Classification of finitely generated modules over Dedekind domains, with and without projective modules, and reconciliation of approaches

Victor Wang

December 20, 2014

In this post (specifically in Section 4.2) we give a proof of the classification of finitely generated (f.g.) modules M over a Dedekind domain A avoiding the notion of projective modules. (Instead we rely on pure submodules, which give a slightly more transparent/natural/direct approach to the classification problem at hand, at the expense of the greater generality afforded by the projective module approach. Along the way we also explain why these approaches are really not so different after all.)

We gradually build up from the more familiar special cases when A is a principal ideal domain (PID) or even just a field. Along the way we discuss some relevant abstractions, such as the splitting lemma (Section 2).

I would like to thank Profs. Yifeng Liu and Bjorn Poonen for teaching me in 18.705 and 18.785, respectively, this past (Fall 2014) semester at MIT. Thanks also to Alison Miller for catching a typo in Exercise 3.

1 Preliminaries

First we recall the simpler case when A is a PID. In fact, we start with the simplest case of fields:

Exercise 1 (Structure theorem for f.g. modules over a field (i.e. vector spaces), "right splitting" approach via free modules)**.** *Let k be the field, V the module (i.e. k-vector space).*

Let W be a k-submodule (i.e. subspace) of V, and suppose V/W is free over k. Lift a basis $\overline{v_1},\dots,\overline{v_\ell}$ of V/W (arbitrarily) to prove that $V \simeq_k W \oplus V/W$.

(The key point is that if some k-linear combination $a_1\overline{v_1}+\cdots+a_\ell\overline{v_\ell}=\overline{0}$, i.e. $a_1v_1+\cdots+a_\ell v_\ell \equiv 0 \pmod W$, then by linear independence in V/W we must have $a_1v_1+\cdots+a_\ell v_\ell=0$.)

Conclude by induction that the f.g. modules over k are precisely the free modules over k, i.e. those isomorphic to k^n for some $n \geq 0$.

Remark 1. *It's a separate (but obviously important) issue to show that the k-dimension is well-defined, i.e. $k^m \simeq_k k^n$ if and only if $m=n$. For (PIDs and) Dedekind domains there is a similar notion of rank in the torsion-free case, but we won't focus on these sorts of issues throughout the post.*

Exercise 2 (Structure theorem for f.g. modules over a PID, algorithmic generators and relations approach)**.** *Let A be the PID, M the module.*

1. *Take a finite set of generators of M, i.e. a surjection $A^g \twoheadrightarrow M$, and look at the kernel L (so $M \simeq A^g/L$), which describes the "relations" among the set of generators. Show that L is f.g. over A. (In other words, M is finitely presented.)*

2. *Take a finite presentation $A^r \xrightarrow{\twoheadrightarrow L \hookrightarrow} A^g \twoheadrightarrow M$ (here $M \simeq A^g/L$), which corresponds to an $r \times g$ (possibly "overdetermined") "relations matrix" X. Mimicking Gaussian elimination (but using only A-row/column operations), show that A can be "diagonalized", i.e. put in a Smith normal form. This corresponds to a suitable A-linear change of generators of M, combined with an alternative A-linear change of the "description" of the relations among the generators. (This shouldn't be confused with diagonalization of linear operators. It's really more or less just solving a system of A-linear equations.)*

Exercise 3 (F.g. torsion-free modules over PIDs are free, "right splitting" approach via free modules)**.** *Let A be the PID, M the torsion-free f.g. module.*

Mimicking Exercise 1, prove that M is a free A-module. (Hint: Take a "saturated" submodule N of M, in the sense that if $am \in N$ for some $a \neq 0$ then $m \in N$, or equivalently, that M/N is torsion-free. Now show that $M \simeq_A N \oplus M/N$.)

Exercise 4 (Torsion part (of f.g. module over PID) breaks off, "right splitting" approach via free modules)**.** *Let A be the PID, M the f.g. module, M_{tors} its torsion submodule.*

Using and then mimicking Exercise 3, prove that $M \simeq_A M_{tors} \oplus M/M_{tors}$.

