or in other words that $qj = 0 : A \to C$. This implies that $\mathrm{image}(j) \leq \ker(q)$.

Finally, take $V = \mathrm{cok}(j) = B/j(A)$, and let $g : B \to V$ be the projection. Then $j^*(g) = gj = 0$, so $g \in \ker(j^*) = \mathrm{image}(q^*)$, so there exists $f : C \to B/j(A)$ with $fq = g : B \to B/j(A)$. Now if $q(b) = 0$ then $b + \mathrm{image}(j) = g(b) = f(q(b)) = 0$, so $b \in \mathrm{image}(j)$. This proves that $\ker(q) = \mathrm{image}(j)$, so $\mathcal{S}$ is exact as claimed. ☐

Proof of Proposition 7.16.

(a) By Lemma 7.17, the sequence

$$0 \to \mathrm{Hom}(C,V) \xrightarrow{q^*} \mathrm{Hom}(B,V) \xrightarrow{j^*} \mathrm{Hom}(A,V)$$

is exact for all V. As V is arbitrary we can replace it by $\mathrm{Hom}(U,V)$, where U and V are both arbitrary. This gives an exact sequence

$$0 \to \mathrm{Hom}(C,\mathrm{Hom}(U,V)) \xrightarrow{q^*} \mathrm{Hom}(B,\mathrm{Hom}(U,V)) \xrightarrow{j^*} \mathrm{Hom}(A,\mathrm{Hom}(U,V)),$$

and we can use Proposition 7.11 to rewrite it as

$$0 \to \mathrm{Hom}(U \otimes C,V) \xrightarrow{(1\otimes q)^*} \mathrm{Hom}(U \otimes B,V) \xrightarrow{(1\otimes j)^*} \mathrm{Hom}(U \otimes A,V).$$

Finally we apply Lemma 7.17 in the opposite direction to see that the sequence $U \otimes A \to U \otimes B \to U \otimes C \to 0$ is exact.

(b) Now suppose instead that we have an injective map $j : A \to B$, and that U is torsion-free. We must show that $(1 \otimes j) : U \otimes A \to U \otimes B$ is injective. If U is actually free then we may assume that $U = \mathbb{Z}[I]$ for some set I. In this case Corollary 7.14 tells us that $1 \otimes j$ is just a direct sum of copies of j and the claim is clear. In particular, this holds whenever U is finitely generated and torsion-free, as we see from Proposition 5.11. The real issue is to deduce the infinitely generated case from the finitely generated case. Suppose we have an element $x \in U \otimes A$ with $(1 \otimes j)(x) = 0$. We can write x in the form $x = \sum_{i=1}^n u_i \otimes a_i$ say. We then have $\sum_{i=1}^n u_i \otimes j(a_i) = 0$. Going back to Definition 7.3, we deduce that $\sum_i [u_i, j(a_i)]$ can be expressed in $\mathbb{Z}[U \times B]$ as a finite $\mathbb{Z}$-linear combination of terms of the form $[u+u',b]-[u,b]-[u',b]$ or $[u,b+b']-[u,b]-[u,b']$. Choose such an expression, and let S be the (finite) set of elements of U that are involved in that expression, together with the elements $u_1,\dots,u_n$ occuring in our expression for x. Let U_0 be the subgroup of U generated by S, which is finitely generated and torsion-free. We now have an element $x_0=\sum_i u_i\otimes a_i$ in $U_0\otimes A$ and we find that $(1\otimes j)(x_0)=0$ in $U_0\otimes B$. By the finitely generated case we see that $x_0=0$, but x is the image of x_0 under the evident homomorphism $A\otimes U_0\to A\otimes U$, so $x=0$ as required.

(c) This is just a straightforward combination of (a) and (b).

□

Note that in part (b) of the Proposition, it is definitely necessary to assume that U is torsion-free. Indeed, we can take $j\colon A\to B$ to be $n.1_{\mathbb{Z}}\colon\mathbb{Z}\to\mathbb{Z}$, and then $1\otimes j$ is just $n.1_U$, and these maps are injective for all $n>0$ if and only if U is torsion free.

For various purposes it is important to understand the kernel of $1\otimes j$ in more detail. We will first discuss the case $U=\mathbb{Z}/n$, which is quite straightforward.

Definition 7.19. We write $A[n]$ for $\{a\in A\mid na=0\}$, which can also be identified with $\mathrm{Hom}(\mathbb{Z}/n,A)$. (A homomorphism $u\colon\mathbb{Z}/n\to A$ corresponds to the element $u(1+n\mathbb{Z})\in A[n]$.)

Proposition 7.20. *Fix an integer $n>0$. For any short exact sequence $A\xrightarrow{j}B\xrightarrow{q}C$, there is a unique homomorphism $\delta\colon C[n]\to A/nA=(\mathbb{Z}/n)\otimes A$ such that $\delta(q(b))=a+nA$ whenever $nb=j(a)$. Moreover, this fits into an exact sequence*

$$0\to A[n]\xrightarrow{j}B[n]\xrightarrow{q}C[n]\xrightarrow{\delta}A/n\xrightarrow{j}B/n\xrightarrow{q}C/n\to 0.$$

Proof. This is just the Snake Lemma (Proposition 2.4) applied to the diagram

$$\begin{tikzcd}
A \arrow[r, tail, "j"] \arrow[d, "n.1_A"'] & B \arrow[r, two heads, "q"] \arrow[d, "n.1_B"'] & C \arrow[d, "n.1_C"'] \\
A \arrow[r, tail, "j"'] & B \arrow[r, two heads, "q"'] & C
\end{tikzcd}$$

□

It turns out that there are similar six-term exact sequences in much greater generality, involving the groups $\mathrm{Tor}(A,B)$ introduced in Definition 7.3. We start by recording an obvious fact:

Lemma 7.21. *There is an isomorphism $\tau_{AB}\colon\mathbb{Z}[A\times B]\to\mathbb{Z}[B\times A]$ given by $\tau_{AB}([a,b])=[b,a]$, and this induces an isomorphism $\tau_{AB}\colon\mathrm{Tor}(A,B)\to\mathrm{Tor}(B,A)$ with inverse τ_{BA}.* □

Lemma 7.22. *Let A and B be abelian groups, and let J and K be ideals in $\mathbb{Z}[A\times B]$ as in Definition 7.3. Then there are natural exact sequences*

$$0\to\mathrm{Tor}(A,B)\to A\otimes I_B^2\xrightarrow{1\otimes j_B}A\otimes I_B\xrightarrow{1\otimes q_B}A\otimes B\to 0$$

and

$$0\to\mathrm{Tor}(A,B)\to I_A^2\otimes B\xrightarrow{j_A\otimes 1}I_A\otimes B\xrightarrow{q_A\otimes 1}A\otimes B\to 0.$$

Proof. Let J and K be as in Definition 7.3. As $JK^2\leq JK$ and $J^2K^2\leq J^2K$ we have a map $f\colon(JK^2)/(J^2K^2)\to(JK)/(J^2K)$ given by $f(x+J^2K^2)=x+J^2K$. The cokernel is $JK/(J^2K+JK^2)$, which is $A\otimes B$ by definition. The kernel is $(JK^2\cap J^2K)/(J^2K^2)$, which is $\mathrm{Tor}(A,B)$ by definition. In other words, we have an exact sequence

$$0\to\mathrm{Tor}(A,B)\to\frac{JK^2}{J^2K^2}\xrightarrow{f}\frac{JK}{J^2K}\to A\otimes B\to 0.$$

Next, we have $\mathbb{Z}[A\times B]=\mathbb{Z}[A]\otimes\mathbb{Z}[B]$ by Corollary 7.14. For $p,q\geq 0$ we have ideals $I_A^p\leq\mathbb{Z}[A]$ and $I_B^q\leq\mathbb{Z}[B]$. These are free abelian groups by Theorem 6.6, so using Proposition 7.16(b) we see that the evident homomorphisms

$$\begin{array}{ccc}
I_A^p \otimes I_B^q & \longrightarrow & I_A^p \otimes \mathbb{Z}[B] \\
\downarrow & & \downarrow \\
\mathbb{Z}[A] \otimes I_B^q & \longrightarrow & \mathbb{Z}[A] \otimes \mathbb{Z}[B]
\end{array}$$

are all injective. This means that $I_A^p \otimes I_B^q$ can be identified with its image in $\mathbb{Z}[A \times B]$, which is just $J^p K^q$. Our exact sequence now takes the form

$$0 \to \mathrm{Tor}(A, B) \to \frac{I_A \otimes I_B^2}{I_A^2 \otimes I_B^2} \xrightarrow{f} \frac{I_A \otimes I_B}{I_A^2 \otimes I_B} \to A \otimes B \to 0.$$

Next, as tensoring is right exact (Proposition 7.16(a)) we can identify $(I_A \otimes I_B^2)/(I_A^2 \otimes I_B^2)$ with $(I_A/I_A^2) \otimes I_B^2$, which is $A \otimes I_B^2$ by Proposition 7.2. Similarly, we can identify $(I_A \otimes I_B^2)/(I_A^2 \otimes I_B^2)$ with $A \otimes I_B$, so our exact sequence becomes

$$0 \to \mathrm{Tor}(A, B) \to A \otimes I_B^2 \to A \otimes I_B \to A \otimes B \to 0$$

as claimed. The other sequence is obtained symmetrically, or by appealing to Lemma 7.21. □

Corollary 7.23. *If A or B is torsion-free then* $\mathrm{Tor}(A, B) = 0$. *In particular, this holds if A or B is free.*

Proof. If A is torsion-free then the homomorphism

$$A \otimes I_B^2 \to A \otimes I_B$$

is injective by Proposition 7.16(b), but $\mathrm{Tor}(A, B)$ is the kernel so $\mathrm{Tor}(A, B) = 0$. The other case follows symmetrically. □

We next discuss the functorial properties of Tor groups. Suppose we have homomorphisms $f\colon A \to A'$ and $g\colon B \to B'$. As discussed in Remark 7.5, these give a homomorphism $f \times g\colon A \times B \to A' \times B'$, which induces a ring map $(f \times g)_\bullet\colon \mathbb{Z}[A \times B] \to \mathbb{Z}[A' \times B']$, sending J and K to the coresponding ideals in $\mathbb{Z}[A' \times B']$. It therefore induces a homomorphism $\mathrm{Tor}(A, B) \to \mathrm{Tor}(A', B')$, which we denote by $\mathrm{Tor}(f, g)$. This makes $\mathrm{Tor}(A, B)$ a functor of the pair (A, B).

Now suppose we have two homomorphisms $f_0, f_1\colon A \to A'$. We then have ring maps $(f_0)_\bullet$, $(f_1)_\bullet$ and $(f_0 + f_1)_\bullet$ from $\mathbb{Z}[A]$ to $\mathbb{Z}[A']$, and it is not true that $(f_0 + f_1)_\bullet = (f_0)_\bullet + (f_1)_\bullet$. Because of this, it is not obvious that $\mathrm{Tor}(f_0 + f_1, g) = \mathrm{Tor}(f_0, g) + \mathrm{Tor}(f_1, g)$. However, this does turn out to be true, as we now prove.

Proposition 7.24.

(a) *Given homomorphisms $f_0, f_1\colon A \to A'$ and $g\colon B \to B'$ we have* $\mathrm{Tor}(f_0 + f_1, g) = \mathrm{Tor}(f_0, g) + \mathrm{Tor}(f_1, g)$.

(b) *Given homomorphisms $f\colon A \to A'$ and $g_0, g_1\colon B \to B'$ we have* $\mathrm{Tor}(f, g_0 + g_1) = \mathrm{Tor}(f, g_0) + \mathrm{Tor}(f, g_1)$.

(c) *Given families of groups $\{A_i\}_{i \in I}$ and $\{B_j\}_{j \in J}$ there is a natural isomorphism*

$$\bigoplus_{i,j} \mathrm{Tor}(A_i, B_j) \to \mathrm{Tor}\left(\bigoplus_i A_i, \bigoplus_j B_j\right).$$

Proof. Lemma 7.22 allows us to describe $\mathrm{Tor}(A, B)$ as the kernel of the map $1 \otimes j\colon A \otimes I_B^2 \to A \otimes I_B$, and claim (a) follows easily from this. Claim (b) is proved similarly.

For (c), let us put $A^* = \bigoplus_i A_i$ and $B^* = \bigoplus_j B_j$ and $T = \bigoplus_{i,j} \mathrm{Tor}(A_i, A_j)$. We have inclusions $\iota_i\colon A_i \to A^*$ and $\iota_j\colon B_j \to B^*$, which give homomorphisms $\mathrm{Tor}(\iota_i, \iota_j)\colon \mathrm{Tor}(A_i, B_j) \to \mathrm{Tor}(A^*, B^*)$. We also have inclusions $\iota_{ij}\colon \mathrm{Tor}(A_i, B_j) \to T$. By the universal property of coproducts (Proposition 3.7) there is a unique homomorphism $\phi\colon T \to \mathrm{Tor}(A^*, B^*)$ with $\phi \circ \iota_{ij} = \mathrm{Tor}(\iota_i, \iota_j)$ for all i and j. It is this map that we claim is an isomorphism.

For fixed j, we can identify $\mathrm{Tor}(A^*, B_j)$ with the kernel of the evident map $A^* \otimes I_{B_j}^2 \to A^* \otimes I_{B_j}$. From this it follows easily that $\mathrm{Tor}(A^*, B_j) = \bigoplus_i \mathrm{Tor}(A_i, B_j)$. A similar argument shows that $\mathrm{Tor}(A^*, B^*) = \bigoplus_j \mathrm{Tor}(A^*, B_j)$, and by putting these together we obtain $\mathrm{Tor}(A^*, B^*) \simeq T$ as claimed. We leave it to the reader to check that the isomorphism arising from this argument is the same as ϕ. □

Proposition 7.25. *For any abelian group U and any short exact sequence $A \to B \to C$ there is a natural exact sequence*

$$0 \to \mathrm{Tor}(U,A) \to \mathrm{Tor}(U,B) \to \mathrm{Tor}(U,C) \to U \otimes A \to U \otimes B \to U \otimes C \to 0.$$

Proof. Apply the Snake Lemma (Proposition 2.4) to the diagram

$$\begin{tikzcd} I_U^2 \otimes A \arrow[r] \arrow[d] & I_U^2 \otimes B \arrow[r] \arrow[d] & I_U^2 \otimes C \arrow[d] \\ I_U \otimes A \arrow[r] & I_U \otimes B \arrow[r] & I_U \otimes C, \end{tikzcd}$$

noting that the rows are short exact because I_U^2 and I_U are free. □

Remark 7.26. Let A and B be abelian groups. We can always choose a free abelian group F and a surjective homomorphism $p\colon F \to B$. Indeed, one possibility is to use the natural map $q\colon I_B \to B$ from Proposition 7.2, but we can also make a less natural choice that is typically much smaller. We then let F' denote the kernel of p, and note that this is again free by Theorem 6.6. Now the Proposition gives an exact sequence

$$0 \to \mathrm{Tor}(A,F') \to \mathrm{Tor}(A,F) \to \mathrm{Tor}(A,B) \to A \otimes F' \xrightarrow{1\otimes i} A \otimes F \to A \otimes B \to 0.$$

As F' and F are free we have $\mathrm{Tor}(A,F') = \mathrm{Tor}(A,F) = 0$, so we conclude that $\mathrm{Tor}(A,B)$ is isomorphic to the kernel of $1 \otimes i$.

A more traditional approach to Tor groups is to *define* $\mathrm{Tor}(A,B)$ as the kernel of $1 \otimes i$. In this approach one has to work to prove that the resulting group is well-defined up to canonical isomorphism, and that $\mathrm{Tor}(A,B) \simeq \mathrm{Tor}(B,A)$ and so on. However, one makes more contact with the general techniques of homological algebra, which are important for other reasons.

Remark 7.27. Suppose we have subgroups $A' \leq A$ and $B' \leq B$. Using Proposition 7.25 we see that the maps

$$\begin{tikzcd} \mathrm{Tor}(A',B') \arrow[r] \arrow[d] & \mathrm{Tor}(A',B) \arrow[d] \\ \mathrm{Tor}(A,B') \arrow[r] & \mathrm{Tor}(A,B) \end{tikzcd}$$

are all injective, so we can regard $\mathrm{Tor}(A',B')$ as a subgroup of $\mathrm{Tor}(A,B)$.

Proposition 7.28. $\mathrm{Tor}(A,B)$ *is the union of the subgroups* $\mathrm{Tor}(A',B')$ *for finite subgroups $A' \leq A$ and $B' \leq B$.*

Proof. Any element of $x \in \mathrm{Tor}(A,B)$ has the form $x = y + z + J^2K^2$ for some $y \in J^2K$ and $z \in JK^2$. We can write y as $\sum_{i=1}^{r} n_i \langle a_i\rangle\langle a_i'\rangle\langle b_i\rangle$ for some $n_i \in \mathbb{Z}$ and $a_i, a_i' \in A$ and $b_i \in B$. Similarly, we can write z as $\sum_{j=1}^{s} m_j \langle c_j\rangle\langle d_j\rangle\langle d_j'\rangle$ for some $m_j \in \mathbb{Z}$ and $c_j \in A$ and $d_j, d_j' \in B$. Let A_0 be the subgroup of A generated by the elements a_i, a_i' and c_j, and let B_0 be the subgroup of B generated by the elements b_i, d_j and d_j'. It is then clear that $x \in \mathrm{Tor}(A_0,B_0) \leq \mathrm{Tor}(A,B)$. Moreover, A_0 and B_0 are finitely generated, so the subgroups $A' = \mathrm{tors}(A_0)$ and $B' = \mathrm{tors}(B_0)$ are finite. It follows from Theorem 5.3 that $A_0 = A' \oplus P$ and $B_0 = B' \oplus Q$, where P and Q are free. This means that $\mathrm{Tor}(P,B') = \mathrm{Tor}(P,Q) = \mathrm{Tor}(A',Q) = 0$ by Corollary 7.23, so $\mathrm{Tor}(A_0,B_0) = \mathrm{Tor}(A',B')$. The claim follows. □

Corollary 7.29. $\mathrm{Tor}(A,B)$ *is always a torsion group.*

Proof. In view of the proposition, it will suffice to prove this when A is finite. In that case there exists n such that $n.1_A = 0$, and so $\mathrm{Tor}(n.1_A, 1_B) = 0\colon \mathrm{Tor}(A,B) \to \mathrm{Tor}(A,B)$. However, using Proposition 7.24 we see that $\mathrm{Tor}(n.1_A, 1_B) = n.\mathrm{Tor}(1_A, 1_B) = n.1_{\mathrm{Tor}(A,B)}$. This means that $nx = 0$ for all $x \in \mathrm{Tor}(A,B)$, so $\mathrm{Tor}(A,B)$ is a torsion group. □

We next show how to construct elements of $\mathrm{Tor}(A,B)$ more explicitly.

Proposition 7.30.

(a) *For $n > 0$ and $a \in A[n]$ and $b \in B[n]$ there is an element $e_n(a, b) \in \mathrm{Tor}(A, B)$ given by*

$$e_n(a, b) = n\langle a\rangle\langle b\rangle + J^2K^2 \in \frac{J^2K \cap JK^2}{J^2K^2} = \mathrm{Tor}(A, B).$$

(b) *The map $e_n : A[n] \times B[n] \to \mathrm{Tor}(A, B)$ is bilinear, so it induces a homomorphism $A[n] \otimes B[n] \to \mathrm{Tor}(A, B)$.*

(c) *Suppose we have elements $a \in A[n]$ and $b \in B[m]$. Let d be any common divisor of n and m. Then $(n/d)a \in A[m]$ and $(m/d)b \in A[n]$ and we have*

$$e_n(a, (m/d)b) = e_{nm/d}(a, b) = e_m((n/d)a, b).$$

(d) *Suppose we have a short exact sequence*

$$0 \to A \xrightarrow{j} B \xrightarrow{q} C \to 0$$

giving rise to an exact sequence

$$0 \to \mathrm{Tor}(U, A) \to \mathrm{Tor}(U, B) \to \mathrm{Tor}(U, C) \xrightarrow{\delta} U \otimes A \to U \otimes B \to U \otimes C \to 0$$

as in Proposition 7.25. Suppose that $u \in U[n]$ and $c \in C[n]$. Then $\delta(e_n(u, c))$ can be described as follows: we choose $b \in B$ with $q(b) = c$, then there is a unique $a \in A$ with $j(a) = nb$, and $\delta(e_n(u, c)) = u \otimes a$.

Proof.

(a) First, as $na = 0$ in $A \simeq I_A/I_A^2$ we see that $n\langle a\rangle \in I_A^2$ and so $n\langle a\rangle\langle b\rangle \in I_A^2 \otimes I_B = J^2K$. Similarly we have $n\langle b\rangle \in I_B^2$ so $n\langle a\rangle\langle b\rangle = \langle a\rangle.(n\langle b\rangle) \in I_A \otimes I_B^2 = JK^2$. Thus, we have $n\langle a\rangle\langle b\rangle \in J^2K \cap JK^2$ and the definition of e_n is meaningful.

(b) Next, recall that $\langle a + a'\rangle - \langle a\rangle - \langle a'\rangle = \langle a\rangle\langle a'\rangle \in I_A^2$, so

$$n\langle a + a'\rangle\langle b\rangle - n\langle a\rangle\langle b\rangle - n\langle a'\rangle\langle b\rangle = (\langle a\rangle\langle a'\rangle).(n\langle b\rangle) \in I_A^2 \otimes I_B^2 = J^2K^2,$$

so $e_n(a + a', b) = e_n(a, b) + e_n(a', b)$. By a symmetrical argument we see that $e_n(a, b)$ is also linear in b, as required.

(c) Suppose we have elements $a \in A[n]$ and $b \in B[m]$. Let d be any common divisor of n and m, so $n = pd$ and $m = qd$ for some $p, q > 0$. Now $m.(n/d)a = pqda = q.na = 0$, so $(n/d)a = pa \in A[m]$, and similarly $(m/d)b = qb \in B[m]$. Next note that

$$pd\langle a\rangle\langle qb\rangle - pqd\langle a\rangle\langle b\rangle = (n\langle a\rangle)(\langle qb\rangle - q\langle b\rangle) \in I_A^2 \otimes I_B^2 = J^2K^2,$$

so $e_{pd}(a, qb) = e_{pqd}(a, b)$, or $e_n(a, (m/d)b) = e_{nm/d}(a, b)$. By a symmetrical argument, we also have $e_{nm/d}(a, b) = e_m((n/d)a, b)$.

(d) For $u \in U[n]$ and $c \in C[n]$ we note that $n\langle u\rangle \in I_U^2$ so we can put $e'_n(u, c) = (n\langle u\rangle) \otimes c \in I_U^2 \otimes C$. Note that it is not legitimate to rewrite this as $\langle u\rangle \otimes nc$ because $\langle u\rangle \notin I_U^2$. However this rewriting becomes legitimate if we work in $I_U \otimes C$, and the result is zero because $nc = 0$. In other words, $e'_n(u, c)$ lies in the kernel of the map $I_U^2 \otimes A \to I_U \otimes A$, which was identified with $\mathrm{Tor}(U, A)$ in Lemma 7.22. It is not hard to check that $e'_n(u, c)$ corresponds to $e_n(u, c)$ under this identification. Now consider the diagram

$$\begin{array}{ccccc} I_U^2 \otimes A & \xrightarrow{1\otimes j} & I_U^2 \otimes B & \xrightarrow{1\otimes q} & I_U^2 \otimes C \\ {\scriptstyle i\otimes 1}\downarrow & & {\scriptstyle i\otimes 1}\downarrow & & \downarrow{\scriptstyle i\otimes 1} \\ I_U \otimes A & \xrightarrow[1\otimes j]{} & I_U \otimes B & \xrightarrow[1\otimes q]{} & I_U \otimes C. \end{array}$$

By inspecting the proof of Proposition 2.4 we find the following prescription for the connecting map $\delta : \mathrm{Tor}(U, C) \to A \otimes C$. Given $z \in I_U^2 \otimes C$ with $(i \otimes 1)(z) = 0$ we choose $y \in I_U^2 \otimes B$ with $(1 \otimes q)(y) = z$, then we check that $(i \otimes 1)(y) \in \ker(1 \otimes q) = \mathrm{image}(1 \otimes j)$ so there exists $x \in I_U \otimes A$ with $(1 \otimes j)(x) = (i \otimes 1)(y)$, and the image of x in $U \otimes A = (I_U/I_U^2) \otimes A$ is by definition $\delta(z)$. Now suppose again that we are given $u \in U[n]$ and $c \in C[n]$ and take $z = e'_n(u, c)$. As q is surjective we can choose $b \in B$ with $q(b) = a$. We then have $q(nb) = na = 0$ so $nb \in \ker(q) = \mathrm{image}(j)$, so there exists $a \in A$ with $j(a) = nb$. We can thus put $y = (n\langle u\rangle) \otimes b \in I_U^2 \otimes B$ and $x = \langle u\rangle \otimes a \in I_U \otimes A$, and we find that $(1\otimes q)(y) = z$ and $(i\otimes 1)(y) = \langle u\rangle \otimes nb = (1\otimes j)(\langle u\rangle \otimes a)$. This means that $\delta(e_n(u,a))$ is the image of $\langle u\rangle \otimes a$ in $U\otimes A$, which is just $u\otimes a$ as claimed.

