GAZETA MATEMATICĂ

SERIA A

ANUL XXVIV(CVIII) **Nr. 3 – 4/ 2011**

ARTICOLE

On exponential convergence of linear recurrence sequences

Mihail Megan[1)], Traian Ceauşu[2)], Ioan-Lucian Popa[3)]

Abstract. In this paper we investigate some exponential convergence concepts for linear recurrence sequences. Some illustrating examples clarify the connections between these concepts.

Keywords: exponential convergence, linear recurrence sequences.

MSC: 34D05

1. Introduction

A real sequence (x_n) defined by the recurrence relation

$$x_{n+1} = a_n x_n, \quad n \in \mathbb{N}, \tag{1}$$

where (a_n) is a given sequence of real numbers, is called the **linear recurrence sequence** generated by the sequence (a_n).

If there exists $k \in \mathbb{N}$ with $a_k = 0$ then $x_n = 0$ for every $n > k$. Let us further assume that $a_n \neq 0$ for any $n \in \mathbb{N}$ and $x_0 \neq 0$. Using these hypotheses we have that $x_n \neq 0$ for any $n \in \mathbb{N}$.

We observe that

$$x_1 = a_0 x_0, \quad x_2 = a_0 a_1 x_0, \quad \dots \quad , \quad x_n = a_0 a_1 \dots a_{n-1} x_0, \quad \dots$$

In what follows we will denote by

$$X_m^n \overset{def}{=} \frac{x_m}{x_n} = \begin{cases} a_n \cdot \ldots \cdot a_{m-1}, & m \geq n+1 \\ 1, & m = n. \end{cases} \tag{2}$$

for all $(m, n) \in \Delta \overset{def}{=} \{(m, n) \in \mathbb{N}^2 : m \geq n\}$.

[1)]Faculty of Mathematics and Computer Science, West University of Timişoara, megan@math.uvt.ro

[2)]Faculty of Mathematics and Computer Science, West University of Timişoara, ceausu@math.uvt.ro

[3)]Faculty of Mathematics and Computer Science, West University of Timişoara, popa@math.uvt.ro

The aim of this paper is to define and exemplify various concepts of convergence as uniform exponential convergence, nonuniform exponential convergence, exponential convergence, strong exponential convergence and to emphasize connections between them.

2. Uniform exponential convergence.

Let (x_n) be the linear recurrence sequence generated by the sequence (a_n).

Definition 1. *The sequence (x_n) is called **uniformly exponentially convergent to** 0, and we write $x_n \xrightarrow{u.e.s.} 0$, if there exist $N \geq 1$ and $\alpha > 0$ such that*

$$|x_m| \leq Ne^{-\alpha(m-n)}|x_n|, \quad \text{for all} \quad (m,n) \in \Delta.$$

Remark 1. It is obvious that if $x_n \xrightarrow{u.e.s.} 0$, then $x_n \to 0$. The following example shows that the converse implication is not valid.

Example 1. Let $x_0 = 1$ and $a_n = \mathrm{e}^{-\frac{1}{n+1}}$. We have that

$$x_n = e^{-\left(1+\frac{1}{2}+\ldots+\frac{1}{n}\right)} \longrightarrow 0.$$

If we suppose that $x_n \xrightarrow{u.e.s.} 0$, then the are some constants $N \geq 1$ and $\alpha > 0$ with

$$\mathrm{e}^{-\left(1+\frac{1}{2}+\ldots+\frac{1}{m}\right)} \leq N\mathrm{e}^{-\alpha m}.$$

This implies

$$\frac{\alpha m}{1+\frac{1}{2}+\ldots+\frac{1}{m}} \leq 1+\ln N.$$

Using Stolz-Cesàro theorem we obtain

$$\infty = \lim_{m\to\infty} \frac{\alpha m}{1+\frac{1}{2}+\ldots+\frac{1}{m}} \leq 1+\ln N,$$

which is a contradiction.

Proposition 1. *For every linear recurrence sequence (x_n) the following statements are equivalent:*

(i) $x_n \xrightarrow{u.e.s.} 0$;

(ii) there are two constants $N \geq 1$ and $\alpha > 0$ such that

$$|X_m^n| \leq Ne^{-\alpha(m-n)}, \quad \text{for all} \quad (m,n) \in \Delta;$$

(iii) there exist $N \geq 1$ and $r \in (0,1)$ such that

$$|X_m^n| \leq Nr^{m-n}, \quad \text{for all} \quad (m,n) \in \Delta.$$

(iv) there exist a constant $N \geq 1$ and a nondecreasing sequence of real numbers $(b_n)_n \subset (0,1]$ with $\lim\limits_{n\to\infty} b_n = 0$ such that

$$|X_m^n| \leq Nb_{m-n}, \quad \text{for all} \quad (m,n) \in \Delta.$$

Proof. The implications $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv)$ are trivial.

$(iv) \Rightarrow (i)$ We observe that if $\lim\limits_{n\to\infty} b_n = 0$, then there exists $k \in \mathbb{N}^*$ such that $Nb_k < 1$. Let $(m,n) \in \Delta$. There are $s, r \in \mathbb{N}$ with $r \in [0,k)$ such that $m - n = ks + r$. Let $\alpha = -\dfrac{\ln(Nb_k)}{k} > 0$. If $s = 0$, then

$$|X_m^n| \le Nb_r \le Ne^{\alpha r}e^{-\alpha r} \le N\mathrm{e}^{\alpha k}\mathrm{e}^{-\alpha(m-n)} =$$
$$= N\mathrm{e}^{-\ln(Nb_k)}\mathrm{e}^{-\alpha(m-n)} = \frac{\mathrm{e}^{-\alpha(m-n)}}{b_k}.$$

For the case $s \in \mathbb{N}^*$ using

$$n < n+k < n+2k < \ldots < n+(s-1)k < n+sk \le m$$

we obtain

$$\begin{aligned}
|X_m^n| &= |X_{n+sk}^n|\ |X_m^{n+sk}| \le\ Nb_r|X_{n+sk}^n| \le \\
&= N|X_{n+(s-1)k}^n|\ |X_{n+sk}^{n+(s-1)k}| \le N(Nb_k)|X_{n+(s-1)k}^n| \le \\
&\le N(Nb_k)^2|X_{n+(s-2)k}^n| \le \ldots \le N(Nb_k)^s = \\
&= Ne^{s\ln(Nb_k)} = Ne^{-\alpha ks} = N\mathrm{e}^{-\alpha(m-n-r)} = \\
&= N\mathrm{e}^{\alpha r}\mathrm{e}^{-\alpha(m-n)} < N\mathrm{e}^{\alpha k}\mathrm{e}^{-\alpha(m-n)} = \frac{\mathrm{e}^{-\alpha(m-n)}}{b_k}.
\end{aligned}$$

This shows that there are $M = \dfrac{1}{b_k} \ge 1$ and $\alpha = -\dfrac{\ln(Nb_k)}{k} > 0$ such that

$$|X_m^n| \le m\mathrm{e}^{-\alpha(m-n)}, \quad \text{for all} \quad (m,n) \in \Delta.$$

□

Theorem 2. *For every linear recurrence sequence (x_n) the following statements are equivalent:*

(i) $x_n \xrightarrow{u.e.s.} 0$;

(ii) there are some constants $D \ge 1$ and $d > 0$ such that

$$\sum_{m=n}^{\infty} \mathrm{e}^{d(m-n)}|X_m^n| \le D, \quad \textit{for all} \quad n \in \mathbb{N};$$

(iii) there is a constant $D \ge 1$ such that

$$\sum_{m=n}^{\infty} |X_m^n| \le D, \quad \textit{for all} \quad n \in \mathbb{N}.$$

Proof. $(i) \Rightarrow (ii)$ Let $n \in \mathbb{N}$. By our hypothesis there are $N \geq 1$ and $\alpha > 0$ such that for all $d \in (0, \alpha)$ we have that

$$\sum_{m=n}^{\infty} \mathrm{e}^{d(m-n)} |X_m^n| \leq \sum_{m=n}^{\infty} N \mathrm{e}^{-(\alpha-d)(m-n)} = \frac{N\mathrm{e}^{\alpha}}{\mathrm{e}^{\alpha} - \mathrm{e}^{d}} = D.$$

$(ii) \Rightarrow (iii)$ It is obvious.

$(iii) \Rightarrow (i)$ Let $(m, n) \in \Delta$. For any $k \in \mathbb{N}$ with $n \leq k \leq m$ we have that $|X_m^k| \leq D$. We deduce that

$$(m-n+1)|X_m^n| = \sum_{k=n}^{m} |X_m^n| = \sum_{k=n}^{m} |X_m^k| \, |X_k^n| \leq$$

$$\leq D \sum_{k=n}^{m} |X_k^n| \leq D \sum_{k=n}^{m} |X_k^n| = D^2 = N,$$

thus,

$$|X_m^n| \leq \frac{N}{m-n+1} = N b_{m-n},$$

where $b_n = \dfrac{1}{n+1}$, for all $n \in \mathbb{N}$. Using Proposition 1 we conclude that $x_n \xrightarrow{u.e.s.} 0$. □

Theorem 3. *For every linear recurrence sequence (x_n) the following statements are equivalent:*

(i) $x_n \xrightarrow{u.e.s.} 0$*;*

(ii) there are $B \geq 1$ *and* $b > 0$ *such that*

$$\sum_{k=0}^{m} \mathrm{e}^{b(m-k)} |X_m^k| \leq B, \quad \textit{for all} \quad m \in \mathbb{N};$$

(iii) there exists $B \geq 1$ *such that*

$$\sum_{k=0}^{m} |X_m^k| \leq B, \quad \textit{for all} \quad m \in \mathbb{N}.$$

Proof. $(i) \Rightarrow (ii)$ Let $m \in \mathbb{N}$. By our hypothesis there are $N \geq 1$ and $\alpha > 0$ such that for all $b \in (0, \alpha)$ we have that

$$\sum_{k=0}^{m} \mathrm{e}^{m-k} |X_m^k| \leq \sum_{k=0}^{m} N e^{-(\alpha-b)(m-k)} \leq \frac{N\mathrm{e}^{\alpha}}{\mathrm{e}^{\alpha} - \mathrm{e}^{b}} = B.$$

$(ii) \Rightarrow (iii)$ It is trivial.

