Summaries, April 12 and 14

The proposition at the end of the last class asserts that a submodule of a free module V of rank m is free, and its rank is at most m. For the proof, we supposed that U is a finitely generated module, which is true, but hasn't been proved. We discuss this point now.

finitely generated modules

Recall that a module V is finitely generated if there exists a finite set $B = (v_1, ..., v_m)$ of generators, a set of elements of V such that every element of V is a combination $a_1v_1 + \cdots + a_mv_m$ in *at least* one way.

Lemma 1. Let $V \xrightarrow{\varphi} W$ be a surjective homomorphism of R-modules, and let U be the kernel of φ.
(i) If U and W are finitely generated, then V is finitely generated.
(ii) If V is finitely generated, then W is finitely generated.

It isn't always true that, when V is finitely generated, the kernel U is finitely generated.

proof (ii) This is very easy. If a set $(v_1, ..., v_m)$ generates V, the set of its images will generate W.

(i) We suppose that U an W are finitely generated. Let $(u_1, ..., u_k)$ be a finite set of gererators for the kernel U, and let $(w_1, ..., w_n)$ be a finite set of generators for the image W. Also, for each $i = 1, ..., n$, let v_i be an element of V such that $\varphi(v_i) = w_i$. We show that the set $(u_1, ..., u_k; v_1, ..., v_n)$ generates V.

Let v be an element of V, and let $w = \varphi(v)$. Then w is a combination of the elements w_j, say $w = a_1w_! + \cdots + a_nw_n$. We form the corresponding combination of the elements v_i: Let $x = a_1v_1 + \cdots + a_nv_n$. Then $\varphi(x) = w = \varphi(v)$ So $\varphi(v - x) = 0$, and $v - x$ is in the kernel U. So it is a combination $v - x = b_1u_1 + \cdots + b_ku_k$, and then $v = (a_1v_1 + \cdots + a_nv_n) + (b_1u_1 + \cdots + b_ku_k)$. □

Noetherian rings

If every ideal of a ring R is finitely generated, R is called a *noetherian ring*. The term is named after the great mathematician Emmy Noether, who used the concept to develop ring theory. Of course she didn't use that term. The first important application of this concept is the next theorem.

Theorem 1. If R is a noetherian ring and U is a submodule of a finitely generated module V, then U is finitely generated.

proof Since the submodules of R are the ideals, the theorem is true when $V = R$.

The first step is to prove the theorem in the case that V is the module R^n of column vectors. To do this we use induction on n, and we consider the surjective homomorphism $R^n \xrightarrow{\pi} R^{n-1}$ that sends a column vector $(x_1, ..., x_n)^t$ to $(x_1, ..., x_{n-1})^t$. Its kernel, the submodule of vectors $(0, ..., 0, x_n)^t$ is isomorphic to R. Therefore the theorem is true for the kernel. Induction allows us to assume that it is true for the image R^{n-1}. Then part (**i**) of Lemma 1 shows that it is true for R^n.

Now if V is any finitely generated module, and if $B = (v_1, ..., v_m)$ is a set of generators, then the map $R^m \xrightarrow{B} V$ that sends X to BX is a surjective homomorphism. The inverse image W of a submodule U of V will be a submodule of R^m, and it will be finitely generated by the first case. Then restricting the map B to W gives us a surjection $W \to U$, and Lemma 1 **(ii)** shows that U is finitely generated. □

presenting a module

Let R be a noetherian ring, let V be a finite R-module, and say that V is generated by a set $C = (v_1, ..., v_m)$ of its elements. Then we have a surjective map

$$R \xrightarrow{C} V$$

that sends a column vector $Y = (y_1, ..., y_m)^t$ to the combination $CY = v_1y_1 + \cdots + c_my_m$. Let U be the kernel of this map. By the First Isomorphism Theorem, V is isomorphic to the quotient module R^m/U, and by the proposition above, U is finitely generated.

Let $B = (u_1, ..., u_n)$ be a set of elements that generates U. Then we obtain a surjective map $R^n \xrightarrow{B} U$ that sends a vector X to the combination $BX = u_1x_1 + \cdots + u_nx_n$.

