MA-219 Linear Algebra

2. Vector spaces – Subspaces

August 18, 2003 ; Submit solutions **before 11:00AM ; August 25, 2003.**

Let $\mathbb{K}$ denote either the field $\mathbb{R}$ of real numbers or the field $\mathbb{C}$ of complex numbers.

2.1. a). Let V be a vector space over a field and let X be any set with a bijection $f : X \to V$. Then X has a K-vector space structure with $f^{-1}(0)$ as a zero element and for $a \in K$, $x, y \in X$, $x + y := f^{-1}\big(f(x) + f(y)\big)$ and $ax := f^{-1}\big(af(x)\big)$.

b). Let X be any set. Then the set-ring $(\mathfrak{P}(X), \Delta, \cap)$ of X (see exercise 1.5) has a natural structure of a vector space over the field $\mathbb{Z}_2$. (**Hint:** The map $\mathfrak{P}(X) \to \mathbb{Z}_2^X$ defined by $A \mapsto e_A$ is a bijective, where e_A denote the indicator function of A. See exercise T1.1.)

2.2. Let V be a vector space over a field K with a field with $|K| \geq n$ and let $V_1, \ldots, V_n$ be K-subspaces of V. If $V_i \neq V$ for every $1 \leq i \leq n$ then show that $V_1 \cup V_2 \cup \cdots \cup V_n \neq V$. Show by an example that the condition $|K| \geq n$ is necessary. (**Hint:** By induction on n, assume that $V_1 \cup V_2 \cup \cdots \cup V_{n-1} \neq V$. Choose $x \in V_n$ with $x \notin V_1 \cup \cdots \cup V_{n-1}$ and $y \in V$ with $y \notin V_n$. Now consider the set $\{ax + y \mid a \in K\}$ which has atleast n distinct elements.)

2.3. Let K be a field and let I be an index set.

a). The set of all functions $f : I \to K$ with finite image i.e. $f(I)$ is a finite subset of K, is a K-subspace of the vector space K^I.

b). The set of all functions $f : I \to K$ with countable image i.e. $f(I)$ is a countable subset of K, is a K-subspace of the vector space K^I.

c). The set $\mathrm{B}_{\mathbb{K}}(I)$ bounded functions $f : I \to \mathbb{K}$ is a $\mathbb{K}$-subspace of $\mathbb{K}^I$.

d). The set W_g (resp. W_u) of all even (resp. odd) functions [1] $\mathbb{R} \to \mathbb{K}$ is a $\mathbb{K}$-subspaces of $\mathbb{K}^{\mathbb{R}}$. Further, show that $W_g \cap W_u = 0$ and $W_g + W_u = \mathbb{K}^{\mathbb{R}}$.

e). The set of all functions $f : \mathbb{C} \to \mathbb{C}$ with $\lim\limits_{z\to\infty} f(z) = 0$ is a $\mathbb{C}$-subspace of the vector space $\mathbb{C}^{\mathbb{C}}$ of all $\mathbb{C}$-valued functions on $\mathbb{C}$.

2.4. For subspaces U, U', W, W' of a vector space V over a field K, show that:

a). The subset $V \setminus (U \setminus W)$ is a subspace of V if and only if $U = V$ or $U \subseteq W$.

b). $U + (U' \cap W) \subseteq (U + U') \cap (U + W)$.

c). $U \cap (U' + W) \supseteq (U \cap U') + (U \cap W)$.

d). (Modular law) $U + (U' \cap W) = U' \cap (U + W)$.

e). Suppose that $U \cap W = U' \cap W'$. Then $U = \big(U + (W \cap U')\big) \cap \big(U + (W \cap W')\big)$.

2.5. Let K be a field and let $K[X]$ be the set of polynomials with coefficients in K. Let Φ denote the (evaluation) map $\Phi : K[X] \to K^K$ defined by $F(X) \mapsto (a \mapsto F(a))$. Show that

a). Φ is injective if and only if K is not finite. (**Hint:** Use T2.3-b)-(3))

b). Φ is surjective if and only if K is finite. (**Hint:** Remember *Polynomial interpolation*! See T2.5)

On the other side one can see (simple) test-exercises ; their solutions need not be submitted.

