EPFL - Fall 2024	Domenico Valloni
Rings and modules	Exercises
Sheet 5 - Solutions	

Exercise 1. For two short exact sequences

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

and

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

we say that there is a map between them if there exists morphisms $f_i: M_i \to N_i$, for $1 \le i \le 3$ and a commuting diagram

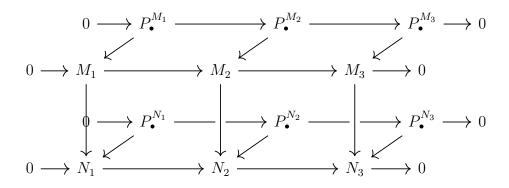
$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

$$\downarrow^{f_1} \qquad \downarrow^{f_2} \qquad \downarrow^{f_3}$$

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0.$$

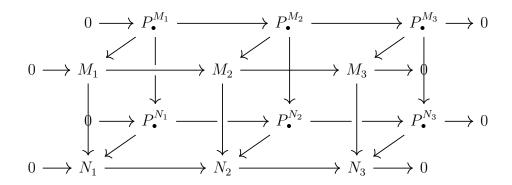
Show that whenever there is a map between two short exact sequences, then there is an induced map between long exact sequences of Ext-modules, making the suitable diagram commute.

Proof. By applying the *Horseshoe Lemma* 5.5.5 in the lecture notes there exists projective resolutions $P_{\bullet}^{M_i}$ of M_i and $P_{\bullet}^{N_i}$ of N_i for i = 1, 2, 3 and a commuting three dimensional diagram:



By Theorem 5.4.20 in the Lecture notes we can extend this diagram, by extending $f_i: M_i \to N_i$ to a (unique up to homotopy) morphism of chain complexes $f_{\bullet}: P_{\bullet}^{M_i} \to P_{\bullet}^{N_i}$ for

i = 1, 2, 3. Therefore we have a three dimensional diagram commuting up to homotopy:



Let K be some R-module, we can apply $\operatorname{Hom}_R(-,K)$ to the above diagram, then we get a diagram which commutes up to homotopy by Remark 5.4.15 and with the backside of the diagram still having exact rows as explained in (5.6.i) in the proof of Theorem 5.5.6. If we take cohomology we get an induced morphism $f_{i,j}:\operatorname{Ext}^j(M_i,K)\to\operatorname{Ext}^i(N_i,K)$ for every $j\geq 0$ and i=1,2,3 which commutes with the horizontal morphisms in the diagram by Proposition 5.4.17. We want to show that these morphisms commute with the connecting homomorphism (denoted δ_M and δ_N respectively) appearing in the long exact sequence Prop 4.5.1, i.e., from what has been said above we have a diagram:

$$\operatorname{Ext}^{i-1}(M_1, K) \xrightarrow{\delta_M} \operatorname{Ext}^i(M_3, K) \longrightarrow \operatorname{Ext}^i(M_2, K) \longrightarrow \operatorname{Ext}^i(M_1, K)$$

$$\downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow \qquad \qquad \downarrow \qquad ,$$

$$\operatorname{Ext}^{i-1}(N_1, K) \xrightarrow{\delta_N} \operatorname{Ext}^i(N_3, K) \longrightarrow \operatorname{Ext}^i(N_2, K) \longrightarrow \operatorname{Ext}^i(N_1, K)$$

where only the commutativity of the first square needs to be checked. I.e we are checking that the long exact sequence of cohomology (Proposition 5.5.1) is *functorial*. To this end we revisit the set up of Proposition 5.5.1. We use the notation in Proposition 5.5.1 to make it easier for the reader. To this end suppose we have a commutative diagram between cocomplexes, with exact rows:

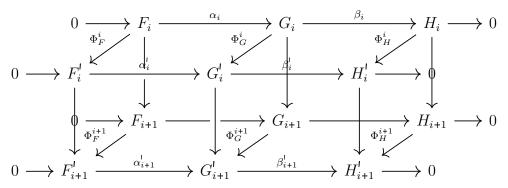
$$0 \longrightarrow F_{\bullet} \xrightarrow{\alpha_{\bullet}} G_{\bullet} \xrightarrow{\beta_{\bullet}} H_{\bullet} \longrightarrow 0$$

$$\downarrow^{\Phi_{F}} \qquad \downarrow^{\Phi_{G}} \qquad \downarrow^{\Phi_{H}} \qquad .$$

$$0 \longrightarrow F_{\bullet}^{I} \xrightarrow{\alpha_{\bullet}^{I}} G_{\bullet}^{I} \xrightarrow{\beta_{\bullet}^{I}} H_{\bullet}^{I} \longrightarrow 0$$

