Math 250A

PROFESSOR KENNETH A. RIBET

Last Midterm Exam

October 29, 2015

2:10–3:30PM, Somewhere in Cory Hall

Please write your NAME clearly:

Please put away all books, calculators, cell phones and other devices. You may consult a single two-sided sheet of notes. Please write carefully and clearly in *complete sentences*.

Problem	Your score	Possible points
1		8 points
2		9 points
3		7 points
4		6 points
Total:		30 points

If not otherwise specified, A is a ring (with 1).

1a. What do we mean when we say that an A-module is *free*?

We mean that the module is isomorphic to the free module on some set. If S is a set, the free A-module on S represents the functor $F : (A\text{-modules}) \to (\text{sets})$ that takes an A-module X to the set of functions from S to the set underlying X. The free module on S, often denoted $A\langle S\rangle$ is the additive group of finite A-linear combinations of elements of S, endowed with the obvious scalar multiplication by elements of A.

b. What do we mean when we say that an A-module is *projective*?

We mean that it satisfies a set of equivalent conditions, one of which is that the module is a direct summand of a free module. If P is an A-module, another one of the equivalent conditions for P to be projective is this: whenever $g : Y \to Z$ is a surjection of A-modules, the induced map $\operatorname{Hom}_A(P, Y) \to \operatorname{Hom}_A(P, Z)$ of abelian groups is surjective.

c. Prove that free modules are projective.

If $P = A\langle S\rangle$, the map $\mathrm{Hom}_A(P,Y) \to \mathrm{Hom}_A(P,Z)$ that was just described may be rewritten $\mathrm{Maps}(S,Y) \to \mathrm{Maps}(S,Z)$. We see easily that this map is surjective: given a surjection $Y \to Z$ and a map $\varphi : S \to Z$, we can lift this map to a map $S \to Y$ by choosing a preimage in Y for each $\varphi(s)$.

d. Give an example of a projective module that is not free, showing that the module is indeed projective but not free.

The first example given in class was this one: Let K be a field and let A be the ring $K \oplus K$. The module $K \oplus K$ is a free module of rank 1 (!). Its submodule $P = K \oplus (0)$ is then a direct summand of a free module. One would like to say that P is visibly not free because its dimension over K is 1, which is an odd number. This seems to work. Namely, if S is a finite set, the free module $A\langle S\rangle$ has K-dimension equal to twice the number of elements of S. If S is infinite, the free module $A\langle S\rangle$ is of infinite dimension over K.

2a. Let F be a covariant functor from a category (which I'll refer to as the "source category") to the category of sets. Precisely what do we mean when we say that F is *representable?*

The functor F is representable if there is a universal object T in the "source category" and a universal element u in the set $F(T)$. These players are required to have the following property: For each object X in the source category and each element s of the set $F(X)$, there is a unique morphism $h \in \mathrm{Mor}(T,X)$ such that $s = F(h)(u)$. The right-hand member of this equation is the element of $F(X)$ gotten by applying $F(h)$ to u. We can denote it also by $h_*(u)$.

b. Let F be the functor from (rings) to (sets) that takes a ring to its underlying set. Show that F is representable.

We take T to be the ring $\mathbf{Z}[x]$ and let u be the element x of the set underlying T. If A is a ring and a is an element of A. there is a unique ring homomorphism $h : T \to A$ taking x to a. We have, in fact, $h(f(x)) = f(a)$.

c. Let F be the functor that takes a ring A to the set of squares in A. Show that F is *not* representable.

Suppose that F is representable by a ring T and an element u of $F(T)$. Then u is a square in T, so $u = t^2$ for some $t \in T$. Let A be the ring $\mathbf{Z}[x]$ and let s be the square x^2 in A. There should then be a unique ring homomorphism $h : T \to A$ such that $h(u) = s$. We shall show that h cannot be unique. If $h(u) = s$, then equivalently $h(t)^2 = h(t^2) = x^2$, which implies that $h(t) = \pm x$. Let $\alpha : A \to A$ be the unique ring homomorphism that takes x to $-x$; thus $\alpha(f(x)) = f(-x)$ for $f \in A$, so that $\alpha(-x) = x$ and $\alpha(x) = -x$. The homomorphism αh then takes t to $\mp x$ and takes u to $(\mp x)^2 = x^2$. Thus αh is a second ring homomorphism taking u to x^2; it is different from h because its value on t is the negative of the value of h on t.

3. Suppose that I is a non-zero ideal of a Dedekind ring A and that a is a non-zero element of I. Prove that there is an element b of I so that I is the ideal (a,b) generated by a and b:

$$I = \{\, ra + sb \,|\, r, s \in A \,\}.$$

Here is an outline of the proof, which depends on the unique factorization of non-zero ideals of A as a product of primes (non-zero prime ideals). The task is to fill in the details:

(1) If $I = P_1^{e_1} \cdots P_t^{e_t}$, then $(a) = P_1^{f_1} \cdots P_t^{f_t} Q_1^{g_1} \cdots Q_s^{g_s}$, where $f_i \geq e_i$ for $i = 1, \ldots, t$.

Because a is in I, we have $(a) \subseteq I$. We say that I divides (a); more precisely, we have $(a) = I \cdot (a)I^{-1}$, and the second factor is an integral ideal J because $(a)I^{-1} \subseteq II^{-1} = A$.

