Math 332 Tuesday March 10

☆ No quiz Thursday

I. Structure theorem for finitely generated abelian groups.

Thm. Let G be a finitely generated abelian group. Then

$$G \simeq \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_k\mathbb{Z}} \times \mathbb{Z}^t$$

for some positive integers $d_1 | d_2 | \cdots | d_k$ and t. The d_i and t are uniquely determined.

(this means $d_i | d_{i+1}$ for each $i = 1, \ldots, k-1$)

Def. With G as above, the elements of G with finite order form a subgroup isomorphic to $\frac{\mathbb{Z}}{t_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{t_w\mathbb{Z}}$. This subgroup is called the torsion part of G. The elements of infinite order along with the identity element forms a subgroup isomorphic to $\mathbb{Z}^t$. This subgroup is called the free part of G, and the number t is the rank of G. The d_i are called the elementary divisors of G.

Loosely sketch of proof: Let $g_1, \dots, g_m$ be generators for G.

Step 1: Define a mapping of groups $\phi : \mathbb{Z}^m \to G$ where e_i is the i^{th} standard basis vector.

$$e_i \longmapsto g_i$$

We get a short exact sequence

$$0 \to \ker\phi \xrightarrow{i} \mathbb{Z}^m \xrightarrow{\phi} G \to 0.$$

We will prove a theorem later that says any subgroup of $\mathbb{Z}^m$ is isomorphic to $\mathbb{Z}^n$ for some n. So $\exists\, \psi : \mathbb{Z}^n \xrightarrow{\sim} \ker\phi$ for some n, and using this isomorphism, we have a short exact sequence

$$0 \to \mathbb{Z}^n \xrightarrow{L} \mathbb{Z}^m \xrightarrow{\phi} G \to 0$$

where $L = i \circ \psi$. We can think of L as the $m \times n$ integer matrix with j^{th} column Le_j, and $G \simeq \mathbb{Z}^m / \mathrm{im}(L)$.

Step 2 Multiplying L on the left by an element of $GL_n(\mathbb{Z})$ is the same as performing invertible integer row operations on L. Multiplying on the right by an element of $GL_m(\mathbb{Z})$ corresponds to invertible integer column operations.

Example

$$\begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = \begin{bmatrix} a & b & c \\ 2a+d & 2b+e & 2c+f \\ g & h & i \end{bmatrix}.$$

Multiplying causes the same thing to happen to $\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$.

Start with identity matrix and add 2× (first row) to the second.

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} 1 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a-3g & b-3h & c-3i \\ d & e & f \\ g & h & i \end{bmatrix}.$$

Start with the identity matrix and add −3× (third row) to the first.

Performing these row and column operations corresponds to a change of "$\mathbb{Z}$-basis".

Step 3

Claim $\exists\ U \in GL_m(\mathbb{Z})$, $V \in GL_n(\mathbb{Z})$ such that $ULV = D$

where $D = \operatorname{diag}(d_1, d_2, \dots, d_k, 0, \dots, 0)$ with $d_1 | d_2 | \cdots | d_k$.

(diag: diagonal matrix; the 0's: n of them)

In terms of mappings we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{L} & \mathbb{Z}^m & \longrightarrow & G & \longrightarrow & 0 \\ & & V^{-1}\downarrow \wr & & \wr\downarrow U & & \wr\downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m & \longrightarrow & \operatorname{cok}(D) & \longrightarrow & 0 \end{array}$$

($\star$ see proposition below)

Def. If $\varphi : A \to B$ is a mapping of abelian groups, then the cokernel of φ is

$$\operatorname{cok}\varphi := B/\operatorname{im}\varphi$$

Prop. $\star$ Given a commutative diagram of abelian groups

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \alpha\downarrow & \circlearrowleft & \downarrow\beta \\ C & \xrightarrow{\psi} & D \end{array}$$

(i) $\exists$ a mapping $\gamma : \operatorname{cok}\varphi \to \operatorname{cok}\psi$ such that the following diagram commutes:

$$\begin{array}{ccc} B & \to & \operatorname{cok}\varphi \\ \beta\downarrow & & \downarrow\gamma \\ C & \to & \operatorname{cok}\psi \end{array}$$

($B \to \operatorname{cok}\varphi$: projection to quotient; $C \to \operatorname{cok}\psi$: projection to quotient)

(ii) If α and β are isomorphisms, so is γ.

