18.312: Algebraic Combinatorics — Lionel Levine

Lecture 22

Lecture date: May 3, 2011 — *Notes by: Lou Odette*

This lecture:

- Smith normal form of an integer matrix (linear algebra over $\mathbb{Z}$).

1 Review of Abelian Groups (= $\mathbb{Z}$-modules)

Recall that given a ring R with 1, an R-module is an Abelian group written additively with a map $R \times M \to M$ ("scalar multiplication") with R the scalars and M the vectors, satisfying

$$\begin{aligned} r(m_1 + m_2) &= rm_1 + rm_2 \\ r(sm) &= (rs)m \\ 1m &= m \end{aligned}$$

which is analogous to a vector space over R, with the difference that we may lack multiplicative inverses in R, by contrast with a vector space over a field.

If G is an group, we have a map $\mathbb{Z} \times G \to G$

$$\begin{aligned} &(n, g) \mapsto \underbrace{g + \cdots + g}_{n \text{ times}} && \text{if } n > 0 \\ &(0, g) \mapsto 0 \\ &(n, g) \mapsto -\left(\underbrace{g + \cdots + g}_{n \text{ times}}\right) && \text{if } n < 0 \end{aligned}$$

so we admit scalar multiplication by integers, but not anything else. In particular, any abelian group has the structure of a $\mathbb{Z}$-module.

Now, say G is an Abelian group, finitely generated from generators $g_1, \ldots, g_n$. Then there is a surjective group homomorphism $f : \mathbb{Z}^n \to G$ taking basis elements to the generators

$$\begin{aligned} f(e_i) &= g_i \\ f\left(\sum_{i \in [n]} c_i e_i\right) &= \sum_{i \in [n]} c_i g_i. \end{aligned}$$

Let K be a kernel of f, the subgroup of $\mathbb{Z}^n$ s.t.

$$K = \ker f = \left\{ \sum_{i\in[n]} c_i g_i \middle| \sum_{i\in[n]} c_i g_i = 0 \text{ in } G \right\}$$

Definition 1 *A group G is* torsion-free *if*

$$\forall g \in G,\ g \neq 0,\ \textit{and } \forall n \in \mathbb{Z},\ n \neq 0 \textit{ we have } ng \neq 0$$

Example 2 *$\mathbb{Z}$ and $\mathbb{Z}^n$ are torsion free, but $\mathbb{Z}/n\mathbb{Z}$ is not torsion free, since $ng = 0$ for all $g \in \mathbb{Z}/n\mathbb{Z}$.*

Note that if G is torsion free then it is infinite or zero since with $g \in G$ and $g \neq 0$, then $g, 2g, 3g, \ldots$ are distinct, since otherwise $ig = jg \Rightarrow (i - j)\, g = 0$.

By the **F**undamental **T**heorem of **F**initely **G**enerated **A**belian **G**roups (FTFGAG), any finitely generated abelian group G has the form

$$G \simeq \mathbb{Z}^r \times (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}) \tag{1}$$

where $r \geq 0$ is unique but the $n_1, \cdots, n_k > 1$ are not necessarily unique.

Example 3 *$\mathbb{Z}_6 \times \mathbb{Z}_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_{12}$, since $\mathbb{Z}_m \times \mathbb{Z}_n = \mathbb{Z}_{nm}$, for $m \perp n$ by the Chinese remainder theorem.*

There are two ways to get uniqueness:

1. require that all the n_i are prime powers
2. or require $n_1 | n_2 | n_3 \cdots | n_k$.

We consider the second of these today.

Lemma 4 *Any subgroup $K \subset \mathbb{Z}^n$ satisfies $K \simeq \mathbb{Z}^r$ for some $r \leq n$.*

Note that unlike subspaces of a vector space, is it possible to have $r = n$ and $K \neq \mathbb{Z}^n$. For example, $2\mathbb{Z}^n \subsetneq \mathbb{Z}^n$ while is it still the case that $2\mathbb{Z}^n \simeq \mathbb{Z}^n$. In this sense abelian groups are "more interesting" than vector spaces.

Now, since $K \subset \mathbb{Z}^n \Rightarrow K \simeq \mathbb{Z}^r$ for some $r \leq n$, pick a basis $x_1, \ldots, x_r \in K$ so that

$$K = \left\{ \sum_{i \in [r]} c_i x_i \middle| c_i \in \mathbb{Z} \right\}$$

and define

$$L : \mathbb{Z}^r \to \mathbb{Z}^n;\ e_i \mapsto x_i$$

so that

$$G \simeq \mathbb{Z}^n / K = \mathbb{Z}^n / \mathrm{Image}\,(L) = \mathbb{Z}^n / L\mathbb{Z}^r$$

We can think of L as an $r \times n$ matrix and each $x_i = \sum_{j \in [n]} a_{i,j} e_i$ for $i \in [r]$, where the $a_{i,j}$ are the matrix entries of L. We can extend L to $\mathbb{Z}^n$, i.e. $L : \mathbb{Z}^n \to \mathbb{Z}^n$ by setting $e_i \mapsto 0$ for $i > r$ (add zero "columns").

