M7210 Lecture 33 Wednesday, November 7, 2012

Cyclic Modules

Let A be a commutative ring with identity and let M be an A-module. Let $m \in M$. The submodule of M generated by m is $Am = \{ am \mid a \in A \}$. (Check this!) We say that M is *cyclic* if $M = Am$ for some $m \in M$. A itself is a cyclic A-module, with 1_A its generator. The map $a \mapsto am : A \to Am$ is an A-module surjection, and its kernel $\operatorname{ann}(m) = \{ a \in A \mid am = 0 \}$ is a submodule (hence an ideal) of A. Thus, as an abelian group Am is isomorphic to $A/\operatorname{ann}(m)$. The module structure is given by the map: $(a', am) \mapsto (a'a)m : A \times Am \to Am$.

Where are we going with this? Suppose A is a PID. We say that Am is *primary* if $\operatorname{ann}(m) = (p^n)$ for some prime element $p \in A$ and some positive integer n. We have seen that primary cyclic $\mathbb{Z}$-modules are the basic building blocks of finitely-generated $\mathbb{Z}$-modules in the sense that every finitely-generated $\mathbb{Z}$-module is a finite direct sum of primary cyclic $\mathbb{Z}$-modules and copies of $\mathbb{Z}$ and is determined up to isomorphism by what summands occur. We also have a very good understanding of $\mathbb{Z}/p^n\mathbb{Z}$, so this gives us a very complete picture of the finitely-generated $\mathbb{Z}$-modules. Our goal in the next few lectures is to generalize this perspective. What we have said about $\mathbb{Z}$ modules is also true, with changes in some details, for modules over an PID.

After $\mathbb{Z}$, the next most important PID is $\mathbb{C}[x]$, or more generally the rings of the form $\mathbb{F}[x]$, where $\mathbb{F}$ is a field. We will show that, just as with $\mathbb{Z}$-modules, every finitely-generated $\mathbb{F}[x]$-module is a finite direct sum of primary cyclic $\mathbb{F}[x]$-modules and copies of $\mathbb{F}[x]$, and is determined up to isomorphism by what summands occur. To make full use of this, we need an understanding of the structure of primary cyclic $\mathbb{F}[x]$-modules. This is what we begin to do in this lecture.

$\mathbb{F}$-modules and $\mathbb{F}[x]$-modules.

Let $\mathbb{F}$ be a field and let M be an $\mathbb{F}$-module (i.e., a vector space over $\mathbb{F}$). Let $L : M \to M$ be a linear map. We can make M into an $\mathbb{F}[x]$-module if we define the $\mathbb{F}[x]$ action as follows: if $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$ and $m \in M$, let $fm = a_0m + a_1L(m) + \cdots + a_nL^n(m)$, where L^n is the n-fold composition of L with itself. (The reader should check that this indeed satisfies the defining identities for modules.) In other words, we define $xm := L(m)$ and extend the action to $\mathbb{F}[x]$ by using the module identities. Conversely, if M is an $\mathbb{F}[x]$-module, then $x(a_1m_1 + a_2m_2) = a_1xm_1 + a_2xm_2$ for all $a_1, a_2 \in \mathbb{F}$ and $m_1, m_2 \in M$, so $m \mapsto xm : M \to M$ is a linear map. To say all this in a nutshell, an $\mathbb{F}[x]$-module is just a $\mathbb{F}$-module equipped with an $\mathbb{F}$-module endomorphism.

Example. Let us apply this perspective to $\mathbb{F}[x]$ itself. By our "official" definition, $\mathbb{F}[x]$ consists of the sequences $c : \mathbb{N} \to \mathbb{F}$ that are finitely non-zero. (Here, c_i, $i \in \mathbb{N}$ is the coefficient of x^i when we write a polynomial in the traditional way: $c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$.) As an $\mathbb{F}$-vector space, $\mathbb{F}[x]$ has a basis consisting of the sequences δ_i, $i = 0, \ldots$, where $\delta_{ii} = 1$ and $\delta_{ij} = 0$ when $i \neq j$, and x acts on this basis by $x\delta_i = \delta_{i+1}$. The use of the symbol δ_i to denote elements of $\mathbb{F}[x]$ is unusual, of course. I have done this to emphasize the structure that we have here. The usual notation for δ_i is x^i. Note that when we view $\mathbb{F}[x]$ as a module, we regard x as the sequence δ_1. When we regard $\mathbb{F}[x]$ a a ring, we are likely to view x as an "indeterminate" (a somewhat evasive label). When we regard $\mathbb{F}[x]$ as the ring of operators of an $\mathbb{F}[x]$-module, x becomes a linear map. (Such mental pictures may serve as a reminder of

the structures that we are working with, but of course mental pictures are personal. You may use whatever pictures you prefer.)

Cyclic $\mathbb{F}[x]$-modules.

Let us try to understand the structure of $\mathbb{F}[x]/(g)$, where $g = a_0 + a_1 x + \cdots + x^n$, $a_i \in \mathbb{F}$. By the division theorem, no polynomial of degree $< n$ belongs to the ideal (g) and thus (using coset notation) $1 + (g), x + (g), x^2 + (g), \ldots, x^{n-1} + (g)$ are independent as elements of the $\mathbb{F}$-vector space $\mathbb{F}[x]/(g)$. (If they were not independent, you would be able to construct a polynomial of degree $< n$ in (g). *How?*) Also by the division theorem, any polynomial $h \in \mathbb{F}[x]$ differs from a multiple of g by a polynomial of degree $< n$, so the set

$$\mathcal{X} = \{\, 1 + (g),\, x + (g),\, x^2 + (g),\, \ldots, x^{n-1} + (g) \,\}$$

spans the $\mathbb{F}$-vector space $\mathbb{F}[x]/(g)$ and hence is a basis for this space.

Now, the linear map $x : \mathbb{F}[x]/(g) \to \mathbb{F}[x]/(g)$ acts on the elements of $\mathcal{X}$ as follows:

$$\begin{aligned}
x\big(1 + (g)\big) &= x + (g) \\
x\big(x + (g)\big) &= x^2 + (g) \\
&\vdots \\
x(x^{n-1} + (g)) &= -a_0\big(1 + (g)\big) - a_1\big(x + (g)\big) - \cdots - a_{n-1}\big(x^{n-1} + (g)\big).
\end{aligned}$$

If we represent each element of $\mathbb{F}[x]/(g)$ as the row vectors whose entries are the constants in $\mathbb{F}$ that we need to express the element as a linear combination of basis vectors, then the matrix for the linear map x is:

$$(x; \mathcal{X}\mathcal{X}) = \begin{pmatrix}
0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 \\
-a_0 & -a_1 & -a_2 & -a_3 & \cdots & -a_{n-1}
\end{pmatrix}.$$

Here, we are using the notational convention introduced in Lecture 23. If $f + (g) \in \mathbb{F}[x]/(g)$, then the row vector that express $f + (g)$ with respect to the basis $\mathcal{X}$ is denoted $(f + (g); \mathcal{X})$. We are assuming that the action of x is represented by matrix multiplication on the right:

$$(f + (g); \mathcal{X})\,(x; \mathcal{X}\mathcal{X}) = (xf + (g); \mathcal{X}).$$

Of course, we could also decide to use column vectors to express the elements of $\mathbb{F}[x]/(g)$ and express x by matrix multiplication on the left. In this case the matrix that we would write would be the transpose of the one written above. If you look in other books, you may see this. Either of these matrices may be called the *companion matrix* of g.