

**E0 219 Linear Algebra and Applications / August-December 2016**

(ME, MSc. Ph. D. Programmes)

Download from : [http://www.math.iisc.ernet.in/patil/courses/courses/Current Courses/...](http://www.math.iisc.ernet.in/patil/courses/courses/Current%20Courses/...)

Tel : +91-(0)80-2293 2239/(Maths Dept. 3212)

E-mails : [dppatil@csa.iisc.ernet.in](mailto:dppatil@csa.iisc.ernet.in) / [patil@math.iisc.ernet.in](mailto:patil@math.iisc.ernet.in)

Lectures : Monday and Wednesday ; 11:00–12:30

Venue: CSA, Lecture Hall (Room No. 117)

Corrections by : Nikhil Gupta ([nikhil.gupta@csa.iisc.ernet.in](mailto:nikhil.gupta@csa.iisc.ernet.in); Lab No.: 303) /  
 Vineet Nair ([vineetn90@gmail.com](mailto:vineetn90@gmail.com); Lab No.: 303) /  
 Rahul Gupta ([rahul.gupta@csa.iisc.ernet.in](mailto:rahul.gupta@csa.iisc.ernet.in); Lab No.: 224) /  
 Sayantan Mukherjee ([meghanamande@gmail.com](mailto:meghanamande@gmail.com); Lab No.: 253) /  
 Palash Dey ([palash@csa.iisc.ernet.in](mailto:palash@csa.iisc.ernet.in); Lab No.: 301, 333, 335)

Midterms : 1-st Midterm : Saturday, September 17, 2016; 15:00–17:00

2-nd Midterm : Saturday, October 22, 2016; 15:00–17:00

Final Examination : December ??, 2016, 09:00–12:00

Evaluation Weightage : Assignments : 20%

Midterms (Two) : 30%

Final Examination : 50%

Range of Marks for Grades (Total 100 Marks)							
Marks-Range	Grade S	Grade A	Grade B	Grade C	Grade D	Grade E	Grade F
	> 90	76–90	61–75	46–60	35–45	< 35	
Marks-Range	Grade A <sup>+</sup>	Grade A	Grade B <sup>+</sup>	Grade B	Grade C	Grade D	Grade F
	> 90	81–90	71–80	61–70	51–60	40–50	< 40

**Supplement 6****Linear Maps and Bases; — The Rank Theorem**

To understand and appreciate the Supplements which are marked with the symbol † one may possibly require more mathematical maturity than one may have! These are steps towards applications to various other branches of mathematics, especially to analysis, number theory and Affine and Projective Geometry.

**Participants may ignore these Supplements — altogether or in the first reading!!**

**S6.1** Determine whether there are  $\mathbb{R}$ -linear maps with the following properties :

(a)  $f: \mathbb{R}^3 \rightarrow \mathbb{R}^2$ ;  $f(1, 0, 1) = (1, 0)$ ,  $f(0, 1, 0) = (0, 1)$ .

(b)  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ ;  $f(1, 2) = (1, 0, 0)$ ,  $f(2, 1) = (0, 1, 0)$ ,  $f(-1, 4) = (0, 0, 1)$ .

(c)  $f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ ;  $f(1, 2) = (1, 0, 0)$ ,  $f(2, 1) = (0, 1, 0)$ ,  $f(-1, 4) = (3, -2, 0)$ .

**S6.2** Show that the vectors  $x_1 := (1, 2, 1)$ ,  $x_2 := (2, 1, 1)$ ,  $x_3 := (1, 1, 1)$  form a basis of  $\mathbb{R}^3$ . For the linear map  $f: \mathbb{R}^3 \rightarrow \mathbb{R}^3$  defined by  $f(x_1) := (1, 0, 3)$ ,  $f(x_2) := (-1, 3, 2)$ ,  $f(x_3) := (0, -1, 1)$  write the image of the vectors  $(2, -1, 5)$ ,  $(-1, 0, 1)$ ,  $(0, 1, 0)$  and further compute a basis of  $\text{Ker } f$  and  $\text{Im } f$ .

**S6.3** Let  $V$  be a finite dimensional  $K$ -vector space and let  $U, W$  be subspaces of  $V$  of equal dimension. Then there exists a  $K$ -automorphism  $f$  of  $V$  such that  $f(U) = W$ .

**S6.4** Let  $V$  be a finite dimensional  $K$ -vector space and let  $f: V \rightarrow V$  be an endomorphism of  $V$ . Show that the following statements are equivalent :

(i)  $f$  is not an automorphism of  $V$ .

(ii) There exists a  $K$ -endomorphism  $g \neq 0$  of  $V$  such that  $g \circ f = 0$ .

(ii') There exists an  $K$ -endomorphism  $g' \neq \text{id}_V$  of  $V$  such that  $g' \circ f = f$ .

(iii) There exists an  $K$ -endomorphism  $h \neq 0$  of  $V$  such that  $f \circ h = 0$ .

(iii') There exists an  $K$ -endomorphism  $h' \neq \text{id}_V$  of  $V$  such that  $f \circ h' = f$ .

**S6.5** Let  $f: V \rightarrow W$  be a homomorphism of finite dimensional  $K$ -vector spaces.

(a) Show that  $f$  injective if and only if there exists a homomorphism  $g: W \rightarrow V$  such that  $g \circ f = \text{id}_V$ .

(b) Show that  $f$  surjective if and only if there exists a homomorphism  $h: W \rightarrow V$  such that  $f \circ h = \text{id}_W$ . (**Remark** : These assertions are also true for arbitrary infinite dimensional vector spaces  $V$  and  $W$ , since for arbitrary vector space there are sufficiently many bases exist!)

**S6.6** Let  $D$  be an arbitrary set and let  $f_1, \dots, f_n \in K^D$  be linearly independent  $K$ -valued functions on the set  $D$ . Further, let  $t_1, \dots, t_n$  be pairwise distinct points in  $D$  and let  $V$  be the subspace

of  $K^D$  ( $n$ -dimensional) generated by  $f_1, \dots, f_n$ . Show that for every choice of  $b_1, \dots, b_n \in K$  the interpolation problem

$$f(t_1) = b_1, \dots, f(t_n) = b_n$$

has a solution  $f \in V$  if and only if the trivial problem

$$f(t_1) = \dots = f(t_n) = 0.$$

has only trivial (the zero function) solution in  $V$ .

**S6.7** Let  $V$  be a  $K$ -vector space of countable infinite dimension. Then  $V$  and the direct sum  $V \oplus V$  are isomorphic. (**Remark** : This is also true for arbitrary infinite dimensional vector spaces  $V$ .)