So far we have seen how defining an abelian group G via generators and relations leads to an $n \times n$ matrix L such that $G \simeq \mathbb{Z}^n / L\mathbb{Z}^n$, where n is the number of generators. The question that Smith normal form address is: given a group in this form, $\mathbb{Z}^n / L\mathbb{Z}^n$, how do we express it in the factored form (1)?

Example 5 *Let*

$$L = \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix} \to G = \langle g_1, g_2 \rangle \Big/ \begin{array}{c} 2g_1 - g_2 = 0 \\ g_1 + 2g_2 = 0 \end{array}$$

and

$$G = \mathbb{Z}^2 / \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix} \mathbb{Z}^2$$

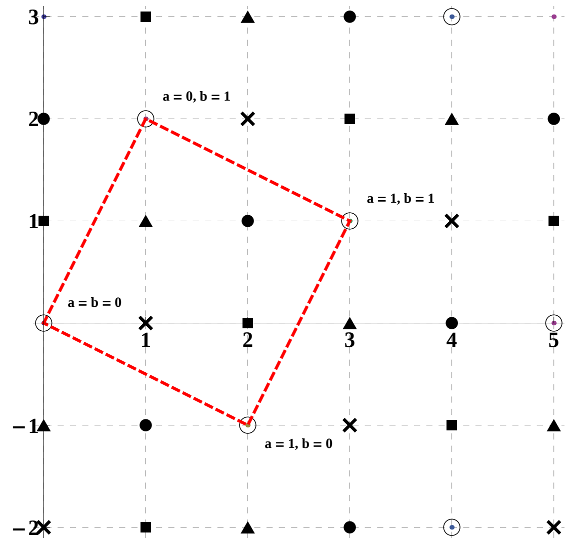

Figure 1: This figure illustrates $G = \mathbb{Z}^2/L\mathbb{Z}^2$, where $L\mathbb{Z}^2$ consists of the points $(2a+b, 2b-a)$ for $a, b \in \mathbb{Z}$, as marked by the symbol $\circ$ on the grid. The remaining symbols represent elements in the respective equivalence classes. The points enclosed by the box represent the members of all equivalence classes, illustrating that $|G| = 5$. So $G \simeq \mathbb{Z}/5\mathbb{Z}$.

Now, consider the kinds of changes to L that don't change the isomorphism type of G. One approach is to change the generators.

Example 6 *Write the group G of example (5) using different generators*

$$G = \langle h_1, h_2 \rangle \,;\; h_1 = g_1,\; h_2 = 3g_1 + g_2$$

In general, if $H \in GL_n(\mathbb{Z})$, where $GL_n(\mathbb{Z})$ is the set of $n \times n$ matrices U with $\det U = \pm 1$, so the inverse also is an integer matrix, then since $U\mathbb{Z}^n = \mathbb{Z}^n$

$$G \simeq \mathbb{Z}^n/L\mathbb{Z}^n = U\mathbb{Z}^n/L\mathbb{Z}^n \simeq \mathbb{Z}^n/U^{-1}L\mathbb{Z}^n$$

In addition, if $V \in GL_n(\mathbb{Z})$, since $V\mathbb{Z}^n = \mathbb{Z}^n$

$$\begin{aligned} \mathbb{Z}^n/U^{-1}L\mathbb{Z}^n &= \mathbb{Z}^n/U^{-1}L\,(V\mathbb{Z}^n) \\ &= \mathbb{Z}^n/\left(U^{-1}LV\right)\mathbb{Z}^n \end{aligned}$$

Example 7 *Write the group G of example (5) with different relations*

$$\begin{matrix} 2g_1 - g_2 = 0 \\ g_1 + 2g_2 = 0 \end{matrix} \;\rightarrow\; \begin{matrix} 2g_1 - g_2 = 0 \\ 3g_1 - g_2 = 0 \end{matrix}$$

Definition 8 *An $n \times n$ integer matrix S is in* Smith Normal Form *(SNF) if S is a diagonal matrix and uniqueness condition (2) is satisfied with the diagonal elements $(S)_{i,i} \equiv d_i$, i.e.*

$$d_1 | d_2 | d_3 \cdots | d_n;\ d_i \geq 0,\ \forall i \in [n]$$

Note that some d_i may be zero, since any integer divides zero.