$(iii) \Rightarrow (i)$ Let $(m,n) \in \Delta$. We have that $|X_k^n| \leq B$ for all $k \in \mathbb{N}$ with $n \leq k \leq m$. Thus, we obtain that

$$(m-n+1)|X_m^n| = \sum_{k=n}^{m} |X_m^n| = \sum_{k=n}^{m} |X_k^n|\,|X_m^k| \leq$$
$$\leq B \sum_{k=n}^{m} |X_m^k| \leq B \sum_{k=0}^{n} |X_m^k| = B^2 = N,$$

thus,

$$|X_m^n| \leq \frac{N}{m-n+1} = N b_{m-n},$$

where $b_n = \dfrac{1}{n+1}$, for all $n \in \mathbb{N}$. Using Proposition 1 we conclude that $x_n \xrightarrow{u.e.s.} 0$. □

A generalization of uniform exponential convergence is introduced by

3. Nonuniform exponential convergence.

Definition 2. *The linear recurrence sequence (x_n) is called* ***nonuniformly exponentially convergent to*** 0 *and we denote $x_n \xrightarrow{n.e.s.} 0$ if there exist a constant $\alpha > 0$ and a nondecreasing sequence of real numbers $N : \mathbb{N} \to [1, \infty)$ such that*

$$|x_m| \leq N(n) e^{-\alpha(m-n)} |x_n|, \quad \textit{for all} \quad (m,n) \in \Delta.$$

Remark 2. The linear recurrence sequence (x_n) is nonuniformly exponentially convergent to 0 if and only if there exist a constant $\alpha > 0$ and a nondecreasing sequence of real numbers $N : \mathbb{N} \to [1, \infty)$ such that

$$|X_m^n| \leq N(n) \mathrm{e}^{-\alpha(m-n)}, \quad \textit{for all} \quad (m,n) \in \Delta.$$

Remark 3. If the linear recurrent sequence (x_n) is nonuniformly exponentially convergent to 0 then there are a constant $\alpha > 0$ and a sequence of real numbers $N : \mathbb{N} \to [1, \infty)$ such that

$$|x_m| \leq N(0) \mathrm{e}^{-\alpha m}, \quad \textit{for all} \quad m \in \mathbb{N}.$$

Remark 4. It is obvious that

$$x_n \xrightarrow{u.e.s.} 0 \Rightarrow x_n \xrightarrow{n.e.s.} 0 \Rightarrow x_n \longrightarrow 0.$$

The converse implications are not valid. In this sense, we present:

Example 4. Let $c > 0$, $x_0 = 1$ and $a_n = \begin{cases} c\mathrm{e}^{-n} & \text{if} \quad n = 2k \\ c\mathrm{e}^{n+1} & \text{if} \quad n = 2k+1. \end{cases}$

We observe that

$$X_m^n = \begin{cases} c^{m-n} a_{mn}, & m > n \\ 1, & m = n, \end{cases}$$

where

$$a_{mn}=\begin{cases} \mathrm{e}^{m-n} & if \quad m=2q \quad \text{and} \quad n=2p \\ \mathrm{e}^{m} & if \quad m=2q \quad \text{and} \quad n=2p+1 \\ \mathrm{e}^{-n} & if \quad m=2q+1 \quad \text{and} \quad n=2p \\ 1 & if \quad m=2q+1 \quad \text{and} \quad n=2p+1. \end{cases}$$

We shall prove that

(i) the sequence (x_n) is not uniformly exponentially convergent to 0;

(ii) $x_n \xrightarrow{n.e.s.} 0$ if and only if $c \in (0, 1/e)$.

Firstly, if we suppose that the sequence $x_n \xrightarrow{u.e.s.} 0$, then there exist some constants $N \geq 1$ and $\alpha > 0$ such that $(ce^{\alpha})^{m-n} a_{mn} \leq N$, for all $(m,n) \in \Delta$. In particular, for $n = 2p+1$ and $m = 2p+2$ it follows that $(ce^{\alpha})e^{2p+2} \leq N$, for all positive integers p, which is a contradiction.

If we suppose that $x_n \xrightarrow{n.e.s.} 0$, then there exist a constant $\alpha > 0$ and a sequence of real numbers $N : \mathbb{N} \to [1, \infty)$ such that $(c\mathrm{e}^{\alpha})^{m-n} a_{mn} \leq N(n)$, for all $(m,n) \in \Delta$.

This implies

$$N(n) \geq \begin{cases} (c\mathrm{e}^{\alpha+1})^{m-n} & \text{if} \quad m=2q \quad \text{and} \quad n=2p \\ (c\mathrm{e}^{\alpha+1})^{m-n}\mathrm{e}^{n} & \text{if} \quad m=2q \quad \text{and} \quad n=2p+1 \\ (ce^{\alpha+1})^{m-n}\mathrm{e}^{-n} & \text{if} \quad m=2q+1 \quad \text{and} \quad n=2p \\ (c\mathrm{e}^{\alpha})^{m-n} & \text{if} \quad m=2q+1 \quad \text{and} \quad n=2p+1. \end{cases}$$

Given any $n \in \mathbb{N}$, the sequence $\left((c\mathrm{e}^{\alpha+1})^{m-n}\right)_m$ is bounded. This shows that $c\mathrm{e}^{\alpha+1} \leq 1$, and from $\alpha > 0$ we deduce that $c \in (0, 1/\mathrm{e})$. Further we observe that the sequence $N : \mathbb{N} \to [1, \infty)$ have the property that $N(n) \geq \mathrm{e}^n$ for all $n \in \mathbb{N}$.

Conversely, for all $c \in (0, 1/e)$, $\alpha = -\ln(c\mathrm{e}) > 0$ and $N(n) = \mathrm{e}^n$, $n \in \mathbb{N}$, we have that $|X_m^n| \leq N(n)e^{-\alpha(m-n)}$, for all $(m,n) \in \Delta$. This shows that $x_n \xrightarrow{n.e.s.} 0$.

Example 5. Let $b, c \in (0,1)$, $x_0 = 1$ and $a_n = \begin{cases} \dfrac{c}{(n+2)^b} & \text{if} \quad n=2k \\ c(n+1)^b & \text{if} \quad n=2k+1. \end{cases}$

Then

$$X_m^n = \begin{cases} c^{m-n} a_{mn}, & m > n \\ 1, & m = n, \end{cases}$$

where

$$a_{mn}=\begin{cases} \left(\dfrac{n+1}{m+1}\right)^b & \text{if} \quad m=2q+1 \quad \text{and} \quad n=2p+1 \\ \dfrac{1}{(m+1)^b} & \text{if} \quad m=2q+1 \quad \text{and} \quad n=2p \\ (n+1)^b & \text{if} \quad m=2q \quad \text{and} \quad n=2p+1 \\ 1 & \text{if} \quad m=2q \quad \text{and} \quad n=2p. \end{cases}$$

We shall prove that the linear recurrence sequence (x_n) is

(i) not uniformly exponentially convergent to 0, and
(ii) $x_n \xrightarrow{n.e.s.} 0$.

If we suppose that $x_n \xrightarrow{n.e.s.} 0$, then there exist some constants $N \geq 1$ and $\alpha > 0$ such that $(c\mathrm{e}^{\alpha})^{m-n} a_{mn} \leq N$ for all $(m,n) \in \Delta$. In particular, for $n = 2p+1$ and $m = 2p+2$ we have that $(c\mathrm{e}^{\alpha})(2p+2)^b \leq N$ for all $p \in \mathbb{N}$, which is a contradiction.

From $\alpha = -\ln c$ we have that $c\mathrm{e}^{\alpha} = 1$. Hence

$$(c\mathrm{e}^{\alpha})^{m-n} a_{mn} = a_{mn} \leq (n+1)^b = N(n),$$

for all $(m,n) \in \Delta$. This shows that $x_n \xrightarrow{n.e.s.} 0$.

Theorem 6. *The linear recurrence sequence $x_n \xrightarrow{n.e.s.} 0$ if and only if there exist a constant $d > 0$ and a nondecreasing sequence of real numbers $S : \mathbb{N} \to [1,\infty)$ such that*

$$\sum_{m=n}^{\infty} \mathrm{e}^{d(m-n)} |X_m^n| \leq S(n), \quad \textit{for all} \quad n \in \mathbb{N}. \tag{3}$$

Proof. If we suppose that $x_n \xrightarrow{n.e.s.} 0$ then there exists a constant $\alpha > 0$ and a sequence $N : \mathbb{N} \longrightarrow [1,\infty)$ such that for all $d \in (0,\alpha)$ we have that

$$\sum_{m=n}^{\infty} \mathrm{e}^{d(m-n)} |X_m^n| \leq \sum_{m=n}^{\infty} N(n) \mathrm{e}^{-(\alpha-d)(m-n)} = \frac{N(n)\mathrm{e}^{\alpha}}{\mathrm{e}^{\alpha} - \mathrm{e}^{d}} = S(n).$$

Conversely, if the relation (3) is true, then there exist a constant $d > 0$ and a sequence $S : \mathbb{N} \longrightarrow [1,\infty)$ such that

$$e^{d(m-n)} |X_m^n| \leq \sum_{k=m}^{\infty} e^{d(k-n)} |X_k^n| \leq S(n), \quad \text{for all} \quad (m,n) \in \Delta.$$

This shows that $x_n \xrightarrow{n.e.s.} 0$. □

Theorem 7. *If there are a constant $b > 0$ and a nondecreasing sequence of real numbers $\varphi : \mathbb{N} \longrightarrow [1,\infty)$ such that*

$$\sum_{k=n}^{m} \mathrm{e}^{b(m-k)} |X_m^k| \leq \varphi(n), \quad \textit{for all} \quad (m,n) \in \Delta,$$

then the linear recurrence sequence $x_n \xrightarrow{n.e.s.} 0$.