**S6.8** Give an example of an endomorphism of a vector space (necessarily infinite dimensional) which is injective, but not surjective (respectively, surjective, but not injective).

**S6.9** Let  $A$  be a finite dimensional  $K$ -algebra and let  $x \in A$ . Let  $\lambda_x$  (respectively,  $\rho_x$ ) denote the left- (respectively, right-)multiplication  $y \mapsto xy$  (respectively,  $y \mapsto yx$ ) by  $x$  in  $A$ . Show that  $\lambda_x$  and  $\rho_x$  are  $K$ -endomorphisms of the  $K$ -vector space  $A$  (but for  $x \neq 1$  are not  $K$ -algebra-endomorphisms). Further, show that the following statements are equivalent: (i)  $x$  is invertible in  $A$ . (ii)  $\lambda_x$  is bijective. (ii')  $\rho_x$  is bijective. (iii)  $\lambda_x$  is injective. (iii')  $\rho_x$  is injective. (iv)  $\lambda_x$  is surjective. (iv')  $\rho_x$  is surjective. (**Remark** : See also Supplement S5.18. The equivalence of (i), (ii) and (ii') also hold for arbitrary  $K$ -algebra  $A$ .)

**S6.10** Let  $A$  be a finite dimensional  $K$ -algebra. If the element  $x \in A$  is invertible in  $A$ , then show that the inverse  $x^{-1}$  already belong to the  $K$ -subalgebra  $K[x]$ .

**S6.11** Let  $A$  be a finite dimensional  $K$ -algebra.

(a) Show that the following statements are equivalent: (i)  $A$  is a division-algebra (ii) For every  $x \in A$ ,  $x \neq 0$ , the left-multiplication  $\lambda_x$  injective, i. e. the left-cancelation rule: from  $xy = xz$  and  $x \neq 0$ , it follows that  $y = z$ . (ii') For every  $x \in A$ ,  $x \neq 0$ , the right-multiplication  $\rho_x$  injective, i. e. the right-cancelation rule: from  $yx = zx$  and  $x \neq 0$ , it follows that  $y = z$ .

(b) If  $A$  is a division-algebra, then every  $K$ -subalgebra of  $A$  is also a division-algebra. (**Hint** : Use the part (a) or Supplement S6.10.)

It is strongly recommended to read and understand the Supplement S6.12. The (complete) solution is provided by using the two basic theorems (stated in Footnote 1 and Footnote 2) in the context of fourier transformations. This problem is important not only for its own sake but also for applications to Physics, Chemistry and Engineering, Signal-Processing and Information Theory, since many data obtained by Spectroscopy, X-ray analysis and the like, are nothing other than Fourier coefficients of functions which one wishes to determine. The simplest way to try to recapture  $f$  by means of the Fourier series of  $f$ .

<sup>†</sup>**S6.12** Let  $\eta$  be a positive real number and let  $V_\eta$  be the  $\mathbb{C}$ -subspace (of the  $\mathbb{C}$ -vector space  $\mathbb{C}^{\mathbb{R}}$  of all functions  $\mathbb{R} \rightarrow \mathbb{C}$ ) generated by the functions  $e^{i\omega t}$ ,  $\omega \in (-\eta, \eta)$ .

(a) The given family of functions form a  $\mathbb{C}$ -basis of  $V_\eta$ . Further, show that the (real-valued) functions  $1, \sin \omega t, \cos \omega t$ ,  $\omega \in (0, \eta)$  also form a  $\mathbb{C}$ -basis of  $V_\eta$ . In particular, the real-valued functions in  $V_\eta$  are precisely the (finite) sums of constant real-functions and of harmonic oscillations with angular frequency  $< \eta$ . (**Proof**: Since  $V_\eta$  is generated (over  $\mathbb{C}$ ) by  $e^{i\omega t}$ ,  $\omega \in (-\eta, \eta)$ , it is enough to prove that they are linearly independent over  $\mathbb{C}$ . For this we need to show that the functions  $e^{i\omega_j t}$ ,  $j = 1, \dots, n \in \mathbb{N}^+$ , are linearly independent over  $\mathbb{C}$  for all pairwise distinct  $\omega_1, \dots, \omega_n \in (-\eta, \eta)$ . We shall prove this by induction on  $n$ . The case  $n = 1$  is trivial. Now, suppose that  $\sum_{j=1}^n a_j e^{i\omega_j t} = 0$  for  $a_1, \dots, a_n \in \mathbb{C}$  and all  $t \in \mathbb{R}$ . Then  $i\omega_n \cdot \sum_{j=1}^n a_j e^{i\omega_j t} = \sum_{j=1}^n i\omega_n \cdot a_j e^{i\omega_j t} = 0$ , on the other hand by differentiating we get  $\sum_{j=1}^n i\omega_j a_j e^{i\omega_j t} = 0$  and hence  $\sum_{j=1}^{n-1} i(\omega_n - \omega_j) \cdot a_j e^{i\omega_j t} = 0$ . Now, since by induction hypothesis, the functions  $e^{i\omega_j t}$ ,  $j = 1, \dots, n-1$  are linearly independent over  $\mathbb{C}$ , it follows that  $i(\omega_n - \omega_j) \cdot a_j = 0$ , and hence  $a_j = 0$ , since  $\omega_n \neq \omega_j$  for all  $j = 1, \dots, n-1$ . Finally, by the case  $n = 1$ ,  $a_n = 0$ .

Since  $e^{i\omega t} = \cos \omega t + i \sin \omega t$ , it follows that the functions  $1, \sin \omega t, \cos \omega t$ ,  $\omega \in (0, \eta)$  also form a generating system for the  $\mathbb{C}$ -vector space  $V_\eta$ . Moreover, they are also linearly independent over  $\mathbb{C}$ : from  $a_0 + \sum_{\omega \in (0, \eta)} (a_\omega \cos \omega t + b_\omega \sin \omega t) = 0$  for all  $t \in \mathbb{R}$  and  $a_0, a_\omega, b_\omega \in \mathbb{C}$ , by replacing  $t$  by  $-t$  it follows

that  $a_0 + \sum_{\omega \in (0, \eta)} (a_\omega \cos \omega t - b_\omega \sin \omega t) = 0$ . Subtracting these equations we get  $0 = \sum_{\omega \in (0, \eta)} 2b_\omega \sin \omega t = -i \sum_{\omega \in (0, \eta)} b_\omega (e^{i\omega t} - e^{i(-\omega)t})$  and hence  $b_\omega = 0$  for all  $\omega$ , since we have already show that the functions  $e^{i\omega t}$ ,  $\omega \in (-\eta, \eta)$  are linearly independent over  $\mathbb{C}$ . Finally, by adding the above two equations conclude that  $a_0 + \sum_{\omega \in (0, \eta)} 2a_\omega (e^{i\omega t} + e^{i(-\omega)t})$  and hence  $a_\omega = 0$  for all  $\omega$ .)

