Remark. A number of students appeared confused about the universal property of free modules. It states:

> Let F be the free module on basis S, and let M be any module and $\phi : S \to M$ be any set map. Then ϕ extends uniquely to a module homomorphism $F \to M$.

Note the difference between "set map" and "module homomorphism".

The extension is of course $\phi(\sum r_i s_i) = \sum r_i \phi(s_i)$.

In practice, one does not state explicitly that one is using this property. One simply defines the map ϕ by specifying $\phi(s_i)$: "Let $\phi : F \to M$ be given by $\phi(s_i) = x_i$". The reader is expected to understand how to extend this by linearity (indeed, I find it jarring to have my attention called to this justification.) One most definitely does not say "Let a homomorphism $\phi : F \to M$ be given by $\phi(s_i) = x_i$; ϕ extends to a map $\phi : F \to M$ by the universal property of free modules." (There is nothing incorrect about this statement, it merely makes it look like you don't know what you're talking about. Here, ϕ extends to F tautologically; it is *well-defined* by the universal property of free modules.)

Problem 1.

(a) *Prove that the following are equivalent for a short exact sequence of R-modules:*

$$0 \to M' \xrightarrow{g} M \xrightarrow{f} M'' \to 0$$

(i) There is a homomorphism $\alpha : M'' \to M$ such that $f\alpha$ is the identity on M''.

(ii) There is a homomorphism $\beta : M \to M'$ such that βg is the identity on M'.

(b) *Prove that $M = \operatorname{Im}(g) \oplus \operatorname{Im}(\alpha) \cong M' \oplus M''$.*

(c) *Prove that α and β can be chosen so that $g\beta + \alpha f$ is the identity on M.*

Solution.

(a) Given α, set $\beta(m) = g^{-1}(m - \alpha f(m))$. This is defined since $m - \alpha f(m) \in \ker f = \operatorname{Im} g$.

Given β, set $\alpha(m'') = m - g\beta(m)$, where m is any element of M such that $f(m) = m''$. This is well-defined because if $f(m) = f(n)$, then $m - n \in \operatorname{Im} g$ and $m - n - g\beta(m) + g\beta(n) = g(g^{-1}(m - n) - \beta(m-n)) = g(g^{-1}(m-n) - \beta g g^{-1}(m-n)) = 0$. □

(b) The isomorphisms are $m \mapsto g\beta(m) + \alpha f(m)$, $g(m') + \alpha(m'') \mapsto m' + m''$, $m' + m'' \mapsto g(m') + \alpha(m'')$. □

(c) Given α, choose β as in part (a). □

Problem 2. *Prove that every R-module is projective if and only if every R-module is injective.*

Solution. Both conditions are equivalent to the condition that every short exact sequence of R-modules splits.

Problem 3. *e is idempotent if $e^2 = e$.*

(a) *If e is idempotent, so is $1 - e$.*

(b) *If I and J are left ideals of R, then $R = I \oplus J$ if and only if $I = Re$ and $J = R(1-e)$ for some idempotent e. In this case, $a = ae$ for all $a \in I$.*

(c) *If I is a left ideal, then R/I is projective if and only if $I = Re$ for some idempotent e.*

(d) *Let e be a central idempotent (i.e., $er = re$ for all $r \in R$.) Show that Re and $R(1-e)$ are two-sided ideals, that $R = Re \times R(1-e)$, and that e and $1-e$ are identities for the subrings Re and $R(1-e)$, respectively.*

Solution.

(a) $(1-e)^2 = 1 - 2e + e = 1 - e$. □

(b) Let $I = Re$ and $J = R(1-e)$. I is fixed by (right) multiplication by e and J by $(1-e)$, so $I \cap J$ is fixed by multiplication by $e(1-e) = 0$. Since $x = xe + x(1-e)$ for any $x \in R$, we have $R = I \oplus J$. Conversely, if $R = I \oplus J$, we have $1 = a + b$, for some $a \in I, b = 1 - a \in J$. Clearly $I = Ra, J = Rb$, so it suffices to show that a is an idempotent. We have $a = (a+b)a = a(a+b) = a^2 + ab = a^2 + ba$, so it suffices to show that $ab = ba = 0$. But $ba \in I, ab \in J$, so $ab \in I \cap J = 0$. □

(c) R/I is projective if and only if the sequence $0 \to I \to R \to R/I \to 0$ splits, i.e., if and only if there exists a submodule (hence, ideal) J of R such that $R = I \oplus J$. □