Where the structure morphism of the complexes are denoted f_i, g_i, h_i and f_i', g_i', h_i' respectively (as in Proposition 4.5.1). We want to check that the morphisms $\delta_i : H^i(H_{\bullet}) \to H^{i+1}(F_{\bullet}), \ \delta_i' : H^i(H_{\bullet}') \to H^{i+1}(F_{\bullet}')$ constructed in Proposition 4.5.1 commutes with the morphisms induced by Φ_F, Φ_H . To this end let $x \in H^i(H_{\bullet})$, and let $\bar{x} \in H_i$ be a lift of x. Let $y \in G_i$ be a preimage under β_i of x then $\Phi_G^i(y) \in G_i'$ is a preimage under β_i' of $\Phi_H^i(\bar{x})$.

The situation is illustrated by the following diagram:



Let now $z \in F_{i+1}$ be such that $\alpha_{i+1}(z) = g_i(y)$ (so that $\delta_i(x)$ is the class of z inside $H^{i+1}(F_{\bullet})$). It is sufficient to show that $\alpha'_{i+1}(\Phi^{i+1}_F(z)) = g'_i(\Phi^i_G(y))$. This follows by some easy diagram chasing as follow: We have $\alpha'_{i+1}(\Phi^{i+1}_F(z)) = \Phi^{i+1}_G(\alpha_{i+1}(z))$, but by definition we have $\alpha_{i+1}(z) = g_i(y)$. By the commutativity of the diagram $\Phi^{i+1}_G(g_i(y)) = g'_i(\Phi^i_G(y))$. Let now $x' \in H^i(H^i_{\bullet})$ be the image of x under the morphism induced by Φ_H . As $\alpha'_{i+1}(\Phi^{i+1}_F(z)) = g'_i(\Phi^i_G(y))$ and $\Phi^i_G(y)$ is a preimage under β'_i of $\Phi^i_H(\bar{x})$, which is a lift of x' to H^i_i , we obtain that $\delta'_i(x')$ is equal to the class of $\Phi^{i+1}_F(z)$ inside $H^{i+1}(F^i_{\bullet})$. The latter is by definition equal to the image of $\delta_i(x)$ under the morphism induced by Φ_F , which concludes the proof. \square

Exercise 2. In this exercise we prove the two 4-lemmas. To this end, suppose that we have a commuting diagram with exact rows:

$$\begin{array}{cccc}
A & \xrightarrow{f_1} & B & \xrightarrow{f_2} & C & \xrightarrow{f_3} & D \\
\downarrow^a & & \downarrow_b & & \downarrow^c & & \downarrow_d \\
A' & \xrightarrow{f_1'} & B' & \xrightarrow{f_2'} & C' & \xrightarrow{f_3'} & D'
\end{array}$$

- (1) Show that if a and c are surjective and d is injective, then b is surjective.
- (2) Show that if b and d are injective and a is surjective, then c is injective
- Proof. (1) Let $\beta' \in B'$, we want to show that there exists $\beta \in B$ such that $b(\beta) = \beta'$. To this end, since c is surjective there exists $\gamma \in C$ such that $c(\gamma) = f_2'(\beta')$. By commutativity we get $df_3(\gamma) = f_3'c(\gamma) = f_3'f_2'(\beta')$. By exactness of the rows $f_3'f_2'(\beta') = 0$ and hence $f_3(\gamma) \in \ker(d)$. By assumption $\ker(d) = 0$ and hence (using exactness of the rows) $\gamma \in \operatorname{im}(f_2)$. Let $\beta_1 \in B$ be such that $f_2(\beta_1) = \gamma$. We have $f_2'(b(\beta_1) \beta') = 0$, by commutativity and definition of β_1 and γ . By exactness of the lower row there therefore exists $\alpha' \in A'$ such that $f_1'(\alpha') = b(\beta_1) \beta'$. By assumption a is surjective, so let $\alpha \in A$ be such that $a(\alpha) = \alpha'$. We have $bf_1(\alpha) = b(\beta_1) \beta'$ by commutativity. Let $\beta = \beta_1 f_1(\alpha)$, then $b(\beta) = b(\beta) b(\beta) + \beta' = \beta'$. We conclude that b is an epimorphism.
- (2) Let $\gamma \in C$ be such that $c(\gamma) = 0$; we want to show that $\gamma = 0$. By commutativity we have $df_3(\gamma) = f_3'c(\gamma) = 0$, and by injectivity of d it follows that $f_3(\gamma) = 0$. By exactness of the rows we get $\gamma \in \text{im}(f_2)$, so let $\beta \in B$ be such that $f_2(\beta) = \gamma$. Now again by commutativity we have $f_2'b(\beta) = cf_2(\beta) = 0$ and thus by exactness of the rows there exists $\alpha' \in A'$ such that $f_1'(\alpha') = b(\beta)$. Then by surjectivity of a we can also