Pf/ This will be HW, eventually. $\square$

oops. I need to fix this matrix.

Example

$L:$ $\begin{bmatrix} 7 & 14 & 21 \\ 35 & 73 & 117 \\ 7 & 20 & 66 \end{bmatrix}$ → (clear out first row using first column) $\begin{bmatrix} 7 & 0 & 0 \\ 35 & 73 & 117 \\ 7 & 20 & 66 \end{bmatrix}$ → (now clear out first column using the first row) $\begin{bmatrix} 7 & 0 & 0 \\ 0 & 3 & 12 \\ 0 & 6 & 45 \end{bmatrix}$ → (clear 2nd row) $\begin{bmatrix} 7 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 6 & 21 \end{bmatrix}$ → (clear 2nd column) $\begin{bmatrix} 7 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 21 \end{bmatrix}$

$U:$ $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ → $\begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$ → $\begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 9 & -2 & 1 \end{bmatrix}$

$V:$ $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ → $\begin{bmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ → $\begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix}$

So far: $ULV = \begin{bmatrix} 7 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 21 \end{bmatrix}$. This shows $\operatorname{cok}(L) \cong \dfrac{\mathbb{Z}^3}{\operatorname{span}_{\mathbb{Z}}\left\langle \begin{pmatrix} 7 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 21 \end{pmatrix} \right\rangle}$ ← $\operatorname{im}(L)$

$$\cong \frac{\mathbb{Z}}{7\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}}.$$

To put this in standard form, $d_1 | d_2 | d_3$ requires more row & column operations.

Note that $\frac{\mathbb{Z}}{7\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}} \simeq \frac{\mathbb{Z}}{1\cdot\mathbb{Z}} \times \frac{\mathbb{Z}}{(3\cdot 7)\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}}$ by the Chinese remainder theorem. So we can see the final form: $\operatorname{cok}(h) \simeq \frac{\mathbb{Z}}{1\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}}$

$\simeq \left(\frac{\mathbb{Z}}{21\mathbb{Z}}\right)^2$.

and $d_1 = 1$, $d_2 = 21$, $d_3 = 21$, $t = 0$.

Shuffle To algorithmically rearrange the diagonal...

input: $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$

(i) Let $d = \gcd(a,b)$, and find u, v s.t. $d = ua + bv$.

(ii) $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \longrightarrow \begin{bmatrix} a & 0 \\ vb & b \end{bmatrix} \longrightarrow \begin{bmatrix} a & 0 \\ ua+vb & b \end{bmatrix} = \begin{bmatrix} a & 0 \\ d & b \end{bmatrix} \xrightarrow{d \text{ divides } a} \begin{bmatrix} 0 & -\frac{a}{d}\cdot b \\ d & b \end{bmatrix} \xrightarrow{d \text{ divides } b} \begin{bmatrix} 0 & -\frac{a}{d}\cdot b \\ d & 0 \end{bmatrix} \xrightarrow{\text{continued on next page}}$

row operations: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1-\frac{a}{d}\cdot u & -\frac{a}{d} \\ u & 1 \end{bmatrix}$

column operations: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 \\ v & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & -\frac{b}{d} \\ v & 1-\frac{b}{d}v \end{bmatrix}$

swap rows, then negate 2nd row

$$\begin{bmatrix} 0 & -\frac{a}{d}\cdot b \\ d & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} d & 0 \\ 0 & \frac{a}{d}b \end{bmatrix}$$

Note: d divides $\frac{a}{d}\cdot b$ since $d \mid b$.

$$\begin{bmatrix} 1-\frac{a}{d}\cdot u & -\frac{a}{d} \\ u & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} u & 1 \\ \frac{a}{d}\cdot u - 1 & \frac{a}{d} \end{bmatrix}$$

$$\begin{bmatrix} 1 & -\frac{b}{d} \\ v & 1-\frac{b}{d}v \end{bmatrix}$$

Final result:

$$\begin{bmatrix} u & 1 \\ \frac{a}{d}u-1 & \frac{a}{d} \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} 1 & -\frac{b}{d} \\ v & 1-\frac{b}{d}v \end{bmatrix} = \begin{bmatrix} d & 0 \\ 0 & \frac{a}{d}b \end{bmatrix}$$

