MATH 436: Homework VII.
Due in class on Monday, Nov 10

1. **[Applications of the Classification of Finitely Generated Abelian Groups.]** (a) Make a list of all the possible Abelian groups of order 72 (up to isomorphism).
(b) Fix an integer $n \geq 1$ and let $\mathbb{Z}^n$ denote the Free Abelian group of rank n, i.e., a direct sum of n copies of $\mathbb{Z}$. Show that if $f : \mathbb{Z}^n \to \mathbb{Z}^n$ is a surjective endomorphism then f is an automorphism of $\mathbb{Z}^n$.

2. **[Partitions of n].** Let n be a positive integer. A partition of n is a sequence of integers $1 \leq \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_k$ such that $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n$. We let $\lambda(n)$ denote the total number of partitions of n. For example the partitions of 4 are: $1+1+1+1, 1+1+2, 1+3, 2+2, 4$ so $\lambda(4) = 5$.
(a) List the partitions of 6 and find $\lambda(6)$.
(b) Let $\sigma \in \Sigma_n$ be a permutation, then we have seen that we may write σ as a product of disjoint cycles (here we will also use the cycles of length 1 contrary to the usual convention), $\sigma = \sigma_1 \dots \sigma_k$. Then if λ_j denotes the length of the cycle σ_j we can rearrange the cycles so that $1 \leq \lambda_1 \leq \lambda_2 \cdots \leq \lambda_k$ and so the sequence $\{\lambda_j | 1 \leq j \leq k\}$ is a partition of n. We denote it by $\lambda(\sigma)$, and call it the partition associated to the permutation σ.

Show that two permutations σ and σ' are conjugate in Σ_n if and only if their associated partitions are equal, i.e., $\lambda(\sigma) = \lambda(\sigma')$.
(c) [This part is disjoint from the previous parts of the problem] Let p be a prime. Show that the number of distinct Abelian groups of order p^n (up to isomorphism) is $\lambda(n)$.

3. **[Divisible Groups].** (a) Recall that $(\mathbb{Q}/\mathbb{Z}, +)$ is a torsion Abelian group. Let p be a prime, the Prufer group of type p^∞ consists of the subgroup of $\mathbb{Q}/\mathbb{Z}$ consisting of elements of order a power of p. This group is denoted $P(p^\infty)$. Show that $P(p^\infty) = \{\frac{m}{p^i} + \mathbb{Z}\} | m, i \in \mathbb{Z}, i \geq 0\}$ and that a nonzero element in this group can be written **uniquely** in the form $\frac{m}{p^i} + \mathbb{Z}$ where $gcd(m, p) = 1$ and $i \geq 1, 0 \leq m < p^i$.
(b) Show that for a fixed $i \geq 0$, $P(p^i) = \{\frac{m}{p^i} + \mathbb{Z} | m \in \mathbb{Z}\}$ is a subgroup of $P(p^\infty)$ and this subgroup is a cyclic group of order p^i. Check that $P(p^\infty) = \cup_{i=1}^{\infty} P(p^i)$ and show that any subgroup H of $P(p^\infty)$ is equal to one of the $P(p^i)$ for some $i = 0, 1, 2, \dots, \infty$.
(c) An abelian group A is called divisible if for every $x \in A$ and positive integer n, there exists $y \in A$ such that $ny = x$. Check that $(\mathbb{Q}, +)$ is a divisible

Abelian group. Show that $P(p^\infty)$ is a divisible Abelian group. [Hint: For this last group, you might want to consider the cases when n is a power of p and when n is relatively prime to p first.]
(d) Show that there are two distinct elements y_1 and y_2 in $P(p^\infty)$ such that $py_1 = \frac{1}{p} + \mathbb{Z} = py_2$. Thus the y in the definition of a divisible group need not be uniquely determined by x and n in general.
(e) Show that if $A = \oplus_{x \in X} \mathbb{Z}$ with $|X| \geq 1$ then A is not a divisible group. Thus conclude that $\mathbb{Q}$ and $P(p^\infty)$ are not free Abelian groups. Hence conclude that $P(p^\infty)$ is an Abelian group such that all proper subgroups are finite cyclic p-groups but such that $P(p^\infty)$ itself is not cyclic. [This is why the Prufer p^∞ groups are sometimes called quasicyclic.]

