Math250aHw4

Trustin Nguyen

December 9, 2023

Exercise 1: Let R be a ring. In the following, "module" means left R-module, and maps are homomorphisms of left R-modules

Definition: A module P is projective if for every short exact sequence of modules

$$0 \longrightarrow M' \xrightarrow{a} M \xrightarrow{b} M'' \longrightarrow 0$$

and every map $c : P \to M''$ there exists a map $d : P \to M$ making the diagram

$$\begin{tikzcd} & & & P \arrow[dl, "d"'] \arrow[d, "c"] & \\ 0 \arrow[r] & M' \arrow[r, "a"] & M \arrow[r, "b"] & M'' \arrow[r] & 0 \end{tikzcd}$$

commute, that is, $bd = c$.

(a) Prove that every free module is projective.

Proof. We know that the mapping c is determined by its action on the generators in $f_i \in P$. So suppose:

$$c(f_i) = m_i \in M''$$

Now because b is surjective, we have some $x_i \in M$ such that

$$b(x_i) = m_i$$

Then define the module homomorphism such that

$$d(f_i) = x_i$$

Now we just need to prove that d is a module homomorphism. For f_i, f_j:

$$\begin{tikzcd} f_i + f_j \arrow[r, "?"] \arrow[rr, bend right, "c"'] & x_i + x_j \arrow[r, "b"] & m_i + m_j \end{tikzcd}$$

Since $f_i + f_j \neq 0$ as we are in a free module, we can define $d(f_i + f_j) = x_i + x_j$. Now if $r \in R$, we have that $rf_i \neq 0$ because it is a free module. Similarly, we can define $d(rf_i) = rd(f_i)$. These two make d into a module homomorphism. So we are done as $bd = c$. □

(b) Prove that every projective module is a direct summand of a free module, and conversely, every direct summand of a free module is projective.

Proof. ($\rightarrow$) If our module is projective, then consider the direct sequence with a mapping from a free module F to a projective module P:

$$\begin{tikzcd}
 & & & P \arrow[dl] \arrow[d] & \\
0 \arrow[r] & M' \arrow[r] & F \arrow[r] & P \arrow[r] & 0
\end{tikzcd}$$

Since there is a splitting, we have $F = M' \oplus P$.

($\leftarrow$) Suppose that we have a direct summand of a free module F as $F = N \oplus M$. Then we have that by definition, we can always find a d_1 for any homomorphism c that makes the diagram:

$$\begin{tikzcd}
 & & & F \arrow[dl, "d_1"'] \arrow[d, "c"] & \\
0 \arrow[r] & M''' \arrow[r] & M' \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

Now we want to show that for any homomorphism $c' : M \to M''$, we can find a d that makes the diagram commute.

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, shift left, "\mathrm{id}"] \arrow[dr, "d"'] & F \arrow[l, shift left, "\mathrm{proj}"] \arrow[r, shift left, "\mathrm{proj}"] \arrow[d, "d_1"] \arrow[dr, "c"] & N \arrow[l, shift left, "\mathrm{id}"] \arrow[r] & 0 \\
0 \arrow[r] & M''' \arrow[r] & M' \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

But we can just consider that $c' = c \circ \mathrm{id}$ and we compose the mappings $d_1 \circ \mathrm{id} = d$. So we have found a mapping. $\square$

Exercise 2: Reversing the direction of all the arrows, a module E is called *injective* if for every short exact sequence of modules

$$\begin{tikzcd}
0 & M' \arrow[l] & M \arrow[l, "a"'] & M'' \arrow[l, "b"'] & 0 \arrow[l]
\end{tikzcd}$$

and every map $c : M'' \to E$ there exists a map $d : M \to E$ making the diagram

$$\begin{tikzcd}
 & & & E & \\
0 & M' \arrow[l] & M \arrow[l, "a"'] \arrow[ur, "d"] & M'' \arrow[l, "b"'] \arrow[u, "c"'] & 0 \arrow[l]
\end{tikzcd}$$

commute, that is, $bd = c$.

Prove that a module is injective if and only if it has the apparently weaker property:

(*): If

$$\begin{tikzcd}
0 & M' \arrow[l] & M \arrow[l, "a"'] & E \arrow[l, "b"'] & 0 \arrow[l]
\end{tikzcd}$$

is a short exact sequence, then there is a map $d : M \to E$ such that db is the identity map of E (and thus $M \cong E \oplus M'$) – the special case where the map c is the identity.

