STABLY FREE MODULES

KEITH CONRAD

1. Introduction

Let R be a commutative ring. When an R-module has a particular module-theoretic property after direct summing it with a finite free module, it is said to have the property *stably*. For example, R-modules M and N are *stably isomorphic* if $R^k \oplus M \cong R^k \oplus N$ for some $k \geq 0$. An R-module M is *stably free* if it is stably isomorphic to a free module: $R^k \oplus M$ is free for some k. When M is finitely generated and stably free, then for some k $R^k \oplus M$ is finitely generated and free, so $R^k \oplus M \cong R^\ell$ for some ℓ. Necessarily $k \leq \ell$ (why?). Are stably isomorphic modules in fact isomorphic? Is a stably free module actually free? Not always, and that's why the concepts are interesting. This "stable mathematics" is part of algebraic K-theory. Our purpose here is to describe the simplest example of a non-free module which is stably free and then discuss what it means for all stably free modules over a ring to be free.

Theorem 1.1. *Let R be the ring $\mathbf{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$. Let $T = \{(f, g, h) \in R^3 : xf + yg + zh = 0$ in $R\}$. Then $R \oplus T \cong R^3$, but $T \not\cong R^2$.*

The module T in this theorem is stably free (it is stably isomorphic to R^2), but it is not a free module. Indeed, if T is free then (since T is finitely generated; the theorem shows it admits a surjection from R^3) for some n we have $T \cong R^n$, so $R \oplus R^n \cong R^3$. Since $R^a \cong R^b$ only if $a = b$, $1+n = 3$ so $n = 2$. But this contradicts the non-isomorphism in the conclusion of the theorem.

It's worth noting that the ranks in the theorem are as small as possible for a non-free stably free module. If R is any commutative ring and M is an R-module such that $R \oplus M \cong R$ then $M = 0$. If $R \oplus M \cong R^2$ then $M \cong R$. The first time we could have $R \oplus M \cong R^\ell$ with $M \not\cong R^{\ell-1}$ is $\ell = 3$, and Theorem 1.1 shows such an example occurs.

2. Proof of Theorem 1.1

In the proof of Theorem 1.1 it will be easy to show $R \oplus T \cong R^3$. But the proof that $T \not\cong R^2$ will require a theorem from topology about vector fields on the sphere. We denote the module as T because it is related to tangent vectors on the sphere.

Proof. Since R is a ring, on R^3 we can consider the dot product $R^3 \times R^3 \to R$. For example, $(x, y, z) \cdot (x, y, z) = x^2 + y^2 + z^2 = 1$. For any $\mathbf{v} \in R^3$, let $r = \mathbf{v} \cdot (x, y, z) \in R$. Then

$$(\mathbf{v} - r(x, y, z)) \cdot (x, y, z) = \mathbf{v} \cdot (x, y, z) - r(x, y, z) \cdot (x, y, z) = r - r = 0,$$

so $\mathbf{v} - r(x, y, z) \in T$. That means $R^3 = R(x, y, z) + T$. This sum is direct since $R(x, y, z) \cap T = (0, 0, 0)$: if $r(x, y, z) \in T$ then dotting $r(x, y, z)$ with (x, y, z) implies $r = 0$. So we have proved

$$R^3 = R(x, y, z) \oplus T. \tag{2.1}$$

Since $R \cong R(x, y, z)$ by $r \mapsto r(x, y, z)$, $R^3 \cong R \oplus T$. Thus T is stably free.

Now we will show by contradiction that $T \not\cong R^2$. Assume $T \cong R^2$, so T has an R-basis of size 2, say (f, g, h) and (F, G, H). By (2.1) the three vectors $(x, y, z), (f, g, h), (F, G, H)$ in R^3 are an R-basis, so the matrix

$$\begin{pmatrix} x & f & F \\ y & g & G \\ z & h & H \end{pmatrix}$$

in $\mathrm{M}_3(R)$ must be invertible: it is the change-of-basis matrix between the standard basis of R^3 and the basis $(x, y, z), (f, g, h), (F, G, H)$. Therefore the determinant of this matrix is a unit in R:

$$\det \begin{pmatrix} x & f & F \\ y & g & G \\ z & h & H \end{pmatrix} \in R^\times. \tag{2.2}$$