(b) The  $\mathbb{C}$ -linear map  $F : V_\eta \rightarrow \mathbb{C}^{\mathbb{N}}$  defined by  $f \mapsto (f(n\pi/\eta))_{n \in \mathbb{N}}$  is injective. (Proof: The  $\mathbb{C}$ -linearity of the map  $F$  is clear by definitions. Consider  $f \in \text{Ker } F$ . By part (a) we know that  $f$  is a (finite) linear combination  $f = \sum_{\omega \in (-\eta, \eta)} a_\omega e^{i\omega t}$ . Since  $f \in \text{Ker } F$ , we have  $f(n\pi/\eta) = 0$  for all  $n \in \mathbb{N}$ . Putting

$\lambda_\omega := e^{i\omega\pi/\eta}$ , we get  $\sum_{\omega \in (-\eta, \eta)} a_\omega \lambda_\omega^n = \sum_{\omega \in (-\eta, \eta)} a_\omega e^{in\omega\pi/\eta} = 0$  for all  $n \in \mathbb{N}$ . From  $-\pi < \omega\pi/\eta < \pi$ , it

follows that the  $\lambda_\omega$  are pairwise distinct. Now Exercise 3.4-(b) shows that  $a_\omega = 0$  for all  $\omega$ , i. e.  $f = 0$ . Therefore we have  $\text{Ker } F = 0$  and hence  $F$  is injective. — **Remarks:** A linear combination  $f$  of harmonic oscillations with angular frequencies  $< \eta$ , i. e. frequencies  $\nu := \eta/2\pi$ , is uniquely determined by its values  $f(n/2\nu)$ ,  $n \in \mathbb{N}$ , measured at times differing by  $1/2\nu$ , i. e. measured with frequency  $2\nu$ . This statement (proved above) is part of the *Sampling Theorem* from signal processing, which can be (rigorously) fully treated in the context of Fourier transformations. The interpolation problem, to reconstruct the function  $f$  from its values  $a_n := f(n/2\nu)$ , measured with frequency  $2\nu$ , arises from this in a natural way. It is solved by the so-called (Whittaker-) Shannon interpolation formula:

$$f(t) = a_0 \text{sinc} \frac{\eta t}{\pi} + \sum_{n=1}^{\infty} \left( a_n \text{sinc} \left( \frac{\eta t}{\pi} - n \right) + a_{-n} \text{sinc} \left( \frac{\eta t}{\pi} + n \right) \right)$$

using the function  $\text{sinc } t := \frac{\sin \pi t}{\pi t}$ . Since this formula is linear in  $f$ , it is enough to prove it in the special case  $f(t) = e^{i\omega t}$ ,  $|\omega| < \eta$ , i. e. to show the equality

(6.5.c) 
$$e^{i\omega t} = \text{sinc} \frac{\eta t}{\pi} + \sum_{n=1}^{\infty} \left( e^{i\pi n\omega/\eta} \text{sinc} \left( \frac{\eta t}{\pi} - n \right) + e^{-i\pi n\omega/\eta} \text{sinc} \left( \frac{\eta t}{\pi} + n \right) \right)$$

for  $|\omega| < \eta$  and all  $t \in \mathbb{R}$ . — **Proof:** We use the formulas from the theorem<sup>1</sup> to compute the complex-Fourier coefficients  $c_n$  of a function  $x(t) := e^{zt}$  for a fixed  $z \in \mathbb{C} \setminus \mathbb{Z}2\pi i$  with respect to the interval  $(-\eta, \eta)$  and get

$$c_n = \frac{1}{2\eta} \int_{-\eta}^{\eta} e^{zt} e^{-(\pi/\eta)int} dt = \frac{1}{2\eta} \int_{-\eta}^{\eta} e^{(z\eta - \pi in)t/\eta} dt = \frac{1}{2\eta} \frac{\eta}{z\eta - \pi in} e^{(z\eta - \pi in)t/\eta} \Big|_{t=-\eta}^{t=\eta} = \frac{1}{\pi n + iz\eta} \frac{-1}{2i} \left( e^{(z\eta - \pi in)} - e^{-(z\eta - \pi in)} \right) = \frac{1}{\pi n + iz\eta} \frac{1}{2i} \left( e^{i(iz\eta + \pi n)} - e^{-i(iz\eta + \pi n)} \right) = \frac{\text{sinc}(iz\eta + n\pi)}{iz\eta + n\pi} = \text{sinc} \left( \frac{iz\eta}{\pi} + n \right).$$

Now the theorem<sup>2</sup> gives (with absolute and uniform convergence in  $t \in (-\eta, \eta)$ )

$$e^{zt} = \sum_{n=-\infty}^{\infty} \text{sinc} \left( \frac{iz\eta}{\pi} + n \right) e^{i\pi nt/\eta}.$$

Replacing first  $t$  by  $\omega$  and then by  $z$  by  $it$ , we obtain (using  $\text{sinc}(-\omega) = \text{sinc}(\omega)$ ) the equality in (6.5.c). •

For the values  $a_{m+\frac{1}{2}} := f\left(\frac{(2m+1)\pi}{2\eta}\right)$ ,  $m \in \mathbb{Z}$ , of  $f$  in the middle between two neighbouring scan points one gets the interpolation formula

$$a_{m+\frac{1}{2}} = \sum_{k=0}^{\infty} \frac{2(-1)^k}{(2k+1)\pi} (a_{m-k} + a_{m+k+1}) = \frac{2}{\pi} (a_m + a_{m+1}) - \frac{2}{3\pi} (a_{m-1} + a_{m+2}) + \frac{2}{5\pi} (a_{m-2} + a_{m+3}) - \dots,$$

with the weights  $2/\pi, 2/\pi, -2/3\pi, -2/3\pi, 2/5\pi, 2/5\pi, \dots$ , occurring in the Leibniz-series

$$\sum_{k=0}^{\infty} \left( \frac{2(-1)^k}{(2k+1)\pi} + \frac{2(-1)^k}{(2k+1)\pi} \right) = 1 \quad (\text{note that this series converges very slowly}).$$