$\square$

Corollary 7.31. *For any abelian group U and $n>0$, the map $u\mapsto e_n(u,1+n\mathbb{Z})$ gives an isomorphism $U[n]\mapsto \mathrm{Tor}(U,\mathbb{Z}/n)$.*

Proof. Consider the short exact sequence $\mathbb{Z}\xrightarrow{n}\mathbb{Z}\to\mathbb{Z}/n$. As $\mathrm{Tor}(U,\mathbb{Z})=0$ and $U\otimes\mathbb{Z}=\mathbb{Z}$ the six-term exact sequence reduces to

$$0\to \mathrm{Tor}(U,\mathbb{Z})\xrightarrow{\delta} U\xrightarrow{n} U\to U/n\to 0,$$

which means that δ gives an isomorphism $\delta\colon \mathrm{Tor}(U,\mathbb{Z})\to U[n]$. Part (d) of the proposition tells us that $\delta(e_n(u,1+n\mathbb{Z}))=u$ for all $u\in U[n]$, and the claim follows from this. $\square$

Corollary 7.32. *For any abelian groups A and B, the group $\mathrm{Tor}(A,B)$ is generated by all the elements $e_n(a,b)$ for $n>0$ and $a\in A[n]$ and $b\in B[n]$.*

Proof. In view of Proposition 7.28, it is enough to prove this when A and B are finite. Now A and B can be written as direct sums of finite cyclic groups, and using Proposition 7.24(c) we reduce to the case where A and B are themselves cyclic. That case is immediate from Corollary 7.31. $\square$

Corollary 7.33. *For any abelian group B, there is a natural isomorphism $\mathrm{Tor}(\mathbb{Q}/\mathbb{Z},B)\simeq \mathrm{tors}(B)$.*

Proof. Let A_m be the subgroup of $\mathbb{Q}/\mathbb{Z}$ generated by $1/m+\mathbb{Z}$, and define $\epsilon_m\colon B[m]\to \mathrm{Tor}(A_m,B)\leq \mathrm{Tor}(\mathbb{Q}/\mathbb{Z},B)$ by $\epsilon_m(b)=e_n(1/m+\mathbb{Z},b)$. Note that A_m is cyclic of order m, so the previous result tells us that ϵ_m is an isomorphism. Now suppose that m divides n, so $B[m]\leq B[n]$. We can take $d=m$ in Proposition 7.30(c) to see that $e_n(a,b)=e_m((n/m)a,b)$ whenever $na=0$ and $mb=0$. Taking $a=1/n+\mathbb{Z}$ we deduce that $\epsilon_n(b)=\epsilon_m(b)$ whenever $mb=0$, so $\epsilon_n|_{B[m]}=\epsilon_m$. It follows that there is a unique homomorphism

$$\epsilon\colon\ \mathrm{tors}(B)=\bigcup_{n>0}B[n]\to \mathrm{Tor}(\mathbb{Q}/\mathbb{Z},B).$$

Every finite subgroup of $\mathbb{Q}/\mathbb{Z}$ has the form A_n for some n, and it follows from this using Proposition 7.28 that ϵ is an isomorphism.

There is an explicit construction of the inverse which is quite instructive. An element $x\in\mathbb{Q}/\mathbb{Z}$ is a coset of $\mathbb{Z}$ in $\mathbb{Q}$, and any such coset intersects the interval $[0,1)$ in a single point, which we call $\lambda(x)$. The function $\lambda\colon \mathbb{Q}/\mathbb{Z}\to\mathbb{Q}$ is not a homomorphism, but $\lambda(x+x')$ and $\lambda(x)+\lambda(x')$ are both representatives of the same coset $x+x'$, so we at least have

$$\lambda(x+x')-\lambda(x)-\lambda(x')\in\mathbb{Z}.$$

We can extend λ to give a group homomorphism $\mathbb{Z}[\mathbb{Q}/\mathbb{Z}]\to\mathbb{Q}$ by $\lambda(\sum_i n_i[x_i])=\sum_i n_i\lambda(x_i)$. We then find that

$$\lambda(\langle x\rangle\langle x'\rangle)=\lambda([x+x']-[x]-[x']+[0])=\lambda(x+x')-\lambda(x)-\lambda(x')\in\mathbb{Z},$$

and thus that $\lambda(I^2_{\mathbb{Q}/\mathbb{Z}})\leq\mathbb{Z}$. We therefore have a homomorphism $\lambda\otimes 1\colon I^2_{\mathbb{Q}/\mathbb{Z}}\otimes B\to\mathbb{Z}\otimes B=B$. Lemma 7.22 allows us to regard $\mathrm{Tor}(\mathbb{Q}/\mathbb{Z},B)$ as a subgroup of $I^2_{\mathbb{Q}/\mathbb{Z}}\otimes B$, so we can restrict to this subgroup to get a homomorphism $\mu\colon \mathrm{Tor}(\mathbb{Q}/\mathbb{Z},B)\to B$. We leave it to the reader to check that the image of μ is $\mathrm{tors}(B)$, and that $\mu\colon \mathrm{Tor}(\mathbb{Q}/\mathbb{Z},B)\to\mathrm{tors}(B)$ is inverse to ϵ. $\square$

Proposition 7.34. *Define maps*

$$\bigoplus_{n,m,d}(A[nd]\otimes B[md]) \underset{\rho}{\overset{\lambda}{\rightrightarrows}} \bigoplus_p(A[p]\otimes B[p]) \xrightarrow{\ \epsilon\ } \mathrm{Tor}(A,B)$$

by

$$\lambda(i_{n,m,d}(a\otimes b))=i_{nd}(a\otimes mb)$$
$$\rho(i_{n,m,d}(a\otimes b))=i_{md}(na\otimes b)$$
$$\epsilon(i_p(a\otimes b))=e_p(a,b).$$

Then the sequence

$$\bigoplus_{n,m,d}(A[nd]\otimes B[md]) \xrightarrow{\lambda-\rho} \bigoplus_p(A[p]\otimes B[p]) \xrightarrow{\epsilon} \mathrm{Tor}(A,B) \longrightarrow 0$$

is exact, so $\mathrm{Tor}(A,B)$ *is the cokernel of* $\lambda-\rho$.

Proof. Let $T(A,B)$ be the cokernel of $\lambda-\rho$, and let $e'_p(a,b)$ be the image of $i_p(a\otimes b)$ in $T(A,B)$, so by construction we have $e'_{nd}(a,mb) = e'_{md}(na,b)$ whenever $nda=0$ and $mdb=0$. Part (c) of Proposition 7.30 shows that $\epsilon\lambda=\epsilon\rho$, so $\mathrm{img}(\lambda-\rho)\leq\ker(\epsilon)$, so there is a unique homomorphism $\overline{\epsilon}\colon T(A,B)\to\mathrm{Tor}(A,B)$ such that $\overline{\epsilon}(e'_p(a,b)) = e_p(a,b)$ for all $p\geq 1$ and $a\in A[p]$ and $b\in B[p]$. This is surjective by Corollary 7.32. We must show that this is also injective.

Consider the special case where A and B are finitely generated. It is easy to see that there are natural splittings

$$T(A\oplus A', B\oplus B') \simeq T(A,B)\oplus T(A,B')\oplus T(A',B)\oplus T(A',B')$$
$$\mathrm{Tor}(A\oplus A', B\oplus B') \simeq \mathrm{Tor}(A,B)\oplus \mathrm{Tor}(A,B')\oplus \mathrm{Tor}(A',B)\oplus \mathrm{Tor}(A',B')$$

so we can reduce to the case where A and B are cyclic. If $A=\mathbb{Z}$ or $B=\mathbb{Z}$ it is clear that $T(A,B)=0=\mathrm{Tor}(A,B)$, so we may assume that $A=\mathbb{Z}/r$ and $B=\mathbb{Z}/s$ say. Let t be the least common multiple of r and s, so we have an element $u=e'_t(1+r\mathbb{Z},1+s\mathbb{Z})\in T(A,B)$. Note that $T(A,B)$ is generated by elements of the form $v=e_p(a+r\mathbb{Z},b+s\mathbb{Z})$ with $pa\in r\mathbb{Z}$ and $pb\in s\mathbb{Z}$, which implies that $pab=tc$ for some $c\in\mathbb{Z}$. We thus have an element

$$x = i_{c,1,t}(1+r\mathbb{Z},1+s\mathbb{Z}) + i_{1,b,ap}(1+r\mathbb{Z},1+s\mathbb{Z}) - i_{a,1,p}(1+r\mathbb{Z},b+s\mathbb{Z}) \in \bigoplus_{n,m,d}(A[nd]\otimes B[md]),$$

and we find that

$$(\lambda-\rho)(x) = i_p((a+r\mathbb{Z})\otimes(b+s\mathbb{Z})) - i_t(c+r\mathbb{Z},1+s\mathbb{Z}) = i_p((a+r\mathbb{Z})\otimes(b+s\mathbb{Z})) - c\, i_t(1+r\mathbb{Z},1+s\mathbb{Z})$$

so $v=cu$. This proves that u generates $T(A,B)$. It is also clear that $ru=su=0$, so if we put $d=(r,s)$ we have $du=0$. This means that $T(A,B)$ is cyclic of order dividing d but the map $T(A,B)\to\mathrm{Tor}(A,B)\simeq\mathbb{Z}/d$ is surjective so it must be an isomorphism.

We now revert to the general case, where A and B may be infinitely generated. Consider an element $w\in\ker(\overline{\epsilon})\leq T(A,B)$. We can write w as $\sum_{i=1}^N e'_{p_i}(a_i,b_i)$ say, and then let A' be the subgroup of A generated by $a_1,\dots,a_N$, and let B' be the subgroup of B generated by $b_1,\dots,b_N$. There is then an evident element $w'\in T(A',B')$ that maps to w in $T(A,B)$. Now consider the diagram

$$\begin{tikzcd}
T(A',B') \arrow[r, "\overline{\epsilon}", "\simeq"'] \arrow[d] & \mathrm{Tor}(A',B') \arrow[d, tail] \\
T(A,B) \arrow[r, two heads, "\overline{\epsilon}"'] & \mathrm{Tor}(A,B).
\end{tikzcd}$$

The top map is an isomorphism by the special case considered above, and the right hand map is injective by Remark 7.27. By chasing w' around the diagram we see that $w=0$. Thus, the map $\overline{\epsilon}\colon T(A,B)\to\mathrm{Tor}(A,B)$ is injective as required. $\square$

8. Ext groups

Definition 8.1. Let A and B be abelian groups, and let j be the inclusion $I_A^2\to I_A$. We define $\mathrm{Ext}(A,B)$ to be the cokernel of the map $j^*\colon \mathrm{Hom}(I_A,B)\to\mathrm{Hom}(I_A^2,B)$. Now suppose we have homomorphisms $f\colon A'\to A$ and $g\colon B\to B'$. We then have compatible homomorphisms $f_\bullet\colon I_{A'}\to I_A$ and $f_\bullet\colon I_{A'}^2\to I_A^2$, and we can use these in an evident way to construct a commutative square of maps

$$\begin{tikzcd}
\mathrm{Ext}(A,B) \arrow[r, "g_*"] \arrow[d, "f^*"'] & \mathrm{Ext}(A,B') \arrow[d, "f^*"] \\
\mathrm{Ext}(A',B) \arrow[r, "g_*"'] & \mathrm{Ext}(A',B')
\end{tikzcd}$$

Remark 8.2. Let q be the usual map $I_A \to A$, with kernel I_A^2. Consider the sequence

$$0 \to \mathrm{Hom}(A,B) \xrightarrow{q^*} \mathrm{Hom}(I_A,B) \xrightarrow{j^*} \mathrm{Hom}(I_A^2,B) \to \mathrm{Ext}(A,B) \to 0.$$

By combining Lemma 7.17 with Definition 8.1, we see that this is exact.

Remark 8.3. If we have two homomorphisms $g_0, g_1 \colon B \to B'$, it is clear that

$$(g_0+g_1)_* = g_{0*} + g_{1*} \colon \mathrm{Ext}(A,B) \to \mathrm{Ext}(A,B').$$

If we have two homomorphisms $f_0, f_1 \colon A' \to A$, it is not obvious from the definitions that $(f_0+f_1)^* = f_0^* + f_1^*$, but later we will give a different description of the Ext groups that makes this fact clear.

Lemma 8.4. *Let F be a free abelian group. Then for every surjective homomorphism $q \colon B \to C$, the resulting map $q_* \colon \mathrm{Hom}(F,B) \to \mathrm{Hom}(F,C)$ is also surjective. Equivalently, for every pair of homomorphisms f and q as shown with q surjective, there exists g with $qg = f$.*

$$\begin{tikzcd} & F \arrow[dl, dotted, "g"'] \arrow[d, "f"] \\ B \arrow[r, two heads, "q"'] & C. \end{tikzcd}$$

Conversely, every group F with this property is free.

Proof. Firstly, there exists a map g as shown if and only if the element $f \in \mathrm{Hom}(F,C)$ lies in the image of $q_* \colon \mathrm{Hom}(F,B) \to \mathrm{Hom}(F,C)$; so the two versions of the statement are indeed equivalent. To prove them, we may assume that $F = \mathbb{Z}[I]$ for some I. We then have elements $f([i]) \in C$ and $q \colon B \to C$ is surjective so we can choose $b_i \in B$ with $q(b_i) = f([i])$. Now there is a unique homomorphism $g \colon \mathbb{Z}[I] \to B$ with $g([i]) = b_i$ for all i, and $qg = f$ as required.

Conversely, let F be any abelian group that has the property under consideration. Take $C = F$ and $B = I_F$, let $q \colon B \to C$ be the usual surjection $I_F \to F$, and let $f \colon F \to C$ be the identity. Then there must exist $g \colon F \to I_F$ with $qg = 1_F$. This means that g is injective, so F is isomorphic to a subgroup of the free group I_F, so F is free by Theorem 6.6. $\square$

Remark 8.5. In the more general context of modules over an arbitrary ring, the property in the lemma is called *projectivity.* Thus, we have shown that an abelian group is projective if and only if it is free. The same argument shows that an R-module is projective if and only if it is a direct summand in a free R-module. The analogue of Theorem 6.6 is not valid for modules over a general ring, so projective modules need not be free.

Proposition 8.6. *Let U be an abelian group, and let $A \xrightarrow{j} B \xrightarrow{q} C$ be a short exact sequence of abelian groups. Then there is a natural exact sequence*

$$0 \to \mathrm{Hom}(U,A) \xrightarrow{j_*} \mathrm{Hom}(U,B) \xrightarrow{q_*} \mathrm{Hom}(U,C) \xrightarrow{\delta} \mathrm{Ext}(U,A) \xrightarrow{j_*} \mathrm{Ext}(U,B) \xrightarrow{q_*} \mathrm{Ext}(U,C) \to 0.$$

Proof. We first claim that the sequence

$$0 \to \mathrm{Hom}(U,A) \xrightarrow{j_*} \mathrm{Hom}(U,B) \xrightarrow{q_*} \mathrm{Hom}(U,C)$$

is exact. Indeed, if $j_*(\alpha) = 0$ then $j(\alpha(u)) = 0$ for all u, but j is injective so $\alpha(u) = 0$ for all u, so $\alpha = 0$; this proves that j_* is injective. Next, suppose that $q_*(\beta) = 0$, so $q(\beta(u)) = 0$ for all $u \in U$, so $\beta(u) \in \ker(q) = \mathrm{image}(j)$, so there exists $\alpha(u) \in A$ with $\beta(u) = j(\alpha(u))$. This element $\alpha(u)$ is in fact unique, because j is injective. We also have

$$j(\alpha(u+u') - \alpha(u) - \alpha(u')) = j(\alpha(u+u')) - j(\alpha(u)) - j(\alpha(u')) = \beta(u+u') - \beta(u) - \beta(u') = 0,$$

but j is injective so $\alpha(u+u') - \alpha(u) - \alpha(u') = 0$, so the map $\alpha \colon U \to A$ is a homomorphism. Clearly $j_*(\alpha) = \beta$, so we see that $\ker(q_*) = \mathrm{image}(j_*)$ as required.

Now consider the sequence

$$0 \to \mathrm{Hom}(I_U,A) \xrightarrow{j_*} \mathrm{Hom}(I_U,B) \xrightarrow{q_*} \mathrm{Hom}(I_U,C) \to 0.$$

As U was arbitrary we can replace it by I_U to see that j_* is injective and $\text{image}(j_*) = \ker(q_*)$. As I_U is free we also see from Lemma 8.4 that q_* is surjective, so the sequence is short exact. The same argument applies with I_U replaced by I_U^2.

Now consider the diagram

$$\begin{tikzcd} \mathrm{Hom}(I_U, A) \arrow[r, tail, "j_*"] \arrow[d] & \mathrm{Hom}(I_U, B) \arrow[r, two heads, "q_*"] \arrow[d] & \mathrm{Hom}(I_U, C) \arrow[d] \\ \mathrm{Hom}(I_U^2, A) \arrow[r, tail, "j_*"'] & \mathrm{Hom}(I_U^2, B) \arrow[r, two heads, "q_*"'] & \mathrm{Hom}(I_U^2, C). \end{tikzcd}$$

We have just seen that the rows are short exact, so we can apply the Snake Lemma (Proposition 2.4) to get a six-term exact sequence involving the kernels and cokernels of the vertical maps. Remark 8.2 identifies these kernels and cokernels as Hom and Ext groups, as required. □

Corollary 8.7. *An abelian group F is free if and only if* $\mathrm{Ext}(F, A) = 0$ *for all A.*

Proof. First suppose that F is free. By applying Lemma 8.4 to the diagram

$$\begin{tikzcd} & F \arrow[dl, dotted, "s"'] \arrow[d, "1"] \\ I_F \arrow[r, two heads, "q"'] & F \end{tikzcd}$$

we obtain a homomorphism $s\colon F \to I_F$ with $qs = 1_F$. This gives a splitting in the usual way, so there is a unique map $r\colon I_F \to \ker(q) = I_F^2$ with $jr = 1 - sq$ and we have $rj = 1_{I_F^2}$. Now for any A we have homomorphisms

$$\mathrm{Hom}(I_F^2, A) \xrightarrow{r^*} \mathrm{Hom}(I_F, A) \xrightarrow{j^*} \mathrm{Hom}(I_F^2, A)$$

with $j^*r^* = (rj)^* = 1^* = 1$. This implies that j^* is surjective, so the cokernel is zero. But $\mathrm{Ext}(F, A)$ is defined to be $\mathrm{cok}(j^*)$, so $\mathrm{Ext}(F, A) = 0$ as claimed.

Conversely, suppose that $\mathrm{Ext}(F, A) = 0$ for all A. Let $q\colon B \to C$ be a surjective homomorphism. If we put $A = \ker(q)$, then Proposition 8.6 gives an exact sequence

$$0 \to \mathrm{Hom}(U, A) \xrightarrow{j_*} \mathrm{Hom}(U, B) \xrightarrow{q_*} \mathrm{Hom}(U, C) \xrightarrow{\delta} 0 \xrightarrow{j_*} 0 \xrightarrow{q_*} 0 \to 0.$$

From this we deduce that q_* is surjective. By the last part of Lemma 8.4, this means that F is free. □

To complete our study of Ext groups, we will need to understand groups D with the "dual" property that $\mathrm{Ext}(A, D) = 0$ for all A. These will turn out to be the divisible groups, as defined below.

Definition 8.8. Let V be an abelian group. We say that V is *divisible* if for all integers $n > 0$ and all $v \in V$ there exists $u \in V$ with $nu = v$. Equivalently, V is divisible iff all the maps $n.1_V\colon V \to V$ (for $n > 0$) are surjective.

Example 8.9. The groups $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{Q}/\mathbb{Z}$ are all divisible. The only divisible finite group is the trivial group.

Remark 8.10. It is clear that any quotient of a divisible group is divisible.

Remark 8.11. If A is divisible, then (using the Axiom of Choice) we can choose functions $d_n\colon A \to A$ for $n > 0$ such that $n.d_n(a) = a$ for all n and a (so in particular $d_1(a) = a$), and we can also ensure that $d_n(0) = 0$ for all n. Of course, d_n need not be a homomorphism. We will call such a system of maps a *division system* for A. In many cases one can make an explicit choice for d_n. For $\mathbb{Q}$ or $\mathbb{R}$ we just have $d_n(a) = a/n$. For $A = \mathbb{Q}/\mathbb{Z}$, every element has a unique representation as $a = x + \mathbb{Z}$ with $0 \le x < 1$, and we put $d_n(a) = x/n + \mathbb{Z}$.

Proposition 8.12. *Let D be a divisible group. Then for any injective homomorphism $j\colon A \to B$, the resulting homomorphism $j^*\colon$ $\mathrm{Hom}(B, D) \to \mathrm{Hom}(A, D)$ is surjective. Equivalently, given homomorphisms j and f as shown below, there exists $g\colon B \to D$ with $gj = f$.*

$$\begin{tikzcd} A \arrow[r, tail, "j"] \arrow[d, "f"'] & B \arrow[dl, dotted, "g"] \\ D. \end{tikzcd}$$

Conversely, any group D that has this property is divisible.

Proof. Firstly, there exists a map g as shown if and only if the element $f \in \mathrm{Hom}(A, D)$ lies in the image of $j^*\colon \mathrm{Hom}(B, D) \to \mathrm{Hom}(A, D)$; so the two versions of the statement are indeed equivalent.

Next, we claim that if D has the above extension property then it is divisible. This is immediate from the special case of the extension property where $A = B = \mathbb{Z}$ and $j = n.1_{\mathbb{Z}}$ for some $n > 0$.

For the main part of the proof, suppose that D is divisible, and that we are given j and f as shown. It will be harmless to replace A by the isomorphic group $j(A) \leq B$ and so assume that $A \leq B$ and that j is just the inclusion. We then need to find $g\colon B \to D$ with $g|_A = f$. For this we choose a division system $(d_n)_{n>0}$ for D and a well-ordering of B. For $b \in B$ we let $B_{<b}$ denote the subgroup generated by $A \cup \{x \in B \mid x < b\}$, and similarly for $B_{\leq b}$. We then have $\{k \in \mathbb{Z} \mid kb \in B_{<b}\} = \mathbb{Z}.n_b$ for some $n_b \geq 0$. Note that if $n_b = 0$ then $B_{\leq b} = B_{<b} \oplus \mathbb{Z}$, with the $\mathbb{Z}$ summand generated by b. We say that a homomorphism $g\colon B_{\leq b} \to D$ is *admissible* if

- $g|_A = f$
- Whenever $x \leq b$ with $n_x = 0$ we have $g(x) = 0$
- Whenever $x \leq b$ with $n_x > 0$ we have $g(x) = d_{n_x}(g(n_x x))$.

