Department of Mathematics
Prof. Dr. Christian Herrmann
Dipl.-Math. Frederick Magata
Dr. Abdelhadi Es-Sarhir

TECHNISCHE
UNIVERSITÄT
DARMSTADT

11. Mai 2006

Linear Algebra II (MCS), SS 2006, Exercise 4

Groupwork

G 15 (i) Determine the polar representation, real and imaginary part of the follwing complex numbers:

$$1+i\,,\quad \sqrt{3}-i\,,\quad \frac{1+i}{1-i}\,,\quad \left(1+\sqrt{-3}\right)^2,\frac{(1-i)^3}{(1+i)^5}\,,\quad \sum_{k=1}^{17} i^k\,,\quad \left(\frac{24-7i}{20+15i}\right).$$

(ii) Show that for all $t \in \mathbb{R}$ we have $\left|\frac{1+it}{1-it}\right| = 1$.

(iii) Determine all roots of $z^3 = 2+2i$ and write them in the form $z = a+ib$ with $a, b \in \mathbb{R}$.

G 16 (i) Decompose the following polynomial into linear factors over $\mathbb{C}$, resp. into linear and quadratic factors over $\mathbb{R}$, by 'guessing' zeros and long division:

$$p = x^6 + 5x^4 + 3x^2 - 9.$$

(ii) Let $f = 2x^4 + x^3 + 4x^2 + 3x + 1$ and $g = x^2 + 1$. Find the unique polynomials q and r, such that $f = q \cdot g + r$ and $\deg(r) < \deg(g)$.

G 17 Let K be an arbitrary finite field. Give an example of a polynomial $p \in K[x]$ such that p is not uniquely determined by its polynomial function $x \mapsto p(x)$. What happens if K has infinitely many elements?

G 18 (i) Show that the set C_n of n-th roots of unity, i.e. the set of complex solutions of $z^n = 1$, form a multiplicative subgroup of $\mathbb{C} \setminus \{0\}$. Give an isomorphism of C_n onto $\mathbb{Z}_n$.

(ii) Divide $x^n - 1$ by $x - 1$ and conclude that $\sum_{\zeta \in C_n} \zeta = 0$.

Homework

H 9 Let $f = x^5 + (a+1)x^4 + (a+1)x^3 + (a-1)x^2 + (a^2-2)x + a - 2$ and $g = x^2 + x + 1$. Determine all values of a such that long division of f by g has remainder zero.

H 10 Let A be a $n \times n$ square matrix with integer coefficients and let $y = (y_1, \ldots, y_n)^t$ be a vector with integer entries. Show that $A \cdot x = y$ has a unique solution x with integer entries, if $\det(A) = \pm 1$.

H 11 Prove the second part of Theorem **29.4**, i.e. every real polynomial $p = a_n x^n + \cdots + a_1 x + a_0$ with $a_0, \ldots, a_n \in \mathbb{R}$, $a_n \neq 0$, $n \geq 1$ can, up to order, be uniquely decomposed as a product

$$p = a_n(x-\lambda_1) \cdot \ldots \cdot (x-\lambda_r) \cdot (x^2 + \alpha_1 x + \beta_1) \cdot \ldots \cdot (x^2 + \alpha_m x + \beta_m),$$

with $\lambda_1, \ldots, \lambda_r, \alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m \in \mathbb{R}$ and $\alpha_i^2 - 4\beta_i < 0$ for $i = 1, \ldots, m$. In particular, $n = 2m+r$ and every real polynomial of odd degree has a real zero.

(Hint: Use the first part of the fundamental theorem, induction over the degree of p and long division! If λ is a complex zero of p, what can one say about $\bar{\lambda}$? What kind of polynomial is $x^2 - (\lambda + \bar{\lambda})x + \lambda\bar{\lambda}$?)

H 12 Let K be a field and $x_0, \ldots, x_n, y_0, \ldots, y_n \in K$ with $x_i \neq x_j$ for all $i \neq j$. Show that there is one and only one polynomial $f \in K[x]$ of degree $\leq n$, such that $f(x_i) = y_i$ for $i = 0, \ldots, n$. Why is this statement not in contradiction to exercise **G 17**?