<sup>1</sup>**Theorem** For every piece-wise continuous function  $x : [a, b] \rightarrow \mathbb{C}$ , there is (in mean square convergence) the Fourier-expansion  $x = \sum_{n \in \mathbb{Z}} c_n \exp\left(\frac{2\pi i}{\ell} n(t-c)\right)$  and  $x = \frac{a_0}{2} + \sum_{n=1}^{\infty} \left( a_n \cos \frac{2\pi}{\ell} n(t-c) + b_n \sin \frac{2\pi}{\ell} n(t-c) \right)$ ,  $\ell := b-a$ , with the Fourier-coefficients  $a_n := \frac{2}{\ell} \int_a^b x(t) \cos \frac{2\pi}{\ell} n(t-c) dt$ ,  $n \in \mathbb{N}$ ,  $b_n := \frac{2}{\ell} \int_a^b x(t) \sin \frac{2\pi}{\ell} n(t-c) dt$ ,  $n \in \mathbb{N}^*$ ,  $c_n := \frac{1}{\ell} \int_a^b x(t) \exp\left(-\frac{2\pi i}{\ell} n(t-c)\right) dt$ ,  $n \in \mathbb{Z}$ .

<sup>2</sup>**Theorem** Let  $x : \mathbb{R} \rightarrow \mathbb{C}$  be a continuous, piece-wise continuously differentiable and periodic function with period 1. Then the Fourier-series of  $x$  normally converges on  $\mathbb{R}$  and in particular, converges absolutely and uniformly to the function  $x$ .

Starting from the premise that the human ear apprehends only frequencies below 20 kHz, the result of this exercise suggests for digital sound recording to determine the amplitude of a sound wave about  $2\nu (= 40000)$ -times a second. For the recording of usual CD audio discs the amplitude is measured 44100-times a second (for the sound of DAT it is 48000 and for DVD-audio 96000) and each value is digitalized with 16 bit = 2 Byte, (according to the Sony red book, Philips uses 14 bytes and over sampling) i.e. with a 0-1-sequence of length 16. Therefore, in order to record one hour of stereo music with two channels, a disc space of

$$2 \cdot 2 \cdot 44100 \cdot 3600 \approx 6.35 \cdot 10^8 \text{ Byte} \approx 600 \text{ Megabyte}$$

(1 Megabyte = 210 Kilobyte (K) =  $2^{20}$  Byte) is needed. (Actually, storage densities for audio CDs and for data CDs differ) For error correction and for information management even more disc space has to be provided. In order to enhance sound reproduction, usually intermediate values are interpolated (This is called **Oversampling**.)

**S6.13** Let  $V$  be a  $K$ -vector space with basis  $x_i, i \in I$  and let  $f: V \rightarrow K$  be a linear form  $\neq 0$  on  $V$  with  $f(x_i) = a_i \in K, i \in I$ . Find a basis of  $\text{Ker } f$ .

**S6.14** Let  $f$  and  $g$  be endomorphisms of the finite dimensional  $K$ -vector space  $V$  with  $g \circ f = 0$ . Then  $\text{Rank } f + \text{Rank } g \leq \text{Dim}_K V$ . In particular, if  $f^2 (= f \circ f) = 0$ , then  $\text{Rank } f \leq \frac{1}{2} \text{Dim}_K V$ .

**S6.15** Let  $g: V \rightarrow W$  be  $K$ -linear and let  $V'$  be a subspace of  $V$ . If  $V$  is finite dimensional, then

$$\text{Dim}_K V - \text{Dim}_K V' \geq \text{Rank } g - \text{Rank } (g|_{V'}).$$

**S6.16** Let  $f$  be an operator on the finite dimensional  $K$ -vector space  $V$  of odd dimension. Then  $\text{Im } f \neq \text{Ker } f$ .

**S6.17** (Inequality of Sylvester) Let  $f: U \rightarrow V$  and let  $g: V \rightarrow W$  be linear maps. If  $U$  and  $V$  are finite dimensional, then

$$\text{Rank } f + \text{Rank } g - \text{Dim } V \leq \text{Rank } (gf) \leq \text{Min}(\text{Rank } f, \text{Rank } g).$$

(**Hint** :  $\text{Rank } (gf) = \text{Rank } f - \text{Dim}_K (\text{Im } f \cap \text{Ker } g)$ .)

**S6.18** (Inequality of Frobenius) Let  $f: U \rightarrow V, g: V \rightarrow W$  and let  $h: W \rightarrow X$  be  $K$ -linear maps. If  $U, V$  and  $W$  are finite dimensional, then

$$\text{Rank } (hg) + \text{Rank } (gf) \leq \text{Rank } g + \text{Rank } (hgf).$$

(**Hint** : We may assume that  $g$  is surjective and apply the inequality of Sylvester, See Supplement S6.17.)

**S6.19** Let  $f: V \rightarrow W$  be a homomorphism of  $K$ -vector spaces. Show that  $\text{Ker } f$  is finite dimensional if and only if there exists a homomorphism of  $K$ -vector space  $g: W \rightarrow V$  and an operator  $h: V \rightarrow V$  on  $V$  such that  $\text{Rank } h$  is finite and  $gf = h + \text{id}_V$ .

**S6.20** Let  $f$  be an operator on the finite dimensional  $K$ -vector space  $V$ . Show that the following statements are equivalent:

- (i)  $\text{Rank } f = \text{Rank } f^2$ .      (i')  $\text{Im } f = \text{Im } f^2$ .      (ii)  $\text{Dim}_K \text{Ker } f = \text{Dim}_K \text{Ker } f^2$ .  
(ii')  $\text{Ker } f = \text{Ker } f^2$ .      (iii)  $\text{Im } f \cap \text{Ker } f = 0$ .      (iv)  $\text{Im } f + \text{Ker } f = V$ .

(**Remark** : (iii) and (iv) together mean that  $V$  is the direct sum of  $\text{Im } f$  and  $\text{Ker } f$ .)

**S6.21** Let  $f_1, \dots, f_r \in \text{Hom}_K(V, W)$  be  $K$ -vector space homomorphisms of finite rank. For arbitrary  $a_1, \dots, a_r \in K$ , show that the rank of  $a_1 f_1 + \dots + a_r f_r$  is finite and

$$\text{Rank } (a_1 f_1 + \dots + a_r f_r) \leq \text{Rank } f_1 + \dots + \text{Rank } f_r.$$

(**Remark** : From this supplement it follows that the subset  $E := \{f \in \text{Hom}_K(V, W) \mid \text{Rank } f \text{ is finite}\}$  is a  $K$ -subspace of  $\text{Hom}_K(V, W)$  and that the subset  $\mathfrak{A} := \{f \in \text{End}_K V \mid \text{Rank } f \text{ is finite}\}$  is a two-sided ideal in the  $K$ -algebra  $\text{End}_K V$ .)

