MAS 5312 – Lecture for March 25, 2020

Richard Crew

The uniqueness part of the structure theorem can be stated as follows:

The uniqueness part of the structure theorem can be stated as follows:

Theorem

Suppose R is a PID, s, t, k, ℓ are natural numbers and $d_1, \ldots, d_k$, $e_1, \ldots, e_\ell$ are nonzero, nonunit elements of R such that

$$d_1 | d_2 | \cdots | d_k \quad \text{and} \quad e_1 | e_2 | \cdots | e_\ell.$$

If

$$R^s \oplus \bigoplus_i R/(d_i) \simeq R^t \oplus \bigoplus_i R/(e_i)$$

then $s = t$, $k = \ell$, and $d_i \sim e_i$ for all i.

The uniqueness part of the structure theorem can be stated as follows:

Theorem

Suppose R is a PID, s, t, k, ℓ are natural numbers and $d_1, \ldots, d_k$, $e_1, \ldots, e_\ell$ are nonzero, nonunit elements of R such that

$$d_1 | d_2 | \cdots | d_k \quad \text{and} \quad e_1 | e_2 | \cdots | e_\ell.$$

If

$$R^s \oplus \bigoplus_i R/(d_i) \simeq R^t \oplus \bigoplus_i R/(e_i)$$

then $s = t$, $k = \ell$, and $d_i \sim e_i$ for all i.

Proof. Denote by M the R-module on both sides of the isomorphism. We have already proven that $s = t$: it's the rank of M. Similarly the direct sum over i is the torsion submodule of this module.

Evidently d_i and e_i can be replaced by any elements such that $d_i' \sim d_i$ and $e_i' \sim e_i$. It will help to make a systematic choice of such d_i and e_i.

Evidently d_i and e_i can be replaced by any elements such that $d_i' \sim d_i$ and $e_i' \sim e_i$. It will help to make a systematic choice of such d_i and e_i. We can (1) choose from each set of associated prime elements of R a representative of that set,

Evidently d_i and e_i can be replaced by any elements such that $d_i' \sim d_i$ and $e_i' \sim e_i$. It will help to make a systematic choice of such d_i and e_i. We can (1) choose from each set of associated prime elements of R a representative of that set, (2) put a total order on this set Σ of representatives, and

Evidently d_i and e_i can be replaced by any elements such that $d_i' \sim d_i$ and $e_i' \sim e_i$. It will help to make a systematic choice of such d_i and e_i. We can (1) choose from each set of associated prime elements of R a representative of that set, (2) put a total order on this set Σ of representatives, and (3) put a total order on the set Σ^* of powers of elements of Σ by requiring that $p^a < q^b$ if and only if $p < q$ or $p = q$ and $a < b$ (note that $p^a = q^b$ implies $p = q$ and $a = b$ by unique factorization). Finally

Evidently d_i and e_i can be replaced by any elements such that $d_i' \sim d_i$ and $e_i' \sim e_i$. It will help to make a systematic choice of such d_i and e_i. We can (1) choose from each set of associated prime elements of R a representative of that set, (2) put a total order on this set Σ of representatives, and (3) put a total order on the set Σ^* of powers of elements of Σ by requiring that $p^a < q^b$ if and only if $p < q$ or $p = q$ and $a < b$ (note that $p^a = q^b$ implies $p = q$ and $a = b$ by unique factorization). Finally (4) we can replace the d_i and e_i by products of elements of Σ^*.

Evidently d_i and e_i can be replaced by any elements such that $d_i' \sim d_i$ and $e_i' \sim e_i$. It will help to make a systematic choice of such d_i and e_i. We can (1) choose from each set of associated prime elements of R a representative of that set, (2) put a total order on this set Σ of representatives, and (3) put a total order on the set Σ^* of powers of elements of Σ by requiring that $p^a < q^b$ if and only if $p < q$ or $p = q$ and $a < b$ (note that $p^a = q^b$ implies $p = q$ and $a = b$ by unique factorization). Finally (4) we can replace the d_i and e_i by products of elements of Σ^*.

Given $d_1|d_2|\cdots d_k$ we can create an increasing list Δ of elements of Σ^* by factoring each of the d_i into elements of Σ^* and then putting the results in order. We can do the same for the $e_1|e_2|\cdots|e_\ell$, obtaining an ordered list E.

Evidently d_i and e_i can be replaced by any elements such that $d_i' \sim d_i$ and $e_i' \sim e_i$. It will help to make a systematic choice of such d_i and e_i. We can (1) choose from each set of associated prime elements of R a representative of that set, (2) put a total order on this set Σ of representatives, and (3) put a total order on the set Σ^* of powers of elements of Σ by requiring that $p^a < q^b$ if and only if $p < q$ or $p = q$ and $a < b$ (note that $p^a = q^b$ implies $p = q$ and $a = b$ by unique factorization). Finally (4) we can replace the d_i and e_i by products of elements of Σ^*.

