Math 101 Fall 2013
Homework #3
Due Wednesday 9 October 2013

1. Recall that a subset S of an R-module is *linearly independent* if given any subset $\{s_1, \cdots, s_m\}$ of distinct elements of S and elements r_i of R such that $r_1 \cdot s_1 + \cdots + r_m \cdot s_m = 0$, then $r_i = 0$ for all i. We call S a *basis* for R if it is linearly independent and generates R (that is, every element of R is a finite linear combination of elements of S). Show that R is free if and only if it has a basis.

ANS: Suppose that M is a free module on S. Then we can assume that $M = \coprod_{s \in S} R$ for a set S; that is, M is the set of functions m from S to R such that $m(s) = 0$ for all but finitely many s. If $S = \emptyset$, then we interpret the latter as the zero module with basis $S = \emptyset$. Otherwise, I claim that $S' = \{ \epsilon_s : s \in S \}$ is a basis for M where we recall that $\epsilon_s : S \to R$ is the function

$$\epsilon_s(s') = \begin{cases} 1 & \text{if } s' = s \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

If $s_1, \ldots, s_m$ are distinct elements and if

$$f = r_1 \cdot \epsilon_{s_1} + \cdots + r_m \cdot \epsilon_{s_m} = 0,$$

then $0 = f(s_j) = r_j$ for all j. It follows that S' is linearly independent. On the other hand, if $f \in M$, then we can suppose that $s_1, \ldots, s_n$ are the only inputs for which $f(s) \neq 0$. But then

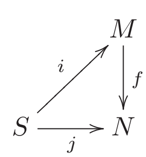
$$f = f(s_1) \cdot \epsilon_{s_1} + \cdots + f(s_n) \cdots \epsilon_{s_n}.$$

This shows that S' generates and that S' is a basis.

Now suppose that S is a basis for M. We can assume that $M \neq \{0\}$ and that S is nonempty. Let $i : S \to M$ be the inclusion map and let $j : S \to N$ be a map of S into another R-module N. Given $m \in M$, there are unique s_i and r_i, with only finitely many $r_i \neq 0$, so that

$$m = \sum r_i \cdot s_i.$$

Hence we can define a function $f : M \to N$ by $f(m) = \sum r_i \cdot j(s_i)$. It is straightforward to check that f is module map and that it is the unique map such that the diagram



commutes. (For example, if $m = \sum r_i \cdot s_i$ and $m' = \sum r_i' \cdot s_i$, then $m + m' = \sum (r_i + r_i') \cdot s_i$; hence, $f(m + m') = f(m) + f(m')$.) Thus $i : S \to M$ has the required UMP and M is free on S.

COMMENT: It should be clear from the proof that for modules over commutative rings that the cardinality of the basis is the same as the rank of the module as a free module.

2. Give a careful statement of Zorn's Lemma (look it up). Then use Zorn's Lemma to prove that if R is a ring (with identity), then every proper ideal of R is contained in a maximal ideal. In particular, R has a maximal ideal.

ANS: A subset U of an ordered set S is *totally ordered* if any pair of elements in U are comparable. A subset U of S has an upper bound in S if there is a $v \in S$ such that $u \leq v$ for all $u \in U$. An element b in S called a maximal element if $s \in S$ is such that $b \leq s$, then $b = s$.

Zorn's Lemma says that if every totally ordered subset of a nonempty set S has an upper bound in S, then S has a maximal element.

As an application, let I be a proper ideal in R and let $\mathcal{S}$ be the set of *proper* ideals containing I. This set is nonempty as it contains I and it is ordered by inclusion. Let $\{J_i\}$ be a totally ordered subset of $\mathcal{S}$. Since each J_i is proper, $1 \notin J_i$. Hence $1 \notin J := \bigcup_i J_i$. Thus J is a proper ideal containing I, and hence belongs to S, which is an upper bound for each J_i. Thus $\mathcal{S}$ has a maximal element which almost by definition is a maximal ideal in R.

