M7210 Lecture 24 Monday October 17, 2012

Abelian Groups IV

We left off last time having finished preparations for the proof of:

Theorem. *If S is subgroup of $\mathbb{Z}^n$, then we can choose a new basis $\{b_1, \ldots, b_n\}$ of $\mathbb{Z}^n$ and a new generating set $\{t_1, \ldots, t_\ell\}$ ($\ell \le n$) for S such that for each $i = 1, \ldots, \ell$, t_i is an integer multiple of b_i, i.e., $t_i = d_i b_i$ for some $d_i \in \mathbb{Z}$.*

Proof. Let $S \subseteq \mathbb{Z}^n$. We know from last Friday that S is finitely generated, so we have a $\mathbb{Z}$-module morphism $\alpha : \mathbb{Z}^m \to \mathbb{Z}^n$ with image S. (We know that we may find a generating set for S with no more than n elements, but we do not *need* to use a generating set for S that satisfies this.) Let E be the standard basis for $\mathbb{Z}^m$ and let F be the standard basis for $\mathbb{Z}^n$. Let $A := \big(\,\alpha\,;\ E\,F\,\big)$. Then A is an $m \times n$ matrix with the generators of S as rows. (That is, the rows of A are the generators of S expressed as row vectors with respect to F.) By the diagonalization procedure described in the last lecture, we may find an invertible[1] $m \times m$ integer matrix P and an invertible[1] $n \times n$ integer matrix Q such that PAQ is diagonal. We may interpret P and Q as change-of-base matrices:

$$P = \big(\,\mathrm{id}_{\mathbb{Z}^m}\,;\ T\,E\,\big),$$
$$Q = \big(\,\mathrm{id}_{\mathbb{Z}^n}\,;\ F\,B\,\big),$$

where, $B = \{b_1, \ldots, b_n\}$ is the basis of $\mathbb{Z}^n$ whose elements are the rows of Q (i.e., the elements of $\mathbb{Z}^n$ that are expressed by the rows of Q with respect to the standard basis) and T is the basis of $\mathbb{Z}^m$ whose elements are the rows of P^{-1}. We have:

$$PAQ = \big(\,\mathrm{id}_{\mathbb{Z}^m}\,;\ T\,E\,\big)\big(\,\alpha\,;\ E\,F\,\big)\big(\,\mathrm{id}_{\mathbb{Z}^n}\,;\ F\,B\,\big) = \big(\,\alpha\,;\ T\,B\,\big).$$

The diagonal entries of PAQ that are non-zero will serve as the d_i referred to in the theorem. The corresponding elements of T serve as the $\{t_1, \ldots, t_\ell\}$. /////

Application to finitely-generated $\mathbb{Z}$-modules

Suppose A is a finitely-generated $\mathbb{Z}$-module. Let $\beta : \mathbb{Z}^n \twoheadrightarrow A$ be a surjection, and let $S \subseteq \mathbb{Z}^n$ be the kernel of this map. Select a data for $\mathbb{Z}^n$ and S as in the theorem. We will show that A is isomorphic to $\oplus_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z} \oplus \mathbb{Z}^{n-\ell}$. Consider the morphism $\mathbb{Z}^n \to \Big(\oplus_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}\Big) \oplus \mathbb{Z}^{n-\ell}$ that sends b_i to $1 + d_i\mathbb{Z}$ for $i = 1, \ldots, \ell$ and sends b_i to 1 for $i = \ell+1, \ldots, n$. (What universal properties are we using to guarantee we have a morphism with these properties?) The kernel of this morphism is the subgroup of $\mathbb{Z}^n$ generated by $d_i b_i$, $i = 1, \ldots, \ell$, i.e., it is S. Thus,

$$A \quad\cong\quad \mathbb{Z}^n/S \quad\cong\quad \left(\bigoplus_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}\right) \oplus \mathbb{Z}^{n-\ell}. \tag{1}$$

We have proved:

Proposition 1. *Every finitely generated abelian group is isomorphic to a finite sum of cyclic groups.*

[1] By "invertible", we mean invertible over $\mathbb{Z}$—i.e., the inverse has entries in $\mathbb{Z}$.