We claim that for all b there is a unique admissible homomorphism $g_b\colon B_{\leq b} \to D$. If not, let b be the least element for which this is false (which is meaningful because B is well-ordered). For all $x < b$, we have a unique admissible map $g_x\colon B_{\leq x} \to D$. By uniqueness, we see that g_x agrees with g_y on $B_{\leq y}$ whenever $y \leq x < b$. It follows that the maps g_x can be combined to give a map $g'\colon B_{<b} \to D$. If $n_b = 0$, we find that there is a unique extension $g_b\colon B_{\leq b} \to D$ satisfying $g_b(u + kb) = g'(u)$ for all $u \in B_{<b}$ and $k \in \mathbb{Z}$. If $n_b > 0$, then we have an element $z = d_{n_b}(g'(n_b b)) \in D$ with $nz = g'(n_b b)$, and we see that there is a unique extension $g_b\colon B_{\leq b} \to D$ satisfying $g_b(u + kb) = g'(u) + kz$ for all $u \in B_{<b}$ and $k \in \mathbb{Z}$. Either way, we find that g_b is the unique admissible map on $B_{\leq b}$, contrary to assumption. Thus, we have g_b for all b, and we again see that g_b agrees with g_c on $B_{\leq c}$ whenever $c \leq b$, so the maps g_b fit together to give a homomorphism $g\colon B \to D$. This clearly satisfies $g|_A = f$ as required. □

Corollary 8.13. *If D is divisible, then $\mathrm{Ext}(A, D) = 0$ for all A.*

Remark 8.14. The converse statement is also true, but it will be more convenient to prove that later.

Proof. $\mathrm{Ext}(A, D)$ is by definition the cokernel of $j^*\colon \mathrm{Hom}(I_A, D) \to \mathrm{Hom}(I_A^2, D)$, but j^* is surjective by the proposition. □

We next want to show that every abelian group can be embedded in a divisible group. This will be proved after some preliminaries.

Proposition 8.15. *Let A be an abelian group, and let a be a nontrivial element of A. Then there is a homomorphism $f\colon A \to \mathbb{Q}/\mathbb{Z}$ with $f(a) \neq 0$.*

Proof. Put $A_0 = \mathbb{Z}a \leq A$. If a has infinite order then $A_0 \simeq \mathbb{Z}$ and we can define $f_0\colon A_0 \to \mathbb{Q}/\mathbb{Z}$ by $f_0(ka) = k/2 + \mathbb{Z}$. If a has finite order n we can instead define $f_0\colon A_0 \to \mathbb{Q}/\mathbb{Z}$ by $f_0(ka) = k/n + \mathbb{Z}$. Either way we have $f_0(a) \neq 0$. Next, as $\mathbb{Q}/\mathbb{Z}$ is divisible, Proposition 8.12 tells us that the restriction map $\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(A_0, \mathbb{Q}/\mathbb{Z})$ is surjective, so we can choose $f\colon A \to \mathbb{Q}/\mathbb{Z}$ with $f|_{A_0} = f_0$. In particular, this means that $f(a) \neq 0$, as required. □

Lemma 8.16. *For any set I, the group $\mathrm{Map}(I, \mathbb{Q}/\mathbb{Z})$ is divisible.*

Proof. Let $(d_n)_{n>0}$ be the standard division system for $\mathbb{Q}/\mathbb{Z}$ as in Remark 8.11. The maps $u \mapsto d_n \circ u$ then give a division system for $\mathrm{Map}(I, \mathbb{Q}/\mathbb{Z})$. □

Now suppose we have a family of homomorphisms $f_i\colon A \to \mathbb{Q}/\mathbb{Z}$ for $i \in I$. We can combine them to give a single homomorphism $j\colon A \to \mathrm{Map}(I, \mathbb{Q}/\mathbb{Z})$ by the rule $j(a)(i) = f_i(a)$. Note that the kernel of j is the intersection of the kernels of all the homomorphisms f_i. Thus, if the family is large enough we can hope that j will be injective.

The most canonical thing to do is to consider the family of *all* homomorphisms $f\colon A \to \mathbb{Q}/\mathbb{Z}$, and thus to take $I = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$. This leads us to the following definitions.

Definition 8.17. We put $E_A = \mathrm{Map}(\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}), \mathbb{Q}/\mathbb{Z})$, and define $j\colon A \to E_A$ by the rather tautological rule $j(a)(f) = f(a)$. We write E_A^2 for the cokernel of j, and q for the quotient map $E_A \to E_A^2$.

Proposition 8.18. *The groups E_A and E_A^2 are divisible, and the sequence*

$$A \xrightarrow{j} E_A \xrightarrow{q} E_A^2$$

is short exact.

Proof. The group E_A is divisible by Lemma 8.16, and E_A^2 is a quotient of E_A so it is also divisible. It is clear by construction that q is surjective with $\mathrm{image}(j) = \ker(q)$. Finally, if $a \in A$ is nonzero then Proposition 8.15 gives us a homomorphism $f \in \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ with $f(a) \neq 0$ or equivalently $j(a)(f) \neq 0$, so $j(a) \neq 0$. This shows that j is injective, so the sequence is short exact as claimed. $\square$

Remark 8.19. Note that for $a \in A$ and $f, g \in \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ we have

$$j(a)(f+g) = (f+g)(a) = f(a) + g(a) = j(a)(f) + j(a)(g),$$

so the map $j(a)\colon \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$ is a homomorphism. In other words, j can be regarded as an injective homomorphism

$$j\colon A \to \mathrm{Hom}(\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}), \mathbb{Q}/\mathbb{Z}).$$

If we use the briefer notation A^* for $\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$, then $j\colon A \to A^{**} \leq E_A$. The group A^{**} is usually not divisible, so E_A is more useful for our immediate applications to Ext groups. However, the group A^{**} will reappear later in other contexts.

Corollary 8.20. *For all A and B, there is a natural exact sequence*

$$0 \to \mathrm{Hom}(A, B) \xrightarrow{j_*} \mathrm{Hom}(A, E_B) \xrightarrow{q_*} \mathrm{Hom}(A, E_B^2) \to \mathrm{Ext}(A, B) \to 0.$$

Proof. Apply Proposition 8.6 to the sequence $B \to E_B \to E_B^2$, noting that $\mathrm{Ext}(A, E_B) = \mathrm{Ext}(A, E_B^2) = 0$ by Corollary 8.13. $\square$

Corollary 8.21. *For any $f_0, f_1\colon A' \to A$ we have $(f_0 + f_1)^* = f_0^* + f_1^*\colon \mathrm{Ext}(A, B) \to \mathrm{Ext}(A', B)$.*

Proof. The corresponding statement is clearly true for the induced maps on $\mathrm{Hom}(A, E_B^2)$, and Corollary 8.20 identifies $\mathrm{Ext}(A, B)$ in a natural way as a quotient group of $\mathrm{Hom}(A, E_B^2)$. $\square$

Corollary 8.22. *The natural maps*

$$\mathrm{Ext}(\bigoplus_i A_i, B) \to \prod_i \mathrm{Ext}(A_i, B)$$
$$\mathrm{Ext}(A, \prod_j B_j) \to \prod_j \mathrm{Ext}(A, B_j).$$

are isomorphisms.

Proof. The functors $\mathrm{Hom}(-, U)$ (for $U \in \{B, E_B, E_B^2\}$) convert coproducts to products, and the cokernel of a product is the product of the cokernels, so the first statement follows from Corollary 8.20. Similarly, the functors $\mathrm{Hom}(T, -)$ (for $T \in \{A, I_A, I_A^2\}$) preserve products, so the second statement follows from our original definition of Ext. $\square$

Proposition 8.23. *Let $A \xrightarrow{i} B \xrightarrow{p} C$ be a short exact sequence of abelian groups, and let V be an abelian group. Then there is a natural exact sequence*

$$0 \to \mathrm{Hom}(C, V) \xrightarrow{p^*} \mathrm{Hom}(B, V) \xrightarrow{i^*} \mathrm{Hom}(A, V) \xrightarrow{\delta} \mathrm{Ext}(C, V) \xrightarrow{p^*} \mathrm{Ext}(B, V) \xrightarrow{i^*} \mathrm{Ext}(A, V) \to 0.$$

Proof. Consider the diagram

$$\begin{array}{ccccc}
\mathrm{Hom}(C,E_V) & \xrightarrow{p^*} & \mathrm{Hom}(B,E_V) & \xrightarrow{i^*} & \mathrm{Hom}(A,E_V) \\
\downarrow{\scriptstyle q_*} & & \downarrow{\scriptstyle q_*} & & \downarrow{\scriptstyle q_*} \\
\mathrm{Hom}(C,E_V^2) & \xrightarrow[p^*]{} & \mathrm{Hom}(B,E_V^2) & \xrightarrow[i^*]{} & \mathrm{Hom}(A,E_V^2)
\end{array}$$

The rows are short exact by Lemma 7.17 together with Proposition 8.12. The Snake Lemma therefore gives us a six-term exact sequence involving the kernels and cokernels of the vertical maps q_*. Corollary 8.20 identifies these kernels and cokernels with Hom and Ext groups as required. □

Corollary 8.24. *For any groups B and V, and any subgroup $A \leq B$, the restriction $\mathrm{Ext}(B,V) \to \mathrm{Ext}(A,V)$ is surjective.* □

Corollary 8.25. *There are natural isomorphisms $\mathrm{Ext}(\mathbb{Z}/n, B) \simeq B/nB$ for $n > 0$, and $\mathrm{Ext}(\mathbb{Z}, B) = 0$.*

Note that in conjunction with Corollary 8.22 this allows us to calculate $\mathrm{Ext}(A,B)$ whenever A is finitely generated.

Proof. Corollary 8.7 tells us that $\mathrm{Ext}(\mathbb{Z}, B) = 0$ for all B. Now consider the short exact sequence

$$\mathbb{Z} \xrightarrow{n.1_{\mathbb{Z}}} \mathbb{Z} \to \mathbb{Z}/n.$$

Using Proposition 8.23 we obtain an exact sequence

$$0 \to \mathrm{Hom}(\mathbb{Z}/n, B) \to \mathrm{Hom}(\mathbb{Z}, B) \to \mathrm{Hom}(\mathbb{Z}, B) \to \mathrm{Ext}(\mathbb{Z}/n, B) \to \mathrm{Ext}(\mathbb{Z}, B) \to \mathrm{Ext}(\mathbb{Z}, B) \to 0.$$

Now $\mathrm{Ext}(\mathbb{Z}, B) = 0$, while $\mathrm{Hom}(\mathbb{Z}, B)$ is easily identified with B, and $\mathrm{Hom}(\mathbb{Z}/n, B)$ with $B[n] = \{b \in B \mid nb = 0\}$. We thus have an exact sequence

$$0 \to B[n] \to B \xrightarrow{n.1_B} B \xrightarrow{\delta} \mathrm{Ext}(\mathbb{Z}/n, B) \to 0.$$

From this it is clear that $\mathrm{Ext}(\mathbb{Z}/n, B) = \mathrm{cok}(n.1_B) = B/nB$. □

Proposition 8.26. *Let A be a torsion group. Then there is a canonical isomorphism*

$$\mathrm{Ext}(A, \mathbb{Z}) = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) = \prod_p \mathrm{Hom}(\mathrm{tors}_p(A), \mathbb{Q}/\mathbb{Z}),$$

and this maps surjectively to $\prod_p \mathrm{Hom}(A[p], \mathbb{Z}/p)$. In particular, if $\mathrm{Ext}(A, \mathbb{Z}) = 0$ then $A = 0$.

Proof. As A is torsion, and both $\mathbb{Z}$ and $\mathbb{Q}$ are torsion free, we see that $\mathrm{Hom}(A, \mathbb{Z}) = \mathrm{Hom}(A, \mathbb{Q}) = 0$. As $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible, we see from Proposition 8.12 that $\mathrm{Ext}(A, \mathbb{Q}) = \mathrm{Ext}(A, \mathbb{Q}/\mathbb{Z}) = 0$. Thus, if we apply Proposition 8.6 to the short exact sequence $\mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ we just get an isomorphism $\delta\colon \mathrm{Ext}(A, \mathbb{Z}) \to \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$. Next, Proposition 4.9 gives $A = \bigoplus_p \mathrm{tors}_p(A)$, so $\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) = \prod_p \mathrm{Hom}(\mathrm{tors}_p(A), \mathbb{Q}/\mathbb{Z})$. Now $A[p]$ is a subgroup of $\mathrm{tors}_p(A)$ and $\mathbb{Q}/\mathbb{Z}$ is divisible so the restriction

$$\mathrm{Hom}(\mathrm{tors}_p(A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(A[p], \mathbb{Q}/\mathbb{Z})$$

is surjective. Moreover, any homomorphism from $A[p] \to \mathbb{Q}/\mathbb{Z}$ necessarily lands in $(\mathbb{Q}/\mathbb{Z})[p]$, which is a copy of $\mathbb{Z}/p$ generated by the element $(1/p) + \mathbb{Z}$. By taking the product over all p, we get a surjection

$$\prod_p \mathrm{Hom}(\mathrm{tors}_p(A), \mathbb{Q}/\mathbb{Z}) \to \prod_p \mathrm{Hom}(A[p], \mathbb{Z}/p)$$

as claimed. The last statement follows from the isomorphism $\mathrm{Ext}(A, \mathbb{Z}) = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ together with Proposition 8.15. □

Example 8.27. We can take $A = \mathbb{Q}/\mathbb{Z}$, and we find that $\mathrm{Ext}(\mathbb{Q}/\mathbb{Z}, \mathbb{Z}) = \mathrm{End}(\mathbb{Q}/\mathbb{Z})$. It is easy to see that $(\mathbb{Q}/\mathbb{Z})[n]$ is a copy of $\mathbb{Z}/n$, generated by $(1/n) + \mathbb{Z}$. It follows that $\mathrm{Hom}((\mathbb{Q}/\mathbb{Z})[p], \mathbb{Z}/p) \simeq \mathbb{Z}/p$, and thus that $\prod_p \mathrm{Hom}((\mathbb{Q}/\mathbb{Z})[p], \mathbb{Z}/p)$ is uncountable, and thus that $\mathrm{End}(\mathbb{Q}/\mathbb{Z})$ is uncountable. Next, we can apply $\mathrm{Hom}(-, \mathbb{Z})$ and $\mathrm{Ext}(-, \mathbb{Z})$ to the sequence $\mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ to get a six term exact sequence. As $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible, we find that $\mathrm{Hom}(\mathbb{Q}, \mathbb{Z}) = \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, \mathbb{Z}) = 0$. We also have $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) = \mathbb{Z}$ and $\mathrm{Ext}(\mathbb{Z}, \mathbb{Z}) = 0$. The six term sequence therefore reduces to a short exact sequence $\mathbb{Z} \to \mathrm{End}(\mathbb{Q}/\mathbb{Z}) \to \mathrm{Ext}(\mathbb{Q}, \mathbb{Z})$. As $\mathbb{Z}$ is countable and $\mathrm{End}(\mathbb{Q}/\mathbb{Z})$ is uncountable, we deduce that $\mathrm{Ext}(\mathbb{Q}, \mathbb{Z})$ is uncountable. In particular, it is nonzero.

Definition 8.28. An *extension of C by A* is a short exact sequence $A \xrightarrow{i} B \xrightarrow{p} C$. We say that two extensions $(A \xrightarrow{i_0} B_0 \xrightarrow{p_0} C)$ and $(A \xrightarrow{i_1} B_1 \xrightarrow{p_1} C)$ are *equivalent* if there exists a map $f\colon B_0 \to B_1$ with $fi_0 = i_1$ and $p_1 f = p_0$. (Any such f is an isomorphism by a straightforward diagram chase, and using this we see that this notion of equivalence is reflexive, symmetric and transitive.)

Proposition 8.29. *Let $E = (A \xrightarrow{i} B \xrightarrow{p} C)$ be an extension of C by A.*

(a) *For any homomorphism $h\colon C' \to C$, we have an extension $h^*E = (A \xrightarrow{i'} B' \xrightarrow{p'} C')$ given by*

$$\begin{aligned} B' &= \{(b, c') \in B \oplus C' \mid p(b) = h(c')\} \\ i'(a) &= (i(a), 0) \\ p'(b, c') &= c'. \end{aligned}$$

(We call this the pullback *of E along h.)*

(b) *Suppose we have another extension $E^* = (A \xrightarrow{i^*} B^* \xrightarrow{p^*} C')$ and a commutative diagram*

$$\begin{tikzcd} A \arrow[r, tail, "i^*"] \arrow[d, equal] & B^* \arrow[r, two heads, "p^*"] \arrow[d, "g"] & C' \arrow[d, "h"] \\ A \arrow[r, tail, "i"'] & B \arrow[r, two heads, "p"'] & C \end{tikzcd}$$

Then E^* is equivalent to h^*E.

(c) *For any map $m\colon C' \to B$, the extension $(h + pm)^*E$ is equivalent to h^*E.*

(d) *If E_0 and E_1 are equivalent extensions of C by A, then h^*E_0 and h^*E_1 are also equivalent.*

Proof.

(a) We can certainly define a group B' and homomorphisms i' and p' by the given formulae. As i is injective, it is clear that i' is injective. Now suppose that $c' \in C'$. We then have $f(c') \in C$ and $p\colon B \to C$ is surjective by assumption, so we can choose $b \in B$ with $p(b) = f(c')$. This gives a point $b' = (b, c') \in B'$ with $p'(b') = c'$, so we see that p' is surjective. It is immediate that $p'i' = 0$, so $\mathrm{image}(i') \leq \ker(p')$. A general element of $\ker(p')$ has the form $b' = (b, 0)$ with $p(b) = f(0) = 0$, so $b \in \ker(p) = \mathrm{image}(i)$, so $b = i(a)$ for some $a \in A$. This means that $b' = i'(a) \in \mathrm{image}(i')$. We conclude that the sequence h^*E is indeed short exact, so it gives an extension of C' by A.

(b) Now suppose we have a commutative diagram as indicated. As $hp^* = pg$ we can define $g'\colon B^* \to B'$ by $g'(b^*) = (g(b^*), p^*(b^*))$. We then have $p'g'(b^*) = p^*(b^*)$ and

$$g'(i^*(a)) = (g(i^*(a)), p^*(i^*(a))) = (i(a), 0) = i'(a),$$

so $p'g' = p^*$ and $g'i^* = i'$. Thus, g' gives an equivalence between E^* and h^*E.

(c) By the construction in part (a), we have a commutative diagram

$$\begin{tikzcd} A \arrow[r, tail, "i'"] \arrow[d, equal] & B' \arrow[r, two heads, "p'"] \arrow[d, "g"] & C' \arrow[d, "h"] \\ A \arrow[r, tail, "i"'] & B \arrow[r, two heads, "p"'] & C \end{tikzcd}$$

(where $g(b, c') = b$). It follows easily that there is also a commutative diagram

$$\begin{tikzcd} A \arrow[r, tail, "i'"] \arrow[d, equal] & B' \arrow[r, two heads, "p'"] \arrow[d, "g+mp'"] & C' \arrow[d, "h+pm"] \\ A \arrow[r, tail, "i"'] & B \arrow[r, two heads, "p"'] & C. \end{tikzcd}$$

Now part (b) tells us that the top row is equivalent to $(h + pm)^*$ of the bottom row, or in other words $h^*E \simeq (h + pm)^*E$ as claimed.

(d) Suppose we have equivalent extensions $E_k = (A \xrightarrow{i_k} B_k \xrightarrow{p_k} C)$ for $k = 0, 1$, so there is an isomorphism $s\colon B_0 \to B_1$ with $si_0 = i_1$ and $p_1 s = p_0$. We can then define $s'\colon B_0' \to B_1'$ by $s'(b_0, c') = (s(b_0), c')$, and we find that $s'i_0' = i_1'$ and $p_1's' = p_0'$; this shows that h^*E_0 and h^*E_1 are equivalent as claimed.

$\square$

Proposition 8.30. *Let $E = (A \xrightarrow{i} B \xrightarrow{p} C)$ be an extension of C by A.*

(a) *For any homomorphism $f\colon A \to A'$, we have an extension $f_*E = (A' \xrightarrow{i'} B' \xrightarrow{p'} C)$ given by*

$$\begin{aligned} R &= \{(f(a), -i(a)) \mid a \in A\} \leq A' \oplus B \\ B' &= (A' \oplus B)/R \\ i'(a') &= (a', 0) + R \\ p'((a', b) + R) &= p(b). \end{aligned}$$

(We call this the pushout of E along f.*)*

(b) *Suppose we have another extension $E^* = (A \xrightarrow{i^*} B^* \xrightarrow{p^*} C')$ and a commutative diagram*

$$\begin{tikzcd} Aq \arrow[r, tail, "i"] \arrow[d, "f"'] & B \arrow[r, two heads, "p"] \arrow[d, "g"'] & C \arrow[d, equal] \\ A^* \arrow[r, tail, "i^*"'] & B^* \arrow[r, two heads, "p^*"'] & C \end{tikzcd}$$

Then E^* is equivalent to f_*E.

(c) *For any map $n\colon B \to A'$, the extension $(f + ni)_*E$ is equivalent to f_*E.*

(d) *If E_0 and E_1 are equivalent extensions of C by A, then f_*E_0 and f_*E_1 are also equivalent.*

Proof.

(a) We can certainly define groups R and B', and a homomorphism i', by the given formulae. If $(a', b) \in R$ then there exists $a \in A$ with $a' = f(a)$ and $b = -i(a)$, so $p(b) = -p(i(a)) = 0$. Given this, we see that the formula $p'((a', b) + R) = p(b)$ also gives a well-defined map $B' \to C$.

If $i'(a') = 0$ we must have $(a', 0) \in R$, so there exists $a \in A$ with $f(a) = a'$ and $i(a) = 0$. As i is injective this gives $a = 0$ and then $a' = f(0) = 0$. This proves that i' is injective. As p is surjective, it is immediate that p' is also surjective. Next, we have $p'i'(a') = p'((a', 0) + R) = p(0) = 0$, so $\text{image}(i') \leq \ker(p')$. Conversely, suppose we have an element $b' = (a', b) + R \in B'$ with $p'(b') = 0$. This means that $p(b) = 0$, so $b = i(a)$ for some $a \in A$. We then find that $(f(a), -i(a)) \in R$

$$b' = (a', b) + R = (a', b) + (f(a), -i(a)) + R = (a' + f(a), 0) + R = i'(a' + f(a)) \in \text{image}(i').$$

We conclude that the sequence f_*E is indeed short exact, so it gives an extension of C by A'.

(b) Now suppose we have a commutative diagram as indicated. Define $g''\colon A' \oplus B \to B^*$ by $g''(a', b) = i^*(a') + g(b)$. We then have $g''(f(a), -i(a)) = (i^*f - gi)(a) = 0$, so $g''(R) = 0$, so there is a unique homomorphism $g'\colon B' \to B^*$ given by $g'(x + R) = g''(x)$. This means that $g'i'(a) = g'((a', 0) + R) = g''(a', 0) = i^*(a')$, so $g'i' = i^*$. We also have

$$p^*g'((a', b) + R) = p^*i^*(a') + p^*g(b) = 0 + p(b) = p(b),$$

so $p^*g' = p$. Thus, g' gives the required equivalence from f_*E to E^*.

(c) By the construction in part (a), we have a commutative diagram

$$\begin{tikzcd} A \arrow[r, tail, "i"] \arrow[d, "f"'] & B \arrow[r, two heads, "p"] \arrow[d, "g"'] & C \arrow[d, equal] \\ A' \arrow[r, tail, "i'"'] & B' \arrow[r, two heads, "p'"'] & C \end{tikzcd}$$

(where $g(b) = (0, b) + R$). It follows easily that there is also a commutative diagram

$$\begin{tikzcd} A \arrow[r, tail, "i"] \arrow[d, "f+ni"'] & B \arrow[r, two heads, "p"] \arrow[d, "g+i'n"'] & C \arrow[d, equal] \\ A' \arrow[r, tail, "i'"'] & B' \arrow[r, two heads, "p'"'] & C \end{tikzcd}$$

Now part (b) tells us that the bottom row is equivalent to $(f + ni)_*$ of the top row, or in other words $f_*E \simeq (f + ni)_*E$ as claimed.