Proof. By hypothesis we have that exists a constant $b > 0$ and a sequences $\varphi : \mathbb{N} \longrightarrow [1,\infty)$ such that

$$\mathrm{e}^{b(m-n)} |X_m^n| \leq \sum_{k=n}^{m} \mathrm{e}^{b(m-k)} |X_m^k| \leq \varphi(n), \quad \text{for all} \quad (m,n) \in \Delta.$$

This shows that $x_n \xrightarrow{n.e.s.} 0$. □

A particular case of nonuniform exponential convergence is introduced next.

4. Exponential convergence.

Definition 3. *The linear recurrence (x_n) is called* ***exponential convergent to*** 0*, and we write $x_n \xrightarrow{e.s.} 0$, if there exist $N \geq 1$, $\alpha > 0$ and $\beta \geq 0$ such that*

$$|x_m| \leq Ne^{-\alpha(m-n)}e^{\beta n}|x_n|, \quad \textit{for all} \quad (m,n) \in \Delta.$$

Remark 5. The sequence $x_n \xrightarrow{e.s.} 0$ if and only if there are $N \geq 1$, $\alpha > 0$ and $\beta \geq 0$ such that

$$|X_m^n| \leq Ne^{-\alpha(m-n)}e^{\beta n}, \quad \textit{for all} \quad (m,n) \in \Delta.$$

Remark 6. It is obvious that if $x_n \xrightarrow{e.s.} 0$, then $x_n \xrightarrow{n.e.s.} 0$. The converse is not valid. This is illustrated by the following

Example 8. Let $c > 0$ and $a_n = \begin{cases} ce^{n(1+2^n)} & \text{if } n = 2k \\ ce^{-(n+1)(1+2^{n+1})} & \text{if } n = 2k+1. \end{cases}$

Then

$$X_m^n = \begin{cases} c^{m-n}a_{mn}, & m > n \\ 1, & m = n, \end{cases}$$

where

$$a_{mn} = \begin{cases} e^{n(1+2^n)}e^{-m(1+2^m)} & \text{if } m = 2q \text{ and } n = 2p \\ e^{-m(1+2^m)} & \text{if } m = 2q \text{ and } n = 2p+1 \\ e^{n(1+2^n)} & \text{if } m = 2q+1 \text{ and } n = 2p \\ 1 & \text{if } m = 2q+1 \text{ and } n = 2p+1. \end{cases}$$

We shall prove that $x_n \xrightarrow{n.e.s.} 0$ and $x_n \overset{e.s.}{\not\to} 0$.

If we suppose that $x_n \xrightarrow{e.s.} 0$, then there exist some constants $N \geq 1$, $\alpha > 0$ and $\beta \geq 0$ such that $(ce^{\alpha})^{m-n}a_{mn} \leq Ne^{\beta n}$. This implies

$$Ne^{\beta n} \geq \begin{cases} (ce^{\alpha})^{m-n}e^{n(1+2^n)}e^{-m(1+2^m)} & \text{if } m = 2q \text{ and } n = 2p \\ (ce^{\alpha})^{m-n}e^{-m(1+2^m)} & \text{if } m = 2q \text{ and } n = 2p+1 \\ (ce^{\alpha})^{m-n}e^{n(1+2^n)} & \text{if } m = 2q+1 \text{ and } n = 2p \\ (ce^{\alpha})^{m-n} & \text{if } m = 2q+1 \text{ and } n = 2p+1. \end{cases}$$

In particular, for $n = 2p$ and $m = 2p+1$ we have that

$$\frac{e^{2\beta p}}{e^{2p(1+2^{2p})}} \geq \frac{ce^{\alpha}}{N}$$

for all $p \in \mathbb{N}$, which is a contradiction.

For $c = 1/e$ and $\alpha = 1$ we have that $ce^{\alpha} = 1$. This shows that $(ce^{\alpha})^{m-n}a_{mn} = a_{mn} \leq e^{n(1+2^n)} = N(n) \leq N(n)e^{\beta n}$ for all $\beta \geq 0$ and $(m,n) \in \Delta$. Finally we obtain that $x_n \xrightarrow{e.s.} 0$.

Theorem 9. *The linear recurrence sequence $x_n \xrightarrow{e.s.} 0$ if and only if there*

are some constants $D \geq 1$, $d > 0$ *and* $c \geq 0$ *such that*

$$\sum_{m=n}^{\infty} \mathrm{e}^{d(m-n)}|X_m^n| \leq D\mathrm{e}^{cn}, \quad \text{for all} \quad n \in \mathbb{N}. \tag{4}$$

Proof. If the sequence $x_n \xrightarrow{e.s.} 0$, then there exist some constants $N \geq 1$, $\alpha > 0$ and $\beta \geq 0$ such that for all $d \in (0, \alpha)$ we have

$$\sum_{m=n}^{\infty} e^{d(m-n)}|X_m^n| \leq \sum_{m=n}^{\infty} Ne^{\beta n}e^{-(\alpha-d)(m-n)} = \frac{Ne^{\alpha}}{e^{\alpha}-e^{d}}e^{\beta n} = De^{cn},$$

for all $n \in \mathbb{N}$.

Conversely, if the relation (4) is true, then there are $D \geq 1$, $d > 0$ and $c \geq 0$ such that

$$e^{d(m-n)}|X_m^n| \leq \sum_{k=n}^{\infty} e^{d(k-n)}|X_k^n| \leq De^{cn}, \quad \text{for all} \quad (m,n) \in \Delta,$$

hence the sequence $x_n \xrightarrow{e.s.} 0$. □

Theorem 10. *The linear recurrence sequence* $x_n \xrightarrow{e.s.} 0$ *if and only if there are some constants* $B \geq 1$, $b > 0$ *and* $c \in [0, b)$ *such that*

$$\sum_{k=0}^{m} e^{b(m-k)}|X_m^k| \leq Be^{cm}, \quad \textit{for all} \quad m \in \mathbb{N}. \tag{5}$$

Proof. If $x_n \xrightarrow{e.s.} 0$, then there are $N \geq 1$, $\alpha > 0$ and $\beta \geq 0$ such that

$$\sum_{k=0}^{m} e^{b(m-k)}|X_m^k| \leq Ne^{(\beta-\alpha)m}\sum_{k=0}^{m} e^{(\alpha+\beta-b)k} = \frac{Ne^{\alpha+\beta}}{e^{\alpha+\beta}-e^{b}}e^{\beta m} = Be^{cm},$$

for all $m \in \mathbb{N}$ and all $b \in (\beta, \alpha+\beta)$.

Conversely, if the relation (5) is true, then there are $B \geq 1$, $b > 0$ and $c \in [0, b)$ such that

$$e^{b(m-n)}|X_m^n| \leq \sum_{k=n}^{m} e^{b(m-k)}|X_m^k| \leq \sum_{k=0}^{m} e^{b(m-k)}|X_m^k| \leq Be^{cm}.$$

It follows that $|X_m^n| \leq Be^{cn}e^{-(b-c)(m-n)}$, for all $(m,n) \in \Delta$ and hence $x_n \xrightarrow{e.s.} 0$. □

5. Strong exponential convergence.

Let (x_n) be a linear recurrence sequence generated by the sequence (a_n).

Definition 4. *The sequence (x_n) is called **strongly exponentially convergent to 0**, and we write $x_n \xrightarrow{s.e.s.} 0$, if there are $N \geq 1$, $\alpha > 0$ and $\beta \in [0, \alpha)$ such that*

$$|x_{m,n}| \leq N\mathrm{e}^{-\alpha(m-n)}\mathrm{e}^{\beta n}\,|x_n| \quad \textit{for all } (m,n) \in \Delta.$$

Remark 7. The sequence $x_n \xrightarrow{s.e.s.} 0$ if and only if there are $N \geq 1$, $\alpha > 0$ and $\beta \in [0, \alpha)$ such that

$$|X_m^n| \leq Ne^{-\alpha(m-n)}e^{\beta n}, \quad \textit{for all} \quad (m,n) \in \Delta.$$

Example 11. Let $c > 0$, $x_0 = 1$ and let (a_n) be the sequence defined in Example 4. Then:

(i) $x_n \xrightarrow{e.s.} 0$ if and only if $c \in (0, 1/e)$;
(ii) $x_n \xrightarrow{s.e.s.} 0$ if and only if $c \in \left(0, 1/e^2\right)$.

If $x_n \xrightarrow{e.s.} 0$, then there are $\alpha > 0$, $\beta \geq 0$ and $N \geq 1$ such that $(ce^{\alpha})^{m-n}a_{mn} \leq Ne^{\beta n}$, for all $(m,n) \in \Delta$, i.e.

$$Ne^{\beta n} \geq \begin{cases} (ce^{\alpha+1})^{m-n} & \text{if} \quad m = 2q \quad \text{and} \quad n = 2p \\ (ce^{\alpha+1})^{m-n}e^{n} & \text{if} \quad m = 2q \quad \text{and} \quad n = 2p+1 \\ (ce^{\alpha+1})^{m-n}e^{-n} & \text{if} \quad m = 2q+1 \quad \text{and} \quad n = 2p \\ (ce^{\alpha})^{m-n} & \text{if} \quad m = 2q+1 \quad \text{and} \quad n = 2p+1. \end{cases}$$

If the previous inequalities hold, then, from the considerations given in Example 4 it follows that $c \in (0, 1/e)$, $\beta \geq 1$ and $N \geq 1$.