Now, $U \subset R^m$, so the elements of U are m-dimensional column vectors. Say that $u_j = (a_{1j}, a_{2j} ..., a_{nj})^t$. We form the $m \times n$ R-matrix

$$A \quad = \quad \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdots & & & \\ \cdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Then the composition $R^n \xrightarrow{B} U \subset R^n$ is simply multiplication by A, i.e., $U = AR^n$. So

$$V \approx R^m/U = R^m/AR^n$$

The matrix A is a *presentation matrix* for the module V. In terms of that matrix, V is generated by a set $(v_1, ..., v_m)$ of elements, with the relations that

$$(v_1, ..., v_m)A = 0 \quad \text{or} \quad v_1a_{1j} + \cdots + v_ma_{mj} = 0 \text{ for } j = 1, ..., n$$

changing generators and relations

The set that generates a module V isn't unique. Even the number of its elements isn't determined. For example, if V is generated by one element v, it can also be generated by the set $(2v, 3v)$. But let's consider changes of generators given by invertible matrices. Let C and B be generating sets for V and U as above, and let Q and P be invertible $m \times m$ and $n \times n$ R-matrices. So Q^{-1} and P^{-1} have coefficients in R too. Then the sets $C' = (v'_1, ..., v'_m) = CQ$ and $B' = (u'_1, ..., u'_n) = BP$ also generate V and U, respectively. We form a diagram of maps of free modules

$$\begin{array}{ccc} R^n & \xrightarrow{A} & R^m \\ {\scriptstyle P}\uparrow & & \uparrow{\scriptstyle Q} \\ R^n & \xrightarrow{A'} & R^m \end{array}$$

where A is the above matrix and $A' = Q^{-1}AP$. Since P and Q are invertible R-matrices, the vertical maps they define are isomorphisms. If $U = AR^n$ is the image of A and $U' = A'R^n$ is the image of A', the isomorphism P defines an isomorphism $U' \to U$:

$$\begin{array}{ccc} U & \xrightarrow{\subset} & R^m \\ \uparrow & & \uparrow{\scriptstyle Q} \\ U1 & \xrightarrow{\subset} & R^m \end{array}$$

in whis diagram the vertical arrows are isomorphisms. Therefore Q defines an isomorphism

$$R^m/U' = V' \to V = R^m/U$$

Example. Let R be the ring of integers $\mathbb{Z}$, and let V be the abelian group (the R-module) generated by elements (v_1, v_2) with relations $2v_1 + 3v_2 = 0$ and $4v_1 + 2v_2 = 0$. So V is presented by the matrix

$$A = \begin{pmatrix} 2 & 4 \\ 3 & 2 \end{pmatrix}$$

We diagonalize A using integer row and column operations:

$$\begin{pmatrix} 2 & 4 \\ 3 & 2 \end{pmatrix} \to \begin{pmatrix} -1 & 2 \\ 3 & 2 \end{pmatrix} \to \begin{pmatrix} -1 & 2 \\ 0 & 8 \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}$$

So V is isomorphic to a module V' generated by elements (v'_1, v'_2) with relations $1v'_1 + 0v'_1 = 0$ and $0v_1$‘ + $8v'_2 = 0$. The generator v'_1 that is equal to zero is useless. So V' is generated by a single elements $v' = v'_2$ with the relation $8v' = 0$. It is a cyclic group of order 8, and so is V.

We can do the analogous thing for any finitely generated $\mathbb{Z}$-module V. We diagonalize a presentation matrix A, obtaining an isomorphic $\mathbb{Z}$-module that is presented by a diagonal matrix. So when $R = \mathbb{Z}$, we may assume that the presentation matrix A is diagonal. Say that its nonzero diagonal entries are $d_1, ..., d_k$. We may also assume that $d_1|d_2|\cdots|d_k$, though that will be less important here.

Then V is generated by elements $(v_1, ..., v_m)$, and the relations given by the columns of the matrix A are

$$d_1v_1 = 0, ; d_2v_2 = 0, \ \cdots, \ d_kv_k = 0$$

the rest of the relations, if there are any, being the trivial relation. Then to represent an element v of V as a unique combination of the generators, we write $v = a_1v_1 + \cdots + a_mv_m$, and we require that $0 \leq a_1 < d_1$, $0 \leq a_2 < d_2$, ...,$0 \leq a_k < d_k$, while the coefficients $a_{k+1}, ..., a_n$ can be arbitrary. There are no relations in the list that involve more than one generator. Looking at this description, one sees that V is isomorphic to an abelian group

$$\mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

with $m - k$ copies of $\mathbb{Z}$. This is a direct sum of cyclic groups, the terms $\mathbb{Z}$ being infinite cyclic. We have proved this theorem:

Theorem. Every finitely generated abelian group is isomorphic to a direct sum of cyclic groups.