Given $d_1|d_2|\cdots d_k$ we can create an increasing list Δ of elements of Σ^* by factoring each of the d_i into elements of Σ^* and then putting the results in order. We can do the same for the $e_1|e_2|\cdots|e_\ell$, obtaining an ordered list E. The elements d_i and e_i can be reconstructed from these lists: d_k is the product of all the largest prime powers (for all the distinct primes), then remove these prime powers, and compute d_{k-1} in the same way, and so forth.

Suppose for example that $R = \mathbb{Z}$ and the d_i are $2|12|360|2520$.

Suppose for example that $R = \mathbb{Z}$ and the d_i are $2|12|360|2520$. Since

$$2 = 2, \quad 12 = 2^2 \cdot 3, \quad 360 = 2^3 \cdot 3^2 \cdot 5, \quad 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$$

Suppose for example that $R = \mathbb{Z}$ and the d_i are $2|12|360|2520$. Since

$$2 = 2, \quad 12 = 2^2 \cdot 3, \quad 360 = 2^3 \cdot 3^2 \cdot 5, \quad 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$$

we find

$$\Delta = \{2, 2^2, 2^3, 2^3, 3, 3^2, 3^2, 5, 5, 7\}.$$

Suppose for example that $R = \mathbb{Z}$ and the d_i are $2|12|360|2520$. Since

$$2 = 2, \quad 12 = 2^2 \cdot 3, \quad 360 = 2^3 \cdot 3^2 \cdot 5, \quad 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$$

we find

$$\Delta = \{2, 2^2, 2^3, 2^3, 3, 3^2, 3^2, 5, 5, 7\}.$$

We recover the d_i from Δ by

$$\begin{aligned}
d_4 &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520, & \Delta &\to \{2, 2^2, 2^3, 3, 3^2, 5\} \\
d_3 &= 2^3 \cdot 3^2 \cdot 5 = 360, & \Delta &\to \{2, 2^2, 3\} \\
d_2 &= 2^3 \cdot 3 = 12, & \Delta &\to \{2\} \\
d_1 &= 2, & \Delta &= \emptyset.
\end{aligned}$$

Continuing with the proof, we can write the p-primary component of M as

$$M_p \simeq \bigoplus_i (R/(p^i)^{m_i^p} \simeq \bigoplus_i (R/(p^i)^{n_i^p}$$

where m_i^p (resp. n_i^p) is the number of times p^i occurs on the list Δ (resp. E); conversely Δ and E can be reconstructed from the m_i^p and n_i^p.

Continuing with the proof, we can write the p-primary component of M as

$$M_p \simeq \bigoplus_i (R/(p^i)^{m_i^p} \simeq \bigoplus_i (R/(p^i)^{n_i^p}$$

where m_i^p (resp. n_i^p) is the number of times p^i occurs on the list Δ (resp. E); conversely Δ and E can be reconstructed from the m_i^p and n_i^p. The latter, finally can be determined directly from the R-modules $p^j M_p$ for all j, as in the last lecture. It follows that $k = \ell$ and $m_i = n_i$ for all i, and we are done. ■

Continuing with the proof, we can write the p-primary component of M as

$$M_p \simeq \bigoplus_i (R/(p^i)^{m_i^p} \simeq \bigoplus_i (R/(p^i)^{n_i^p}$$

where m_i^p (resp. n_i^p) is the number of times p^i occurs on the list Δ (resp. E); conversely Δ and E can be reconstructed from the m_i^p and n_i^p. The latter, finally can be determined directly from the R-modules $p^j M_p$ for all j, as in the last lecture. It follows that $k = \ell$ and $m_i = n_i$ for all i, and we are done. ■

The d_i in the last two theorems, which are now known to be isomorphism invariants of M are called the *invariant factors* of M. The prime powers in the factorization of the d_i are called the *elementary divisors* of M.

Abelian Groups

Before going on let's recall what this says for abelian groups:

Abelian Groups

Before going on let's recall what this says for abelian groups:

Theorem

Any finitely generated abelian group G has a unique direct sum decomposition

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$$

such that $d_1|d_2|\cdots|d_n$.

Abelian Groups

Before going on let's recall what this says for abelian groups:

Theorem

Any finitely generated abelian group G has a unique direct sum decomposition

$$G \simeq \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$$

such that $d_1|d_2|\cdots|d_n$. It also has a unique direct sum decomposition

$$G \simeq \mathbb{Z}^r \oplus \bigoplus_p G_p$$

where for each p, G_p is the p-primary component of G, and there is a unique direct sum decomposition

$$G_p = \sum_i (\mathbb{Z}/p^i\mathbb{Z})^{m_i}.$$

The elementary divisors of G are the list of p^i, each repeated m_i times, for each prime p dividing the order of the group. We saw in the last lecture that the m_i can be determined from the subgroups $p^i G$.