(Hint: Either construct polynomials $g_j \in K[x]$ of degree $\leq n$, such that

$$g_j(x_i) = \begin{cases} 1 & \text{for} \quad i = j \\ 0 & \text{for} \quad i \neq j \end{cases},$$

or, more systematically, formulate the problem as a system of linear equations $M \cdot a = y$, with $a = (a_0, \ldots, a_n)^t$ as the coefficients of the desired polynomial f and $y = (y_0, \ldots, y_n)^t$. What is the matrix M? How can you solve this system of linear equations?

Linear Algebra II (MCS), SS 2006, Exercise 4, Solution

Groupwork

G 15 (i) Determine the polar representation, real and imaginary part of the follwing complex numbers:

$$1+i\,,\quad \sqrt{3}-i\,,\quad \frac{1+i}{1-i}\,,\quad \left(1+\sqrt{-3}\right)^2,\frac{(1-i)^3}{(1+i)^5}\,,\quad \sum_{k=1}^{17} i^k\,,\quad \left(\frac{24-7i}{20+15i}\right).$$

(ii) Show that for all $t \in \mathbb{R}$ we have $\left|\frac{1+it}{1-it}\right| = 1$.

(iii) Determine all roots of $z^3 = 2+2i$ and write them in the form $z = a+ib$ with $a, b \in \mathbb{R}$.

(i) $1+i = \sqrt{2}\cdot e^{i\pi/4}$, $\sqrt{3}-i = 2\cdot e^{i\pi/6}$, $\frac{1+i}{1-i} = i = e^{i\pi/2}$, $\left(1+\sqrt{-3}\right)^2 = 4\cdot e^{i2\pi/3}$, $\frac{(1-i)^3}{(1+i)^5} = \frac{1}{2}$, $\sum_{k=1}^{17} i^k = 1+i$, $\left(\frac{24-7i}{20+15i}\right) = 3/5 - 4/5i = e^{i\arccos(3/5)}$

(ii) $\frac{1+it}{1-it} = \frac{(1+it)^2}{1+t^2} = \frac{1-t^2+2it}{1+t^2}$, *thus* $\left|\frac{1+it}{1-it}\right|^2 = \frac{(1-t^2)^2+4t^2}{(1+t^2)^2} = \frac{(1+t^2)^2}{(1+t^2)^2} = 1$.

(iii) $2+2i = \sqrt{8}\cdot e^{i\pi/4}$ *and therefore one solution of* $z^3 = 2+2i$ *is* $\xi := \sqrt{2}\cdot e^{i\pi/12}$ *the other solutions can be obtained by multiplying* ξ *with the third roots of unity* $\zeta_3^k = e^{2\pi ik/3}$, $k = 1,2,3$. *Hence,* $\xi_k = \sqrt{2}\cdot e^{\pi i(8k+1)/12} = \sqrt{2}\cos(\pi(8k+1)/12) + \sqrt{2}\sin(\pi(8k+1)/12)i$, $k = 1,2,3$ *are the roots.*

G 16 (i) Decompose the following polynomial into linear factors over $\mathbb{C}$, resp. into linear and quadratic factors over $\mathbb{R}$, by 'guessing' zeros and long division:

$$p = x^6 + 5x^4 + 3x^2 - 9.$$

(ii) Let $f = 2x^4 + x^3 + 4x^2 + 3x + 1$ and $g = x^2 + 1$. Find the unique polynomials q and r, such that $f = q\cdot g + r$ and $\deg(r) < \deg(g)$.

(i) By guessing, we see that 1 *and* -1 *are zeros and long division by* x^2-1 *yields* $p = (x^4+6x^2+9)(x^2-1)$. *The term* $x^4+6x^2+9 = (x^2+3)^2$ *is a bi-square. Thus the decomposition over the reals is* $p = (x^2+3)^2(x+1)(x-1)$. *Over* $\mathbb{C}$, *the factor* x^2+3 *can be further decomposed into* $x^2+3 = (x-\sqrt{3}i)(x+\sqrt{3}i)$ *and therefore* $p = (x-\sqrt{3}i)^2(x+\sqrt{3}i)^2(x+1)(x-1)$.