Hint: Let $N = E \oplus M/(\Delta(M''))$ where $\Delta(e) = (c(e), b(e))$, called the *pushout* of (c, b). Let $b' : E \to N$ be the map sending e to $(e, 1) \mod \Delta(M'')$. Show that

$$\begin{tikzcd}
0 & M' \arrow[l] & N \arrow[l, "a"'] & E \arrow[l, "b'"'] & 0 \arrow[l]
\end{tikzcd}$$

is also a short exact sequence, and use the property $(*)$.

Proof. ($\rightarrow$) Suppose that we have

$$
\begin{tikzcd}
 & & & E & \\
0 & M' \arrow[l] & M \arrow[l, "a"'] \arrow[ur, "d"] & M'' \arrow[l, "b"'] \arrow[u, "c"'] & 0 \arrow[l]
\end{tikzcd}
$$

where E is injective. Then let $M'' = E$ and $c = \mathrm{id}$.

$$
\begin{tikzcd}
 & & & E & \\
0 & M' \arrow[l] & M \arrow[l, "a"] \arrow[ur, "d"] & E \arrow[l, "b"] \arrow[u, "\mathrm{id}"'] & 0 \arrow[l]
\end{tikzcd}
$$

So we have the diagram commuting and $db = \mathrm{id}$.

($\longleftarrow$) Consider the hint and the diagram we get from it:

$$
\begin{tikzcd}
0 & M' \arrow[l] & M \arrow[l, "a"'] \arrow[d, "i_2"] & M'' \arrow[l, "b"'] \arrow[d, "c"] \arrow[dl, "\Delta"] & 0 \arrow[l] \\
0 & E \oplus M/(\Delta(M'')) \arrow[l] \arrow[u, "a'"] \arrow[ur, "\pi"] & E \oplus M \arrow[l] & E \arrow[l, "i_1"] \arrow[ll, bend left, "b'"] & 0 \arrow[l]
\end{tikzcd}
$$

We will show that

$$
\begin{tikzcd}
0 & M' \arrow[l] & N \arrow[l, "a"'] & E \arrow[l, "b'"'] & 0 \arrow[l]
\end{tikzcd}
$$

is an exact sequence.

(Injectivity) By definition, the kernel of b' are elements $e \in E$ such that $(e, 0) \in \Delta(M'')$. So we see that since M'' is injective, we conclude that only $0 \in M'' \mapsto 0$ from the action of b. Therefore, there can only be one element in the kernel of b' which is 0. So b' is injective. Now the image of b' are just copies of e in $E \oplus M/(\Delta(M''))$ since b' is injective.

(Surjectivity) Now we take the mapping $\pi : E \oplus M/(\Delta(M''))$ to be the projection of $E \oplus M/(\Delta(M''))$ onto M. This is a surjective mapping, and because $a : M \to M'$ is also surjective, we have $a' = a \circ \pi$ is surjective.

($\mathfrak{I}b' = \ker a'$) Clearly, by our mapping of π, the kernel is the copy of E in $E \oplus M/(\Delta(M''))$. We also have that $\mathfrak{I}b$ should be the kernel of a'. But the image is 0 in the quotient $E \oplus M/(\Delta(M''))$. Therefore, $\mathfrak{I}b' = \ker a'$ as desired.

(*): Since we have a direct sequence, we conclude that there is a d' such that $d'b' = \mathrm{id}$:

$$
\begin{tikzcd}
 & & & M \arrow[dll, bend right] \arrow[dr, "d"] & M'' \arrow[l] \arrow[d] & 0 \arrow[l] \\
0 & M' \arrow[l] & N \arrow[l, "a"'] \arrow[ur, "\pi"] \arrow[rr, shift left, "d'"] & & E \arrow[ll, shift left, "b'"] & 0 \arrow[l]
\end{tikzcd}
$$

Therefore, for some $n_i \in N$, we have $d'(n_i) = e'_i \in E$. And by π, $\pi((e_i, m_i) + \Delta(M'')) = m_i$. So now we take $d : m_i \mapsto e'_i$ which makes the diagram commute? □

Group Theory:

Exercise 1: Show that if G is a group such that $g^2 = 1$ for all $g \in G$, then G is abelian.

Proof. Since $g^2 = e$, we have $g = g^{-1}$. Now consider the element

$$ghg^{-1}h^{-1} = ghgh = (gh)^2 = e$$

Since the commutator subgroup is a normal subgroup, we take the quotient to get an abelian group. So $G/\{e\} = G$ is abelian. □

Exercise 2: Show that the group of automorphisms of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ is the multiplicative group of integers relatively prime to n, modulo n. Show that this group is cyclic if n is prime (Hint: $\mathbb{Z}/p\mathbb{Z}$ is a field), and find a decomposition of this group into cyclic groups in case $n = 9$.

