Abelian Groups (with modules on the side)

Our goal for the next few lectures is to prove the structure theorem for finitely-generated abelian groups. This topic provides us with an opportunity to apply concepts that we have already viewed (in the context of vector spaces, as well as some categorical ideas) and to anticipate concepts that we will be studying in more depth in the future— modules. Where there is no additional effort needed, I will introduce the terminology for modules and prove basic results.

On Wednesday, we finished the material from Lecture 20 and then started discussing modules.

Prelude on modules

Until further notice, "ring" means ring with multiplicative identity. R, whenever it is used, refers to a ring with multiplicative identity.

Definition. Let R be a ring. A *left R-module* is an abelian group A equipped with a scalar multiplication $R \times A \to A; (r, a) \mapsto ra$ such that $1_R\, a = a$, $(r + s)a = ra + sa$, $r(sa) = (rs)a$ and $r(a + a') = ra + ra'$ for all $r, s \in R$ and a, a' in A. An R-module homomorphism $\phi : A \to B$ is a group homomorphism that respects the action of R: $\phi(ra) = r\phi(a)$.

Example. A vector space over a field $\mathbb{F}$ is an $\mathbb{F}$-module.

Example. Any abelian group is a $\mathbb{Z}$-module, where the action of $\mathbb{Z}$ is defined by $na := a + \cdots + a$ (n-fold sum). Any homomorphism of abelian groups is automatically a $\mathbb{Z}$-module homomorphism.

The category of $\mathbb{Z}$-modules is formally distinct from the category of abelian groups, but the difference is in terminology only. Every abelian group is a $\mathbb{Z}$ module in a unique way, and every homomorphism of abelian groups is a $\mathbb{Z}$-module homomorphism in a unique way.

Example. Just as any field $\mathbb{F}$ is vector space over $\mathbb{F}$, any ring R is an R-module. A word of caution: the ring-morphisms from R to R are not generally the same as the R-module morphisms from R to R. The former must satisfy $f(rs) = f(r)f(s)$. The latter must satisfy $\phi(rs) = r\phi(s)$. (Complex conjugation is a ring-morphism from $\mathbb{C}$ to $\mathbb{C}$, but it is not a $\mathbb{C}$-vector-space morphism from $\mathbb{C}$ to $\mathbb{C}$.)

The parallels between $\mathbb{F}$-vector-spaces and R-modules are limited. Consider quotients. The $\mathbb{Z}$-module $\mathbb{Z}$ has many $\mathbb{Z}$-module quotients (any cyclic group) that are not isomorphic to $\mathbb{Z}$. When $\mathbb{F}$ is a field, the $\mathbb{F}$-module $\mathbb{F}$ has no quotients as an $\mathbb{F}$-module other than $\mathbb{F}$ and $\{0\}$. Every $\mathbb{F}$-vector space is a sum of copies of $\mathbb{F}$—i.e., has a basis—but this is not true for $\mathbb{Z}$-modules (nor for modules over any ring that has a non-trivial ideal).

(Friday October 12, 2012)

Sums of R-modules. If M_λ, $\lambda \in \Lambda$ 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 Λ. (If Λ 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 Λ-indexed vector that is 0 at all places except the λ-th, where the entry is m.

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

Proof. Suppose T is an R-module and $\phi_\lambda : M_\lambda \to T$ is and R-module morphism for each $\lambda \in \Lambda$. Define $\phi : \bigoplus_{\lambda\in\Lambda} M_\lambda$ by

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

Because only finitely many of the m_λ are non-zero, the sum is meaningful. It is left to the reader to check that ϕ preserves sums and R-action. /////

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_λ, $\lambda \in \Lambda$ 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_λ is so significant that it has a special name.

Definition. We say F is the *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_λ to f_λ. Can we recognize when such an isomorphism exists from "internal data"?

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) B generates F and b) the only finite $\mathbb{Z}$-linear combination of elements of B that equals 0 is the one with all coefficients 0.

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_λ to f_λ. 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.