take $\alpha \in A$ with $a(\alpha) = \alpha'$. Thus we get by commutativity $bf_1(\alpha) = f'_1 a(\alpha) = b(\beta)$, and by injectivity of b it follows that $f_1(\alpha) = \beta$. But thus $\gamma = f_2(\beta) = f_2 f_1(\alpha)$, which by exactness gives $\gamma = 0$. Hence γ is a monomorphism.

Exercise 3. 1

- (1) Set $k = \mathbb{F}_p$ and $G = \mathbb{Z}/p\mathbb{Z}$. Find all the submodules (i.e. ideals) of R = k[G]. [Hint: To understand $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ in terms of more common rings, it might be a good idea to look for ring morphisms $\mathbb{F}_p[x] \to \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ and investigate both kernel and image.]
- (2) For p = 2, let x denote a generator of G and set $M = (x + 1) \subseteq k[G]$. Compute $\operatorname{Ext}_R^i(M, M)$ for all $i \ge 0$.
- *Proof.* (1) We define a k-algebra morphism (i.e. a ring morphism that is also k-linear) $\Phi: k[x] \to k[G]$ by mapping $x \mapsto \delta_g$, where δ_{\bullet} is defined as in the hint and $g \in G$ is a generator (such a morphism always exists by the universal property of k[x]). Then notice that

$$\Phi(x^p - 1) = (\delta_q)^p - 1 = \delta_{q^p} - 1 = \delta_{e_G} - 1 = 0$$

and thus $(x^p-1) \subseteq \text{Ker } \Phi$. Thus we obtain a k-algebra map $\phi: k[x]/(x^p-1) \to k[G]$. Now as the image contains $\{\delta_{g^i}\}_{0 \le i < p}$ which is a k-basis of k[G], we get that ϕ is a surjective map of k-vector spaces of dimension p. Hence ϕ is an isomorphism.

Now the ideals of $k[x]/(x^p-1)$ are in one-to-one correspondence with the ideals I of k[x] containing x^p-1 . Notice that $x^p-1=(x-1)^p$ as we are in characteristic p, and thus as k[x] is a PID we obtain that the ideals of k[x] containing x^p-1 are exactly $I_i=((x-1)^i)$ for $0 \le i \le p$. Translating this to k[G], we obtain that the ideals of k[G] are precisely $\Phi(I_i)=((\delta_q-1)^i)$ for $0 \le i \le p$.

(2) Denote R = k[G]. The map $R \to M$ mapping $r \in R$ to r(x+1) is clearly surjective. To compute the kernel, suppose that r(x+1) = 0. By the isomorphism ϕ of the previous point, we can view this as an equation inside $k[x]/(x^2-1)$. As $x^2-1=(x+1)^2=0$, we see that the solutions to the equation are precisely the multiples of x+1. That is, the kernel of $R \to M$ is again M. Hence we get a free resolution

$$\cdots \rightarrow R \rightarrow R \rightarrow R \rightarrow M \rightarrow 0$$

where all the arrows are just multiplication by x+1. Dropping the M from the sequence and applying $\operatorname{Hom}_R(-,M)$, and under the identification $\operatorname{Hom}_R(R,M) \cong M$, we obtain the sequence

$$\cdots \leftarrow M \leftarrow M \leftarrow M \leftarrow 0$$

where again every map is multiplication by x + 1. But as $(x + 1)^2 = 0$ in M, every map is equal to 0, and thus all cohomology groups are equal to M. Thus $\operatorname{Ext}_R^i(M, M) = M$ for all $i \ge 0$.

as modules over k[G] correspond to representations of G over k, we see that something is really wrong for $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ compared to the case of exercise 3.

Exercise 4. In this exercise we define injective modules and prove Baer's criterion. Let R be a (not necessarily commutative) ring; any R-module and any R-morphism appearing in this exercise will be a left R-module resp. a morphism of left R-modules.

