Lecture 10-16: The hom functor

October 16, 2024

Returning now to noncommutative rings, I investigate what happens when one takes the group of homomorphisms from a fixed module to an arbitrary one.

Let R be a ring (not necessarily commutative), M a left R-module. I now want to consider the set $\hom_R(M, N)$ of R-module homomorphisms from M into N, for all left modules N at the same time. The map sending N to the abelian group $\hom_R(M, N)$, often denoted $\hom_R(M, -)$ is called a functor; it is covariant since given another R-module P and a fixed R-homomorphism $f : N \to P$, one can attach the composite homomorphism $gf \in \hom_R(M, P)$ to any $g \in \hom_R(M, N)$ (see p. 391). Similarly, one could look instead at the map sending N to $\hom_R(N, M)$, denoted $\hom_R(-, M)$, which is also a functor; it is contravariant since given a fixed $f : N \to P$ and any $g \in \hom_R(P, M)$, one now gets a composite homomorphism $gf \in \hom_R(N, M)$. Thus applying $\hom_R(M, -)$ preserves the direction of a homomorphism from N to P, going from the object attached to N to the one attached to P, while $\hom_R(-, M)$ does the reverse. You can read more about functors in Appendix II in the text.

Now I want to take a step further, by studying the effect of these functors on sequences of homomorphisms of R-modules. To do this, I need to say more about such sequences.

Definition, p. 378

A pair of R-module homomorphisms $\alpha : X \to Y, \beta : Y \to Z$ is called *exact* (at Y) if the image im α of α equals the kernel $\ker \beta$ of β. A sequence of homomorphisms $\alpha_1 : M_1 \to M_2, \alpha_2 : M_2 \to M_3, \ldots, \alpha_n : M_n \to M_{n+1}$ is called exact if it is exact at M_i for $2 \leq i \leq n$.

Suppressing the labels of the homomorphisms, one sees that the sequence $0 \to A \to B$ is exact if and only if the map from A to B is injective; similarly $A \to B \to 0$ is exact if and only if the map from A to B is surjective. The sequence $0 \to A \to B \to C \to 0$ is exact if and only if the map from A to B is injective and the map from B to C is surjective with kernel equal to the image of A in B. This last sequence is called short exact (see p. 379). This short exact sequence is called split if B is the direct sum of the image of A in it and a submodule mapping isomorphically onto C (p. 384). Given an exact sequence $\alpha : X \to Y, \beta : Y \to Z$ one has the short exact sequence $0 \to \text{im}\,\alpha \to Y \to Y/\ker\beta \to 0$. Thus the study of exact sequences reduces to that of short exact sequences.

As you might have guessed, of all sequences of homomorphisms, exact ones turn out to be the best behaved. What happens when one applies $\hom_R(M, -)$ or $\hom_R(-, M)$ to a short exact sequence $0 \to A \to B \to C \to 0$ of R-modules? In the first case one gets the sequence $0 \to \hom_R(M, A \to \hom_R(M, B) \to \hom_R(M, C) \to 0$ of abelian groups, since the functor is covariant; in the second case one gets the sequence $0 \to \hom_R(C, M) \to \hom_R(B, M) \to \hom_R(A, M) \to 0$. The first of these starts out being exact, since any nonzero map from M to A remains nonzero when regarded as a map from M to B, identifying A with its image in B. Likewise, a map from M into B becomes 0 when its range is pushed into C if and only if this range lies in the image of A inside B.

Unfortunately the map from $\hom_R(M, B)$ to $\hom_R(M, C)$ is not surjective, in general; not every map $f : M \to C$ can be "lifted" to a map $g : M \to B$, in the sense that f is the composite map hg, where h is the surjective map from B to C. One expresses this situation by saying that $\hom_R(M, -)$ is left exact, but not necessarily exact (see p. 391). The possible trouble with the other homomorphism $\hom_R(-, M)$ also occurs at the right end: the first four terms of the second sequence above form an exact sequence, but in general, not every map from A to M is the restriction to A of a map from B to M. Thus $\hom_R(-, M)$ is also left exact but not generally exact.

At this point it is natural to ask whether some modules M are "better" than others, in the sense that $\hom_R(M, -)$ or $\hom_R(-, M)$ is exact, transforming short exact sequences to short exact sequences. As you might expect, the answer is yes, or I wouldn't bother to ask the question.

Definition, p. 390

The left R-module is called *projective* if the functor $\hom_R(M, -)$ is exact; equivalently, given any surjective R-homomorphism $f : B \to C$ and an R-map $g : M \to C$, this map *lifts* to B in the sense that there is an R-map $h : M \to B$ with $fh = g$.

An upcoming HW problem will transfer this notion to groups (in the more or less obvious way) and ask you to show that a group is projective if and only if it is free.