---

[1]) A function $f : \mathbb{R} \to \mathbb{K}$ is called even if $f(-x) = f(x)$ for all $x \in \mathbb{R}$ and is called odd if $f(-x) = -f(x)$ for all $x \in \mathbb{R}$.

Test-Exercises

T2.1. Let V be a vector space over a field K.

a). (General Distributive law) For arbitrary finite families a_i, $i \in I$, in K and x_j, $j \in J$, in V, show that

$$\Big(\sum_{i\in I} a_i\Big)\Big(\sum_{j\in J} x_j\Big) = \sum_{(i,j)\in I\times J} a_i x_j\,.$$

b). (Sign Rules) For arbitrary elements $a, b \in K$ and arbitrary vectors $x, y \in V$. Prove that:

(1) $0\cdot x = a\cdot 0 = 0$. (2) $a(-x) = (-a)x = -(ax)$. (3) $(-a)(-x) = ax$.

(4) $a(x-y) = ax - ay$ and $(a-b)x = ax - bx$.

c). (Cancellation Rule) Let $a \in K$ and let $x \in V$. If $ax = 0$ then $a = 0$ or $x = 0$.

T2.2. Recall the concepts *convergent sequence, null- sequence, Cauchy sequence, bounded sequence* and *limit point of a sequence.* [2])

a). Let $(\mathbb{R}^{\mathbb{N}})_{\text{conv}}$ (respectively, $(\mathbb{R}^{\mathbb{N}})_{\text{null}}$, $(\mathbb{R}^{\mathbb{N}})_{\text{Cauchy}}$, $(\mathbb{R}^{\mathbb{N}})_{\text{bdd}}$, $(\mathbb{R}^{\mathbb{N}})_{\text{lpt}}$, $(\mathbb{R}^{\mathbb{N}})_{\text{const}}$) denote the set of all convergent (respectively, null-sequences, Cauchy sequences, bounded sequences, sequences with exactly one limit point). Which of these are subspaces of the $\mathbb{R}$-vector space $\mathbb{R}^{\mathbb{N}}$ of all sequences of real numbers?

b). Verify the inclusions and equalities in the following diagram:

$$\begin{array}{ccccccccc}
\mathbb{R}^{\mathbb{N}} & \supseteq & (\mathbb{R}^{\mathbb{N}})_{\text{bdd}} & & & & & & \\
\cup\!| & & \cup\!| & & & & & & \\
(\mathbb{R}^{\mathbb{N}})_{\text{lpt}} & \supseteq & (\mathbb{R}^{\mathbb{N}})_{\text{lpt}} \cap (\mathbb{R}^{\mathbb{N}})_{\text{bdd}} & = & (\mathbb{R}^{\mathbb{N}})_{\text{Cauchy}} & = & (\mathbb{R}^{\mathbb{N}})_{\text{conv}} & \supseteq & (\mathbb{R}^{\mathbb{N}})_{\text{const}} \\
 & & & & & & \cup\!| & & \\
 & & & & & & (\mathbb{R}^{\mathbb{N}})_{\text{null}} & &
\end{array}$$

c). Let $I \subseteq \mathbb{R}$ be an interval and let $a_0, \ldots, a_{n-1}$ be complex valued continuous functions on I. The set of all functions $y \in C^n_{\mathbb{C}}(I)$ satisfying the (homogeneous linear) differential equation

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1\dot{y} + a_0 y = 0$$

is a $\mathbb{C}$-subspace of $C^n_{\mathbb{C}}(I)$.

