**M7210 Lecture 22** Friday October 12, 2012

## Abelian Groups II

### Sums of $R$-modules

If $M_\lambda$, $\lambda \in \Lambda$ is any set of $R$-modules, then $\bigoplus_{\lambda\in\Lambda} M_\lambda$ denotes the subset of the cartesian product $\prod_{\lambda\in\Lambda} M_\lambda$ consisting of those elements that are non-zero for at most finitely many indices of $\Lambda$. (If $\Lambda$ is finite, then $\bigoplus_{\lambda\in\Lambda} M_\lambda = \prod_{\lambda\in\Lambda} M_\lambda$.) Let $\iota_\lambda : M_\lambda \to \bigoplus_{\lambda\in\Lambda} M_\lambda$ take $m \in M_\lambda$ to the $\Lambda$-indexed vector that is 0 at all places except the $\lambda$-th, where the entry is $m$.

**Proposition.** *$\bigoplus_{\lambda\in\Lambda} M_\lambda$ together with the embeddings $\iota_\lambda$ is the categorical sum of the $M_\lambda$.*

*Proof*. We need to prove that this object and these morphisms satisfy the universal mapping property that defines the categorical sum (see Lecture 20). Suppose $T$ is an $R$-module and $\phi_\lambda : M_\lambda \to T$ is and $R$-module morphism for each $\lambda \in \Lambda$. Define $\phi : \bigoplus_{\lambda\in\Lambda} M_\lambda \to T$ by

$$\phi\big((m_\lambda)_{\lambda\in\Lambda}\big) = \sum_{\lambda\in\Lambda} \phi_\lambda(m_\lambda).$$

Because only finitely many of the $m_\lambda$ are non-zero, the sum is meaningful. It is left to the reader to check that $\phi$ preserves sums and $R$-action, and that it indeed satisfies the conditions required by the definition of sums. /////

### Free $\mathbb{Z}$-modules

The abelian group $\mathbb{Z}$ has the following universal mapping property: If $A$ is any abelian group and $a \in A$, then there is a unique group morphism $\phi : \mathbb{Z} \to A$ such that $\phi(1) = a$. The morphism is defined thus: $\phi(n) := na$. It follows from the UMP of $\mathbb{Z}$ and the UMP of the sum that if $a_\lambda$, $\lambda \in \Lambda$ is any set of elements in $A$, then there is a unique group homomorphism $\phi : \bigoplus_{\lambda\in\Lambda} \mathbb{Z} \to A$ such that $\phi(e_\lambda) = a_\lambda$, where $e_\lambda := \iota_\lambda(1)$. This property of $\bigoplus_{\lambda\in\Lambda} \mathbb{Z}$ and its elements $e_\lambda$ is so significant that it has a special name.

**Definition.** We say $F$ is *a free abelian group—or free $\mathbb{Z}$-module—on the set* $\{ f_\lambda \mid \lambda \in \Lambda\} \subset F$ if, for any abelian group $A$ and any set map $\alpha : \{ f_\lambda \mid \lambda \in \Lambda\} \to A$, there is a unique group morphism $\overline{\alpha} : F \to A$ such that $\overline{\alpha}(f_\lambda) = \alpha(f_\lambda)$.

Obviously, $\bigoplus_{\lambda\in\Lambda} \mathbb{Z}$ is free on $\{ e_\lambda \mid \lambda \in \Lambda \}$. It is also a routine consequence of the UMP that a $\mathbb{Z}$-module $F$ is free on $\{ f_\lambda \mid \lambda \in \Lambda \}$ if and only if there is an isomorphism from $\bigoplus_{\lambda\in\Lambda} \mathbb{Z}$ to $F$ that takes $e_\lambda$ to $f_\lambda$. Can we recognize when such an isomorphism exists from "internal data"? Yes! The next definition and proposition show how:

**Definition.** Let $F$ be a $\mathbb{Z}$-module. We call a subset $B = \{ f_\lambda \mid \lambda \in \Lambda\} \subset F$ a *basis of* $F$ if a) the only finite $\mathbb{Z}$-linear combination of elements of $B$ that equals 0 is the one with all coefficients 0 (i.e., $B$ is independent) and b) $B$ generates $F$.

Conditions a) and b) are closely related to the *existence* and *uniqueness* conditions in the definition of freeness. Independence assures that there are no relations between elements of $B$ that could conflict with an attempt to extend a set morphism from $B$ to a $\mathbb{Z}$-module $A$ to a group morphism from $F$ to $A$. If $B$ generates $F$, then a set morphism defined on $B$ can have no more than one extension to a group morphism defined on $F$.

**Proposition.** *A $\mathbb{Z}$-module $F$ is free on a subset $B = \{ f_\lambda \mid \lambda \in \Lambda\} \subset F$ if and only if $B$ is a basis of $F$.*

*Proof*. Suppose $F$ has basis $B = \{ f_\lambda \mid \lambda \in \Lambda\} \subset F$. Using the UMP of $\bigoplus_{\lambda\in\Lambda} \mathbb{Z}$, there is a $\mathbb{Z}$-module morphism from this object to $F$ that takes $e_\lambda$ to $f_\lambda$. Since $B$ generates, this morphism is surjective. Suppose $\sum_\lambda n_\lambda e_\lambda = 0$. Then $\sum_\lambda n_\lambda f_\lambda = 0$, so each $n_\lambda = 0$ by definition of basis. Our morphism is both injective and surjective, so it is an isomorphism. /////

### Free $R$-modules

The entire discussion of free $\mathbb{Z}$-modules generalizes to $R$-modules. I leave it to you to check the details. This is a matter of checking that all definitions, theorems and proofs are compatible with the $R$-action.