Conversely, for any $c \in (0, 1/e)$, $\alpha = -\ln(ce) > 0$, $\beta = 1$ and $N = 1$ we have that $|X_m^n| \leq Ne^{-\alpha(m-n)}e^n$ for all $(m,n) \in \Delta$.

The second statement can be obtain analogously, with the additional condition that $\ln e = 1 \leq \beta < \alpha \leq \ln(ce)^{-1}$.

Remark 8. It is obvious that

$$x_n \xrightarrow{u.e.s.} 0 \Rightarrow x_n \xrightarrow{s.e.s.} 0 \Rightarrow x_n \xrightarrow{e.s.} 0 \Rightarrow x_n \xrightarrow{n.e.s.} 0$$

The converse implications are not true, as we shown in the previous examples.

Theorem 12. *The linear recurrence sequence $x_n \xrightarrow{s.e.s.} 0$ if and only if there are $D \geq 1$, $d > 0$ and $c \geq 0$ with $0 \leq c < d$ such that*

$$\sum_{m=n}^{\infty} e^{d(m-n)}|X_m^n| \leq De^{cn}, \quad \textit{for all} \quad n \in \mathbb{N}.$$

Proof. It follows from the Definition 4 and the proof of Theorem 9. □

Similarly, from the proof of Theorem 10 it follows the following

Theorem 13. *The linear recurrence sequence $x_n \xrightarrow{s.e.s} 0$ if and only if there*

are $B \geq 1$, $b > 0$ *and* $c \geq 0$ *with* $0 \leq 2c < b$ *such that*

$$\sum_{k=0}^{m} e^{b(m-k)} |X_m^k| \leq Be^{cm}, \quad \text{for all} \quad m \in \mathbb{N}.$$

Remark 9. From $x_n \longrightarrow x \in \mathbb{R} \Leftrightarrow x_n - x \longrightarrow 0$, the preceding considerations can be generalized to the exponential convergence to $x \in \mathbb{R}$.

References

[1] R.P. Agarwal, *Difference Equations and Ineqalities. Theory, Methods, and Applications*, 2nd ed., Vol. 228, Marcel Dekker, New York 2000.

[2] A. Halanay, D. Wexler, *Teoria calitativă a sistemelor cu impulsuri*, Editura Academiei 1968.

[3] M. Megan, P. Preda, *Şiruri reale recurente*, Colecţia Caiete Metodico-Ştiinţifice, Universitatea din Timişoara, 1985.

[4] I.-L. Popa, T. Ceauşu, M. Megan, *On exponential stability for linear discrete-time systems in Banach spaces*, Seminar of Mathematical Analysis and Applications, West University of Timişoara, 2011.

[5] I.-L. Popa, M. Megan, T. Ceauşu, *Nonuniform behaviors for linear discrete-time systems in Banach spaces*, Acta Universitatis Apulensis, Special Issue 2011, 339-347.

On homogeneous and approximately homogeneous functions

Dorian Popa[1)]

Abstract. We give some properties of homogeneous functions and prove that for every approximately homogeneous function there exists a homogeneous function near it.

Keywords: Homogeneous functions, approximately homogeneous functions, Euler equation.

MSC: 26D10, 39B82

1. Homogeneous functions

Homogeneous functions play an important role in many branches of mathematics, as geometry, analysis, differential equations. They are also often used in economic theory as production functions (see [1], [2]) and in physics. A precise definition and a characterization of homogeneous functions of several real variables will be given in what follows.

Recall that a nonempty set $K \subseteq \mathbb{R}^n$ is called a *cone* if for every $x \in K$ and every $t \in (0, \infty)$ we have $tx \in K$.

Definition 1.1. *Let* K *be a cone in* $\mathbb{R}^n$ *and* $p \in \mathbb{R}$. *A function* $f : K \to \mathbb{R}$ *is called* ***homogeneous function of degree*** p *if*

$$f(tx_1, tx_2, \ldots, tx_n) = t^p f(x_1, x_2, \ldots, x_n)$$

for every $x = (x_1, \ldots, x_n) \in K$ *and every* $t \in (0, \infty)$.

[1)]Technical University of Cluj-Napoca, Department of Mathematics

For example the function $f(x_1, x_2) = x_1^2 + 2x_1x_2 - 2x_2^2$ defined for all $(x_1, x_2) \in \mathbb{R}^2$ is homogeneous of degree $p = 2$ and $g(x_1, x_2) = \ln x_1 - \ln x_2$ defined for $x_1, x_2 \in (0, \infty)$ is homogeneous of degree $p = 0$.Throughout this paper by $D_i f$ we denote the partial derivative of f with respect to i-th variable.

A characterization of differentiable homogeneous functions is given in the following theorem.

Theorem 1.2. (**Euler**) *Let K be an open cone in $\mathbb{R}^n$ and $f : K \to \mathbb{R}$ be a differentiable function. Then f is a homogeneous function of degree $p \in \mathbb{R}$ if and only if the following relation holds*

$$x_1 D_1 f(x) + x_2 D_2 f(x) + \ldots + x_n D_n f(x) = p f(x) \tag{1}$$

for all $x = (x_1, x_2, \ldots, x_n) \in K$.

Proof. „⇒“ Suppose that f is a homogeneous function of degree p. Then

$$f(tx_1, tx_2, \ldots, tx_n) = t^p f(x_1, x_2, \ldots, x_n) \tag{2}$$

for all $x = (x_1, \ldots, x_n) \in K$. Differentiating with respect to t, the relation (2) becomes

$$D_1 f(tx)x_1 + D_2 f(tx)x_2 + \ldots + D_n f(tx)x_n = pt^{p-1} f(x). \tag{3}$$

Now (1) follows for $t = 1$ in (3).

„⇐“ Suppose that (1) holds for all $x \in K$. Fix $x \in K$ and define the function $\varphi : (0, \infty) \to \mathbb{R}$ by

$$\varphi(t) = \frac{f(tx_1, tx_2, \ldots, tx_n)}{t^p}, \ \forall\ t \in (0, \infty).$$

We prove that $\varphi'(t) = 0$ for all $t \in (0, \infty)$. Let $u_1 = tx_1$, $u_2 = tx_2, \ldots$, $u_n = tx_n$. We have

$$\begin{aligned}
\varphi'(t) &= \frac{(D_1 f(tx)x_1 + \ldots + D_n f(tx)x_n)t^p - f(tx)pt^{p-1}}{t^{2p}} \\
&= \frac{(D_1 f(tx)x_1 + \ldots + D_n f(tx)x_n)t - pf(tx)}{t^{p+1}} \\
&= \frac{tx_1 D_1 f(tx) + \ldots + tx_n D_n f(tx) - pf(tx)}{t^{p+1}} = 0, \ \forall\ t > 0.
\end{aligned}$$

The function φ is constant, therefore $\varphi(t) = \varphi(1)$ for all $t \in (0, \infty)$, which is equivalent with $f(tx) = t^p f(x)$, and since $x \in K$ is an arbitrary element, it follows that f is a homogeneous function of degree p. □

A property of the partial derivatives of a homogeneous function is given in the next theorem.

Theorem 1.3. *Let $K \subseteq \mathbb{R}^n$ be an open cone and $f : K \to \mathbb{R}$ a differentiable and homogeneous function of degree $p \in \mathbb{R}$. Then the partial derivatives $D_i f$, $1 \leq i \leq n$, are homogeneous functions of degree $p - 1$.*

Proof. Take $x \in K$, $h = (0, \ldots, 0, h_i, 0, \ldots, 0) \in K$, where $h_i \neq 0$ is the i-th coordinate, such that $x + h \in K$. We have

$$\frac{f(tx + th) - f(tx)}{th_i} = \frac{t^p f(x + h) - t^p f(x)}{th_i} = t^{p-1} \frac{f(x + h) - f(x)}{h_i}.$$

Now letting $h_i \to 0$ in the previous relation we get

$$D_i f(tx) = t^{p-1} D_i f(x),$$

i.e., D_i is a homogeneous function of degree $p - 1$. □

2. Approximately homogeneous functions

In what follows let $\mathbb{R}_+ = (0, \infty)$ and $\varepsilon \in \mathbb{R}_+$.

Definition 2.1. *A function $f : \mathbb{R}^n_+ \to \mathbb{R}$ of class C^1 is called* ε-homogeneous function of degree $p \in \mathbb{R}$ *if*

$$|x_1 D_1 f(x) + \ldots + x_n D_n f(x) - p f(x)| \leq \varepsilon \tag{4}$$

for all $x = (x_1, \ldots, x_n) \in \mathbb{R}^n_+$.

A function $f : \mathbb{R}^n_+ \to \mathbb{R}$ which is ε-homogeneous function of degree p for some $\varepsilon > 0$ and for some $p \in \mathbb{R}$ is called *approximately homogeneous function*. In other words an approximately homogeneous function satisfies approximately Euler's equation for homogeneous functions. This notion is in connection with Hyers-Ulam stability of functional equations (for more details see [3], [4], [5]).

The main result of this work is contained in the next theorem.

