Solutions to second midterm

Dave Bayer, Modern Algebra, Exam date November, 1998

[1] Find the multiplicative inverse of 23 mod 103.

Solution: By the extended euclidean algorithm, we compute

$$\begin{bmatrix} 103 & 1 & 0 \\ 23 & 0 & 1 \\ 11 & 1 & -4 \\ 1 & -2 & 9 \end{bmatrix} \quad \text{which we interpret as} \quad \begin{bmatrix} 103 = 1\cdot 103 + 0 \cdot 23 \\ 23 = 0 \cdot 103 + 1 \cdot 23 \\ 11 = 1 \cdot 103 - 4 \cdot 23 \\ 1 = -2 \cdot 103 + 9 \cdot 23 \end{bmatrix}$$

so $23^{-1} = 9 \bmod 103$. We check our answer: $23 \cdot 9 = 230 - 23 = 207 = (2 \cdot 103) + 1$.

Alternatively, the multiplicative group of integers mod 103 has order 102 because 103 is prime, so $x \cdot x^{101} = x^{102} = 1$ for any integer x which is nonzero mod 103. Writing $101 = 64 + 32 + 4 + 1$, we can compute x^{101} as $x^{64} \cdot x^{32} \cdot x^4 \cdot x$. We compute $23^{-1} = 23^{101}$ by hand, reducing mod 103 whenever it helps:

$$\begin{aligned}
23^2 &= (25-2)^2 = 625 - 4 \cdot 25 + 4 = 529 = 14 \\
23^4 &= 14^2 = (15-1)^2 = 225 - 2 \cdot 15 + 1 = 196 = -10 \\
23^8 &= (-10)^2 = 100 = -3 \\
23^{16} &= (-3)^2 = 9 \\
23^{32} &= 9^2 = 81 = -22 \\
23^{64} &= (-22)^2 = 4 \cdot 11^2 = 4 \cdot 121 = 4 \cdot 18 = 72 = -31 \\
23^{-1} &= 23^{101} = 23^{64} \cdot 23^{32} \cdot 23^4 \cdot 23 = (-31)(-22)(-10)23 = -(620+62)230 \\
&= -(2+62)24 = -64 \cdot 24 = -16 \cdot 96 = 16 \cdot 7 = 80 + 32 = 112 = 9
\end{aligned}$$

We have used several times the formula $(a-b)^2 = a^2 - 2ab + b^2$ to rewrite squares into products we can recall without the tedium of direct multiplication. We chose negative representatives mod 103 whenever they had a smaller magnitude. The point is to meander through the arithmetic, keeping sufficiently amused to avoid making mistakes. It is unlikely that any two people would follow the same course through this calculation.

Can you think of a way of computing x^{101} that takes fewer than the 9 multiplies

$$x^2 = x \cdot x, \quad x^4 = x^2 \cdot x^2, \quad x^8 = x^4 \cdot x^4, \quad x^{16} = x^8 \cdot x^8, \quad x^{32} = x^{16} \cdot x^{16}, \quad x^{64} = x^{32} \cdot x^{32},$$

$$x^5 = x \cdot x^4, \quad x^{37} = x^5 \cdot x^{32}, \quad x^{101} = x^{37} \cdot x^{64}$$

used here? What about for other powers of x? How would you teach a computer to exponentiate, if multiplication was *extremely* expensive, and you were allowed all the preparation time you needed to plan the calculation?

[2] *Prove* **ONE** *of the following two assertions:*

(a) Let V and W be subspaces of a vector space U. Then

$$\dim(V) + \dim(W) = \dim(V \cap W) + \dim(V + W).$$

Solution: Choose a basis $u_1, \ldots, u_j$ for $V \cap W$. Extend $u_1, \ldots, u_j$ to a basis $u_1, \ldots, u_j, v_1, \ldots, v_k$ for V. Also extend $u_1, \ldots, u_j$ to a basis $u_1, \ldots, u_j, w_1, \ldots, w_\ell$ for W. We claim that $u_1, \ldots, u_j, v_1, \ldots, v_k, w_1, \ldots, w_\ell$ is a basis for $V + W$. Counting basis elements, the formula will follow as

$$(j+k) \; + \; (j+\ell) \quad = \quad (j) \; + \; (j+k+\ell).$$

Independence: For any expression

$$\sum_{i=1}^{j} r_i \, u_i \; + \; \sum_{i=1}^{k} s_i \, v_i \; + \; \sum_{i=1}^{\ell} t_i \, w_i \quad = \quad 0$$

we need to show that all coefficients r_i, s_i, t_i are zero. Write

$$\alpha \quad = \quad \sum_{i=1}^{j} r_i \, u_i \; + \; \sum_{i=1}^{k} s_i \, v_i \quad = \quad -\sum_{i=1}^{\ell} t_i \, w_i.$$

