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/...

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 ; 11:00–12:30 **Venue:** CSA, Lecture Hall (Room No. 117)

Corrections by : **Nikhil Gupta** (nikhil.gupta@csa.iisc.ernet.in ; **Lab No.: 303**) /
Vineet Nair (vineetn90@gmail.com ; **Lab No.: 303**) /
Rahul Gupta (rahul.gupta@csa.iisc.ernet.in ; **Lab No.: 224**) /
Sayantan Mukherjee (meghanamande@gmail.com ; **Lab No.: 253**) /
Palash Dey (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)						
	Grade S	**Grade A**	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	> 90	76 — 90	61 — 75	46 — 60	35 — 45	< 35

	Grade A$^+$	**Grade A**	**Grade B$^+$**	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	> 90	81 — 90	71 — 80	61 — 70	51 — 60	40 — 50	< 40

Supplement 2

Vector Spaces

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!!

S2.1 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) (Cancelation Rule) Let $a \in K$ and let $x \in V$. If $ax = 0$ then $a = 0$ or $x = 0$.

S2.2 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 $ax := f^{-1}\big(af(x)\big)$.

S2.3 Let X be any set. Then the set-ring $(\mathfrak{P}(X), \Delta, \cap)$ of X 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 Supplement S1.9 (d).)

S2.4 Recall the concepts *convergent sequence*, *null- sequence*, *Cauchy sequence*, *bounded sequence* and *limit point of a sequence*.[1]

[1] 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 $x_n \to x$ or $x_n \to_{n\to\infty} x$ 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 $\mathbb{R}$

(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, constant sequences). 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 :

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

S2.5 (Polynomials—Polynomial ring) A polynomial (in one variable or indeterminate X) with coefficients in a commutative ring A or over A is a formal expression of the form :

$$F = F(X) = a_0 + a_1 X + \cdots + a_n X^n = \sum_{i \in \mathbb{N}} a_i X^i,$$

where $n \in \mathbb{N}$ and the coefficients $a_0, \ldots, a_n \in A$. The polynomial F over A is, by definition, uniquely determined by the coefficient tuple $(a_i)_{i \in \mathbb{N}} \in A^{(\mathbb{N})}$ (where we put $a_i = 0$ for $i \geq n$). Therefore, *we identify polynomial with its coefficient tuple.*

Two polynomials

$$F = \sum_{i \in \mathbb{N}} a_i X^i,\ (a_i) \in A^{(\mathbb{N})} \quad \text{and} \quad G = \sum_{i \in \mathbb{N}} b_i X^i,\ (b_i) \in A^{(\mathbb{N})}$$

can be added coefficient-wise, as the tuples are added in $A^{(\mathbb{N})}$:

$$F + G := \sum_{i \in \mathbb{N}} (a_i + b_i) X^i,$$

and multiplied by a scalar $a \in A$ also coefficient-wise :

$$aF := \sum_{i \in \mathbb{N}} a a_i X^i.$$

The multiplication of two polynomials is performed by using the formal distributive laws and expanding :

$$FG := \sum_{i \in \mathbb{N}} c_i X^i, \quad \text{where} \quad c_i := \sum_{j=0}^{i} a_j b_{i-j} = a_0 b_i + \cdots + a_i b_0,\ i \in \mathbb{N}.$$

An easy verification shows that : *The set of polynomials $A[X]$ with this A-module structure and the above multiplication is a commutative A - algebra.*[2] This A-algebra is called the polynomial algebra (in one variable) over A.

By definition X^m, $m \in \mathbb{N}$, is a A-basis of $A[X]$, this corresponds to the standard basis e_m, $m \in \mathbb{N}$, of $A^{(\mathbb{N})}$. Further, X^m is the m-th power of X in the A-algebra $A[X]$. The unit element in $A[X]$ is the constant polynomial 1 and we shall identify this with the unit element in K. Similarly, we identify the multiples $a \cdot 1 = a$, $a \in K$, with the elements $A \in K$. These elements a in K are called the constant polynomials.

