# Construction of $\mathrm{Ext}^1_R(A,B)$

We begin by constructing a category, **SES**. The objects are short exact sequences $0 \to A \to E \to B \to 0$ (suppose of $R$-modules) and the arrows are diagrams, which is to say, vertical maps such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & E' & \longrightarrow & B' & \longrightarrow & 0 \end{array}$$

Now, fix $A$ and $B$ and consider extensions $0 \to A \to E \to B \to 0$. We define an equivalence relation on extensions by $(0 \to A \to E \to B \to 0) \sim (0 \to A \to E' \to B \to 0)$ if and only if we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}_B} & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

where $\theta : E \to E'$ is an isomorphism.

**Exercise 1** $\sim$ defines an equivalence relation on extensions.

We show $\sim$ is symmetric, reflexive, and transitive:

- Symmetric: $\mathrm{id}_E$ is an isomorphism.
- Reflexive: $\theta : E \to E'$ an isomorphism means $\theta^{-1} : E' \to E$ is an isomorphism.
- Transitive: $\theta_1 : E \to E'$ and $\theta_2 : E' \to E''$ isomorphisms mean $(\theta_2 \circ \theta_1) : E \to E''$ is an isomorphism.

Now, we define an extension $0 \to A \to E \to B \to 0$ to be **split** if it is equivalent to the short exact sequence $0 \to A \to A \oplus B \to B \to 0$ with maps inclusion and projection.

**Exercise 2** Prove that the following are equivalent:

1. $0 \to A \xrightarrow{f} E \xrightarrow{g} B \to 0$ is split in the above definition;
2. the map $f$ is split;
3. the map $g$ is split.

First, recall that for $f$ to be split means there exists $\varphi : E \to A$ such that $\varphi f = \mathrm{id}_A$. For $g$ to be split means there exists $\psi : B \to E$ such that $g\psi = \mathrm{id}_B$.

Now for 1 implies 2: we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\quad f \quad} & E & \xrightarrow{\quad g \quad} & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}_B} & & \\ 0 & \longrightarrow & A & \xrightarrow{a \mapsto (a,0)} & A \oplus B & \xrightarrow{(a,b) \mapsto b} & B & \longrightarrow & 0 \end{array}$$

Since the diagram commutes in the second square, for all $e \in E$, $\theta(e) = (x, g(e))$. Define $\varphi : E \to A$ to be $\varphi(e) = x$. Then see that as the diagram commutes in the first square, for all $a \in A$, $(a, 0) = \theta f(a)$. Therefore

$$(a, 0) = \theta f(a) = \theta(fa) = (\varphi(fa), g(fa)) = (\varphi f(a), g(fa)),$$

so $\varphi f = \mathrm{id}_A$, as desired.

Now, 1 implies 3: the same diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & E & \xrightarrow{g} & B & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle \mathrm{id}_A} & & \big\downarrow{\scriptstyle \theta} & & \big\downarrow{\scriptstyle \mathrm{id}_B} & & \\ 0 & \longrightarrow & A & \xrightarrow{a \mapsto (a,0)} & A \oplus B & \xrightarrow{(a,b) \mapsto b} & B & \longrightarrow & 0 \end{array}$$

commuting means that $g(e) = \pi_2\theta(e)$, for $\pi_2$ projection to the second factor. If we choose $\psi : B \to E$ to be $\psi(b) = \theta^{-1}(0, b)$, then

$$g\psi(b) = \pi_2\theta\theta^{-1}(0, b) = \pi_2(0, b) = b,$$

and $g\psi = \mathrm{id}_B$ as desired.

Now for 2 implies 1: since $f$ is split, there exists $\varphi : E \to A$ with $\varphi f = \mathrm{id}_A$. We need to show there is some isomorphism $\theta : E \to A \oplus B$ such that $0 \to A \to E \to B \to 0$ is split. We claim it is $\theta(e) = (\varphi(e), g(e))$. $\theta$ will indeed be an isomorphism by the five lemma once we establish the commutativity of the diagram. To see that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & E & \xrightarrow{g} & B & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle \mathrm{id}_A} & & \big\downarrow{\scriptstyle \theta} & & \big\downarrow{\scriptstyle \mathrm{id}_B} & & \\ 0 & \longrightarrow & A & \xrightarrow{a \mapsto (a,0)} & A \oplus B & \xrightarrow{(a,b) \mapsto b} & B & \longrightarrow & 0 \end{array}$$

commutes, observe that for all $a \in A$,

$$\theta f(a) = (\varphi(f(a)), g(f(a))) = (a, gf(a)) = (a, 0),$$

so the left square commutes. Also for all $e \in E$,

$$\pi_2\theta(e) = \pi_2(\varphi(e), g(e)) = g(e) = \mathrm{id}_B\, g(e),$$

so the right square commutes. Thus the extension is exact.

