A note on lifting isomorphisms of modules over PIDs

Darij Grinberg

version 0.4, 8 Oct 2018

This note has been written to supplement Keith Conrad's [1], though it is largely independent of the latter. I am going to show some (rather elementary) properties of free modules over PIDs and apply them to drop the "full submodule" resp. "nonzero determinant" restraints which qualify many statements made in [1]. Thanks are due to Keith Conrad for a correction and helpful remarks.

The LaTeX sourcecode of this note contains additional details of proofs inside "verlong" environments (i. e., between "`\begin{verlong}`" and "`\end{verlong}`"). I doubt they are of any use.

§1. Some properties of modules

Before we make any statements, let us clarify some notation:

Convention. In the following, $\mathbf{N}$ will denote the set of all nonnegative integers. This set includes 0.

Definition. An *integral domain* is defined as a commutative ring R with unity such that $1 \neq 0$ in R (that is, the unity of R does not equal the zero of R) and such that any two elements $a \in R$ and $b \in R$ satisfying $ab = 0$ must satisfy $(a = 0 \text{ or } b = 0)$. A *principal ideal domain* is defined as an integral domain R in which every ideal is principal (i.e., every ideal I of R can be written in the form $I = (a)$ for some $a \in R$). The word "PID" is an abbreviation for "principal ideal domain".

Definition. Let R be a commutative ring with unity. An R-module is said to be *finite free* if it has a finite basis.

We are going to prove all but one (Lemma A.2) of the following seven statements. Of course, very few of them are new.

Lemma A.1. Let R be a commutative ring with unity (not necessarily a PID). Let S be a finite free R-module. Let M be any R-module. Let $f : M \to S$ be a surjective R-module homomorphism. Then, there exists an R-submodule N of M such that $M = N \oplus (\operatorname{Ker} f)$ (an internal direct sum) and such that $f\mid_N : N \to S$ is an R-module isomorphism.

Lemma A.2. Let R be a PID. Every submodule of a finite free R-module is finite free.

Lemma A.3. Let R be a commutative ring with unity (not necessarily a PID). Let M be a finitely-generated R-module. Let f be a surjective R-module homomorphism $M \to M$. Then, f is an R-module isomorphism.

Lemma A.4. Let R be a commutative ring with unity (not necessarily a PID). Let $n \in \mathbf{N}$ and $m \in \mathbf{N}$ be such that $n \neq m$. Assume that $R^n \cong R^m$ as R-modules. Then, R is the trivial ring.

Lemma A.5. Let R be a commutative ring with unity (not necessarily a PID). Let S_1, S_2 and T be three finite free R-modules such that $S_1 \oplus T \cong S_2 \oplus T$ as R-modules. Then, $S_1 \cong S_2$ as R-modules.

Lemma A.6. Let R be a PID. Let M, N_1 and N_2 be three finite free R-modules. Let $p_1 : M \to N_1$ and $p_2 : M \to N_2$ be two surjective R-module homomorphisms. Let $j : N_1 \to N_2$ be an R-module isomorphism. Then, there exists an R-module isomorphism $k : M \to M$ such that $p_2 \circ k = j \circ p_1$. [1]

Proposition A.7. Let R be a PID. Let M be a finite free R-module. Let A_1 and A_2 be two R-module endomorphisms of M. Then, $A_1(M) = A_2(M)$ if and only if there exists a $U \in \operatorname{GL}(M)$ satisfying $A_1 = A_2 U$. (Note that $\operatorname{GL}(M)$ denotes the group of all R-module automorphisms of M. This group is isomorphic to the group of invertible $n \times n$ matrices over R, where n is the rank of the free R-module M.)

Proposition A.7 is the main result of this note, as it will help us generalize [1].

Lemma A.1 is one incarnation of the well-known fact that free modules are projective (and that projections on projective modules split); we will nevertheless give a proof of it for the sake of completeness. (It should be noticed that it doesn't really require commutativity of R.)

Lemma A.2 is a well-known fact and we will merely give references to its proof, not least because its proofs are not too easy.

