With this terminology, the pair of homomorphisms $A \xrightarrow{\psi} B \xrightarrow{\varphi} C$ above is exact at B. We can also use this terminology to express the fact that for these maps ψ is injective and φ is surjective:

Proposition 22. Let A, B and C be R-modules over some ring R. Then

(1) The sequence $0 \to A \xrightarrow{\psi} B$ is exact (at A) if and only if ψ is injective.
(2) The sequence $B \xrightarrow{\varphi} C \to 0$ is exact (at C) if and only if φ is surjective.

Proof: The (uniquely defined) homomorphism $0 \to A$ has image 0 in A. This will be the kernel of ψ if and only if ψ is injective. Similarly, the kernel of the (uniquely defined) zero homomorphism $C \to 0$ is all of C, which is the image of φ if and only if φ is surjective.

Corollary 23. The sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is exact if and only if ψ is injective, φ is surjective, and image $\psi = \ker\varphi$, i.e., B is an extension of C by A.

Definition. The exact sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is called a *short exact sequence.*

In terms of this notation, the extension problem can be stated succinctly as follows: given modules A and C, determine all the short exact sequences

$$0 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\varphi} C \longrightarrow 0. \tag{10.9}$$

We shall see below that the exact sequence notation is also extremely convenient for analyzing the extent to which properties of A and C determine the corresponding properties of B. If A, B and C are groups written multiplicatively, the sequence (9) will be written

$$1 \longrightarrow A \xrightarrow{\psi} B \xrightarrow{\varphi} C \longrightarrow 1 \tag{10.9$'$}$$

where 1 denotes the trivial group. Both Proposition 22 and Corollary 23 are valid with the obvious notational changes.

Note that any exact sequence can be written as a succession of short exact sequences since to say $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is exact at Y is the same as saying that the sequence $0 \to \alpha(X) \to Y \to Y/\ker\beta \to 0$ is a short exact sequence.

Examples

(1) Given modules A and C we can always form their direct sum $B = A \oplus C$ and the sequence

$$0 \to A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \to 0$$

where $\iota(a) = (a, 0)$ and $\pi(a, c) = c$ is a short exact sequence. In particular, it follows that there always exists at least one extension of C by A.

(2) As a special case of the previous example, consider the two $\mathbb{Z}$-modules $A = \mathbb{Z}$ and $C = \mathbb{Z}/n\mathbb{Z}$:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \oplus (\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

giving one extension of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$.

Another extension of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$ is given by the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$$

where n denotes the map $x \mapsto nx$ given by multiplication by n, and π denotes the natural projection. Note that the modules in the middle of the previous two exact sequences are not isomorphic even though the respective "A" and "C" terms are isomorphic. Thus there are (at least) two "essentially different" or "inequivalent" ways of extending $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$.

(3) If $\varphi : B \to C$ is any homomorphism we may form an exact sequence:

$$0 \longrightarrow \ker\varphi \xrightarrow{\ \iota\ } B \xrightarrow{\ \varphi\ } \text{image}\,\varphi \longrightarrow 0$$

where ι is the inclusion map. In particular, if φ is surjective, the sequence $\varphi : B \to C$ may be extended to a short exact sequence with $A = \ker\varphi$.

(4) One particularly important instance of the preceding example is when M is an R-module and S is a set of generators for M. Let $F(S)$ be the free R-module on S. Then

$$0 \longrightarrow K \xrightarrow{\ \iota\ } F(S) \xrightarrow{\ \varphi\ } M \longrightarrow 0$$

is the short exact sequence where φ is the unique R-module homomorphism which is the identity on S (cf. Theorem 6) and $K = \ker\varphi$.

More generally, when M is any group (possibly non-abelian) the above short exact sequence (with 1's at the ends, if M is written multiplicatively) describes a *presentation* of M, where K is the normal subgroup of $F(S)$ generated by the *relations* defining M (cf. Section 6.3).

(5) Two "inequivalent" extensions G of the Klein 4-group by the cyclic group Z_2 of order two are

$$1 \longrightarrow Z_2 \xrightarrow{\ \iota\ } D_8 \xrightarrow{\ \varphi\ } Z_2 \times Z_2 \longrightarrow 1, \text{ and}$$
$$1 \longrightarrow Z_2 \xrightarrow{\ \iota\ } Q_8 \xrightarrow{\ \varphi\ } Z_2 \times Z_2 \longrightarrow 1,$$

where in each case ι maps Z_2 injectively into the center of G (recall that both D_8 and Q_8 have centers of order two), and φ is the natural projection of G onto $G/Z(G)$.

Two other inequivalent extensions G of the Klein 4-group by Z_2 occur when G is either of the abelian groups $Z_2 \times Z_2 \times Z_2$ or $Z_2 \times Z_4$ for appropriate maps ι and φ.

Examples 2 and 5 above show that, for a fixed A and C, in general there may be several extensions of C by A. To distinguish different extensions we define the notion of a homomorphism (and isomorphism) between two exact sequences. Recall first that a diagram involving various homomorphisms is said to *commute* if any compositions of homomorphisms with the same starting and ending points are equal, i.e., the composite map defined by following a path of homomorphisms in the diagram depends only on the starting and ending points and not on the choice of the path taken.

Definition. Let $0 \to A \to B \to C \to 0$ and $0 \to A' \to B' \to C' \to 0$ be two short exact sequences of modules.

(1) A *homomorphism of short exact sequences* is a triple α, β, γ of module homomorphisms such that the following diagram commutes:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0 \end{tikzcd}$$

The homomorphism is an *isomorphism of short exact sequences* if α, β, γ are all isomorphisms, in which case the extensions B and B' are said to be *isomorphic extensions*.