Finally, for 3 implies 1: we have the existence of $\psi : B \to E$ such that $g\psi = \mathrm{id}_B$. It is equivalent to have the isomorphisms showing the extension is exact go in the other direction, so we let $\sigma : A \oplus B \to E$ be $\sigma(a, b) = f(a) + \psi(b)$. First, $\sigma$ is indeed an isomorphism again by the five lemma after showing the diagram commutes. And to see that

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{a \mapsto (a,0)} & A \oplus B & \xrightarrow{(a,b) \mapsto b} & B & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \mathrm{id}_B} & & \\
0 & \longrightarrow & A & \xrightarrow{\quad f \quad} & E & \xrightarrow{\quad g \quad} & B & \longrightarrow & 0
\end{array}$$

commutes, on the left square we get $\sigma(a, 0) = f(a) + \psi(0) = f(a) = f \,\mathrm{id}_A(a)$. On the right square we get $g\sigma(a, b) = g(f(a) + \psi(b)) = gf(a) + g\psi(b) = b = \mathrm{id}_B \, \pi_2(a, b)$.

Now, given two extension $0 \to A \xrightarrow{f} E \xrightarrow{g} B \to 0$ and $0 \to A \xrightarrow{f'} E' \xrightarrow{g'} B \to 0$, we can build a pullback:

$$\Gamma = E \times_B E' = \{(e, e') \in E \times E' \mid g(e) = g'(e')\} .$$

In other words, the following commutes:

$$\begin{array}{ccccc}
 & & \Gamma & & \\
 & {\scriptstyle \pi_1} \swarrow & & \searrow {\scriptstyle \pi_2} & \\
E & & & & E' \\
 & {\scriptstyle g} \searrow & & \swarrow {\scriptstyle g'} & \\
 & & B & &
\end{array}$$

**Exercise 3** Show that $\Gamma$ is an $R$-module.

If it is, it is clearly a submodule of $E \oplus E'$, so we use the submodule criterion. We must show $\Gamma \neq \emptyset$ and $\mathbf{x} + r\mathbf{y} \in \Gamma$ for all $r \in R$ and $\mathbf{x}, \mathbf{y} \in \Gamma$. Clearly $\Gamma \neq \emptyset$, since $(0, 0) \in \Gamma$ as $g(0) = g'(0) = 0$. Now let $r \in R$ and $(x, x'), (y, y') \in \Gamma$. See that

$$g(x + ry) = g(x) + rg(y) = g'(x') + rg'(y') = g'(x' + ry'),$$

so $(x, x') + r(y, y') \in \Gamma$, and $\Gamma$ is an $R$-module, as desired.

**Exercise 4** Show that $\Delta = \{(f(t), -f'(t)) \mid t \in A\}$ is a submodule of $\Gamma$.

Now we really use the submodule criterion. $\Delta \neq \emptyset$ because $(0, 0) \in \Delta$, since $(0, 0) = (f(0), -f'(0))$ for $0 \in A$. And if $(x, x'), (y, y') \in \Delta$ and $r \in R$, then there is some $t \in A$ such that $(f(t), -f'(t)) = (x, x')$ and some $s \in A$ such that $(f(s), -f'(s)) = (y, y')$. Now see that

$$(x,x') + r(y,y') = \big(f(t), -f'(t)\big) + r\big(f(s), -f'(s)\big) = \big(f(t+rs), -f'(t+rs)\big) \in \Delta,$$

as $t + rs \in A$.

**Exercise 5** Show that $0 \to A \to {}^{\Gamma}\!/_{\Delta} \to B \to 0$ is an extension; i.e., show that it is a short exact sequence.

Define the maps to be

$$0 \to A \xrightarrow{F} {}^{\Gamma}\!/_{\Delta} \xrightarrow{G} B \to 0,$$

where $F(t) = (f(t), 0) \bmod \Delta$ and $G(e, e') \bmod \Delta = g(e)$. Note first that

$$F(t) = (f(t), 0) \bmod \Delta = (f(t), 0) - (f(t), -f'(t)) \bmod \Delta = (0, f'(t)) \bmod \Delta$$

and that

$$G(e, e') \bmod \Delta = g(e) = g'(e').$$

Also, $F$ is clearly well-defined, but $G$ not as clearly. If $(e_1, {e'}_1) \bmod \Delta = (e_2, {e'}_2) \bmod \Delta$, then

$$(e_1 - e_2, {e'}_1 - {e'}_2) \bmod \Delta = (f(t), -f'(t)) \bmod \Delta,$$

so $e_1 - e_2 \in \operatorname{im} f = \ker g$ and ${e'}_1 - {e'}_2 \in \operatorname{im} f' = \ker g'$. Thus

$$0 = g(e_1 - e_2) = g(e_1) - g(e_2), \text{ so } g(e_1) = g(e_2), \text{ and}$$
$$0 = g'({e'}_1 - {e'}_2) = g'({e'}_1) - g'({e'}_2), \text{ so } g'({e'}_1) = g'({e'}_2).$$

Thus $G$ is well-defined.