We see that $\alpha \in V$ and $\alpha \in W$, so $\alpha \in V \cap W$. Since $u_1, \ldots, u_j$ is a basis for $V \cap W$, α can be written in a unique way as a linear combination of $u_1, \ldots, u_j$. This same expression must be the unique way of writing α as a linear combination of the basis $u_1, \ldots, u_j, w_1, \ldots, w_\ell$ for W, so we have $t_1 = \ldots = t_\ell = 0$. Thus $\alpha = 0$. Because $u_1, \ldots, u_j, v_1, \ldots, v_k$ is a basis for V, we have $r_1 = \ldots = r_j = 0$ and $s_1 = \ldots = s_k = 0$ as desired.

Spanning: If $u \in V + W$, we need to show that u can be written as a linear combination of the vectors $u_1, \ldots, u_j, v_1, \ldots, v_k, w_1, \ldots, w_\ell$. Write $u = v + w$ where $v \in V$ and $w \in W$, and write

$$v \quad = \quad \sum_{i=1}^{j} r_i \, u_i \; + \; \sum_{i=1}^{k} s_i \, v_i \quad \text{and} \quad w \quad = \quad \sum_{i=1}^{j} r'_i \, u_i \; + \; \sum_{i=1}^{\ell} t_i \, w_i.$$

Then

$$u \quad = \quad v + w \quad = \quad \sum_{i=1}^{j} (r_i + r'_i) \, u_i \; + \; \sum_{i=1}^{k} s_i \, v_i \; + \; \sum_{i=1}^{\ell} t_i \, w_i$$

as desired.

(b) Let $T : V \to W$ be a linear transformation of vector spaces. Then

$$\dim(\ker(T)) \; + \; \dim(\text{image}(T)) \quad = \quad \dim(V).$$

Solution: There are various ways to prove this; here is one: Choose a basis $u_1, \ldots, u_j$ for $\ker(T)$, and choose a basis $w_1, \ldots, w_k$ for image(T). For each $w_i \in W$, choose a vector $v_i \in V$ so $T(v_i) = w_i$. We claim that $u_1, \ldots, u_j, v_1, \ldots, v_k$ is a basis for V. Counting basis elements, the formula will follow as

$$(j) \; + \; (k) \quad = \quad (j+k).$$

Independence: For any expression

$$\sum_{i=1}^{j} r_i \, u_i \; + \; \sum_{i=1}^{k} s_i \, v_i \quad = \quad 0$$

we need to show that all coefficients r_i, s_i are zero. Applying T, we have

$$T\left(\sum_{i=1}^{j} r_i\, u_i \;+\; \sum_{i=1}^{k} s_i\, v_i\right) \quad=\quad 0 \;+\; \sum_{i=1}^{k} s_i\, T(v_i) \quad=\quad \sum_{i=1}^{k} s_i\, w_i \quad=\quad 0,$$

so $s_i = \ldots = s_k = 0$ because $w_1, \ldots, w_k$ is a basis for image(T). Now $r_i = \ldots = r_j = 0$ because $u_1, \ldots, u_j$ is a basis for $\ker(T)$.

Spanning: If $v \in V$, we need to show that v can be written as a linear combination of the vectors $u_1, \ldots, u_j, v_1, \ldots, v_k$. Write $T(v) = \sum_{i=1}^{k} s_i\, w_i$. Then $T(v) = T(\sum_{i=1}^{k} s_i\, v_i)$, so $v - \sum_{i=1}^{k} s_i\, v_i$ belongs to $\ker(T)$. Write

$$v - \sum_{i=1}^{k} s_i\, v_i = \sum_{i=1}^{j} r_i\, u_i, \qquad \text{so} \quad v = \sum_{i=1}^{j} r_i\, u_i \;+\; \sum_{i=1}^{k} s_i\, v_i \quad \text{as desired.}$$

[3] Let

$$A = \begin{bmatrix} 5 & -4 \\ 1 & 1 \end{bmatrix}.$$

Find a change of basis matrix B so $A = B\,C\,B^{-1}$ where C is in Jordan canonical form. Use B and C to give an expression for e^{At}. You do not need to multiply this expression out.

