Class notes, rings and modules : some of 23/03/2017 and 04/04/2017

Thomas Rüd and Julia Gordon

Fundamental Theorem of finitely generated modules over PIDs

Theorem 0.1. *Let R be a PID and M a finitely generated $R-$module. Then we can write*

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_n^{\alpha_n}),$$

for some $r, n \geq 0$ and p_i prime elements (not necessarily distinct) of R.

Moreover, this decomposition is unique, i.e. if there is another decomposition

$$M \cong R^\ell \oplus R/(q_1^{\beta_1}) \oplus \cdots \oplus R/(q_m^{\beta_m}),$$

then $r = \ell, m = n$ and up to reordering, $(p_i^{\alpha_i}) = (q_i^{\beta_i})$ (equality of ideals not generators).

The number r in the decomposition is the **rank** of our module.

This is the theorem in *Elementary divisor* form. The proof we followed in class was: first, prove this theorem in the *Invariant factor* form, and then simply decompose the invariant factors as products of prime elements, and use the Chinese Remainder Theorem.

The main step in the proof of the fundamental theorem

Since every finitely generated module M is isomorphic to a quotient of a free module R^n by a submodule N (see the first paragraph of the proof of Theorem 5 in §12.1 in DF), all we really need to understand is the submodules of free modules, and the corresponding quotients.

Theorem 0.2 (Theorem 12.4 in DF)**.** *Let R be a PID and $F = R^n$ a free $R-$module of rank n. If $N \leq F$ is a submodule, then*

(a) *N is free of rank $m \leq n$.*

(b) *There is a basis* $\{x_1, \ldots, x_n\}$ *of* F *and elements* $a_1, \ldots, a_m \in R$ *such that* $a_i | a_{i+1}$ *and* $\{a_1 f_1, \ldots, a_n f_m\}$ *is a basis for* N. (I called such bases of F and N "aligned with each other").

These numbers a_i *are called the* Invariant factors *of the quotient module* F/N.

The proof is an algorithm for finding such a bases for F and N. Instead of the proof, we illustrate this algorithm by an example.

Take $R = \mathbb{Z}$, and $F = \mathbb{Z}^2$. Let N be generated by the vectors $v_1 = \langle 1, 2 \rangle$ and $v_2 = \langle 3, 1 \rangle$. Here is a picture:

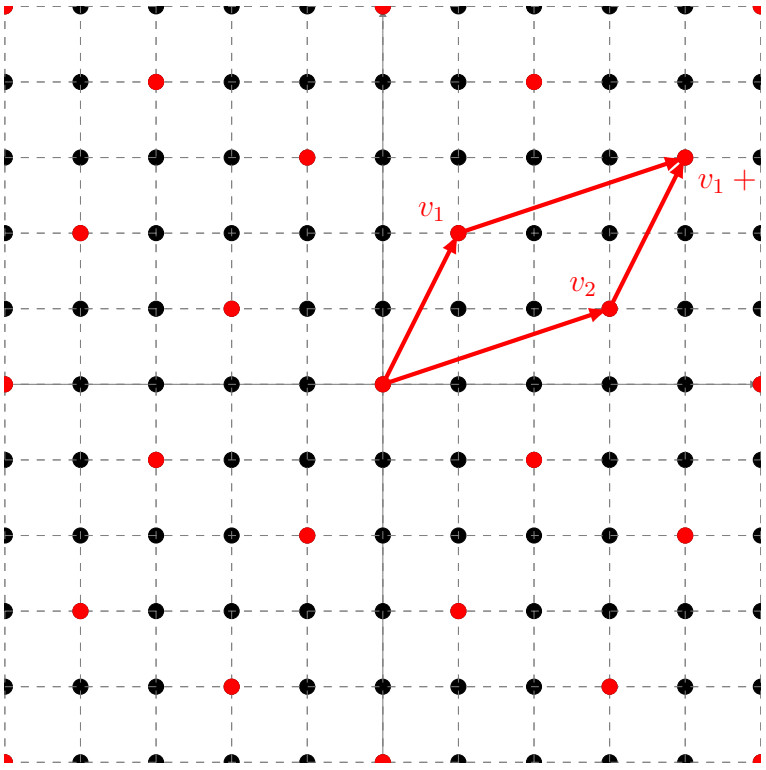

Figure 1: Situation of the problem: elements of N are the red dots

As we see, the quotient is not completely obvious. On the other hand, if the basis of N had been "aligned" with the standard basis of $\mathbb{Z}^2$, it would have been easy to compute the quotient: compare this with the picture of a different submodule, $N' \subset \mathbb{Z}^2$:

