Solution Set 8

Math 123
April 7, 2002

1. *Artin §12.7 #6*

Since the eigenvalue 5 has multiplicity 3 in the characteristic polynomial, given that the 5-eigenspace is 2-dimensional we can conclude that the normal form for this matrix is

$$\begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{bmatrix}.$$

---

2. *Artin §12.7 #9b*

A general algorithm for this kind of problem is given in Artin; this case is easy enough to solve explicitly. Setting $X(t) = (x(t), y(t))$ we have $AX(t) = (0, x(t)) = (x'(t), y'(t))$ which means that $x(t) = x_0$ is constant, and $y(t) = tx_0 + y_0$ by integrating. Thus $X(t) = (x_0, tx_0 + y_0)$ for some x_0, y_0.

---

3. *Artin §12.7 #18*

The problem as stated is ambiguous as it does not specify what ring or field the entries of the matrix are contained in; it is reasonable to assume that the coefficients are in an arbitrary field F.[1] Let $V = F^n$ be an n-dimensional vector space and let $T : V \to V$ be the operator associated with the matrix A. This definition gives V the structure of a $F[t]$-module; we would like to find a presentation of the module.

Clearly V is finitely generated as an $F[t]$ module since it is finitely generated as an F-module (i.e. vector space). Indeed, let v_i be the i-th coordinate vector of $V = F^n$, and let e_i be the i-th coordinate vector of $F[t]^n$ (i.e. $e_1 = (1, 0, \ldots, 0)$); we thus have a map $\varphi : F[t]^n \to V$ sending $e_i \mapsto v_i$ (and thus $f(t) \cdot e_i \mapsto f(T)v_i$). Now we would like to find the relations, i.e. elements of the kernel of φ. Well, if $Tv_i = w_i$ we have $\varphi(te_i - w_i) = 0$ (where we are thinking of w_i as an element of both F^n and $F[t]^n \supset F^n$). Now, we know that once we have determined the operator T we have determined V as an $F[t]$-module (and have thus found all relations); since a linear operator is completely determined by how it acts on a basis, we know that we have a complete set of relations. Thus if $w_i = (w_{i1}, \ldots, w_{in})$ our

[1] Most people assumed that the field was $\mathbf{C}$ and used Jordan normal form to solve the problem. This combined with permanence of identities can yield a proof for an arbitrary ring, but I think that misses the point of the problem. Also, you *really* need to be able to understand this proof.

presentation matrix is

$$M = \begin{bmatrix} t - w_{11} & -w_{21} & \cdots & -w_{n1} \\ -w_{12} & t - w_{22} & \cdots & -w_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ -w_{1n} & -w_{2n} & \cdots & t - w_{nn} \end{bmatrix} = tI_n - A$$

and $\det(M) = p(t)$ is the characteristic polynomial of A. Now, by Cramer's rule we know we can find a matrix (the adjoint matrix) M' with $MM' = \det(M)I_n$, (i.e. $M^{-1} = \det(M)^{-1}\operatorname{Adj}(M)$) so $M(M'e_i) = p(t)e_i$ which means $p(t)e_i \in \operatorname{im}(M)$. But since M is a presentation matrix we have $V \cong F[t]^n/MF[t]^n$, so if $x = (x_1, \dots, x_n) \in F^n$ is any vector we have $p(t)x = (p(t)x_1, \dots, p(t)x_n) \in MF[t]^n$, so $p(T)x = 0$ in V for all x, i.e. $p(T) = 0$.

---

4. *Artin §12.7 #21*

It suffices to show that a Jordan block is similar to its transpose, because then if our vector space V is $\oplus_i W_i$ where W_i is stable under A and the matrix A_i for A on W_i is a Jordan block, then we can find P_i such that $P_i A_i P_i^{-1} = A_i^t$; defining an operator P on V that acts as P_i on W_i will give $PAP^{-1} = A^t$. (Or, more concretely, let P be the block diagonal matrix with each P_i on the diagonal.)

So assume that A is a Jordan block with eigenvalue α, i.e. if $v_1, \dots, v_n$ is the basis for A then $Av_1 = \alpha v_1 + v_2, \dots, Av_{n-1} = \alpha v_{n-1} + v_n, Av_n = \alpha v_n$. Well, choosing the basis $w_i = v_{n-i}$ we have $Aw_1 = \alpha w_1, Aw_2 = \alpha w_2 + w_1, \dots, Aw_n = \alpha w_n + w_{n-1}$. In other words,

$$\begin{bmatrix} \alpha & 1 & \cdots & 0 & 0 \\ 0 & \alpha & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \alpha & 1 \\ 0 & 0 & \cdots & 0 & \alpha \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix} \begin{bmatrix} \alpha & 0 & \cdots & 0 & 0 \\ 1 & \alpha & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \alpha & 0 \\ 0 & 0 & \cdots & 1 & \alpha \end{bmatrix} \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

which shows that $A \sim A^t$. A more abstract way of seeing this is that A^t also has characteristic polynomial $(x-\alpha)^n$ and has a one-dimensional α-eigenspace, which means it must have the same Jordan canonical form.

---

5. *Artin §13.1 #3*

This proof is nearly identical to the proof that a finite integral domain is a field (indeed, a finite integral domain is always a finite dimensional vector space over some subring isomorphic to $\mathbf{F}_p$). Let $a \in R$ be nonzero; we wish to show that a has an inverse. Define $m_a : R \to R$ by $m_a(x) = ax$. Clearly m_a is F-linear; also, if $m_a(x) = 0$ then $ax = 0$ which means that $x = 0$ since R is an integral domain and $a \neq 0$. Thus m_a is injective; since it is a linear operator on a finite-dimensional vector space, it is also surjective; therefore, $1 \in \operatorname{im}(m_a)$ so there is some b with $1 = m_a(b) = ab$.