**S6.22** Let  $f: U \rightarrow V$  and let  $g: V \rightarrow W$  be homomorphisms of  $K$ -vector spaces. If one of these homomorphism have a finite rank, then the composition  $g \circ f$  also has a finite rank. If  $f$  is surjective (respectively,  $g$  is injective), then  $\text{Rank } (g \circ f) = \text{Rank } g$  (respectively,  $\text{Rank } (g \circ f) = \text{Rank } f$ ).

**S6.23** Let  $f: V \rightarrow W$  be a homomorphism of  $K$ -vector spaces and let  $u_i, i \in I$ , be a basis of  $\text{Ker } f$ . Then for a family  $v_j, j \in J$ , of vectors of  $V$ , the family  $f(v_j), j \in J$ , of the image vectors is a basis

of  $\text{Im } f$  if and only if the families  $u_i, i \in I; v_j, j \in J$ , together form a basis of  $V$ . (**Hint** : Look at the proof of the Rank-Theorem.)

**S6.24** Let  $V$  and  $W$  be finite dimensional  $K$ -vector space and let  $V', W'$  be subspaces of  $V$  and  $W$  respectively. Show that there exists a  $K$ -homomorphism  $f: V \rightarrow W$  with  $\text{Ker } f = V'$  and  $\text{Im } f = W'$  if and only if  $\text{Dim}_K V' + \text{Dim}_K W' = \text{Dim}_K V$ .

**S6.25** Let  $a_{ij} \in K, i = 1, \dots, m, j = 1, \dots, n$ . Then the linear system of equations

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= b_1 \\ \dots & \\ a_{m1}x_1 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

over  $K$  has a solution in  $K^n$  for every  $(b_1, \dots, b_m) \in K^m$  if and only if its rank is  $m$ . Moreover, in this case the solution space is an *affine subspace* of dimension  $n - m$ .

**S6.26** Let  $s, n \in \mathbb{N}, s \leq n$ . Then every affine subspace of  $K^n$  of dimension  $s$  is a solution space of a linear system of equations of rank  $n - s$  in  $n$  unknowns and  $n - s$  equations.

You might enjoy the recreational-application of Linear Algebra in the following Supplement S6.13. Its complete solution has been given below, however, I hope that one may be tempted to find their own (different) solution!

**†S6.27 (Magic-squares<sup>3</sup>)** Let  $n \in \mathbb{N}^*$  and let  $K$  be a field. A  $n \times n$ -matrix

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \in K^{\{1, \dots, n\} \times \{1, \dots, n\}} = M_n(K)$$

with elements  $a_{ij} \in K$  is called **magic** if its row-sums  $\sum_{j=1}^n a_{ij}$  and its column-sums  $\sum_{i=1}^n a_{ij}$  are all equal. Further, it is called **super-magic** if in addition both the diagonal-sums  $\sum_{i=1}^n a_{ii}$  and  $\sum_{i=1}^n a_{i, n+1-i}$  are also equal to the common row-sums (as well as column-sums).

Show that the magic (respectively, super-magic)  $n \times n$ -matrices  $\text{Mag}_n(K)$  (respectively,  $\text{Mag}_n^s(K)$ ) form a  $K$ -subspace of  $M_n(K)$  and compute the dimensions of these subspaces.

(Ans:  $\text{Dim}_K \text{Mag}_n(K) = (n-1)^2 + 1$  and  $\text{Dim}_K \text{Mag}_n^s(K) = \begin{cases} 1, & \text{if } n = 1, 2, \\ 3, & \text{if } n = 3, \\ 8, & \text{if } n = 4 \text{ and } \text{Char } K \neq 2, \\ 9, & \text{if } n = 4 \text{ and } \text{Char } K = 2, \\ n(n-2), & \text{if } n \geq 5. \end{cases}$  More-

over, one can easily find a  $K$ -basis of  $\text{Mag}_n(K)$ .)

(**Remark** : A famous super-magic matrix (over  $\mathbb{Q}$ ) is the  $4 \times 4$ -matrix

$$\begin{pmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{pmatrix}$$

was first found in the right-hand upper corner of the famous copper-plate engraving <sup>4</sup> by German 16-th century painter Albrecht Dürer. It is an allegorical composition entitled *Melencolia I* which has

<sup>3</sup>In the notion of magic-squares given here we have dropped the usual condition that all entries in it should be different from each other or even from natural numbers  $1, 2, \dots, n^2$ , because this way we can make use of Linear Algebra, otherwise it would be just combinatorics!

<sup>4</sup>In a modern context, "melancholy" applies only to the mental or emotional symptoms of depression or despondency; historically, "melancholia" could be physical as well as mental, and melancholic conditions were classified as such by their common cause rather than by their properties. Similarly, melancholia in ancient usage also encompassed mental disorders which might now be classed as schizophrenias or bipolar disorders

been the subject of many interpretations.<sup>5</sup> This engraving portrays melancholia as the state of waiting for inspiration to strike, and not necessarily as a depressive affliction. The image in turn inspired a passage in *The City of Dreadful Night* by James Thomson (B.V.), and, a few years later, a sonnet by Edward Dowden.)



<sup>5</sup>One interpretation suggests the image references the depressive or melancholy state and accordingly explains various elements of the picture. Among the most conspicuous are: (i) The tools of geometry and architecture surround the figure, unused. (ii) The  $4 \times 4$  magic-square, with the two middle cells of the bottom row giving the year of the engraving: 1514. This  $4 \times 4$  magic square, as well as having traditional magic square rules, its four quadrants, corners and centers equal the same number, 34, which happens to belong to the Fibonacci sequence. (iii) The truncated rhombohedron with a faint human skull on it. This shape is now known as Dürer's solid; over the years, there have been numerous articles disputing the precise shape of this polyhedron. (iv) The hourglass showing time running out. (v) The empty scale (balance). (vi) The despondent winged figure of genius. (vii) The purse and keys. (viii) The beacon and rainbow in the sky.

(**Proof:** For  $\mathfrak{A}, \mathfrak{B} \in \text{Mag}_n(K)$  (respectively,  $\text{Mag}_n^s$ ), it is easy to see that  $\mathfrak{A} + \mathfrak{B}$  and  $a\mathfrak{A}$ ,  $a \in K$ , belong to  $\text{Mag}_n(K)$  (respectively,  $\text{Mag}_n^s$ ) and hence both  $\text{Mag}_n(K)$  and  $\text{Mag}_n^s$  are  $K$ -subspaces of  $\mathbb{M}_n(K)$ .)