(d) $Re = eR$ since e is central. Thus Re is a two-sided ideal. It is a subring with identity e since $e(re) = (re)e = re$ for every $re \in Re$. $R = Re \oplus R(1-e) = Re \times R(1-e)$. □

Problem 4. *Show that the following are equivalent:*

(i) *P is a projective R-module.*

(ii) *There is a set $\{x_i\}$ of generators of P and a set $\{f_i : P \to R\}$ of homomorphisms, such that, for any $x \in P$, $x = \sum f_i(x) x_i$.*

(iii) *Given any set $\{x_i\}$ of generators of P, there exists a set of homomorphisms $\{f_i\}$ such that $x = \sum f_i(x) x_i$ for all $x \in P$.*

Solution. A set of generators $\{x_i\}_{\mathcal{I}}$ corresponds to an exact sequence $E : 0 \to K \to F \xrightarrow{g} P \to 0$, with $F = \bigoplus_{\mathcal{I}} R$ and the second map given by $g : e_i \mapsto x_i$. (This is also called a *presentation* of P.)

(i)⇒(iii): E splits, so there is a map $f : P \to F$ such that gf is the identity on P. Let $f_i = \pi_i f$, where π_i is the canonical projection from F to the i^{th} copy of R.

(iii)⇒(ii): There exists a set of generators of P. (For example, P generates itself.)

(ii)⇒(i): $f = \sum f_i$ splits g, so P is a direct summand of the free module F. □

Problem 5. *Let R be a domain with quotient field F. An R-module M is called* divisible *if $aM = M$ for all nonzero a, i.e., given $x \in M$ there exists $y \in M$ such that $ay = x$. M is called* torsion-free *if, for any $a \in R, x \in M$, the equation $ax = 0$ implies that $a = 0$ or $x = 0$.*

(a) *Prove that an injective R-module Q is divisible.*

(b) Let M be divisible and torsion free. Prove that M is injective.

Solution.

(a) Given any x, a, let $g : (a) \to Q$ be given by $f(ra) = rx$. Since Q is injective, g may be extended to a map $g : R \to Q$. Take $y = g(1)$. □

(b) Observe first that, since M is torsion free, there is a unique $y = \frac{x}{a}$ satisfying $ay = x$. By Baer's criterion, it suffices to show that for any ideal I and any map $g : I \to M$, g may be extended to R.

Let g be given and choose nonzero $a \in I$. We claim that g is multiplication by $\frac{g(a)}{a}$. Indeed, for any $b \in I$, we have $g(b) = \frac{g(ab)}{a} = \frac{bg(a)}{a}$. Thus g may be extended to R by $g(1) = \frac{g(a)}{a}$.

Problem 6. *Let R be a domain with fraction field F. A* fractional ideal *of R is a sub-R-module $I \subset F$ such that $cI \subset R$ for some nonzero $c \in R$. Let I and J be fractional ideals of R.*

(a) Prove that $I + J$ and IJ are fractional ideals of R.

(b) Prove that $I \cong J$ as R-modules if and only if $I = xJ$ for some $x \in F$.

(c) The inverse of I is $I^{-1} = \{c \in F : cI \subset R\}$. Prove that I^{-1} is a fractional ideal of R, and give an isomorphism $I^{-1} \to \mathrm{Hom}_R(I, R)$.

(d) I is invertible *if $II^{-1} = R$. Prove that I is invertible if and only if I is projective.*

(e) Prove that if I is invertible, then I is finitely generated.

Solution.

(a) Let c, d be such that $cI, dJ \subset R$. Then $cd(I + J) \subset R, cdIJ \subset R$. □

(b) If $I = xJ$, then multiplication by x is an isomorphism from J to I. Conversely, if $\phi : J \to I$ is an isomorphism, then set $x = \frac{\phi(a)}{a}$ for any nonzero $a \in J$. Then for $b \in J$, we have $\phi(b) = \frac{\phi(c^2ab)}{c^2a} = \frac{b\phi(a)}{a}$, so ϕ is multiplication by x and $I = xJ$. □

(c) $I^{-1} = \bigcap_{x \in I \setminus \{0\}} x^{-1}R$ is an R-module, with $xI^{-1} \subset R$ for any $x \in I$. Since F is injective as an R-module, any homomorphism $g : I^{-1} \to R \subset F$ extends to F and so must be multiplication by something. The map $c \mapsto m_c$, the "multiplication by c" homomorphism, is a (canonical) isomorphism from I^{-1} to $\mathrm{Hom}_R(I, R)$. □

