E0 219 Linear Algebra and Applications / August-December 2011

(ME, MSc. Ph. D. Programmes)

Tel : +91-(0)80-2293 2239/(Maths Dept. 3212) **E-mails :** dppatil@csa.iisc.ernet.in / patil@math.iisc.ernet.in

Lectures : Monday and Wednesday ; 11:30–13:00 **Venue:** CSA, Lecture Hall (Room No. 117)

Corrections by : **Jasine Babu** (jasinekb@gmail.com) / **Nitin Singh** (nitin@math.iisc.ernet.in) / **Amulya Ratna Swain** (amulya@csa.iisc.ernet.in) / **Meghana Mande** (meghanamande@gmail.com) / **Achintya Kundu** (achintya.ece@gmail.com)

1-st Midterm : Saturday, September 17, 2011; 10:30 -12:30 **2-nd Midterm :** Saturday, October 22, 2011; 10:30 -12:30
Final Examination : December ??, 2011, 10:00 -13:00

Evaluation Weightage : Assignments : 20% **Midterms (Two) :** 30% **Final Examination :** 50%

3. Generating systems, Linear independence, Bases

Submit a solution of the $*$-Exercise ONLY

Due Date : Monday, 29-08-2011 (Before the Class)

3.1 **(a)** Let K be a field of characteristic $\neq 2$, i. e. $1+1\neq 0$ in K and let $a\in K$. Compute the solution set of the following systems of linear equations over K:

$$\begin{aligned} ax_1 + x_2 + x_3 &= 1\\ x_1 + ax_2 + x_3 &= 1\\ x_1 + x_2 + ax_3 &= 1\,; \end{aligned} \qquad \text{and} \qquad \begin{aligned} x_1 + x_2 - x_3 &= 1\\ 2x_1 + 3x_2 + ax_3 &= 3\\ x_1 + ax_2 + 3x_3 &= 2\,; \end{aligned}$$

For which a these systems have exactly one solution ?

(b) The set of m-tuples $(b_1,\ldots,b_m)\in K^m$ for which a linear system of equations $\sum_{j=1}^n a_{ij}x_j = b_i$, $i=1,\ldots,m$, over a field K has a solution is a K-subspace of K^m.

(c) Let K be a subfield of the field L and let $\sum_{j=1}^n a_{ij}x_j = b_i\,, i=1,\ldots,m$ be a system of linear equations over K. If this system has a solution $(x_1,\ldots,x_n)\in L^n$, then it also has a solution in K^n.

***3.2** **(a)** Let $x_1,\ldots,x_n\in V$ be linearly independent (over K) in a K-vector space V and let $x := \sum_{i=1}^n a_i x_i \in V$ with $a_i\in K$. Show that $x_1-x,\ldots,x_n-x$ are linearly independent over K if and only if $a_1+\cdots+a_n\neq 1$.

(b) Let $x_1,\ldots,x_n$ be a basis of the K-vector space V and let $a_{ij}\in K$, $1\le i\le j\le n$. Show that

$$y_1 = a_{11}x_1\,,\ y_2 = a_{12}x_1 + a_{22}x_2\,,\ \ldots\ ,\ y_n = a_{1n}x_1 + a_{2n}x_2 + \cdots + a_{nn}x_n$$

is a basis of V if and only if $a_{11}\cdots a_{nn}\neq 0$.

(c) Show that the family $\{\ln p \mid p \text{ prime number}\}$ of real numbers is linearly independent over $\mathbb{Q}$. (**Hint :** Use the Fundamental Theorem of Arithmetic, see Test-Exercise T3.1.)

3.3 Let K be a field and let $K[X]$ (respectively, $K[X]_m$, $m\in\mathbb{N}$) be the K-vector space of all polynomials (respectively, polynomials of degree $<m$) with coefficients in K. Let $f_n\in K[X]$, $n\in\mathbb{N}$, be a sequence of polynomials with $\deg f_n\le n$ for all $n\in\mathbb{N}$. Show that:

(a) For every $m\in\mathbb{N}$, $f_0,\ldots,f_{m-1}$ is a K-basis of the subspace $K[X]_m$ if and only if $\deg f_n = n$ for all $n=0,\ldots,m-1$.

(b) $f_n\,, n\in\mathbb{N}$, is a basis of the K-vector space $K[X]$ if and only if $\deg f_n = n$ for all $n\in\mathbb{N}$. (**Hint :** Use part (a).)