If $F = \sum_{i \in \mathbb{N}} a_i X^i$, $(a_i) \in A^{(\mathbb{N})}$, is a non-zero polynomial in $A[X]$ and if $a_n \neq 0$, but $a_m = 0$ for all $m > n$, then $F = a_0 + a_1 X + \cdots + a_n X^n$, $a_n \neq 0$, and hence n is called the degree of F abd a_n is called the leading coefficient of F. If the leading coefficent of a polynomial F is 1,

---

such that $|x_n| \leq S$ 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 $n_0 \in \mathbb{N}$ $|x_m - x_n| \leq \varepsilon$ for all natural numbers $m, n \geq n_0$.

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.

[2] Let A be a commutative ring. An A-module B on which multiplication $B \times B \to B$ is defined is called an A - algebra if the following compatibility conditions are satisfied : (1) With the A-module-addition and the given multiplication B is a ring. (2) For all $A, b \in A$ and all $x, y \in B$, $(ax)(by) = (ab)(xy)$.

then f is called m o n i c. The degree of the zero polynomial is by definition $-\infty$. The polynomials of degree 0 are precisely non-zero constant polynomials. The degree of a polynomial is denoted by $\deg F$.

Let $A = K$ be a field.

(a) For polynomials $F, G \in A[X]$, we have :

$$\deg(F+G) \leq \max\{\deg F, \deg G\} \text{ and } \deg(FG) \leq \deg F + \deg G.$$

Moreover, the second inequality is an equality if either the leading coefficient of F or of G is a non-zero divisor in A. (Recall that an element $a \in A$ in a (commutative) ring A is called a z e r o d i v i s o r if there exists $b \in A$, $b \neq 0$ with $ab = 0$; An element which is not a zero divisor is called a n o n - z e r o d i v i s o r in A. For example, in the ring $\mathbb{Z}_n$ residue classes of divisors of n are precisely zero divisors. In the ring of integers $\mathbb{Z}$ every non-zero element is a non-zero divisor. In a field every non-zero element is a unit and hence a non-zero divisor. More generally, every unit in any commutative ring is a non-zero divisor. A commutative ring which does not have any non-zero zero divisors is called an i n t e g r a l d o m a i n. For example, the ring of integers $\mathbb{Z}$ is an integral domain and every field K is an integral domain.)

If A is an integral domain, then the unit group $A[X]^\times$ of the polynomial ring $A[X]$ is the unit group of the ring A, i. e. $A[X]^\times = A^\times$. In particular, a non-zero polynomial $F \in K[X]$ over a field K is a unit in $K[X]$ if and only if it is a non-zero constant polynomial. In particular, X is never a unit in $K[X]$ and hence $K[X]$ is never a field.

The n-dimensional K-subspace of the polynomials in $K[X]$ of degrees $< n$ is denoted by $K[X]_n$; $1, X, \ldots, X^{n-1}$ is a K-basis of $K[X]_n$.

(b) (D i v i s i o n w i t h r e m a i n d e r) Let K be a field. As in the case of integers, we have division with remainder in $K[X]$. Let F and $G \neq 0$ be polynomials over a field K. Then there exist unique polynomials Q and R over K such that

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

The polynomial Q is called the q u o t i e n t and the polynomial R is called the r e m a i n d e r of the division of F by G. In particular, if $a \in K$, then $F = F(a) + Q(X-a)$, where Q is a polynomial over K. (**Remark :** More generally, one can perform division with remainder over arbitrary commutative ring by the polynomial G if the leading coefficient of G is a unit in A.)

(c) (E u c l i d e a n a l g o r i t h m) As in the case of integers, we have the E u c l i d e a n a l g o r i t h m : Let F and G be polynomials in $K[X]$, $G \neq 0$. We put $R_0 := F$ and $R_1 := G$ and define polynomials $R_2, \ldots, R_{k+1} \in K[X]$ by recursion :

$$\begin{aligned}
R_0 &= Q_1 R_1 + R_2, && 0 < \deg R_2 < \deg R_1;\\
R_1 &= Q_2 R_2 + R_3, && 0 < \deg R_3 < \deg R_2;\\
&\ldots \quad \ldots \quad \ldots && \ldots \quad \ldots \quad \ldots\\
R_{k-1} &= Q_k R_k + R_{k+1}, && 0 < \deg R_{k+1} < \deg R_k;\\
R_k &= Q_{k+1} R_{k+1}.
\end{aligned}$$