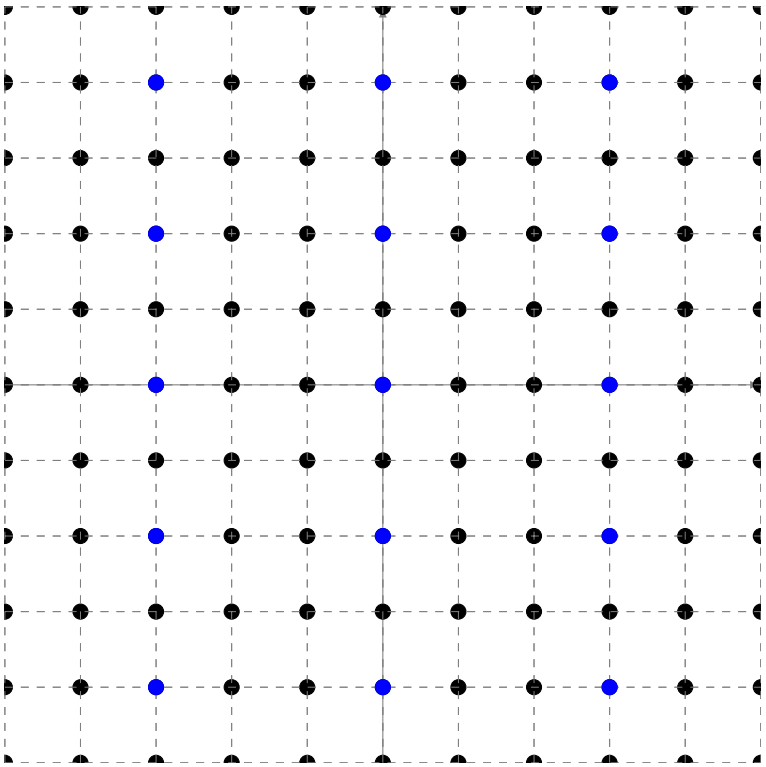

Figure 2: Situation of the problem: elements of N' are the blue dots

Here N' is a direct sum of $2\mathbb{Z}$ and $3\mathbb{Z}$, and we have $\mathbb{Z}^2/N' = \mathbb{Z} \oplus \mathbb{Z}/(2\mathbb{Z} \oplus 3\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. This example illustrates that it is very convenient to have the basis of N to be "aligned" with a basis of M in order to compute the quotient. Thus, our goal now is to find such aligned bases for the submodule N from the first picture.

Here is an algorithm for doing it. We write the coordinates of the generators of N as rows of a matrix (called relations matrix). In our example, it is:

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}.$$

Then we do row and column operations (very much like Gaussian elimination, but we are not allowed to divide by any numbers) in order to try and diagonalize the matrix A. The allowed operations are:

1. permute rows or columns of A,
2. For some i, j, replace Row number i of A with (Row i)+c(Row j), where $c \in \mathbb{Z}$,
3. Similar operation on columns instead of rows.

Here is what happens to our matrix: we first replace Row 2 with (Row 2-3(Row1)), and then replace Column 2 with (Column 2-2(Column 1)) and get:

$$\begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 2 \\ 0 & -5 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 \\ 0 & -5 \end{bmatrix}.$$

Now, one can check (easy) that row operations correspond to operations on a generating set for N. In particular, our first operation of replacing Row 2 with (Row 2-3(Row1)) corresponded to replacing the vector v_2 with $v_2 - 3v_1$. It is slightly harder to see that column operations correspond to changing the generating set of the ambient module $F = \mathbb{Z}^2$. In particular, our second operation corresponded to replacing the standard basis e_1, e_2 of $\mathbb{Z}^2$ with the vectors e_1 and $e_1 + 2e_2$. Here is what we got:

