Linear Algebra II
Exercise Sheet no. 3

TECHNISCHE UNIVERSITÄT DARMSTADT

SS 2011
April 29, 2011

Prof. Dr. Otto
Dr. Le Roux
Dr. Linshaw

Exercise 1 (Warm-up: Multiple Zeroes)
For a polynomial $p = \sum_{i=0}^{n} a_i X^i \in \mathbb{F}[X]$ define its *formal derivative* p' by

$$p' := \sum_{i=1}^{n} i a_i X^{i-1}.$$

(a) Check that the usual product rule for differentiaton applies to the formal derivative of polynomials considered here!

(b) Let α be a zero of P. Show the equivalence of the following:
   i. α is a multiple zero of p. (In other words, $(X-\alpha)^2$ divides p.)
   ii. α is a zero of p'.
   iii. α is a zero of $\gcd(p, p')$.

Solution:

a) The map $p \mapsto p'$ is linear by definition, so it suffices to check that the claim holds for monomials $p = X^k$ and $q = X^l$. On the one hand $(pq)' = (X^{k+l})' = (k+l)X^{k+l-1}$; on the other hand $p'q + q'p = kX^{k-1}X^l + lX^{l-1}X^k = (k+l)X^{k+l-1}$.

b) Let α be a zero of p. Then $p = (X-\alpha)^r q$ for some $q \in \mathbb{F}[X]$ not divisible by $X - \alpha$. Then

$$p' = (X-\alpha)^r q' + r(X-\alpha)^{r-1} q.$$

To see that (i) and (ii) are equivalent, note that α is a multiple root of p iff $r \geq 2$, which is clearly equivalent to (ii). To see that (ii) and (iii) are equivalent, note that α is a zero of both p and p' iff $(X-\alpha)$ is a divisor of $\gcd(p, p')$.

Exercise 2 (Commutative subrings of matrix rings)
Let $A \in \mathbb{F}^{(n,n)}$ be an $n \times n$ matrix over a field $\mathbb{F}$. Let $R_A \subseteq \mathbb{F}^{(n,n)}$ be the subring generated by A, which consists of all linear combinations of powers of A.

(a) Prove that R_A is a commutative subring of $\mathbb{F}^{(n,n)}$.

(b) Consider the evaluation map $\tilde{}: \mathbb{F}[X] \to R_A$ defined by $\tilde{p} = \sum_i^n a_i A^i$ for $p = \sum_i^n a_i X^i$. Show that this map is a ring homomorphism. Is it surjective? Injective?

   Hint: By forgetting about the multiplicative structure, we may regard $\mathbb{F}[X]$ and R_A as vector spaces over $\mathbb{F}$, and we may regard $\tilde{}$ as a vector space homomorphism. Do $\mathbb{F}[X]$ and R_A have the same dimension as $\mathbb{F}$-vector spaces?

Solution:

a) We have $A^k A^l = A^{k+l} = A^l A^k$ for all $0 \leq k, l$ and since every element of the ring is a linear combination of powers of A, the claim follows.

b) It is straightforward to check that it is a ring homomorphism, and it is surjective by definition. Since $\mathbb{F}^{(n,n)}$ is a finite-dimensional vector space over $\mathbb{F}$ and R_A is a subspace of $\mathbb{F}^{(n,n)}$, R_A is also a finite-dimensional vector space over $\mathbb{F}$. On the other hand $\mathbb{F}[X]$ is an infinite-dimensional vector space over $\mathbb{F}$. (See exercise $T3.1$.) Therefore the map cannot be injective. (Note that this is consistent with the Cayley-Hamilton Theorem.)

Exercise 3 (The Euclidean algorithm revisited)

Recall the Euclidean algorithm from Exercise Sheet 2. In particular, given natural numbers a, b, we normalise so that $d_1 = \min\{a, b\}$ and $d_0 = \max\{a, b\}$. In each step, we divide with remainder, obtaining $d_{k-1} = q_k d_k + d_{k+1}$. At the end of this procedure $d_{k+1} = 0$, and $d_k = \gcd(a, b)$.

(a) Let k be the number of steps needed to compute $\gcd(a_0, b_0)$ in this way. Consider the matrix $M \in \mathbb{Z}^{(2,2)}$ given by

$$M = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}.$$

Show that M is regular and that M^{-1} is again a matrix over $\mathbb{Z}$. Compute $M^{-1} \begin{pmatrix} d_1 \\ d_0 \end{pmatrix}$.

(b) Interpret the entries in second row of M^{-1} in terms of $\gcd(d_0, d_1)$.