Continuing our earlier example:

$$\begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 9 & -2 & 1 \end{bmatrix}\begin{bmatrix} 7 & 14 & 21 \\ 35 & 73 & 117 \\ 7 & 20 & 66 \end{bmatrix}\begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 7 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 21 \end{bmatrix}$$

U' L V' D' — Rearrange

$1\cdot 7 + (-2)\cdot 3 = 1$

$u\ a\ v\ b\ d$

$$\begin{bmatrix} u & 1 \\ \frac{a}{d}u-1 & \frac{a}{d} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 6 & 7 \end{bmatrix}, \quad \begin{bmatrix} 1 & -\frac{b}{d} \\ v & 1-\frac{b}{d}v \end{bmatrix} = \begin{bmatrix} 1 & -3 \\ -2 & 7 \end{bmatrix}.$$

Thus,

$$\begin{bmatrix} 1 & 1 & 0 \\ 6 & 7 & 0 \\ 0 & 0 & 1 \end{bmatrix}\underbrace{\begin{bmatrix} 7 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 21 \end{bmatrix}}_{U'LV'}\begin{bmatrix} 1 & -3 & 0 \\ -2 & 7 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 21 & 0 \\ 0 & 0 & 21 \end{bmatrix}.$$

$$U = \begin{bmatrix} 1 & 1 & 0 \\ 6 & 7 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ -5 & 1 & 0 \\ 9 & -2 & 1 \end{bmatrix} = \underline{\begin{bmatrix} -4 & 1 & 0 \\ -29 & 7 & 0 \\ 9 & -2 & 1 \end{bmatrix}}, \quad V = \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & -3 & 0 \\ -2 & 7 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \underline{\begin{bmatrix} 5 & -17 & 5 \\ -2 & 7 & -4 \\ 0 & 0 & 1 \end{bmatrix}}$$

$$\begin{bmatrix} -4 & 1 & 0 \\ -29 & 7 & 0 \\ 9 & -2 & 1 \end{bmatrix} \begin{bmatrix} 7 & 14 & 21 \\ 35 & 73 & 117 \\ 7 & 20 & 66 \end{bmatrix} \begin{bmatrix} 5 & -17 & 5 \\ -2 & 7 & -4 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 21 & 0 \\ 0 & 0 & 21 \end{bmatrix}$$

$U \qquad L \qquad V \qquad D$

elementary divisors:
$1, 21, 21$

rank: 0

$$0 \longrightarrow \mathbb{Z}^3 \xrightarrow{L} \mathbb{Z}^3 \longrightarrow G \longrightarrow 0$$

$$L = \begin{bmatrix} 7 & 14 & 21 \\ 35 & 73 & 117 \\ 7 & 20 & 66 \end{bmatrix}$$

$G \cong \mathbb{Z}^3 / \mathrm{im}(L)$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}^3 & \xrightarrow{L} & \mathbb{Z}^3 & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr & & \\ 0 & \longrightarrow & \mathbb{Z}^3 & \xrightarrow{D} & \mathbb{Z}^3 & \longrightarrow & \frac{\mathbb{Z}}{1\cdot\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

$$\begin{bmatrix} 7 & 17 & 33 \\ 2 & 5 & 10 \\ 0 & 0 & 1 \end{bmatrix} = V^{-1} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 21 & 0 \\ 0 & 0 & 21 \end{bmatrix} = D \qquad \begin{bmatrix} -4 & 1 & 0 \\ -29 & 7 & 0 \\ 9 & -2 & 1 \end{bmatrix} = U$$

$$\frac{\mathbb{Z}}{1\cdot\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}} \cong \frac{\mathbb{Z}}{21\mathbb{Z}} \times \frac{\mathbb{Z}}{21\mathbb{Z}}$$

$$(a,b,c) \mapsto (b,c)$$

Remarks

* $ULV = \begin{bmatrix} d_1 & & & \\ & \ddots & & \\ & & d_h & \\ & & & 0 \end{bmatrix}$ (with t zero columns)

The rank of G (the cokernel of L) is the dimension of the kernel of L as a matrix over $\mathbb{Q}$ (or $\mathbb{R}$).

* If L is a square matrix (i.e. L has full rank) and the rank of G is 0, so $G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_h\mathbb{Z}}$, then $|G| = d_1 \cdots d_h = \det(ULV) = \underbrace{\det(U)}_{\pm 1} \det(L) \underbrace{\det(V)}_{\pm 1}$.