3. Recall that the family of subsets of any set are ordered by containment: $A \leq B$ if and only if $A \subset B$. Prove the following assertions that were used without proof in our proof that submodules of free modules are free for modules over at PID.

(a) Let $\mathcal{S} := \{(C, f)\}$ be a nonempty collection of functions $f : C \to A$ where C is a subset of a set B. Order $\mathcal{S}$ by $(C, f) \leq (D, g)$ if $C \subset D$ and $g|_C = f$. Let $\{(C_i, f_i)\}$ be a *totally ordered* subset of $\mathcal{S}$. Define $C = \bigcup C_i$. Show that we get a well-defined function $f : C \to A$ be letting $f(c) = f_i(c)$ if $c \in C_i$.

(b) Let B be a basis for a free module F over R. Let $\{C_i\}$ be a *totally ordered* collection of subsets of B whose union is all of B. Show that $F = \bigcup \langle C_i \rangle$ where, as usual, $\langle C \rangle$ is the submodule of F generated by C. (We don't actually need $\{C_i\}$ to be totally ordered. We just need it to be *cofinal* in that given C_i and C_j there is a C_k containing both of them.)

4. Let V be a finite-dimensional k-vector space and $R : V \to V$ be a linear operator such that $R^2 = \mathrm{id}_V$. Assume the characteristic of k is not 2. Show that V has a basis β such that

$$[R]_\beta^\beta = \begin{pmatrix} I_r & 0 \\ 0 & -I_s \end{pmatrix}$$

where of course I_p is the $p \times p$ identity matrix.

ANS: Consider V as a $k[x]$-module in the usual way: $p(x) \cdot v = p(R)v$. Let $I = (1-x)$ and $J = (1+x)$. Then $IJ \cdot V = \{0\}$. Since $\frac{1}{2}(1-x) + \frac{1}{2}(1+x) = 1$, we clearly have $I + J = R$. Hence by the Primary Decomposition Theorem from lecture, $V = {}_IV \oplus {}_JV$ where

$$ {}_IV = \{ v \in V : (1-x) \cdot v = 0 \} = \{ v \in V : Rv = v \} = \mathcal{E}_1. $$

Similarly, ${}_JV$ is the eigenspace $\mathcal{E}_{-1} = \{ v \in V : Rv = -v \}$. Now we can let β_1 be a basis for $\mathcal{E}_1$ and β_2 a basis for $\mathcal{E}_{-1}$. Then $\beta = \beta_1 \cup \beta_2$ is a basis for V and $[R]_\beta^\beta$ has the required form.
ALTERNATE SOLUTION: Let $P = \frac{1}{2}(I - R)$. Then $P^2 = P$ and you can apply a previous homework problem.

5. Let $f : \mathbf{Z}^n \to \mathbf{Z}^n$ be a $\mathbf{Z}$-module map.

(a) If f is surjective, show that it must also be injective.

(b) If f is injective, it need not be surjective, but show that it must be *almost surjective* in that its cokernel is finite.

(I found the $S^{-1}(\cdot)$ functor helpful.)

ANS: (a) Since $S^{-1}(\cdot)$ is exact, the short exact sequence

$$ 0 \longrightarrow \ker f \longrightarrow \mathbf{Z}^n \xrightarrow{f} \mathbf{Z}^n \longrightarrow 0 $$

gives rise to the short exact sequence

$$ 0 \longrightarrow S^{-1}(\ker f) \longrightarrow \mathbf{Q}^n \xrightarrow{S^{-1}(f)} \mathbf{Q}^n \longrightarrow 0 $$

of $\mathbf{Q}$-vector spaces. Thus $S^{-1}(\ker f) = \{0\}$ by the rank-nullity theorem. On the other hand, as a submodule of a free module, $\ker f$ is free. By the above, it has rank zero (recall, the rank of any module over an integral domain is the dimension of $S^{-1}(M)$ as a vector space over $S^{-1}R$). Hence $\ker f = \{0\}$.