$F$ is injective because if $F(t) = (0,0) \bmod \Delta$, then $(f(t), 0) = (0, f'(t)) = (0,0) \bmod \Delta$, and since (overkilling) both $f$ and $f'$ are injective, $t = 0$. $G$ is surjective becase $G(e, e') \bmod \Delta = g(e) = g'(e')$ and $g$, $g'$ are surjective.

Now we show that $\operatorname{im} F = \ker G$. Let $(x, y) \bmod \Delta \in \operatorname{im} F$. Then there exists $t \in A$ such that $F(t) = (f(t), 0) \bmod \Delta = (0, f'(t)) \bmod \Delta = (x, y) \bmod \Delta$. Then compute

$$G(x, y) \bmod \Delta = g(x) = g'(y).$$

Since $x = f(t)$, $x \in \operatorname{im} f = \ker g$, so $g(x) = 0$. Identically we overkill and $y \in \operatorname{im} f' = \ker g'$, so $g'(y) = 0$. Thus $(x, y) \bmod \Delta \in \ker G$.

Let $(x, y) \bmod \Delta \in \ker G$. Then $G(x, y) = g(x) = g'(y) = 0$, so $x \in \ker g = \operatorname{im} f$ and $y \in \ker g' = \operatorname{im} f'$. So there exists $t, s \in A$ such that $f(t) = x$ and $f'(s) = y$. We need to show there exists $u \in A$ such that

$$F(u) = (f(u), 0) \bmod \Delta = (0, f'(u)) \bmod \Delta = (x, y) \bmod \Delta$$

Since

$$\begin{aligned}(x, y) \bmod \Delta &= (f(t), f'(s)) \bmod \Delta \\ &= (f(t), f'(s)) - (f(t), -f'(t)) \bmod \Delta \\ &= (0, f'(s + t)) \bmod \Delta,\end{aligned}$$

or symmetrically

$$\begin{aligned}(x, y) \bmod \Delta &= (f(t), f'(s)) \bmod \Delta \\ &= (f(t), f'(s)) + (f(s), -f'(s)) \bmod \Delta \\ &= (f(t + s), 0) \bmod \Delta,\end{aligned}$$

let $u = t + s$. Then

$$F(u) = F(t + s) = (f(t + s), 0) \bmod \Delta = (0, f'(t + s)) \bmod \Delta = (x, y) \bmod \Delta,$$

and $(x, y) \bmod \Delta \in \operatorname{im} F$. Thus $0 \to A \to {}^{\Gamma}\!/_{\Delta} \to B \to 0$ is exact, as desired.

**Exercise 6** Show that the set of equivalence classes of extensions $0 \to A \to E \to B \to 0$ under the binary operation $E \boxplus E' = {}^{\Gamma}\!/\!_{\Delta}$ is an $R$-module. We denote this module $\mathrm{Ext}^1_R(A,B)$. Show that its identity is the equivalence class of the split short exact sequence.

First, to see $\mathrm{Ext}^1_R(A,B)$ is an abelian group:

1. $\boxplus$ is closed by Exercise 5. It's well-defined on equivalence classes, since if

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & E & \xrightarrow{g} & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}_B} & & \\ 0 & \longrightarrow & A & \xrightarrow{f'} & E' & \xrightarrow{g'} & B & \longrightarrow & 0 \end{array}$$

   commutes (i.e., if $E \sim E'$), then we need to show $E \boxplus \widetilde{E} = E' \boxplus \widetilde{E}$. Observe that since $E \sim E'$, we can use the commutativity of the diagram to write

$$\begin{aligned} E \boxplus \widetilde{E} &= {\{(e,\widetilde{e}) \mid g(e) = \widetilde{g}(\widetilde{e})\}}\big/{\{(f(t), -\widetilde{f}(t))\}} \\ &= {\{(e,\widetilde{e}) \mid g'(\theta(e)) = \widetilde{g}(\widetilde{e})\}}\big/{\{(\theta^{-1}(f'(t)), -\widetilde{f}(t))\}}, \end{aligned}$$

   and since $\theta$ is an isomorphism,

$$\begin{aligned} &{\{(e,\widetilde{e}) \mid g'(\theta(e)) = \widetilde{g}(\widetilde{e})\}}\big/{\{(\theta^{-1}(f'(t)), -\widetilde{f}(t))\}} \\ &\cong {\{(e',\widetilde{e}) \mid g'(e') = \widetilde{g}(\widetilde{e})\}}\big/{\{(f'(t), -\widetilde{f}(t))\}} \\ &= E' \boxplus \widetilde{E}. \end{aligned}$$