(ii) $q = 2x^2 + x + 2$ *and* $r = 2x - 1$.

G 17 Let K be an arbitrary finite field. Give an example of a polynomial $p \in K[x]$ such that p is not uniquely determined by its polynomial function $x \mapsto p(x)$. What happens if K has infinitely many elements?

Let $K = \{a_1, \ldots, a_n\}$ *and* $p = (x-a_1)\cdot\ldots\cdot(x-a_n)$. *Then* $p(x) = 0$ *for all* $x \in K$, *but* p *is not the zero polynomial. If* K *has infinitely many elements, then Corollary 30.7 tells us that every polynomial is uniquely determined by its associated polynomial function.*

G 18 (i) Show that the set C_n of n-th roots of unity, i.e. the set of complex solutions of $z^n = 1$, form a multiplicative subgroup of $\mathbb{C}\setminus\{0\}$. Give an isomorphism of C_n onto $\mathbb{Z}_n$.

(ii) Divide $x^n - 1$ by $x - 1$ and conclude that $\sum_{\zeta\in C_n}\zeta = 0$.

(i) Clearly, $1^n - 1 = 0$ *so* $1 \in \mathbb{C}_n$. *Furthermore, let* $a, b \in C_n$ *be arbitrary. Then* $(ab^{-1})^n - 1 = \frac{a^n}{b^n} - 1 = \frac{1}{1} - 1 = 0$. *Hence,* C_n *is indeed a multiplicative subgroup of* $\mathbb{C}\setminus\{0\}$.

(ii) $x^n - 1 : x - 1 = \sum_{k=0}^{n-1} x^k$ *(telescope sum). By (i),* C_n *is generated by some element* ξ. *I.e.* ξ^k *ranges through all elements of* C_n *as* $k = 0, \ldots, n-1$. *Since* $\xi \neq 1$, *it necessarily annihilates the factor* $\sum_{k=0}^{n-1} x^k$ *of* $x^n - 1$. *Hence,* $\sum_{\zeta\in C_n}\zeta = \sum_{k=0}^{n-1}\xi^k = 0$.

Homework

H 9 Let $f = x^5 + (a+1)x^4 + (a+1)x^3 + (a-1)x^2 + (a^2-2)x + a - 2$ and $g = x^2 + x + 1$. Determine all values of a such that long division of f by g has remainder zero.

$f = q \cdot g + r$ with $q = x^3 + ax^2 - 1$ and $r = (a^2-1)x + (a-1)$. We have $r = 0$ if and only if $a = 1$.

H 10 Let A be a $n \times n$ square matrix with integer coefficients and let $y = (y_1, \ldots, y_n)^t$ be a vector with integer entries. Show that $A \cdot x = y$ has a unique solution x with integer entries, if $\det(A) = \pm 1$.

Using Cramers rule, we have the unique solution $x = (x_1, \ldots, x_n)^t$ with $x_i = \frac{\det(A_i)}{\det(A)} = \pm \det A_i$, $i = 1, \ldots, n$, where A_i is the matrix obtained from A by replacing its i-th column by y.

H 11 Prove the second part of Theorem **29.4**, i.e. every real polynomial $p = a_n x^n + \cdots + a_1 x + a_0$ with $a_0, \ldots, a_n \in \mathbb{R}$, $a_n \neq 0$, $n \geq 1$ can, up to order, be uniquely decomposed as a product

$$p = a_n(x - \lambda_1) \cdot \ldots \cdot (x - \lambda_r) \cdot (x^2 + \alpha_1 x + \beta_1) \cdot \ldots \cdot (x^2 + \alpha_m x + \beta_m),$$

with $\lambda_1, \ldots, \lambda_r, \alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m \in \mathbb{R}$ and $\alpha_i^2 - 4\beta_i < 0$ for $i = 1, \ldots, m$. In particular, $n = 2m + r$ and every real polynomial of odd degree has a real zero.

(Hint: Use the first part of the fundamental theorem, induction over the degree of p and long division! If λ is a complex zero of p, what can one say about $\bar{\lambda}$? What kind of polynomial is $x^2 - (\lambda + \bar{\lambda})x + \lambda\bar{\lambda}$?)