So $|G| = \pm \det L$.

* Over $\mathbb{Q}$ or $\mathbb{R}$ the cokernel is less interesting:

$$0 \to \mathbb{R} \xrightarrow{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 21 & 0 \\ 0 & 0 & 21 \end{bmatrix}} \mathbb{R} \to 0$$

over $\mathbb{Q}$ or $\mathbb{R}$, $\operatorname{coker}(L) = 0$, not $\frac{\mathbb{Z}}{21} \times \frac{\mathbb{Z}}{21}$.

Outline of General Smith Normal Form Algorithm

Step 1: Diagonalize

$\begin{bmatrix} & \\ & \end{bmatrix}$ → swap rows and columns to get non-zero 1,1 entry, a_1 → $\left[\begin{array}{c|c} a_1 & \\ \hline & \end{array}\right]$ → column operations to get $a_2 = \gcd(\text{first row})$ → $\left[\begin{array}{c|c} a_2 & \\ \hline & \end{array}\right]$ → use 1st column to zero out first row → $\left[\begin{array}{c|c} a_2 & 0\,0\cdots0 \\ \hline & \end{array}\right]$

→ row operations to get $a_3 = \gcd(\text{first column})$ and then zero out first column. This probably messes up the first row. → $\left[\begin{array}{c|c} a_3 & *\,*\cdots* \\ \hline 0 & \\ 0 & \\ \vdots & \\ 0 & \end{array}\right]$ → column operations $a_4 = \gcd(\text{first row})$ then zero out → $\left[\begin{array}{c|c} a_4 & 0\,0\cdots0 \\ \hline * & \\ * & \\ \vdots & \\ * & \end{array}\right]$ → row operations again → $\left[\begin{array}{c|c} a_5 & *\,*\cdots* \\ \hline 0 & \\ 0 & \\ \vdots & \\ 0 & \end{array}\right]$ → Etc. back-and-forth → ⋯ → $\left[\begin{array}{c|c} a_t & 0\,0\cdots0 \\ \hline 0 & \\ 0 & \\ \vdots & \\ 0 & \end{array}\right]$

Eventually stabilizes since $a_2 | a_1$, $a_3 | a_2$, $a_4 | a_3$, etc.

Recurse on ☆ to get $\begin{bmatrix} a & & & 0 \\ & b & & \\ & & c & \\ 0 & & & \ddots \end{bmatrix}$, a diagonal matrix.

For most applications, you can stop here, having identified G as $\frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}} \times \cdots$.

The Chinese remainder theorem lets you rearrange things to get $\prod_{i=1}^{k} \frac{\mathbb{Z}}{d_i\mathbb{Z}} \times \mathbb{Z}^t$ with $d_1 | \cdots | d_k$. But if you compelled to find the change of basis, read on.

Step 2: Elementary divisors.

Recall the trick described above. If $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ is given with $\gcd(a,b) = d$, write $d = au + bv$. Then

$$\begin{bmatrix} u & 1 \\ \frac{a}{d}u - 1 & \frac{a}{d} \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} 1 & -\frac{b}{d} \\ v & 1 - \frac{b}{d}v \end{bmatrix} = \begin{bmatrix} d & 0 \\ 0 & \frac{a}{d}b \end{bmatrix}$$

where $d \mid (\frac{a}{d}b)$. Thus,

$$\left[\begin{array}{cc|c} u & 1 & \\ \frac{a}{d}u - 1 & \frac{a}{d} & 0 \\ \hline & & \begin{matrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots \end{matrix} \end{array}\right] \left[\begin{array}{cc|c} a & & 0 \\ & b & \\ \hline 0 & & \begin{matrix} c & \\ & \ddots \end{matrix} \end{array}\right] \left[\begin{array}{cc|c} 1 & -\frac{b}{d} & \\ v & 1 - \frac{b}{d}v & 0 \\ \hline & & \begin{matrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots \end{matrix} \end{array}\right]$$

$$= \left[\begin{array}{cc|c} d & 0 & \\ 0 & \frac{a}{d}b & \\ \hline & & \begin{matrix} c & \\ & \ddots \end{matrix} \end{array}\right].$$

Repeating with pairs of diagonal elements eventually leads to $\begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_k \end{bmatrix}$ with $d_1 \mid d_2 \mid \cdots \mid d_k$.