The elementary divisors of G are the list of p^i, each repeated m_i times, for each prime p dividing the order of the group. We saw in the last lecture that the m_i can be determined from the subgroups $p^i G$. The formula was

$$m_i = e_{i+i} - 2e_i + e_{i-1}.$$

where

$$e_i = \log_p |p^i G_p|.$$

The elementary divisors of G are the list of p^i, each repeated m_i times, for each prime p dividing the order of the group. We saw in the last lecture that the m_i can be determined from the subgroups $p^i G$. The formula was

$$m_i = e_{i+i} - 2e_i + e_{i-1}.$$

where

$$e_i = \log_p |p^i G_p|.$$

We can also determine these numbers from the number of elements of order dividing p^i for all i. To see how this is so we denote by $G(p^i)$ the subgroup of elements of order divisible by p^i.

The elementary divisors of G are the list of p^i, each repeated m_i times, for each prime p dividing the order of the group. We saw in the last lecture that the m_i can be determined from the subgroups $p^i G$. The formula was

$$m_i = e_{i+i} - 2e_i + e_{i-1}.$$

where

$$e_i = \log_p |p^i G_p|.$$

We can also determine these numbers from the number of elements of order dividing p^i for all i. To see how this is so we denote by $G(p^i)$ the subgroup of elements of order divisible by p^i. By the first isomorphism theorem,

$$G/G(p^i) \simeq p^i G$$

since the homomorphism $p^i G :\to G$ has kernel $G(p^i)$ and image $p^i G$. Therefore

$$|p^i G| = |G|/|p^i G|$$

$$|p^i G| = |G|/|p^i G|$$

and substituting this into the formula for m_i yields

$$m_i = -\log_p |G(p^{i+1})| + 2\log_p |G(p^i)| - \log_p |G(p^{i-1})|.$$

$$|p^i G| = |G|/|p^i G|$$

and substituting this into the formula for m_i yields

$$m_i = -\log_p |G(p^{i+1})| + 2\log_p |G(p^i)| - \log_p |G(p^{i-1})|.$$

Example: Suppose G is an abelian group with 2^6 elements of order dividing 2, 2^9 elements of order dividing 4, 2^{10} elements of order dividing 8 and 2^{11} elements of order dividing 16 or any larger power of 2.

$$|p^i G| = |G|/|p^i G|$$

and substituting this into the formula for m_i yields

$$m_i = -\log_p |G(p^{i+1})| + 2\log_p |G(p^i)| - \log_p |G(p^{i-1})|.$$

Example: Suppose G is an abelian group with 2^6 elements of order dividing 2, 2^9 elements of order dividing 4, 2^{10} elements of order dividing 8 and 2^{11} elements of order dividing 16 or any larger power of 2. Then $\log_2 |G(2)| = 6$, $\log_2 |G(4)| = 9$, $\log_2 |G(8)| = 10$, $\log_2 |G(16)| = 11$, and

$$\begin{aligned} m_1 &= -9 + 2 \cdot 6 = 3 \\ m_2 &= -10 + 2 \cdot 9 - 6 = 2 \\ m_3 &= -11 + 2 \cdot 10 - 9 = 0 \\ m_4 &= -11 + 2 \cdot 11 - 10 = 1 \end{aligned}$$

and finally $m_i = 0$ for $i \geq 5$.

$$|p^i G| = |G|/|p^i G|$$

and substituting this into the formula for m_i yields

$$m_i = -\log_p |G(p^{i+1})| + 2\log_p |G(p^i)| - \log_p |G(p^{i-1})|.$$

Example: Suppose G is an abelian group with 2^6 elements of order dividing 2, 2^9 elements of order dividing 4, 2^{10} elements of order dividing 8 and 2^{11} elements of order dividing 16 or any larger power of 2. Then $\log_2 |G(2)| = 6$, $\log_2 |G(4)| = 9$, $\log_2 |G(8)| = 10$, $\log_2 |G(16)| = 11$, and

$$\begin{aligned} m_1 &= -9 + 2 \cdot 6 = 3 \\ m_2 &= -10 + 2 \cdot 9 - 6 = 2 \\ m_3 &= -11 + 2 \cdot 10 - 9 = 0 \\ m_4 &= -11 + 2 \cdot 11 - 10 = 1 \end{aligned}$$

and finally $m_i = 0$ for $i \geq 5$. We conclude that

$$G \simeq (\mathbb{Z}/2\mathbb{Z})^3 \oplus (\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/16\mathbb{Z}).$$

In this last example it would have been sufficient to know $|G| = 2^{11}$ and the number of elements of order dividing 2, 4, 8 and 16, for as soon as we have found $m_1, \ldots, m_4$ we have found a subgroup of order 2^{11}, which is therefore all of G. Obviously this works quite generally.