(d) Suppose we have equivalent extensions $E_k = (A \xrightarrow{i_k} B_k \xrightarrow{p_k} C)$ for $k = 0, 1$, so there is an isomorphism $s \colon B_0 \to B_1$ with $si_0 = i_1$ and $p_1 s = p_0$. We can then define $s' \colon B'_0 \to B'_1$ by

$$s'((a', b_0) + R_0) = (a', s(b_0)) + R_1.$$

We find that $s' i'_0 = i'_1$ and $p'_1 s' = p'_0$; this shows that $h^* E_0$ and $h^* E_1$ are equivalent as claimed.

□

Proposition 8.31. *Let A and C be abelian groups, and let $\mathrm{Ext}'(C, A)$ denote the set of equivalence classes of extensions of C by A. Let Q denote the extension $(I_C^2 \xrightarrow{j} I_C \xrightarrow{q} C)$. Then there is a well-defined bijection*

$$\zeta \colon \mathrm{Ext}(C, A) = \frac{\mathrm{Hom}(I_C^2, A)}{j^*(\mathrm{Hom}(I_C, A))} \to \mathrm{Ext}'(C, A)$$

given by $\zeta(\alpha + \mathrm{image}(j^*)) = [\alpha_*(Q)]$.

Proof. Using Proposition 8.30 (especially part (c)) we see that there is a well-defined map ζ as described. We must show that it is a bijection. Consider an arbitrary extension $E = (A \xrightarrow{i} B \xrightarrow{p} C)$. As I_C is free and p is surjective, Lemma 8.4 gives us a homomorphism $\beta \colon I_C \to B$ with $p\beta = q$. This means that $p\beta j = qj = 0$, so $\mathrm{image}(\beta j) \leq \ker(p) = \mathrm{image}(i)$, so there is a unique map $\alpha \colon I_C^2 \to A$ with $i\alpha = \beta j$. We now have a commutative diagram

$$\begin{tikzcd}
I_C^2 \arrow[r, tail, "j"] \arrow[d, "\alpha"'] & I_C \arrow[r, two heads, "q"] \arrow[d, "\beta"'] & C \arrow[d, equal] \\
A \arrow[r, tail, "i"'] & B \arrow[r, two heads, "p"'] & C,
\end{tikzcd}$$

so Proposition 8.30(b) tells us that $E \simeq \alpha_* Q$, or in other words $[E] = \zeta(\alpha + \mathrm{image}(j^*))$. This proves that ζ is surjective. Suppose we also have $[E] = \zeta(\alpha' + \mathrm{image}(j^*))$. There is then another commutative diagram

$$\begin{tikzcd}
I_C^2 \arrow[r, tail, "j"] \arrow[d, "\alpha'"'] & I_C \arrow[r, two heads, "q"] \arrow[d, "\beta'"'] & C \arrow[d, equal] \\
A \arrow[r, tail, "i"'] & B \arrow[r, two heads, "p"'] & C.
\end{tikzcd}$$

In particular we have $p\beta' = q = p\beta$ so $p(\beta' - \beta) = 0$, so $\beta' - \beta$ factors through $\ker(p) = \mathrm{image}(i)$, so there is a unique homomorphism $\gamma \colon I_C \to A$ with $\beta' = \beta + i\gamma$. Now $\beta' j = i\alpha'$ and $\beta j = i\alpha$ so the equation $\beta' = \beta + i\gamma$ yields $i\alpha' = i\alpha + i\gamma j$, or $i(\alpha' - \alpha - \gamma j) = 0$. As i is injective we conclude that $\alpha' = \alpha + j^*(\gamma)$, so α' and α have the same image in $\mathrm{cok}(j^*) = \mathrm{Ext}(C, A)$. This proves that ζ is also injective. □

The above proposition gives a bijection from the group $\mathrm{Ext}(C, A)$ to the set $\mathrm{Ext}'(C, A)$. There is thus a unique group structure on $\mathrm{Ext}'(C, A)$ for which this bijection is a homomorphism. We would like to understand this more intrinsically.

Definition 8.32. Suppose we have two extensions $E_k = (A \xrightarrow{i_k} B_k \xrightarrow{p_k} C)$ for $k = 0, 1$. The *Baer sum* of E_0 and E_1 is the sequence $E_2 = (A \xrightarrow{i_2} B_2 \xrightarrow{p_2} C)$ where

$$\begin{aligned}
U &= \{(b_0, b_1) \in B_0 \oplus B_1 \mid p_0(b_0) = p_1(b_1)\} \\
V &= \{(i_0(a), -i_1(a)) \mid a \in A\} \\
B_2 &= U/V \\
i_2(a) &= (i_0(a), 0) + V = (0, i_1(a)) + V \\
p_2((b_0, b_1) + V) &= p_0(b_0) = p_1(b_1).
\end{aligned}$$

Proposition 8.33. *In the above context, the sequence E_2 is an extension of C by A, with $[E_2] = [E_0] + [E_1]$ in $\mathrm{Ext}'(C, A)$. Moreover, the zero element in $\mathrm{Ext}'(C, A)$ is the equivalence class consisting of all split extensions.*

Proof. First, if $i_2(a) = 0$ we must have $(i_0(a), 0) \in V$, so $(i_0(a), 0) = (i_0(a'), -i_1(a'))$ for some $a' \in A$. As i_1 is injective and $i_1(a') = 0$ we have $a' = 0$, so the equation $i_0(a) = i_0(a')$ gives $i_0(a) = 0$ and then $a = 0$. This shows that i_2 is injective. Next, suppose we have $c \in C$. As both p_0 and p_1 are surjective we can choose $b_0 \in B_0$ and $b_1 \in B_1$ with $p_0(b_0) = p_1(b_1) = c$. The element $b_2 = (b_0, b_1) + V \in B_2$ then satisfies $p_2(b_2) = c$, so p_2 is surjective. Next, as $p_0 i_0 = 0 = p_1 i_1$ we see from the definitions that $p_2 i_2 = 0$, so $\mathrm{image}(i_2) \leq \ker(p_2)$. Now suppose we have an element $b_2 = (b_0, b_1) + V \in B_2$ with $p_2(b_2) = 0$. This means that $p_0(b_0) = 0 = p_1(b_1)$, so there is a unique element $a_0 \in A$ with $b_0 = i_0(a_0)$, and also a unique element $a_1 \in A$ with $b_1 = i_1(a_1)$. Put $a_2 = a_0 + a_1$ and note that

$$i_2(a_2) = i_2(a_0) + i_2(a_1) = (i_0(a_0), 0) + (0, i_1(a_1)) + V = (b_0, b_1) + V = b_2.$$

This proves that $\ker(p_2) = \mathrm{image}(i_2)$, so we have an extension as claimed. Now suppose that $[E_k] = \zeta(\alpha_k + \mathrm{image}(j^*))$ for $k = 0, 1$, so there are commutative diagrams

$$\begin{tikzcd}
I_C^2 \arrow[r, tail, "j"] \arrow[d, "\alpha_k"'] & I_C \arrow[r, two heads, "q"] \arrow[d, "\beta_k"'] & C \arrow[d, equal] \\
A \arrow[r, tail, "i_k"'] & B_k \arrow[r, two heads, "p_k"'] & C
\end{tikzcd}$$

for $k = 0, 1$. We define $\alpha_2 \colon I_C^2 \to A$ by $\alpha_2(y) = \alpha_0(y) + \alpha_1(y)$, and we define $\beta_2 \colon I_C \to B_2$ by $\beta_2(x) = (\beta_0(x), \beta_1(x)) + V$. It is straightforward to check that this gives a commutative diagrams as above, showing that

$$[E_2] = \zeta(\alpha_2 + \mathrm{image}(j^*)) = \zeta(\alpha_0 + \mathrm{image}(j^*)) + \zeta(\alpha_1 + \mathrm{image}(j^*)) = [E_0] + [E_1].$$

Thus, the sum in $\mathrm{Ext}'(C, A)$ is the Baer sum, as claimed. The zero element is $\zeta(0)$, which is the pushout of the extension $Q = (I_C^2 \xrightarrow{j} I_C \xrightarrow{q} C)$ along the map $0 \colon I_C^2 \to A$. If we use the notation of Proposition 8.30 in this context we have

$$\begin{aligned}
R &= \{(0, -j(y)) \mid y \in I_C^2\} = 0 \oplus I_C^2 \leq A \oplus I_C \\
B' &= \frac{A \oplus I_C}{R} = \frac{A \oplus I_C}{0 \oplus I_C^2} = A \oplus (I_C / I_C^2) \simeq A \oplus C \\
i'(a) &= (a, 0) \\
p'(a, c) &= c.
\end{aligned}$$

Thus, $0_* Q$ is just the obvious split extension of C by A. □

We now present a result that will help us relate homology groups to cohomology groups. There are very standard theorems that deduce information about cohomology from information about homology. To go in the opposite direction we need the following proposition, which is less well-known.

Proposition 8.34. *Suppose that* $\mathrm{Hom}(A, \mathbb{Z})$ *and* $\mathrm{Ext}(A, \mathbb{Z})$ *are finitely generated. Then A is finitely generated.*

The proof will follow after some lemmas.

Lemma 8.35. *Suppose that* $\mathrm{Hom}(A, \mathbb{Z})$ *is finitely generated. Then $A = B \oplus F$ for some subgroups B and F such that F is free and finitely generated, and* $\mathrm{Hom}(B, \mathbb{Z}) = 0$.

Proof. Choose maps $f_1, \ldots, f_r \colon A \to \mathbb{Z}$ that generate $\mathrm{Hom}(A, \mathbb{Z})$, and define $f \colon A \to \mathbb{Z}^r$ by $f(a) = (f_1(a), \ldots, f_r(a))$. Now $f(A)$ is a subgroup of $\mathbb{Z}^r$, so it is free, with basis $f(a_1), \ldots, f(a_s)$ say. Put $B = \ker(f)$, and let $F \leq A$ be the subgroup generated by $a_1, \ldots, a_s$. We find that $f \colon F \to f(A) \simeq \mathbb{Z}^s$ is an isomorphism, and thus that $A = B \oplus F$. Consider a homomorphism $g \colon B \to \mathbb{Z}$. Then the composite

$$A = B \oplus F \xrightarrow{\mathrm{proj}} B \xrightarrow{g} \mathbb{Z}$$

is an element of the group $\mathrm{Hom}(A, \mathbb{Z})$, which is generated by the maps f_i, but $f_i(B) = 0$, so we see that $g = 0$. This proves that $\mathrm{Hom}(B, \mathbb{Z}) = 0$. □

Lemma 8.36. *Suppose that* $\mathrm{Hom}(A, \mathbb{Z}) = \mathrm{Ext}(A, \mathbb{Z}) = 0$. *Then $A = 0$.*

Proof. Corollary 8.24 implies that $\mathrm{Ext}(\mathrm{tors}(A), \mathbb{Z}) = 0$, so Proposition 8.26 gives $\mathrm{tors}(A) = 0$, so A is torsion free. We thus have short exact sequences $A \xrightarrow{n} A \to A/n$ for all $n > 0$, and using the resulting six term sequences we deduce that $\mathrm{Ext}(A/n, \mathbb{Z}) = 0$. As A/n is torsion we can use Proposition 8.26 again to see that $A/n = 0$, so $n.1_A$ is surjective. It is also injective because $\mathrm{tors}(A) = 0$, so it is an isomorphism. We can thus make A into a vector space over $\mathbb{Q}$ by the rule $(m/n).a = (n.1_A)^{-1}(ma)$. Linear algebra therefore tells us that either A is zero, or it has $\mathbb{Q}$ as a summand. In the latter case $\mathrm{Ext}(A, \mathbb{Z})$ would contain the uncountable group $\mathrm{Ext}(\mathbb{Q}, \mathbb{Z})$ as a summand, which is impossible as $\mathrm{Ext}(A, \mathbb{Z}) = 0$. We therefore have $A = 0$ as claimed. $\square$

Proof of Proposition 8.34. Using Lemma 8.35 we reduce to the case where $\mathrm{Hom}(A, \mathbb{Z}) = 0$. We next claim that there are only finitely many primes p for which $A[p] \neq 0$. Indeed, for any such p we see (by linear algebra over the field $\mathbb{Z}/p$) that $\mathrm{Hom}(A[p], \mathbb{Z}/p) \neq 0$. If there are infinitely many such primes, we deduce that the group $P = \prod_p \mathrm{Hom}(A[p], \mathbb{Z}/p)$ is uncountable, which is impossible as Proposition 8.26 tells us that P is a quotient of the finitely generated group $\mathrm{Ext}(A, \mathbb{Z})$. We can thus choose p such that $A[p] = 0$, so we have a short exact sequence $A \xrightarrow{p} A \to A/p$. Proposition 8.23 then tells us that multiplication by p is surjective on $\mathrm{Ext}(A, \mathbb{Z})$. By the structure theory of finitely generated groups, we see that $\mathrm{Ext}(A, \mathbb{Z})$ must be finite, of order n say, and that n must be coprime to p.

Next we have short exact sequences $A[n] \xrightarrow{i} A \xrightarrow{f} nA$ and $nA \xrightarrow{j} A \xrightarrow{g} A/n$, where $f(a) = na$ and g is the quotient map. By assumption we have $\mathrm{Hom}(A, \mathbb{Z}) = 0$, and also $\mathrm{Hom}(A[n], \mathbb{Z}) = \mathrm{Hom}(A/n, \mathbb{Z}) = 0$ because $\mathbb{Z}$ is torsion free. From the six term sequences we find that $\mathrm{Hom}(nA, \mathbb{Z}) = 0$. We also find that $j^* \colon \mathrm{Ext}(A, \mathbb{Z}) \to \mathrm{Ext}(nA, \mathbb{Z})$ is surjective and $f^* \colon \mathrm{Ext}(nA, \mathbb{Z}) \to \mathrm{Ext}(A, \mathbb{Z})$ is injective, but the composite $f^* j^* = (jf)^*$ is just multiplication by n. As n was defined to be the order of $\mathrm{Ext}(A, \mathbb{Z})$ we deduce that $f^* j^* = 0$, which implies that $\mathrm{Ext}(nA, \mathbb{Z}) = 0$. Lemma 8.36 therefore tells us that $nA = 0$, so A is torsion and $\mathrm{Ext}(A, \mathbb{Z}) = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) = A^*$. This is finitely generated by assumption. Moreover, we have $nA = 0$ and therefore $nA^* = 0$, so A^* is a finite group. It follows that A^{**} is finite but Remark 8.19 gives an embedding $A \to A^{**}$ so A is finite, as required. $\square$

9. Localisation

Definition 9.1. A *multiplicative set* is a set S of positive integers that contains 1 and is closed under multiplication.

Definition 9.2. Let A be an abelian group, and let S be a multiplicative set. We introduce an equivalence relation on the set $A \times S$ by declaring that $(a, s) \sim (b, t)$ iff $bsx = atx$ for some $x \in S$. We write a/s for the equivalence class of the pair (a, s), and we write $A[S^{-1}]$ for the set of equivalence classes. We make this into an abelian group by the rule

$$a/s + b/t = (at + bs)/st.$$

Remark 9.3. Various checks are required to ensure that this definition is meaningful. First, we must show that the given relation really is an equivalence relation. It is clearly reflexive (as we can take $x = 1$) and symmetric. Suppose that $(a, s) \sim (b, t) \sim (c, u)$, so there are elements $x, y \in S$ with $atx = bsx$ and $buy = cty$. Put $z = txy \in S$ and note that

$$auz = (au)(txy) = (atx)(uy) = (bsx)(uy) = (buy)(sx) = (cty)(sx) = (cs)(txy) = csz,$$

so $(a, s) \sim (c, u)$, as required.

Next, we should check that addition is well-defined. More specifically, suppose that $(a_0, s_0) \sim (a_1, s_1)$ and $(b_0, t_0) \sim (b_1, t_1)$. Put $(c_k, u_k) = (a_k t_k + b_k s_k, s_k t_k)$; we must show that $(c_0, u_0) \sim (c_1, u_1)$. By hypothesis there are elements $x, y \in S$ such that $a_0 s_1 x = a_1 s_0 x$ and $b_0 t_1 y = b_1 t_0 y$. We multiply these two equations by $t_0 t_1 y$ and $s_0 s_1 x$ respectively, and then add them together to get

$$a_0 s_1 x t_0 t_1 y + b_0 t_1 y s_0 s_1 x = a_1 s_0 x t_0 t_1 y + b_1 t_0 y s_0 s_1 x,$$

or equivalently

$$(a_0 t_0 + b_0 s_0)(s_1 t_1) xy = (a_1 t_1 + b_1 s_1)(s_0 t_0) xy.$$

If we put $z = xy \in S$ this can be rewritten as $c_0 u_1 z = c_1 u_0 z$, so $(c_0, u_0) \sim (c_1, u_1)$ as required.

Finally, we should show that addition is commutative and associative, that the element $0/1$ is an additive identity, and that $(-a)/s$ is an additive inverse for a/s. All this is left to the reader.

Remark 9.4. From the definitions we see that $a/s = 0$ in $A[S^{-1}]$ if and only if there exists $t \in S$ with $at = 0$.

Remark 9.5. In the case $A = \mathbb{Z}$ it is not hard to see that $\mathbb{Z}[S^{-1}]$ can be identified with the set $\{n/s \in \mathbb{Q} \mid n \in \mathbb{Z},\ s \in S\}$, which is a subring of $\mathbb{Q}$.

Remark 9.6. Consider the case where A is finite, so A is the direct sum of its Sylow subgroups, say $A = A_1 \oplus \dots \oplus A_r$ with $|A_i| = p_i^{v_i}$ for some primes $p_1, \dots, p_r$ and integers $v_i > 0$. We then find that $A[S^{-1}] = \bigoplus_k A_k[S^{-1}]$. Suppose that there exists $n \in S$ that is divisible by p_k. In $A_k[S^{-1}]$ we then have $a/s = (an^{v_k})/(sn^{v_k}) = 0/(sn^{v_k}) = 0$, so $A_k[S^{-1}] = 0$. On the other hand, if there is no such n then for each $s \in S$ we see that $s.1_{A_k}$ is invertible for all $s \in S$, and using this we will see later that $A_k[S^{-1}] = A_k$. Thus, $A[S^{-1}]$ is just the direct sum of some subset of the Sylow subgroups.

Definition 9.7. We use different notation for the most popular cases, as follows:

(a) If $S = \{n^k \mid k \geq 0\}$ we write $A[n^{-1}]$ or $A[1/n]$ for $A[S^{-1}]$.
(b) If p is prime and $S = \{n > 0 \mid n \neq 0 \pmod{p}\} = \mathbb{N} \setminus p\mathbb{N}$ then we write $A_{(p)}$ for $A[S^{-1}]$. This is called the *p-localisation* of A.
(c) If $S = \{n \in \mathbb{N} \mid n > 0\}$ then we write $A\mathbb{Q}$ or $A_{(0)}$ for $A[S^{-1}]$. This is called the *rationalisation* of A.

Proposition 9.8. *Let S be a multiplicative set. Then any homomorphism $f\colon A \to B$ gives a homomorphism $f[S^{-1}]\colon A[S^{-1}] \to B[S^{-1}]$ by the rule $f[S^{-1}](a/s) = f(a)/s$. This construction gives an additive functor, and there is a natural map $\eta\colon A \to A[S^{-1}]$ given by $\eta(a) = a/1$.*

Proof. First, we see from the definitions that if $(a_0, s_0) \sim (a_1, s_1)$ then $(f(a_0), s_0) \sim (f(a_1), s_1)$. This shows that $f[S^{-1}]$ is well-defined. It also follows directly from the definitions that it is a homomorphism. Next, if we have maps $A \xrightarrow{f} B \xrightarrow{g} C$ then

$$(gf)[S^{-1}](a/s) = gf(a)/s = g[S^{-1}](f(a)/s) = g[S^{-1}](f[S^{-1}](a/s)),$$

which shows that our construction is functorial. We also claim that η is natural, which means that for any $f\colon A \to B$ the square

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\eta"'] & B \arrow[d, "\eta"] \\ A[S^{-1}] \arrow[r, "f[S^{-1}]"'] & B[S^{-1}] \end{tikzcd}$$

commutes. This is again straightforward. □

Remark 9.9. When there is no danger of confusion, we will just write f rather than $f[S^{-1}]$ for the induced map $A[S^{-1}] \to B[S^{-1}]$.

Proposition 9.10. *If $A \xrightarrow{f} B \xrightarrow{g} C$ is exact (or short exact), then so is the localised sequence*

$$A[S^{-1}] \xrightarrow{f[S^{-1}]} B[S^{-1}] \xrightarrow{g[S^{-1}]} C[S^{-1}].$$

Proof. First, as $gf = 0$ and localisation is functorial we see that $g[S^{-1}]f[S^{-1}] = (gf)[S^{-1}] = 0$, so $\mathrm{image}(f[S^{-1}]) \leq \ker(g[S^{-1}])$. Now consider an element $b/s \in \ker(g[S^{-1}])$. We then have $g(b)/s = 0/1$ in $B[S^{-1}]$, or equivalently $g(b)\,x = 0$ for some $x \in S$. This means that $g(xb) = 0$ so $xb \in \ker(g) = \mathrm{image}(f)$, so there exists $a \in A$ with $f(a) = xb$. This implies that $f[S^{-1}](a/(xs)) = f(a)/(xs) = xb/xs = b/s$, so $b/s \in \mathrm{image}(f[S^{-1}])$. We now see that the sequence $A[S^{-1}] \xrightarrow{f[S^{-1}]} B[S^{-1}] \xrightarrow{g[S^{-1}]} C[S^{-1}]$ is exact as claimed. Now suppose that the original sequence is short exact. It is equivalent to say that the sequences $0 \to A \to B$ and $A \to B \to C$ and $B \to C \to 0$ are all exact, and it follows from this that the sequences $0 \to A[S^{-1}] \to B[S^{-1}]$ and $A[S^{-1}] \to B[S^{-1}] \to C[S^{-1}]$ and $B[S^{-1}] \to C[S^{-1}] \to 0$ are also exact. We can then reassemble these pieces to see that the sequence $A[S^{-1}] \xrightarrow{f[S^{-1}]} B[S^{-1}] \xrightarrow{g[S^{-1}]} C[S^{-1}]$ is again short exact. □

Proposition 9.11. *There is a natural isomorphism $\mu\colon \mathbb{Z}[S^{-1}]\otimes A \to A[S^{-1}]$ given by $\mu((n/s)\otimes a) = (na)/s$.*

Proof. First, it is straightforward to check that there is a well-defined bilinear map $\mu_0\colon \mathbb{Z}[S^{-1}]\times A \to A[S^{-1}]$ given by $\mu_0(n/s, a) = (na)/s$. By the universal property of tensor products, this gives a homomorphism $\mu\colon \mathbb{Z}[S^{-1}] \otimes A \to A[S^{-1}]$ with $\mu((n/s) \otimes a) = (na)/s$. In the opposite direction, we would like to define $\nu\colon A[S^{-1}] \to \mathbb{Z}[S^{-1}] \otimes A$ by $\nu(a/s) = (1/s) \otimes a$. To see that this is well-defined, suppose that $a/s = b/t$, so $xta = xsb$ for some $x \in S$. From the definition of tensor products, we have $mu \otimes v = u \otimes mv$ in $U \otimes V$ for all $u \in U$, $v \in V$ and $m \in \mathbb{Z}$. We can apply this with $u = 1/(stx) \in \mathbb{Z}[S^{-1}]$ and $v = a$ and $m = tx$ to get $(1/s)\otimes a = (1/(stx))\otimes xta$. By a symmetrical argument, we have $(1/t)\otimes b = (1/(stx))\otimes xsb$, but $xta = xsb$ so we find that $(1/s) \otimes a = (1/t) \otimes b$, as required. It is clear that $\mu\nu = 1_{A[S^{-1}]}$. The other way around, we have

$$\nu\mu((n/s) \otimes a) = \nu((na)/s) = (1/s) \otimes na = (n/s) \otimes a.$$

Thus, ν is inverse to μ. □

Definition 9.12. Let S be a multiplicative set, and let A be an abelian group. We say that A is *S-torsion* if for all $a \in A$ there exists $s \in S$ with $sa = 0$. We say that A is *S-local* if for each $s \in S$, the endomorphism $s.1_A\colon A \to A$ is invertible.