(2) The two exact sequences are called *equivalent* if $A = A'$, $C = C'$, and there is an isomorphism between them as in (1) that is the identity maps on A and C (i.e., α and γ are the identity). In this case the corresponding extensions B and B' are said to be *equivalent* extensions.

If B and B' are isomorphic extensions then in particular B and B' are isomorphic as R-modules, but more is true: there is an R-module isomorphism between B and B' that restricts to an isomorphism from A to A' and induces an isomorphism on the quotients C and C'. For a given A and C the condition that two extensions B and B' of C by A are equivalent is stronger still: there must exist an R-module isomorphism between B and B' that restricts to the *identity* map on A and induces the *identity* map on C. The notion of isomorphic extensions measures how many different extensions of C by A there are, allowing for C and A to be changed by an isomorphism. The notion of equivalent extensions measures how many different extensions of C by A there are when A and C are rigidly fixed.

Homomorphisms and isomorphisms between short exact sequences of multiplicative groups (9′) are defined similarly.

It is an easy exercise to see that the composition of homomorphisms of short exact sequences is also a homomorphism. Likewise, if the triple α, β, γ is an isomorphism (or equivalence) then $\alpha^{-1}, \beta^{-1}, \gamma^{-1}$ is an isomorphism (equivalence, respectively) in the reverse direction. It follows that "isomorphism" (or equivalence) is an equivalence relation on any set of short exact sequences.

Examples

(1) Let m and n be integers greater than 1. Assume n divides m and let $k = m/n$. Define a map from the exact sequence of $\mathbb{Z}$-modules in Example 2 of the preceding set of examples:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r, "n"] \arrow[d, "\alpha"] & \mathbb{Z} \arrow[r, "\pi"] \arrow[d, "\beta"] & \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & \mathbb{Z}/k\mathbb{Z} \arrow[r, "\iota"] & \mathbb{Z}/m\mathbb{Z} \arrow[r, "\pi'"] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

where α and β are the natural projections, γ is the identity map, ι maps $a \bmod k$ to $na \bmod m$, and π' is the natural projection of $\mathbb{Z}/m\mathbb{Z}$ onto its quotient $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z})$

(which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$). One easily checks that this is a homomorphism of short exact sequences.

(2) If again $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$ is the short exact sequence of $\mathbb{Z}$-modules defined previously, map each module to itself by $x \mapsto -x$. This triple of homomorphisms gives an isomorphism of the exact sequence with itself. This isomorphism is not an equivalence of sequences since it is not the identity on the first $\mathbb{Z}$.

(3) The short exact sequences in Examples 1 and 2 following Corollary 23 are not isomorphic—the extension modules are not isomorphic $\mathbb{Z}$-modules (abelian groups). Likewise the two extensions, D_8 and Q_8, in Example 5 of the same set are not isomorphic (hence not equivalent), even though the two end terms "A" and "C" are the same for both sequences.

(4) Consider the maps

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\psi"] \arrow[d, "\mathrm{id}"] & \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} \arrow[r, "\varphi"] \arrow[d, "\beta"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\psi'"] & \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} \arrow[r, "\varphi'"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

where ψ maps $\mathbb{Z}/2\mathbb{Z}$ injectively into the first component of the direct sum and φ projects the direct sum onto its second component. Also ψ' embeds $\mathbb{Z}/2\mathbb{Z}$ into the *second* component of the direct sum and φ' projects the direct sum onto its *first* component. If β maps the direct sum $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ to itself by interchanging the two factors, then this diagram is seen to commute, hence giving an equivalence of the two exact sequences that is not the identity isomorphism.

(5) We exhibit two isomorphic but inequivalent $\mathbb{Z}$-module extensions. For $i = 1, 2$ define

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi_i} \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

where $\psi : 1 \mapsto (2, 0)$ in both sequences, φ_1 is defined by $\varphi_1(a \bmod 4, b \bmod 2) = (a \bmod 2, b \bmod 2)$, and $\varphi_2(a \bmod 4, b \bmod 2) = (b \bmod 2, a \bmod 2)$. It is easy to see that the resulting two sequences are both short exact sequences.

An evident isomorphism between these two exact sequences is provided by the triple of maps id, id, γ, where $\gamma : \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is the map $\gamma((c, d)) = (d, c)$ that interchanges the two direct factors.

We now check that these two isomorphic sequences are *not equivalent*, as follows. Since $\varphi_1(0, 1) = (0, 1)$, any equivalence, id, β, id, from the first sequence to the second must map $(0, 1) \in \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ to either $(1, 0)$ or $(3, 0)$ in $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, since these are the two possible elements mapping to $(0, 1)$ by φ_2. This is impossible, however, since the isomorphism β cannot send an element of order 2 to an element of order 4.

Put another way, equivalences involving the same extension module B are automorphisms of B that restrict to the identity on both $\psi(A)$ and $B/\psi(A)$. Any such automorphism of $B = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ must fix the coset $(0, 1) + \psi(A)$ since this is the unique nonidentity coset containing elements of order 2. Thus maps which send this coset to different elements in C give inequivalent extensions. In particular, there is yet a third inequivalent extension involving the same modules $A = \mathbb{Z}/2\mathbb{Z}$, $B = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $C = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, that maps the coset $(0, 1) + \psi(A)$ to the element $(1, 1) \in \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

By similar reasoning there are three inequivalent but isomorphic group extensions of $Z_2 \times Z_2$ by Z_2 with $B \cong D_8$ (cf. the exercises).