---

6. *Artin §13.2 #1*

Let $\beta = 1 + \alpha^2$. Using a neat linear algebra trick that you know if you came to my section or by simply noting that $4 = (\beta - 1)^3 = \beta^3 - 3\beta^2 + 3\beta - 1$, we find that with $f(x) = x^3 - 3x^2 + 3x - 5$, we have $f(\beta) = 0$. In order to show that f is irreducible over $\mathbf{Q}$ we only need to show that f has no rational roots; since f is monic, it suffices to show that f has no roots modulo 7, which is true by a simple calculation. Thus f is the irreducible polynomial for $1 + \alpha^2$. (Or, using the fact that the degree of a field extension is multiplicative [which you weren't allowed to use here], since 3 is prime and $\beta \notin \mathbf{Q}$, we must have that the degree of β over $\mathbf{Q}$ is 3, so f is automatically irreducible.)

---

7. *Artin §13.2 #3*

Using the same linear algebra trick as before, or by noting that $60 = (\alpha^2 - 8)^2 = \alpha^4 - 16\alpha^2 + 64$, we find that α is a root of $f(x) = x^4 - 16x^2 + 4$. Using the quadratic formula we find that the roots of $f(x)$ are $\pm\sqrt{8 \pm 2\sqrt{15}}$; note that by squaring both sides we see that $\sqrt{5} + \sqrt{3} = \sqrt{8 + 2\sqrt{15}}$ and $\sqrt{5} - \sqrt{3} = \sqrt{8 - 2\sqrt{15}}$. Let $\beta = \sqrt{5} - \sqrt{3}$. Now, if f is not irreducible (over some field) then f has a linear or a quadratic factor. If f has no root then one of the following must be a quadratic factor:

$$f_1(x) = (x - \alpha)(x + \alpha) = x^2 - \alpha^2 = x^2 - (8 + 2\sqrt{15})$$
$$f_2(x) = (x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta = x^2 - 2x\sqrt{5} + 2$$
$$f_3(x) = (x - \alpha)(x + \beta) = x^2 - (\alpha - \beta)x - \alpha\beta = x^2 - 2x\sqrt{3} - 2.$$

a) Clearly f has no rational roots and none of f_1, f_2, f_3 is a rational polynomial, so f is irreducible over $\mathbf{Q}$.

b) Since $\sqrt{3} \notin \mathbf{Q}(\sqrt{5})$ (as you showed on a previous homework assignment), f has no roots in $\mathbf{Q}(\sqrt{5})$. However, $f_2 \in \mathbf{Q}(\sqrt{5})[x]$, so f_2 is the minimal polynomial for α over $\mathbf{Q}(\sqrt{5})$.

c) Similarly, $\pm\alpha, \pm\beta \notin \mathbf{Q}(\sqrt{10})$, so f has no linear factors; however, none of $f_1, f_2, f_3 \in \mathbf{Q}(\sqrt{10})[x]$, so f is the minimal polynomial for α over $\mathbf{Q}(\sqrt{10})$ as well.

d) Since $\sqrt{3}, \sqrt{5} \notin \mathbf{Q}(\sqrt{15})$, f has no linear factors; however $f_1 \in \mathbf{Q}(\sqrt{15})[x]$, so f_1 is the minimal polynomial for α.

---

8. *Artin §13.2 #4*

To do this problem, one could simply solve the equation

$$(1 + \alpha + \alpha^2)(a + b\alpha + c\alpha^2) = 1$$

for a, b, c; this would require solving some linear equations. However, there is a slicker, more algorithmic way to get at these equations. Let $K = \mathbf{Q}(\alpha)$. For any $\beta \in K$ we can define a map $m_\beta : K \to K$ taking $x \mapsto \beta x$; this will be a $\mathbf{Q}$-linear map with inverse $m_\beta^{-1} = m_{\beta^{-1}}$ if $\beta \neq 0$. Now, m_β will have a matrix with respect to the basis $(1, \alpha, \alpha^2)$; therefore, m_β^{-1} will have the inverse matrix. Since $m_\beta^{-1}(1) = \beta^{-1}$ we can read off β^{-1} in terms of $(1, \alpha, \alpha^2)$ from the entries of the first column.

In our case, $\beta = 1 + \alpha + \alpha^2$. Noting that $m_\alpha(1) = \alpha, m_\alpha(\alpha) = \alpha^2$, and $m_\alpha(\alpha^2) = \alpha^3 = 3\alpha - 4$, it is an easy calculation to find that

$$m_\beta = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & -4 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & -4 & 0 \\ 0 & 3 & -4 \\ 1 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 1 & -4 & -4 \\ 1 & 4 & -1 \\ 1 & 1 & 4 \end{bmatrix}.$$

Using any matrix inversion algorithm we thus find

$$m_\beta^{-1} = \frac{1}{49} \begin{bmatrix} 17 & 12 & 20 \\ -5 & 8 & -3 \\ -3 & -5 & 8 \end{bmatrix}$$

so $\beta^{-1} = (17 - 5\alpha - 3\alpha^2)/49$.

---

9. *Artin §13.2 #5*

We have

$$\begin{aligned} 0 &= \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \\ \implies -a_0 &= \alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) \\ \implies \alpha^{-1} &= -\frac{1}{a_0}(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1). \end{aligned}$$

Note that $a_0 \neq 0$ because $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is irreducible.

Joe Rabinoff