**Finite generation**

Before turning to the structure theorem, we derive some information about finitely-generated abelian groups.

**Proposition.** (4.52, page 157). *A subgroup of an abelian group that is generated by $n$ elements is generated by $n$ or fewer elements.*

The proof makes use of a

**Lemma.** (4.51, page 157). *Suppose $\phi : G \to B$ is surjective with kernel $K$. If $K$ has a generating set of cardinality $m$ and $B$ has a generating set of cardinality $n$, then $G$ has a generating set of cardinality $m+n$.*

*Proof*. Let $x_1, \ldots, x_m$ be generators of $K \subseteq G$. Let $y_1, \ldots, y_n$ be generators for $B$ and let $x_1', \ldots, x_n'$ be elements of $G$ such that $\phi(x_i') = y_i$. If $x \in G$, then $\phi(x) = \sum_{i=1}^n a_i y_i$ for some $a_i \in \mathbb{Z}$, so $x - \sum_{i=1}^n a_i x_i' \in K$, so there are $b_j \in \mathbb{Z}$ such that $x - \sum_{i=1}^n a_i x_i' = \sum_{j=1}^m b_i x_j$, i.e., $x = \sum_{j=1}^m b_i x_j - \sum_{i=1}^n a_i x_i'$. Thus, $\{x_1, \ldots, x_m, x_1', \ldots, x_n'\}$ generate $G$. /////

*Proof of 4.52.* We prove the theorem by induction on $n$. The theorem is clearly true when $n = 1$.* Suppose the theorem is known for all natural numbers up to $n$. Let $G$ be an abelian group with $n+1$ generators, and let $H$ be a subgroup of $G$. Let $K$ be the subgroup of $G$ generated by the first $n$ generators, and let $\phi : G \to G/K$. Then $H \cap K$ has a generating set with $n$ elements, and $\phi(H) = (H+K)/K \subseteq G/K$ is cyclic. By the lemma, $H$ has a generating set with $n+1$ elements. /////

**Rank**

The *rank* of a free abelian group is the cardinality of a basis. It is not obvious that every basis has the same cardinality but this follows from

**Lemma.** *Any linearly independent subset of the free abelian group $\mathbb{Z}^n$ has cardinality $\leq n$.*

*Proof*. Note that $\mathbb{Z}^n \subseteq \mathbb{Q}^n$. If $\{z_1, \ldots, z_k\} \subset \mathbb{Z}^n$ is not independent considered as a set of elements in $\mathbb{Q}^n$, then there are integers $p_i, q_i$ with not all the $p_i = 0$ such that $\sum_{i=1}^k \frac{p_i}{q_i} z_i = 0$. By multiplying by the least common multiple of the $q_i$, we get a non-trivial $\mathbb{Z}$-linear combination of the $z_i$. /////

**Proposition.** *Any two bases of a finitely-generated free abelian group have the same number of elements.*

*Proof*. Suppose basis $B$ of $G$ has cardinality $n$ and basis $B'$ has cardinality $n'$. Using $B$, we have an isomorphism of $G$ with $\mathbb{Z}^n$, and since $B'$ is independent, $n' \leq n$. Reversing the roles of $B$ and $B'$, we have $n \leq n'$.

**Subgroups of free abelian groups:** a preview of what's up next.

Suppose $S$ is subgroup of $A \cong \mathbb{Z}^n$. Then $S$ has a generating set $\{s_1, \ldots, s_k\}$ with $k \leq n$. By itself, this is not very informative. We are going to prove an amazing result that vastly strengthens this.

**Theorem.** *If $S$ is subgroup of $A \cong \mathbb{Z}^n$, then we can choose a new basis $\{b_, \ldots, b_n\}$ of $A$ and a new generating set $\{t_1, \ldots, t_\ell\}$ for $S$ such that $t_i = m_i b_i$ for $i = 1, \ldots, \ell$, where $m_i \in \mathbb{Z}$.*

This has remarkable consequences. First, it means that every subgroup of a free abelian group is free, for the $t_i$ form a basis for $S$. Second, the structure theorem for finitely generated abelian groups falls out. Here's how. If $G$ is any finitely-generated abelian group, then there is a surjection $\mathbb{Z}^n \twoheadrightarrow G$. Let $S$ be the kernel of this map, and choose $\{b_1, \ldots, b_n\}$ and $\{t_1, \ldots, t_\ell\}$ as in the theorem. Then $G \cong \mathbb{Z}^n/S \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \oplus \cdots \mathbb{Z}/m_\ell\mathbb{Z} \oplus \mathbb{Z}^{n-\ell}$.

But wait! There's more! The proof of the theorem is constructive. The proof actually constructs the basis and the $m_i$.

---

* One proof is, "A subgroup of a cyclic group is cyclic." Another goes as follows. Any non-zero subgroup of $\mathbb{Z}$ is generated by its least positive element. If $G = \langle g \rangle$, then there is a surjection $\phi : \mathbb{Z} \to G$ with $\phi(1) = g$. If $H$ is a subgroup of $G$, then $\phi^{-1}(H)$ is a subgroup of $\mathbb{Z}$, and hence has a single generator. Therefore, $\phi\big(\phi^{-1}(H)\big) = H$ has a single generator.