Some care is needed in relating the above definition to the traditional terminology in the most popular cases:

Definition 9.13.

(a) Definition 4.1(c) is equivalent to the following: we say that A is a *torsion group* if it is S_0-torsion, where $S_0 = \{n \in \mathbb{N} \mid n > 0\}$.
(b) We say that A is *rational* if it is S_0-local. (We will see that in this case, A can be regarded as a vector space over $\mathbb{Q}$.)
(c) Now let p be a prime number. We say that A is *p-torsion* if it is $p^{\mathbb{N}}$-torsion, where $p^{\mathbb{N}} = \{p^n \mid n \in \mathbb{N}\}$.
(d) However, we say that A is *p-local* if it is S_p-local, where $S_p = \mathbb{N} \setminus p\mathbb{N}$.

Proposition 9.14.

(a) *The group $A[S^{-1}]$ is always S-local.*
(b) *The map $\eta\colon A \to A[S^{-1}]$ is an isomorphism if and only if A is S-local.*
(c) *If A is S-local then it can be regarded as a module over the ring $\mathbb{Z}[S^{-1}] \leq \mathbb{Q}$ by the rule $(n/s).a = (s.1_A)^{-1}(na)$.*
(d) *Suppose that $f\colon A \to B$ is a homomorphism, and that B is S-local. Then there is a unique homomorphism $f'\colon A[S^{-1}] \to B$ such that $f' \circ \eta = f\colon A \to B$.*

Proof.

(a) One can check that for each $s \in S$ there is a well-defined map $d_s\colon A[S^{-1}] \to A[S^{-1}]$ given by $d_s(a/t) = a/(st)$. This is inverse to $s.1_{A[S^{-1}]}$.
(b) If η is an isomorphism then it follows from (a) that A is S-local. Conversely, if A is S-local one can check that the formula $\zeta(a/s) = (s.1_A)^{-1}(a)$ gives a well-defined map $\zeta\colon A[S^{-1}] \to A$, and that this is inverse to η.
(c) First we must check that the multiplication rule is well-defined. Suppose that $n/s = m/t$, so $ntx = msx$ for some $x \in S$. As this is an equation in $\mathbb{Z}$ and $x > 0$ it reduces to $tn = ms$. If we write n_A for $n.1_A$ and so on, we deduce that $t_A n_A = m_A s_A\colon A \to A$. We can compose on the left by t_A^{-1} and on the right by s_A^{-1} to get $n_A s_A^{-1} = t_A^{-1} m_A$. As s_A^{-1} is a homomorphism, it commutes with multiplication by n, so $s_A^{-1} n_A = t_A^{-1} m_A$. This means that the definition of multiplication is consistent. We will leave it to the reader that it has the usual associativity and distributivity properties.
(d) We define $f'\colon A[S^{-1}] \to B$ by $f'(a/s) = (s.1_B)^{-1}(f(a))$. We leave it to the reader to show that this is well-defined and is a homomorphism. Note that $f'(a/1) = f(a)$, so $f'\eta = f$. If f'' is another homomorphism with $f''\eta = f$, we have

$$s_A(f''(a/s)) = s.f''(a/s) = f''(s.(a/s)) = f''(a/1) = f''(\eta(a)) = f(a).$$

As s_A is invertible we can rewrite this as $f''(a/s) = s_A^{-1}(f(a)) = f'(a/s)$. As a/s was arbitrary this means that $f'' = f'$, which gives that claimed uniqueness statement.

□

Remark 9.15. As a consequence of (b), we can identify $A[S^{-1}]$ with $A[S^{-1}][S^{-1}]$. There is a slight subtlety here: there are two apparently different isomorphisms $A[S^{-1}] \to A[S^{-1}][S^{-1}]$, and to keep everything straight it is necessary to prove that they are the same. Indeed, for any B, we have a map $\eta_B \colon B \to B[S^{-1}]$. We can specialise to the case $B = A[S^{-1}]$ to get a map $\eta_{A[S^{-1}]} \colon A[S^{-1}] \to A[S^{-1}][S^{-1}]$, given by $\eta_{A[S^{-1}]}(a/s) = (a/s)/1$. Alternatively, we can apply Proposition 9.8 to the map $\eta_A \colon A \to A[S^{-1}]$ to get another map $\eta_A[S^{-1}] \colon A[S^{-1}] \to A[S^{-1}][S^{-1}]$, given by $(\eta_A[S^{-1}])(a/s) = (a/1)/s$. It is clear that

$$s.\eta_{A[S^{-1}]}(a/s) = (a/1)/1 = s.(\eta_A[S^{-1}])(a/s),$$

and multiplication by s is an isomorphism on $A[S^{-1}][S^{-1}]$, so $\eta_{A[S^{-1}]} = \eta_A[S^{-1}]$.

Proposition 9.16. (a) *If we have a short exact sequence $A \to B \to C$ in which two of the three terms are S-local, then so is the third.*
(b) *Direct sums, products and retracts of S-local groups are S-local.*
(c) *The kernel, cokernel and image of any homomorphism between S-local groups are S-local.*
(d) *p-torsion groups are p-local.*

Proof.
(a) Note that U is S-local iff for each $n \in S$ we have $U[n] = 0$ and $U/n = 0$. Recall also that Proposition 7.20 gives exact sequences

$$0 \to A[n] \xrightarrow{j} B[n] \xrightarrow{q} C[n] \xrightarrow{\delta} A/n \xrightarrow{j} B/n \xrightarrow{q} C/n \to 0.$$

The claim follows by diagram chasing.
(b) This is clear, because direct sums, products and retracts of isomorphisms are isomorphisms.
(c) Let $f \colon A \to B$ be a homomorphism between S-local groups. Then $\mathrm{img}(f)$ is a subgroup of B so for $n \in S$ we have $\mathrm{img}(f)[n] \leq B[n] = 0$. Similarly, $\mathrm{img}(f)$ is a quotient of A so $\mathrm{img}(f)/n$ is a quotient of A/n and so is zero. It follows that $\mathrm{img}(f)$ is S-local. We can therefore apply (a) to the short exact sequences $\ker(f) \to A \xrightarrow{f} \mathrm{img}(f)$ and $\mathrm{img}(f) \to B \to \mathrm{cok}(f)$ to see that $\ker(f)$ and $\mathrm{cok}(f)$ are also S-local.
(d) Let A be a p-torsion group. Consider $m \in \mathbb{Z} \setminus p\mathbb{Z}$; we must show that $m.1_A$ is an isomorphism. For any $a \in A$ we can choose $k \geq 0$ such that $p^k a = 0$, and p^k is coprime with m so we can choose $r, s \in \mathbb{Z}$ with $p^k r + ms = 1$. It follows that $a = msa = (m.1_A)(sa)$. Using this we see that $m.1_A$ is surjective. Also, if $ma = 0$ then $a = sma = 0$, so $A[m] = 0$, so $m.1_A$ is also injective.

□

Proposition 9.17. *If A is a torsion group, then $A_{(0)} = 0$ and $A_{(p)} = \mathrm{tors}_p(A)$.*

Proof. First suppose that A is a p-torsion group, so $A = \bigcup_k A[p^k]$. If m is not divisible by p then we can find $n > 0$ with $mn = 1 \pmod{p^k}$, so $n.1_{A[p^k]}$ is inverse to $m.1_{A[p^k]}$. It follows that $m.1_A$ is also an isomorphism. This holds for all $m \in \mathbb{Z} \setminus p\mathbb{Z}$, so A is p-local, so $A = A_{(p)}$. Now suppose instead that A is a q-torsion group for some prime $q \neq p$. For any element $a \in A$ we have $q^v a = 0$ for some $v \geq 0$, so in $A_{(p)}$ we have $a/m = (q^v a)/(q^v m) = 0/(q^v m) = 0$. This shows that $A_{(p)} = 0$. Finally, for a general torsion group A we have $A = \bigoplus_q \mathrm{tors}_q(A)$ by Proposition 4.9, so $A_{(p)} = \bigoplus_q \mathrm{tors}_q(A)_{(p)}$. By the special cases that we have just discussed, this sum contains only the single factor $\mathrm{tors}_p(A)_{(p)} = \mathrm{tors}_p(A)$, as claimed. It is also clear from Remark 9.4 that $A_{(0)} = 0$. □

10. Colimits of sequences

Definition 10.1. By a *sequence* we mean a diagram of the form

$$A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \xrightarrow{f_3} \cdots .$$

Given such a sequence and natural numbers $i \leq j$, we write f_{ij} for the composite

$$A_i \xrightarrow{f_i} A_{i+1} \to \cdots \xrightarrow{f_{j-1}} A_j.$$

In particular, f_{ii} is the identity map of A_i, and $f_{i,i+1} = f_i$.

Definition 10.2. Given such a sequence, we consider the group $A_+ = \bigoplus_i A_i$. For each k we have an inclusion $\iota_k \colon A_k \to A_+$ and also a homomorphism $\iota_{k+1} \circ f_k \colon A_k \to A_+$. We let R_k denote the image of $(\iota_k - \iota_{k+1} f_k) \colon A_k \to A_+$, and put $R_+ = \sum_k R_k \leq A_+$ and $\varinjlim_i A_i = A_+/R_+$. This group is called the *colimit* of the sequence.

Next, we write $\bar{\iota}_k$ for the composite

$$A_k \xrightarrow{\iota_k} A_+ \to A_+/R_+ = \varinjlim_i A_i.$$

By construction we have $\bar{\iota}_k = \bar{\iota}_{k+1} f_k$, so the following diagram commutes:

$$\begin{tikzcd}
A_0 \arrow[r, "f_0"] \arrow[d, "\bar{\iota}_0"'] & A_1 \arrow[r, "f_1"] \arrow[d, "\bar{\iota}_1"'] & A_2 \arrow[r, "f_2"] \arrow[d, "\bar{\iota}_2"'] & A_3 \arrow[r, "f_3"] \arrow[d, "\bar{\iota}_3"'] & \cdots \\
\varinjlim_i A_i \arrow[r, equal] & \varinjlim_i A_i \arrow[r, equal] & \varinjlim_i A_i \arrow[r, equal] & \varinjlim_i A_i \arrow[r, equal] & \cdots
\end{tikzcd}$$

This implies that $\bar{\iota}_k = \bar{\iota}_m f_{k,m}$ whenever $k \leq m$.

Remark 10.3. The definition can be reformulated slightly as follows. We can define an endomorphism S of A_+ by

$$S(a_0, a_1, a_2, a_3, \dots) = (0, f_0(a_0), f_1(a_1), f_2(a_2), f_3(a_3), \cdots).$$

Equivalently, S is the unique map such that the following diagram commutes for all k:

$$\begin{tikzcd}
A_k \arrow[r, "f_k"] \arrow[d, tail, "\iota_k"'] & A_{k+1} \arrow[d, "\iota_{k+1}"] \\
A_+ \arrow[r, "S"'] & A_+
\end{tikzcd}$$

We can then say that $\varinjlim_i A_i$ is the cokernel of $1 - S \colon A_+ \to A_+$. Note that if a_i is the first nonzero entry in a then the i'th entry in $(1 - S)(a)$ is again a_i, so $(1 - S)(a) \neq 0$. This shows that $1 - S$ is injective, so we actually have a short exact sequence

$$A_+ \xrightarrow{1-S} A_+ \twoheadrightarrow \varinjlim_i A_i.$$

Remark 10.4. The colimit can also be characterised by a universal property, as follows. A *cone* for the sequence is a group B with a collection of maps $u_k \colon A_k \to B$ such that $u_{k+1} f_k = u_k$ for all $k \geq 0$. By construction, the maps $\bar{\iota}_k \colon A_k \to \varinjlim_i A_i$ form a cone. We claim that for any cone $\{A_k \xrightarrow{u_k} B\}_{k \in \mathbb{N}}$ there is a unique homomorphism $u_\infty \colon \varinjlim_i A_i \to B$ such that $u_\infty \bar{\iota}_k = u_k$ for all k. Indeed, Proposition 3.7 gives us a unique map $v \colon A_+ \to B$ with $v i_k = u_k$ for all k, and the cone property tells us that $v(R_k) = 0$ for all k, so $v(R_+) = 0$, so v induces a map $u_\infty \colon \varinjlim_i A_i = A_+/R_+ \to B$. This is easily seen to be the unique map such that $u_\infty \bar{\iota}_k = u_k$ for all k.

In many cases colimits are just unions, as we now explain.

Proposition 10.5. *We have*

$$\bar{\iota}_0(A_0) \leq \bar{\iota}_1(A_1) \leq \bar{\iota}_2(A_2) \leq \cdots \leq \varinjlim_i A_i.$$

Moreover, $\varinjlim_i A_i$ is the union of the groups $\bar{\iota}_k(A_k)$, and we have $\bar{\iota}_k(a) = 0$ iff $f_{k,m}(a) = 0$ for some $m \geq k$.

Proof. First, when $k \leq m$ we have $\bar{\imath}_k = \bar{\imath}_m f_{k,m}$, and this implies that $\bar{\imath}_k(A_k) \leq \bar{\imath}_m(A_m)$. Next, as $\varinjlim_i A_i$ is a quotient of A_+, we see that every element $a \in \varinjlim_i A_i$ can be written as $a = \sum_{k=0}^N \bar{\imath}_k(a_k)$ for some $N \geq 0$ and $a_k \in A_k$. Now $\bar{\imath}_k(a_k) \in \bar{\imath}_k(A_k) \leq \bar{\imath}_N(A_N)$ for all k, so $a \in \bar{\imath}_N(A_N)$. Thus $\varinjlim_i A_i = \bigcup_N \bar{\imath}_N(A_N)$ as claimed. Now suppose we have $a \in A_k$ and that $f_{km}(a) = 0$ for some $m \geq k$. Using $\bar{\imath}_k = \bar{\imath}_m f_{km}$ we deduce that $\bar{\imath}_k(a) = 0$. Conversely, suppose that $\bar{\imath}_k(a) = 0$, so $i_k(a) \in R_+$, so

$$i_k(a) = \sum_{m=0}^{N-1} (i_m(b_m) - i_{m+1}(f_m(b_m)))$$

for some $N > k$ and some $b_0, \ldots, b_{N-1}$ with $b_i \in A_i$. Now let $h\colon \bigoplus_{m=0}^N A_m \to A_N$ be the map given by f_{mN} on A_m, or more formally the unique map with $hi_m = f_{mN}$. We note that

$$h(i_m(b_m) - i_{m+1}(f_m(b_m))) = f_{m,N}(b_m) - f_{m+1,N}(f_m(b_m)) = 0,$$

so we can apply h to the above equation for $i_k(a)$ to get $f_{kN}(a) = 0$ as required. $\square$

Corollary 10.6. *Suppose we have a sequence $\{A_i\}_{i\in\mathbb{N}}$ and a cone $\{u_i\colon A_i \to B\}_{i\in\mathbb{N}}$ giving rise to a homomorphism $u_\infty\colon \varinjlim_i A_i \to B$. Then*

(a) *The image of u_∞ is the union of the subgroups $u_k(A_k)$.*
(b) *The map u_∞ is injective iff whenever $u_k(a) = 0$, there exists $m \geq k$ with $f_{km}(a) = 0$.*

Proof. This is clear from the Proposition. $\square$

Example 10.7. Let A be any abelian group. Suppose we have a chain of subgroups

$$A_0 \leq A_1 \leq A_2 \leq A_3 \leq \cdots \leq A.$$

Let $f_k\colon A_k \to A_{k+1}$ be the inclusion. Then the colimit of the resulting sequence is just $\bigcup_i A_i$. Indeed, the inclusions $A_n \to \bigcup_i A_i$ form a cone, which clearly has both the properties in Corollary 10.6.

The following examples are instructive as well as useful.

Proposition 10.8. *Let A be an arbitrary abelian group. Then the colimit of the sequence*

$$A \xrightarrow{n} A \xrightarrow{n} A \xrightarrow{n} A \xrightarrow{n} A \to \cdots$$

is $A[1/n]$, whereas the colimit of the sequence

$$A \xrightarrow{1} A \xrightarrow{2} A \xrightarrow{3} A \xrightarrow{4} A \to \cdots$$

is the rationalisation $A_{(0)}$.

Proof. We will prove the second statement; the first is similar but easier. Let C denote the colimit, so we have maps $\bar{\imath}_k\colon A \to C$ with $\bar{\imath}_k(a) = (k+1)\bar{\imath}_{k+1}(a)$. Define $u_n\colon A \to A_{(0)}$ by $u_n(a) = a/n!$. As $((n+1)a)/(n+1)! = a/n!$ we see that these maps form a cone, so there is a unique map $u_\infty\colon C \to A_{(0)}$ with $u_\infty \bar{\imath}_k = u_k$ for all k. Any element $a \in A_{(0)}$ can be written as $a = a'/n$ for some $a' \in A$ and $n > 0$, so $a = ((n-1)!a')/n! = u_n((n-1)!a')$, so $A_{(0)}$ is the union of the images of the maps u_n. Now suppose that $u_n(a') = 0$. By the definition of $A_{(0)}$ this just means that $ma' = 0$ for some $m > 0$. The map $f_{n,n+m}$ in our sequence is multiplication by the integer

$$p = (n+1)(n+2)\cdots(n+m) = \frac{(n+m)!}{n!} = m! \binom{n+m}{n},$$

which is divisible by m, so $f_{n,n+m}(a') = 0$. The claim follows by Corollary 10.6. $\square$

Proposition 10.9. *Suppose we have a commutative diagram as shown*

$$\begin{tikzcd}
A_0 \arrow[r, "f_0"] \arrow[d, "p_0"'] & A_1 \arrow[r, "f_1"] \arrow[d, "p_1"'] & A_2 \arrow[r, "f_2"] \arrow[d, "p_2"'] & A_3 \arrow[r, "f_3"] \arrow[d, "p_3"'] & \cdots \\
B_0 \arrow[r, "g_0"'] & B_1 \arrow[r, "g_1"'] & B_2 \arrow[r, "g_2"'] & B_3 \arrow[r, "g_3"'] & \cdots
\end{tikzcd}$$

Let $\bar{\imath}_k$ be the canonical map $A_k \to \varinjlim_i A_i$, and let $\bar{\jmath}_k$ be the canonical map $B_k \to \varinjlim_i B_i$. Then there is a unique map p_∞ such that the diagram

$$\begin{tikzcd} A_k \arrow[r, "\bar{\imath}_k"] \arrow[d, "p_k"'] & \varinjlim_i A_i \arrow[d, "p_\infty"] \\ B_k \arrow[r, "\bar{\jmath}_k"'] & \varinjlim_i B_i \end{tikzcd}$$

commutes for all k. Moreover, if all the maps p_k are injective, or surjective, or bijective, then p_∞ has the same property.

Proof. The maps $\bar{\jmath}_k p_k \colon A_k \to \varinjlim_i B_i$ satisfy

$$\bar{\jmath}_k p_k = \bar{\jmath}_{k+1} g_k p_k = \bar{\jmath}_{k+1} p_{k+1} f_k,$$

so they form a cone for the sequence $\{A_i\}$. There is thus a unique map $p_\infty \colon \varinjlim_i A_i \to \varinjlim_i B_i$ with $p_\infty \bar{\imath}_k = \bar{\jmath}_k p_k$ for all k, as claimed.

(a) Now suppose that all the maps p_k are injective. Consider an element $a \in \ker(p_\infty)$. By Proposition 10.5 we have $a = \bar{\imath}_k(a')$ for some k and some $a' \in A_k$. We then have $\bar{\jmath}_k(p_k(a')) = p_\infty(\bar{\imath}_k(a')) = p_\infty(a) = 0$. The same proposition therefore tells us that $g_{km}(p_k(a')) = 0$ for some $m \geq k$. Now $g_{km} p_k = p_m f_{km}$ and p_m is injective, so $f_{km}(a') = 0$. This means that $a = i_k(a') = i_m(f_{km}(a')) = 0$. Thus, p_∞ is injective as claimed.

(b) Suppose instead that all the maps p_k are surjective. Consider an element $b \in \varinjlim_i B_i$. By Proposition 10.5 we have $b = \bar{\jmath}_k(b')$ for some k and some $b' \in B_k$. As p_k is surjective, we can choose $a' \in A_k$ with $p_k(a') = b'$, and then put $b = \bar{\imath}_k(a)$; we find that $p_\infty(a) = b$. Thus, p_∞ is also surjective.

(c) If the maps p_k are all isomorphisms, then (a) and (b) together imply that p_∞ is an isomorphism.

□

Proposition 10.10. *Suppose we have a commutative diagram as shown, in which all the columns are exact:*

$$\begin{tikzcd} A_0 \arrow[r, "f_0"] \arrow[d, "p_0"'] & A_1 \arrow[r, "f_1"] \arrow[d, "p_1"'] & A_2 \arrow[r, "f_2"] \arrow[d, "p_2"'] & A_3 \arrow[r, "f_3"] \arrow[d, "p_3"'] & \cdots \\ B_0 \arrow[r, "g_0"'] \arrow[d, "q_0"'] & B_1 \arrow[r, "g_1"'] \arrow[d, "q_1"'] & B_2 \arrow[r, "g_2"'] \arrow[d, "q_2"'] & B_3 \arrow[r, "g_3"'] \arrow[d, "q_3"'] & \cdots \\ C_0 \arrow[r, "h_0"'] & C_1 \arrow[r, "h_1"'] & C_2 \arrow[r, "h_2"'] & C_3 \arrow[r, "h_3"'] & \cdots \end{tikzcd}$$

Then the resulting sequence

$$\varinjlim_i A_i \xrightarrow{p_\infty} \varinjlim_i B_i \xrightarrow{q_\infty} \varinjlim_i C_i$$

is also exact.

Proof. First, any element $a \in \varinjlim_i A_i$ has the form $a = \bar{\imath}_n(a')$ for some n and a'. We can then chase a' around the diagram

$$\begin{tikzcd} A_n \arrow[r, "\bar{\imath}_n"] \arrow[d, "p_n"'] & \varinjlim_i A_i \arrow[d, "p_\infty"] \\ B_n \arrow[r, "\bar{\jmath}_n"] \arrow[d, "q_n"'] & \varinjlim_i A_i \arrow[d, "q_\infty"] \\ C_n \arrow[r, "\bar{k}_n"] & \varinjlim_i A_i \end{tikzcd}$$

to see that $q_\infty(p_\infty(a)) = 0$. Conversely, suppose we have an element $b \in \ker(q_\infty)$. We then have $b = \bar\jmath_n(b')$ for some n and some $b' \in B_n$. We then have $\overline{k}_n(q_n(b')) = q_\infty(\bar\jmath_n(b')) = q_\infty(b) = 0$, so $h_{n,m}(q_n(b')) = 0$ for some $m \geq n$. Now $h_{n,m}(q_n(b')) = q_m(g_{n,m}(b'))$, so $g_{n,m}(b') \in \ker(q_m) = \operatorname{image}(p_m)$, so we can find $a' \in A_m$ with $p_m(a') = g_{n,m}(b')$. Now put $a = \bar\imath_m(a')$. We find that

$$p_\infty(a) = \bar\jmath_m(p_m(a')) = \bar\jmath_m(g_{n,m}(b')) = \bar\jmath_n(b') = b,$$

so $b \in \operatorname{image}(p_\infty)$. The claim follows. □

Proposition 10.11. *Suppose we have a sequence*

$$A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \xrightarrow{f_3} \cdots$$

and a nondecreasing function $u\colon \mathbb{N} \to \mathbb{N}$ such that $u(i) \to \infty$ as $i \to \infty$. Put

$$g_i = f_{u(i),u(i+1)} = (A_{u(i)} \xrightarrow{f_{u(i)}} A_{u(i)+1} \xrightarrow{f_{u(i)+1}} \cdots \xrightarrow{f_{u(i+1)-1}} A_{u(i+1)}),$$

so we have a sequence

$$A_{u(0)} \xrightarrow{g_0} A_{u(1)} \xrightarrow{g_1} A_{u(2)} \xrightarrow{g_2} A_{u(3)} \xrightarrow{g_3} \cdots$$

Then there is a canonical isomorphism $\varinjlim_j A_{u(j)} = \varinjlim_i A_i$.