It makes sense to evaluate elements of R at points (x_0, y_0, z_0) on the unit sphere S^2: polynomials in $\mathbf{R}[x, y, z]$ which are congruent modulo $x^2 + y^2 + z^2 - 1$ take the same value at any $(x_0, y_0, z_0) \in S^2$ since $x_0^2 + y_0^2 + z_0^2 - 1 = 0$. A unit in R takes nonzero values everywhere on the sphere: if $a(x, y, z)b(x, y, z) = 1$ in R then $a(x_0, y_0, z_0)b(x_0, y_0, z_0) = 1$ in $\mathbf{R}$ when $(x_0, y_0, z_0) \in S^2$. In particular, at each point $\mathbf{v} \in S^2$ the determinant in (2.2) has a nonzero value, so $(f(\mathbf{v}), g(\mathbf{v}), h(\mathbf{v})) \in \mathbf{R}^3 - \{\mathbf{0}\}$. Thus $\mathbf{v} \mapsto (f(\mathbf{v}), g(\mathbf{v}), h(\mathbf{v}))$ is a nowhere vanishing vector field on S^2 with continuous components (polynomial functions are continuous). But this is impossible: the hairy ball theorem in topology says every continuous vector field on the sphere vanishes at least once. $\square$

There is a stably free non-free module $T_{\mathbf{Z}}$ over $\mathbf{Z}[x, y, z](x^2+y^2+z^2-1)$. The construction is analogous to the previous one. Elements of $\mathbf{Z}[x, y, z]/(x^2+y^2+z^2-1)$ can be evaluated on the real sphere, and the proof that $T_{\mathbf{Z}}$ is not a free module uses evaluations of polynomials at points on the real sphere as before.

For any $d \geq 1$, every continuous vector field on the $2d$-dimensional sphere S^{2d} vanishes somewhere, so over

$$R = \mathbf{R}[x_1, \ldots, x_{2d+1}]/(x_1^2 + \cdots + x_{2d+1}^2 - 1) \tag{2.3}$$

the tangent module $T = \{(f_1, \ldots, f_{2d+1}) \in R^{2d+1} : \sum x_i f_i = 0 \text{ in } R\}$ is stably free but not free: $R \oplus T \cong R^{2d+1}$ but $T \not\cong R^{2d}$.

3. When Stably Free Modules Must Be Free

For some rings R, all stably free finitely generated R-modules are free. This holds if R is a field since all vector spaces are free (have bases). It also holds if R is a PID: a stably free R-module is a submodule of a finite free R-module, and any submodule of a finite free module over a PID is a free module. A much more difficult example is when $R = k[X_1, \ldots, X_n]$, where k is a field. (This is Serre's conjecture, proved independently by Quillen and Suslin with k even allowed to be a PID rather than a field.[1]) In this section we show how the task of proving all stably free finitely generated modules over a particular ring R are free can be formulated as a linear algebra problem over R. (It is shown in the

[1]The actual problem put forward by Serre was to show any finitely generated projective module over $k[X_1, \ldots, X_n]$ is free. He showed such modules are stably free, so his problem reduces to the version we stated about freeness of stably free finitely generated modules over $k[X_1, \ldots, X_n]$.

appendix that over any ring, every non-finitely generated module which is stably free is free, so there is no loss of generality in focusing on finitely generated modules.)

To distinguish n-tuples $(a_1, \ldots, a_n)$ in R^n from the ideal $(a_1, \ldots, a_n) = Ra_1 + \cdots + Ra_n$ in R, denote the n-tuple in R^n as $[a_1, \ldots, a_n]$.

Theorem 3.1. *Fix a nonzero commutative ring R and a positive integer n. The following conditions are equivalent.*

(1) *For any R-module M, if $M \oplus R \cong R^n$ then M is free.*
(2) *Every vector $[a_1, \ldots, a_n] \in R^n$ satisfying $(a_1, \ldots, a_n) = R$ is part of a basis of R^n.*

Proof. Both (1) and (2) are true (for all R) when $n = 1$, so we may suppose $n \geq 2$.