Solution: A has characteristic polynomial

$$\lambda^2 - \text{trace(A)}\lambda + \det(A) \quad=\quad \lambda^2 - 6\lambda + 9 = (\lambda - 3)^2,$$

so A has a repeated eigenvalue of 3. We have

$$A - 3I \quad=\quad \begin{bmatrix} 2 & -4 \\ 1 & -2 \end{bmatrix}$$

which is a nonzero matrix, so we have the Jordan canonical forms

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{for} \quad A - 3I, \qquad \text{and} \qquad \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix} \quad \text{for} \quad A,$$

with respect to any basis v_1, v_2 such that

$$(A - 3I)\, v_2 \quad=\quad v_1 \qquad \text{and} \qquad (A - 3I)\, v_1 \quad=\quad 0.$$

This will hold for most choices of v_2, so we try $v_2 = (1, 0)$. We have $(A - 3I)(1, 0) = (2, 1)$, and $(A - 3I)(2, 1) = (0, 0)$ as desired. Thus

$$A \;=\; \begin{bmatrix} 5 & -4 \\ 1 & 1 \end{bmatrix} \;=\; \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}.$$

We check our work:

$$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \;=\; \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \text{and} \quad \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 3 & 1 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \;=\; \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 3 & -6 \end{bmatrix} \;=\; \begin{bmatrix} 5 & -4 \\ 1 & 1 \end{bmatrix}.$$

It follows that

$$e^{At} \;=\; \begin{bmatrix} 5 & -4 \\ 1 & 1 \end{bmatrix} \;=\; \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} e^{3t} & te^{3t} \\ 0 & e^{3t} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}.$$

[4] Let $T : V \to V$ be a linear transformation from the n-dimensional vector space V to itself, such that $T^2 = 0$. Prove that for some basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$ of V, the matrix A for T with respect to this basis is in Jordan canonical form.

Solution: We have image$(T) \subset \ker(T)$, because $w \in \text{image}(T) \Rightarrow w = T(v) \Rightarrow T(w) = T^2(v) = 0$. Choose a basis $w_1, \ldots, w_j$ for image(T), and extend this basis to a basis $w_1, \ldots, w_j, u_1, \ldots, u_k$ for $\ker(T)$. For each w_i, choose a vector $v_i \in V$ so $T(v_i) = w_i$. We claim that $w_1, \ldots, w_j, u_1, \ldots, u_k, v_1, \ldots, v_j$ is a basis for V. Arranging this basis in the order $v_1, w_1, \ldots, v_j, w_j, u_1, \ldots, u_k$ and relabeling as $\mathbf{v}_1, \ldots, \mathbf{v}_n$ gives the desired Jordan form.
Independence: For any expression

$$\sum_{i=1}^{j} r_i\, w_i \;+\; \sum_{i=1}^{k} s_i\, u_i \;+\; \sum_{i=1}^{j} t_i\, v_i \;\;=\;\; 0$$

we need to show that all coefficients r_i, s_i, t_i are zero. Applying T, we have

$$T\left(\sum_{i=1}^{j} r_i\, w_i \;+\; \sum_{i=1}^{k} s_i\, u_i \;+\; \sum_{i=1}^{j} t_i\, v_i\right) \;\;=\;\; 0 \;+\; 0 \;+\; \sum_{i=1}^{j} t_i\, T(v_i) \;\;=\;\; \sum_{i=1}^{j} y_i\, w_i \;\;=\;\; 0,$$

so $t_i = \ldots = t_j = 0$ because $w_1, \ldots, w_k$ is a basis for image(T). Now $r_i = \ldots = r_j = 0$ and $s_i = \ldots = s_k = 0$ because $w_1, \ldots, w_j, u_1, \ldots, u_k$ is a basis for $\ker(T)$.
Spanning: If $v \in V$, we need to show that v can be written as a linear combination of the vectors $u_1, \ldots, u_j, v_1, \ldots, v_k$. Write $T(v) = \sum_{i=1}^{j} t_i\, w_i$. Then $T(v) = T(\sum_{i=1}^{j} t_i\, v_i)$, so $v - \sum_{i=1}^{j} t_i\, v_i$ belongs to $\ker(T)$. Write

$$v - \sum_{i=1}^{j} t_i\, v_i = \sum_{i=1}^{j} r_i\, w_i \;+\; \sum_{i=1}^{k} s_i\, u_i,$$

so

$$v \;\;=\;\; \sum_{i=1}^{j} r_i\, w_i \;+\; \sum_{i=1}^{k} s_i\, u_i \;+\; \sum_{i=1}^{j} t_i\, v_i$$

as desired.