Proof. Let $\bar\imath_n\colon A_n \to \varinjlim_i A_i$ and $\bar\jmath_n\colon A_{u(n)} \to \varinjlim_j A_{u(j)}$ be the usual maps. As $\bar\imath_n = \bar\imath_{n+1} f_n$ for all n we find by induction that $\bar\imath_n = \bar\imath_m f_{n,m}$ for all $n \leq m$. By applying this to the pair $u(k) \leq u(k+1)$, we see that $\bar\imath_{u(k)} = \bar\imath_{u(k+1)} g_k$, so the maps $\bar\imath_{u(k)}$ form a cone for the sequence $\{A_{u(j)}\}_{j\in\mathbb{N}}$, so there is a unique map $p\colon \varinjlim_j A_{u(j)} \to \varinjlim_i A_i$ with $p\bar\jmath_k = \bar\imath_{u(k)}$ for all k. In the opposite direction, suppose we have $n \in \mathbb{N}$. As $u(j) \to \infty$ as $j \to \infty$, we can choose k such that $n \leq u(k)$, and form the composite

$$q_{nk} = (A_n \xrightarrow{f_{n,u(k)}} A_{u(k)} \xrightarrow{\bar\jmath_k} \varinjlim_j A_{u(j)}).$$

As $\bar\jmath_k = \bar\jmath_{k+1} g_k = \bar\jmath_{k+1} f_{u(k),u(k+1)}$ and $f_{u(k),u(k+1)} f_{n,u(k)} = f_{n,u(k+1)}$ we see that $q_{n,k} = q_{n,k+1}$. Thus q_{nk} is independent of k, so we can denote it by q_n. We also find that $q_n = q_{n+1} f_n$, so the maps q_n form a cone for the sequence $\{A_i\}_{i\in\mathbb{N}}$, so there is a unique map $q\colon \varinjlim_i A_i \to \varinjlim_j A_{u(j)}$ with $q\bar\imath_n = q_n$ for all n.

Now note that any element $a \in \varinjlim_i A_i$ has the form $a = \bar\imath_n(a')$ for some n and $a' \in A_n$. If we choose k with $u(k) \geq n$ we have

$$pq(a) = pq_n(a') = p\bar\jmath_k f_{n,u(k)}(a') = \bar\imath_{u(k)} f_{n,u(k)}(a') = \bar\imath_n(a') = a,$$

so pq is the identity. A similar argument shows that qp is the identity. □

Proposition 10.12. *Suppose we have a commutative diagram*

$$\begin{tikzcd}
A_{00} \arrow[r, "f_{00}"] \arrow[d, "g_{00}"'] & A_{01} \arrow[r, "f_{01}"] \arrow[d, "g_{01}"'] & A_{02} \arrow[r, "f_{02}"] \arrow[d, "g_{02}"'] & A_{03} \arrow[r, "f_{03}"] \arrow[d, "g_{03}"'] & \cdots \\
A_{10} \arrow[r, "f_{10}"] \arrow[d, "g_{10}"'] & A_{11} \arrow[r, "f_{11}"] \arrow[d, "g_{11}"'] & A_{12} \arrow[r, "f_{12}"] \arrow[d, "g_{12}"'] & A_{13} \arrow[r, "f_{13}"] \arrow[d, "g_{13}"'] & \cdots \\
A_{20} \arrow[r, "f_{20}"] \arrow[d, "g_{20}"'] & A_{21} \arrow[r, "f_{21}"] \arrow[d, "g_{21}"'] & A_{22} \arrow[r, "f_{22}"] \arrow[d, "g_{22}"'] & A_{23} \arrow[r, "f_{23}"] \arrow[d, "g_{23}"'] & \cdots \\
A_{30} \arrow[r, "f_{30}"] \arrow[d, "g_{30}"'] & A_{31} \arrow[r, "f_{31}"] \arrow[d, "g_{31}"'] & A_{32} \arrow[r, "f_{32}"] \arrow[d, "g_{32}"'] & A_{33} \arrow[r, "f_{33}"] \arrow[d, "g_{33}"'] & \cdots \\
\cdots & \cdots & \cdots & \cdots &
\end{tikzcd}$$

and thus sequences

$$\varinjlim_j A_{0j} \xrightarrow{g_{0\infty}} \varinjlim_j A_{1j} \xrightarrow{g_{1\infty}} \varinjlim_j A_{2j} \xrightarrow{g_{2\infty}} \varinjlim_j A_{3j} \xrightarrow{g_{3\infty}} \cdots$$

and

$$\varinjlim_i A_{i0} \xrightarrow{f_{\infty 0}} \varinjlim_i A_{i1} \xrightarrow{f_{\infty 1}} \varinjlim_i A_{i2} \xrightarrow{f_{\infty 2}} \varinjlim_i A_{i3} \xrightarrow{f_{\infty 3}} \cdots$$

Suppose we also put

$$h_i = g_{i,j+1} f_{ij} = f_{i+1,j} g_{ij} \colon A_{ii} \to A_{i+1,i+1},$$

giving a third sequence

$$A_{00} \xrightarrow{h_0} A_{11} \xrightarrow{h_1} A_{22} \xrightarrow{h_2} A_{33} \xrightarrow{h_3} \cdots$$

Then there are canonical isomorphisms

$$\varinjlim_i \varinjlim_j A_{ij} \simeq \varinjlim_i A_{ii} \simeq \varinjlim_j \varinjlim_i A_{ij}.$$

Example 10.13. In conjunction with Proposition 10.8, this will give

$$A[\frac{1}{n}][\frac{1}{m}] = A[\frac{1}{nm}] = A[\frac{1}{m}][\frac{1}{n}]$$

Proof. Put $A_{++} = \bigoplus_{n,m} A_{nm}$, and let $i_{nm} \colon A_{nm} \to A_{++}$ be the canonical inclusion. Put

$$P_{nm} = \text{image}(i_{nm} - i_{n,m+1} f_{nm} \colon A_{nm} \to A_{++})$$
$$Q_{nm} = \text{image}(i_{nm} - i_{n+1,m} g_{nm} \colon A_{nm} \to A_{++}).$$

From the definitions we have

$$\bigoplus_n \varinjlim_j A_{nj} = A_{++} / \sum_{n,m} P_{nm}$$
$$\bigoplus_m \varinjlim_i A_{im} = A_{++} / \sum_{n,m} Q_{nm}.$$

It follows easily that

$$\varinjlim_i \varinjlim_j A_{ij} = A_{++} / \left(\sum_{n,m} P_{nm} + \sum_{n,m} Q_{nm} \right) = \varinjlim_j \varinjlim_i A_{ij}.$$

We write $A_{\infty\infty}$ for this group, and we write $\bar{\imath}_{nm}$ for the obvious map $A_{nm} \to A_{\infty\infty}$. By construction, the following diagram commutes:

$$\begin{tikzcd} A_{nm} \arrow[r, "f_{nm}"] \arrow[d, "g_{nm}"'] \arrow[dr, "\bar{\imath}_{nm}"] & A_{n,m+1} \arrow[d, "\bar{\imath}_{n,m+1}"] \\ A_{n+1,m} \arrow[r, "\bar{\imath}_{n+1,m}"'] & A_{\infty\infty}. \end{tikzcd}$$

It follows that $\bar{\imath}_{kk} = \bar{\imath}_{k+1,k+1} h_k$, so the maps $\bar{\imath}_{kk}$ form a cone for the sequence $\{A_{ii}\}_{i \in \mathbb{N}}$. Thus, if we write $\bar{\jmath}_k$ for the usual map $A_{kk} \to \varinjlim_i A_{ii}$, we find that there is a unique map $p \colon \varinjlim_i A_{ii} \to A_{\infty\infty}$ with $p\bar{\jmath}_k = \bar{\imath}_{kk}$ for all k. In the opposite direction, suppose we have $n, m, k \in \mathbb{N}$ with $n, m \leq k$. By composing f's and g's in various orders we can form a number of maps $A_{nm} \to A_{kk}$ but they are all the same because the original diagram is commutative. We write u_{nmk} for this map, and put $q_{nmk} = \bar{\jmath}_k u_{nmk} \colon A_{nm} \to \varinjlim_i A_{ii}$. Now $\bar{\jmath}_k = \bar{\jmath}_{k+1} h_k$ and $h_k u_{nmk} = u_{n,m,k+1}$ so $q_{n,m,k} = q_{n,m,k+1}$. Thus q_{nmk} is independent of k (provided that $k \geq \max(n, m)$) so we can denote it by q_{nm}. We can now put the maps q_{nm} together to give a map $q' \colon A_{++} \to \varinjlim_i A_{ii}$ with $q' i_{nm} = q_{nm}$. When $k > \max(n, m)$ we have $u_{nmk} = u_{n,m+1,k} f_{nm} = u_{n+1,m,k} g_{nm}$, and using this we see that $q'(P_{nm}) = 0 = q'(Q_{nm})$. There is thus an induced map $A_{\infty\infty} \to \varinjlim_i A_{ii}$ with $q\bar{\imath}_{nm} = q_{nm}$. We leave it to the reader to check that q is inverse to p. $\square$

Definition 11.1. A *tower* is a diagram of the form

$$B_0 \xleftarrow{f_0} B_1 \xleftarrow{f_1} B_2 \xleftarrow{f_2} B_3 \xleftarrow{f_3} \cdots$$

Given such a tower an integers $i \geq j$, we write f_{ij} for the composite

$$B_i \xrightarrow{f_{i-1}} B_{i-1} \xrightarrow{f_{i-2}} \cdots \xrightarrow{f_j} B_j.$$

Note that f_{ii} is the identity map, and $f_{i+1,i} = f_i$, and $f_{jk}f_{ij} = f_{ik}$ whenever $i \geq j \geq k$.

Definition 11.2. Suppose we have a tower as above. The *limit* (or *inverse limit*) of the tower is the group

$$\varprojlim_i B_i = \{a \in \prod_i B_i \mid a_i = f_i(a_{i+1}) \text{ for all } i\}.$$

Equivalently, if we define $D\colon \prod_i B_i \to \prod_i B_i$ by $D(a)_i = a_i - f_i(a_{i+1})$, then $\varprojlim_i B_i = \ker(D)$. We also write $\varprojlim^1_i B_i$ for the cokernel of D. We define $p_n\colon \varprojlim_i B_i \to B_n$ by $p_n(a) = a_n$, so $p_n = f_n p_{n+1}$.

Remark 11.3. The limit can also be characterised by a universal property, as follows. A *cone* for the tower is a group A with a collection of maps $u_k\colon A \to B_k$ such that $u_k = f_k u_{k+1}$ for all k. Tautologically, the maps $p_k\colon \varprojlim_i B_i \to B_k$ form a cone. Moreover, for any cone $\{A \xrightarrow{u_k} B_k\}_{k\in\mathbb{N}}$ we can define $u_\infty\colon A \to \varprojlim_i B_i$ by

$$u_\infty(a) = (u_0(a), u_1(a), u_2(a), \dots),$$

and this is the unique map with $p_k u_\infty = u_k$ for all k.

Example 11.4. Suppose we have a chain of subgroups

$$B_0 \geq B_1 \geq B_2 \geq \cdots$$

and we take the maps f_i to be the inclusion maps. Then we see from the definitions that

$$\varprojlim_i B_i = \{(b, b, b, \cdots) \mid b \in \bigcap_i B_i\} \simeq \bigcap_i B_i.$$

Example 11.5. Suppose we have a system of groups C_i (for $i \in \mathbb{N}$). Put $B_k = \prod_{i=0}^k C_i$ and let $f_k\colon B_{k+1} \to B_k$ be the obvious projection map. If $b \in \varprojlim_k B_k$ then $b_k \in \prod_{i=0}^k C_i$ so $b_{kk} \in C_k$. We can thus define

$$d\colon \varprojlim_k B_k \to \prod_k C_k$$

by

$$d(b) = (b_{00}, b_{11}, b_{22}, \dots).$$

By the definition of $\varprojlim_k B_k$, we have $b_{kj} = b_{jj}$ for $j \leq k$. Using this, we see that d is an isomorphism.

Example 11.6. Suppose we have a tower in which the groups are arbitrary but the maps are all zero. Then the map D is the identity, so both $\varprojlim$ and $\varprojlim^1$ are zero.

Example 11.7. Suppose we have a sequence

$$A_0 \xrightarrow{f_0} A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \xrightarrow{f_3} \cdots,$$

and another group B. This gives us a tower

$$\mathrm{Hom}(A_0, B) \xleftarrow{f_0^*} \mathrm{Hom}(A_1, B) \xleftarrow{f_1^*} \mathrm{Hom}(A_2, B) \xleftarrow{f_2^*} \mathrm{Hom}(A_3, B) \xleftarrow{f_3^*} \cdots$$

The elements of $\varprojlim_i \mathrm{Hom}(A_i, B)$ are precisely the cones from the sequence $\{A_i\}_{i\in\mathbb{N}}$ to B, which biject with homomorphisms from $\varinjlim_i A_i$ to B. In other words, we have

$$\varprojlim_i \mathrm{Hom}(A_i, B) = \mathrm{Hom}(\varinjlim_i A_i, B).$$

Example 11.8. Fix a prime p. We then have a tower

$$\mathbb{Z}/p \leftarrow \mathbb{Z}/p^2 \leftarrow \mathbb{Z}/p^3 \leftarrow \mathbb{Z}/p^4 \leftarrow \cdots .$$

The inverse limit is called *the ring of p-adic integers*, and is denoted by $\mathbb{Z}_p$. We will investigate it in more detail in Section 12. We can also form a tower

$$\mathbb{Z}/0! \leftarrow \mathbb{Z}/1! \leftarrow \mathbb{Z}/2! \leftarrow \mathbb{Z}/3! \leftarrow \cdots$$

The inverse limit is called *the profinite completion of* $\mathbb{Z}$, and is denoted by $\widehat{\mathbb{Z}}$. Using the Chinese Remainder Theorem (Proposition 4.7) one can show that $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. For yet another description, recall that

$$\mathbb{Q}/\mathbb{Z} = \bigcup_n (\mathbb{Q}/\mathbb{Z})[n!] = \varinjlim_n (\mathbb{Q}/\mathbb{Z})[n!],$$

so

$$\mathrm{End}(\mathbb{Q}/\mathbb{Z}) = \varprojlim_n \mathrm{Hom}((\mathbb{Q}/\mathbb{Z})[n!], \mathbb{Q}/\mathbb{Z}).$$

Now we have a map $m\colon \mathbb{Z} \to \mathrm{End}(\mathbb{Q}/\mathbb{Z})$ defined by $m(k) = k.1_{\mathbb{Q}/\mathbb{Z}}$, and this fits in a commutative diagram

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "m"] \arrow[d, two heads] & \mathrm{End}(\mathbb{Q}/\mathbb{Z}) \arrow[d, "\text{restrict}"] \\
\mathbb{Z}/n! \arrow[r, "m_n"'] & \mathrm{Hom}((\mathbb{Q}/\mathbb{Z})[n!], \mathbb{Q}/\mathbb{Z}).
\end{tikzcd}$$

Using the fact that $(\mathbb{Q}/\mathbb{Z})[n!]$ is generated by $(1/n!) + \mathbb{Z}$ we see that m_n is an isomorphism. By passing to inverse limits, we obtain an isomorphism $m_\infty\colon \widehat{\mathbb{Z}} \to \mathrm{End}(\mathbb{Q}/\mathbb{Z})$.

Proposition 11.9. *Suppose we have a commutative diagram as shown*

$$\begin{tikzcd}
A_0 \arrow[d, "p_0"'] & A_1 \arrow[l, "f_0"'] \arrow[d, "p_1"'] & A_2 \arrow[l, "f_1"'] \arrow[d, "p_2"'] & A_3 \arrow[l, "f_2"'] \arrow[d, "p_3"'] & \cdots \arrow[l, "f_3"'] \\
B_0 & B_1 \arrow[l, "g_0"] & B_2 \arrow[l, "g_1"] & B_3 \arrow[l, "g_2"] & \cdots \arrow[l, "g_3"]
\end{tikzcd}$$

and we define $p = \prod_i p_i\colon \prod_i A_i \to \prod_i B_i$. Then the central square below commutes, so there are induced maps p_∞ and p^1_∞ as shown.

$$\begin{tikzcd}
\varprojlim_i A_i \arrow[r, tail] \arrow[d, "p_\infty"'] & \prod_i A_i \arrow[r, "D"] \arrow[d, "p"'] & \prod_i A_i \arrow[r, two heads] \arrow[d, "p"] & \varprojlim{}^1_i A_i \arrow[d, "p^1_\infty"] \\
\varprojlim_i B_i \arrow[r, tail] & \prod_i B_i \arrow[r, "D"'] & \prod_i B_i \arrow[r, two heads] & \varprojlim_i{}^1 B_i .
\end{tikzcd}$$

Proof. Clear from the definitions. $\square$

Proposition 11.10. *Suppose we have a commutative diagram as shown, in which all the columns are short exact:*

$$\begin{tikzcd}
A_0 \arrow[d, tail, "p_0"'] & A_1 \arrow[l, "f_0"'] \arrow[d, tail, "p_1"'] & A_2 \arrow[l, "f_1"'] \arrow[d, tail, "p_2"'] & A_3 \arrow[l, "f_2"'] \arrow[d, tail, "p_3"'] & \cdots \arrow[l, "f_3"'] \\
B_0 \arrow[d, two heads, "q_0"'] & B_1 \arrow[l, "g_0"'] \arrow[d, two heads, "q_1"'] & B_2 \arrow[l, "g_1"'] \arrow[d, two heads, "q_2"'] & B_3 \arrow[l, "g_2"'] \arrow[d, two heads, "q_3"'] & \cdots \arrow[l, "g_3"'] \\
C_0 & C_1 \arrow[l, "h_0"] & C_2 \arrow[l, "h_1"] & C_3 \arrow[l, "h_2"] & \cdots \arrow[l, "h_3"]
\end{tikzcd}$$

Then there is an associated exact sequence

$$\begin{tikzcd}
\varprojlim_i A_i \arrow[r, tail, "p_\infty"] & \varprojlim_i B_i \arrow[r, "q_\infty"] & \varprojlim_i C_i \arrow[r, "\delta"] & \varprojlim{}^1_i A_i \arrow[r, "p^1_\infty"] & \varprojlim{}^1_i B_i \arrow[r, two heads, "q^1_\infty"] & \varprojlim{}^1_i C_i
\end{tikzcd}$$

Proof. Apply the Snake Lemma to the diagram

$$\begin{array}{ccccc}
\prod_i A_i & \xrightarrow{\prod_i p_i} & \prod_i B_i & \xrightarrow{\prod_i q_i} & \prod_i C_i \\
\downarrow D & & \downarrow D & & \downarrow D \\
\prod_i A_i & \xrightarrow[\prod_i p_i]{} & \prod_i B_i & \xrightarrow[\prod_i q_i]{} & \prod_i C_i
\end{array}$$

in which the rows are easily seen to be short exact. ☐

In practice the groups $\varprojlim_i^1 A_i$ are usually either zero, or enormous and untractable. We will thus be very interested in results that force them to be zero.

Proposition 11.11. *Suppose we have a tower in which the maps $f_i\colon A_{i+1} \to A_i$ are all surjective. Then $\varprojlim_i^1 A_i = 0$, and the projection maps $p_k\colon \varprojlim_i A_i \to A_k$ are all surjective.*

Proof. Consider an element $a \in \prod_i A_i$. We will choose elements $b_k \in A_k$ recursively as follows: we start with $b_0 = 0$, and then take b_n to be any element with $f_{n-1}(b_n) = b_{n-1} - a_{n-1}$. These elements b_k give an element $b \in \prod_i A_i$ with $D(b) = a$, so D is surjective and $\varprojlim_i^1 A_i = \operatorname{cok}(D) = 0$.

Now suppose we have an element $a \in A_k$. Define $c_i = f_{k,i}(a)$ for all $i \leq k$. Then define $c_i \in A_i$ recursively for $i > k$ by choosing c_i to be any element with $f_{i-1}(c_i) = c_{i-1}$. This gives an element $c \in \varprojlim_i A_i$ with $p_k(c) = a$. ☐

Definition 11.12. We say that a tower $A_0 \xleftarrow{f_0} A_1 \xleftarrow{f_1} \cdots$ is *nilpotent* if for all i there exists $j > i$ such that $f_{ji} = 0\colon A_j \to A_i$.

Proposition 11.13. *For a nilpotent tower as above, we have $\varprojlim_i A_i = \varprojlim_i^1 A_i = 0$.*

Proof. Define $E\colon \prod_i A_i \to \prod_i A_i$ by

$$E(a)_i = \sum_{j=i}^{\infty} f_{j,i}(a_j).$$

Although the sum is formally infinite, the nilpotence hypothesis means that there are only finitely many nonzero terms, so the expression is meaningful. It is then not hard to check that $DE = ED = 1$, so the kernel and cokernel of D are zero. ☐

Definition 11.14. Consider a tower $A_0 \xleftarrow{f_0} A_1 \xleftarrow{f_1} \cdots$, so for each i we have a descending chain of subgroups

$$A_i \geq f_{i+1,i}(A_{i+1}) \geq f_{i+2,i}(A_{i+2}) \geq f_{i+3,i}(A_{i+3}) \geq \cdots$$

We say that the tower is *Mittag-Leffler* if for each i there exists $j \geq i$ such that $f_{ki}(A_k) = f_{ji}(A_j)$ for all $k \geq j$ (so the above chain is eventually constant).

Example 11.15. Towers of surjections are Mittag-Leffler, as are nilpotent towers.

Proposition 11.16. *If all the groups A_i are finite, then the tower is Mittag-Leffler. Similarly, if the groups A_i are finite-dimensional vector spaces over a field K, and the maps f_i are all K-linear, then the tower is Mittag-Leffler.*

Proof. In the first case, we just choose $j \geq i$ such that the order $|f_{ji}(A_j)|$ is as small as possible; it then follows that $f_{ki}(A_k) = f_{ji}(A_j)$ for $k \geq i$. In the second case, use dimensions instead of orders. ☐

Proposition 11.17. *If A is a Mittag-Leffler tower, we have $\varprojlim_i^1 A_i = 0$.*

Proof. By the Mittag-Leffler condition, there is a subgroup $A'_i \leq A_i$ such that $f_{ji}(A_j) = A'_i$ for all sufficiently large j. Thus, for j very large we have both $A'_{i+1} = f_{j,i+1}(A_j)$ and $A'_i = f_{ji}(A_j) = f_i(f_{j,i+1}(A_j)) = f_i(A'_{i+1})$. Thus, the groups A'_i form a subtower of A, with surjective maps $f'_i\colon A'_{i+1} \to A'_i$. Now put $A''_i = A_i/A'_i$, so there are induced maps $f''_i\colon A''_{i+1} \to A''_i$, giving a third tower. If j is much larger than i we have $f_{ji}(A_j) = A'_i$ and so $f''_{ji} = 0\colon A''_j \to A''_i$; this shows that the tower A'' is nilpotent. Now apply Proposition 11.10 to the short exact sequence $A' \to A \to A''$ to give an exact sequence

$$\varprojlim_i A'_i \rightarrowtail \varprojlim_i A_i \longrightarrow \varprojlim_i A''_i \xrightarrow{\delta} \varprojlim_i{}^1 A'_i \longrightarrow \varprojlim_i{}^1 A_i \longrightarrow\!\!\!\!\rightarrow \varprojlim_i{}^1 A''_i$$

Here $\varprojlim_i^1 A'_i = 0$ because the maps in A' are surjective, and $\varprojlim_i^1 A''_i = 0$ because A'' is nilpotent, so $\varprojlim_i^1 A_i = 0$ as claimed. (We also have $\varprojlim_i A''_i = 0$ and so $\varprojlim_i A'_i = \varprojlim_i A_i$.) ∎

We also have the following result analogous to Proposition 10.11, which again indicates that $\varprojlim_i A_i$ and $\varprojlim_i^1 A_i$ only depend on the asymptotic behaviour of the tower.