(1) $\Rightarrow$ (2): Suppose $(a_1, \ldots, a_n) = R$, so $\sum a_i b_i = 1$ for some $b_i \in R$. Set $\mathbf{a} = [a_1, \ldots, a_n]$ and $\mathbf{b} = [b_1, \ldots, b_n]$. Let $f \colon R^n \to R$ by $f(\mathbf{v}) = \mathbf{v} \cdot \mathbf{b}$, so $f(\mathbf{a}) = 1$ and $R^n = R\mathbf{a} \oplus \ker f$ by the decomposition

$$\mathbf{v} = f(\mathbf{v})\mathbf{a} + (\mathbf{v} - f(\mathbf{v})\mathbf{a}).$$

(This sum decomposition is unique because if $\mathbf{v} = r\mathbf{a} + \mathbf{w}$ with $r \in R$ and $\mathbf{w} \in \ker f$ then applying f to both sides shows $f(\mathbf{v}) = r$, so $\mathbf{w} = \mathbf{v} - r\mathbf{a} = \mathbf{v} - f(\mathbf{v})\mathbf{a}$.) Since $R\mathbf{a} \cong R$ by $\mathbf{v} \mapsto \mathbf{v} \cdot \mathbf{b}$ (concretely, $r\mathbf{a} \mapsto r$), R^n is isomorphic to $R \oplus \ker f$, so $\ker f$ is free by (1). Adjoining $\mathbf{a}$ to a basis of $\ker f$ provides us with a basis of R^n.

(2) $\Rightarrow$ (1): Let $g \colon M \oplus R \to R^n$ be an R-module isomorphism. Set $\mathbf{a} = g(0,1) = [a_1, \ldots, a_n]$. To show the ideal $(a_1, \ldots, a_n)$ is R, suppose it is not. Then there is a maximal ideal $\mathfrak{m}$ containing each a_i, so $g(0,1) \subset \mathfrak{m}^n$. However, the isomorphism g restricts to an isomorphism from $\mathfrak{m}(M \oplus R) = \mathfrak{m}M \oplus \mathfrak{m}$ to $\mathfrak{m}R^n = \mathfrak{m}^n$, so $g(0,1)$ being in $\mathfrak{m}^n$ implies $(0,1) \in \mathfrak{m}M \oplus \mathfrak{m}$, which is false.

By (2) there is a basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of R^n where $\mathbf{v}_1 = \mathbf{a}$. Then $g^{-1}(\mathbf{v}_1), \ldots, g^{-1}(\mathbf{v}_n)$ is a basis of $M \oplus R$, with $g^{-1}(\mathbf{v}_1) = (0,1)$. For $i = 2, \ldots, n$, write $g^{-1}(\mathbf{v}_i) = (m_i, c_i)$. Subtracting a multiple of $(0,1)$ from each (m_i, c_i) for $i = 2, \ldots, n$, we get a basis $(0,1), (m_2, 0), \ldots, (m_n, 0)$ of $M \oplus R$. Writing any $(m, 0)$ as a linear combination of these shows $m_2, \ldots, m_n$ spans M as an R-module and is linearly independent, so M is free. $\square$

Corollary 3.2. *For a commutative ring R, the following conditions are equivalent.*

(1) *For all R-modules M, if $M \oplus R \cong R^n$ for some n then M is free.*
(2) *For all $n \geq 1$, every vector $[a_1, \ldots, a_n] \in R^n$ satisfying $(a_1, \ldots, a_n) = R$ is part of a basis of R^n.*
(3) *All stably free finitely generated R-modules are free.*

Proof. (1) $\Leftrightarrow$ (2): This equivalence is Theorem 3.1 for all n.

(1) $\Rightarrow$ (3): Suppose M is a stably free R-module, so $M \oplus R^k \cong R^\ell$ for some k and ℓ. We want to show M is free. If $k = 0$ then obviously M is free. If $k \geq 1$ then $(M \oplus R^{k-1}) \oplus R \cong R^\ell$, so (1) with $n = \ell$ tells us that $M \oplus R^{k-1}$ is free. By induction on k, the module M is free.