Remark 2. *Exercise 2 is the first proof on Wikipedia, as well as the proof in Artin's "Algebra".*

Another approach, with key steps outlined in Exercises 3 and 4, (which doesn't explicitly reduce or otherwise work with generators/relations) is to (less explicitly) find a special A-submodule N of M and try to prove that N is a direct summand of M. (The whole point is that this is generally sutble when A isn't a vector space—this is one of the main problems of representation theory.) For instance, see the second proof on Wikipedia, or Emerton's answer at the discussion on MathOverflow. (These are effectively done using the fact that free modules A^n are projective, which is also the standard approach to the general Dedekind domain problem.)

Nonetheless, these two approaches have the same overall flavor: intuitively, the fully "saturated" submodules are the ones that break off (as direct summands), whether we identify them algorithmically (as in the first approach) or through some characterization (as in the second approach).

2 Starting from scratch: (canonical) direct sum decomposition

In general, say we have an R-submodule $N \subseteq M$ (or slightly more generally, an injection $N \hookrightarrow M$, though importantly, this injection may not be unique), and we wish to prove N is a direct summand of M, i.e. $M = N \oplus P$ for some $P \subseteq M$.

Slightly more generally, let's look at (all the terms of) the whole short exact sequence $N \hookrightarrow M \twoheadrightarrow P$ (sometimes it's better to think in terms of P, so that $N = \ker(M \twoheadrightarrow P)$, and sometimes it's better to think in terms of N, so that $P \simeq M/N$). What does it take to get a "canonical" splitting? (We roughly follow the terminology in the linked Wikipedia article.)

2.1 ("Canonical") left splitting

Viewing N as a submodule of M, it suffices to get a "compatible R-projection" $\pi : M \twoheadrightarrow N$, i.e. a (surjective) map such that $\pi\iota = \mathrm{Id}_N$, where $\iota : N \hookrightarrow M$ is the inclusion map. (Then $\iota\pi : M \to M$ will be a projection in the usual linear algebra sense.)

For instance, when $R = k[G]$ is a group algebra, one can prove Maschke's theorem by constructing a $k[G]$-projection (specifically, by "averaging" a k-projection into a $k[G]$-projection).

(N is called an injective module if and only if we have such a "left splitting" whenever M is a module containing N.)

2.2 ("Canonical") right splitting

Let π' denote the surjection $M \twoheadrightarrow P$. It suffices to get a "compatible R-inclusion" $\iota' : P \hookrightarrow M$, i.e. an (injective) map such that $\pi'\iota' = \mathrm{Id}_P$.

(P is called a projective module if and only if we have such a "right splitting" whenever M is a module with a surjection onto P.

For instance, when $R = A$ is a Dedekind domain, see Exercise 6.)

2.3 Briefly, the relation between splittings and the direct sum decomposition

In the $N \subseteq M \twoheadrightarrow M/N$ case (for definiteness), the $\pi : M \twoheadrightarrow N$ and $\iota' : M/N \hookrightarrow M$ are related as follows: $m = \pi(m) + \iota'(m \pmod{N})$ for any $m \in M$.

Exercise 5 (based on Exercise 3.38 from Pete Clark's aforementioned commutative algebra notes)**.** *Let R be a ring. Prove that [every R-module is injective] if and only if [every R-module is projective].*

For example, prove that if $\operatorname{char} k \nmid |G|$ for a field k and finite group G, then both statements hold for $R = k[G]$ the group algebra.

3 Sketch of (classical?) projective module approach

We now return to the general case of Dedekind domains A. Let K be the fraction field of A.

Exercise 6 (F.g. torsion-free modules over Dedekind domains are projective, "right splitting" approach via projective modules)**.** *Let A be the Dedekind domain, M the torsion-free module.*

For a detailed treatment of projective modules, we defer to Pete Clark's notes. (Incidentally, he also started an interesting MathOverflow discussion on the difficulties of teaching free, projective, and flat modules.)

