Math 372 lecture for Monday, Week 11

Finitely generated abelian groups

An *abelian group* is a pair $(A, +)$ consisting of a set A and an operation $+\colon A \times A \to A$ called *addition* such that $+$ is associative and commutative, there exists $0 \in A$ such that $a + 0 = 0 + a = a$ for all $a \in A$, and each $a \in A$ has an additive inverse $-a$ such that $a + (-a) = 0$. (*Subtraction* is defined using additive inverses: $a - b := a + (-b)$.) It is *finitely generated* if there exists and $a_1, \dots, a_m \in A$ for some m such that for each $a \in A$, there exists $n_1, \dots, n_m \in \mathbb{Z}$ such that

$$a = n_1 a_1 + \cdots + n_m a_m.$$

Examples.

- A *cyclic group* is by definition generated by a single element, and every cyclic group is abelian. Every cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some nonnegative integer n. The case $n = 0$ yields the infinite cyclic group $\mathbb{Z} = \mathbb{Z}/0\mathbb{Z}$.
- Every finite abelian group is generated by the finite set consisting of all of its elements. For instance, $\mathbb{Z}/4\mathbb{Z} = \langle 0, 1, 2, 3 \rangle$. Of course, we also have $\mathbb{Z}/4\mathbb{Z} = \langle 1 \rangle = \langle 3 \rangle$. We do not require the set of generators to be minimal (with respect to inclusion).
- A finite product of cyclic groups is a finitely generated abelian group. A typical instance is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}^2$. Recall that addition is defined component-wise, e.g., $(2, 5, 8, -2) + (3, 3, 7, 2) = (1, 2, 15, 0)$ in this group.

The last example is about as complicated as a f.g. abelian group can get: it turns out that every f.g. abelian group is a product of a finite number of cyclic groups, i.e., has the form $\prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$ for suitable n_i (and where n_i might be 0). The *structure* of the group is then given by the list of the n_i. Different choices for the n_i may produce isomorphic groups, but it turns out that the ambiguity is accounted for by the following well-known result:

Theorem. (Chinese remainder theorem.) Let $m, n \in \mathbb{Z}$. Then

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

if and only if m and n are relatively prime. If $\gcd(m, n) = 1$, then an isomorphism is provided by $a \mapsto (a \bmod m, a \bmod n)$.

Thus, $\mathbb{Z}/24\mathbb{Z} \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, but $\mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Theorem. (Structure theorem for f.g. abelian groups) A group is a finitely generated abelian group if and only if it is isomorphic to

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^r$$

for some list (possibly empty) of integers $n_1, \ldots, n_k$ with $n_i > 1$ for all i and some integer $r \geq 0$. These integers may be required to satisfy either of the following two conditions, and in either case they are uniquely determined by the isomorphism class of the group.

Condition 1: $n_i | n_{i+1}$ (n_i evenly divides n_{i+1}) for all i. In this case, the n_i are the *invariant factors* of the group.

Condition 2: There exist primes $p_1 \leq \cdots \leq p_k$ and positive integers m_i such that $n_i = p_i^{m_i}$ for all i. In this case, the n_i are the *elementary divisors* and the $\mathbb{Z}/n_i\mathbb{Z}$ are the *primary factors* of the group.

The number r is the *rank* of the group.

How does one go about computing the rank and invariant factors of a finitely generated abelian group A? Let $\{a_1, \ldots, a_m\}$ be generators, and define the group homomorphism determined by

$$\begin{aligned} \mathbb{Z}^m &\xrightarrow{\pi} A \\ e_i &\mapsto a_i \end{aligned}$$

where e_i is the i-th standard basis vector. Saying that the a_i generate A is the same as saying that π is surjective. Next, by a standard theorem from algebra[1] every subgroup of $\mathbb{Z}^m$ is finitely generated. In particular, there exists a finite set of generators $\{b_1, \ldots, b_n\}$ for the kernel of π. Define

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m$$

where M is the $m \times n$ integer matrix with i-th column b_i. Combining these two mappings yields a *presentation* of A:

$$\mathbb{Z}^n \xrightarrow{M} \mathbb{Z}^m \twoheadrightarrow A$$

Hence, π induces an isomorphism

$$\begin{aligned} \operatorname{cok}(M) := \mathbb{Z}^m/\operatorname{im}(M) &\simeq A \\ e_i &\mapsto a_i, \end{aligned}$$

[1]The key point is that abelian groups are modules over $\mathbb{Z}$, and $\mathbb{Z}$ is a Noetherian ring.

where $\operatorname{cok}(M)$ denotes the cokernel of $M\colon \mathbb{Z}^n \to \mathbb{Z}^m$. In this way, A is determined by the single matrix M.

We have just seen that each finitely generated abelian group is the cokernel of an integer matrix. Conversely, each integer matrix determines a finitely generated abelian group. However, the correspondence is not bijective. The construction of M, above, depended on arbitrary choices for generators of A and of the kernel of π. Making different choices creates a different matrix representing A. This is especially obvious if we choose a different number of generators for A or $\ker \pi$. However, there can be a difference even if the number of generators is kept constant. In that case, changing the choice of generators corresponds to integer changes of coordinates for the codomain and domain of M, or equivalently, to performing integer row and column operations on M.