For a  $n \times n$ -Matrix  $\mathfrak{A} = (a_{ij})$ , let  $z_i := \sum_{j=1}^{n-1} a_{ij}$  be the sum of the first  $n-1$  elements in the  $i$ -th row,  $i = 1, \dots, n-1$ , and  $s_j := \sum_{i=1}^{n-1} a_{ij}$  be the sum of the first  $n-1$  elements in the  $j$ -th column,  $j = 1, \dots, n-1$ , of  $\mathfrak{A}$  and further  $a := \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_{ij} = \sum_{i=1}^{n-1} z_i = \sum_{j=1}^{n-1} s_j$ . Then the matrix  $\mathfrak{A}$  is magic with the row- and column sum  $s$  if and only if  $a_{in} = s - z_i$  for  $i = 1, \dots, n-1$ ,  $a_{nj} = s - s_j$  for  $j = 1, \dots, n-1$  and  $a_{nn} = a - (n-2)s$ . (The choice of  $a_{in}$  and  $a_{nj}$  is necessary and sufficient for the row-sum and the column-sum for the first  $n-1$  rows as well as columns is  $s$ ) The sum of the elements in the  $n$ -th row is  $s$  if and only if  $\sum_{j=1}^{n-1} a_{nj} + a_{nn} = \sum_{j=1}^{n-1} (s - s_j) + a_{nn} = (n-1)s - a + a_{nn} = s$ , i. e.  $a_{nn} = a - (n-2)s$ . In this case it is automatic that the sum of the elements in the  $n$ -th column is also equal to  $s$  because  $\sum_{i=1}^{n-1} a_{in} + a_{nn} = \sum_{i=1}^{n-1} (s - z_i) + a - (n-2)s = (n-1)s - a + a - (n-2)s = s$ . Therefore the general form of a magic matrix with row- and column sum  $s$  is:

$$f(a_{11}, \dots, a_{1,n-1}, \dots, a_{n-1,1}, \dots, a_{n-1,n-1}, s) := \begin{pmatrix} a_{11} & \cdots & a_{1,n-1} & s - z_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & s - z_{n-1} \\ s - s_1 & \cdots & s - s_{n-1} & a - (n-2)s \end{pmatrix}.$$

This define the map  $f: K^{(n-1)^2+1} \rightarrow \text{Mag}_n(K)$  which is clearly  $K$ -linear and further surjective as seen above. If  $f(a_{11}, \dots, a_{1,n-1}, \dots, a_{n-1,1}, \dots, a_{n-1,n-1}, s) = 0$ , then first  $a_{ij}$  are 0 for all  $1 \leq i, j \leq n-1$  and then the  $z_i, s_j, s$  are 0 and finally, also  $a$ . Therefore  $\text{Ker } f = 0$  and hence  $f$  is injective. Altogether  $f$  is an isomorphism and hence  $\text{Dim}_K \text{Mag}_n(K) = (n-1)^2 + 1$ .

The image of the standard basis of  $K^{(n-1)^2+1}$  is clearly a basis of  $\text{Mag}_n(K)$ . These are precisely the following  $(n-1)^2$  magic-matrices with the upper-left  $(n-1) \times (n-1)$ -submatrix which has  $(p, q)$ -th entry is 1 and all other entries are 0, where  $p, q = 1, \dots, n-1$ ,

$$\mathfrak{E}_{pq} - \mathfrak{E}_{nq} - \mathfrak{E}_{pn} + \mathfrak{E}_{nn} = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & \cdots & 0 & -1 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & 0 \\ 0 & \cdots & -1 & \cdots & 0 & 1 \end{pmatrix}$$

and the  $n \times n$ -matrix

$$\mathfrak{E}_{n1} + \cdots + \mathfrak{E}_{n,n-1} + (2-n)\mathfrak{E}_{nn} + \mathfrak{E}_{1n} + \cdots + \mathfrak{E}_{1,n-1} = \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 & 1 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & 1 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 & 1 \\ 1 & \cdots & 1 & \cdots & 1 & 2-n \end{pmatrix}.$$

In the case  $n = 1$  every matrix is super-magic, if  $n = 2$ , then clearly the matrices with all equal entries are precisely the super-magic matrices. In both these cases  $\text{Dim}_K \text{Mag}_n^s(K) = 1$ .

Now, assume that  $n \geq 3$ . Then  $f(a_{11}, \dots, a_{1,n-1}, \dots, a_{n-1,1}, \dots, a_{n-1,n-1}, s)$  is super-magic if and only if

$$\sum_{i=1}^{n-1} a_{ii} + a - (n-2)s = s \quad \text{and} \quad s - z_1 + \sum_{i=2}^{n-1} a_{i,n-i+1} + s - s_1 = s,$$

i. e. if and only if  $(a_{11}, \dots, a_{1,n-1}, \dots, a_{n-1,1}, \dots, a_{n-1,n-1}, s)$  is a solution of the system of linear equations

$$\sum_{i=1}^{n-1} a_{ii} + \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_{ij} - (n-1)s = 0, \quad s - \sum_{j=1}^{n-1} a_{1j} - \sum_{i=1}^{n-1} a_{i1} + \sum_{i=2}^{n-1} a_{i,n-i+1} = 0.$$

This solution space of this system of linear equations has (see Theorem 5.E.6 in the Lecture-Notes) has dimension  $(n-1)^2 + 1 - r$ , where  $r$  is the rank of the homogeneous system of linear equations, therefore is the dimension of  $\text{Im } g$ , where  $g: K^{(n-1)^2+1} \rightarrow K^2$  is defined by:

$$g(a_{11}, \dots, a_{1,n-1}, \dots, a_{n-1,1}, \dots, a_{n-1,n-1}, s) := \left( \sum_{i=1}^{n-1} a_{ii} + \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_{ij} - (n-1)s, s - \sum_{j=1}^{n-1} a_{1j} - \sum_{i=1}^{n-1} a_{i1} + \sum_{i=2}^{n-1} a_{i,n-i+1} \right).$$

If we put all  $a_{ij} = 0$  and  $s = 1$ , then  $g(0, \dots, 0, 1) = (1-n, 1) \neq 0$ , i. e.  $\text{Dim}_K \text{Im } g \geq 1$ . If we put  $s = 0$  and all  $a_{ij} = 0$ , but  $a_{12} = -1$ , then  $g(0, -1, 0, \dots, 0, 0) = (-1, 1)$ . In the case  $n = 3$  both  $(-2, 1)$  and

$(-1, 1)$  are contained in  $\text{Im } g$  and since  $-2 \neq -1$ , they are linearly independent, i. e.  $r = \text{Dim}_K \mathfrak{S}g = 2$  and  $\text{Dim}_K \text{Mag}_n^s(K) = (n-1)^2 + 1 - 2 = 5 - 2 = 3$ .