1. *The* ***rank*** *of M is defined as the (clearly finite) dimension of $K \otimes_A M$, or equivalently the localization $(A^\times)^{-1}M$, as a vector space over K. (In other words, we're embedding the A-module M inside a K vector space in the only reasonable way.)*

2. *(Key step.) Prove that rank-1 modules M are just (up to A-module isomorphism) the fractional ideals $I \subset K$ of A, and show that these are projective.*

3. *Prove that direct sums of projective modules are projective, and conclude by induction that the f.g. torsion-free modules over A are (projective and) precisely (up to isomorphism) the finite direct sums of fractional ideals of A.*

4. *Give a direct proof (not using that direct sums of projective modules are projective) that f.g. torsion-free modules over A are projective, by mimicking the proof for rank-1 modules. Of course, by induction, this further induces an alternative proof of the classification of f.g. torsion-free modules.*

Remark 3. *Exercise 6 is the heart of the (classical?—I believe it's Steinitz' original proof) projective module approach to breaking off submodules (as direct summands). The use of localization (or similar Bezout's identity arguments) seems pretty fundamental in general; we use it as well to verify the the pure submodule criterion below (in the alternative approach: see the key Theorem 13). Exercise 7 further clarifies the similarity.*

Here are some references:

1. *hilbertthm90's sequence of three blog posts, which I believe roughly follow May's notes on Dedekind domains.*

2. *Chapter III, section 22, page 144 of "Representation theory of finite groups and associative algebras" by C. Curtis and I. Reiner.*

3. *Pete Clark's commutative algebra notes, Chapter 20.6. Finitely generated modules over a Dedekind domain, page 290.*

4. *The first chapter of Henri Cohen's "Advanced Topics in Computational Number Theory" gives an interesting proof of the projectivity: $I \oplus I^{-1} \simeq A \oplus II^{-1} = A \oplus A$, so I is a direct summand of a free module, hence projective.*

5. *This was the approach given in 18.785 (MIT Fall 2014, taught by Prof. Bjorn Poonen) Problem Set 4.*

Remark 4. *It seems difficult to apply the generators and relations approach (from Exercise 2) to the Dedekind domain problem. For instance, it doesn't seem easy to describe an analogous Smith normal form—in the final decomposition into $A/\wp^e$ (torsion) and $I \subset K$ (torsion-free fractional ideals), the fractional ideals are not principal (though they are generated by at most 2 elements). That said, since $I_1 \oplus \cdots \oplus I_n \simeq A^{n-1} \oplus I_1 \cdots I_n$, all but one component can be taken principal (in general), so maybe there's some hope. Also maybe "Hermite and Smith normal form algorithms over Dedekind domains" by Henri Cohen is relevant.*

4 Alternative pure submodule approach

4.1 Pure submodule criterion, in the spirit of generators and relations

Let R be a ring, $N \subseteq M$ a submodule. The usefulness of the following definition will soon become clear. Overall the idea is to refine the "right splitting approach" from Exercises 3 and 4 in the direction of the algorithmic generators-and-relations ideas of Exercise 2, rather than the projective module direction from Exercise 6.

Definition 5. *We define a submodule N (of a fixed R-module M) to be **pure** if the following condition holds: if we choose finitely many $z_1, \ldots, z_r \in N$, and we can write the z_i as R-linear combinations $z_i = \sum_{j=1}^{\ell} x_{ij} m_j$ of some $m_1, \ldots, m_\ell \in M$, then the z_i can in fact be written as corresponding R-linear combinations **with the** m_j **taken inside** N. In other words, we can find $n_1, \ldots, n_\ell \in N$ such that $z_i = \sum_{j=1}^{\ell} x_{ij} n_j$ for all i.*

Of course, we can rephrase this condition concisely in terms of matrices: for $Z \in N^{r\times 1}$ and $X \in R^{r\times \ell}$, we have $Z \in X \cdot M^{\ell\times 1}$ if and only if $Z \in X \cdot N^{\ell\times 1}$.

