Math 101 Fall 2013
Homework #2
Due 2 October 2013

1. Let $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\pi} M'' \longrightarrow 0$ be a short exact sequence of R-modules. Show that if i has a retraction $r : M \to M'$, then $M \cong M' \oplus M''$.

ANS: From a result in lecture, it suffices to see that π has a section. For this it suffices to see that $\pi|_{\ker r}$ is an isomorphism onto M''. (Then our section is just the inverse.)

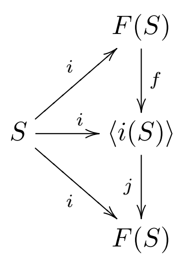
But if $m \in \ker \pi \cap \ker r$, then $m = i(m')$. But then $m' = r \circ i(m') = 0$. Thus, $m = 0$ and $\pi|_{\ker r}$ is injective.

But if $m'' \in M''$, then $m'' = \pi(m)$ for some $m \in M$. Consider $y := m - i \circ r(m)$. Then on the one hand, $\pi(y) = \pi(m) = m''$. On the other hand, $r(y) = r(m) - r(m) = 0$. Thus $y \in \ker r$, and $\pi|_{\ker r}$ is surjective. This completes the proof.

2. Let M be an R-module and let $S \subset M$ be a subset. Show that there is a smallest submodule, $\langle S \rangle$, of M containing S. We say that $\langle S \rangle$ is the submodule generated by S. Of course, if $\langle S \rangle = M$, then we say that S generates M. Now let S be any set and $F(S)$ together with $i : S \to F(S)$ a free module on S. Show that $F(S)$ is generated by $i(S)$.

ANS: As mentioned in lecture, $\langle S \rangle$ is just the intersection of all submodules of M containing S.

Let $j : \langle i(S) \rangle \to F(S)$ be the inclusion map. The UMP of $F(S)$ says that there is a module map $f : F(S) \to \langle i(S) \rangle$ such that the diagram



commutes. But the UMP also ensures that $j \circ f$ is the identity. Hence j is surjective and $\langle i(S) \rangle = F(S)$.

3. Give an example of a group G with subgroups H and K such that $HK = \{ hk : h \in H \text{ and } k \in K \}$ is not a subgroup of G. (Groups start to get interesting at $G = S_3$.)

ANS: Let $G = S_3$ the set of permutations on $\{1, 2, 3\}$. Let $H = \langle (1\ 2) \rangle$ and $K = \langle (2\ 3) \rangle$. We have $H \cap K = \{1\}$ so $|HK| = 4$. But $4 \nmid 6 = |G|$. Hence HK can't be a subgroup.

4. Let $\mathbf{Q}$ be the additive group of rationals. Show that $\mathbf{Q}$ is indecomposable as a $\mathbf{Z}$-module: that is, show that it is not possible to write $\mathbf{Q} \cong A \oplus B$ for $\mathbf{Z}$-modules A and B. Conclude that $\mathbf{Q}$ is not a free $\mathbf{Z}$-module.

ANS: Suppose that $\mathbf{Q} = A \oplus B$ as $\mathbf{Z}$-modules. Assuming, as you should, that A and B are both nonzero, let $\frac{a}{b} \in A$ and $\frac{c}{d} \in B$ be nonzero rational numbers. Then $bc \cdot \frac{a}{b} = ac \in A$ and $ad \cdot \frac{c}{d} = ac \in B$. Since $A \cap B = \{0\}$, we must have $ac = 0$. But as $\mathbf{Z}$ is an integral domain, this forces either a or c to be zero contradicting our choices above. Thus $\mathbf{Q}$ is indecomposable.

If $\mathbf{Q}$ were free on more than one generator, then $\mathbf{Q}$ would decompose nontrivially. Hence the only way $\mathbf{Q}$ could be free is to be isomorphic to $\mathbf{Z}$ as a $\mathbf{Z}$-module. That is, $\mathbf{Q}$ would have to be isomorphic to $\mathbf{Z}$ as abelian groups. But this is impossible since every nonzero element in $\mathbf{Q}$ has a "square root"; that is, given $x \in \mathbf{Q} \setminus \{0\}$, there is a $y \in \mathbf{Q}$ such that $2 \cdot y = x$. But this fails for lots of elements in Z — for example, $2 \cdot x = 1$ has no solution in $\mathbf{Z}$.

5. Let $\mathbf{Q}^\times$ be the multiplicative group of nonzero rational numbers. Show that as a $\mathbf{Z}$-module, $\mathbf{Q}^\times \cong \left(\coprod_{i=1}^\infty \mathbf{Z}\right) \oplus \mathbf{Z}_2$. (First write $\mathbf{Q}^\times \cong H \oplus K$ where $H = \{\, q \in \mathbf{Q}^\times : q > 0 \,\}$. Let $\{p_i\}$ be the set of primes in $\mathbf{N}$ and define $\phi_i : \mathbf{Z} \to H$ by $\phi_i(k) = p_i^k$.)