Lemma A.3 is a known fact and will be proven using Nakayama's lemma (other proofs can be found in literature, to which we will give haphazard

[1] In other words, there exists an R-module isomorphism $k : M \to M$ which makes the diagram

$$\begin{tikzcd}
M \arrow[r, dotted, "k"] \arrow[d, two heads, "p_1"'] & M \arrow[d, two heads, "p_2"] \\
N_1 \arrow[r, "\cong", "j"'] & N_2
\end{tikzcd}$$

commute.

references). It is a generalization of the known linear-algebraic fact that a surjective endomorphism of a finite-dimensional vector space is always an isomorphism. Notice that the analogous property of **injective** endomorphisms does not generalize to modules over arbitrary rings.

Lemma A.4 is a quick and well-known corollary of Lemma A.3; it is the so-called "IBN property" ("IBN" stands for "invariant basis number") of commutative rings (and holds not only for commutative rings, but also for certain classes of noncommutative ones).

Lemma A.5 is a very easy consequence of Lemma A.4. It would fail if the word "finite" would be dropped from "finite free", and it would also fail if "finite free" would be replaced by "finitely-generated".

§2. Proofs

Proof of Lemma A.1. We have $S = f(M)$ (since f is surjective). Let $(e_1, e_2, ..., e_n)$ be a finite basis of the R-module S (such a basis exists since S is finite free). For every $i \in \{1, 2, ..., n\}$, pick an element x_i of M satisfying $e_i = f(x_i)$ (such an x_i exists since $e_i \in S = f(M)$).

Now, recall that we can define an R-linear map from a free R-module by specifying its values on the elements of a basis. This allows us to define an R-linear map $g : S \to M$ by setting

$$(g(e_i) = x_i \qquad \text{for every } i \in \{1, 2, ..., n\}).$$

Consider the R-linear map $g : S \to M$ defined this way. Clearly, $g(S)$ is an R-submodule of M.

Every $i \in \{1, 2, ..., n\}$ satisfies

$$(f \circ g)(e_i) = f\left(\underbrace{g(e_i)}_{=x_i}\right) = f(x_i) = e_i = \mathrm{id}_S(e_i).$$

In other words, the two maps $f \circ g : S \to S$ and $\mathrm{id}_S : S \to S$ are equal to each other on each element of the basis $(e_1, e_2, ..., e_n)$ of S. Since these two maps $f \circ g$ and id_S are both R-linear, this yields that the two maps $f \circ g$ and id_S must be identical (because any two linear maps which are equal to each other on each element of a basis of their domain must be identical). In other words, $f \circ g = \mathrm{id}_S$.

Now, let $x \in g(S) \cap (\operatorname{Ker} f)$. Then, $x \in g(S) \cap (\operatorname{Ker} f) \subseteq g(S)$, so that there exists some $y \in S$ such that $x = g(y)$. Consider this y. Then, $f\left(\underbrace{x}_{=g(y)}\right) = f(g(y)) = \underbrace{(f \circ g)}_{=\mathrm{id}_S}(y) = \mathrm{id}_S(y) = y$. Compared with $f(x) = 0$

(since $x \in g(S) \cap (\operatorname{Ker} f) \subseteq \operatorname{Ker} f$), this yields $y = 0$. Hence, $x = g\left(\underbrace{y}_{=0}\right) = g(0) = 0$ (since g is R-linear).

Now forget that we fixed x. We have thus shown that every $x \in g(S) \cap (\operatorname{Ker} f)$ satisfies $x = 0$. In other words, $g(S) \cap (\operatorname{Ker} f) = 0$. The internal direct sum $g(S) \oplus (\operatorname{Ker} f)$ is thus well-defined.