The uniqueness being clear, we show the existence of the stated decomposition by induction over the degree n of p. If $\deg(p) = n = 1$ then $p = a_1 x + a_0 = a_1(x - (-\frac{a_0}{a_1}))$ and $\lambda_1 = -\frac{a_0}{a_1}$ is the unique real zero of p. If $\deg(p) = n = 2$, then one argues similarly, that p posseses either two real zeros or has no real zero and is therefore of the form $a_2 \cdot (x^2 + \alpha x + \beta)$ with discriminant $\alpha^2 - 4\beta < 0$.

For $n \to n+1$, let λ be a (probably) complex zero of p. If λ is real, then $p : (x - \lambda)$ is a real polynomial of degree n which, by induction hypothesis, admits a unique factorization as stated. We conclude that p has such a factorization as well. If λ is not real, then $p(\bar{\lambda}) = \overline{p(\lambda)} = 0$, since p has real coefficients. Therefore $\bar{\lambda}$ is another zero of p, distinguished from λ. Forming $g = (x-\lambda)(x-\bar{\lambda}) = x^2 - (\lambda+\bar{\lambda})x + \lambda\bar{\lambda}$ yields a real polynomial (because $\lambda + \bar{\lambda} = 2\Re(\lambda)$ and $\lambda\bar{\lambda} = |\lambda|^2$) which divides p. Applying the induction hypothesis on the real polynomial $p : g$ of degree $n - 1$, we obtain a unique factorization as stated. Observe that $(\lambda + \bar{\lambda})^2 - 4\lambda\bar{\lambda} = (\lambda - \bar{\lambda})^2 = -\Im(\lambda)^2 < 0$. Hence, g is a quadratic factor as in the statement and p admits the desired factorization.

H 12 Let K be a field and $x_0, \ldots, x_n, y_0, \ldots, y_n \in K$ with $x_i \neq x_j$ for all $i \neq j$. Show that there is one and only one polynomial $f \in K[x]$ of degree $\leq n$, such that $f(x_i) = y_i$ for $i = 0, \ldots, n$. Why is this statement not in contradiction to exercise **G 17**?

(Hint: Either construct polynomials $g_j \in K[x]$ of degree $\leq n$, such that

$$g_j(x_i) = \begin{cases} 1 & \text{for} \quad i = j \\ 0 & \text{for} \quad i \neq j \end{cases},$$

or, more systematically, formulate the problem as a system of linear equations $M \cdot a = y$, with $a = (a_0, \ldots, a_n)^t$ as the coefficients of the desired polynomial f and $y = (y_0, \ldots, y_n)^t$. What is the matrix M? How can you solve this system of linear equations?

Either put $g_j(x) := \frac{\prod_{j \neq i=0}^n (x - x_i)}{\prod_{j \neq i=0}^n (x_j - x_i)}$, then $f = \sum_{j=0}^n y_j \cdot g_j$. Or alternatively we make the following Ansatz to determine the coefficients of the desired $f = \sum_{i=0}^n a_i x^i$. Consider the following system of linear equations:

$$\begin{aligned} f(x_0) = \sum_{i=0}^n a_i x_0^i &= y_0 \\ \vdots &= \vdots \\ f(x_n) = \sum_{i=0}^n a_i x_n^i &= y_n, \end{aligned}$$

which has the matrix form $M \cdot a = y$ *with* $M = \begin{pmatrix} 1 & x_0 & \dots & x_0^n \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \dots & x_0^n \end{pmatrix}$ *and* a *and* y *as indicated in the hint. According to exercise* **H7**, $\det(M) = \prod_{0 \leq i < j \leq n} (x_j - x_i)$ *is a Vandermonde determinant. By assumption, it is not zero and we may compute coefficients* $a_0, \dots, a_n$ *by Cramers rule, such that the associated polynomial* f *has the desired properties. Furthermore, if* $\tilde{f}$ *is another polynomial which satisfies the same conditions as* f *and has degree* $\leq n$*, then its coefficients must coincide by uniqueness of the solution of* $M \cdot a = y$ *with these of* f*. Hence* $f = \tilde{f}$*. The statement does not contradict* ***G 17****, since every polynomial constructed there has degree* $> n$.