(3) $\Rightarrow$ (1): If $M \oplus R \cong R^n$ for some n then M is stably free, and thus M is free by (3). $\square$

Corollary 3.2(2) expresses the freeness of all stably free finitely generated R-modules as a problem in linear algebra in R^n (over all n). The condition there that the coordinates generate the unit ideal is necessary if $[a_1, \ldots, a_n]$ has a chance to be part of a basis of R^n:

Theorem 3.3. *If $[a_1, \ldots, a_n] \in R^n$ is part of a basis of R^n then the ideal $(a_1, \ldots, a_n)$ is the unit ideal.*

Proof. We are assuming there is a basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of R^n such that $\mathbf{v}_1 = [a_1, \ldots, a_n]$. Write each $\mathbf{v}_j$ in coordinates relative to the standard basis of R^n, say $\mathbf{v}_j = [c_{1j}, \ldots, c_{nj}]$ (so $a_i = c_{i1}$). Then the matrix (c_{ij}) has the $\mathbf{v}_j$'s as its columns, so this matrix describes the linear transformation $R^n \to R^n$ sending the standard basis of R^n to $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Since the $\mathbf{v}_j$'s form a basis, this matrix is invertible: $\det(c_{ij}) \in R^\times$. Expanding the determinant along its first column shows $\det(c_{ij})$ is an R-linear combination of $a_1, \ldots, a_n$, so $\det(c_{ij}) \in (a_1, \ldots, a_n)$. Therefore the ideal $(a_1, \ldots, a_n)$ contains a unit, so the ideal is R. $\square$

Thus all stably free finitely generated R-modules are free if and only if for all n the "obvious" necessary condition for a vector in R^n to be part of a basis of R^n is a sufficient condition.

Example 3.4. If $[a_1, \ldots, a_n]$ in $\mathbf{Z}^n$ is part of a basis of $\mathbf{Z}^n$ then $\gcd(a_1, \ldots, a_n) = 1$. For example, the vector $[6, 9, 15]$ is not part of a basis of $\mathbf{Z}^3$ since its coordinates are all multiples of 3. The vector $[6, 10, 15]$ has no common factors among its coordinates (although each *pair* of coordinates has a common factor). Is it part of a basis of $\mathbf{Z}^3$? Essentially we are asking if the necessary condition in Theorem 3.3 is also sufficient over $\mathbf{Z}$. It is in this case: the vectors $[6, 10, 15], [1, 1, 0]$, and $[0, 3, 11]$ are a basis of $\mathbf{Z}^3$. (A matrix with these vectors as the columns has determinant ± 1.)

For any R, the necessary condition $(a_1, \ldots, a_n) = R$ in Theorem 3.3 is actually sufficient for $[a_1, \ldots, a_n]$ to be part of a basis of R^n when $n = 1$ and $n = 2$. For $n = 1$, if $(a_1) = R$ then a_1 is a unit and thus is a basis of R as an R-module. For $n = 2$, if $(a_1, a_2) = R$ then there are $b_1, b_2 \in R$ such that $a_1 b_1 + a_2 b_2 = 1$, so the matrix $\left(\begin{smallmatrix} a_1 & -b_2 \\ a_2 & b_1 \end{smallmatrix}\right)$ has determinant 1 and therefore its columns are a basis of R^2. What if $n > 2$? The necessary condition is sufficient when R is a PID by Corollary 3.2 since we already saw that stably free $\Rightarrow$ free when R is a PID. (*e.g.*, $R = \mathbf{Z}$ or $F[X]$). More generally, the necessary condition is sufficient when R is a Dedekind domain [6], [7], but Theorem 1.1 provides us with a ring admitting a stably free module that is not free, and this leads to a counterexample when $n = 3$.