Now, let $z \in M$. Then,

$$\begin{aligned} f(z - g(f(z))) &= f(z) - \underbrace{f(g(f(z)))}_{\substack{=(f\circ g)(f(z)) \\ =\operatorname{id}_S(f(z)) \\ (\text{since } f\circ g = \operatorname{id}_S)}} \qquad (\text{since } f \text{ is } R\text{-linear}) \\ &= f(z) - \underbrace{\operatorname{id}_S(f(z))}_{=f(z)} = f(z) - f(z) = 0, \end{aligned}$$

so that $z - g(f(z)) \in \operatorname{Ker} f$. Thus,

$$z = g\left(\underbrace{f(z)}_{\in S}\right) + \underbrace{(z - g(f(z)))}_{\in \operatorname{Ker} f} \in g(S) + (\operatorname{Ker} f) = g(S) \oplus (\operatorname{Ker} f)$$

(since we know that the internal direct sum $g(S) \oplus (\operatorname{Ker} f)$ is well-defined). Now forget that we fixed z. We hence have proven that every $z \in M$ satisfies $z \in g(S) \oplus (\operatorname{Ker} f)$. In other words, $M \subseteq g(S) \oplus (\operatorname{Ker} f)$. Combined with $g(S) \oplus (\operatorname{Ker} f) \subseteq M$ (which is obvious), this yields $M = g(S) \oplus (\operatorname{Ker} f)$.

A moment of thought reveals that $\operatorname{Ker}\left(f \mid_{g(S)}\right) = g(S) \cap (\operatorname{Ker} f)$. In light of $g(S) \cap (\operatorname{Ker} f) = 0$, this rewrites as $\operatorname{Ker}\left(f \mid_{g(S)}\right) = 0$. Thus, the R-linear map $f \mid_{g(S)}$ is injective.

On the other hand,

$$\left(f \mid_{g(S)}\right)(g(S)) = f(g(S)) = \underbrace{(f \circ g)}_{=\operatorname{id}_S}(S) = \operatorname{id}_S(S) = S.$$

Thus, the R-linear map $f \mid_{g(S)}$ is surjective. Combined with the fact that the R-linear map $f \mid_{g(S)}$ is injective, this yields that the R-linear map $f \mid_{g(S)}$ is bijective. Thus, $f \mid_{g(S)}$ is an R-module isomorphism.

Altogether, we thus know that $g(S)$ is an R-submodule of M such that $M = g(S) \oplus (\operatorname{Ker} f)$ (an internal direct sum) and such that $f \mid_{g(S)} : g(S) \to S$ is an R-module isomorphism. Thus, there exists an R-submodule N of M such that $M = N \oplus (\operatorname{Ker} f)$ (an internal direct sum) and such that $f \mid_N : N \to S$ is an R-module isomorphism (namely, $N = g(S)$). This proves Lemma A.1. □

Proof of Lemma A.2. Lemma A.2 is probably the most well-known among the many consequences of the Smith normal form. As such, it appears (in one or another form) in almost every good book written about abstract algebra, and in a multitude of lecture notes[2]. We will not give a proof of Lemma A.2, but instead just refer to some of many places where it is proven:

- Lemma A.2 follows from [2, Theorem 8.25].
- Lemma A.2 follows from [12, Theorem 2.1].
- Lemma A.2 is part of [4, Theorem 3.7.1].
- Lemma A.2 is a consequence of [3, Chapter XI, Theorem 12].
- Lemma A.2 follows from the (somewhat stronger) Theorem 6.0.1 in Chapter 11 ("Finitely-generated modules") of Paul Garrett's lecture notes [5].
- Lemma A.2 also follows from The Freedom Theorem in Lecture 5 of McNulty's [6].
- Lemma A.2 follows from [7, Chapter 4, Corollary 4.6.2].

□

Proof of Lemma A.3. There is no real need to give a proof of Lemma A.3 here, since it is known: For example, it appears in [13] as Theorem 5.3, with my f renamed as φ. But let me give a slightly different proof of Lemma A.3 (though a rather well-known one; for example, it is identical with the one given in [8, Theorem 0.3.2], [10, Theorem 2.4] and [11, Theorem 1]). We will use the following fact:

> **Nakayama lemma:** Let S be a commutative ring with unity, and let N be a finitely-generated S-module. Let I be an ideal of S such that $I \cdot N = N$. Then, there exists an $s \in S$ such that $s \equiv 1 \operatorname{mod} I$ and $sN = 0$.

This is merely one of the many forms of the Nakayama lemma[3], but it is the one most suitable for our needs. Proofs of the Nakayama lemma, in (more

[2] Actually, googling for the statement of Lemma A.2 is a good way to find lecture notes in abstract algebra.