Example 1. *If N is a direct summand of M, i.e. $M = N \oplus P$ for some $P \subseteq M$ (internal direct sum), then the projection $\pi : M \twoheadrightarrow N$ allows us to simply take $n_i = \pi(m_i)$ for all i in any such scenario. So N is a pure submodule of M.*

Observation 6 (Equivalent definition of purity)**.** *$N \subseteq M$ is pure if and only if following condition holds: for any finite choice of $m_1, \ldots, m_\ell \in M$ and $X \in R^{r\times \ell}$ with $X(m_1, \ldots, m_\ell)^T \equiv 0 \pmod{N}$, there exist $n_1, \ldots, n_\ell \in N$ with $X(m_1 - n_1, \ldots, m_\ell - n_\ell)^T = 0$.*

Theorem 7 (Pure submodule criterion (for direct summands), 18.705 (MIT Fall 2014, taught by Prof. Yifeng Liu) Midterm, Problem 3.4)**.** *Let R be a ring, $N \subseteq M$ a submodule. Further suppose M/N is finitely presented (e.g. if R is noetherian and M/N is f.g.).*

*If N is a pure submodule of M, then N is a direct summand of M, i.e. $M = N \oplus P$ **internally** for some submodule $P \subseteq M$ (in particular, the direct sum here must be canonical). In other words, when M/N is finitely presented, the converse of Example 1 holds.*

Proof. Everything will be canonical here, i.e. we'll prove that the short exact sequence $N \hookrightarrow M \twoheadrightarrow M/N$ splits (in the sense of the splitting lemma from Section 2).

Observation 8. *If $\overline{m_i} = m_i + N$ $(1 \le i \le \ell)$ generate M/N, then a right splitting (induced by) $\iota' : M/N \hookrightarrow M$ is just a well-defined map sending each $\overline{m_i}$ to some lift/pre-image $m_i - n_i \equiv m_i \pmod{N}$ (i.e. the n_i must lie in N).*

It's easy to see that a choice of $n_1, \ldots, n_\ell \in N$ works (i.e. the corresponding construction of ι' is consistent) if and only if we have $\sum x_i(m_i - n_i) = 0$ whenever $\sum x_i m_i \equiv 0 \pmod{N}$ (because the latter is equivalent to $\sum x_i \overline{m_i} = \overline{0} \in M/N$). (And if ι' is well-defined, then the corresponding projection $\pi : M \twoheadrightarrow N$ satisfies $n_i = \pi(m_i)$.)

This closely resembles the condition for purity given in Observation 6, modulo a final technical point—since M/N is finitely presented, the generators $\overline{m_1}, \ldots, \overline{m_\ell}$ can be chosen such that **we only have to worry about finitely many R-linear conditions** (since in a finite presentation, the set of R-linear conditions, viewed via corresponding "coefficient vectors" as a submodule of R^ℓ, is f.g.). So we're done.

□

Remark 9. *Example 1 and Theorem 7 together show that when M/N is finitely presented, purity is more or less a "relative (to M)" version of injective modules.)*

Exercise 7 (Connection between projective module and pure submodule approaches)**.** *Prove that a **finitely presented** R-module P is projective if and only if the following condition holds: for any R-surjection $\phi : Y \twoheadrightarrow P$, the kernel $\ker\phi \subseteq Y$ is a pure submodule of Y.*

Given the "equational" nature of Definition 5, is this connection related to the dual basis lemma, or another "equational" characterization of projective modules? (I haven't thought through this much myself.)

Remark 10. *If we only assume M/N to be f.g., then as long as we tweak Definition 5 to include **infinite** systems of equations, the natural analog of Theorem 7 holds, with essentially the same proof. This is probably still useful; for instance, I believe the proof of the Dedekind module classification below would still go through. Cf. Greg Kuperberg's related comments in the aforementioned MathOverflow discussion.*

(I believe this is more or less a "relative (to M)" version of algebraically compact (or pure-injective) modules.)

Although we won't need it for the application below, here's the rest of Problem 3:

Exercise 8 (Based on 18.705 (MIT Fall 2014, taught by Prof. Yifeng Liu) Midterm, Problem 3)**.** *In this exercise we do **not** assume that M/N is finitely presented.*

1. *Show that N is pure if and only if the induced R-map $N \otimes_R E \hookrightarrow M \otimes_R E$ is injective for every finitely presented R-module E. (This is the usual first definition.)*

   Remark 11. *It may or may not help to use the equational criterion for vanishing of elements of tensor products; I haven't thought about this too carefully myself.*