Example 3.5. Let $R = \mathbf{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$. In the free module R^3, the triple $[x, y, z]$ satisfies the condition of Theorem 3.3: the ideal (x, y, z) of R is the unit ideal since $x^2 + y^2 + z^2 = 1$ in R. However, there is no basis of R^3 containing $[x, y, z]$. Indeed, assume there is a basis $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ where $\mathbf{v}_1 = [x, y, z]$. Then there is a matrix in $\mathrm{GL}_3(R)$ with first column $\mathbf{v}_1$, and the argument in the proof of Theorem 1.1 derives a contradiction from this.

The "sphere rings" $\mathbf{R}[x_1, \ldots, x_n]/(x_1^2 + \cdots + x_n^2 - 1)$ for any odd $n \geq 3$ provide additional examples where the condition in Theorem 3.3 is not sufficient to guarantee an n-tuple in R^n is part of a basis of R^n.

Another use of the ring $R = \mathbf{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$ as a counterexample in algebra involves matrices with trace 0. Since $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, any matrix of the form $AB - BA$ (called a commutator) has trace 0. Over a field, the converse holds [1]: every square matrix with trace 0 is a commutator. However, the matrix $\left(\begin{smallmatrix} x & y \\ z & -x \end{smallmatrix}\right)$ in $\mathrm{M}_2(R)$ has trace 0 and it is proved in [8] that this matrix is not a commutator in $\mathrm{M}_2(R)$. But all is not lost. A matrix with trace 0 is always a sum of two commutators [5].

Appendix A. Theorems of Gabel and Bass

Our discussion of stably free modules focused on finitely generated ones. The reason is that in the case of non-finitely generated modules there are no interesting stably free modules.

Theorem A.1 (Gabel)**.** *If M is stably free and not finitely generated then M is free.*

Proof. Let $F := M \oplus R^k$ be free. We want to show M is free.

Projection from F onto M is a surjective linear map, so M not being finitely generated implies F is not finitely generated. Let $\{e_i\}_{i\in I}$ be a basis of F, so the index set I is infinite.

Projection from F onto R^k is a surjective linear map $f\colon F \twoheadrightarrow R^k$ with kernel M. The standard basis of R^k is in the image of the span of finitely many e_i's, say the submodule $F' := Re_1 + \cdots + Re_\ell$ has $f(F') = R^k$. For any $\mathbf{v} \in F$, $f(\mathbf{v}) = f(\mathbf{v}')$ for some $\mathbf{v}' \in F'$. Then $\mathbf{v} - \mathbf{v}' \in \ker f = M$, so $F = F' + M$. The module F' is finite free and $F'/(M \cap F') \cong R^k$. Since R^k is free (and thus a projective module), there is an isomorphism $F' \cong N \oplus R^k$ where $N = M \cap F'$. Since $F' + M = F$, $F/F' \cong M/N$ and $F/F' = \bigoplus_{i>\ell} Re_i$ is free with *infinite* rank, so we can write $F/F' \cong R^k \oplus F''$ for some free F''. Therefore M/N is free, so

$$M \cong N \oplus (M/N) \cong N \oplus (F/F') \cong N \oplus R^k \oplus F'' \cong F' \oplus F'',$$

which is free. $\square$

To prove all stably free modules over a (nonzero) ring R are free is the same as showing $M \oplus R^k \cong R^\ell \Rightarrow M$ is free for any k and ℓ. When such an isomorphism occurs, $\ell - k = \dim_{R/\mathfrak{m}}(M/\mathfrak{m}M)$ for all maximal ideals $\mathfrak{m}$ in R, so $\ell - k$ is well-defined by M although ℓ and k are not. We call $\ell - k$ the *rank* of M. For example, if $M \oplus R \cong R^n$ then M has rank $n - 1$. We will prove a theorem of Bass which reduces the verification that all stably free R-modules are free to the case of even rank.