The polynomial R_{k+1} is the last non-zero remainder and as in the case of integers, we also have :

$$R_{k+1} = \gcd(F, G).$$

(**Remark :** Note that $\gcd(F,G)$ denote a g r e a t e s t c o m m o n d i v i s o r of F and G; this is a common divisor of F and G which is divisible by every other common divisor. Two greatest common divisors of F and G divide each other and hence on the degree argument (see) they differ by a non-zero constant. The greatest common divisor of the polynomials F and G (at least one of which is $\neq 0$; otherwise $\gcd(F,G) = 0$) is therefore only up to a non-zero constant, uniquely determined. Choose a greatest common divisor which is a monic polynomial, so that it is uniquely determined.)

Two polynomials F and G in $K[X]$ are called r e l a t i v e l y p r i m e if $\gcd(F,G) = 1$. Euclidean algorithm implies much more, with its help, we get :

(d) (B e z o u t ' s L e m m a) For two polynomials F and G in $K[X]$, there exist polynomials $S, T \in K[X]$ such that

$$\gcd(F,G) = SF + TG,$$

In particular, if F and G are relatively polynomials in $K[X]$, then there exist polynomials $S, T \in K[X]$ such that $1 = SF + TG$. (**Hint :** Similar to that of the case of integers.)

(e) (Prime polynomials) A polynomial $P \in K[X]$ is called a prime polynomial or just prime if $\deg P \geq 1$ and every divisor of P is constant or a multiple aP, $a \in K^\times$ of P. (Clearly a polynomial $P \in K[X]$ of degree ≥ 1 is prime if and only if there is no decomposition $P = FG$ of P as a product of polynomials $F, G \in K[X]$ of degrees $< \deg P$. Prime polynomials are therefore also indecomposable of irreducible. If P is a prime polynomial which does not divide the polynomial $F \in K[X]$, then $\gcd(F,P) = 1$.)

(f) (Lemma of Euclid) If a prime polynomial $P \in K[X]$ divide a product $F_1 \cdots F_r$ of polynomials $F_1, \ldots, F_r \in K[X]$, then P divides at least one of the factor $F_1, \ldots, F_r$. (**Hint :** Follows from the Bezout's Lemma.)

(g) (Theorem on the uniqueness of prime factorization in $K[X]$) Every polynomial $F \in K[X]$ with $\deg F \geq 1$ can be written as a product of prime polynomials. Moreover, the prime factors are uniquely determined, up to permutation and up to multiplication by constants, by F.

Collecting together same prime factors, we obtain prime polynomial poweres to get the canonical prime factorisation: Let $\mathcal{P} = \mathcal{P}(K[X])$ be the set of monic prime polynomials in $K[X]$. For every polynomial $F \in K[X]$, $F \neq 0$, there exist natural numbers ν_P, $P \in \mathcal{P}$, (almost all of which are 0) such that

$$F = a \prod_{P \in \mathcal{P}} P^{\nu_P}.$$

The element $a \in K$ is necessarily the leading coefficient of F. The exponent ν_P is called the multiplicity of P in F. In the monic polynomials $P \in \mathcal{P}$, there are, in particular, the linear factors $X - c$, $c \in K$.

S2.6 (Zeros of polynomials) Let K be a field. An element $a \in K$ is called a zero of the polynomial $F \in K[X]$ if $F(a) = 0$.

(a) Let $a \in K$ and let $F \in K[X]$. Then a is a zero of F if and only if $X - a$ is a factor of F (in $K[X]$).

(b) Let $F \in K[X]$, $F \neq 0$, and

$$F = a \prod_{c \in K} (X - c)^{\nu_c} \prod_{P \in \mathcal{P}, \deg P \geq 2} P^{\nu_P}.$$

be the canonical prime factorization of F, then by (a) for an element $c \in K$ the multiplicity ν_c of the linear factor $X - c$ is > 0 if and only if c is a zero of F. For $c \in K$, ν_c is also called the multiplicity of the zero c ($\nu_c = 0$ mean c is not a zero of F). Obviously,

$$\sum_{c \in K} \nu_c \leq \deg F.$$

Moreover, the above inequality is equality if and only if F has no prime factors of degrees ≥ 2.