(b) Here we consider the short exact sequence

$$ 0 \longrightarrow \mathbf{Z}^n \xrightarrow{f} \mathbf{Z}^n \xrightarrow{q} \mathbf{Z}^n/f(\mathbf{Z}^n) \longrightarrow 0. $$

Then we get the short exact sequence

$$ 0 \longrightarrow \mathbf{Q}^n \xrightarrow{S^{-1}(f)} \mathbf{Q}^n \xrightarrow{S^{-1}(q)} S^{-1}(\mathbf{Z}^n/f(\mathbf{Z}^n)) \longrightarrow 0. $$

By the rank-nullity theorem, $S^{-1}(f)$ is surjective. Thus, the rank of $\mathbf{Z}^n/f(\mathbf{Z}^n)$ is zero. Thus it is a finite group (every finitely generated abelian group factors as a finite group cross a free group).

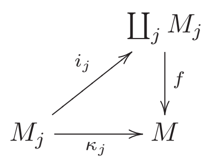
6. (Internal coproducts) Let M be an R-module. Suppose there are submodules $\{M_j\}_{j \in J}$ such that

(a) the submodule $\sum_j M_j$ generated by the set $S = \bigcup_j M_j$ is all of M;

(b) and for each j, $M_j \cap \sum_{i \neq j} M_i = \{0\}$.

Then show that M is isomorphic to $\coprod_{j \in J} M_j$ as R-modules.

ANS: Let $\kappa_j : M_j \to M$ be the inclusion map. Then by the UMP of the coproduct, we have a unique module map $f : \coprod_j M_j \to M$ such that



commutes. Clearly, $f(h) = \sum_j f(j)$ (which is a finite sum of nonzero elements). Therefore, if $f(h) = 0$, then we have $\sum_j f(j) = 0$. Thus for each $j \in J$,

$$h(j) = \sum_{i \neq j} f(i).$$

It follows that $h(j) \in M_j \cap \sum_{i \neq j} M_i = \{0\}$. Hence $h = 0$ and f is injective. On the other hand, the range of f clearly contains M_j for each j. Hence it contains the subspace $\sum_j M_j$ generated by the M_j. Thus f is surjective. Thus f is the required isomorphism.

7. (Primary Decomposition) Let M be a torsion abelian group and let P be the positive primes in $\mathbf{Z}$. For each $p \in P$ and $n \in \mathbf{N}$ let ${}_{p^n}M = \{ m \in M : p^n \cdot m = 0 \}$ be the submodule of M annihilated by p^n. Let $M[p] := \bigcup_{n=1}^{\infty} \bigl({}_{p^n}M \bigr)$. Then $M[p]$ is a submodule of M called the *p-primary component* of M. Show that $M \cong \coprod_{p \in P} M[p]$. (I used question 6 and the observation that if $(a_1, \dots, a_n) = 1$ — that is, if the integers $a_1, \dots, a_n$ have no common factor other than 1 — then there are integers b_i such that $b_1 a_1 + \cdots + b_n a_n = 1$.)

ANS: Suppose that $m \in M[p] \cap M[q]$ with $q \neq p$. Then there are integers m and n such that $p^m \cdot m = 0 = q^n \cdot m$. Since $(p^m, q^n) = 1$, then there are integers a and b such that $ap^m + bq^n = 1$. Then $m = (ap^m + bq^n) \cdot m = 0$. Hence we certainly have $M[p] \cap \sum_{q \neq p} M[q] = \{0\}$. On the other hand, since M is torsion, if $m \in M$, then there is an integer N such that $N \cdot m = 0$. Let $M = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes p_i and $e_i \geq 1$. Let $N_i = N / p_i^{e_i}$. Then $(N_1, \dots, N_k) = 1$ and there are integers a_i such that $a_1 N_1 + \cdots a_k N_k = 1$. But then $m = (a_1 N_1 + \cdots a_k N_k) \cdot m = m_1 + \cdots m_k$ with $m_i = a_i N_i \cdot m$. But $p_i^{e_i} \cdot m_i = 0$ and $m_i \in M[p_i]$. Hence $\sum_p M[p] = M$. Now we can apply question 6.