[5] Let

$$A = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}.$$

Find a formula for e^{At}.

Solution: We first need a formula for A^n. We have

$$A^1 = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix},\; A^2 = \begin{bmatrix} \lambda^2 & 2\lambda & 1 \\ 0 & \lambda^2 & 2\lambda \\ 0 & 0 & \lambda \end{bmatrix},\; A^3 = \begin{bmatrix} \lambda^3 & 3\lambda^2 & 3\lambda \\ 0 & \lambda^3 & 3\lambda^2 \\ 0 & 0 & \lambda \end{bmatrix},\; A^4 = \begin{bmatrix} \lambda^4 & 4\lambda^3 & 6\lambda^2 \\ 0 & \lambda^4 & 4\lambda^3 \\ 0 & 0 & \lambda \end{bmatrix},\; A^5 = \begin{bmatrix} \lambda^5 & 5\lambda^4 & 10\lambda^3 \\ 0 & \lambda^5 & 5\lambda^4 \\ 0 & 0 & \lambda \end{bmatrix}$$

allowing us to guess that

$$A^n = \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \frac{n(n-1)}{2}\lambda^{n-2} \\ 0 & \lambda^n & n\lambda^{n-1} \\ 0 & 0 & \lambda^n \end{bmatrix}$$

We check this formula inductively:

$$A^{n+1} = A\,A^n = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix} \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \frac{n(n-1)}{2}\lambda^{n-2} \\ 0 & \lambda^n & n\lambda^{n-1} \\ 0 & 0 & \lambda^n \end{bmatrix} = \begin{bmatrix} \lambda^{(n+1)} & (n+1)\lambda^n & \frac{(n+1)n}{2}\lambda^{n-1} \\ 0 & \lambda^{(n+1)} & (n+1)\lambda^n \\ 0 & 0 & \lambda^{(n+1)} \end{bmatrix}$$

as desired. Now,

$$\begin{aligned} e^{At} &= \sum_{n=0}^{\infty} A^n \frac{t^n}{n!} = \sum_{n=0}^{\infty} \begin{bmatrix} \lambda^n & n\lambda^{n-1} & \frac{n(n-1)}{2}\lambda^{n-2} \\ 0 & \lambda^n & n\lambda^{n-1} \\ 0 & 0 & \lambda^n \end{bmatrix} \frac{t^n}{n!} \\ &= \begin{bmatrix} \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} & \sum_{n=0}^{\infty} \frac{n\lambda^{n-1} t^n}{n!} & \sum_{n=0}^{\infty} \frac{\frac{n(n-1)}{2}\lambda^{n-2} t^n}{n!} \\ 0 & \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} & \sum_{n=0}^{\infty} \frac{n\lambda^{n-1} t^n}{n!} \\ 0 & 0 & \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} \end{bmatrix} \end{aligned}$$

Now,

$$\begin{aligned} \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} &= e^{\lambda t} \\ \sum_{n=0}^{\infty} \frac{n\lambda^{n-1} t^n}{n!} &= t \sum_{n=1}^{\infty} \frac{\lambda^{n-1} t^{n-1}}{(n-1)!} = t \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} = t\,e^{\lambda t} \\ \sum_{n=0}^{\infty} \frac{\frac{n(n-1)}{2}\lambda^{n-2} t^n}{n!} &= \frac{t^2}{2} \sum_{n=2}^{\infty} \frac{\lambda^{n-2} t^{n-2}}{(n-2)!} = \frac{t^2}{2} \sum_{n=0}^{\infty} \frac{\lambda^n t^n}{n!} = \frac{t^2}{2}\,e^{\lambda t} \end{aligned}$$

so

$$e^{At} = \begin{bmatrix} e^{\lambda t} & te^{\lambda t} & \frac{t^2}{2}e^{\lambda t} \\ 0 & e^{\lambda t} & te^{\lambda t} \\ 0 & 0 & e^{\lambda t} \end{bmatrix}$$

giving us the desired formula.