3.4 **(a)** Let $f\colon I\to K$ be a K-valued function with image $f(I)$ infinite. Then the sequence f^n, $n\in\mathbb{N}$ of powers of f is linearly independent (over K) in the K-vector space K^I.

(b) The sequences $(1,\lambda,\lambda^2,\ldots,\lambda^n,\ldots)\in K^{\mathbb{N}}$, $\lambda\in K$, are linearly independent over K. (**Hint :** See Test-Exercise T3.6.)

On the other side one can see auxiliary results and (simple) test-exercises.

Auxiliary Results/Test-Exercises

To understand and appreciate the Test-Exercises which are marked with the symbol † one may possibly require more mathematical maturity than one has!

T3.1 (Fundamental Theorem of Arithmetic[1]) Proposition 14 of Book IX of Euclid's "Elements" embodies the result which later became known as the **Fundamental Theorem of Arithmetic:** *Every Natural number $a > 1$ is a product of prime numbers and this representation is "essentially" unique, apart from the order in which the prime factors occur.*

(a) (Existence of prime decomposition) *Every natural number $a > 1$ has a prime decomposition $a = p_1 \cdots p_n$, where we may choose p_1 as the smallest (prime) divisor t of a.* (**Proof :** Either a is prime or composite.; in the former case there is nothing to prove. If a is composite, then by the minimality principle (applied to the non-empty subset $T = \{d \in \mathbb{N}^* \mid d \big| a \text{ and } d > 1\}$, $a \in T$) there exists a smallest prime divisor p_1 of a, i. e. $a = p_1 \cdot b$ with $1 \leq b < a$ (since $1 < p_1 \leq a$). Now, by induction hypothesis b has a prime decomposition $b = p_2 \cdots p_n$ and hence a has a prime decomposition $a = p_1 \cdot p_2 \cdots p_n$.)

(b) (Uniqueness of prime decomposition) *A prime decomposition of every natural number $a > 1$ is essentially unique. More precisely, if $a = p_1 \cdots p_n$ and $a = q_1 \cdots q_m$ are two prime decompositions of a with prime numbers $p_1, \ldots, p_n \,;\, q_1, \ldots, q_m$, then $m = n$ and there exists a permutation $\sigma \in \mathfrak{S}_n$ such that $q_i = p_{\sigma(i)}$ for every $i = 1, \ldots, n$.* (**Remark :** For a proof of uniqueness one uses the *Euclid's lemma*[2] on the prime property and hence uses implicitly the division algorithm and therefore make use of the additive structure of $\mathbb{N}$. The existence of prime decomposition only uses the multiplicative structure on $\mathbb{N}$ and not the additive structure on $\mathbb{N}$. This leads to the question : *Can one give a proof of the uniqueness of the prime decomposition which only depends on the multiplicative structure of* $\mathbb{N}$? The answer to this question is negative!)

T3.2 Let $x_1, \ldots, x_n, x$ be elements of a vector space over a field K. Then

(a) The family $x_1, \ldots, x_n, x_1 + \cdots + x_n$ is linearly dependent over K, but every n of these vectors are linearly independent over K.

(b) Show that $x_1, \ldots, x_n, x$ are linearly independent over K if and only if $x_1, \ldots, x_n$ are linearly independent over K and $x \notin Kx_1 + \cdots + Kx_n$.

(c) Show that $x_1, \ldots, x_n$ is a generating system of V if and only if $x_1, \ldots, x_n, x$ is a generating system of V and $x \in Kx_1 + \cdots + Kx_n$.

T3.3 Let V be a vector space over a field K.

(a) If V has a finite (respectively, a countable) generating system, then every generating system of V has a finite (respectively, a countable) generating system.

(b) If V has a countable infinite basis, then every basis of V is countable infinite.

(c) If there is an uncountable linearly independent system in V, then no generating system of V is countable.

(d) If K is countable and if V has a countable generating system, then V is countable. In particular, every Hamel-basis of $\mathbb{R}$ over $\mathbb{Q}$ is uncountable.

(e) If v_i, $i \in I$, is a generating system for V, then every maximal linearly independent subsystem of v_i, $i \in I$, is a basis of V.

T3.4 Let a_n, $n \in \mathbb{N}^*$, be a sequence of elements in K. Show that :

---

[1] The Fundamental Theorem of Arithmetic does not seem to have been stated explicitly in Euclid's elements, although some of the propositions in book VII and/or IX are almost equivalent to it. Its first clear formulation with proof seems to have been given by Gauss in *Disquisitiones arithmeticae* §16 (Leipzig, Fleischer, 1801). It was, of course, familiar to earlier mathematicians; but Gauss was the first to develop arithmetic as a systematic science.