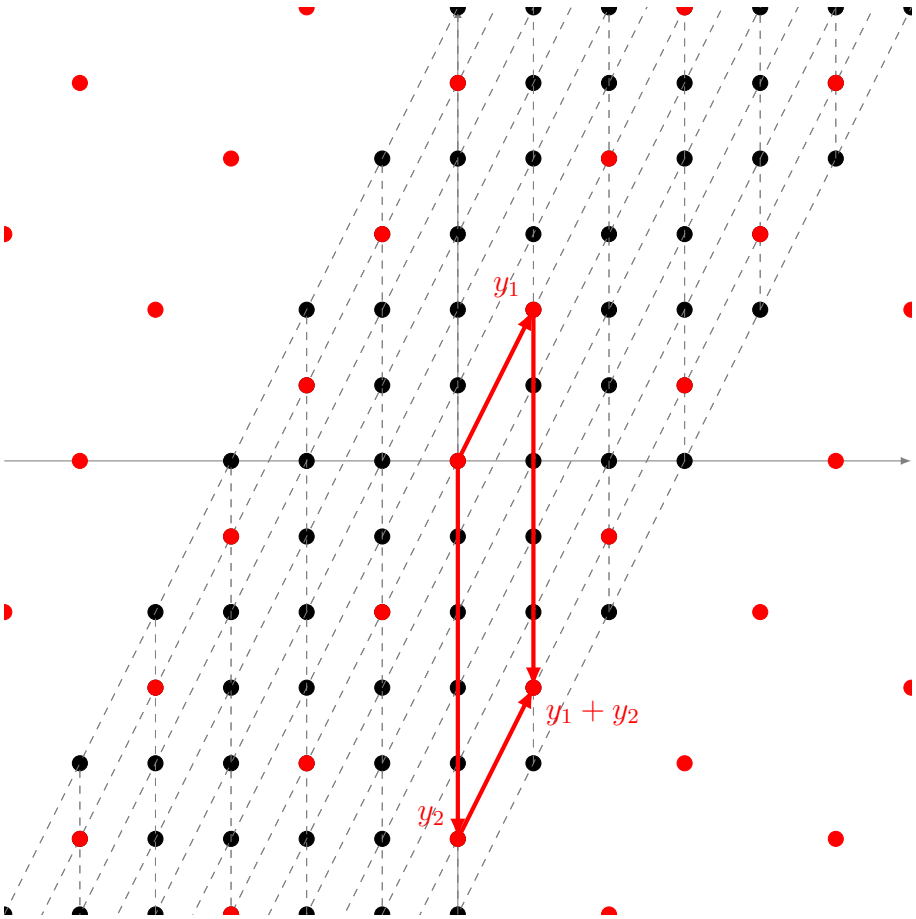

Figure 3: dashed lines go along the new basis for $\mathbb{Z}^2$, and the red vectors are the new basis for N (aligned with the new basis for $\mathbb{Z}^2$). Note that both the black lattice ($\mathbb{Z}^2$) and the red lattice (N) are exactly the same as in Figure 1, just the bases changed.

Now we have the new bases for both $\mathbb{Z}^2$ and or N: the new basis of $\mathbb{Z}^2$ is $x_1 = \langle 1, 2\rangle$ (in the old coordinates), and $x_2 = \langle 0, 1\rangle$. The new basis of N is $y_1 = x_1$, and $y_2 = -5x_2$. This is reflected in the fact that the new relations matrix is diagonal. (In the notation of the theorem, we have $a_1 = 1$, and $a_2 = -5$). Our picture illustrates this: the new basis of N is aligned with the new basis of $\mathbb{Z}^2$.

Finally, it is easy to find the quotient $\mathbb{Z}^2/N$:

$$Z^2/N = (\mathbb{Z}x_1 \oplus \mathbb{Z}x_2)/(\mathbb{Z}y_1 \oplus \mathbb{Z}y_2) \simeq \mathbb{Z}x_1/\mathbb{Z}x_1 \oplus \mathbb{Z}x_2/\mathbb{Z}(-5x_2) \simeq \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/(-5) \simeq \mathbb{Z}/(5).$$