(c) A polynomial $F \in K[X]$ of degree $n \geq 0$ has at most n zeros in K, even if these zeros are counted with their multiplicities.

For example, all non-zero elements in $\mathbf{K}_p$ are zeros of the polynomial $X^{p-1} - 1$ (by Fermat's Little Theorem). Therefore: $X^{p-1} - 1 = \prod_{k=1}^{p-1} (X - k)$. In particular, we get the well-known Wilson's formula: $-1 \equiv (p-1)! \pmod{p}$.

More generally, if K is a finite field with n elements, then $x^{n-1} = 1$ for every $x \in K^\times$ and the equation $X^{n-1} - 1 = \prod_{x \in K^\times} (X - x)$. In particular, $-1 = \prod_{x \in K^\times} x$ and $\prod_{x \in K} (X - x) = X(X^{n-1} - 1) = X^n - X$.

How many zeros the polynomial $X^2 + X$ has in the ring $\mathbb{Z}_4$? The polynomial $X^3 + X^2 + X + 1$ in $\mathbb{Z}_4[X]$ is a multiple of $X + 1$ and $X + 3$, but not of $(X + 1)(X + 3)$. Give an example of a polynomial $F \in A[X]$ over a commutative ring A such that F has infinitely many zeros in A.

(d) (Identity Theorem for Polynomials) Let $F, G \in K[X]$ be two polynomials of degrees $\leq n$. Suppose that there exist distinct $t_1, \ldots, t_{n+1} \in K$ such that $F(t_i) = G(t_i)$ for all $i = 1, \ldots, n+1$. Then $F = G$. (**Hint :** Since $t_1, \ldots, t_{n+1} \in K$ are zeros of the polynomial $F - G$ of degree $\deg(F - G) \leq n$, it follows that $F - G = 0$ by (c).)

From Identity Theorem it follows that: *If K is an infinite field, then distinct polynomials define distinct polynomial functions. Therefore in this case, we may identify polynomials with the corresponding polynomial functions.*

(e) From the Nullstellensatz of Bolzano[3] we have:

Theorem *A real polynomial $F \in \mathbb{R}[X]$ of odd degree has at least one zero in $\mathbb{R}$.*

(f) If there is no prime polynomial in $K[X]$ of degree ≥ 2, then every polynomial $F \in K[X]$, $F \neq 0$, has the prime factorization $F = a\prod_{c\in K}(X-c)^{\nu_c}$ into only linear factors. This is exactly the case if every polynomial of degree ≥ 1 in $K[X]$ has at least one zero in K (since prime polynomial of degree ≥ 2 cannot have zero in K).

(g) A field K is called algebraically closed if every non-constant polynomial $F \in K[X]$ has a zero in K. With this definition, the Fundamental Theorem of Algebra can be formulated as follows:

Theorem (FTA — d'Alembert (1748)-Gauss (1899)) *The field $\mathbb{C}$ of complex numbers is algebraically closed. In particular, every polynomial $F \neq 0$ in $\mathbb{C}[X]$ with leading coefficient $a \in \mathbb{C}$, (up to an order) there exists uniquely determined pairwise distinct complex numbers $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$ with multiplicities $n_1, \ldots, n_r \in \mathbb{N}^*$ such that:*

$$F = a(X-\alpha_1)^{n_1}\cdots(X-\alpha_r)^{n_r}.$$

(h) The field $\mathbb{R}$ of real numbers is not algebraically closed, since the polynomial X^2+1 has no zero in $\mathbb{R}$ and hence it is a prime polynomial. From the assertion in the above theorem one can also get a finier decomposition for non-zero real polynomials, namely, if $F \in \mathbb{R}[X] \subseteq \mathbb{C}[X]$ is a non-zero real polynomial which has the decomposition over $\mathbb{C}$:

$$F = a(X-\alpha_1)^{n_1}\cdots(X-\alpha_r)^{n_r}$$

with $a \in \mathbb{R}$, $\alpha_1, \alpha_r \in \mathbb{C}$, then by conjugating, we also get the decomposition

$$F = a(X-\overline{\alpha}_1)^{n_1}\cdots(X-\overline{\alpha}_r)^{n_r}.$$

The uniqueness in the above theorem shows that: for every zero $\alpha \in \mathbb{C}\setminus\mathbb{R}$ of F, its conjugate $\overline{\alpha}$ is also a zero of F with the same multiplicity as that of α. Further, since

$$(X-\alpha)(X-\overline{\alpha}) = X^2 - 2(\operatorname{Re}\alpha) + |\alpha|^2 \in \mathbb{R}[X]$$

is a monic quadratic polynomial without real zeros, we have the following real-version of the Fundamental Theorem of Algebra:

Theorem (Real-Version of FTA) *Every real polynomial $F \neq 0$ in $\mathbb{R}[X]$ with leading coefficient $a \in \mathbb{R}$, (up to an order) there exists uniquely determined pairwise distinct real numbers $\alpha_1, \ldots, \alpha_s \in \mathbb{R}$ with multiplicities $n_1, \ldots, n_s \in \mathbb{N}^*$ and pairwise distinct monic quadratic polynomials $q_1, \ldots, q_t$ without any zeros in $\mathbb{R}$ with multiplicities $m_1, \ldots, m_t \in \mathbb{N}^*$ such that:*

$$F = a(X-\alpha_1)^{n_1}\cdots(X-\alpha_s)^{n_s}q_1^{m_1}\cdots q_t^{m_t}.$$

In particular, the monic prime polynomials in $\mathbb{R}[X]$ are precisely the polynomials:

$$X-c,\ c\in\mathbb{R}, \quad \text{and} \quad X^2+pX+q,\ p,q\in\mathbb{R} \ \text{ with } \ p^2-4q<0.$$

S2.7 (Horner's Scheme) Let K be a field and let $F = a_0 + a_1X + \cdots + a_nX^n \in K[X]$. 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:

$$\begin{aligned}
F_0 &:= a_n\\
F_1 &:= a_{n-1} + XF_0 = a_{n-1} + a_nX\\
&\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots\\
F_{k+1} &:= a_{n-k-1} + F_kX = a_{n-k-1} + \cdots + a_{n-1}X^k + a_nX^{k+1}\\
&\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots\\
F_n &:= a_0 + F_{n-1}X = F.
\end{aligned}$$

[3] **Theorem** (Nullstellensatz — Bolzano, (1817)) *Let $f : [a,b] \to \mathbb{R}$ be a continuous real-valued function on the closed interval $[a,b] \subseteq \mathbb{R}$. If $f(a)$ and $f(b)$ have different signs, then f has a zero x_0 in the interval $[a,b]$,* i.e., *there exists $x_0 \in [a,b]$ with $f(x_0) = 0$.*

These polynomials are called the Ruffini's polynomials corresponding to F. The value $F(a) = F_n(a)$ is then obtained by the recursion-scheme:

$$F_0(a) = a_n\,, \qquad F_{k+1}(a) = a_{n-k-1} + F_k(a)a\,, \quad k = 0,\dots,n-1$$

The values $F_0(a),\dots,F_n(a)$ can be easily computed one after the another and the division algorithm by $X-a$ is given by

$$F = Q\cdot(X-a) + F(a) \quad \text{where} \quad Q = F_0(a)X^{n-1} + F_1(a)X^{n-2} + \cdots + F_{n-1}(a)\,,\ F(a) = F_n(a)\,.$$

With this process also one can easily compute all coefficients b_ν in the *Taylor's expansion* :

$$F = b_0 + b_1(X-a) + \cdots + b_n(X-a)^n\,,\ b_k = F^{(k)}(a)/k!\,,$$

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

S2.8 (Polynomial Interpolation) Let K be a field and let $m \in \mathbb{N}$. The existence of a polynomial $f \in K[X]$ of degree $\le m$ which has given $m+1$ values (in K) at distinct $m+1$ places is called an interpolation problem.

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

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

is the unique polynomial (by the Identity Theorem Supplement S2.6 (d)) of degree $\le m$ such that $f(a_i) = b_i$ for all $i = 0,\dots,m$.

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

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

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

S2.9 (Polynomial Functions) Let K be a field and let $D \subseteq K$ be a subset of K. A function $f : D \to K$ is called a polynomial function if it is of the form $t \mapsto f(t) := a_0 + a_1 t + \cdots + a_n t^n$, $t \in D$, with fixed coefficients $a_0, a_1, \dots, a_n \in K$.