2. For associativity, see that given

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & E & \xrightarrow{g} & B & \longrightarrow & 0, \\ 0 & \longrightarrow & A & \xrightarrow{f'} & E' & \xrightarrow{g'} & B & \longrightarrow & 0, \\ 0 & \longrightarrow & A & \xrightarrow{f''} & E'' & \xrightarrow{g''} & B & \longrightarrow & 0, \end{array}$$

we have

$$
\begin{aligned}
&E \boxplus (E' \boxplus E'') \\
&= E \boxplus {}^{\{(e', e'') \mid g'(e') = g''(e'')\}}\!\big/\!{}_{\{(f'(t), -f''(t))\}} \\
&= {}^{\{(e, (e', e'')) \mid g(e) = G'(e', e'') = g'(e') = g''(e'')\}}\!\big/\!{}_{\{(f(t), -(f'(t), -f''(t)))\}} \\
&= {}^{\{(e, e', e'') \mid g(e) = g'(e') = g''(e'')\}}\!\big/\!{}_{\{(f(t), -f'(t), f''(t))\}} \\
&= {}^{\{((e, e'), e'') \mid g(e) = g'(e') = G(e, e') = g''(e'')\}}\!\big/\!{}_{\{((f(t), -f'(t)), -f''(t))\}} \\
&= {}^{\{(e, e') \mid g(e) = g'(e')\}}\!\big/\!{}_{\{(f(t), -f'(t))\}} \boxplus E'' \\
&= (E \boxplus E') \boxplus E''
\end{aligned}
$$

The maps line up nicely because the short exact sequence of a ${}^{\Gamma}\!\big/\!{}_{\Delta}$ is just the maps modulo $\Delta$.

3. The identity element is (the equivalence class of) $E = A \oplus B$ in the extension $0 \to A \xrightarrow{\iota_1} A \oplus B \xrightarrow{\pi_2} B \to 0$. Clearly this is exact, as $\operatorname{im} f = A \oplus 0 = \ker g$. And for any $E$,

$$\Gamma = \{(e, (a, b)) \mid g(e) = b\} \cong \{(a, e) \mid g(e) = b\} = A \oplus E,$$

since $g$ is surjective, and

$$\Delta = \{(f(t), -(t, 0)) \mid t \in A\} \cong \{(-t, 0) \mid t \in A\} = A \oplus 0,$$

since $f$ is injective. Then $E \boxplus A \oplus B = {}^{\Gamma}\!\big/\!{}_{\Delta} = {}^{A \oplus E}\!\big/\!{}_{A \oplus 0} \cong E$. And $A \oplus B \boxplus E = E$ will come from abelian-ness.

4. The inverse of (the equivalence class of) $0 \to A \xrightarrow{f} E \xrightarrow{g} B \to 0$ is (the equivalence class of) $0 \to A \xrightarrow{f} E \xrightarrow{-g} B \to 0$. Indeed, see that

$$
\begin{aligned}
\Gamma &= \{(e_1, e_2) \mid g(e_1) = -g(e_2)\} \\
&= \{(e_1, e_2) \mid g(e_1 + e_2) = 0\} \\
&= \{(e_1, e_2) \mid e_1 + e_2 \in \ker g\} \\
&= \{(e_1, e_2) \mid e_1 + e_2 \in \operatorname{im} f\},
\end{aligned}
$$

so there exists a map $s : E \to A$ such that $s(e_1 + e_2) = x$ where $f(x) = e_1 + e_2$. We claim this map $s$ induces a section $S : {}^{\Gamma}\!/_{\Delta} \to A$, defined by $S(e, e') \bmod \Delta = x$ when $f(x) = e$, for the inclusion $F : A \hookrightarrow {}^{\Gamma}\!/_{\Delta}$ defined by $F(x) = (f(x), 0) \bmod \Delta$. First, note that $S$ is well-defined since $f$ is injective; if we wish to compute $S(e, e') \bmod \Delta$ and both $f(x) = e$ and $f(y) = e$, then since $f$ is injective, $x = y$. Now, to see the claim, observe that

$$\begin{aligned} SF(x) &= S(f(x), 0) \bmod \Delta \\ &= S(e_1 + e_2, 0) \bmod \Delta \\ &= x, \end{aligned}$$

and the claim is shown. This means that by Exercise 2,

$$0 \to A \xrightarrow{F} {}^{\Gamma}\!/_{\Delta} \xrightarrow{G} B \to 0$$

is split, and thus by definition equivalent to

$$0 \to A \to A \oplus B \to B \to 0,$$

the identity element.