Proposition 11.18. *Suppose we have a tower*

$$A_0 \xleftarrow{f_0} A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3 \xleftarrow{f_3} \cdots$$

and a nondecreasing function $u\colon \mathbb{N} \to \mathbb{N}$ *such that* $u(i) \to \infty$ *as* $i \to \infty$*. Put*

$$g_i = f_{u(i+1),u(i)} = (A_{u(i+1)} \xrightarrow{f_{u(i+1)-1}} A_{u(i+1)-1} \cdots \xrightarrow{f_{u(i)}} A_{u(i)}),$$

so we have a tower

$$A_{u(0)} \xleftarrow{g_0} A_{u(1)} \xleftarrow{g_1} A_{u(2)} \xleftarrow{g_2} A_{u(3)} \xleftarrow{g_3} \cdots$$

Then there are canonical isomorphisms $\varprojlim_j A_{u(j)} = \varprojlim_i A_i$ *and* $\varprojlim_j^1 A_{u(j)} = \varprojlim_i^1 A_i$.

Proof. Define $v\colon \mathbb{N} \to \mathbb{N}$ by $v(i) = \min\{j \mid u(j) \geq i\}$. We will construct a diagram as follows:

$$\begin{array}{ccccc}
\prod_j A_{u(j)} & \xrightarrow{\phi} & \prod_i A_i & \xrightarrow{\psi} & \prod_j A_{u(j)} \\
{\scriptstyle D'}\downarrow & & {\scriptstyle D}\downarrow & & \downarrow{\scriptstyle D'} \\
\prod_j A_{u(j)} & \xrightarrow[\lambda]{} & \prod_i A_i & \xrightarrow[\mu]{} & \prod_j A_{u(j)}
\end{array}$$

The maps are:

$$\begin{aligned}
D'(b)_j &= b_j - f_{u(j+1),u(j)}(b_{j+1}) & \qquad D(a)_i &= a_i - f_{i+1,i}(a_{i+1}) \\
\phi(b)_i &= f_{uv(i),i}(b_{v(i)}) & \psi(a)_j &= a_{u(j)} \\
\lambda(b)_i &= \sum_{u(j)=i} b_j & \mu(a)_j &= \sum_{u(j)\leq i<u(j+1)} f_{i,u(j)}(a_i).
\end{aligned}$$

Thus D and D' are the usual maps whose kernels and cokernels are the $\varprojlim$ and $\varprojlim^1$ groups under consideration. We claim that the diagram commutes. To see this, consider a point $b \in \prod_j A_{u(j)}$. We then have

$$\begin{aligned}
D(\phi(b))_i &= \phi(b)_i - f_{i+1,i}(\phi(b)_{i+1}) \\
&= f_{uv(i),i}(b_{v(i)}) - f_{uv(i+1),i}(b_{v(i+1)}) \\
\lambda(D'(b))_i &= \sum_{u(j)=i} D'(b)_j = \sum_{u(j)=i} (b_j - f_{u(j+1),u(j)} b_{j+1}).
\end{aligned}$$

If $u^{-1}\{i\} = \emptyset$ we find that $v(i+1) = v(i)$ and so $D(\phi(b))_i = 0 = \lambda(D'(b))_i$. If $u^{-1}\{i\}$ is nonempty then it will be an interval, say $u^{-1}\{i\} = \{j_0, \ldots, j_1 - 1\}$. In our expression for $\lambda(D'(b))_i$, the map $f_{u(j+1),u(j)}$ is just the identity except when $j = j_1 - 1$. The expression therefore cancels down to $b_{j_0} - f_{u(j_1),i}(b_{j_1})$. On the other hand, we also find that $v(i) = j_0$ and $v(i+1) = j_1$, so

$$D(\phi(b))_i = f_{ii}(b_{j_0}) - f_{u(j_1),i}(b_{j_1}) = \lambda(D'(b))_i.$$

Thus, the left square commutes. For the right square, consider an element $a \in \prod_i A_i$. We have

$$\begin{aligned}
\mu(D(a))_j &= \sum_{u(j) \leq i < u(j+1)} f_{i,u(j)}(D(a)_i) \\
&= \sum_{u(j) \leq i < u(j+1)} (f_{i,u(j)}(a_i) - f_{i+1,u(j)}(a_{i+1})) \\
&= a_{u(j)} - f_{u(j+1),u(j)}(a_{u(j+1)}) \\
&= \psi(a)_j - f_{u(j+1),u(j)}(\psi(a)_{j+1}) = D'(\psi(a))_j
\end{aligned}$$

as required. We therefore have induced maps

$$\varprojlim_j A_{u(j)} \xrightarrow{\phi'} \varprojlim_i A_i \xrightarrow{\psi'} \varprojlim_j A_{u(j)}$$

and

$$\varprojlim_j{}^1 A_{u(j)} \xrightarrow{\lambda'} \varprojlim_i{}^1 A_i \xrightarrow{\mu'} \varprojlim_j{}^1 A_{u(j)}.$$

It is straightforward to check that $\phi'\psi'$ and $\psi'\phi'$ are the respective identity maps. Now define $\sigma \colon \prod_i A_i \to \prod_i A_i$ by

$$\sigma(a)_i = \sum_{i \leq h < uv(i)} f_{h,i}(a_h).$$

We claim that $\lambda\mu + D\sigma = 1$ (which implies that $\lambda'\mu' = 1$). The proof that $\lambda(\mu(a))_i + D(\sigma(a))_i = a_i$ splits into two cases, depending on whether $i \in \text{image}(u)$ or not. If $i \notin \text{image}(u)$ we find that the inequality $i \leq u(v(i))$ cannot be an equality, so $v(i+1) = v(i)$. Using this we deduce that $D(\sigma(a))_i$ is the difference between two sums that mostly have the same terms, and thus that $D(\sigma(a))_i = a_i$. On the other hand, we have $\lambda(\mu(a))_i = \sum_{u(j)=i} \mu(a)_j$ which is zero as the sum has no terms. Now consider instead the case where $i \in \text{image}(u)$. Let j_1 be the largest integer such that $u(j_1) = i$, and put $i' = u(j_1 + 1) > i$. From the definitions we have

$$\lambda(\mu(a))_i = \sum_{u(j)=i} \sum_{u(j) \leq h < u(j+1)} f_{h,u(j)}(a_h).$$

However, the inner summation is empty unless $j = j_1$, so the formula reduces to $\lambda(\mu(a))_i = \sum_{i \leq h < i'} f_{h,i}(a_h)$. We also have $uv(i) = i$, so $\sigma(a)_i = 0$, and $uv(i+1) = u(j_1+1) = i'$, so $\sigma(a)_{i+1} = \sum_{i < h < i'} h_{h,i+1}(a_h)$. From this it is easy to see that $\lambda(\mu(a))_i + D(\sigma(a))_i = a_i$ as required.

We now consider instead the map $\mu\lambda$. Define $\tau \colon \prod_j A_{u(j)} \to \prod_j A_{u(j)}$ by

$$\tau(b)_j = \sum_{k<j,\ u(k)=u(j)} b_k.$$

We claim that $\mu\lambda = 1 + D\tau$ (which implies that $\mu'\lambda' = 1$). The proof that $\mu(\lambda(b))_j = b_j + D(\tau(b))_j$ again splits into two cases. First suppose that $u(j+1) = u(j)$. It is then immediate from the definitions that $\mu(\lambda(b))_j = 0$. On the other hand, the sums defining $\tau(b)_j$ and $\tau(b)_{j+1}$ differ only by a single term, so $D(\tau(b))_j = -b_j$, as required. Now suppose instead that $u(j+1) > u(j)$. In this case we have $\tau(b)_{j+1} = 0$, so

$$b_j + D(\tau(b))_j = b_j + \tau(b)_j = b_j + \sum_{k<j,\ u(k)=u(j)} b_k = \sum_{u(k)=u(j)} b_k.$$

On the other hand, we have

$$\mu(\lambda(b))_j = \sum_{u(j) \leq i < u(j+1)} \sum_{u(k)=i} f_{i,u(j)}(b_k).$$

The inner sum has no terms unless $i = u(j)$, and in that context $f_{i,u(j)}$ is the identity, so the above reduces to

$$\mu(\lambda(b))_j = \sum_{u(k)=u(j)} b_k = b_j + D(\tau(b))_j$$

as required. $\square$

12. Completion and derived completion

Definition 12.1. Let p be a prime. For any abelian group A we have a tower of surjections

$$0 = A/p^0 \leftarrow A/p \leftarrow A/p^2 \leftarrow A/p^3 \leftarrow \cdots$$

We write A_p for the inverse limit of this tower, and call this the *p-completion* of A. In particular, we have a group $\mathbb{Z}_p$, whose elements are called *p-adic integers*. For any A we have a homomorphism $\eta\colon A \to A_p$ given by

$$\eta(a) = (a + p^0 A, a + p^1 A, a + p^2 A, a + p^3 A, \dots).$$

We say that A is *p-complete* if η is an isomorphism.

Example 12.2. Let A be a finite abelian group, so A splits as $B \oplus C$ say, where $|B|$ is a power of p and $|C|$ is coprime to p. For all k we have $p^k C = C$, and for large k we have $p^k B = 0$. It follows that $A_p = B$. In particular, we see from this that finite abelian p-groups are p-complete.

Example 12.3. Suppose that A is divisible. Then for all k we have $p^k A = A$, so $A/p^k = 0$; it follows that $A_p = 0$. In particular, we have $\mathbb{Q}_p = 0$ and $(\mathbb{Q}/\mathbb{Z})_p = 0$.

Remark 12.4. The symbol $\mathbb{Q}_p$ is often used for $\mathbb{Q} \otimes \mathbb{Z}_p$, which is not zero; it is known as the field of p-adic rationals. However, this is different from the group that we have called $\mathbb{Q}_p$, which is trivial.

Proposition 12.5. *For all A and $k \geq 0$ the projection $\pi_k\colon A \to A/p^k A$ induces an isomorphism $A_p/p^k A_p = A/p^k A$.*

Proof. For notational simplicity, we will treat only the case $k = 1$. The general case is essentially the same, after we have used Proposition 11.18 to identify A_p with the inverse limit of the sequence

$$A/p^k \leftarrow A/p^{2k} \leftarrow A/p^{3k} \leftarrow \cdots.$$

First, the projection $\pi_1\colon \prod_i A/p^i \to A/p$ restricts to give a homomorphism $\phi\colon A_p = \varprojlim_i A/p^i \to A/p$. Proposition 11.11 tells us that this is surjective. As A/p has exponent p, the subgroup pA_p is contained in the kernel. We need to prove that the kernel is precisely pA_p. Suppose that $a \in \ker(\phi)$. Choose $a_i \in A$ representing the component of a in $A/p^i A$. As $A/p^0 A = 0$ and $\phi(a) = 0$ we can take $a_0 = a_1 = 0$. By the definition of the inverse limit we see that a_i is the image of a_{i+1} in $A/p^i A$, so $a_{i+1} = a_i + p^i b_i$ for some $b_i \in A$ (and we may take $b_0 = 0$). Now put $c_n = \sum_{i=1}^n p^{i-1} b_i \in A$. It is visible that $c_{n+1} = c_n + p^n b_{n+1} = c_n \pmod{p^n A_n}$, so the cosets $c_n + p^n A$ define an element $c \in A_p$. We also see by induction that $pc_k = a_{k+1} = a_k \pmod{p^k A_k}$, so $pc = a$. Thus $a \in pA_p$ as claimed. $\square$

Remark 12.6. We see from the proposition that $A_p = (A_p)_p$, so A_p is p-complete, as one would expect. There is a subtlety analogous to Remark 9.15 here; we leave it to the reader to check that the two natural maps $A_p \to (A_p)_p$ are the same, and they are both isomorphisms.

We next examine the structure of $\mathbb{Z}_p$ in more detail. First, as the groups $\mathbb{Z}/p^k$ have canonical ring structures, and the maps $\mathbb{Z}/p^{k+1} \to \mathbb{Z}/p^k$ are ring maps, we see that $\mathbb{Z}_p$ is a subring of $\prod_k \mathbb{Z}/p^k$. We will write π_k for the projection $\mathbb{Z}_p \to \mathbb{Z}/p^k$, which is a surjective ring homomorphism. Note also that for $n \in \mathbb{Z}$ we have $\eta(n) = 0$ iff $\pi_k \eta(n) = 0$ for all k iff n is divisible by p^k for all k iff $n = 0$. Thus, η gives an injective ring map $\mathbb{Z} \to \mathbb{Z}_p$. We will usually suppress notation for this and regard $\mathbb{Z}$ as a subring of $\mathbb{Z}_p$.

Definition 12.7. For $a \in \mathbb{Z}_p$ we define $v(a) = \min\{k \mid \pi_k(a) \neq 0\}$ (or $v(a) = \infty$ if $\pi_k(a) = 0$ for all k, which means that $a = 0$). We also define $d(a,b) = p^{-v(a-b)}$, with the convention $p^{-\infty} = 0$.

Proposition 12.8. *The function d defines a metric on $\mathbb{Z}_p$ (called the* p-adic metric*), with respect to which it is complete and compact. Moreover, the subspace $\mathbb{Z}$ is dense.*

Proof. It is clear that $d(a,b) = d(b,a)$, and that this is nonnegative and vanishes if and only if $a = b$. This just leaves the triangle inequality $d(a,c) \leq d(a,b) + d(b,c)$. This is clear if $a = b$ or $b = c$, so suppose that $a \neq b \neq c$. Put $m = \min(v(a-b), v(b-c))$. For $k < m$ we have $\pi_k(a) = \pi_k(b) = \pi_k(c)$. It follows that $v(c-a) \geq m$, so

$$d(a,c) \leq p^{-m} = \max(d(a,b), d(b,c)) \leq d(a,b) + d(b,c)$$

as required.

Now consider a Cauchy sequence $(a_0, a_1, a_2, \dots)$ in $\mathbb{Z}_p$. Given $k \in \mathbb{N}$ we can choose m such that $d(a_i, a_j) < p^{-k}$ for all $i, j \geq m$. From the definition of d, this means that the element $\pi_k(a_i) \in \mathbb{Z}/p^k$ is independent of i for $i \geq m$. Let b_k denote this element. If i is large enough we will have $b_k = \pi_k(a_i)$ and also $b_{k+1} = \pi_{k+1}(a_i)$; using this we see that the projection $\mathbb{Z}/p^{k+1} \to \mathbb{Z}/p^k$ sends b_{k+1} to b_k. Thus, sequence $(b_0, b_1, b_2, \dots)$ is an element $b \in \mathbb{Z}_p$, and by construction $a_i \to b$ as $i \to \infty$. This shows that $\mathbb{Z}_p$ is compact.

Next, suppose we are given $k \in \mathbb{N}$, and we put $T_k = \{0, 1, \dots, p^k - 1\}$ and $a \in \mathbb{Z}_p$. The map $T_k \to \mathbb{Z}/p^k$ is a bijection, so for any $a \in \mathbb{Z}_p$ there is a unique $m \in T_k$ with $\pi_k(m) = \pi_k(a)$, so $d(m, a) < p^{-k}$. Using this we see that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Next, recall that an *ϵ-net* in a metric space X is a finite set $F \subseteq X$ such that every point is within ϵ of a point in F, that X is *totally bounded* if it has an ϵ-net for every $\epsilon > 0$, and that a complete metric space is compact if and only if it is totally bounded. The set T_k is a 2^{-k}-net, so $\mathbb{Z}_p$ is totally bounded, so it is compact. □

Proposition 12.9. *Put $D = \{0, 1, 2, \dots, p-1\}$ (the set of p-adic digits). Then there is a bijection*

$$\sigma \colon \prod_{i=0}^{\infty} D \to \mathbb{Z}_p$$

given by $\sigma(u) = \sum_i u_i p^i$ (a convergent sum with respect to the p-adic metric). In particular, $\mathbb{Z}_p$ is uncountable. We call $\sigma^{-1}(a)$ the base p expansion *of a.*

Proof. It is elementary that the corresponding map $\prod_{i=0}^{k-1} D \to \mathbb{Z}/p^k$ is a bijection, and the claim follows by passing to inverse limits. □

Proposition 12.10. *The ring $\mathbb{Z}_p$ is torsion free and is an integral domain. It is also a local ring, with $p.\mathbb{Z}_p$ being the unique maximal ideal. The group of units is*

$$\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid \pi_0(a) \neq 0\} = \mathbb{Z}_p \setminus p\mathbb{Z}_p,$$

and every nonzero element is a unit times p^k for some k.

Proof. First, consider an element $a \in \mathbb{Z}_p$ with $\pi_0(a) = 1$. We see from Proposition 12.5 that $a = 1 - px$ for some $x \in \mathbb{Z}_p$. It follows easily that the series $\sum_i (px)^i$ is Cauchy, so it converges to some $b \in \mathbb{Z}_p$, and we find that $ab = 1$. More generally, suppose merely that $\pi_0(a) \neq 0$ in $\mathbb{Z}/p$. As $\mathbb{Z}/p$ is a field, we can find $b \in \mathbb{Z}$ such that $\pi_0(b)$ is inverse to $\pi_0(a)$. We then find that ab is invertible by the previous case, and it follows that a is invertible. Conversely, as π_0 is a ring map it certainly sends units to nonzero elements. We therefore see that

$$\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid \pi_0(a) \neq 0\} = \mathbb{Z}_p \setminus p\mathbb{Z}_p$$

as claimed. Note also that $\mathbb{Z}_p/p\mathbb{Z}_p$ is the field $\mathbb{Z}/p$, so $p\mathbb{Z}_p$ is a maximal ideal. If $\mathfrak{m}$ is any maximal ideal we must have $\mathfrak{m} \cap \mathbb{Z}_p^\times = \emptyset$, so $\mathfrak{m} \leq p\mathbb{Z}_p$, so $\mathfrak{m} = p\mathbb{Z}_p$ by maximality. Thus, $\mathbb{Z}_p$ is a local ring.

Next, using base p expansions we see easily that multiplication by p is injective, and that every nonzero element $a \in \mathbb{Z}_p$ can be written as $a = p^k b$ for some $k \geq 0$ and b with $\pi_0(b) \neq 0$, so $b \in \mathbb{Z}_p^\times$. As multiplication by p^k is injective and b is invertible we see that multiplication by a is injective. This means that $\mathbb{Z}_p$ is an integral domain. By considering $a \in \mathbb{Z} \subset \mathbb{Z}_p$ we also see that $\mathbb{Z}_p$ is torsion free. □

We can now understand the completion of free modules.

Definition 12.11. Let I be a set, and let f be a function from I to $\mathbb{Z}_p$. We say that f is *asymptotically zero* if for all k, the set $\{i \mid v(f(i)) < k\}$ is finite. We write $AZ(I)$ for the set of asymptotically zero maps, which is a group under addition.

Proposition 12.12. *The completion $\mathbb{Z}[I]_p$ is naturally isomorphic to $AZ(I)$.*

Proof. First, we put

$$(\mathbb{Z}/p^k)[I] = \{f \colon I \to \mathbb{Z}/p^k \mid \{i \mid f(i) \neq 0\} \text{ is finite } \}.$$

We write π_k for the projection $\mathbb{Z} \to \mathbb{Z}/p^k$, or the projection $\mathbb{Z}_p \to \mathbb{Z}/p^k$. We then write $\pi'_k(f) = \pi_k \circ f$; this defines a map $AZ(I) \to (\mathbb{Z}/p^k)[I]$, which we can restrict to $\mathbb{Z}[I] \leq AZ(I)$. Note that $\pi'_k(f) = 0$ iff $f(i) \in p^k\mathbb{Z}_p$ for all i, in which case we can define $g = f/p^k \colon I \to \mathbb{Z}_p$ and we find that g is again asymptotically zero, so $f \in p^k AZ(I)$. This shows that π'_k induces an isomorphism $AZ(I)/p^k AZ(I) \to (\mathbb{Z}/p^k)[I]$. By a similar argument, it also induces an isomorphism $\mathbb{Z}[I]/p^k\mathbb{Z}[I] \to (\mathbb{Z}/p^k)[I]$. Thus, we have $\mathbb{Z}[I]_p = \varprojlim_k (\mathbb{Z}/p^k)[I]$. The maps $\pi'_k\colon AZ(I) \to (\mathbb{Z}/p^k)[I]$ therefore assemble to give a homomorphism $\pi'\colon AZ(I) \to \mathbb{Z}[I]_p$. In the opposite direction, suppose we have $g \in \mathbb{Z}[I]_p$. For each $k \geq 0$ we therefore have $\pi_k(g) \in \mathbb{Z}[I]/p^k\mathbb{Z}[I] = (\mathbb{Z}/p^k)[I]$, so there is a unique map

$$g_k\colon I \to \{0, 1, \dots, p^k - 1\}$$

with $\pi_k(g)(i) = g_k(i) \pmod{p^k}$ for all k. Note that the set $\{i \mid g_k(i) \neq 0\}$ is finite for all k. If we fix i, we find that the sequence $\{g_k(i)\}_{k\geq 0}$ is Cauchy, converging to some element $g_\infty(i) \in \mathbb{Z}_p$ say, and we have $g_\infty(i) = g_k(i) \pmod{p^k}$ for all k. This means that $g_\infty \in AZ(I)$ and $\pi'(g_\infty) = g$, so π' is surjective. We also have $\pi'(h) = 0$ iff $h(i)$ is divisible by p^k for all i and k, which implies that $h = 0$. Thus, the map π' is an isomorphism. □

Proposition 12.13. *For any abelian groups A and B there is a natural map $\mu\colon A_p \otimes B_p \to (A \otimes B)_p$, which induces an isomorphism $(A_p \otimes B_p)_p \to (A \otimes B)_p$.*

Proof. Note that $p^k.1_{A\otimes B} = (p^k.1_A) \otimes 1_B = 1_A \otimes (p^k.1_B)$. Using the right exactness of tensor products we see that

$$(A \otimes B)/p^k = (A/p^k) \otimes B = A \otimes (B/p^k) = (A/p^k) \otimes (B/p^k).$$

Combining this with Proposition 12.5 gives

$$(A_p \otimes B_p)/p^k = (A_p/p^k) \otimes (B_p/p^k) = (A/p^k) \otimes (B/p^k) = (A \otimes B)/p^k.$$

Passing to inverse limits gives an isomorphism $(A_p \otimes B_p)_p = (A \otimes B)_p$. We can compose this with the map $\eta\colon A_p \otimes B_p \to (A_p \otimes B_p)_p$ to get a map $\mu\colon A_p \otimes B_p \to (A \otimes B)_p$, which is what we most often need for applications. □

Proposition 12.14. *There is a natural map $\mathbb{Z}_p \otimes A \to A_p$, which is an isomorphism when A is finitely generated.*

Proof. The map is just the composite

$$\mathbb{Z}_p \otimes A \xrightarrow{1\otimes\eta} \mathbb{Z}_p \otimes A_p \xrightarrow{\mu} (\mathbb{Z} \otimes A)_p = A_p$$

(or it can be defined more directly by the method used for μ). By the classification of finitely generated abelian groups, it will suffice to prove that we have an isomorphism when $A = \mathbb{Z}$ or $A = \mathbb{Z}/p^k$ or $A = \mathbb{Z}/q^k$ for some prime $q \neq p$. The case $A = \mathbb{Z}$ is clear. When $A = \mathbb{Z}/p^k$ we have $A_p = A$ as in Example 12.2. We also $\mathbb{Z}_p \otimes A = \mathbb{Z}_p/p^k\mathbb{Z}_p$ by the right exactness of tensoring, and this is the same as $\mathbb{Z}/p^k = A$ by Proposition 12.5, so $\mathbb{Z}_p \otimes A = A_p$ as claimed. Finally, if q is different from p then q^k is invertible in $\mathbb{Z}_p$ so $\mathbb{Z}_p \otimes \mathbb{Z}/q^k = \mathbb{Z}_p/q^k\mathbb{Z}_p = 0$, and similarly $(\mathbb{Z}/q^k)_p = 0$ as in Example 12.2 again. □

Corollary 12.15. *If $A \to B \to C$ is an exact sequence of finitely generated abelian groups, then the resulting sequence $A_p \to B_p \to C_p$ is also exact.*

Proof. As $\mathbb{Z}_p$ is torsion free, Proposition 7.16 tells us that the sequence $\mathbb{Z}_p \otimes A \to \mathbb{Z}_p \otimes B \to \mathbb{Z}_p \otimes C$ is exact. □

We can now assemble our results to prove something closely analogous to Proposition 9.14:

Proposition 12.16.