T2.3. a). (Division algorithm for polynomials) Let F and G be polynomials over a coomutative ring A. Suppose that $G \neq 0$ and the leading coefficient of G is a unit in A. Then there exist unique polynomials Q and R over A such that

$$F = QG + R \ \text{ and } \ \deg R < \deg G\,.$$

---

[2]) A sequence $(x_n) = (x_n)_{n\in\mathbb{N}}$ of elements of $\mathbb{K}$ is called convergent (in $\mathbb{K}$) if there exists an element $x \in \mathbb{K}$ which satisfy the following property: For every positive (however small) real number $\varepsilon \in \mathbb{R}$ there exists a natural number $n_0 \in \mathbb{N}$ such that $|x_n - x| \le \varepsilon$ for all natural numbers $n \ge n_0$. This element x is uniquely determined by the sequence (x_n) and is called the limit of the sequence (x_n); usually denoted by $\lim x_n = \lim_{n\to\infty} x_n$. If x is the limit of (x_n), then this is also shortly written as

$$x_n \to x \quad \text{or} \quad x_n \xrightarrow{n\to\infty} x$$

and say that (x_n) converges to x. The sequence (x_n) converges to x if and only if the sequence $(x_n - x)$ converges to 0. A convergent sequence with limit 0 is called a null-sequence. A sequence that is not convergent is called divergent.

A sequence $(x_n) = (x_n)_{n\in\mathbb{N}}$ of elements of $\mathbb{K}$ is called bounded sequence if there exists an element S in $\mathbb{R}$ such that $|x_n| \le S$ for all $n \in \mathbb{N}$.

A sequence $(x_n) = (x_n)_{n\in\mathbb{N}}$ of elements of $\mathbb{K}$ is called a Cauchy sequence if for every $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, there exists a natural number $n_0 \in \mathbb{N}$ $|x_m - x_n| \le \varepsilon$ for all natural numbers $m, n \ge n_0$.

An element $x \in \mathbb{K}$ is called a limit point of the sequence $(x_n) = (x_n)_{n\in\mathbb{N}}$ of elements of $\mathbb{K}$ if it is a limit point of the set $\{x_n \mid n \in \mathbb{N}\}$, i.e. every (however small) neighbourbood of x contain infinitely many terms of the sequence.

In particular, if $a \in A$, then $F = F(a) + Q(X-a)$, where Q is a polynomial over A. We say that $a \in A$ is a zero of F if $F(a) = 0$. Therefore $a \in A$ is a zero of F if and only if $X - a$ divide F (in $A[X]$).

b). Let A be an integral domain and let $F \in A[X]$, $F \neq 0$ be a polynomial of degree d in indeterminate X over A. Then

(1) F has atmost d zeros in A.
(2) F is uniquely determined by its values on $m+1$ distinct elements of A, where $m \geq d$.
(3) How many zeros the polynomial $X^2 + X$ has in the ring $\mathbb{Z}_4$?
(4) The polynomial $X^3 + X^2 + X + 1$ in $\mathbb{Z}_4[X]$ is amultiple of $X+1$ and $X+3$, but not of $(X+1)(X+3)$.

T2.4. (Horner's scheme) Let K be a field and let $F = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$. To compute the value of F at a point a one can apply the well-known Horner's scheme. For this define a sequence of polynomials recursively as follows:

$$\begin{aligned} F_0 &:= a_n \\ F_1 &:= XF_0 + a_{n-1} = a_n X + a_{n-1} \\ F_2 &:= XF_1 + a_{n-2} = a_n X^2 + a_{n-1} X + \cdots + a_{n-2} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ F_n &:= Xf_{n-1} + a_0 = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = F\,. \end{aligned}$$

These polynomials are called the Ruffini's polynomials corresponding to F. The values $F_0(a), \ldots, F_n(a)$ can be easily computed one after the another by using the division algorithm by $X - a$. Then $F = Q \cdot (X-a) + F(a)$ where $Q = F_0(a)X^{n-1} + F_1(a)X^{n-2} + \cdots + F_{n-1}(a)$, $F(a) = F_n(a)$. With this process also one can easily compute all coefficients b_ν in the *Taylor's expansion*:

$$F = b_0 + b_1(X-a) + \cdots + b_n(X-a)^n\,, \quad b_0 = F(a)\,,$$

for this one has to repeat the above process for the polynomial Q instead of F and hence $b_1 = Q(a)$, and so on. For example, the polynomial $F = 2X^3 + 2X^2 - X + 1$ and $a = -2$ we have the following scheme:

	2	2	−1	1
−2	2	−2	3	−5(= b_0)
−2	2	−6	15(= b_1)	
−2	2	−10(= b_2)		
−2	2(= b_3)			

Therefore $F = 2(X+2)^3 - 10(X+2)^2 + 15(X+2) - 5$.