2. *Prove Example 1 using the tensor product formulation.*

3. *When R is a PID (e.g. take $R = \mathbb{Z}$), show that a submodule N of M is pure if and only if $N \cap xM = xN$ for all nonzero $x \in R^\times$. (In other words, the $r = s = 1$ condition in Definition 5 is "enough" over PIDs!)*

   Remark 12. *Hint: Probably the easiest solution is to combine the tensor product formulation with the structure theorem over PIDs. It would be interesting to find a more conceptual way to prove the result without the structure theorem, which might even lead to an alternative proof of the structure theorem.*

4. *Does the previous part still work for Dedekind domains A? If not, what's the best analog (e.g. how many (r, s) pairs are necessary in Definition 5)? (I haven't actually worked this out myself, but I imagine there's a reasonable answer. Feel free to take the structure theorem over Dedekind domains A for granted.)*

4.2 Applying pure submodule criterion to original problem

The following is the key result.

Theorem 13 (Saturated submodules (of f.g. modules over Dedekind domains) break off as direct summands, "right splitting approach" via pure submodule criterion)**.** *Let A be a Dedekind domain, M a f.g. module over A. Let N be an $A^\times$-saturated submodule of M, i.e. such that if $am \in N$ for some nonzero $a \in A^\times$ and $m \in M$, then $m \in N$, or equivalently, M/N is torsion-free. (For intuition, think about avoiding $\mathbb{Z}$-submodules like $2\mathbb{Z}/2^2\mathbb{Z} \subset \mathbb{Z}/2^2\mathbb{Z}$ or $2\mathbb{Z} \subset \mathbb{Z}$. One could also phrase this in terms of suitable tensor products, e.g. by $K = \operatorname{Frac}(A)$ in the torsion-free case, or a "semi-localization" of A at a finite set of primes in the torsion case.)*

Then N is a pure submodule of M, hence a direct summand of M by the pure submodule criterion (Theorem 7)—indeed, M/N is f.g. over the noetherian ring A, hence finitely presented.

Proof. Suppose for some (finitely many) $z_1, \ldots, z_r$ in N we have $(z_1, \ldots, z_r)^T = X(m_1, \ldots, m_\ell)^T$ for some matrix $X \in A^{r \times \ell}$. The key idea is localization: if we temporarily "add denominators to N", then the system of equations will be easier to solve. Then in the spirit of Bezout's identity, we'll take a suitable linear combination to get a solution with denominator 1.

Let $\wp$ be a prime of A, and $S = A - \wp$ the corresponding multiplicative subset. Then $S^{-1}N$ is a $(S^{-1}A)^\times$-saturated $S^{-1}A$-submodule of $S^{-1}M$, i.e. $S^{-1}M/S^{-1}N = S^{-1}(M/N)$ (via exactness of localization) is torsion-free. But $S^{-1}A = A_\wp$ is a DVR, hence a PID, so by the structure theorem over PIDs (specifically Exercise 3), $S^{-1}M/S^{-1}N$ is a free $A_\wp$-module. Consequently (following the reasoning from Exercises 3 and 4), $S^{-1}N$ is a direct summand of $S^{-1}M$.

Thus (by Example 1) $S^{-1}N$ is a pure $A_\wp$-submodule of $S^{-1}M$. But $(z_1/1, \ldots, z_r/1)^T = X(m_1/1, \ldots, m_\ell/1)^T$, so by Definition 5 (of purity) we have $(z_1/1, \ldots, z_r/1)^T \in X(n_1/s_1, \ldots, n_\ell/s_\ell)^T$ for some $n_i/s_i \in S^{-1}N$.

It follows that for each prime $\wp$ of A, there exists $s_\wp \in S$ with $s_\wp \cdot (z_1, \ldots, z_r)^T \in XN^{\ell \times 1}$. Finally, it suffices to find an A-linear combination of $s_\wp$ equal to 1. But this is easy: the A-ideal $\langle \{s_\wp\} \rangle_A$ generated by the $s_\wp$ is not contained in $\wp$ for any prime ideal $\wp$ (because it contains the element $s_\wp \in A - \wp$), so $\langle \{s_\wp\} \rangle_A = A$, i.e. there exists a finite A-linear combination of $s_\wp$ equal to 1. □

