LINEAR ALGEBRA MATH 50003 Solutions to Problem Sheet 3

1. (a) Eg. the companion matrix of this poly.

(b) Multiplying through by A, we get $I = A^4 + A^2 + A$, so we want A to satisfy the poly $x^4 + x^2 + x - 1$. Choose A to be the companion matrix of this poly.

(c) Here we need $2A^4 + 2A = I$. Since $2 = -1$ in the field $\mathbb{F}_3$, this can be written as $A^4 + A + I = 0$. Let C be the 4×4 companion matrix over $\mathbb{F}_3$ of the poly $x^4 + x + 1$. Notice that $1 \in \mathbb{F}_3$ is a root of this poly. So a 5×5 matrix over $\mathbb{F}_3$ which satisfies the poly is the block-diagonal $C \oplus (1)$.

(d) We want A to satisfy the poly $x^7 + 1$. This factorizes over $\mathbb{F}_2$ as $(x+1)(x^3+x+1)(x^3+x^2+1)$. So take A to be the companion matrix of one of the cubic factors, say $x^3 + x + 1$.

(e) We have the factorization $x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$. Take A to be the companion matrix of the second factor.

2. Let $c(x)$ be the char poly of A. By Cayley-Hamilton, $c(A) = 0$, and we are also given that $A^k = 0$. So A satisfies the polys $c(x)$ and x^k. If $d(x)$ is the gcd of these polys then $d(x) = r(x)c(x) + s(x)x^k$ for some polys $r, s \in F[x]$. Hence A also satisfies $d(x)$. But $d(x)$ is just the highest power of x that divides $c(x)$, so $d(x) = x^r$ for some $r \leq n$. Hence $A^r = 0$, and so $A^n = A^r A^{n-r} = 0$.

3. (a) The char poly of A is $c(x) = (x-1)^2(x-2) = x^3 - 4x^2 + 5x - 2$. By Cayley-Hamilton, $c(A) = 0$, so $A(A^2 - 4A + 5I) = 2I$. Therefore $A^{-1} = p(A)$ where $p(x) = (x^2 - 4x + 5)/2$.

(b) From $c(A) = 0$ we get $A^4 = 4A^3 - 5A^2 + 2A = 4(4A^2 - 5A + 2I) - 5A^2 + 2A = 11A^2 - 18A + 8I$.

(c) From $c(A) = 0$ we get $A^3 - 4A^2 = -5A + 2I$. This has the same evectors as A, which has eigenspaces $E_1 = \mathrm{Sp}(e_1, e_2 + e_3)$ and $E_2 = \mathrm{Sp}(2e_1 + 3e_3 + 4e_4)$.

4. (a) Let A be upper triangular with diagonal entries $\lambda_1, \ldots, \lambda_n$. So the characterictic poly of A is $p(x) = \prod_1^n (x - \lambda_i)$. Then $p(A) = (A - \lambda_1 I) \cdots (A - \lambda_n I)$. Note that the i^{th} factor $A - \lambda_i I$ in this product is upper triangular, and has its i^{th} diagonal entry equal to 0. Now argue by induction on i that the product of the first i factors $(A - \lambda_1 I) \cdots (A - \lambda_i I)$ has its first i columns all equal 0 (the zero column vector): this is true for $i = 1$, and the induction step is just a matter of observing that the product of a matrix with its first i columns 0 and an upper triangular matrix with $i + 1^{st}$ diagonal entry 0 has its first $i + 1$ cols 0. Hence $p(A)$ has its first n cols 0, ie. $p(A) = 0$, as required.

(b) Let A be an $n \times n$ matrix over $\mathbb{C}$ with char poly $p(x)$. By the Triangularisation Thm, $\exists$ P such that $B = P^{-1}AP$ is upper triangular. Then B also has char poly $p(x)$, and by (a) we have $p(B) = 0$. As $p(A) = Pp(B)P^{-1}$, it follows that $p(A) = 0$.

5. (a) The ii-entry of AB is $\sum_{j=1}^n a_{ij} b_{ji}$, so

$$\mathrm{tr}(AB) = \sum_{i=1}^n \sum_{j=1}^n a_{ij} b_{ji}.$$

Similarly $\mathrm{tr}(BA) = \sum_{k=1}^n \sum_{l=1}^n b_{kl} a_{lk}$. Chnaging the order of summation this is $\sum_{l=1}^n \sum_{k=1}^n a_{lk} b_{kl}$, and this is $\mathrm{tr}(AB)$.

(b) Let $C = AB$, so $C^2 = 0$. Cayley-Hamilton gives $C^2 - \mathrm{tr}(C)\, C + (\det C)\, I = 0$. Since $C^2 = 0$ and $\det C = 0$, this gives $\mathrm{tr}(C)\, C = 0$. So either $\mathrm{tr}(C) = 0$ or $C = 0$, and in either case $\mathrm{tr}(C) = 0$.

So $\mathrm{tr}(C) = \mathrm{tr}(AB) = 0$. By (a) therefore, $\mathrm{tr}(BA) = 0$. Now Cayley-Hamilton for BA gives

$$(BA)^2 - \mathrm{tr}(BA)\, BA + (\det BA)\, I = 0.$$

Since $\mathrm{tr}(BA) = \det BA = 0$, this implies $(BA)^2 = 0$.