T2.5. (Polynomial interpolation) Let A be an integral domain and let $m \in \mathbb{N}$. The existence of a polynomial $f \in A[X]$ of degree $\leq m$ which has given $m+1$ values (in A) at distinct $m+1$ places is called an interpolation problem. We shall only consider the case when $A = K$ is a field. [3])

a). (Lagrange's interpolation formula) Let $a_0, \ldots, a_m \in K$ be distinct and let $b_0, \ldots, b_m \in K$ be given. Then

$$f := \sum_{i=0}^{m} \frac{b_i}{c_i} \prod_{j \in \{0,\ldots,m\} \setminus \{i\}} (X - a_j)\,,\; c_i := \prod_{j \in \{0,\ldots,m\} \setminus \{i\}} (a_i - a_j)$$

is the unique polynomial (by T2.3-b)-(2)) of degree $\leq m$ such that $f(a_i) = b_i$ for all $i = 0, \ldots, m$.

b). (Newton's interpolation) Let $f_0 := 1$, $f_1 := X - a_0$, $f_2 := (X-a_0)(X-a_1), \ldots, f_m := (X-a_0)\cdots(X-a_{m-1})$. Then, since $f_j(a_j) \neq 0$, we can recursively find the coefficients $\alpha_0, \ldots, \alpha_m \in K$ such that

$$\left(\sum_{j=0}^{r} \alpha_j f_j \right)(a_r) = b_r\,,\; 0 \leq r \leq m\,.$$

The polynomials $\sum_{j=0}^{r} \alpha_j f_j$ have degree $\leq r$ and values b_i at the points a_i for all $i = 0, \ldots, m$.

[3]) Let A be an integral domain, $a_0, \ldots, a_m \in A$ be distinct and let $b_0, \ldots, b_m \in A$ be given. Then we can construct (by using the Newton's interpolation) an interpolation polynomial over the quotient field K of A by the above recursion process. This polynomial has coefficients in A if and only if $\alpha_0, \ldots, \alpha_m \in A$ (proof!).

T2.6. (Rational functions in one variable over a field) Let K be a field. The quotient of two polynomials over K are called the rational functions in one variable X over K. Therefore a rational function in one variable X over K is of the form F/G with $F, G \in K[X]$. The set of rational function in one variable X over K is denoted by $K(X)$.

a). Sum and product of rational functions are again rational functions and so $K(X)$ is a vector space over K and $K[X]$ is a K-subspace of $K(X)$. Further, $K(X)$ this is a field, this field [4]) is called the rational function field in one variable X over K.

b). Every rational function F/G in one indeterminate X over K can also be represented as $F/G = Q + R/G$, where Q and R are polynomials over K with $\deg R < \deg G$.

c). (Partial fraction decomposition) Let F and G be polynomials over K with $\deg F < \deg G$ and $F = (X-\alpha_1)^{n_1} \cdots (X-\alpha_r)^{n_r}$, $\alpha_i \neq \alpha_j$ for $i \neq j$, $n_i \in \mathbb{N}^*$. Then there exists a unique representation

$$\frac{F}{G} = \frac{\alpha_{11}}{(X-\alpha_1)} + \frac{\alpha_{12}}{(X-\alpha_1)^2} + \cdots + \frac{\alpha_{1n_1}}{(X-\alpha_1)^{n_1}} + \cdots\cdots + \frac{\alpha_{r1}}{(X-\alpha_r)} + \frac{\alpha_{r2}}{(X-\alpha_r)^2} + \cdots + \frac{\alpha_{rn_r}}{(X-\alpha_r)^{n_r}}.$$

with $\alpha_{ik} \in K$, $i = 1, \ldots, r$; $k = 1, \ldots, n_i$.

[4]) In fact the *quotient field* of the integral domain $K[X]$.