[2] **Euclid's Lemma** *If a prime number p divides a product ab of two natural numbers a and b, then p divides one of the factor a or b.* (**Proof :** The set $A := \{x \in \mathbb{N}^* \mid p \big| ax\}$ contains p and b and hence by the minimality principle it has a smallest element c. We claim that $c \big| y$ for every $y \in A$. For, by division algorithm $y = qc + r$ with $q, r \in \mathbb{N}$ and $0 \leq r < c$. Then, since $p \big| ay$ and $p \big| ac$, $p \big| ay - q(ac) = ar$. This proves that $r = 0$; otherwise $r \in A$ and $r < c$ a contradiction to the minimality of c in A. Therefore $c \big| y$ for every $y \in A$; in particular, $c \big| p$ and hence $c = 1$ or $c = p$. If $c = 1$, then $p \big| ac = a$. If $c = p$, then (since $b \in A$) by the above claim $p \big| b$.

(a) For every $m \in \mathbb{N}$, the polynomials $1, X-a_1, \ldots, (X-a_1)\cdots(X-a_{m-1})$ form a K-basis of $K[X]_m$.

(b) The polynomials $(X-a_1)\cdots(X-a_n)$, $n \in \mathbb{N}$, form a K-basis of $K[X]$.

†**T3.5** Let $D \subseteq \mathbb{R}$ be an infinite subset and let $Q \subseteq \mathbb{R}[X]$ be the set of all monic polynomials of degree 2 witout any real zeros. Then

$$t^n,\ n \in \mathbb{N}, \quad \frac{1}{(t-a)^m},\ m \in \mathbb{N}^*,\ a \in \mathbb{R}\setminus D, \quad \text{and} \quad \frac{t^r}{q^\ell},\ r \in \{0,1\},\ \ell \in \mathbb{N}^*,\ q \in Q,$$

together form a $\mathbb{R}$-basis of the $\mathbb{R}$-vector space of real rational functions defined on D.

T3.6 Let $\lambda_1, \ldots, \lambda_n$ be pairwise distinct elements in a field K. Then the elements

$$x_1 := (1, \lambda_1, \lambda_1^2, \ldots, \lambda_1^{n-1}), \ldots, x_n := (1, \lambda_n, \lambda_n^2, \ldots, \lambda_n^{n-1}) \in K^n$$

are linearly independent over K. (**Hint :** Induction on n. Assume the result for $n-1$ and $a_1x_1 + \cdots + a_nx_n = 0$. Then we have the equations: $a_1\lambda_n x_1' + \cdots + a_n\lambda_n x_n' = 0$ and $a_1\lambda_1 x_1' + \cdots + a_n\lambda_n x_n' = 0$, and so $a_1(\lambda_n - \lambda_1)x_1' + \cdots + a_{n-1}(\lambda_n - \lambda_{n-1})x_{n-1}' = 0$, where $x_i' := (1, \lambda_i, \ldots, \lambda_i^{n-2})$, $i = 1, \ldots, n$.)

†**T3.7** **(a)** The vector space of all sequences $K^{\mathbb{N}}$ has no countable generating system over K. (**Hint :** Consider the cases K countable and uncountable separately to show that $K^{\mathbb{N}}$ is never countable and use Test-Exercises T3.3-(c), (d) and Exercise 3.4-(b).)

(b) Let I be an infinite set. Then the K-vector space K^I of K-valued functions on I has no countable generating system over K.

(c) The K-subspace of $K^{\mathbb{N}}$ generated by the characteristic functions e_A, $A \subseteq \mathbb{N}$ has no countable generating system. (**Hint :** *If $\mathfrak{K}$ is a totally ordered subset of $\mathfrak{P}(\mathbb{N}) \setminus \{\emptyset\}$, then the family e_A, $A \in \mathfrak{K}$ is linearly independent.* Now, use the fact that there are uncountable totally ordered subsets in the ordered set $(\mathfrak{P}(\mathbb{N}), \subseteq)$.)

†**T3.8** **(a)** Let $I \subseteq \mathbb{R}$ be an interval which contain more than one point. Then none of the $\mathbb{K}$-vector space $\mathrm{C}^\alpha_{\mathbb{K}}(I)$, $\alpha \in \mathbb{N} \cup \{\infty, \omega\}$, has a countable generating system.

