M7210 Lecture 34 Friday, November 9, 2012

Cyclic $\mathbb{F}[x]$-modules (continued)

From now on, rather than using coset notation for elements of $\mathbb{F}[x]/(g)$, we will simply use u^0 as a name for $1+(g)$. We let $u := xu_0 = x+(g)$ and $u^i := x^i u_0$. In general if $f \in \mathbb{F}[x]$, then we will write $f(u)$ as an abbreviation for $f+(g)$. Since $\mathbb{F}[x]/(g)$ is a ring—as well as an $\mathbb{F}[x]$-module—we could think of u^i as the i-fold product $u \cdot u \cdots u$. But of course we do not multiply elements of a module, so we must bear in mind that u^i is just a symbol. Similarly, $f(u)$ is "really" $f(x)u_0$—the image of u_0 under the action of $f(x)$—or equally really the residue of f mod (g).

If $g = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$, then $\{1, u, \ldots, u^{n-1}\}$ is a basis for the $\mathbb{F}$-vector space $\mathbb{F}[x]/(g)$, and the action of x is given by $xu^{i-1} = u^i$ for $i = 1, \ldots, n-1$, and $xu^{n-1} = -a_0 - a_1 u - \cdots - a_{n-1}u^{n-1}$. We have just repeated the description of the companion matrix.

Suppose g in the last example of the last lecture is a power of a polynomial—say

$$h = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + x^k, \text{ and } g = h^\ell = a_0^\ell + \cdots + x^{k\ell}.$$

There are natural bases for (the vector space) $\mathbb{F}[x]/(h^\ell)$ other than $\{1, u, u^2, \ldots, u^{k\ell-1}\}$. For example

$$\begin{aligned}\big\{&1, u, u^2, \ldots, u^{k-1},\\ &h(u), uh(u), u^2h(u), \ldots, u^{k-1}h(u),\\ &h^2(u), uh^2(u), u^2h^2(u), \ldots, u^{k-1}h^2(u),\\ &\vdots\\ &h^{\ell-1}(u), uh^{\ell-1}(u), u^2h^{\ell-1}(u), \ldots, u^{k-1}h^{\ell-1}(u)\big\}\end{aligned}$$

Problem. Justify the claim that this is a base. What does the matrix that expresses

$$f(u) \mapsto xf(u) : \mathbb{F}/(h^\ell) \to \mathbb{F}/(h^\ell)$$

look like?

Let us look at the specific case when $h = x - c$ and $g = (x-c)^n$. In this case, we have a basis $\mathcal{V} = \{v_0, \ldots, v_{n-1}$ defined as follows: $v_0 = u^0$, $v_1 = (x-c)u^0$, $v_2 = (x-c)v_1 = (x-c)^2u_0$, …, $v_{n-1} = (x-c)v_{n-2} = (x-c)^{n-1}u^0$. Note that $(x-c)v_{n-1} = 0$. Thus:

$$\big((x-c); \mathcal{V}\mathcal{V}\big) = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0\\ 0 & 0 & 1 & 0 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \cdots & 0 & 1\\ 0 & 0 & 0 & 0 & \cdots & 0 & 0\end{pmatrix}.$$

Thus, with respect to this basis for $\mathbb{F}[x]/(x-c)^n$ we express the action of x by a so-called "Jordan block":

$$\big(x; \mathcal{V}\mathcal{V}\big) = \begin{pmatrix} c & 1 & 0 & 0 & \cdots & 0 & 0\\ 0 & c & 1 & 0 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \cdots & c & 1\\ 0 & 0 & 0 & 0 & \cdots & 0 & c\end{pmatrix}.$$

Applications to linear maps

Suppose V is a finite-dimensional vector space over $\mathbb{F}$ and $L : V \to V$ is a linear map. Then, as we explained in the last lecture, we can view V as an $\mathbb{F}[x]$-module. I will refer to this as (V, L). In general,(V, L) is *not* cyclic as an $\mathbb{F}[x]$-module. This is quite obvious if L is the zero map. Then the orbit of any non-zero $v_0 \in V$ under the action of $\mathbb{F}[x]$ is just the one-dimensional subspace spanned by v_0.

Since V is finite-dimensional, (V, L) is at least finitely-generated as an $\mathbb{F}[x]$-module. Any $\mathbb{F}$-vector-space basis of V will obviously generate (V, L) as an $\mathbb{F}[x]$-module. In general, the elements of an $\mathbb{F}$-vector-space basis of V will not be independent over $\mathbb{F}[x]$.

To be continued ...