(a) *The group A_p is always p-complete.*
(b) *The map $\eta\colon A \to A_p$ is an isomorphism if and only if A is p-complete.*
(c) *If A is p-complete then it can be regarded as a module over $\mathbb{Z}_p$.*
(d) *Suppose that $f\colon A \to B$ is a homomorphism, and that B is p-complete. Then there is a unique homomorphism $f'\colon A_p \to B$ such that $f' \circ \eta = f\colon A \to B$.*

Proof.

(a) As mentioned previously, this follows from Proposition 12.5 by taking inverse limits.
(b) This is true by definition, and is only mentioned to complete the correspondence with Proposition 9.14.

(c) Proposition 12.13 gives a map

$$\mathbb{Z}_p \otimes A = \mathbb{Z}_p \otimes A_p \to (\mathbb{Z} \otimes A)_p = A_p = A.$$

For $r \in \mathbb{Z}_p$ and $a \in A$ we can thus define $ra = \mu(r \otimes a)$. Equivalently, this is characterised by the fact that $\pi_k(ra) = \pi_k(r)\pi_k(a)$ in A/p^kA (where we have used the obvious structure of A/p^kA as a module over $\mathbb{Z}/p^k$). From this description it is clear that our multiplication rule is associative, unital and distributive, so it makes A into a module over $\mathbb{Z}_p$.

(d) The map $f\colon A \to B$ induces an isomorphism $f_p\colon A_p \to B_p$, and we have an isomorphism $\eta\colon B \to B_p$. We can and must take $f' = \eta^{-1} \circ f_p$.

□

While our definition of completion is quite natural and straightforward, its exactness properties for infinitely generated groups are very delicate, and they do not relate well to topological constructions. We will therefore introduce a different definition that often agrees with completion, but has better formal properties.

Definition 12.17. For any abelian group A, we let $A[\![x]\!]$ denote the group of formal power series $v(x) = \sum_{i=0}^{\infty} a_i x^i$ with $a_i \in A$ for all i. This is a module over $\mathbb{Z}[\![x]\!]$ by the obvious rule

$$\left(\sum_i n_i x^i\right)\left(\sum_j a_j x^j\right) = \sum_k \left(\sum_{i=0}^{k} n_i a_{k-i}\right) x^k.$$

We define

$$\begin{aligned} L_0A &= A[\![x]\!]/((x-p).A[\![x]\!]) \\ L_1A &= \{v(x) \in A[\![x]\!] \mid (x-p)v(x) = 0\}. \end{aligned}$$

We can identify A with the set of constant series in $A[\![x]\!]$, and then restrict the quotient map $A[\![x]\!] \to L_0A$ to A to get a natural map $\eta\colon A \to L_0A$. We say that A is *Ext-p-complete* if $\eta\colon A \to L_0A$ is an isomorphism and $L_1A = 0$. We also call L_0A the *derived completion* of A.

Remark 12.18. Readers familiar with the general theory of derived functors should consult Corollary 12.27 to see why the term is appropriate here.

Remark 12.19. It will follow from Proposition 12.28 that the condition $L_1A = 0$ is actually automatic when $\eta\colon A \to L_0A$ is an isomorphism. However, it is easier to develop the theory if we have both conditions in the initial definition.

Remark 12.20. There is an evident product map

$$\mu\colon A[\![x]\!] \otimes B[\![x]\!] \to (A \otimes B)[\![x]\!]$$

given by

$$\mu\left(\left(\sum_i a_i x^i\right) \otimes \left(\sum_j b_j x^j\right)\right) = \sum_k \left(\sum_{k=i+j} a_i \otimes b_j\right) x^k.$$

This induces a map $\mu\colon (L_0A) \otimes (L_0B) \to L_0(A \otimes B)$, which fits in a commutative diagram

$$\begin{tikzcd} & A \otimes B \arrow[dl, "\eta\otimes\eta"'] \arrow[dr, "\eta"] & \\ (L_0A) \otimes (L_0B) \arrow[rr, "\mu"'] & & L_0(A \otimes B). \end{tikzcd}$$

Remark 12.21. If we have a short exact sequence $A \to B \to C$, we can apply the Snake Lemma to the diagram

$$\begin{tikzcd} A[\![x]\!] \arrow[r, tail] \arrow[d, "x-p"'] & B[\![x]\!] \arrow[r, two heads] \arrow[d, "x-p"'] & C[\![x]\!] \arrow[d, "x-p"] \\ A[\![x]\!] \arrow[r, tail] & B[\![x]\!] \arrow[r, two heads] & C[\![x]\!] \end{tikzcd}$$

to obtain an exact sequence

$$L_1A \rightarrowtail L_1B \to L_1C \to L_0A \to L_0B \twoheadrightarrow L_0C.$$

Proposition 12.22. (a) *If we have a short exact sequence $A \to B \to C$ in which two of the three terms are Ext-p-complete, then so is the third.*
(b) *Finite sums and retracts of Ext-p-complete groups are Ext-p-complete.*
(c) *The kernel, cokernel and image of any homomorphism between Ext-p-complete groups are Ext-p-complete.*
(d) *The product of any (possibly infinite) family of Ext-p-complete groups is Ext-p-complete.*
(e) *If $p^k.1_A = 0$ for some k then A is Ext-p-complete.*
(f) *If A is p-complete then it is Ext-p-complete.*

Proof.
(a) Chase the diagram

$$\begin{tikzcd}
 & & & A \arrow[r, tail] \arrow[d] & B \arrow[r, two heads] \arrow[d] & C \arrow[d] \\
L_1A \arrow[r, tail] & L_1B \arrow[r] & L_1C \arrow[r] & L_0A \arrow[r] & L_0B \arrow[r, two heads] & L_0C
\end{tikzcd}$$

(b) Clear.
(c) Consider a homomorphism $f\colon A \to B$ between Ext-p-complete groups, and the resulting short exact sequences $\mathrm{img}(f) \to B \to \mathrm{cok}(f)$ and $\ker(f) \to A \to \mathrm{img}(f)$. These give diagrams

$$\begin{tikzcd}
 & & & \mathrm{img}(f) \arrow[r, tail] \arrow[d] & B \arrow[r, two heads] \arrow[d, "\simeq"] & \mathrm{cok}(f) \arrow[d] \\
L_1\,\mathrm{img}(f) \arrow[r, tail] & 0 \arrow[r] & L_1\,\mathrm{cok}(f) \arrow[r] & L_0\,\mathrm{img}(f) \arrow[r] & L_0B \arrow[r, two heads] & L_0\,\mathrm{cok}(f)
\end{tikzcd}$$

and

$$\begin{tikzcd}
 & & & \ker(f) \arrow[r, tail] \arrow[d] & A \arrow[r, two heads] \arrow[d, "\simeq"] & \mathrm{img}(f) \arrow[d] \\
L_1\ker(f) \arrow[r, tail] & 0 \arrow[r] & L_1\,\mathrm{img}(f) \arrow[r] & L_0\ker(f) \arrow[r] & L_0A \arrow[r, two heads] & L_0\,\mathrm{img}(f).
\end{tikzcd}$$

From the first diagram we see that $L_1\,\mathrm{img}(f) = 0$ and that the map $\mathrm{img}(f) \to L_0\,\mathrm{img}(f)$ is injective, and from the second we see that the map $\mathrm{img}(f) \to L_0\,\mathrm{img}(f)$ is surjective; thus $\mathrm{img}(f)$ is Ext-p-complete. Given this, it is a special case of (a) that $\ker(f)$ and $\mathrm{cok}(f)$ are also Ext-p-complete as claimed.
(d) This is clear, because $(\prod_i A_i)[\![x]\!] = \prod_i A_i[\![x]\!]$.
(e) If $k = 1$ the definitions give $L_0A = A[\![x]\!]/(x.A[\![x]\!]) = A$ and $L_1A = \{v(x) \in A[\![x]\!] \mid xv(x) = 0\} = 0$ as required. The general case follows by induction using (a) and the short exact sequence $pA \to A \to A/pA$.
(f) As the tower $\{A/p^k\}$ consists of surjections, the $\varprojlim^1$ term is zero. As A is p-complete, we therefore have a short exact sequence

$$A \rightarrowtail \prod_k A/p^k \twoheadrightarrow \prod_k A/p^k.$$

The second and third terms are Ext-p-complete by parts (e) and (d), so A is Ext-p-complete by part (a).

□

Proposition 12.23. *Let A be any abelian group. Then $L_1A = \varprojlim_k A[p^k]$ and there is a natural short exact sequence*

$$\varprojlim_k{}^1 A[p^k] \overset{\xi}{\rightarrowtail} L_0A \overset{\zeta}{\twoheadrightarrow} A_p.$$

The limit symbols here refer to the tower

$$0 = A[p^0] \xleftarrow{p} A[p] \xleftarrow{p} A[p^2] \xleftarrow{p} A[p^3] \xleftarrow{p} \cdots$$

Proof. First, an element of $L_1 A$ is a series $v(x) = \sum_i a_i x^i$ with $(x-p)v(x) = 0$, which means that $pa_0 = 0$ and $pa_{i+1} = a_i$ for all $i \geq 0$. It follows inductively that $p^{i+1}a_i = 0$ for all i, so the sequence $(0, a_0, a_1, \dots)$ is an element of $\varprojlim_i A[p^i]$. All steps here can be reversed so $L_1 A = \varprojlim_i A[p^i]$. Next, define $\zeta_i' \colon A[\![x]\!] \to A/p^i A$ by

$$\zeta_i'(\sum_j a_j x^j) = \sum_{j<i} a_j p^j + p^i A.$$

It is clear that $\zeta_i'(v(x)) = \zeta_{i+1}'(v(x)) \pmod{p^i A}$, so the maps ζ_i' fit together to give a homomorphism $\zeta' \colon A[\![x]\!] \to A_p$, which can be described heuristically as $\zeta'(v(x)) = v(p)$. It is also easy to check that $\zeta'((x-p)w(x)) = 0$ for all $w(x)$, so there is an induced map $\zeta \colon L_0 A \to A_p$. Given an arbitrary element $b \in A_p$ we can choose $b_i \in A$ representing the coset $\pi_i(b) \in A/p^i A$. These will then satisfy $b_{i+1} = b_i \pmod{p^i A}$, so we can choose $a_i \in A$ with $b_{i+1} = p^i a_i + b_i$. The series $v(x) = \sum_i a_i x^i$ then has $\zeta(v(x)) = b$, so we see that ζ is surjective.

Next, for any $c \in \prod_i A[p^i]$ put $\xi''(c) = \sum_i c_i x^i \in A[\![x]\!]$, and let $\xi'(c)$ denote the image of $\xi''(c)$ in $L_0 A$. It is clear by construction that $\zeta\xi' = 0$. Suppose that c lies in the image of the map $D \colon \prod_i A[p^i] \to \prod_i A[p^i]$, so there is a sequence $(d_i)_{i\geq 0}$ with $p^i d_i = 0$ and $c_i = d_i - pd_{i+1}$ for all i. Note that $d_0 = p^0 d_0 = 0$ and put $w(x) = \sum_i d_{i+1} x^i$; we find that $\xi''(c) = (x-p)w(x)$ and so $\xi'(c) = 0$. We thus have an induced map $\xi \colon \operatorname{cok}(D) = \varprojlim^1_i A[p^i] \to L_0 A$ with $\zeta\xi = 0$. Consider an arbitrary element $v(x) = \sum_i a_i x^i \in A[\![x]\!]$ with $\zeta'(v(x)) = 0$. This means that for all $i \geq 0$ we can choose $b_i \in A$ with $\sum_{j<i} a_j p^j = p^i b_i$. It follows that $b_0 = 0$ and $p^i b_i + p^i a_i = p^{i+1} b_{i+1}$, so the element $c_i = b_i + a_i - pb_{i+1}$ has $p^i c_i = 0$, so $c \in \prod_i A[p^i]$. If we put $w(x) = \sum_i b_{i+1} x^i$ we find that

$$v(x) = \xi''(c) - (x-p)w(x),$$

so in $L_0 A$ we have $v = \xi(c)$. This proves that the map $\xi \colon \varprojlim^1_i A[p^i] \to \ker(\zeta)$ is surjective.

Finally, suppose we have $c \in \prod_i A[p^i]$ with $\xi'(c) = 0$. This means that there exists $u(x) = \sum_i b_i x^i \in A[\![x]\!]$ with $\xi''(c) = (x-p)u(x)$, so $c_0 = -pb_0$ and $c_{i+1} = b_i - pb_{i+1}$ for all $i \geq 0$. Form this it follows easily that $p^{i+1} b_i = 0$ for all $i \geq 0$, so we have an element $b' = (0, b_0, b_1, \dots) \in \prod_i A[p^i]$. We now see that $c = D(b')$, so c represents the zero element of $\varprojlim^1_i A[p^i]$, thus, the map $\xi \colon \varprojlim^1_i A[p^i] \to \ker(\zeta)$ is injective. $\square$

Remark 12.24. It is clear from the definitions that the diagram

$$\begin{tikzcd} & A \arrow[dl, "\eta"'] \arrow[dr, "\eta"] & \\ L_0 A \arrow[rr, "\zeta"'] & & A_p \end{tikzcd}$$

commutes.

Definition 12.25. We say that an abelian group A has *bounded p-torsion* if there exists $k \geq 0$ such that $p^k . \operatorname{tors}_p(A) = 0$.

Corollary 12.26. *If A has bounded p-torsion (in particular, if A is a free abelian group) then $L_1 A = 0$ and $L_0 A = A_p$.*

Proof. The tower $\{A[p^i]\}$ is nilpotent, so $\varprojlim_i A[p^i] = \varprojlim^1_i A[p^i] = 0$ by Proposition 11.13. $\square$

Corollary 12.27. *Suppose we have a short exact sequence $P \xrightarrow{f} Q \to A$ where P and Q are free abelian groups. Then $L_0 A$ and $L_1 A$ are the cokernel and kernel of the induced map $P_p \to Q_p$.*

Proof. This is immediate from Corollary 12.26 and Remark 12.21. $\square$

Proposition 12.28. *For any abelian group A, the groups $L_0 A$, $L_1 A$, A_p and $\varprojlim^1_k A[p^k]$ are all Ext-p-complete.*

Proof. The groups $A[p^k]$ and A/p^k are Ext-p-complete by part (e) of Proposition 12.22. It follows by part (d) that $\prod_k A[p^k]$ and $\prod_k A/p^k$ are Ext-p-complete, and then by part (c) that the groups $\varprojlim_k A[p^k] = L_1 A$, $\varprojlim^1_k A[p^k]$ and $\varprojlim_k A/p^k = A_p$ are Ext-p-complete. We can thus apply part (a) to the short exact sequence

$$\varprojlim^1_k A[p^k] \xrightarrow{\xi} L_0 A \xrightarrow{\zeta} A_p$$

to deduce that $L_0 A$ is Ext-p-complete. □

Proposition 12.29. *For any abelian group A, we have $L_0 A = 0$ iff $A_p = 0$ iff $A/p = 0$.*

Proof. Proposition 12.23 shows that A_p is a quotient of $L_0 A$, and Proposition 12.5 shows that A/p is a quotient of A_p. Conversely, if $A/p = 0$ then $p.1_A$ is surjective, so $A/p^k = 0$ for all k and the maps in the tower $\{A[p^k]\}$ are all surjective. It follows that $A_p = \varprojlim_k A/p^k = 0$ and (using Proposition 11.17) that $\varprojlim^1_k A[p^k] = 0$, so the short exact sequence in Proposition 12.23 shows that $L_0 A = 0$. □

We next explain a more traditional construction of the functors L_0 and L_1. This involves a group known as $\mathbb{Z}/p^\infty$.

Definition 12.30. Define $f_k \colon \mathbb{Z}/p^k \to \mathbb{Z}/p^{k+1}$ by $f_k(a + p^k\mathbb{Z}) = pa + p^{k+1}\mathbb{Z}$, so we have a sequence

$$0 = \mathbb{Z}/p^0 \xrightarrow{f_0} \mathbb{Z}/p \xrightarrow{f_1} \mathbb{Z}/p^2 \xrightarrow{f_2} \mathbb{Z}/p^3 \xrightarrow{f_3} \mathbb{Z}/p^4 \xrightarrow{f_4} \cdots$$

We define $\mathbb{Z}/p^\infty$ to be the colimit of this sequence.

Proposition 12.31. *There are canonical isomorphisms*

$$\mathbb{Z}/p^\infty = \mathbb{Z}[1/p]/\mathbb{Z} = \mathrm{tors}_p(\mathbb{Q}/\mathbb{Z}) = (\mathbb{Q}/\mathbb{Z})_{(p)} = \mathbb{Q}/\mathbb{Z}_{(p)}.$$

Proof. First, consider the diagram

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, equal] \arrow[d, "1"'] & \mathbb{Z} \arrow[r, equal] \arrow[d, "p"'] & \mathbb{Z} \arrow[r, equal] \arrow[d, "p^2"'] & \mathbb{Z} \arrow[r, equal] \arrow[d, "p^3"'] & \mathbb{Z} \arrow[r, equal] \arrow[d, "p^4"'] & \cdots \\
\mathbb{Z} \arrow[r, tail, "p"] \arrow[d, two heads] & \mathbb{Z} \arrow[r, tail, "p"] \arrow[d, two heads] & \mathbb{Z} \arrow[r, tail, "p"] \arrow[d, two heads] & \mathbb{Z} \arrow[r, tail, "p"] \arrow[d, two heads] & \mathbb{Z} \arrow[r, tail, "p"] \arrow[d, two heads] & \cdots \\
\mathbb{Z}/p^0 \arrow[r, tail, "f_0"'] & \mathbb{Z}/p^1 \arrow[r, tail, "f_1"'] & \mathbb{Z}/p^2 \arrow[r, tail, "f_2"'] & \mathbb{Z}/p^3 \arrow[r, tail, "f_3"'] & \mathbb{Z}/p^4 \arrow[r, tail, "f_4"'] & \cdots
\end{tikzcd}$$

Using Propositions 10.10 and 10.8 we obtain a short exact sequence $\mathbb{Z} \to \mathbb{Z}[1/p] \to \mathbb{Z}/p^\infty$, so $\mathbb{Z}/p^\infty = \mathbb{Z}[1/p]/\mathbb{Z}$. Next, for $a \in \mathbb{Q}$ we note that $a + \mathbb{Z}$ is a p-torsion element in $\mathbb{Q}/\mathbb{Z}$ iff $p^k a \in \mathbb{Z}$ for some k, iff $a \in \mathbb{Z}[1/p]$. It follows that $\mathrm{tors}_p(\mathbb{Q}/\mathbb{Z}) = \mathbb{Z}[1/p]/\mathbb{Z}$. We also know from Proposition 9.17 that $\mathrm{tors}_p(\mathbb{Q}/\mathbb{Z}) = (\mathbb{Q}/\mathbb{Z})_{(p)}$. It is clear that $\mathbb{Q}$ is p-local, so $\mathbb{Q}_{(p)} = \mathbb{Q}$. We can thus apply Proposition 9.10 to the sequence $\mathbb{Z} \rightarrowtail \mathbb{Q} \twoheadrightarrow \mathbb{Q}/\mathbb{Z}$ to see that $(\mathbb{Q}/\mathbb{Z})_{(p)} = \mathbb{Q}/\mathbb{Z}_{(p)}$. □

Proposition 12.32. *There are natural isomorphisms $L_0 A = \mathrm{Ext}(\mathbb{Z}/p^\infty, A)$ and $L_1 A = \mathrm{Hom}(\mathbb{Z}/p^\infty, A)$.*

Proof. In this proof we will identify $\mathbb{Z}/p^\infty$ with $\mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$. Put $F = \bigoplus_{i=0}^\infty \mathbb{Z}$, and let e_i be the i'th basis vector in F. Define maps

$$F \xrightarrow{\phi} F \xrightarrow{\psi} \mathbb{Z}/p^\infty$$

by

$$\phi(e_i) = e_{i-1} - pe_i \qquad\qquad \psi(e_i) = p^{-i-1} + \mathbb{Z}$$

(where e_{-1} is interpreted as 0), or equivalently

$$\phi(n_0, n_1, n_2, \dots) = (pn_0 - n_1, pn_1 - n_2, pn_2 - n_3, \dots)$$
$$\phi(m_0, m_1, m_2, \dots) = \sum_i m_i p^{-i-1} + \mathbb{Z}.$$

By considering the first nonzero entry in $n = (n_0, n_1, \dots)$, we see that ϕ is injective. Any element of $\mathbb{Z}/p^\infty$ can be written as $k/p^{i+1} + \mathbb{Z}$ for some $i \geq 0$ and $k \in \mathbb{Z}$, and this is the same as $\psi(ke_i)$, so ψ is surjective.

It is clear from the definitions that $\psi\phi = 0$, so $\mathrm{img}(\phi) \leq \ker(\psi)$. Conversely, suppose we have $n \in F$ with $\psi(n) = 0$, so the number $q = \sum_i n_i p^{-1-i}$ actually lies in $\mathbb{Z}$. Put $m_i = \sum_{j<i} n_j p^{i-j-1} - p^i q$, and note that $m_i = 0$ for $i \gg 0$, so $m \in F$. We find that $\phi(m) = n$, so the sequence $F \xrightarrow{\phi} F \xrightarrow{\psi} \mathbb{Z}/p^\infty$ is short exact. As F is free, this gives us an exact sequence

$$\mathrm{Hom}(\mathbb{Z}/p^\infty, A) \xrightarrow{\psi^*} \mathrm{Hom}(F, A) \xrightarrow{\phi^*} \mathrm{Hom}(F, A) \longrightarrow \mathrm{Ext}(\mathbb{Z}/p^\infty, A).$$

Next, for any series $v(x) = \sum_i a_i x^i \in A[\![x]\!]$ we have a homomorphism $\alpha(v(x)) \colon F \to A$ given by $\alpha(v(x))(e_i) = a_i$ for all $i \geq 0$. This construction gives an isomorphism $A[\![x]\!] \to \mathrm{Hom}(F, A)$. If we make the conventions $a_{-1} = 0$ and $e_{-1} = 0$ we also have

$$\alpha((x-p)v(x))(e_j) = \alpha\left(\sum_i (a_{i-1} - pa_i)x^i\right)(e_j) = a_{j-1} - pa_j = \alpha(v(x))(e_{j-1} - pe_j) = \alpha(v(x))(\phi(e_j))$$

Thus, multiplication by $x - p$ on $A[\![x]\!]$ corresponds to ϕ^* on $\mathrm{Hom}(F, A)$, and the claim follows from this. $\square$

References

[1] A. K. Bousfield and Daniel M. Kan, *Homotopy limits, completions and localizations*, Lecture notes in Mathematics, vol. 304, Springer–Verlag, 1972.