5. Finally, to see that $\operatorname{Ext}^1_R(A, B)$ is abelian, see that

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \longrightarrow & E \boxplus E' & \longrightarrow & B & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & A & \longrightarrow & \{(e,e') \mid g(e) = g'(e)\} \big/ \{(f(t), -f'(t)) \mid t \in A\} & \longrightarrow & B & \longrightarrow & 0 \\
 & & \downarrow \mathrm{id}_A & & \downarrow \theta & & \downarrow \mathrm{id}_B & & \\
0 & \longrightarrow & A & \longrightarrow & \{(e',e) \mid g(e) = g'(e)\} \big/ \{(f'(t), -f(t)) \mid t \in A\} & \longrightarrow & B & \longrightarrow & 0 \\
 & & \| & & \| & & \| & & \\
0 & \longrightarrow & A & \longrightarrow & E' \boxplus E & \longrightarrow & B & \longrightarrow & 0,
\end{array}$$

where $\theta : E \boxplus E' \to E' \boxplus E$ is the map

$$\theta(e, e') \bmod (f(t), -f'(t)) = (e', e) \bmod (f'(t), -f(t)).$$

Clearly if $\theta$ is well-defined, then the squares above commute, and by the five lemma $\theta$ is an isomorphism. We just show that $\theta$ is well-defined. If

$$(e_1, {e_1}') = (e_2, {e_2}') \bmod (f(t), -f'(t)),$$

then

$$(e_1 - e_2, {e_1}' - {e_2}') = (f(t), -f'(t)) \bmod (f(t), -f'(t)),$$

and thus by swapping coordinates,

$$\begin{aligned}({e_1}' - {e_2}', e_1 - e_2) &= (-f'(t), f(t)) \bmod (-f'(t), f(t)) \\ &= (-f'(t), f(t)) - 2(-f'(t), f(t)) \bmod (-f'(t), f(t)) \\ &= (f'(t), -f(t)) \bmod (-f'(t), f(t)) \\ &= (f'(t), -f(t)) \bmod (f'(t), -f(t)),\end{aligned}$$

and so

$$({e_1}', e_1) = ({e_2}', e_2) \bmod (f'(t), -f(t)).$$

The left is $\theta(e_1, {e_1}')$ and the right is $\theta(e_2, {e_2}')$, so $\theta$ is indeed well-defined.

Next, to see that $\mathrm{Ext}^1_R(A,B)$ is an $R$-module, observe that $E \boxplus E' = {}^{\Gamma}\!/\!_{\Delta}$ is a quotient of $R$-modules (Exercises 3 and 4), hence an $R$-module. Then for $r, s \in R$ and equivalence classes $E = 0 \to A \to E \to B \to 0$ and $E' = 0 \to A \to E' \to B \to 0$ in $\mathrm{Ext}^1_R(A,B)$, we have

1.

$$r(E \boxplus E') = r(0 \to A \to {}^{\Gamma}\!/\!_{\Delta} \to B \to 0) = 0 \to rA \to r{}^{\Gamma}\!/\!_{\Delta} \to rB \to 0 = rE \boxplus rE';$$

2.

$$\begin{aligned}(r+s)E &= (r+s)(0 \to A \to E \to B \to 0)\\ &= 0 \to (r+s)A \to (r+s)E \to (r+s)B \to 0\\ &= 0 \to rA+sA \to rE+sE \to rB+sB \to 0\\ &= r(0 \to A \to E \to B \to 0) + s(0 \to A \to E \to B \to 0)\\ &= rE+sE;\end{aligned}$$

3.

$$\begin{aligned}(rs)E &= (rs)(0 \to A \to E \to B \to 0)\\ &= 0 \to (rs)A \to (rs)E \to (rs)B \to 0\\ &= 0 \to r(sA) \to r(sE) \to r(sB) \to 0\\ &= r(0 \to sA \to sE \to sB \to 0)\\ &= r(sE);\end{aligned}$$

4.

$$1E = 1(0 \to A \to E \to B \to 0) = 0 \to 1A \to 1E \to 1B \to 0 = 0 \to A \to E \to B \to 0 = E.$$