ANS: Since $H \cap K = \{1\}$ and $HK = \mathbf{Q}^\times$, we have $\mathbf{Q}^\times \cong H \oplus K$ as an internal direct sum. Since $K \cong \mathbf{Z}_2$, it only remains to show that $H \cong \coprod_{i=1}^\infty \mathbf{Z}$ as $\mathbf{Z}$-modules (or as abelian groups). Define the ϕ_i as above and observe that these are $\mathbf{Z}$-module homomorphisms: $\phi_i(n+m) = p_i^{n+m} = p_i^n p_i^m = \phi_i(n)\phi_i(m)$. Hence the UMP of the coproduct gives us a unique homomorphism $\phi : \coprod_{i=1}^\infty \mathbf{Z} \to H$ given by

$$\phi\big((e_i)\big) = \prod_{i=1}^{\infty} \phi_i(e_i) = p_1^{e_1} p_2^{e_2} \cdots$$

which makes sense since all but finitely many terms in the two products are 1. However, by the fundamental theorem of arithmetic, every $n \in Z$ factors uniquely as $p_1^{e_1} p_2^{e_2} \cdots$ where the $e_i \geq 1$ and only finitely many are not equal to 1. But any positive rational number has the form $r = \frac{n}{m}$ with $(n, m) = 1$. Thus if we write n as above and $m = p_1^{f_1} p_2^{f_2} \cdots$, then for each i at most one of e_i and f_i are different from 1. It follows that r has a unique expression as $p_1^{e_1} p_2^{e_2} \cdots$ where now the e_i are integers all but finitely many of which are 1. It now follows that ϕ is a bijection. This completes the proof.

6. In lecture, we proved that if R is a *commutative* ring, then $R^n \cong R^m$ as R-modules if and only if $n = m$. If R is not commutative, this is no longer true. Show that if V is a (countably) infinite dimensional k-vector space and if $R = \operatorname{End}_k(V) = \hom_k(V, V)$, then $R \cong R \oplus R$ (as R-modules). (You might want to start by observing that $\hom_k(V, V)$ has a nice ring structure.)

ANS: Let V be a k-vector space of countably infinite dimension with basis $\beta = \{\, e_i \,\}_{i=1}^\infty$. First we observe that $\hom_k(V, V)$ is just the set of linear maps from V to itself. Hence it has an obvious vector space structure and a ring structure (multiplication is given by composition). The vector space direct sum $V \oplus V$ has basis $\{(e_i, 0)\} \cup \{(0, e_j)\}_{j=1}^{\infty}$. Then we get a vector space isomorphism $\phi : V \oplus V \to V$ by defining

$$\phi(e_i, 0) = e_{2i} \quad \text{and} \quad \phi(0, e_j) = e_{2j-1},$$

and extending linearly. This induces a vector space isomorphism $\phi^* : \hom_k(V, V) \to \hom_k(V \oplus V, V)$ given by $T \mapsto T \circ \phi$.

Similarly, from a previous homework problem, we have a vector space isomorphism

$$\sigma : \hom_k(V \oplus V, V) \to \hom_k(V, V) \oplus \hom_k(V, V)$$

given by $f \mapsto (f \circ i_1, f \circ i_2)$ for the natural inclusions $i_j : V \to V \oplus V$. Thus by compostion we obtain a vector space isomorphism $\psi : \hom_k(V, V) \to \hom_k(V, V) \oplus \hom_k(V, V)$ given by

$$\hom_k(V, V) \xrightarrow{\phi^*} \hom_k(V \oplus V, V) \xrightarrow{\sigma} \hom_k(V, V) \oplus \hom_k(V, V) \ :$$

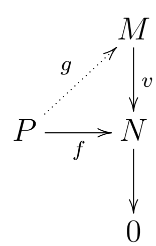
thus, $\psi(T) = (T \circ \phi \circ i_1, T \circ \phi \circ i_2)$.

Now we consider $R = \hom_k(V, V)$ as a ring. Then ψ will be a R-module map if it preserves the R-action. The R action on R is just multiplication and on $R \oplus R$ is given by multiplication in each coordinate. But

$$\phi(S \cdot T) = \phi(ST) = (ST \circ \phi \circ i_1, ST \circ \phi \circ i_2) = S \cdot (T \circ \phi \circ i_1, T \circ \phi \circ i_2) = S \cdot \psi(T).$$

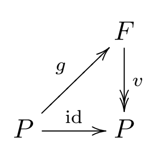
This completes the proof.

7. An R-module P is called *projective* if whenever we have an R-module epimorphism $v : M \to N$ and R-module map $f : F \to N$ there is an R-module map g lifting f in the sense that the diagram



commutes. (Note that g is not required to be unique.) Show that P is projective if and only if P is a direct summand of a free R-module (i.e., there is an R-module Q such that $P \oplus Q$ is free).