It is possible to diagonalize an integer matrix in many ways, so we may wind up representing our group in different ways. Nonetheless, we can say much about the features of a decomposition of a given finitely generated abelian group into cyclic summands that must be preserved in any sum decomposition.

Uniqueness of the rank of the torsion-free part

Our first goal is to show is that the number of summands isomorphic to $\mathbb{Z}$ is independent of the sum decomposition. It is helpful to give a definition.

Definition. Let A be an abelian group. The *torsion subgroup* of A is

$$\{\, a \in A \mid \exists n \in \mathbb{Z} \text{ such that } n \neq 0 \text{ and } na = 0 \,\}.$$

If the torsion subgroup of A is $\{0\}$, we say that A is *torsion-free*. If the torsion subgroup of A is all of A, we say that A is *torsion*.

Lemma. *If A is finitely generated and torsion-free, then $A \cong \mathbb{Z}^r$ for a unique integer $r \geq 0$.*

Proof. We know that $A \cong \mathbb{Z}^r$ for *some* r by Proposition 1. But we have already proved that $\mathbb{Z}^r \cong \mathbb{Z}^s \implies r = s$ (see the discussion of rank in Lecture 22). /////

Lemma. *Suppose A is finitely generated with torsion subgroup T. Then A/T torsion-free.*

Proof. **Exercise.**

Remark. Under the hypotheses of the lemma, A/T is finitely generated so it's isomorphic to $\mathbb{Z}^r$ for a unique integer $r \geq 0$.

Referring to (1), we see that the torsion subgroup of the sum is the part inside the parentheses. Thus, $n - \ell$ must be the same for any sum decomposition. This establishes our first goal.

> *Some parenthetical remarks.* We can prove directly (i.e., without using equation (1)) that any finitely generated abelian group is a direct sum of its torsion subgroup and a free abelian group
>
> **Proposition.** *Suppose A is finitely generated. Let T be the torsion subgroup of A. Then*
>
> $$A \cong T \oplus A/T.$$
>
> *Proof.* Select $\{f_1, \ldots, f_r\} \subseteq A$ so that $\{f_1 + T, \ldots, f_r + T\}$ is a basis for A/T. Let F the subgroup of A generated by these elements. Then $F \cong A/T$. Moreover, $T \cap F = \{0\}$ and $T + F = A$, so $A \cong T \oplus F$. /////
>
> **Exercise.** This exercise asks you to prove a general version of the idea used in the proof of the proposition. (Look up "split exact sequence" to see how the fact you will verify is often referred to.) Suppose A is any $\mathbb{Z}$-module, K is a sub-$\mathbb{Z}$-module and $\pi : A \to A/K$ is the canonical quotient morphism. Suppose there is a $\mathbb{Z}$-module morphism $\sigma : A/K \to A$ such that $\pi\sigma = \mathrm{id}_{A/K}$. Show that $A \cong K \oplus A/K$.

Analysis of the torsion part

Our next goal is to examine the torsion part of the sum decomposition. First, we show that any cyclic group can decomposed as a sum of cyclic groups of prime power order. This follows from

Proposition. *Suppose p and q are integers greater than 1 and $(p, q) = 1$ (i.e., p and q are relatively prime). Then $\mathbb{Z}/(pq)\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/q\mathbb{Z}$.*

Proof. Let a be a generator of $\mathbb{Z}/(pq)\mathbb{Z}$, i.e. $\mathbb{Z}a = \mathbb{Z}/(pq)\mathbb{Z}$. Then $\mathbb{Z}(qa)$ is cyclic of order p and $\mathbb{Z}(pa)$ is cyclic of order q. Since $(p, q) = 1$, there are integers u, v such that $up + vq = 1$. Thus $\mathbb{Z}(qa) + \mathbb{Z}(pa) = \mathbb{Z}a$. On the other hand, if $na \in \mathbb{Z}(qa) \cap \mathbb{Z}(pa)$, then n is divisible by both p and q, so $na = 0$. Thus $\mathbb{Z}(qa) \cap \mathbb{Z}(pa) = \{0\}$. The proposition follows by Lecture 19, Proposition 1./////