Theorem 2.2. *For every ε-homogeneous function $f : \mathbb{R}^n_+ \to \mathbb{R}$ of degree $p \in \mathbb{R} \setminus \{0\}$ there exists a unique continuous homogeneous function $g : \mathbb{R}^n_+ \to \mathbb{R}$ of degree p with the property*

$$|f(x) - g(x)| \leq \frac{\varepsilon}{|p|}, \ \forall \ x \in \mathbb{R}^n_+. \tag{5}$$

Proof. Existence. Let $f : \mathbb{R}^n_+ \to \mathbb{R}$ be a function satisfying (4) for some $\varepsilon > 0$ and some $p \in \mathbb{R} \setminus \{0\}$ and denote

$$x_1 D_1 f(x) + \ldots + x_n D_n f(x) - p f(x) =: h(x), \mathbb{Q}x \in \mathbb{R}^n_+. \tag{6}$$

Consider the function w defined by

$$f(x_1, x_2, \ldots, x_n) = w\left(x_1, \frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}\right) \Leftrightarrow$$

$$\Leftrightarrow (z_1, \ldots, z_n) = u\left(z_1, z_1 z_2, \ldots, z_1 z_n\right),$$

where $z_1 = x_1$, $z_k = \dfrac{x_k}{x_1}$, $x_k, z_k \in \mathbb{R}_+$, $2 \leq k \leq n$. We have, omitting the arguments of functions (for simplicity)

$$\begin{aligned} D_1 f &= D_1 w - \frac{x_2}{x_1^2} D_2 w - \ldots - \frac{x_n}{x_1^2} D_n w \\ D_2 f &= \frac{1}{x_1} D_2 w \\ &\ldots\ldots\ldots\ldots \\ D_n f &= \frac{1}{x_1} D_n w \end{aligned}$$

and replacing in (6) it follows

$$z_1 D_1 w(z_1, \ldots, z_n) = p w(z_1, \ldots, z_n) + h(z_1, z_1 z_2, \ldots, z_1 z_n)$$

which is equivalent to

$$D_1 \left(\frac{1}{z_1^p} w\left(z_1, \ldots, z_n\right) \right) = \frac{1}{z_1^{p+1}} h(z_1, z_1 z_2, \ldots, z_1 z_n).$$

An integration with respect to z_1 leads to

$$w(z_1, \ldots, z_n) = z_1^p \left(\int_1^{z_1} \frac{1}{s^{p+1}} h\left(s, z_2 s, \ldots, z_n s\right) \mathrm{d}s + \varphi\left(z_2, \ldots, z_n\right) \right),$$

where $\varphi : \mathbb{R}_+^n \to \mathbb{R}$ is an arbitrary function of class C^1, or

$$f(x_1, \ldots, x_n) = x_1^p \left(\varphi\left(\frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1} \right) + \int_1^{x_1} \frac{1}{s^{p+1}} h\left(s, \frac{x_2}{x_1} s, \ldots, \frac{x_n}{x_1} s \right) \mathrm{d}s \right).$$

We distinguish two cases in the definition of g, as follows:
i) If $p > 0$ let $g : \mathbb{R}_+^n \to \mathbb{R}$ be given by

$$g(x_1, \ldots, x_n) = x_1^p \left(\varphi\left(\frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1} \right) + \int_1^{\infty} \frac{1}{s^{p+1}} h\left(s, \frac{x_2}{x_1} s, \ldots, \frac{x_n}{x_1} s \right) \mathrm{d}s \right).$$

The function g is well defined, since by the relation $|h(x)| \leq \varepsilon$ for all $x \in \mathbb{R}_+^n$ and $p > 0$ it follows that

$$\int_1^{\infty} \frac{1}{s^{p+1}} h\left(s, \frac{x_2}{x_1} s, \ldots, \frac{x_n}{x_1} s \right) \mathrm{d}s$$

is absolutely convergent. On the other hand, g is obviously a continuous homogeneous function of degree p. We get

$$|f(x)-g(x)| = \left| x_1^p \int_{x_1}^{\infty} \frac{1}{s^{p+1}} h\left(s\frac{x_2}{x_1}s, \ldots, \frac{x_n}{x_1}s\right) \mathrm{d}s \right| \leq$$

$$\leq x_1^p \int_{x_1}^{\infty} \frac{\varepsilon}{s^{p+1}} \mathrm{d}s = \frac{\varepsilon}{p}, \quad x \in \mathbb{R}_+^n.$$

ii) If $p<0$ let $g : \mathbb{R}_+^n \to \mathbb{R}$ be given by

$$g(x_1, \ldots, x_n) = x_1^p \left(\varphi\left(\frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}\right) + \int_0^1 \frac{1}{s^{p+1}} f\left(s, \frac{x_2}{x_1}s, \ldots, \frac{x_n}{x_1}s\right) \mathrm{d}s \right).$$

The existence and homogeneity of g follows analogously as in the previous case i) and

$$|f(x)-g(x)| = \left| x_1^p \int_0^{x_1} \frac{1}{s^{p+1}} f\left(s, \frac{x_2}{x_1}s, \ldots, \frac{x_n}{x_1}s\right) \mathrm{d}s \right| \leq$$

$$\leq x_1^p \int_0^{x_1} \frac{\varepsilon}{s^{p+1}} = \frac{\varepsilon}{|p|}, \quad x \in \mathbb{R}_+^n.$$

The existence is proved.

Uniqueness. Suppose that for an ε-homogeneous function f of degree $p \in \mathbb{R} \setminus \{0\}$ there exist two continuous homogeneous functions $g_1, g_2 : \mathbb{R}_+^n \to \mathbb{R}$ of degree p satisfying (5). Since $g_1 \neq g_2$ there exists $x_0 \in \mathbb{R}_+^n$ with $g_1(x_0) \neq g_2(x_0)$. For every $t>0$ we have

$$|g_1(tx_0) - g_2(tx_0)| \leq |g_1(tx_0) - f(tx_0)| + |f(tx_0) - g_2(tx_0)| \leq \frac{2\varepsilon}{|p|}.$$

Taking account of the homogeneity of g_1, g_2 it follows

$$t^p |g_1(x_0) - g_2(x_0)| \leq \frac{2\varepsilon}{|p|},$$

contradiction, since t is an arbitrary positive number.

The theorem is proved. □

Remark 2.3. The result proved in Theorem 2.2 states that for every approximate homogeneous function of degree $p \neq 0$ there exists a homogeneous function of degree p close to it, i.e., Euler's equation characterizing homogeneous functions of degree $p \neq 0$ is stable in Hyers-Ulam sense (see [3]).

Remark 2.4. A surprising result holds for homogeneous functions of degree zero, proving that Euler's equation is not stable in this case. Indeed, let $f : \mathbb{R}_+^n \to \mathbb{R}$ be a solution of the equation

$$x_1 D_1 f(x) + \ldots + x_n D_n f(x) = \varepsilon, \quad \varepsilon > 0,$$

i.e., an ε-homogeneous function of degree zero.

Then it can be easily proved that

$$f(x_1, \ldots, x_n) = \varphi(x_1, \ldots, x_n) + \varepsilon \ln x_1$$

for all $(x_1, \ldots, x_n) \in \mathbb{R}_+^n$, where φ is a homogeneous function of degree zero. Let now $g : \mathbb{R}_+^n \to \mathbb{R}$ be an arbitrary homogeneous function of degree zero. Then for every $t > 0$

$$|f(t, t, \ldots, t) - g(t, t, \ldots, t)| = |\varphi(1, \ldots, 1) - g(1, \ldots, 1) + \varepsilon \ln t| \overset{t \to 0_+}{\longrightarrow} \infty,$$

therefore

$$\sup_{x \in \mathbb{R}_+^n} |f(x) - g(x)| = +\infty.$$

Remark 2.5. Professor Valeriu Anisiu from Babeş-Bolyai University, Cluj-Napoca, proved that we cannot choose the function g from Theorem 2.2 in C^1 (see [6]). Indeed, consider $q : \mathbb{R} \to \mathbb{R}$ defined by

$$q(x) = \frac{x^2}{2} \text{ for } |x| \leq 1 \text{ and } q(x) = |x| \text{ for } |x| > 1.$$

The function q is in $C^1(\mathbb{R})$. For the function $f(x_1, x_2) = q(x_1 - x_2)$, denoting

$$h(x_1, x_2) = x_1 D_1 f(x_1, x_2) + x_2 D_2 f(x_1, x_2) - f(x_1, x_2)$$

we have

$$|h(x_1, x_2)| = |(x_1 - x_2) q'(x_1 - x_2) - q(x_1 - x_2)|, \text{ hence}$$
$$|h(x_1, x_2)| = 0 \text{ for } |x_1 - x_2| \geq 1 \text{ and}$$
$$|h(x_1, x_2)| \leq \frac{1}{2} \text{ for } |x_1 - x_2| < 1.$$

So, f satisfies the hypothesis of Theorem 2.2 for $n = 2$, $\varepsilon = \frac{1}{2}$ and $p = 1$. Taking $g(x_1, x_2) = |x_1 - x_2|$ we have

$$|f(x_1, x_2) - g(x_1, x_2)| = |p(x_1 - x_2) - |x_1 - x_2|| \leq \frac{1}{2}.$$

We know that g is unique but it is not differentiable at the points (x, x), $x > 0$.

References

[1] R.G.D. Allen, *Mathematical Analysis for Economists*, Mac Millan & Co LTD, New York - St. Martin's Press, 1960.
[2] T. Apostol, *Calculus II*, John Willey & Sons, New York, London, Sidney, Toronto, 1969.
[3] D.S. Cîmpean, D. Popa, *Hyers-Ulam stability of Euler's equation*, Appl. Math. Lett., 24(2011), 1539-1543.
[4] D.H. Hyers, G. Isac, Th.M. Rassias, *Stability of Functional Equations in Several Variables*, Birkhäuser, Basel, 1998.
[5] N. Lungu, D. Popa, *Hyers-Ulam stability of a first order partial differential equation*, J. Math. Anal. Appl., 385(2011), 86-91.
[6] http://math.ubbcluj.ro/ anisiu/IMC/2011lalescu-constanta.pdf

An Elementary Characterization of the Orders of Non-Abelian Groups

Nicolae Anghel[1)]

Abstract. In this note we present an elementary proof of a result due to Dickson characterizing those integers n admitting non-abelian groups of order n.