The question is then which R-modules are projective. One answer is provided by Theorem 6 on p. 354: we know that for any free module F, any homomorphism π from F to another R-module N is completely determined by the images $\pi(b_i)$ of the elements of a free basis (b_i) of F and these images are arbitrary. Thus given $f : B \to C$ and $g : F \to C$ as above it suffices to choose a free basis (f_i) of F, then for each i to choose $b_i \in B$ with $f(b_i) = g(f_i)$ (possible since f is surjective), and then the unique homomorphism $h : F \to B$ with $h(f_i) = b_i$ is such that gh agrees with f on a basis of F, so agrees with it everywhere. We conclude that free modules are projective.

More generally, suppose that M is a direct summand of a free R-module F, so that $F = M \oplus N$ for some module N. Given $f : B \to C$ and $g : M \to C$ as above, extend g to F by decreeing that $g(N) = 0$, lift g as extended to $h : F \to M \to B$, and finally restrict h to M. Then one deduces that direct summands of free modules are projective. Now conversely let P be projective and choose a surjective homomorphism $\pi : F \to P$ (by choosing a set of generators of P). The identity map from P to itself then lifts to a map g from P to F, so that there is a submodule P' of F mapping isomorphically to P under π. But then F is the direct sum of P' and $Q = \ker \pi$, since any $f \in F$ has $\pi(f) = \pi(p')$ for a unique $p' \in P'$. I have shown that any projective R-module is a direct summand of a free module.

In conclusion one gets

Theorem; cf. Proposition 30, p. 389

An R-module is projective if and only if it is a direct summand of a free module.

At first glance, it's hard to see how a direct summand of a free module could fail to be free itself. But as it happens, you have already seen two examples where this happens. First, if m and n are relatively prime integers, then it is well known that the cyclic group $\mathbb{Z}_{mn}$ of order mn is isomorphic to the direct sum $\mathbb{Z}_m \oplus \mathbb{Z}_n$. It follows that $\mathbb{Z}_m$ and $\mathbb{Z}_n$ are nonfree projective modules over $\mathbb{Z}_{mn}$; in a sense you could regard them as "free" of ranks $\frac{m}{m+n}, \frac{n}{m+n}$, respectively. More recently, the ring $A = M_n(R)$ of $n \times n$ matrices over a ring R has arisen in the course (at least in the special case where $R = D$ is a division ring); letting A_i be the additive subgroup of A consisting of all matrices that are 0 apart from their ith columns, one finds that A_i is a left A-submodule of A itself for $1 \leq i \leq n$ and that A is the direct sum of the A_i, whence the A_i are nonfree projective modules over A. Here the A_i could be regarded as "free" modules of rank $\frac{1}{n}$.

Turning now to the other functor $\hom_R(-, M)$, note first, as observed above, that this functor is exact if and only if given a submodule A of an R-module B and a homomorphism f from A to M, f always extends to a homomorphism from B to N. There is no simple necessary and sufficient criterion for this last condition to hold in general, but at least one has a definition:

Definition, p. 395

The R-module M is called *injective* if (with notation as above) every R-homomorphism from A to M extends to B.

Although injective modules were historically defined earlier than projective ones, they are much harder to characterize. The best condition that one has in general is called Baer's Criterion.

Proposition 36 (i), p. 396

The R-module Q is injective if and only if any R-homomorphism from a left ideal I of R into M extends to a homomorphism from R into M.

Proof.

As a left ideal of R is the same thing as a submodule of R, the necessity of this condition is obvious. To see that it is sufficient start with a homomorphism $f : A \to Q$ and an inclusion $A \subset B$. If the condition is satisfied and $A \neq B$ then choose $b \in B, b \notin A$. The set of all $r \in R$ with $rb \in A$ is then a left ideal I of R and one has a map $g : I \to M$ defined via $g(i) = f(ib)$. If the condition holds then g extends to a map from R to M (also denoted by g) and one now extends f to the submodule $A' = A + Rb$ of B via $f(rb) = g(r)$. The submodule A' is then strictly larger than A; if it is not all of B, then one iterates this process. I will address the question of why it comes to an end with a homomorphism defined on all of B next time. □

As a corollary one does get a simple criterion for an R-module to be injective if R is a PID, or principal ideal domain; that is, an integral domain such that all ideals of R are generated by a single element.

Proposition 36 (ii), p. 396

If R is a PID then an R-module Q is injective if and only if we have $Q = rQ$ for all $r \neq 0$ in R.

Proof.

An R-module map f from the principal ideal (r) generated by r to Q is completely determined by the image $f(r)$, which can be any element of Q. If $r \neq 0$, then such a map extends to R if and only if $f(r) = rq$ for some $q \in Q$; if $r = 0$ then this map always extends to R, taking $f(1)$ to be any element of Q. Thus all such maps extend to R if and only if $Q = rQ$ for $r \neq 0$. □

Modules Q over $\mathbb{Z}$ with $Q = rQ$ for $r \in \mathbb{Z}, r \neq 0$, are called divisible (p. 396). Thus a $\mathbb{Z}$-module (that is, an abelian group) is injective if and only if it is divisible. Note that this condition is completely different than the one for projectivity; in particular, free $\mathbb{Z}$-modules are never injective.