(b) The $\mathbb{K}$-vector space of all convergent power series $\sum_{n=0}^\infty a_n x^n$ with coefficients a_n from $\mathbb{K}$ has no countable generating system over $\mathbb{K}$.

T3.9 Which of the following systems of functions are linearly independent over $\mathbb{R}$ in the $\mathbb{R}$-vector space $\mathbb{R}^{\mathbb{R}}$ of all functions.

(a) $1, \sin t, \cos t$. **(b)** $\sin t, \cos t, \sin(\alpha + t)$ ($\alpha \in \mathbb{R}$ fixed).

(c) $t, |t|, \mathrm{Sign}\, t$. **(d)** $e^t, \sin t, \cos t$.

†**T3.10** **(a)** (Q u a s i - p o l y n o m i a l s) The functions $t^n e^{\alpha t}$, $n \in \mathbb{N}$, $\alpha \in \mathbb{C}$, are linearly independent in the $\mathbb{C}$-vector space $\mathbb{C}^D$ of $\mathbb{C}$-valued functions on a subset $D \subseteq \mathbb{C}$ which has a limit point in $\mathbb{C}$. (**Remark :** The $\mathbb{C}$-subspace generated by these functions is called the s p a c e o f q u a s i - p o l y n o m i a l s. One usually proves in the first course on differential equation that: *The quasi-polynomials are the solutions of the linear differential equations with constant coefficients $P(D)y = 0$, $P \in \mathbb{C}[X] \setminus \{0\}$.* More precisely: *Let $P = (X-\lambda_1)^{\alpha_1} \cdots (X-\lambda_r)^{\alpha_r} \in \mathbb{K}[X]$ be a polynomial with pairwise distinct zeros $\lambda_1, \ldots, \lambda_r \in \mathbb{K}$. Then $e^{\lambda_1 t}, \ldots, t^{\alpha_1 - 1}e^{\lambda_1 t}, \ldots, e^{\lambda_r t}, \ldots, t^{\alpha_r - 1}e^{\lambda_r t}$ is a $\mathbb{K}$-basis of the solution space $\{y \in \mathrm{C}^n_{\mathbb{K}}(I) \mid P(D)y = 0\}$ of the corresponding homogeneous differential equation $P(D)(y) = (D-\lambda_1)^{\alpha_1} \cdots (D-\lambda_r)^{\alpha_r}(y) = 0$ consisting $n := \alpha_1 + \cdots + \alpha_r = \deg P$ elements.*)

(b) The functions $t^m e^{bt} \cos \beta t$, $m \in \mathbb{N}$, $b \in \mathbb{R}$, $\beta \in \mathbb{R}_+$; $t^k e^{ct} \sin \gamma t$, $k \in \mathbb{N}$, $c \in \mathbb{R}$, $\gamma \in \mathbb{R}_+^\times$, together form a basis of the $\mathbb{R}$-vector space of the real valued quasi-polynomials $\mathbb{R} \to \mathbb{R}$. (See part (a).)

(c) Let Λ be the set of numbers $\lambda \in \mathbb{C}$ with $\mathrm{Re}\,\lambda > 0$ or with $\mathrm{Re}\,\lambda = 0$ and $\mathrm{Im}\,\lambda > 0$. Then the functions

$$t^n,\quad n \in \mathbb{N}; \qquad t^m \cos \beta t,\quad m \in \mathbb{N},\ \beta \in \Lambda; \qquad t^k \sin \gamma t,\quad k \in \mathbb{N},\ \gamma \in \Lambda,$$

together form a basis of the $\mathbb{C}$-vector space of the quasi-polynomials $\mathbb{R} \to \mathbb{C}$. (See part (a).)

T3.11 Let K be a field. Let f_i, $i \in I$, and g_j, $j \in J$, be linearly independent K-valued functions on the sets X resp. Y. Then the functions $f_i \otimes g_j \colon (x,y) \longmapsto f_i(x)\, g_j(y)$, $(i,j) \in I \times J$, are linearly independent in $K^{X \times Y}$.

T3.12 Let $K \subseteq L$ be a field extension and let b_i, $i \in I$, be a K-basis of L. If V is a L-vector space with L-basis y_j, $j \in J$, then $b_i y_j$, $(i,j) \in I \times J$, is a K-basis of V.