Keywords: Non-abelian group, Maximal subgroup, Automorphism, Centralizer, Normalizer.

MSC: Primary: 20D60, 20E28. Secondary: 11A41, 20D45, 20E34, 20E45.

The classification, up to isomorphism, of the abelian groups of a given order is a fully-understood topic, a chapter in any book on finite groups. They are uniquely representable as direct products of cyclic p-groups and there are $\pi(\alpha_1)\pi(\alpha_2)\dots\pi(\alpha_m)$ non-isomorphic abelian groups of order n, if $\alpha_1, \alpha_2, \dots, \alpha_m$ are the exponents in the prime factorization of n and $\pi(\alpha)$ denotes the number of *partitions* of a positive integer α [2]. By comparison, the similar problem for non-abelian groups is extremely hard, but not hopelessly hard, given the current state of the art in finite group theory [7]. Meanwhile, there are many interesting and approachable topics regarding general non-abelian groups of finite order. One of them is the description of the positive integers n for which there are non-abelian groups of order n. In its equivalent form, the characterization of those integers n for which all the groups of order n are abelian, the problem was solved by Dickson in 1905 [1]. Dickson's proof relied on work by Miller and Moreno on the non-abelian groups whose proper subgroups are all abelian [5], which in turn relied on Jordan's work on permutation groups [3]. As such, the proof can be judged as non-elementary. That is also the case for more modern treatments of this problem [6], where it

[1)]Department of Mathematics, University of North Texas, Denton, anghel@unt.edu

appears as a specialization of a certain arithmetic description of the *nilpotent* groups, the direct products of p-groups corresponding to distinct primes.

The main purpose of this note is to give an elementary proof to *Dickson*'s result. It relies only on very basic concepts in group theory, such as center, centralizer, normalizer, and automorphism group, and on the *Lagrange* and *Cauchy* theorems for groups.

Theorem 1. *Let $n > 1$ be an integer with prime factorization $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, p_k distinct primes, $\alpha_k > 0$ for all k's. Then there is a non-abelian group of order n if and only if either $\alpha_i \geq 3$ for some index i (n contains perfect cubes), or n is cube-free ($\alpha_k \leq 2$ for all k's) and there are indices i and j such that p_i divides $p_j^{\alpha_j} - 1$.*

The Theorem provides a simple arithmetic criterion for testing integers n vis-a-vis the existence of non-abelian groups of order n, as soon as their prime factorization is known. At the same time, it can be seen to yield, for a fixed n, a sieve for detecting all the integers m, $1 \leq m \leq n$, with the property that all the groups of order m are abelian, much like, and at the same level of difficulty as, the Eratosthenes sieve. For instance, there are no non-abelian groups of order $91 = 7 \cdot 13$, however there are non-abelian groups of order $1,183 = 7 \cdot 13^2$. Also, there are exactly 43 numbers m, $1 \leq m \leq 100$, for which all the groups of order m are abelian.

The overall proof of the Theorem rests heavily on the following Lemma. In addition, for the necessity part of it we are going to employ a method developed by Jungnickel [4] for the purpose of characterizing the integers n admitting only one (cyclic) group of order n, in fact a particular instance of the present Theorem.

Lemma 2. *Let p be a prime number and let H be a finite abelian group of order $|H|$. Then there is a non-abelian group G of order $p|H|$ possessing an element a of order p and a normal subgroup $\widetilde{H}$ isomorphic to H such that the cyclic group $\langle a \rangle$ generated by a and $\widetilde{H}$ intersect trivially if and only if p divides $|Aut(H)|$, where $Aut(H)$ represents the automorphism group of H.*

Proof. [Proof of the Lemma] Assume first that G, a, and $\widetilde{H}$, exist as stated. Then any element of G is uniquely representable as $a^{\alpha}\widetilde{h}$, for some integer $0 \leq \alpha \leq p-1$ and $\widetilde{h} \in \widetilde{H}$. In terms of this representation the multiplication in G can be written as

$$(a^{\alpha}\widetilde{h})(a^{\beta}\widetilde{k}) = a^{\alpha+\beta}((a^{-\beta}\widetilde{h}a^{\beta})\widetilde{k}), \quad 0 \leq \alpha, \beta \leq p-1, \quad \widetilde{h}, \widetilde{k} \in \widetilde{H}. \qquad (1)$$

Also, since G is non-abelian and $\widetilde{H}$ is abelian there is an element $\widetilde{l}$ in $\widetilde{H}$ such that $a\widetilde{l} \neq \widetilde{l}a$. This and the fact that $\widetilde{H}$ is a normal subgroup of G yield a non-trivial automorphism ϕ of $\widetilde{H}$, namely the restriction to $\widetilde{H}$ of the inner automorphism of G given by $g \longmapsto a^{-1}ga$. In $Aut(\widetilde{H})$, a group under

composition, ϕ has order p, since p is prime and a has order p in G. Then the Lagrange theorem for groups implies that p divides $|Aut(\widetilde{H})| = |Aut(H)|$.

Conversely, suppose $|Aut(H)|$ is divisible by p and, by *Cauchy*'s theorem, let ϕ be a (non-trivial) element of order p in $Aut(H)$. If C_p is the cyclic group of order p, with generator x, take G to be, as a set, the cartesian product $C_p \times H$, and suggested by (1) define on G an internal operation $*$ by

$$(x^\alpha, h) * (x^\beta, k) = (x^{\alpha+\beta}, \phi^\beta(h)k), \qquad 0 \leq \alpha, \beta \leq p-1, \quad h, k \in H. \tag{2}$$

The choices of x and ϕ imply that the definition (2) is correct even if α, β are unrestricted non-negative integers. It is easy to check now that $(G, *)$ is a group of order $p|H|$ with identity element $(1, 1)$. In particular, the inverse of (x^α, h) is seen to be $(x^{p-\alpha}, \phi^{p-\alpha}(h^{-1}))$. $(G, *)$ is also non-abelian since for any element $l \in H$ such that $\phi(l) \neq l$, $(x, 1) * (1, l) \neq (1, l) * (x, 1)$.

By setting $a := (x, 1)$ and $\widetilde{H} := \{1\} \times H$ it is clear that a and $\widetilde{H}$ have all the properties specified in the Lemma. □

Remark. The reader more seasoned in group theory may have noticed that the construction in the Lemma is merely a particular instance of a semi-direct product.

Proof. [Proof of the Theorem — Sufficiency] If $\alpha_i \geq 3$ for some index i, then the Lemma applied to $p = p_i$ and $H = C_{p_i^2}$, the cyclic group of order p_i^2, with generator x, guarantees the existence of a non-abelian group G of order p_i^3, since any automorphism of H is uniquely determined by an assignment $x \longmapsto x^\alpha$, α relatively prime to p_i^2, and therefore $|Aut(H)| = p_i^2 - p_i = p(p-1)$. Then the direct product $G \times C_{n/p_i^3}$ yields a non-abelian group of order n.

If instead n is cube-free and for some necessarily distinct i and j, p_i divides $p_j^{\alpha_j} - 1$, two cases present themselves.

If $\alpha_j = 1$ then the Lemma applies to $p = p_i$ and $H = C_{p_j}$, $|Aut(H)| = p_j - 1$, to give a non-abelian group G of order $p_i p_j$, and so $G \times C_{n/(p_i p_j)}$ is a non-abelian group in support of the conclusion of the Theorem.

If $\alpha_j = 2$ one can implement the Lemma as above, by taking $p = p_i$ and $H = C_{p_j} \times C_{p_j}$, with generators x and y. Clearly, any automorphism of H is uniquely determined by sending x to some element of $H \setminus \{1\}$, say z, then sending y to any element of $H \setminus \langle z \rangle$, i.e., $|Aut(H)| = (p_j^2 - 1)(p_j^2 - p_j)$. □

Proof. [Proof of the Theorem — Necessity] Arguing by contradiction, let n be the least positive integer with prime factorization $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, $1 \leq \alpha_k \leq 2$ for any index k, with no indices i and j such that p_i divides $p_j^{\alpha_j} - 1$, for which there is a non-abelian group G of order n. In order to provide the reader with a better way of following the flow of the proof we divide the argument below into several sub-steps, some trivial, others not.

i) The center $Z(G)$ is a proper subgroup of G. — G is non-abelian.

ii) Any proper subgroup of G is abelian. — It follows from the the Lagrange theorem for groups and the minimality of $|G|$.

iii) For any $a \in G \setminus Z(G)$ the centralizer of a in G, $C_G(a)$, contains $Z(G)$ and is a maximal (abelian) subgroup of G. — This is true because $C_G(a) \neq G$ and any proper subgroup of G containing a, being abelian is contained in $C_G(a)$.

iv) $Z(G)$ cannot be a maximal subgroup of G. — By iii), if $a \in G \setminus Z(G)$, $Z(G) \subsetneq C_G(a) \subsetneq G$.

v) All maximal subgroups of G must be of type $C_G(a)$ for some $a \in G \setminus Z(G)$. — If U is a maximal subgroup, there is $a \in U \setminus Z(G)$. By ii), $U \subset C_G(a)$, therefore $U = C_G(a)$.

vi) If U is a maximal subgroup of G and $a \in U \setminus Z(G)$, then $U = C_G(a)$. — Same proof as that of v).

vii) if U and V are two distinct maximal subgroups of G, then $(U \setminus Z(G)) \cap (V \setminus Z(G)) = \emptyset$. — It follows from vii), by contradiction.