We say that an R-module Q is injective if it satisfies the following universal property:

Whenever we have an injective R-morphism $f: X \hookrightarrow Y$ and an R-morphism $g: X \to Q$, then there exists an R-morphism $h: Y \to Q$ making the following diagram commute:

$$0 \longrightarrow X \xrightarrow{f} Y$$

$$\downarrow_{g} \qquad h$$

$$Q$$

We will prove the following:

Theorem (Baer's Criterion). Suppose that the left R-module Q has the property that if I is any left ideal of R and $f: I \to Q$ is an R-morphism, there exists an R-morphism $F: R \to Q$ extending f. Then Q is an injective R-module.

We will prove Baer's criterion in several steps. Assume that the R-module Q satisfies Baer's criterion.

- (1) Let X, Y be R-modules, and assume that Y is cyclic (generated by $b \in Y$). Let $f: X \hookrightarrow Y$ be an injective R-morphism. Show that for every R-morphism $g: X \to Q$, there exists an R-morphism $h: Y \to Q$ making the appropriate diagram commute. [Hint: Identify X with a submodule of Y and consider the subset I of R defined by $I = \{r \in R : rb \in X\}$.]
- (2) Let X, Y be left R-modules with an injective R-morphism $f: X \hookrightarrow Y$ (we identify X with its image under f). Let $b \in Y$ be arbitrary. With a similar approach as in the previous point, prove that any R-morphism $g: X \to Q$ can be extended to an R-morphism $h: X + Rb \to Q$ making the appropriate diagram commute.
- (3) Use Zorn's Lemma to conclude the proof.

Axiom 1 (Zorn's Lemma / Axiom of Choice). If (\mathcal{P}, \leq) is a partially ordered set with the property that every totally ordered subset (often called a chain) has an upper bound, then there exists a maximal $M \in \mathcal{P}$. (that is, for $N \in \mathcal{P}$, we have $M \nleq N$)

[Hint: Try to think of what it means for one partial extension of $g: X \to Q$ to be smaller than another.]

- Proof. (1) Let $I = \{r \in R | rb \in X\}$ where we consider $Ra \subseteq Rb$ via f; it is straightforward to check that this is an ideal. Then the map $l: I \to Q$ defined by l(r) = g(rb) is a homomorphism, so we can extend to $L: R \to Q$, by the hypothesis. Define $h: Rb \to Q$ by h(rb) = L(r). This is well-defined because if rb = r'b, then $r r' \in I$ and thus L(r-r') = g((r-r')b) = 0. Also, it is straightforward to check that h is an R-morphism extending g, so we are done.
- (2) As above, let $I = \{r \in R | rb \in X\}$ and extend $l: I \to Q$ defined by l(r) = g(rb) to $L: R \to Q$. Then we can define $h: X + Rb \to Q$ by h(x + rb) = g(x) + L(r). To show that this is well-defined, assume that x + rb = x' + r'b. Then $(r r')b = x' x \in X$ and thus $r r' \in I$, which implies

$$a(x-x') + L(r-r') = a(x-x') + a(r(b-b')) = 0.$$

Furthermore, it is straightforward to check that h is an R-morphism extending g, so we are done.

(3) Say that $X \subset Y$ and $g: X \to Q$ is a homomorphism. Consider the set

$$\mathcal{P} = \{ (X', g') \mid X \subseteq X' \subseteq Y, g' : X' \to Y, g|_{X} = g \}.$$

We can define a partial order \leq on \mathcal{P} as follows: $(X',g') \leq (X'',g'')$ if and only if $X' \subseteq X''$ and $g''|_X' = g'$. Then if $\{(X_i',g_i')\}_{i\in\Omega}$ is a totally ordered subset indexed by some set Ω , we can form $\bigcup_{i\in\Omega}f_i:\bigcup_{i\in\Omega}A_i\to Q$, which then is an upper bound to the chain. Hence there exists a maximal $h:X'\to Q$, by Zorn's Lemma.

Now if we have some $b \in Y - X'$, we can extend h to X' + Rb, by the previous point. This contradicts the maximality of h, so we must have X' = Y, and we are done.

Exercise 5. Use Baer's Criterion to show that \mathbb{Q} is an injective \mathbb{Z} -module.

Proof. Let I be an ideal of \mathbb{Z} , then $I = n\mathbb{Z}$ some $n \in \mathbb{Z}$. Let $g : n\mathbb{Z} \to \mathbb{Q}$ be a group homomorphism. If n = 0 then the zero map from \mathbb{Z} to \mathbb{Q} extends g. Otherwise suppose $g(n) = \frac{a}{b}$. We can extend f by $h : \mathbb{Z} \to \mathbb{Q}$ defined by $h(k) = \frac{ka}{nb}$ for all k.