

Notes on elementary divisors for modules over a PID
Patrick Brosnan

I wanted to write down a proof of the classification of modules over a PID. We had one presented in class on Friday, November 7. However, I wanted to have a version on the web as well. The point of this proof is to stay as close to the proof that Milne gives in his group theory text as possible.

Lemma 0. We have $\gcd(a_1, \dots, a_r) = \gcd(a_1, \gcd(a_2, \dots, a_r))$. Moreover, in a PID, $\gcd(a, b)R = aR + bR$ and $\gcd(a_1, \dots, a_r)R = a_1R + a_2R + \dots + a_rR$.

Proof. We already showed that $\gcd(a, b)R = aR + bR$ in class. The rest is very easy and I leave it as an exercise.

Lemma 1. Let M be a module over a PID R generated by two elements $x, y \in M$. Suppose $a, b \in R$ and $\gcd(a, b) = 1$. Then M is generated by $ax + by$ and one other element of M .

Proof. Since $\gcd(a, b) = 1$, we can find $s, t \in R$ such that $sa + tb = 1$. Then I claim that M is generated by $ax + by$ and $tx - sy$. To see this, let N be the submodule of M generated by $ax + by$ and $tx - sy$. Then clearly $N \subset M$. But also $x = s(ax + by) + b(tx - sy)$ and $y = t(ax + by) - a(tx - sy)$, so $M \subset N$.

Lemma 2. Let M be a module over a PID R generated by elements $m_1, \dots, m_r \in M$. Suppose, we have $(a_i)_{i=1}^r$ in R such that $\gcd(a_1, \dots, a_r) = 1$. Then there exists generators m'_1, \dots, m'_r for M such that $m'_1 = \sum a_i m_i$.

Proof. Assume, to get a contradiction, that r is the smallest integer for which the lemma is false. We know by the previous lemma that $r > 2$. Then there is a module M generated by elements $m_1, \dots, m_r \in M$ and elements $a_i \in R$ such that $\gcd(a_1, \dots, a_r) = 1$ but such that there exist no generators m'_1, \dots, m'_r of M with $m'_1 = \sum a_i m_i$. We must necessarily have all a_i non-zero (or else we could easily contradict the minimality of r). Let N denote the submodule of M generated by m_2, \dots, m_r . Set $d = \gcd(a_2, \dots, a_r)$. Then by our assumption that r is a minimal counterexample, there exists m''_2, \dots, m''_r generators for N such that $m''_2 = \sum_{i=2}^r (a_i/d)m_i$. But then $\gcd(a_1, d) = 1$ so, since $m'_1 = a_1 m_1 + d m''_2$, we have $m_1 R + m''_2 R = m'_1 R + m''_2 R$ for some $m'_2 \in m_1 R + m''_2 R$. We now set $m'_i = m''_i$ for $i > 2$ and get a contradiction because the m'_i generate M .

Now, if N_1, N_2 are two modules over a PID R , then $N_1 \oplus N_2$ is simply the group $N_1 \times N_2$ equipped with the module structure $r(n_1, n_2) = (rn_1, rn_2)$ for $r \in R, n_i \in N_i$.

Theorem. Let M be a finitely generated module over a PID R . Let $r = r(M)$ be the minimum number of generators required. Then, there exists nonunits $d_1, \dots, d_r \in R$ such that

- (a) $d_1 | d_2 | \dots | d_r$.
- (b) $M \cong \bigoplus_{i=1}^r R/d_i R$.

Moreover, if $M \cong \bigoplus_{i=1}^s R/d'_i$ with $d'_1 | d'_2 \dots | d'_s$ then $r = s$ and $d_i \sim d'_i$.

Proof. We induct on r . For $r = 0$, this is clear because then $M = 0$. So suppose $r \geq 1$. Choose generators m_1, \dots, m_r for M such that $\text{Ann}(m_1)$ is as large as possible. (We can do this because R is noetherian.) Since R is a PID, we can write $(d_1) = \text{Ann}(m_1)$ for some non-unit $d_1 \in R$. Now I claim that

$$Rm_1 \cap (Rm_2 + \dots + Rm_r) = 0.$$

To see this, it suffices to show that there is no relation

$$\sum_{i=1}^r a_i m_i = 0$$

with $a_1 m_1 \neq 0$.

Let I denote the ideal of all a_1 such that there is a relation as above. (It is easy to see that this is an ideal.) Note that $\text{Ann}(m_1) \subset I$. Since R is a PID, we can find a relation as above where $I = a_1R$. Set $d = \gcd(a_1, \dots, a_r)$ and $b_i = a_i/d$. Then, by Lemma 2, there exists a generating set m'_1, \dots, m'_r for M where $m'_1 = \sum b_i m_i$. Now note that $\text{Ann}(m'_1) \supset (d) \supset (a_1) = I \supset \text{Ann}(m_1)$. Since, by assumption $\text{Ann}(m_1)$ is the largest possible, this implies that $\text{Ann}(m'_1) = I = \text{Ann}(m_1)$. Thus $a_1 m_1 = 0$. This implies that $M \cong Rm_1 \oplus (Rm_2 + \dots + Rm_r)$.

Now I claim that $\text{Ann}(m_1) \supset \text{Ann}(m_i)$ for all i . To see this, suppose $J := \text{Ann}(m_1) + \text{Ann}(m_i)$ is strictly bigger than $\text{Ann}(m_1)$. Since R is a PID, we can write $\text{Ann}(m_i) = d_i$. But then set $d = \gcd(d_1, d_i)$ and write $m'_1 := (d_1/d)m_1 + (d_i/d)m_i$. By Lemma 2, there is an r element generating set m'_1, \dots, m'_r for M . But, since $\text{Ann}(m'_1) \supset J = dR$, this contradicts our assumption that m_1 had the largest possible annihilator among elements of r -element generating sets.

Now that we have existence, let us prove uniqueness. That is we wish to show that, for any decomposition $M \cong \bigoplus_{i=1}^s R/d'_i$ as in the statement of the theorem, we have $r = s$ and $d_i \sim d'_i$. To get a contradiction, let us assume that M is a module for which this does not hold with $r(M)$ minimal.

Now, note that, for $a, b \in R$, we have $a(R/bR) \cong (aR + bR)/bR$. If $d = \gcd(a, b)$, then $a(R/bR) \cong R/(b/d)R$. It follows that $d_1 M \cong \bigoplus_{i=2}^r R/(d_i/d_1)R \cong \bigoplus_{i=1}^s R/(d'_i/\gcd(d_1, d'_i))R$. By induction, we must have $d_i/d_1 \sim d'_i/\gcd(d'_i, d_1)$ for all $i = 1, \dots, s$. In particular, $\gcd(d'_1, d_1) = d'_1 \Rightarrow d'_1 | d_1$. Using the same argument but switching the roles of d_1 and d'_1 , we see that $d_1 | d'_1$. Thus $d_1 \sim d'_1$.

Now, we want to prove that $r = s$. Let I be a maximal ideal containing d_1 (and thus d'_1). It follows that M/IM is a vector space over the field R/I of dimension s and of dimension r . This is true because, for the factor, $M_i := R/d_i R$ we have $M_i/IM_i \cong R/I$. It follows that $r = s$.

Now the uniqueness follows from an easy induction from the fact that $d_1 \sim d'_1$.