[3] The statements referred to as the "Nakayama lemma" in literature are numerous, and some of them are harder to derive from each other than prove from scratch. Nevertheless, they are widely regarded as equivalent (not merely like any two correct assertions). The form of the Nakayama lemma that we are using is probably the one most familiar to commutative algebraists.

The Nakayama lemma is also known as the "NAK lemma", with "NAK" abbreviating "Nakayama-Azumaya-Krull" rather than "NAKayama".

or less) the form given above, can be found in [9, Corollary 2.5], [8, Theorem 0.3.1], [11, Lemma 2], [10, Theorem 2.2] and various other places.

Consider the situation of Lemma A.3. Let T be an indeterminate, and consider the polynomial ring $R[T]$. By the universal property of the polynomial ring, there exists one and only one R-algebra homomorphism $R[T] \to \operatorname{End} M$ which sends T to f. Consider the R-module M as an $R[T]$-module via this homomorphism. Then, clearly, T acts as f on this $R[T]$-module M. In other words, $Tm = f(m)$ for every $m \in M$.

Let I be the ideal (T) of $R[T]$. Then, $T \in I$, so that $T \cdot M \subseteq I \cdot M$. But since

$$T \cdot M = \left\{ \underbrace{Tm}_{=f(m)} \mid m \in M \right\} = \{f(m) \mid m \in M\} = f(M) = M$$

(since M is surjective), this rewrites as $M \subseteq I \cdot M$. Combined with the obvious inclusion $I \cdot M \subseteq M$, this yields $I \cdot M = M$. Hence, the Nakayama lemma (applied to $S = R[T]$ and $N = M$) yields that there exists an $s \in R[T]$ such that $s \equiv 1 \bmod I$ and $sM = 0$. Consider this s.

Since $s \equiv 1 \bmod I$, there exists a $q \in I$ such that $s = 1 + q$. Consider this q. Since $q \in I = (T)$, the polynomial q is divisible by T. Thus, there exists some $r \in R[T]$ such that $q = rT$. Consider this r. Then, $s = 1 + \underbrace{q}_{=rT} = 1 + rT$, so that every $m \in M$ satisfies

$$m - (-rT)m = m + rTm = \underbrace{(1 + rT)}_{=s} m = sm = 0$$

(since $s \underbrace{m}_{\in M} \in sM = 0$). In other words, every $m \in M$ satisfies

$$m = (-rT)m = -r \underbrace{Tm}_{=f(m)} = -r \cdot f(m).$$

Hence, every $m \in M$ such that $f(m) = 0$ satisfies $m = -r \cdot \underbrace{f(m)}_{=0} = -r \cdot 0 = 0$. In other words, f is injective. Since we know that f is surjective, this yields that f is bijective. Combined with the fact that f is an R-module homomorphism, this yields that f is an R-module isomorphism. Lemma A.3 is proven. □

Proof of Lemma A.4. Since $n \neq m$, we have either $n < m$ or $m < n$. Since the scenery is symmetric in n and m, we can WLOG assume that $n < m$. Assume this.

Since $R^n \cong R^m$ as R-modules, there exists an isomorphism $I : R^n \to R^m$. Consider this I. Since I is an isomorphism, we have $I(R^n) = R^m$.

Let $(e_1, e_2, ..., e_n)$ be the standard basis of the free R-module R^n. Let $(f_1, f_2, ..., f_m)$ be the standard basis of the free R-module R^m.

Now, recall that we can define an R-linear map from a free R-module by specifying its values on the elements of a basis. Hence, we can define an R-linear map $g : R^m \to R^n$ by setting

$$\left(g(f_i) = \begin{cases} e_i, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases} \qquad \text{for every } i \in \{1, 2, ..., m\} \right).$$

Consider this map g. Since $n < m$, it is easily seen that the map g is surjective (since all elements of the basis $(e_1, e_2, ..., e_n)$ of R^n occur as images of basis vectors f_i under g). Hence, $g \circ I : R^m \to R^m$ is also surjective (as I is an isomorphism). According to Lemma A.3 (applied to $M = R^n$ and $f = g \circ I$), this entails that $g \circ I$ is an R-module isomorphism. Thus, $g \circ I$ is injective, so that g is injective as well. But the definition of g yields $g(f_m) = 0$ (since $m > n$), and thus (by the injectivity of g) we have $f_m = 0$. Since f_m is an element of a basis of the R-module R^m (namely, of the basis $(f_1, f_2, ..., f_m)$), this yields that $1 = 0$ in R. In other words, R is the trivial ring. Lemma A.4 is proven.