Theorem 9 *An integer matrix $L = (a_{i,j})_{i,j \in [n]}$ can be written as*

$$L = USV$$

where S is in SNF and $U, V \in GL_n\mathbb{Z}$ (invertible over the integers). Moreover, the non-zero d_i on the diagonal of S are unique (note, $\gcd(\cdot)$ is non-negative by definition):

$$\begin{aligned}
d_1 &= \gcd(a_{i,j}) \\
d_1 d_2 &= \gcd(a_{i,j}a_{k,l} - a_{i,l}a_{j,k}) \qquad (\textit{i.e. the } 2 \times 2 \textit{ determinants}) \\
&\vdots \\
d_1 \cdots d_k &= \gcd(\textit{all } k \times k \textit{ minors of } L) \\
&\vdots \\
d_1 \cdots d_n &= |\det L|
\end{aligned}$$

with $|G| = |\det L|$. In terms of the group G, if L has SNF S then

$$\begin{aligned}
G = \mathbb{Z}^n / L\mathbb{Z}^n &\simeq \mathbb{Z}^n / S\mathbb{Z}^n \\
&\simeq \langle g_1, \cdots, g_n \rangle / (d_i g_i = 0,\ i \in [n]) \\
&\simeq \langle g_1 \rangle / (d_1 g_1) \times \cdots \times \langle g_n \rangle / (d_n g_n) \\
&\simeq \mathbb{Z} / (d_1 \mathbb{Z}) \times \cdots \times \mathbb{Z} / (d_n \mathbb{Z})
\end{aligned}$$

in particular

- *the rank of G is $\# \{ i | d_i = 0 \}$*
- *if G is finite (all $d_i > 0$) then $|G| = d_1 \cdots d_n = |\det L|$*

Note: row and column operations don't change the gcd$(\cdot)$ result since, if $n_1, \ldots, n_k \neq 0$ (noting that if $(m,n) = 1$ then $\exists c, c' \in \mathbb{Z}$ s.t. $cm + c'n = 1$)

$$\gcd(n_1, \ldots, n_k) = \min \left\{ d > 0 \middle| \, d = \sum_{i \in [n]} c_i n_i \textit{ for some } c_1, \cdots, c_k \in \mathbb{Z} \right\}$$

so $L = USV$.

Example 10 *Consider*

$$L = \begin{pmatrix} 1 & 3 & 1 \\ 3 & 1 & 3 \\ 1 & 3 & 5 \end{pmatrix} \to \mathbb{Z}^3 / L\mathbb{Z}^3 \simeq \mathbb{Z}_4 \times \mathbb{Z}_8$$

since

$$\begin{aligned} d_1 &= \gcd(a_{i,j}) = 1 \\ d_1 d_2 &= \gcd(-8, 0, 8, 0, 4, 12, 8, 12, -4) = 4 \\ d_1 d_2 d_3 &= |\det L| = 32 \end{aligned}$$

2 Commutative Monoids

Definition 11 *A monoid M is a set with an associative operation*

$$\mu : M \times M \to M$$

and an identity element $e \in M$

$$(e, m) \mapsto m, \forall m \in M$$

M is commutative if $\mu(m_1, m_2) = \mu(m_2, m_1)$.

We are interested in how to get a group from this object

Example 12 *Consider*

$$\begin{aligned} m &= \langle g \rangle / (10g = 6g)\,;\ (k+4)_g = kg, \forall g \geq 6 \\ &= \{e, g, 2g, \ldots, 9g\} \end{aligned}$$

and so, writing μ as addition

$$8g + 8g = 16g = 12g = 8g$$

Definition 13 *An ideal of a monoid M is a subset satisfying*

$$I \subseteq M \text{ s.t. } I + M \subseteq I$$

i.e. $\forall x \in I, \forall m \in M$ we have $m + x \in I$.

Theorem 14 *Let M be a finite commutative monoid and let J be the minimal ideal of M*

$$J = \bigcap_{ideals\ I} I$$

Then J is an Abelian group.

In example (12)

$$\begin{aligned} I &= \{8g\} + M \\ &= \{8g + m \mid m \in M\} \end{aligned}$$

e.g.

$$\begin{array}{c} 8g + g = 9g \\ 8g + 2g = 6g \\ 8g + 3g = 7g \\ 8g + 4g = 8g \end{array} \rightarrow I = \{6g, 7g, 8g, 9g\}$$

and in the table below, the second last column is the identity, while the last column is cyclic of order 4, with $9g$ the generator

	$6g$	$7g$	$8g$	$9g$
$6g$	$8g$	$9g$	$6g$	$7g$
$7g$	$9g$	$6g$	$7g$	$8g$
$8g$	$6g$	$7g$	$8g$	$9g$
$9g$	$7g$	$8g$	$9g$	$6g$