ANS: First, suppose that P is projective. Since P is an R-module, there is a free module F and a surjection $v : F \to P$. Then there is a map g such that the diagram



commutes. But then the short exact sequence

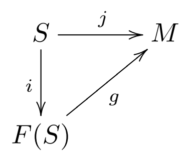
$$0 \longrightarrow \ker v \longrightarrow F \xrightarrow{v} P \longrightarrow 0$$

has a section, namely g, for v. Hence $F \cong \ker v \oplus P$.

For the converse, we first prove a lemma:

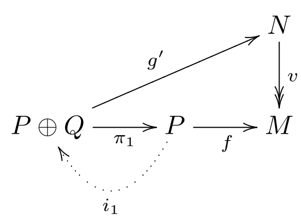
Lemma. *Free modules are projective.*

Proof. Suppose $F = F(S)$ with $i : S \to F(S)$ the universal map. Suppose that $v : N \to M$ is a surjective module map with $f : F(S) \to M$ another module map. Since v is surjective, given $s \in S$, let $j(s) \in N$ be such that $v(j(s)) = f(i(s))$. By the UMP of $i : S \to F(S)$ there is a module map g such that



commutes. Note that $g \circ v = f$ on $i(S)$. But the set of $m \in F(S)$ where two module maps coincide is a submodule. Hence $g \circ v$ and f agree on $\langle i(S) \rangle = F(S)$. This shows that $F(S)$ is projective. $\square$

Now suppose there is an R-module Q such that $P \circ Q$ is free. Suppose $v : N \to M$ is surjective and that $f : P \to M$ is a module map. Then, since $P \circ Q$ is projective, we get module map $g' : P \oplus Q \to N$ such that the diagram



commutes. But then $v \circ g' \circ i_1 = f \circ \pi_1 \circ i_1 = f$. Hence $g = g' \circ i_1$ lifts f to N as required. That is, P is projective.

8. Recall that an ideal in a ring R is called *prime* if $ab \in I$ implies that either $a \in I$ and $b \in I$. Show that in a commutative ring R and ideal I is prime if and only if R/I is an integral domain.

ANS: Check your favorite undergrad algebra text.

9. Suppose that p is a prime and that $P = p\mathbf{Z}$ is the corresponding prime ideal in $\mathbf{Z}$. Then $\mathbf{Z}_P$ is the ring $S^{-1}\mathbf{Z}$ for $S = \mathbf{Z} \setminus p\mathbf{Z}$. Show that $\mathbf{Z}_P$ can be realized as the subring of $\mathbf{Q}$ given by $\{\, \frac{a}{b} : a, b \in \mathbf{Z},\, b \neq 0 \text{ and } p \nmid b \,\}$. Show $p = \frac{p}{1}$ is prime in Z_P and that every element of $\mathbf{Z}_P$ is of the form $p^\nu u$ for u a unit in $\mathbf{Z}_P$.

ANS: Let $R = \{\, \frac{a}{b} : a, b \in \mathbf{Z},\, b \neq 0 \text{ and } p \nmid b \,\}$, and let $i : Z \to R$ be the inclusion map. I claim that i has the UMP for $S^{-1}\mathbf{Z}$. Let $f : Z \to A$ be a ring map for which $F(S) \subset A^\times$. We want to define $\tilde{f} : R \to A$ by $\tilde{f}(\frac{a}{b}) = f(a)f(b)^{-1}$. The right-hand side makes sense since $b \in S$ and $f(S) \subset A^\times$. To see that $\tilde{f}$ is well defined, suppose that $\frac{a}{b} = \frac{c}{d}$. Then $ad = bc$ and $f(a)f(d) = f(b)f(c)$. It follows that $f(a)f(b)^{-1} = f(c)f(d)^{-1}$. Thus $\tilde{f}$ is well defined. It is easy to see that it is a ring map. For example,

$$\begin{aligned} \tilde{f}\big(\frac{a}{b} + \frac{c}{d}\big) &= f\big(\frac{ad+bc}{bd}\big) \\ &= f(ad+bc)f(bd)^{-1} \\ &= f(a)f(b)^{-1} + f(c)f(d)^{-1} \\ &= \tilde{f}(\frac{a}{b}) + \tilde{f}(\frac{c}{d}). \end{aligned}$$

To see that p is a prime, suppose that p divides $\frac{a}{b} \cdot \frac{c}{d}$. Then $\frac{ac}{bc} = \frac{p}{1} \cdot \frac{e}{f}$. In particular, $fac = pef$. Since $p \nmid f$, we must have $p \mid ac$. Thus p divides a or c and hence $\frac{a}{b}$ or $\frac{c}{d}$. This proves that p is prime in R.

Now if $\frac{a}{b}$ is any element of R, we can, using the Fundamental Theorem of Arithmetic, write $a = p^\nu c$ where $p \nmid c$. But the $\frac{a}{b} = p^\nu \frac{c}{b}$ and $\frac{c}{b}$ is a unit with inverse $\frac{d}{c}$. This establishes the last assertion.

This last assertion says that p is the *only* prime in R.