In the case  $n=4$  and  $\text{Char } K \neq 2$ , both  $(-3, 1)$  and  $(-1, 1)$  belong to the  $\text{Im } g$  and since  $-3 \neq -1$ , they are linearly independent, i. e.  $r = \text{Dim}_K \text{Im } g = 2$  and  $\text{Dim}_K \text{Mag}_n^s(K) = (n-1)^2 + 1 - 2 = 10 - 2 = 8$ .

In the case  $n=4$  and  $\text{Char } K = 2$ , since  $2 = 0$ , we have  $-a_{ij} = a_{ij}$  and  $-3s = s$ ,

$$\begin{aligned} g(a_{11}, \dots, a_{33}, s) &= \\ (2(a_{11} + a_{22} + a_{33}) + a_{12} + a_{13} + a_{21} + a_{23} + a_{31} + a_{32} - 3s, s - 2a_{11} - a_{12} - a_{13} - a_{21} - a_{31} + a_{23} + a_{32}) \\ &= (s + a_{12} + a_{13} + a_{21} + a_{31} + a_{23} + a_{32}) \cdot (1, 1), \end{aligned}$$

i. e.  $\text{Im } g$  is only 1-dimensional and hence  $\text{Dim}_K \text{Mag}_n^s(K) = (n-1)^2 + 1 - 1 = 10 - 1 = 9$ .

Now assume that  $n \geq 5$ . Then the index  $(2, 3)$  is smaller than the indices  $(i, n-i+1)$ , since  $n-2+1 \geq 4$ . We put  $s=0$  and all  $a_{ij}=0$ , but  $a_{23}=1$ , then  $g(0, \dots, 0, 0, 0, 1, \dots, 0, \dots, 0, \dots, 0, 0) = (1, 0)$ . Since  $g(0, \dots, 0, 1) = (1-n, 1) \neq 0$  and  $(1, 0)$  are linearly independent, we have  $r=2$ , and hence  $\text{Dim}_K \text{Mag}_n^s(K) = (n-1)^2 + 1 - 2 = n(n-2)$ .

†**S6.28** (Theorem of Noether-Skolem-Brauer and Theorem of Wedderburn) In this Supplement we provide proofs of classical theorems on division rings by using the generalisation of Lemma of Dedekind-Artin **Supplement S5.11 (a)**.

Let  $D$  be a division ring<sup>6</sup> with the center  $Z(D) := \{x \in D \mid xy = yx \text{ for every } y \in D\} = k$ . We consider  $D$  as an  $k$ -algebra.

(a) Let  $x_i, i \in I$ , be a family of non-zero elements in  $D$ . Then the inner automorphisms  $\varkappa_{x_i}, i \in I$ , in  $D^D$  is linearly independent over  $D$  if and only if the family  $x_i^{-1}, i \in I$ , is linear independent over  $k$ . In particular, if  $D$  is finite dimensional over  $k$ , then  $\text{End}_k D$  has a  $D$ -basis of the form  $\varkappa_{x_i}, i = 1, \dots, n$ , with  $x_i \in D^\times$ . (Hint: Let  $x_0, x_1, \dots, x_n \in D^\times$  and  $x_0^{-1} = \sum_{i=1}^n \alpha_i x_i^{-1}, \alpha_i \in k$ . Then  $x_0 y x_0^{-1} = \sum_{i=1}^n \alpha_i x_0 y x_i^{-1} = \sum_{i=1}^n \alpha_i x_0 x_i^{-1} (x_i y x_i^{-1})$ , i. e.,  $\varkappa_{x_0} = \sum_{i=1}^n \alpha_i \varkappa_{x_i}, \alpha_i := \alpha_i x_0 x_i^{-1}$ . Conversely, from  $\varkappa_{x_0} = \sum_{i=1}^n \alpha_i \varkappa_{x_i}$ , all  $\alpha_i \neq 0$  and by **Supplement S5.11 (a)**, we get  $\varkappa_{x_0} = \varkappa_{\alpha_i x_i} = \varkappa_{\alpha_i x_i}$  and therefore  $\alpha_i x_i = \alpha_i x_0$  with  $\alpha_i \in k$  and  $x_0^{-1} = \varkappa_{x_0}(x_0^{-1}) = \sum_{i=1}^n \alpha_i x_i x_0^{-1} x_i^{-1} = \sum_{i=1}^n \alpha_i x_i^{-1}$ .)

(b) (Theorem of Noether-Skolem-Brauer)<sup>7</sup> If  $D$  is finite dimensional over  $k$ , then every  $k$ -algebra automorphism of  $D$  is an inner automorphism of  $D$ . (Proof: Let  $\Phi : D \rightarrow D$  be a  $k$ -algebra automorphism of  $D$  and write  $\Phi = a_1 \varkappa_{x_1} + \dots + a_n \varkappa_{x_n}$ , where  $x_1^{-1}, \dots, x_n^{-1}$  is a  $k$ -basis of  $D$  and  $a_1, \dots, a_n \in D, n := \text{Dim}_k D$  (see part (a)). Then  $\Phi = \varkappa_{\alpha_i x_i} = \varkappa_{\alpha_i x_i}$  for all  $i$  with  $\alpha_i \neq 0$  by **Supplement S5.11 (a)**. — We give a generalisation of this result: If  $f : K \rightarrow L$  is a  $k$ -isomorphism of  $k$ -subalgebras  $K, L$  of  $D$ . Then  $f = \varkappa_a|_K$  is the restriction of a conjugation  $\varkappa_a$  of  $D, a \in D^\times$ . In particular,  $k$ -isomorphic  $k$ -subalgebras of  $D$  are conjugates. — Proof: By part (a)  $\text{End}_k D$  has a  $D$ -basis of the form  $\varkappa_{x_i}, i = 1, \dots, n$ , with  $x_i \in D^\times$ . Since the  $D$ -homomorphism  $\text{End}_k D \rightarrow \text{Hom}_k(K, D), g \mapsto g|_K$  is surjective, we may assume that the first  $r$  of these conjugations is a  $D$ -basis of  $\text{Hom}_k(K, D)$ , where  $r := [K : k]$ . Then  $f = (\sum_{i=1}^r a_i \varkappa_{x_i})|_K$  with  $a_i \in D, i = 1, \dots, r$ . Now, since  $f$  is also a character, it follows from **Supplement S5.11 (a)** that  $f = \varkappa_{\alpha_i x_i}|_K = \varkappa_{\alpha_i x_i}|_K$  for every  $i$  with  $\alpha_i \neq 0$ .)