□

An alternative proof of Lemma A.4 would be to apply [14, Corollary 5.11].

Proof of Lemma A.5. Since S_1, S_2 and T are finite free R-modules, there exist elements s_1, s_2 and t of $\mathbf{N}$ such that $S_1 \cong R^{s_1}$, $S_2 \cong R^{s_2}$ and $T \cong R^t$ as R-modules. Consider these s_1, s_2 and t.

If $s_1 = s_2$, then Lemma A.5 is obvious (since $s_1 = s_2$ leads to $S_1 \cong R^{s_1} = R^{s_2} \cong S_2$ as R-modules). Hence, let us now assume (for the rest of the proof of Lemma A.5) that $s_1 \neq s_2$. Thus, $s_1 + t \neq s_2 + t$. But

$$\underbrace{S_1}_{\cong R^{s_1}} \oplus \underbrace{T}_{\cong R^t} \cong R^{s_1} \oplus R^t \cong R^{s_1+t} \qquad \text{as } R\text{-modules},$$

and similarly $S_2 \oplus T \cong R^{s_2+t}$ as R-modules. Thus, $R^{s_1+t} \cong S_1 \oplus T \cong S_2 \oplus T \cong R^{s_2+t}$ as R-modules. Thus, Lemma A.4 (applied to $n = s_1 + t$ and $m = s_2 + t$) yields that R is the trivial ring. But since every module over the trivial ring is 0, this shows that $S_1 = 0$ and $S_2 = 0$, so that $S_1 = 0 = S_2$ as R-modules. This proves Lemma A.5.

□

Proof of Lemma A.6. Applying Lemma A.1 to $S = N_1$ and $f = p_1$, we obtain the following: There exists an R-submodule J_1 of M such that $M = J_1 \oplus (\operatorname{Ker}(p_1))$ (an internal direct sum) and such that $p_1 \mid_{J_1} \colon J_1 \to N_1$ is an R-module isomorphism. Fix such a J_1.

Similarly, fix an R-submodule J_2 of M such that $M = J_2 \oplus (\operatorname{Ker}(p_2))$ (an internal direct sum) and such that $p_2 \mid_{J_2} \colon J_2 \to N_2$ is an R-module isomorphism. The existence of such a J_2 is guaranteed by Lemma A.1 again.

We know that every submodule of a finite free R-module is finite free (due to Lemma A.2). Thus, the R-modules J_1, J_2, $\operatorname{Ker}(p_1)$ and $\operatorname{Ker}(p_2)$ are finite free (being submodules of the finite free R-module M).

Since the map $p_2 \mid_{J_2} \colon J_2 \to N_2$ is an R-module isomorphism, its inverse $(p_2 \mid_{J_2})^{-1} : N_2 \to J_2$ is well-defined and an R-module isomorphism as well.

Since all three maps $p_1 \mid_{J_1} \colon J_1 \to N_1$, $j : N_1 \to N_2$ and $(p_2 \mid_{J_2})^{-1} : N_2 \to J_2$ are R-module isomorphisms, their composition $(p_2 \mid_{J_2})^{-1} \circ j \circ (p_1 \mid_{J_1}) : J_1 \to J_2$ must also be an R-module isomorphism. Thus, $J_2 \cong J_1$ as R-modules. Now,

$$\begin{aligned}(\operatorname{Ker}(p_1)) \oplus J_1 = J_1 \oplus (\operatorname{Ker}(p_1)) = M = \underbrace{J_2}_{\cong J_1} \oplus (\operatorname{Ker}(p_2)) \\ \cong J_1 \oplus (\operatorname{Ker}(p_2)) = (\operatorname{Ker}(p_2)) \oplus J_1\end{aligned}$$

as R-modules. Thus, Lemma A.5 (applied to $S_1 = \operatorname{Ker}(p_1)$, $S_2 = \operatorname{Ker}(p_2)$ and $T = J_1$) yields that $\operatorname{Ker}(p_1) \cong \operatorname{Ker}(p_2)$ as R-modules. Thus, there exists an R-module isomorphism $I : \operatorname{Ker}(p_1) \to \operatorname{Ker}(p_2)$. Consider this I.