(a) The set of all polynomial functions $\mathrm{Pol}_K(D)$ form a K-subspace of the K-vector space K^D. Moreover, if $K = \mathbb{K}$ and if $D = I \subseteq \mathbb{R}$ is an interval with more than one point, then $\mathrm{Pol}_{\mathbb{K}}(I) \subseteq \mathrm{C}^\omega_{\mathbb{K}}(I)$.

(b) If D is a finite subset of K, then every K-valued function on D is a polynomials function, i. e. $K^D = \mathrm{Pol}_K(D)$. (**Hint :** Use Lagrange-Interpolation Supplement S2.8 (a).)

(c) If D is an infinite set, then the coefficients $a_0, a_1, \dots, a_n \in K$ of the polynomial function $f : D \to K$, $t \mapsto a_0 + a_1 t + \cdots + a_n t^n$ are uniquely determined by the function f.

(d) The functions $\mathbb{R} \to \mathbb{R}$, $x \mapsto |x|$; $x \mapsto \sin x$; $x \mapsto \cos x$ are not polynomial functions. Is the exponential function $x \mapsto e^x$ a polynomial function?

†**S2.10** (Function Spaces) Let $\mathbb{K}$ be either $\mathbb{R}$ or $\mathbb{C}$ and let $D \subseteq \mathbb{K}$ be an arbitrary subset.

(a) The set

$$\mathrm{C}^0_{\mathbb{K}}(D) := \{f : D \to \mathbb{K} \mid f \text{ is continuous}\}$$

of all $\mathbb{K}$-valued continuous functions on D is a $\mathbb{K}$-subspace of all $\mathbb{K}$-valued functions $\mathbb{K}^D$ on D.

(b) Let $I \subseteq \mathbb{R}$ be an interval in $\mathbb{R}$ with more than one point and let $n \in \mathbb{N}$. The set

$$\mathrm{C}^n_{\mathbb{K}}(I) := \{f : I \to \mathbb{K} \mid f \text{ is } n-\text{timescontinuously differnetiable}\}$$

of all $\mathbb{K}$-valued n-times continuously differentiable functions on I is a $\mathbb{K}$-subspace the $\mathbb{K}$-vector space $\mathrm{C}^0_{\mathbb{K}}(D)$. The $\mathbb{K}$-subspaces $\mathrm{C}^n_{\mathbb{K}}(I)$, $n \in \mathbb{N}$ form a descending chain

$$\mathrm{C}^0_{\mathbb{K}}(I) \supsetneq \mathrm{C}^1_{\mathbb{K}}(I) \supsetneq \mathrm{C}^2_{\mathbb{K}}(I) \supsetneq \cdots \supsetneq \mathrm{C}^n_{\mathbb{K}}(I) \supsetneq \mathrm{C}^{n+1}_{\mathbb{K}}(I) \supsetneq \cdots$$

where all inclusions are proper. The intersection of these K-subspaces is the K-subspace

$$\mathrm{C}^\infty_{\mathbb{K}}(I) = \bigcap_{n\in\mathbb{N}} \mathrm{C}^n_{\mathbb{K}}(I)$$

of all infinitely many times differentiable $\mathbb{K}$-valued functions on I. Further, the set

$$\mathrm{C}^\omega_{\mathbb{K}}(I) := \{f : I \to \mathbb{K} \mid f \text{ is analytic}\}$$

of all $\mathbb{K}$-valued analytic functions on I is a $\mathbb{K}$-subspace the $\mathbb{K}$-vector space $\mathrm{C}^\infty_{\mathbb{K}}(I)$. Moreover, the inclusion $\mathrm{C}^\omega_{\mathbb{K}}(I) \subsetneq \mathrm{C}^\infty_{\mathbb{K}}(I)$ is proper. (This follows from the existence of a "*flat functions*")

(c) Let $I \subseteq \mathbb{R}$ be an interval with more than one point and let $a_0, \ldots, a_{n-1}$ be complex valued continuous functions on I. The set of all functions $y \in \mathrm{C}^n_{\mathbb{C}}(I)$ 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 $\mathrm{C}^n_{\mathbb{C}}(I)$.