4. [$GL_n(\mathbb{Z})$.] Let $Mat_n(\mathbb{Z})$ denote the monoid of $n \times n$ matrices with **integer** entries under the usual matrix multiplication $\mathbb{C} = \mathbb{A}\mathbb{B}$ given by $\mathbb{C}_{ij} = \sum_{k=1}^{n} \mathbb{A}_{ik}\mathbb{B}_{kj}$. In this exercise we will view the elements of $\mathbb{Z}^n$ as column vectors $\hat{u}$ with n integer entries. Thus we may define for every $\mathbb{A} \in Mat_n(\mathbb{Z})$, the function $f_{\mathbb{A}} : \mathbb{Z}^n \to \mathbb{Z}^n$ given by $f_{\mathbb{A}}(\hat{u}) = \mathbb{A}\hat{u}$.
(a) Check that $f_{\mathbb{A}} : \mathbb{Z}^n \to \mathbb{Z}^n$ is an endomorphism of $\mathbb{Z}^n$ and show that the correspondence $\Theta : Mat_n(\mathbb{Z}) \to End(\mathbb{Z}^n)$ given by $\Theta(\mathbb{A}) = f_{\mathbb{A}}$ is an isomorphism of monoids.
(b) By (a), it follows that the group of units of $End(\mathbb{Z}^n)$ i.e., $Aut(\mathbb{Z}^n)$ is isomorphic to

$$GL_n(\mathbb{Z}) = \{\mathbb{A} \in Mat_n(\mathbb{Z}) | \exists \mathbb{B} \in Mat_n(\mathbb{Z}) \text{ such that } \mathbb{A}\mathbb{B} = \mathbb{I} = \mathbb{B}\mathbb{A}\}.$$

It is easy to check from basic linear algebra that $det : Mat_n(\mathbb{Z}) \to \mathbb{Z}$, i.e., the determinant of a matrix with integer entries is an integer. Also recall for any real matrix, if $det(\mathbb{A}) \neq 0$ then $\mathbb{A}^{-1}$ exists in $Mat_n(\mathbb{R})$ and is given by $\mathbb{A}^{-1} = \frac{1}{det(\mathbb{A})} adj(\mathbb{A})$ where $adj(\mathbb{A}) = \mathbb{C}^T$. Here $\mathbb{C}$ is the cofactor matrix whose entries are given by $\mathbb{C}_{ij} = (-1)^{i+j} det(\mathbb{A}(i,j))$ where $\mathbb{A}(i,j)$ is the matrix obtained from $\mathbb{A}$ by deleting the ith row and jth column.

Use this to show that if $\mathbb{A} \in Mat_n(\mathbb{Z})$ has $det(\mathbb{A}) \neq 0$ then $\mathbb{A}^{-1}$ exists in $Mat_n(\mathbb{R})$ and is a matrix with rational entries. Furthermore when we express these entries in the form $\frac{m}{s}$ with $gcd(m,s) = 1$, we have s divides $det(\mathbb{A})$. Use this to give an example of a matrix $\mathbb{A} \in Mat_2(\mathbb{Z})$ where $det(\mathbb{A}) \neq 0$ but $\mathbb{A} \notin GL_2(\mathbb{Z})$.
(c) Show that if $\mathbb{A} \in Mat_n(\mathbb{Z})$ then $\mathbb{A} \in GL_n(\mathbb{Z})$ if and only if $det(\mathbb{A}) = \pm 1$.
(d) Given $\mathbb{A} \in Mat_n(\mathbb{Z})$ let $\hat{a}_1, \ldots, \hat{a}_n$ denote the columns of $\mathbb{A}$ regarded as

elements of $\mathbb{Z}^n$. We define the Column subgroup of $\mathbb{A}$ to be the subgroup of $\mathbb{Z}^n$ generated by the columns of $\mathbb{A}$ and denote it by $Col(\mathbb{A})$. Thus