(d) If I is invertible, there exist $x_i \in I$ and $f_i \in I^{-1}$ such that $1 = \sum f_i x_i$. Thus for any $x \in I$, we have $x = \sum f_i x x_i$, so I satisfies the conditions of problem 4. Conversely, if I satisfies the conditions of problem 4, there exist $f_i \in \mathrm{Hom}_R(I, R) = I^{-1}$ such that $x = x \sum f_i x_i$ for all x, i.e., $1 = \sum f_i x_i \subset II^{-1}$. □

(e) If I is invertible, we may write 1 as a finite sum $1 = \sum f_i x_i$. Then, for any $x \in I$, we have $x = \sum (f_i x) x_i$; since $f_i x \in R$, we have $x \in (\{x_i\})$. Thus I is generated by the x_i. □

Problem 7. *Let $R = \mathbb{Z}[\sqrt{-5}]$, $I = (3, 2 + \sqrt{-5})$, $J = (3, 2 - \sqrt{-5})$.*

(*a*) *Show that* $IJ = (3)$.

(*b*) *Prove that* I *is an invertible ideal, and find* I^{-1}.

(*c*) *Prove that* I *is not principal.*

Solution.

(a) $IJ = (9, 6 \pm 3\sqrt{-5}, 9) \subset (3)$. Since $(6+\sqrt{-5}) + (6-\sqrt{-5}) - 9 = 3$, we have $IJ = (3)$. ☐

(b) We have $\frac{1}{3}IJ = (1)$, so $I^{-1} \supset \frac{1}{3}J = (1, \frac{2-\sqrt{-5}}{3})$. We may compute $I^{-1} = \frac{1}{3}J$.

(c) Suppose that $I = (a)$ were principal. Then we would have $f \in \frac{1}{3}J$ such that $fa = 1$, and so $b \in J$ such that $ab = 3$. But then $\mathrm{N}_{F/\mathbb{Q}}(ab) = 9$, (recall that $\mathrm{N}_{F/\mathbb{Q}}(x + y\sqrt{-5}) = x^2 + 5y^2$,) so, without loss of generality, $\mathrm{N}_{F/\mathbb{Q}}(a) = 1$ or 3. No element of R has norm 3, and if $\mathrm{N}_{F/\mathbb{Q}}(a) = 1$, then $a = \pm 1 \notin I$. ☐

Problem 8. *Let* $0 \to M \xrightarrow{\phi} Q \xrightarrow{\psi} L \to 0$ *and* $0 \to M \xrightarrow{\phi'} Q' \xrightarrow{\psi'} L' \to 0$ *be exact, with* Q *and* Q' *injective. Show that* $Q \oplus L' \cong Q' \oplus L$ *as* R*-modules.*

Solution. Since Q' is injective, there exists a homomorphism $f : Q \to Q'$ extending ϕ'. Since $\ker \psi = \phi(M)$ is in the kernel of $\psi' f$, the universal property of the quotient map ψ yields a homomorphism $g : L \to L'$ such that $g\psi = \psi' f$:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & M & \xrightarrow{\phi} & Q & \xrightarrow{\psi} & L & \longrightarrow & 0 \\
 & & \| & & \downarrow f & & \downarrow g & & \\
0 & \longrightarrow & M & \xrightarrow{\phi'} & Q' & \xrightarrow{\psi'} & L' & \longrightarrow & 0
\end{array}
$$

Let $\alpha : Q \to Q' \oplus L$ and $\beta : Q' \oplus L \to L'$ be given by $\alpha(q) = f(q) + \overline{q}$ and $\beta(q' + \overline{q}) = \overline{q'} - g(\overline{q})$. We claim that $\ker \beta = \operatorname{Im} \alpha$. Clearly $\operatorname{Im} \alpha \subset \ker \beta$, so it suffices to show that if $\beta(q' + \overline{q}) = 0$, then $q' + \overline{q} \in \operatorname{Im}(\alpha)$, i.e., q may be chosen so that $f(q) = q'$.

Choose any q above $\overline{q}$. Then we have $\overline{f(q)} = g(\overline{q}) = \overline{q'}$, i.e., there exists m such that $f(q) - q' = \phi'(m) = f\phi(m)$. Replacing q with $q - \phi(m)$ gives us the desired equality.

Thus the sequence $0 \to Q \xrightarrow{\alpha} Q' \oplus L \xrightarrow{\beta} L' \to 0$ is exact. Since Q is injective, it splits and $Q \oplus L' \cong Q' \oplus L$ as desired. ☐

Remark. This problem can also be solved by showing that $Q \oplus L'$ and $Q' \oplus L$ are isomorphic to the pushout $Q \oplus Q' / \langle \phi(m) - \phi'(m) \rangle$, using the maps f and f'.