Math 525 Class 39 December 4

Q: (from last time) Is a finitely-generated module over a Noetherian ring necessarily a Noetherian module?

A: Yes, in fact this is an iff. See Ex 8, Sec 15.1, p. 668. The fundamental lemma is Ex 6:

If $0 \to M' \to M \to M'' \to 0$ is an exact sequence of R-modules, M is Noetherian iff M' and M'' are Noetherian.

From this it follows that (Ex 7) submodules, quotients, and finite direct sums of Noetherian R-modules are Noetherian.

The R-module R is Noetherian iff R is a Noetherian ring.

<u>More about this next semester.</u>

In the meantime: a technique for learning about rational canonical form, and other things. Sometimes there is a mysterious-seeming procedure and we can learn by trying to figure out why it works.

An example from my nephew:

Let $f(x) = 2x + 3$ find $f^{-1}(x)$.

Procedure: ① replace $f(x)$ with y

$$y = 2x + 3$$

② Solve for x.

$$x = \frac{1}{2}(y - 3)$$

③ Replace x with y and vice versa.

$$y = \frac{1}{2}(x-3)$$

④ Replace y with $f^{-1}(x)$.

$$f^{-1}(x) = \frac{1}{2}(x - 3)$$

Asking why, with my nephew:

Q: What is $f^{-1}(x)$?

A: It is an f with a -1 on top.

Q: What is $f^{-1}(f(x))$?

A: How should I know? Why would you even ask that question?

Q: What is the definition of $f^{-1}(x)$?

A: The thing you obtain with the procedure above, We now present a mysterious procedure for finding the conjugacy classes of $GL_3(\mathbb{F}_2)$ and propose to ask some appropriate "why" questions, later.

$$|GL_3(\mathbb{F}_2)| = (2^3-1)(2^3-2)(2^3-2^2) = 168 = 2^3 \cdot 3 \cdot 7$$

So the possible orders of elements include:

1, 2, 3, 4, 7

Suppose (following Example 5, p. 487) that $A \in GL_3(\mathbb{F}_2)$ and $A^7 = I$

The minimal polynomial of A must divide $x^7 - 1$.

In $\mathbb{F}_2[x]$ $\quad x^7 - 1 = x^7 + 1 = (x+1)(x^3+x^2+1)(x^3+x+1)$

~~The minimal minimal polynomial of A any matrix B in $GL_3(\mathbb{F}_2)$ which~~

If $B \in GL_3(\mathbb{F}_2)$ has $m_B(x) \mid (x^7-1)$ in $\mathbb{F}_2[x]$,

then $B^7 = I$. Also $\deg(m_B(x)) \leq 3$.

Thus $m_B(x) = x+1$, x^3+x^2+1, or x^3+x+1.

If $m_B(x) = x+1$ $\quad B = I$

If $m_B(x) = x^3+x^2+1$, then $c_B(x) = x^3+x^2+1$

and we have B (up to conjugacy) is

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Similarly if $m_B(x) = x^3 + x + 1 = c_B(x)$

up to conjugacy $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

Now suppose we consider the possibility of an element of order 4. Then the minimal polyn. must divide

$$x^4 - 1 = x^4 + 1 = (x+1)^4 \in \mathbb{F}_2[x]$$

If $B \in GL_3(\mathbb{F}_2)$ is a matrix with $m_B(x) \mid (x+1)^4$ then $m_B(x) = x+1$, $(x+1)^2$, or $(x+1)^3$, because $\deg m_B(x) \leq 3$.

If $m_B(x) = x+1$, then $B = I$.

If $m_B(x) = (x+1)^2 = x^2+1$, $B^2 = I$ and B has order 2, not order 4.

Thus $m_B(x) = (x+1)^3 = x^3 + x^2 + x + 1$.

$$= c_B(x).$$

Up to conjugacy, $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

Now we can explain why there are no elements of order 6 or 8.

Consider first the possibility of an element of order 8. Then we would have $m_B(x) \mid x^8+1 = (x+1)^8$

So $m_B(x) = x+1, (x+1)^2$, or $(x+1)^3$.

Thus the order of B is 1, 2, or 4.

So no elements of order 8.

Suppose we had an element of order 6.

Then $m_B(x) \mid (x^6+1) = (x+1)^2(x^2+x+1)^2$

and thus $m_B(x) = x+1, (x+1)^2, (x^2+x+1)$, or $(x+1)(x^2+x+1)$

~~Si~~ Since $(x^2+x+1)(x+1) = x^3+1$, the last 2 cases result in an element of order 3 and the first two give elements of orders 1, 2.

Notice that if there is no element of order 6, there is no element of order $42 = 6 \cdot 7$.

Reasoning similar to the previous reasoning will eliminate all orders of elements except 1, 2, 3, 4, 7.

For elements of order 2, we know that

$m_B(x) \mid (x^2+1) = (x+1)^2$, so $m_B(x) = (1+x)^2$

and $c_B(x) = (x+1)^3 = x^3+x^2+x+1$

Thus up to conjugacy $B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

Now we can do 2 things:

- Go through this reasoning and ask "why?"
- Check our work with the computer!

Quiz Wed Dec 6. Example (5) p. 487 Sec 12.2.

Slightly pathological linear transformations of ∞-dim'l vector spaces.

$V =$ sequences of real numbers

$\{(a_0, a_1, a_2, \ldots) \mid a_i \in \mathbb{R}\}$.

$W = \{$ sequences in V that are eventually 0.

$T: V \to V \qquad T(a_0, a_1, a_2, \ldots) = (a_1, a_2, a_3, \ldots)$

$S: V \to V \qquad S(a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots)$