Proof. (Part I) Notice that all automorphisms of $\mathbb{Z}/n\mathbb{Z}$ are of the form

$$n \mapsto an$$

for some $a \in \mathbb{Z}$. For this map to be an isomorphism, we just require a surjection or for there to be an inverse for a. We will show that a is invertible iff it is relatively prime to n.

If b is relatively prime to n, we have that $(b) \subseteq \mathbb{Z}$ an ideal of the integers is a PID, and that $(b, n) = \mathbb{Z}$. Therefore, we have that

$$1 = ab + nc$$

for some $a, c \in \mathbb{Z}$. Indeed

$$ab + nc \equiv ab \equiv 1 \pmod{n}$$

so we have found an inverse a. Now we need to show that this inverse is also relatively prime to n. We can do this by proving the converse of the previous statement. Suppose we have a, b such that

$$ab \equiv 1 \pmod{n}$$

Suppose for contradiction that $\mathrm{gcd}\left(() a, n\right) = p$ where $p \neq 0, n$, otherwise the above expression is false. Then

$$pk_1 = n$$
$$pk_2 = a$$

So we have

$$pk_2 b \equiv 1 \pmod{n}$$

or

$$pk_1 k_2 b \equiv k_1 \equiv 0 \pmod{n}$$

which is a contradiction. So elements that have inverses are exactly the ones that are relatively prime to n. So all automorphisms are determined by

$$1 \mapsto a$$

where a is relatively prime to n, so the multiplicative group on $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the group of automorphisms on $\mathbb{Z}/n\mathbb{Z}$ by choosing a to be our representative of the automorphism.

Since we have a composition of $\mathbb{Z}/p\mathbb{Z}$ into a direct sum of cyclic groups, each of order dividing the next, we have

$$\mathbb{Z}/p\mathbb{Z} \cong \bigoplus_i \mathbb{Z}/q_i\mathbb{Z}$$

for $q_1 \mid q_2 \mid \cdots \mid q_n$. If d is the largest order of an element of the group, then we know that for all $g \in \mathbb{Z}/p\mathbb{Z}$,

$$g^d = 1$$

Also, $x^d - 1 = 0$ has at most d solutions and can be factored as

$$(x - r_1) \cdots (x - r_d) = 0$$

Otherwise, if we have more solutions, we get that all factors, non-zero multiply to 0. But $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, which is a contradiction. So since d is the power such that

$$x^d - 1 = 0$$

for any $x \in \mathbb{Z}/p\mathbb{Z}$, If $d \neq p-1$, then we find out that the equation has $p-1 > d$ solutions, contradiction. So $d = p-1$. There is an element of order $p-1$, the order of the group. So $\mathbb{Z}/p\mathbb{Z}$ is cyclic.

(Part III) We have that

$$\mathbb{Z}/9\mathbb{Z} = \{1, 2, 4, 5, 7, 8\}$$

Now we find the orders of each element:

$$1, 6, 3, 6, 3, 2$$

so for primes $p = 2, 3$, we follow the decomposition steps:

$$\mathbb{Z}/p\mathbb{Z} \cong \{1, 8\} \oplus \{1, 4, 7\}$$

which is the decomposition. ☐

Exercise 3: Show that if $H < G$ is a subgroup of a finite group G, and $G : H = p$ where p is the smallest prime dividing $|G|$, then H is normal (the case $p = 2$ is done in Lang.)

Proof. Consider the action of G on the permutations of the cosets of G by left multiplication:

$$\varphi : G \circlearrowleft \mathrm{Aut}(G/H)$$
$$\varphi : g \mapsto (rH \mapsto grH)$$

Notice that the kernel is a subgroup of H. Using the fact that

$$|G : \ker\varphi| = |G : H||H : \ker\varphi|$$

we consider the fact that $G/\ker\varphi$ gives us an injective and surjective mapping into the image of φ which is a subgroup of the group of automorphisms on G/H. Then the order of this group divides $p!$. Furthermore, we have $|G : H| = p$. Therefore:

$$|H : \ker\varphi| \,\Big|\, (p-1)!$$

to which we conclude that $|H : \ker\varphi| = 1$, otherwise, we can find a smaller prime that divides $H/\ker\varphi$ and therefore, G. ☐