viii) Any maximal subgroup U of G is in fact equal to its normalizer, $N_G(U)$. — If not, for some $a \in G \setminus Z(G)$ there is $x \in N_G(C_G(a))$ such that $x \notin C_G(a)$. The automorphism ϕ_x of $C_G(a)$ induced by conjugation with x has order the least integer $q > 1$ such that $x^q \in C_G(a)$. Obviously, this order is also a divisor of $n = |G|$. Without loss of generality, x can be chosen so that the order of ϕ_x is a prime divisor of $|G|$, say p_i. The subset K of G consisting of elements of the form $x^\alpha h$, $0 \leq \alpha \leq p_i - 1$, $h \in C_G(a)$, is seen, by an argument similar to that presented in Equation (1), to be closed under group multiplication and inverse taking. So K is a group and since $C_G(a)$ is maximal, $K = G$. Notice also that the choice of x makes the elements of K uniquely representable in terms of α and h. Consequently,

$$|K| = p_i |C_G(a)| = n = |G|. \tag{3}$$

Now a simple argument by induction on the number of primes appearing in the order of the abelian group $C_G(a)$ shows that if $p_j^{\beta_j}$, $1 \leq \beta_j \leq 2$, appears in the prime factorization of $|C_G(a)|$, then $p_j^{\beta_j}$ contributes to $|Aut(C_G(a))|$ a factor of type

$$\begin{cases} p_j - 1 & \text{if } \beta_j = 1, \\ p_j^2 - p_j & \text{if } \beta_j = 2 \text{ and } C_G(a) \text{ has an element of order } p_j^2, \\ (p_j^2 - 1)(p_j^2 - p_j) & \text{if } \beta_j = 2 \text{ and } C_G(a) \text{ has no element of order } p_j^2, \end{cases} \tag{4}$$

and these are precisely all the factors of $|Aut(C_G(a))|$. However, the assumption made on the order of G and Equations (3) and (4) show that p_i, the order of ϕ_x, cannot divide $|Aut(C_G(a))|$, a contradiction. Thus, $U = N_G(U)$.

ix) The conjugates of any maximal subgroup U of G by elements in G are also maximal subgroups.

For $a, b \in G$, $a \notin Z(G)$, $bC_G(a)b^{-1} = C_G(bab^{-1})$, and clearly, $bab^{-1} \notin Z(G)$.

x) If U is a maximal subgroup of G of order $u|Z(G)|$, $u > 1$, then the total number of elements in all the distinct conjugates of U but not in $Z(G)$ equals $n - n/u$.

Indeed, the number of distinct conjugates of U is the index of the normalizer of U in G, i.e., $n/(u|Z(G)|)$, from $N_G(U) = U$. Since by ix) and vii) the distinct conjugates of U are disjoint outside $Z(G)$ and since $|U \setminus Z(G)| = (u-1)|Z(G)|$, the claim follows.

xi) There are elements in G which do not belong to the conjugates of some fixed maximal subgroup U of G.

True, since from x), $u|Z(G)| < n$ is equivalent to $|Z(G)| + n - n/u < n$.

xii) Statement xi) contradicts $|G| = n$.

If V is a maximal subgroup of G containing an element as in xi), with order $v|Z(G)|$, $v > 1$, there are another $n - n/v$ elements in G, in addition to those $|Z(G)| + n - n/u$, already provided by U. However, this is impossible since $|G| \geq |Z(G)| + (n - n/u) + (n - n/v) > n = |G|$.

The necessity part of the proof of the Theorem is now complete. □

Remark. In particular, the Theorem shows that a group of order p^2, p prime, must be abelian, a well-known fact. Our proof differs from the standard one, based on the use of the class equation for a group.

We end this note by inviting the interested reader to explore, in connection with the above Theorem, other stimulating and rewarding problems.

a) Make precise the sieve alluded to after the statement of the Theorem.

b) For which integers n is there exactly one non-abelian group of order n?

c) What is the asymptotic behavior, as $n \longrightarrow \infty$, of the function $NA(n) :=$ *the number of integers* m, $1 \leq m \leq n$, *such that there are non-abelian groups of order* m?

References

[1] L. Dickson, *Definitions of a Group and a Field by Independent Postulates*, Trans. Amer. Math. Soc. **6**, 198-204, (1905).

[2] I. Herstein, *Topics in Algebra*, 2rd Edition, John Wiley & Sons, New York, (1974).

[3] C. Jordan, *Traité des Substitutions et des Équations Algebriques*, Gauthier-Villars, Paris, (1870).

[4] D. Jungnickel, *On the Uniqueness of the Cyclic Group of Order n*, Amer. Math. Monthly **99**, 545-547, (1992).

[5] G. Miller, H. Moreno, *Non-Abelian Groups in Which Every Subgroup is Abelian*, Trans. Amer. Math. Soc. **4**, 398-404, (1903).

[6] J. Pakianathan, K. Shankar, *Nilpotent Numbers*, Amer. Math. Monthly **107**, 631-634, (2000).

[7] R. Solomon, *A Brief History of the Classification of the Finite Simple Groups*, Bulletin Amer. Math. Soc. **38**, 315-352, (2001).

Matrix adjugates and Additive Commutators

CEZAR LUPU[1)],

Abstract. In this note we study some properties of the additive commutator of two matrices in the spirit of the well-known problem which states that if $[A, B] = AB - BA = A$, then A is nilpotent. We give four proofs for this problem and then we study the relation between the commutator $[A, B]$ and the adjugate of A and we will show that if $[A, B] = \text{adj}(A)$, then $(\text{adj}(A))^2 = O_n$. Other related problems between the additive commutator and the adjugate are also given.

Keywords: matrix, commutator of a matrix, nilpotent matrix, adjugate of a matrix.

MSC: 15A24, 15A27, 15A60.

1. Introduction and Main Results

Let $M_n(\mathbb{C})$ denote the ring of $n \times n$ matrices with complex entries. Recall that:

(1) a matrix $A \in M_n(\mathbb{C})$ is *nilpotent* if $A^m = O_n$ for some positive integer m,

(2) the (*additive*) *commutator* of two matrices $A, B \in M_n(\mathbb{C})$ is $[A, B] = AB - BA$.

An interresting property proved by Shoda in 1936 is that only additive commutators have zero trace. For a detailed proof of this result see [8] or [7]. Later, Thompson showed in [21] that if $M_n(F)$ denotes the algebra of n-square matrices with elements in a field F and $M \in M_n(F)$ such that M has zero trace, then $M = AB - BA$ for certain $A, B \in M_n(F)$, where A is nilpotent and B has zero trace, apart from the cases when $n = 2, 3$. In [21] it is also determined when $M = MB - BM$ for some $B \in M_n(F)$. Sufficient conditions for a matrix in $M_n(\mathbb{C})$ to be nilpotent can be stated in terms of commutators (see [5], [7]):

Theorem 1. *Let $A \in M_n(\mathbb{C})$. If $[A, B] = A$ for some $B \in M_n(\mathbb{C})$, then A is nilpotent.*

Our first main result provides a similar sufficient condition for the adjugate of a matrix in $M_n(\mathbb{C})$ to be nilpotent; recall that the *adjugate* or *classical adjoint* of $A = [a_{ij}] \in M_n(\mathbb{C})$, written $\text{adj}(A)$, is the $n \times n$ matrix whose (i, j)-entry is the cofactor of a_{ij}.

Theorem 2. *Let $A \in M_n(\mathbb{C})$. If $[A, B] = \text{adj}(A)$ for some $B \in M_n(\mathbb{C})$, then $(\text{adj}(A))^2 = O_n$.*

[1)]University of Pittsburgh, Department of Mathematics, Pittsburgh, PA 15260, USA, lupucezar@gmail.com

A key ingredient of the proof is the following theorem of Jacobson [6, Lemma 2] which provides a sufficient condition for a commutator to be nilpotent:

Theorem 3. *Let $A, B \in M_n(\mathbb{C})$. If $A[A,B] = [A,B]A$, then the commutator $[A,B]$ is nilpotent.*

Combining Theorems 1 and 3, we prove a version of the former — Theorem 4 below — and the Jacobson-type Theorem 5.

Theorem 4. *Let $A, B \in M_n(\mathbb{C})$.*

(a) *If $[\mathrm{adj}(A), B] = \mathrm{adj}(A)$, then $(\mathrm{adj}(A))^2 = O_n$;*
(b) *If $[\mathrm{adj}(A), B] = A$, then A is nilpotent.*

Theorem 5. *Let $A, B \in M_n(\mathbb{C})$, and let $[A,B]_{\mathrm{adj}} = [\mathrm{adj}(A), \mathrm{adj}(B)]$.*

(a) *If $\mathrm{adj}(A)$ and $[A,B]_{\mathrm{adj}}$ commute, then $(\mathrm{adj}([A,B]))^2 = O_n$;*
(b) *If A and $[A,B]_{\mathrm{adj}}$ commute, then $(\mathrm{adj}([A,B]))^2 = O_n$.*

For further properties of the two commutators see [7], [13] and [22]. The additive commutator has also deep connections with Lie algebras because one can turn an associative algebra A into a Lie algebra by the Lie bracket $[X,Y] = XY - YX$. Now, $\mathrm{Lie}(A)$ becomes a Lie algebra together with this Lie bracket. Many important Lie algebras arise in this way. For example the Lie algebra $\mathfrak{g}l_n = \mathrm{Lie}(A)$, where A is the algebra of $n \times n$ matrices with the usual matrix multiplication. For more details one see [3].