(c) Not true for 3×3, eg. $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

6. (a) Suppose both d and d' are gcd's of f, g. Then as d' divides both f and g, we have $d|d'$. Similalry $d'|d$. Therefore $d' = \lambda d$ for some scalar λ.

(b) Let $d = \gcd(f, g)$, and let $r, s \in F[x]$ be such that $d = rf + sg$. Define $l = fg/d$. As $d|g$, $g/d \in F[x]$ and so $f|l$, and similarly $g|l$. Now let $k \in F[x]$ be a poly that is divisible by f and g. We need to show that $l|k$, or equivalently, that $fg|dk$. Now $dk = k(rf + sg)$, and both kf and kg are divisible by fg. Hence $fg|dk$, as required.

7. gcd is $x + 2$, and $x + 2 = \frac{1}{4}(f - (x + 1)g)$.

8. (a) Let $f(x) \in \mathbb{R}[x]$ be irreducible. Over $\mathbb{C}$, $f(x)$ factorizes as $\prod(x-\alpha_i)\prod(x-\beta_i)(x-\bar{\beta}_i)$, where α_i are the real roots and $\beta_i, \bar{\beta}_i$ conjugate pairs of non-real roots. Note that $(x - \beta_i)(x - \bar{\beta}_i)$ is a real quadratic. Hence as f is irreducible, either $f(x) = x - \alpha$ with α real, or $f(x) = (x - \beta)(x - \bar{\beta})$ with β non-real.

(b) $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$

(c) Monic quadratic irreds over $\mathbb{F}_3$: $x^2 + 1$, $x^2 + x - 1$, $x^2 - x - 1$

(d) An irred cubic over $\mathbb{F}_5$: $x^3 + x + 1$ (has no roots in $\mathbb{F}_5$)

(e) Over $\mathbb{F}_2$, $x^4 + 1 = (x + 1)^4$

(f) $x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$

9. (a) Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where $a_i \in \mathbb{Z}$ for all i. Let $\alpha = r/s$ be a root of $p(x)$, where r, s are integers, and suppose for a contradiction that $\alpha \notin \mathbb{Z}$. Then we can take it that r, s are coprime and $s > 1$. Then

$$r^n = s^n \left(-a_{n-1}r^{n-1}/s^{n-1} - \cdots - a_1 r/s - a_0\right).$$

The RHS is divisible by s, but the LHS is not (as r, s are coprime), a contradiction. Hence $\alpha \in \mathbb{Z}$.

(b) Suppose $x^3 + x + k$ is reducible over $\mathbb{Q}$. Then it has a root α, which is in $\mathbb{Z}$ by (a). So $k = -\alpha^3 - \alpha$. Since k is a positive integer and $k \leq 100$, the possible values of k are those with $\alpha = -1, -2, -3, -4$, namely $k = 2, 10, 30, 68$.

(c) Suppose $p(x) = x^4 + x + 1$ is reducible in $\mathbb{Q}[x]$. If it has a linear factor then it has a root in $\alpha \in \mathbb{Q}$, and then $\alpha \in \mathbb{Z}$ by (a). But then α divides the constant term 1 (as $\alpha^4 + \alpha + 1 = 0$), so $\alpha = \pm 1$, neither of which is a root of $p(x)$. Hence $p(x)$ must factorize as a product of quadratics, and by Gauss's Lemma (8.4(2)) of lecture notes, it has factorization $p(x) = (x^2 + ax + b)(x^2 + cx + d)$, where the coeffs $a, b, c, d \in \mathbb{Z}$. Then

$$a + c = 0, \; b + d + ac = 0, \; ad + bc = 1, \; bd = 1.$$

From the last eqn, $b = d = 1$ or $b = d = -1$, from which the 3rd eqn gives $a + c = \pm 1$. This conflicts with the 1st eqn, contradiction. Hence $p(x)$ is irred in $\mathbb{Q}[x]$.

10. Let A be $n \times n$ over $\mathbb{C}$ with $\text{tr}(A^i) = 0$ for all $i \geq 1$. By the Triangularisation Thm, $\exists\, P$ such that $B = P^{-1}AP$ is upper triangular. The diagonal entries of B are the eigenvalues. If these are all 0, then the char poly of A is x^n, so $A^n = 0$ by Cayley-Hamilton, which is the required result.

So assume now (for a contradiction) that A (and B) has at least one nonzero eigenvalue. Let the distinct evalues be $\lambda_1, \ldots, \lambda_r$ with multiplicities $m_1, \ldots, m_r$. Since similar matrices have the same trace (Q5 of Sheet 1), we have

$$\text{tr}(A^i) = \text{tr}(B^i) = m_1\lambda_1^i + \cdots + m_r\lambda_r^i$$

for each $i \geq 1$. These traces are all 0, so thinking of the m_i's as variables, they give a solution of the system of linear equations

$$\begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_r \\ \lambda_1^2 & \lambda_2^2 & \cdots & \lambda_r^2 \\ & & \cdots & \\ \lambda_1^r & \lambda_2^r & \cdots & \lambda_r^r \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_r \end{pmatrix} = 0.$$

The coefficient matrix is a Vandermonde matrix, and a well-known result (you probably saw this in the 1st year) states that this has determinant $\prod_1^r \lambda_i \prod_{i<j}(\lambda_i - \lambda_j)$. As the λ_i are distinct and nonzero, this det is nonzero, so the Vandermonde matrix is invertible, and the above system has only the zero solution. This is a contradiction, as the m_i are positive integers.