(c) Suppose that  $n := \text{Dim}_k D$  is finite and  $y_1, \dots, y_n \in D$  be a  $k$ -basis of  $D$ . Let  $\lambda_i = \lambda_{y_i} : D \rightarrow D, x \mapsto y_i x$ , (resp.  $\rho_i = \rho_{y_i} : D \rightarrow D, x \mapsto x y_i$ ) be the left multiplication by  $y_i$  (resp. right multiplication by  $y_i$ ). Then  $\lambda_i \rho_j = \rho_j \lambda_i, 1 \leq i, j \leq n$  is a  $k$ -basis of  $\text{End}_k D$ .

— (Theorem of Brauer) The canonical  $k$ -algebra homomorphism  $D \otimes_k D^{\text{op}} \rightarrow \text{End}_k D, x \otimes y \mapsto L_x \cdot R_y = R_y \cdot L_x$ , is a  $k$ -algebra isomorphism. (Use part (a). — The following corollary of this result is used in the proof in part (d): **Corollary:** If  $K$  is a maximal commutative  $k$ -subalgebra of  $D$ . Then  $[K : k]^2 = [D : k]$ . — Proof: It follows that  $K$  is a subfield of  $K$ . We consider  $D$  as a  $K$ -vector

<sup>6</sup>A ring  $D \neq 0$  is called a division ring if every non-zero element in  $D$  is invertible, i. e., the unit group of  $D$  is  $D^\times = D \setminus \{0\}$ . A division ring satisfies all axioms of a field other than commutativity; for this reason division rings are also called skew-fields. Modules over a division ring are also called vector spaces over  $D$ . The same proof as in the case of vector spaces over a field shows that: Every vector space over a division ring  $D$  has a  $D$ -basis and that any two bases have the same cardinality. It is easy to see that the center of a division ring  $D$  is a subfield of  $D$  and hence  $D$  is a vector space over, in fact an algebra, its center.

<sup>7</sup>This theorem was first published in 1927 by Thoralf Skolem, best remembered for his work in mathematical logic. Emmy Noether rediscovered it in 1933 and it is perhaps due to her recognition of its significance in the architecture of modern algebra that it is sometimes known as the first fundamental theorem of the theory of division algebras.



space. Put  $n := [D : k]$ ,  $m := [D : K]$ ,  $r := [K : k]$  and  $e := \text{Dim}_k \text{End}_K D$ . Then by degree-formula  $n = rm$  and  $e = r \cdot \text{Dim}_K \text{End}_K D = rm^2$ . Therefore, it is enough to verify:  $e = rn (= r^2 m)$ . To prove this, let  $x_1, \dots, x_n \in D$  be  $k$ -basis of  $D$ , where  $x_1, \dots, x_r$  is a  $k$ -basis of  $K$ . Then by part (c)  $\lambda_{x_i} \rho_{x_j}$ ,  $1 \leq i, j \leq n$ , is a  $k$ -basis of  $\text{End}_k D (\supseteq \text{End}_K D)$ . Now, we claim that  $\lambda_{x_i} \rho_{x_j}$ ,  $i = 1, \dots, r$ ,  $j = 1, \dots, n$ , is a  $k$ -basis of  $\text{End}_K D$ . Obviously, these elements belong to  $\text{End}_K D$ . It remains to show that: If  $a_j \in D$ ,  $j = 1, \dots, n$ , are such that  $\sum_{j=1}^n \lambda_{a_j} \rho_{x_j}$  is  $K$ -linear, then  $a_1, \dots, a_n \in K$ . Clearly,  $\sum_{j=1}^n \lambda_{a_j} \rho_{x_j}$  is  $K$ -linear if and only if  $\sum_{j=1}^n \lambda_a \lambda_{a_j} \rho_{x_j} = \sum_{j=1}^n \lambda_{a_j} \lambda_a \rho_{x_j}$  for all  $a \in K$ . If this is satisfied, then it follows from the  $k$ -linear independence of  $\lambda_{x_i} \rho_{x_j}$ ,  $1 \leq i, j \leq n$ , that  $\lambda_{(aa_j - a_j a)} = 0$  for all  $a \in K$  and all  $j = 1, \dots, n$ . But, this mean that  $aa_j = a_j a$  for all  $a \in K$  and hence  $a_j \in K$ ,  $j = 1, \dots, n$ , since  $K$  is a maximal commutative  $k$ -subalgebra of  $D$ .)

**(d) (Theorem of Wedderburn):** Every finite division ring  $D$  is commutative, i. e., a field. **(Proof:** By part (b) all maximal commutative  $k$ -subalgebras have the same degree over  $k$  and are therefore isomorphic  $k$ -subalgebras. Hence, by part (c),  $D^\times = \bigcup_{x \in D^\times} x E_0^\times x^{-1}$  for some fixed maximal commutative  $k$ -subalgebra  $E_0$ . This implies that  $D^\times = E_0^\times$  and  $D = E_0$  by the following simple fact: If  $H \subset G$  is a proper subgroup of a finite group  $G$ , then  $G \neq \bigcup_{x \in G} x H x^{-1}$ . Equivalently: There is a  $g \in G$  with  $g(xH) \neq xH$  for all cosets  $xH \in G/H$ . — For the real quaternions  $\mathbb{H}(\mathbb{R}) = \mathbb{H} := \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ , we have  $\mathbb{R} = \mathbb{Z}(\mathbb{H})$  and  $\mathbb{H}^\times = \bigcup_{x \in \mathbb{H}^\times} x \mathbb{C}^\times x^{-1}$ , where  $\mathbb{C} \subseteq \mathbb{H}$  is the standard embedding of  $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$  into  $\mathbb{H}$ . — Note also that by part (b) all ring automorphisms of  $\mathbb{H}$  are inner automorphisms, since  $\text{id}_{\mathbb{R}}$  is the only field endomorphism of  $\mathbb{R} = \mathbb{Z}(\mathbb{H})$ . Prove the same result for  $\mathbb{H}(\mathbb{Q})$  also.)