(c) Recall that the *least common multiple* $\mathrm{lcm}(d_0, d_1)$ is an integer z characterized by the following properties:

i. $d_0 | z$ and $d_1 | z$.

ii. If a is any integer for which $d_0 | a$ and $d_1 | a$, then $z | a$.

Interpret the entries in the first row of M^{-1} in terms of $\mathrm{lcm}(d_0, d_1)$.

Solution:

a) Each matrix $\begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}$ has determinant -1. Therefore $\det(M) = (-1)^k$, so M is regular. It follows that

$$M^{-1} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}^{-1} = (-1)^k \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix}$$

which clearly has integer entries. Using the above notation we have

$$\begin{pmatrix} 0 & 1 \\ 1 & q_l \end{pmatrix} \begin{pmatrix} d_{l+1} \\ d_l \end{pmatrix} = \begin{pmatrix} d_l \\ d_{l-1} \end{pmatrix}.$$

It follows that

$$\begin{aligned} M^{-1} \begin{pmatrix} d_1 \\ d_0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & q_{k-1} \end{pmatrix}^{-1} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}^{-1} \begin{pmatrix} d_1 \\ d_0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & q_{k-1} \end{pmatrix}^{-1} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}^{-1} \begin{pmatrix} d_2 \\ d_1 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ \gcd(d_0, d_1) \end{pmatrix}. \end{aligned}$$

b) Let $M^{-1} = \begin{pmatrix} p & l \\ m & n \end{pmatrix}$. So $md_1 + nd_0 = \gcd(d_0, d_1)$. Therefore m and n are the coefficients used to write $\gcd(d_0, d_1)$ as an integer linear combination of d_0 and d_1.

c) We have $pd_1 + ld_0 = 0$ so $pd_1 = -ld_0$. It follows that $d_0 | pd_1$ and $d_1 | pd_1$. Let $z = \mathrm{lcm}(d_0, d_1)$. Then z also divides pd_1, that is $pd_1 = rz$ for some r. Moreover $\det(M^{-1}) = \pm 1$, so p and l are relatively prime. Since $pd_1 = -ld_0 = rz$ and since $z = \mathrm{lcm}(d_0, d_1)$, it follows that r divides p and l. So $r = \pm 1$ and $|pd_1| = |ld_0| = \mathrm{lcm}(d_0, d_1)$. (See the OWO Lecture Notes from 2008/09.)

Exercise 4 (Polynomial factorisation and diagonalisation)

Consider the following polynomials in $\mathbb{F}[X]$ for $\mathbb{F} = \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$:

$$p_1 = X^3 - 2, \qquad p_2 = X^3 + 4X^2 + 2X, \qquad p_3 = X^3 - X^2 - 2X + 2.$$

(a) Which of these polynomials are irreducible in $\mathbb{F}[X]$?

(b) Which of these polynomials decompose into linear factors over $\mathbb{F}[X]$?

(c) Suppose p_i is the characteristic polynomial of a matrix $A_i \in \mathbb{F}^{(3,3)}$. Which of the A_i is diagonalisable over $\mathbb{F}$?

Solution:

Over the complex numbers these polynomials decompose as

$$\begin{aligned} p_1 &= (X - \sqrt[3]{2})(X - \sqrt[3]{2}\omega)(X - \sqrt[3]{2}\omega^2), \\ p_2 &= X(X + 2 + \sqrt{2})(X + 2 - \sqrt{2}), \\ p_3 &= (X - 1)(X + \sqrt{2})(X - \sqrt{2}), \end{aligned}$$

with $\omega = e^{\frac{2}{3}\pi i}$.

a) Since p_1 has no rational roots, it is irreducible over $\mathbb{Q}$, while p_2 and p_3 are not.

None of these polynomials is irreducible over $\mathbb{R}$ or $\mathbb{C}$ (every third degree polynomial is reducible over $\mathbb{R}$ and $\mathbb{C}$).

b) None of the above polynomials decompose into linear factors over $\mathbb{Q}$.

p_2 and p_3 decompose into linear factors over $\mathbb{R}$, while p_1 does not.

All polynomials in $\mathbb{C}[X]$ decompose into linear factors over $\mathbb{C}$, especially so do p_1, p_2 and p_3.

c) Applying Propositions 1.1.15 and 1.3.1, it follows that

1. the matrices A_i are diagonalisable over $\mathbb{C}$;
2. A_2 and A_3, but not A_1, are diagonalisable over $\mathbb{R}$;
3. none of the A_i are diagonalisable over $\mathbb{Q}$.