Now, define a map

$$\Phi : J_1 \oplus (\operatorname{Ker}(p_1)) \to J_2 \oplus (\operatorname{Ker}(p_2))$$

by

$$\Phi(u, v) = \left(\left((p_2 \mid_{J_2})^{-1} \circ j \circ (p_1 \mid_{J_1})\right)(u), I(v)\right) \qquad \text{for every } (u, v) \in J_1 \times (\operatorname{Ker}(p_1)).$$

Clearly, Φ is an R-module isomorphism from $J_1 \oplus (\operatorname{Ker}(p_1))$ to $J_2 \oplus (\operatorname{Ker}(p_2))$ (in fact, Φ is the direct sum of the isomorphisms $(p_2 \mid_{J_2})^{-1} \circ j \circ (p_1 \mid_{J_1}) : J_1 \to J_2$ and $I : \operatorname{Ker}(p_1) \to \operatorname{Ker}(p_2)$). Since both $J_1 \oplus (\operatorname{Ker}(p_1))$ and $J_2 \oplus (\operatorname{Ker}(p_2))$ are simply M, this means that Φ is an R-module isomorphism from M to M.

Now, every $x \in M$ satisfies

$$(p_2 \circ \Phi)(x) = (j \circ p_1)(x)$$

(as revealed by a straightforward computation[4]). In other words, $p_2 \circ \Phi = j \circ p_1$.

[4] *Proof.* Let $x \in M$. Since $x \in M = J_1 \oplus (\operatorname{Ker}(p_1))$, we can write x in the form $x = u + v$

So we know that Φ is an R-module isomorphism from M to M such that $p_2 \circ \Phi = j \circ p_1$. Hence, there exists an R-module isomorphism $k : M \to M$ such that $p_2 \circ k = j \circ p_1$ (namely, $k = \Phi$). This proves Lemma A.6. □

Proof of Proposition A.7. First of all, if there exists a $U \in \operatorname{GL}(M)$ satisfying $A_1 = A_2 U$, then we clearly have $A_1(M) = A_2(M)$ [5].

for some $u \in J_1$ and $v \in \operatorname{Ker}(p_1)$. Consider these u and v. Then, $x = u + v$ corresponds to the pair (u, v) under the identification of the internal direct sum $M = J_1 \oplus (\operatorname{Ker}(p_1))$ with the external direct sum $J_1 \oplus (\operatorname{Ker}(p_1))$. Hence, $x = (u, v)$. On the other hand, identifying the internal direct sum $M = J_2 \oplus (\operatorname{Ker}(p_2))$ with the external direct sum $J_2 \oplus (\operatorname{Ker}(p_2))$, we have

$$\left(\left(\left(p_2 \mid_{J_2}\right)^{-1} \circ j \circ \left(p_1 \mid_{J_1}\right)\right)(u), I(v)\right) = \left(\left(p_2 \mid_{J_2}\right)^{-1} \circ j \circ \left(p_1 \mid_{J_1}\right)\right)(u) + I(v),$$

so that

$$\begin{aligned}\Phi\left(\underbrace{x}_{=(u,v)}\right) &= \Phi(u, v) = \left(\left(\left(p_2 \mid_{J_2}\right)^{-1} \circ j \circ \left(p_1 \mid_{J_1}\right)\right)(u), I(v)\right) \\ &= \left(\left(p_2 \mid_{J_2}\right)^{-1} \circ j \circ \left(p_1 \mid_{J_1}\right)\right)(u) + I(v).\end{aligned}$$