Lemma A.2. *If $M \oplus R \cong R^{2d}$ for some $d \geq 1$ then $M \cong R \oplus N$ for some R-module N.*

Proof. Composing an isomorphism $R^{2d} \cong M \oplus R$ with projection to the second summand gives us a surjective map $\varphi\colon R^{2d} \to R$ with kernel isomorphic to M. Since any linear map $R^{2d} \to R$ is dotting with a fixed vector, there is some $\mathbf{w} \in R^{2d}$ such that $\varphi(\mathbf{v}) = \mathbf{v} \cdot \mathbf{w}$ for all $\mathbf{v} \in R^{2d}$. Set $\mathbf{w} = (c_1, \ldots, c_{2d})$. Then

$$\varphi(c_2, -c_1, \ldots, c_{2d}, -c_{2d-1}) = 0.$$

Let $\mathbf{u} = (c_2, -c_1, \ldots, c_{2d}, -c_{2d-1}) \in \ker \varphi \cong M$. We will show there is a submodule N of M such that $M \cong R \oplus N$.

Choose $(r_1, \ldots, r_{2d}) \in R^{2d}$ such that $\varphi(r_1, \ldots, r_{2d}) = 1$, so $c_1 r_1 + \cdots + c_{2d} r_{2d} = 1$. Then $\mathbf{u} \cdot (r_2, -r_1, \ldots, r_{2d}, -r_{2d-1}) = 1$, so the linear map $f\colon R^{2d} \to R$ given by $f(\mathbf{v}) = \mathbf{v} \cdot (r_2, -r_1, \ldots, r_{2d}, -r_{2d-1})$ satisfies $f(\mathbf{u}) = 1$. Since $\mathbf{u} \in \ker \varphi$, the restriction of f to a linear map $\ker \varphi \to R$ is surjective and restricts to an isomorphism $R\mathbf{u} \to R$. Thus $M \cong \ker \varphi = R\mathbf{u} \oplus \ker f \cong R \oplus \ker f$. $\square$

Remark A.3. It is generally false that if $M \oplus R \cong R^{2d+1}$ then $M \cong R \oplus N$ for some N. An example is R being the sphere ring (2.3) when $2d + 1 \neq 1, 3$ or 7 and M being the tangent module T. Our work in Section 2 shows $T \oplus R \cong R^{2d+1}$. A proof that $T \not\cong R \oplus N$ for any N is in [3, pp. 33–35].

Theorem A.4 (Bass)**.** *The following conditions on a commutative ring R are equivalent.*

1. *All stably free finitely generated R-modules are free.*
2. *All stably free finitely generated R-modules of even rank are free.*

Proof. It's clear that (1) $\Rightarrow$ (2). To show (2) $\Rightarrow$ (1), suppose $M \oplus R^k \cong R^\ell$ (so $k \leq \ell$) with $\ell - k$ an odd number. If $k = 0$ then M is free. If $k > 0$ then $(M \oplus R) \oplus R^{k-1} \cong R^\ell$, so $M \oplus R$ is stably free of even rank $\ell - (k-1)$. Then $M \oplus R \cong R^{\ell-k+1}$, so $M \cong R \oplus N$ for some N

by Lemma A.2. Therefore $N \oplus R^2$ is free of even rank $\ell - k + 1$, so N is stably free of odd rank $(\ell - k + 1) - 2 = \ell - k - 1$. By induction $N \cong R^{\ell-k-1}$, so $M \cong R \oplus N \cong R^{\ell-k}$. $\square$

References

[1] A. A. Albert and B. Muckenhoupt, *On matrices of trace zero*, Michigan Math. J. **4** (1957), 1–3.

[2] W.H. Gustafson, P. R. Halmos, J. M. Zelmanowitz, *The Serre Conjecture*, Amer. Math. Monthly **85** (1978), 357–359.

[3] T. Y. Lam, "Serre's Problem on Projective Modules," Springer-Verlag, Berlin, 1978.

[4] B. McDonald, "Linear Algebra over Commutative Rings," Marcel Dekker, New York, 1984.

[5] Z. Mesyan, *Commutator Rings*, Bull Austral. Math Soc. **74** (2006), 279–288.

[6] I. Reiner, *Unimodular Complements*, Amer. Math. Monthly **63** (1956), 246–247.

[7] I. Reiner, *Completion of Primitive Matrices*, Amer. Math. Monthly **73** (1966), 380–381.

[8] M. Rosset and S. Rosset, *Elements of trace zero that are not commutators*, Comm. Algebra **28** (2000), 3059–3072.