In this last example it would have been sufficient to know $|G| = 2^{11}$ and the number of elements of order dividing 2, 4, 8 and 16, for as soon as we have found $m_1, \ldots, m_4$ we have found a subgroup of order 2^{11}, which is therefore all of G. Obviously this works quite generally.

If G is a finite abelian group one can similarly determine the elementary divisors of G from the subgroups $G(p^i)$ for all i and p dividing the order of G, for this tells us the structure of the p-primary components of G, and hence of G itself.

The proof of the first part of the structure theorem yields the following fun fact:

Proposition

Suppose A is an $n \times n$ matrix with integral entries and let $G = \mathbb{Z}^n / A\mathbb{Z}^n$. Then G is finite if and only if $\det(A) \neq 0$, *and if so,* $|G| = \det(A)$.

Proof. The theorem says that there are invertible matrices P, $Q \in M_{nn}(\mathbb{Z})$ such that $PAQ = D$ is a diagonal matrix with diagonal entries d_i satisfying $d_1 | d_2 | \cdots | d_n$. Then $G \simeq \bigoplus_{1 \leq i \leq n} \mathbb{Z}/d_i\mathbb{Z}$ and the rank of G is the number of d_i that are zero. Furthermore $\det(A) = \prod_i d_i$, so $\det(A) = 0$ if and only if the rank is positive. If the rank is zero, $|G| = \prod_i d_i = \det(A)$. ∎

An Example

Let's work out a bloody explicit example of finding the invariant factors of a matrix with integer entries. I will use the *totally random* matrix

$$A = \begin{pmatrix} -25 & -3 & 21 & 21 \\ 15 & 7 & -5 & -5 \\ -72 & -2 & 70 & 70 \\ 35 & -1 & -37 & -37 \end{pmatrix}.$$

The existence part of the proof consisted of multiplying this on the left and right by invertible integral matrices until the desired result was acheived. Here we are dealing with a Euclidean domain, which means two things, (1) that instead of the order relation on R that was used in the proof we can use the Euclidean norm, and (2) we can use ordinary row and column operations. So I start by looking for an element of smallest Euclidean norm. It's in row 4, column 2...

So I switch rows 1&4 and then columns 1&2, and then multiply the first column by -1. Also, columns 3&4 are the same, so I'll then subtract column 3 from column 4:

$$\to \begin{pmatrix} 1 & 35 & -37 & -37 \\ -7 & 15 & -5 & -5 \\ 2 & -72 & 70 & 70 \\ 3 & -25 & 21 & 21 \end{pmatrix} \to \begin{pmatrix} 1 & 35 & -37 & 0 \\ -7 & 15 & -5 & 0 \\ 2 & -72 & 70 & 0 \\ 3 & -25 & 21 & 0 \end{pmatrix}.$$

Next I add 7 times row 1 to row 2, subtract twice it from row 3 and 3 times it from row 4. Then I can clean out the remaining entries in the first row, since there are no nonzero entries in column 1 below the first:

$$\to \begin{pmatrix} 1 & 35 & -37 & 0 \\ 0 & 260 & -264 & 0 \\ 0 & -142 & 144 & 0 \\ 0 & -130 & 132 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 260 & -264 & 0 \\ 0 & -142 & 144 & 0 \\ 0 & -130 & 132 & 0 \end{pmatrix}$$

So now we know $d_1 = 1$ and we can start working on the principal minor. Move the -130 up to the first row, then subtract row 1 from row 2 and add twice row 1 to row 3. Then the remaining row and/or column operations are evident:

$$\begin{pmatrix} -130 & 132 & 0 \\ -142 & 144 & 0 \\ 260 & -264 & 0 \end{pmatrix} \to \begin{pmatrix} -130 & 132 & 0 \\ -12 & 12 & 0 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} -12 & 12 & 0 \\ -130 & 132 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\to \begin{pmatrix} -12 & 12 & 0 \\ -10 & 12 & 0 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} -10 & 12 & 0 \\ -12 & 12 & 0 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} -10 & 12 & 0 \\ -2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\to \begin{pmatrix} 2 & 0 & 0 \\ -10 & 12 & 0 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

We find $d_2 = 2$, $d_3 = 12$ and $d_4 = 0$. Finally

$$\mathbb{Z}^3/A\mathbb{Z}^3 \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}.$$

And if you thought that was fun, just imagine how it's going to work when R is a polynomial ring...

And that's all for today...