Applying the map p_2 to both sides of this equality, we obtain

$$\begin{aligned}(p_2 \circ \Phi)(x) &= p_2\left(\left(\left(p_2 \mid_{J_2}\right)^{-1} \circ j \circ \left(p_1 \mid_{J_1}\right)\right)(u) + I(v)\right) \\ &= p_2\left(\left(\left(p_2 \mid_{J_2}\right)^{-1} \circ j \circ \left(p_1 \mid_{J_1}\right)\right)(u)\right) + \underbrace{p_2(I(v))}_{\substack{=0 \\ (\text{since } I(v) \in \operatorname{Ker}(p_2))}} \\ &= p_2\left(\left(\left(p_2 \mid_{J_2}\right)^{-1} \circ j \circ \left(p_1 \mid_{J_1}\right)\right)(u)\right) \\ &= \underbrace{\left(p_2 \circ \left(p_2 \mid_{J_2}\right)^{-1}\right)}_{=\left(p_2 \mid_{J_2}\right) \circ \left(p_2 \mid_{J_2}\right)^{-1} = \operatorname{id}} \left(\left(j \circ \left(p_1 \mid_{J_1}\right)\right)(u)\right) \\ &= \left(j \circ \left(p_1 \mid_{J_1}\right)\right)(u) = j(p_1(u)).\end{aligned}$$

On the other hand, since $x = u + v$, we have

$$\begin{aligned}p_1(x) &= p_1(u + v) = p_1(u) + \underbrace{p_1(v)}_{\substack{=0 \\ (\text{since } v \in \operatorname{Ker}(p_1))}} \qquad (\text{since } p_1 \text{ is linear}) \\ &= p_1(u),\end{aligned}$$

so that $p_1(u) = p_1(x)$. Thus, $(p_2 \circ \Phi)(x) = j\left(\underbrace{p_1(u)}_{=p_1(x)}\right) = j(p_1(x)) = (j \circ p_1)(x)$, qed.

[5] *Proof.* Assume that there exists a $U \in \operatorname{GL}(M)$ satisfying $A_1 = A_2 U$. Consider this U. Since $U \in \operatorname{GL}(M)$, we know that U is an R-module automorphism of M, so that $U(M) = M$.

We now only need to prove the opposite direction . So assume that $A_1(M) = A_2(M)$. We shall prove that there exists a $U \in \operatorname{GL}(M)$ satisfying $A_1 = A_2 U$.

Let M' be the R-submodule $A_1(M)$ of M.

By Lemma A.2, every submodule of a finite free R-module is finite free. Thus, M' (being a submodule of the finite free R-module M) is finite free.

Since $A_1(M) = M'$, we can define a surjective R-module homomorphism $p_1 : M \to M'$ by

$$(p_1(x) = A_1(x) \text{ for every } x \in M). \tag{1}$$

Consider this p_1.

Since $A_2(M) = A_1(M) = M'$, we can define a surjective R-module homomorphism $p_2 : M \to M'$ by

$$(p_2(x) = A_2(x) \text{ for every } x \in M). \tag{2}$$

Consider this p_2.

Lemma A.6 (applied to $N_1 = M'$, $N_2 = M'$ and $j = \operatorname{id}_{M'}$) shows that there exists an R-module isomorphism $k : M \to M$ such that $p_2 \circ k = \operatorname{id}_{M'} \circ p_1$. Consider this k. We know that k is an R-module isomorphism $M \to M$, thus an R-module automorphism of M. Thus, $k \in \operatorname{GL}(M)$.

But we have $A_2 \circ k = A_1$. (Indeed, this follows from $p_2 \circ k = \operatorname{id}_{M'} \circ p_1 = p_1$ upon noticing that the maps p_1 and p_2 are identical with the maps A_1 and A_2, respectively, apart from having a different target set.)