Write $M \sim N$ for integer matrices M and N if one may be obtained from the other through a sequence of integer row and column operations. Since the operations are reversible, $\sim$ is an equivalence relation.

Suppose M is an $m \times n$ integer matrix and $M \sim N$. Start with identity matrices $P = I_m$ and $Q = I_n$, and consider the sequence of integer row and column operations transforming M into N. Whenever a row operation is performed in this sequence, apply the same row operation to P. Similarly, whenever a column operation is made, apply the same column operation to Q.

Exercise. Explain why the resulting matrices P and Q are invertible over the integers and why $PMQ = N$. The converse of this statement is also true: given any matrices P and Q, invertible over the integers and such that $PMQ = N$, it follows that $M \sim N$. However, the proof of this converse requires the existence of the Smith normal form.

The relation $PMQ = N$ can be expressed in terms of a commutative diagram with exact rows:

$$\begin{tikzcd}
\mathbb{Z}^n \arrow[r, "M"] \arrow[d, "Q^{-1}"', "\wr"] & \mathbb{Z}^m \arrow[r] \arrow[d, "P", "\wr"'] & \operatorname{cok} M \arrow[r] \arrow[d, dashed] & 0 \\
\mathbb{Z}^n \arrow[r, "N"] & \mathbb{Z}^m \arrow[r] & \operatorname{cok} N \arrow[r] & 0.
\end{tikzcd} \tag{1}$$

The mapping $\operatorname{cok}(M) \to \operatorname{cok}(N)$ is induced by P.

Proposition. Let M and N be $m \times n$ integer matrices. Then if $M \sim N$, it follows that $\operatorname{cok}(M) \simeq \operatorname{cok}(N)$.

Proof. Since P and Q in the commutative diagram are isomorphisms the mapping of cokernels induced by P is an isomorphism. $\square$

Exercise. Suppose $M \sim N$ where $N = \operatorname{diag}(m_1, \ldots, m_\ell)$, a diagonal integer matrix with nonnegative entries. Show that

$$\operatorname{cok}(M) \simeq \prod_{i=1}^{\ell} \mathbb{Z}/m_i\mathbb{Z}.$$

The previous exercise shows that to determine the structure of $\operatorname{cok}(M)$, we should seek to transform M through integer row and column operations into a diagonal matrix of a particularly nice form.

Definition. An $m \times n$ integer matrix M is in *Smith normal form* if

$$M = \operatorname{diag}(s_1, \ldots, s_k, 0, \ldots, 0),$$

a diagonal matrix, where $s_1, \ldots, s_k$ are positive integers such that $s_i | s_{i+1}$ for all i. The s_i are called the *invariant factors* of M.

Example. The matrix

$$M := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

is in Smith normal form with invariant factors $s_1 = 1$, $s_2 = 2$, and $s_3 = 12$.

We have

$$\operatorname{cok}(M) := \mathbb{Z}^5/\operatorname{im}(M) \simeq \mathbb{Z}/1\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}^2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}^2.$$

So $\operatorname{cok}(M)$ has rank $r = 2$ and its invariant factors are 2 and 12.

Note that 1 is an invariant factor of M but not of $\operatorname{cok}(M)$. By definition, the invariant factors of a finitely generated abelian group are greater than 1; the invariant factors of M equal to 1 do not affect the isomorphism class of $\operatorname{cok}(M)$ since $\mathbb{Z}_1$ is the trivial group.

Aside on $\mathbb{Z}$-modules. A $\mathbb{Z}$-module is a triple $(M, +, \cdot)$ where $+\colon M \times M \to M$ and $\cdot\colon \mathbb{Z} \times M \to \mathbb{Z}$ satisfy the usual rules for a vector space. The difference is that the scalars are the ring $\mathbb{Z}$ rather than a field. It is immediate to see that a $\mathbb{Z}$-module is the same thing as an abelian group since if A is an abelian group and $n \in \mathbb{Z}$, then na is well-defined as repeated addition of a with itself.

Let M be a $\mathbb{Z}$-module. Then M is *free* if it has a basis—a spanning set that is linearly independent. Not every $\mathbb{Z}$-module has a basis. For example, $M = \mathbb{Z}/5\mathbb{Z}$ has no basis. For instance, although $\mathbb{Z}/5\mathbb{Z}$ is generated by 1, we have $5 \cdot 1 = 0$ as a non-trivial linear relation. To say that M is *finitely generated* means that M has a finite spanning set. We have that M is finitely generated and free if and only if there is a $\mathbb{Z}$-linear isomorphism

$$M \simeq \mathbb{Z}^n$$

for some n. By the structure theorem for finite abelian groups, a submodule of a f. g. free $\mathbb{Z}$-module is free. A quotient of f.g. free $\mathbb{Z}$-modules is not necessarily free. For instance, let N be the $\mathbb{Z}$-span of the vectors $(2,0)$ and $(0,3)$ in $\mathbb{Z}^2$. Then N is free with basis $(2,0)$ and $(0,3)$, and we have the isomorphism

$$\begin{gathered} N \simeq \mathbb{Z}^2 \\ (2a, 3b) \mapsto (a, b). \end{gathered}$$

However, we also have $N \subset \mathbb{Z}^2$, and $\mathbb{Z}^2/N \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.