The ideal $J = (a)I^{-1}$ decomposes as a product of primes, which we group as usual into prime powers. Some of the primes might be among the primes P_i that occur in the factorization of I; the rest of the primes are primes that don't occur in I's factorization, and we can call them Q_j. If we write $J = P_1^{f_1 - e_1} \cdots P_t^{f_t - e_t} Q_1^{g_1} \cdots Q_s^{g_s}$, we get the expression for (a) that was in the hint.

(2) There is an element $b \in A$ such that b is divisible exactly by $P_i^{e_i}$ for all $i = 1, \ldots, t$ but not divisible by any of the Q_j.

This is a standard application of the Chinese Remainder Theorem. We chose, for each i, an x_i that is in $P_i^{e_i}$ but not in $P_i^{e_i+1}$. We choose, for each j, a z_j in the ring that is not in Q_j. (For example, we can take $z_j = 1$.) The CRT allows us to choose a b that is x_i mod $P_i^{e_i+1}$ for each i and is also congruent to z_j mod Q_j for each j.

(3) The ring element b is in I and we have $(a,b) = I$.

To say that b is in I is to say, in other language, that I divides (b). It is obvious that this is true because (b) is divisible by $P_i^{e_i}$ for all i.

To say that $(a,b) = I$ is to say that the gcd of (a) and (b) is I. This is also obvious from the point of view of prime factorizations; we chose b to make it so! The amazing thing is that the gcd is really the ideal generated by a and b. We come away with the striking observation that I is generated by two elements. The first element can be taken to be any old non-zero member of I, but then the second element then needs to be chosen carefully using the Chinese Remainder Theorem.

4a. Exhibit two non-zero modules M and N over a commutative ring A with the following property: if X is an A-module, all bilinear maps $M \times N \to X$ are zero. Explain carefully why M and N have this property.

We take A to be $\mathbf{Z}$ and take $M = \mathbf{Z}/m\mathbf{Z}$ and $N = \mathbf{Z}/n\mathbf{Z}$, where m and n are relatively prime integers > 1. For example, we could take $m = 2$, $n = 3$. Every bilinear map $b : M \times N \to X$ (where X is an abelian group) will be annihilated (i.e., sent to 0) by multiplication by m, and also by multiplication by n. Hence it will be sent to zero by multiplication by 1, since 1 is a $\mathbf{Z}$-linear combination of m and n. Something sent to 0 by multiplication by 1 is definitely 0.

b. What do we mean when we say that a module is *flat*?

We mean that tensoring with this module sends injections to injections. If F is an A-module, we say that F is flat if the map $X \otimes_A F \to Y \otimes_A F$ induced by a homomorphism of A-modules $f : X \to Y$ is injective whenever f is injective.

c. Explain why $\mathbf{Q}$ is a flat $\mathbf{Z}$-module but not a projective $\mathbf{Z}$-module.

If F is a free $\mathbf{Z}$-module, 0 is the only element of F that is infinitely divisible, i.e., is in $n \cdot F$ for all $n \geq 1$. The $\mathbf{Z}$-module $\mathbf{Q}$ is *divisible*: every rational number can be divided by every positive integer. Thus $\mathbf{Q}$ cannot be embedded in a free $\mathbf{Z}$-module (i.e., free abelian group). Thus it is certainly not a direct summand of a free abelian group and consequently is not projective.

On the other hand, $\mathbf{Q}$ is flat because it is torsion free. (We discussed in class that torsion free modules over PIDs are flat.) Alternatively, $\mathbf{Q}$ is flat because it's a localization. Perhaps it's best in this situation if I try to explain what's really going on:

Let M be a $\mathbf{Z}$-module (i.e., an abelian group). The tensor product $\mathbf{Q} \otimes M$ (taken over $\mathbf{Z}$) consists of sums of terms $\frac{a}{b} \otimes m$, where a and b are integers (with b non-zero) and m is in M. We can write $\frac{a}{b} \otimes m = \frac{1}{b} \otimes am$ by bilinearity. Thus each term $\alpha \otimes m$ may be rewritten $\frac{1}{d} \otimes m'$ whenever d is a denominator for α. A general term of the tensor product is a sum of terms like this. But we can combine terms by selecting a common denominator for each of them. Thus $\mathbf{Q} \otimes M$ is the set of tensors $\frac{1}{d} \otimes m$ with $d \geq 1$ in $\mathbf{Z}$ and $m \in M$.

Now $\mathbf{Q}$ is $S^{-1}\mathbf{Z}$, where S is the multiplicative set of non-zero integers. If M is an abelian group, I'll write V_M for $S^{-1}M$, which is the set of quotients $\frac{m}{d}$, modulo the usual relations. In particular, $\frac{m}{d} = 0$ if and only if m is a torsion element of M (i.e., is killed by some positive integer).

There is a fairly obvious isomorphism $\mathbf{Q} \otimes M \to V_M$. The bilinear map $(\alpha, m) \mapsto \alpha m \in V_M$ induces a map from the tensor product to V_M. There's a map in the other direction, $\frac{m}{d} \mapsto \frac{1}{d} \otimes m$. This second map is a homomorphism (check!) and is an inverse to the first (check!).

Now the flatness is pretty clear. Suppose that we have an inclusion of abelian groups $M \subseteq N$ and want to check the injectivity of the map on tensor products $\mathbf{Q} \otimes M \to \mathbf{Q} \otimes N$. This amounts to showing that $\frac{m}{d}$ is 0 in V_M if and only if it is 0 in V_N. As I said, however, an expression like this is 0 if and only if m is torsion. Whether or not m is torsion is the same question whether we regard m as living in M or in N.