Thus, there exists a $U \in \operatorname{GL}(M)$ satisfying $A_1 = A_2 U$ (namely, $U = k$). This completes the proof of Proposition A.7. □

§3. Generalizing [1]

Proposition A.7 allows us to generalize the results of Conrad's [1]. First of all, our Proposition A.7 is obviously a generalization of [1, Lemma 2]. The notions of "aligned bases" and "simultaneously aligned bases" defined in [1] can be generalized:

> **Definition.** Let R be a PID, n be a positive integer, and M be a finite free R-module of rank n.
>
> **(a)** Let M' be a submodule of M (not necessarily of rank n). The structure theorem for modules over a PID (or the theory of the

Now, from $A_1 = A_2 U$, we conclude that $A_1(M) = (A_2 U)(M) = A_2\left(\underbrace{U(M)}_{=M}\right) = A_2(M)$, qed.

Smith normal form) shows that there exists a basis $(e_1, e_2, ..., e_n)$ of M and scalars $a_1, a_2, ..., a_n$ such that $M' = \bigoplus_{i=1}^{n} Ra_i e_i$. In such a situation, we will say that $(e_1, e_2, ..., e_n)$ and $(a_1 e_1, a_2 e_2, ..., a_n e_n)$ are a pair of *aligned* bases for M and M', whether or not $(a_1 e_1, a_2 e_2, ..., a_n e_n)$ is a basis of M'. (Of course, $(a_k e_k)_{k \in \{1,2,...,n\};\ a_k \neq 0}$ **is** a basis of M' in this case, so the only thing that can keep the sequence $(a_1 e_1, a_2 e_2, ..., a_n e_n)$ from being a basis of M' are zero elements.)

(b) Let M' and M'' be two submodules of M. If there exists a basis $(e_1, e_2, ..., e_n)$ of M and scalars $a'_1, a'_2, ..., a'_n$ such that $M' = \bigoplus_{i=1}^{n} Ra_i e_i$, as well as scalars $a''_1, a''_2, ..., a''_n$ such that $M'' = \bigoplus_{i=1}^{n} Rb_i e_i$, then we say that M' and M'' admit *simultaneously aligned bases*.

With this definition, [1, Theorem 3] still holds without the conditions $\det A \neq 0$ and $\det B \neq 0$, and [1, Corollary 5] is still valid if the "with nonzero determinants" condition is removed. The proofs of these results don't require any new arguments apart from replacing the (easy) proof of [1, Lemma 2] by the (not so easy) proof of our Proposition A.7.

References

[1] Keith Conrad, *Simultaneously aligned bases*, 2013.
`http://www.math.uconn.edu/~kconrad/blurbs/`

[2] Anthony W. Knapp, *Basic Algebra*, digital second edition, 2016.
`http://www.math.stonybrook.edu/~aknapp/download.html`

[3] Saunders Mac Lane, Garrett Birkhoff, *Algebra*, 3rd edition, AMS 1999.

[4] Jonathan Brundan, *Math 647/8/9 notes, Fall 2004*.
`http://darkwing.uoregon.edu/~brundan/math647fall04/`

[5] Paul Garrett, *Abstract Algebra*, course notes, last updated 20 Oct 2012.
`http://www.math.umn.edu/~garrett/m/algebra/`

[6] George F. McNulty, *Rings and Modules*, Fall 2010 course notes, January 21, 2011.
`http://www.math.sc.edu/~mcnulty/algebra/grad/fall2010.pdf`

[7] Robert B. Ash, *Abstract Algebra: The Basic Graduate Year*, revised 11/02.
`http://www.math.uiuc.edu/~r-ash/Algebra.html`

[8] Robert B. Ash, *A Course In Commutative Algebra*, revised Jan 2006.
`http://www.math.uiuc.edu/~r-ash/ComAlg.html`

[9] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley 1969.

[10] Hideyuki Matsumura, *Commutative ring theory*, CUP 1989.

[11] Kazimierz Szymiczek, *NAK and injectivity of surjections*, 2004.
`http://www.math.us.edu.pl/zatl/szymiczek/referaty/`

[12] Keith Conrad, *Modules over a PID*, 2014.
`http://www.math.uconn.edu/~kconrad/blurbs/`

[13] Keith Conrad, *Universal Identities I*, 2013.
`http://www.math.uconn.edu/~kconrad/blurbs/`

[14] Keith Conrad, *Exterior powers*, 2013.
`http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/extmod.pdf`