Remark 14. *We can avoid localizing at sets containing zerodivisors by instead carefully semi-localizing, i.e. working with S of the form $S := (A - \wp) \cap (\bigcap_{\mathfrak{p} | \mathrm{z.div}(M)} (A - \mathfrak{p}))$(note that $1 \notin \mathrm{z.div}(M)$). This actually makes the final paragraph easier; we just need to check $S^{-1}A$ is still a PID, which follows from a "pretty strong approximation theorem" (essentially the Chinese remainder theorem (CRT) for Dedekind domains) argument.*

Corollary 15 (Torsion part (of f.g. module over Dedekind domain) breaks off, "right splitting approach" via pure submodule criterion)**.** *If M is f.g. over a Dedekind domain A, then M_{tors} is a direct summand of M.*

Proof. M/M_{tors} is torsion-free, so we may apply Theorem 13. □

Remark 16. *Note that the proof here doesn't (at least explicitly) use on the classification/characterization of torsion-free modules over A. This contrasts with the standard development where one uses Exercise 6 (specifically, that torsion-free modules are projective) to prove the right splitting of $M_{tors} \hookrightarrow M \twoheadrightarrow M/M_{tors}$, which is in fact also the approach for PIDs given in Exercises 3 and 4.*

By the previous corollary, $M \simeq_A M_{tors} \oplus M/M_{tors}$, where M/M_{tors} is torsion-free, so it remains to (separately) classify decompositions of torsion and torsion-free modules M.

Corollary 17 (Decomposition of f.g. torsion-free modules over Dedekind domains, "right splitting approach" via pure submodule criterion)**.** *If M is f.g. torsion-free over a Dedekind domain A, then $M \simeq I_1 \oplus \cdots \oplus I_n$ for $n = \dim_K(K \otimes_A M = S^{-1}A) < \infty$ (the **rank** of M) fractional ideals $I_1, \ldots, I_n$, and fractional ideals $I \subset K$ of A are indeed (of rank 1 and hence) indecomposable.*

Proof. In view of Theorem 13, our strategy is to find $A^\times$-saturated submodules of M. We may think of M as living inside a f.d. K-vector space $K \otimes_A M \simeq K^n$ (equivalently, localize M w.r.t. the set $A^\times$). Then we'll show that the K-coordinates correspond to indecomposable direct summands of M, which will be isomorphic to fractional ideals of A (which are generally not principal—this is why the Smith normal form approach seems difficult—see Remark 4).

Let $m \neq 0$ in M. Saturate the submodule $\langle m \rangle_A$ to get $N := (\langle m \rangle_A)^S$ (in general it will no longer be principal), where $S = A^\times$. Then $\dim_K(S^{-1}N = K \otimes_A \langle m \rangle_A) = 1$, so $N \simeq I$ for some fractional ideal $I \subset K$ of A, which (since N is saturated) breaks off as a direct summand of M. The K-dimension of the localization/tensored-up K-vector space $S^{-1}M = K \otimes_A M$ decreases by 1 each time we break a fractional ideal off, so the eventual decomposition is $M \simeq I_1 \oplus \cdots \oplus I_n$ for some fractional ideals $I_1, \ldots, I_n$, with each I_j indeed indecomposable (as it has corresponding K-dimension 1). □

The hard work is done, but for completeness we include the proof of the torsion classification:

Theorem 18 (Classification of f.g. torsion modules over Dedekind domains)**.** *If $M = M_{tors}$ is torsion, then M is an $A/\operatorname{Ann}(M) = \prod A/\wp^{v_\wp(\operatorname{Ann}(M))}$-module (here we've used CRT), which induces a decomposition $M = \bigoplus (A - \wp)^{-1}M$ (there are certainly more concrete ways to think about all of this). (One could probably phrase this in terms of primary decompositions, but it doesn't seem particularly worthwhile.) Each localized $(A - \wp)^{-1}M$ is easy to classify, since $A/\wp^e$ is a PID.*

(Actually, without the CRT prime power decomposition, we could've directly noted that $A/\operatorname{Ann}(M)$ is a PID (cf. Remark 14)—though the proof happens to use "pretty strong approximation"/CRT (but in a different way).)