$$Col(\mathbb{A}) =< \hat{a}_1, \ldots, \hat{a}_n > .$$

Show that $Col(\mathbb{A}) = Im(f_{\mathbb{A}})$, i.e., that $Col(\mathbb{A})$ is the image of the endomorphism $f_{\mathbb{A}}$ defined in part (a).
(e) Use part (d) to show that if $\mathbb{S} \in GL_n(\mathbb{Z})$ then $Col(\mathbb{A}) = Col(\mathbb{AS})$. Furthermore show that the automorphism $f_{\mathbb{S}}$ of $\mathbb{Z}^n$ has $f_{\mathbb{S}}(Col(\mathbb{A})) = Col(\mathbb{SA})$.
(f) We define a relation $\sim$ on $Mat_n(\mathbb{Z})$ as follows: We say $\mathbb{A} \sim \mathbb{A}'$ if $\mathbb{A}' = \mathbb{TAS}$ for some $\mathbb{T}, \mathbb{S} \in GL_n(\mathbb{Z})$. Show that $\sim$ is an equivalence relation on $Mat_n(\mathbb{Z})$. We say that $\mathbb{A}$ and $\mathbb{A}'$ are equivalent matrices if $\mathbb{A} \sim \mathbb{A}'$. Show that if $\mathbb{A} \sim \mathbb{A}'$ then $\mathbb{Z}^n/Col(\mathbb{A}) \cong \mathbb{Z}^n/Col(\mathbb{A}')$.
(g) Let $\mathbb{A} \in Mat_n(\mathbb{Z})$ have ith row denoted by $\hat{a}_i$. An elementary row operation on $\mathbb{A}$ is one of the following:
(1) For fixed $i \neq j$ and some $n \in \mathbb{Z}$, we replace $\hat{a}_i$ with $\hat{a}_i + n\hat{a}_j$, i.e., we add n times the jth row to the ith row.
(2) We permute two rows.
(3) We multiply a row by -1.
Check that if $\mathbb{A}'$ is obtained from $\mathbb{A}$ by one of the row operations above, then $\mathbb{A}' = \mathbb{TA}$ for some $\mathbb{T} \in GL_n(\mathbb{Z})$. Describe $\mathbb{T}$ for each of the row operations. We define elementary column operations analogously. Show that if $\mathbb{A}'$ is obtained from $\mathbb{A}$ by one of the column operations then $\mathbb{A}' = \mathbb{AS}$ for some $\mathbb{S} \in GL_n(\mathbb{Z})$. Describe $\mathbb{S}$ for each of the column operations. Conclude that if $\mathbb{A}'$ is obtained from $\mathbb{A}$ by a finite sequence of row and column operations then $\mathbb{A}' \sim \mathbb{A}$.
(h) Let $\mathbb{D}(s_1, \ldots, s_n)$ denote the diagonal matrix with entries $s_1, \ldots, s_n$ on the main diagonal (s_1 on top left, s_n on bottom right) and zero entries off the main diagonal. We will now prove

Theorem 0.1. *Let $\mathbb{A} \in Mat_n(\mathbb{Z})$ then there exists $0 \leq r \leq n$ and $1 \leq d_1|d_2|\ldots|d_r$ such that $\mathbb{A} \sim \mathbb{D}(d_1, \ldots, d_r, 0, \ldots, 0)$.*

Please fill in the requested details in the following proof: We prove the theorem by induction on n. The case $n = 1$ is trivial so assume $n > 1$ and all smaller cases have been proven. If $\mathbb{A} = \mathbb{O}$ the result is trivial so assume $\mathbb{A} \neq \mathbb{O}$.

Define d_1 to be the smallest positive entry of **any** matrix equivalent to

$\mathbb{A}$. Thus there exists $\mathbb{B} \sim \mathbb{A}$ such that $\mathbb{B} = \begin{bmatrix} d_1 & * & \dots & * \\ a_2 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots \\ a_n & * & \dots & * \end{bmatrix}$. (Explain why we can assume d_1 in upper left corner.)

Now write $a_j = k_j d_1 + r_j$ with $k_j, 0 \leq r_j < d_1$ integers for each $2 \leq j \leq n$. Show that $\mathbb{B} \sim \begin{bmatrix} d_1 & * & \dots & * \\ r_2 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots \\ r_n & * & \dots & * \end{bmatrix}$. and use this to conclude that $r_2 = \dots = r_n = 0$. Use a similar argument for the entries in the first row to the right of d_1 to conclude that

$$\mathbb{A} \sim \begin{bmatrix} d_1 & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & * & \dots & * \end{bmatrix}.$$

Use induction to explain why there exists $0 \leq r \leq n$ and $1 \leq d_2 | d_3 | \dots | d_r$ such that $\mathbb{A} \sim \mathbb{D}(d_1, d_2, \dots, d_r, 0, \dots, 0)$. Finally to show $d_1 | d_2$ write $d_2 = sd_1 + r$ for $s, 0 \leq r < d_1$ integers. Show that

$$\begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} \sim \begin{bmatrix} d_1 & -d_1 \\ sd_1 & r \end{bmatrix}$$

and use this to conclude $r = 0$, i.e., that $d_1 | d_2$. This completes the proof of the theorem.

(i) Show that if $\mathbb{A} \sim \mathbb{D}(d_1, \dots, d_r, 0, \dots, 0)$ then

$$\mathbb{Z}^n / Col(\mathbb{A}) \cong \mathbb{Z}^{n-r} \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_r\mathbb{Z}$$

and use this to conclude that the numbers $r, d_1, \dots, d_r$ in the previous theorem are uniquely determined from $\mathbb{A}$. (r is called the rank and $d_1, \dots, d_r$ are called the invariant factors of $\mathbb{A}$. Thus you have shown that two integer matrices $\mathbb{A}$ and $\mathbb{B}$ are equivalent if and only if they have the same rank and the same invariant factors.)

(j) If $H = \{s \begin{bmatrix} 2 \\ 5 \end{bmatrix} + t \begin{bmatrix} 5 \\ 7 \end{bmatrix} | s, t \in \mathbb{Z}\}$ find the invariant factor decomposition of $\mathbb{Z}^2/H$.