2. Preliminaries and Proofs of Main Results

The adjugate of a matrix plays an important role in matrix theory. The computation of the adjugate from its definition involves the computation of n^2 determinants of order $n-1$, which is a prohibitively expensive $O(n^4)$ process. More details and properties can be found in [10]. In [16] and [11] other properties of the adjugate are developed. In what follows we state a couple of Lemmas and give a proof of Theorem 3. Recall that a matrix $X \in M_n(\mathbb{C})$ is *quasinilpotent* if $\lim_{n\to\infty} ||X^n||^{1/n} = 0$. Equivalently, the matrix X is quasinilpotent if the spectrum of X, denoted by $\sigma(X)$, is $\{0\}$, that is, X is nilpotent. In [1], it was proved that a quasinilpotent operator $T \in \mathcal{L}(\mathcal{H})$ is the uniform limit of a sequence $\{Q_k\}$ of nilpotent operators in $\mathcal{H}$ where $\mathcal{H}$ is a Hilbert space. We begin with the following well-known result

Lemma 6. *Let $A \in M_n(\mathbb{C})$. Then $\mathrm{tr}(A^k) = 0, k = 1, 2, \ldots, n$ if and only if A is nilpotent.*

A proof of this Lemma can be found in [14]. Recall the following

Definition 5. *Let $\mathbb{H}$ be a complex Hilbert space and $X : \mathbb{H} \to \mathbb{H}$ a linear bounded operator. The spectrum of X is given by*

$$\sigma(X) = \{\lambda \in \mathbb{C} : X - \lambda I \text{ is noninvertible}\}.$$

The spectral radius of X is denoted by $\rho(X)$ and

$$\rho(X) = \sup_{\lambda \in \sigma(X)} |\lambda|.$$

Concerning the spectral radius, there exists a formula (see [15]), namely

$$\rho(X) = \lim_{n \to \infty} \|X^n\|^{1/n}.$$

If $\mathbb{H} = \mathbb{C}^n$ is finite-dimensional, then X is a matrix and the definition above says that $\rho(X)$ is the largest absolute value of an eigenvalue of X.

We have to prove that $\rho(X) = 0$, in our case $\rho([A, B]) = 0$. This means that the matrix $[A, B]$ is quasinilpotent which implies that the commutator is nilpotent.

Definition 6. *Let $\mathcal{A}$ be an algebra. We say that $D : \mathcal{A} \to \mathcal{A}$ is a derivation* if D is a linear mapping such that

$$D(ab) = aD(b) + bD(a), \forall a, b \in \mathcal{A}.$$

The following property due to Leibniz holds:

$$D^n(ab) = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) (D^{n-i}a)(D^i b).$$

In [4] one can find other useful properties of D. For example, we have $D(a^n) = na^{n-1}D(a)$ iff $aD(a) = bD(b)$ and if $D^2(a) = 0$, then by induction and Leibniz property, we infer that $D^n(a^n) = n!(Da)^n, n \geq 1$.

Proof of Theorem 3. Consider the derivation $D : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ given by $D_A(X) = XA - AX$, for all $X \in M_n(\mathbb{C})$. From the hypothesis, we have that $D_A^2(B) = O_n$ and thus $D_A^n(B^n) = n!(D_A(B))^n$. Since $||D_A|| \Leftarrow q2||A||$, it follows that

$$||(D_A(B))^n|| \leq q\frac{2^n}{n!}||A||^n||B||^n$$

which is equivalent to

$$||(D_A(B))^n||^{1/n} \leq q\frac{2}{(n!)^{1/n}}||A||||B||, n \geq 1.$$

By passing to the limit when $n \to \infty$, we have that $\lim_{n \to \infty} ||(D_A(B))^n||^{1/n} = 0$, so we finally obtain $\rho([A, B]) = 0$ and thus $[A, B]$ is quasinilpotent which implies that $[A, B]$ is nilpotent. □

Remark. This proof of Theorem 3 has its origins in a more general framework. If we consider a Banach algebra $\mathcal{A}$ and for $a, b \in \mathcal{A}$ we define $[a, b] =$

$ab - ba$ such that $a[a, b] = [a, b]a$, then $[a, b]$ is quasinilpotent. This was conjectured for the first time by Kaplansky and later proved independently by Kleinecke in 1957 and Shikorov in [17] in 1961. For more details and history of this problem we recommend [4].

We use Theorem 3 in order to prove Theorem 1.

First proof of Theorem 1. We can prove by induction that

$$A^kB - B^kA = kA^k, k \geq 1.$$

Now, for an operator X we define its norm by $||X|| = \sup_{||x||=1} ||Xx||$ and satisfies the inequality $||XY|| \leq ||X|| \cdot ||Y||$. In our case, we have that

$$n||A^n|| = ||A^nB - B^nA|| \leq ||A^nB|| + ||BA^n|| \leq 2||A^n|| \cdot ||B||, n \geq 1.$$

From the relation above it follows that $||A^n|| = 0$, so A is nilpotent.

Remark. This proof shows that the theorem holds true for infinite dimensional spaces.

Second proof of Theorem 1. We have $A^kB - B^kA = kA^k, k \geq 1$. Let $f \in \mathbb{R}[X]$ and define $g(x) = xf'(x)$, where f' is the derivative of f. We prove that if $f(A) = O_n$, then $g(A) = O_n$. Denote $f(x) = a_kx^k + \ldots + a_1x + a_0$ and $f'(x) = ka_kx^{k-1} + \ldots + a_1$ and from here, we have $g(x) = ka_kx^k + (k-1)a_{k-1}x^{k-1} + \ldots + a_1x$. Since $f(A) = O_n$ we obtain

$$a_kA^k + \ldots + a_1A + a_0I_n = O_n.$$

Multiplying the above equality right and left with B we deduce that

$$a_kA^kB + \ldots + a_1AB + a_0B = O_n$$

and

$$a_kBA^k + \ldots + a_1BA + a_0B = O_n.$$

Thus, we obtain

$$a_k(A^kB - B^kA) + a_{k-1}(A^{k-1}B - B^{k-1}A) + \ldots + a_1(AB - BA) = O_n.$$

Since $A^kB - B^kA = kA^k$ for any $k = 1, 2, \ldots, n$, the equality becomes

$$ka_kA^k + (k-1)a_{k-1}A^{k-1} + \ldots + a_1A = O_n = g(A).$$

On the other hand $xg'(x) = x(f'(x) + xf''(x)) = xf'(x) + x^2f''(x)$. By putting $x = A$, we have

$$Af'(A) + A^2f''(A) = O_n.$$

But, from $Af'(A) = O_n$, we have that $A^2f''(A) = O_n$. By an easy induction we deduce that $A^kf^{(k)}(A) = O_n$. Considering the characteristic polynomial of the matrix A, we have

$$P_A(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0.$$

From $P_A(A) = O_n$ we deduce that $A^nP_A^{(n)}(A) = O_n$, and thus, A is nilpotent. □

Remark. Since $[A, B] = A$ the condition from the Theorem 1.3 is automatically satisfied, so it follows that the commutator $[A, B]$ is nilpotent, so A is nilpotent.

The following two Lemmas will be used in the proof of the Theorems 2, 4 and 5.

Lemma 7. *(see also* [18]*) Let $A \in M_n(\mathbb{C})$ be a singular matrix. Then there exists a complex number λ such that* $(\mathrm{adj}(A))^2 = \lambda\,\mathrm{adj}(A)$.

Proof. Let $r = \mathrm{rank}(A)$. Since $\det(A) = 0$ we have that $r \leq n-1$. If $r \leq n-2$, then all minors of order $n-1$ of the matrix A are zero, so $\mathrm{adj}(A) = O_n$ and thus our conclusion will be valid for any $\lambda \in \mathbb{C}$. If $r = n-1$, let $d_j = \begin{pmatrix} d_{1j} \\ d_{2j} \\ \dots \\ d_{nj} \end{pmatrix}$ be the j-column of $\mathrm{adj}(A)$, where d_{ij} is the algebraic complement of the element a_{ij}. Thus, we have $Ad_{ij} = O_{n,1}$, $\forall\, j = 1, 2, \dots, n$, so the columns of $\mathrm{adj}(A)$ are solutions of the homogenous system $AX = O_{n,1}$. It follows that every two columns of $\mathrm{adj}(A)$ are proportional so $\mathrm{rank}(\mathrm{adj}(A)) = 1$. In this case, there exists $M \in M_{n,1}(\mathbb{C})$ and $N \in M_{1,n}(\mathbb{C})$ such that $\mathrm{adj}(A) = MN$. Simple calculations yield

$$(\mathrm{adj}(A))^2 = (MN)^2 = (MN)(MN) = M(NM)N =$$

$$= M\lambda N = \lambda MN = \lambda\,\mathrm{adj}(A).$$

Lemma 8. *If $A \in M_n(\mathbb{C})$ is a matrix such that the adjugate* $\mathrm{adj}(A)$ *is nilpotent, then* $(\mathrm{adj}(A))^2 = O_n$.

Proof. From the hypothesis, it follows that $\det(\mathrm{adj}(A)) = 0$. By Lemma 7 we have that $(\mathrm{adj}(A))^2 = \lambda\,\mathrm{adj}(A)$. Since $\mathrm{adj}(A)$ is nilpotent there exists $k \geq 1$ such that $(\mathrm{adj}(A))^k = O_n$. On the other hand, by iteration, we deduce that

$$O_n = (\mathrm{adj}(A))^k = \lambda^{k-1}\,\mathrm{adj}(A).$$

If $\mathrm{adj}(A) = O_n$ the conclusion is clear; if not we have $\lambda = 0$ and then $(\mathrm{adj}(A))^2 = O_n$.

Finally, we prove our main theorems. We begin with the

First proof of Theorem 2. Since $\mathrm{adj}(A)$ commutes with A, it follows that A commutes with $[A, B]$, so by Theorem 3 it follows that the commutator $[A, B]$ is nilpotent and thus $\mathrm{adj}(A)$ is nilpotent. By Lemma 8 we have $(\mathrm{adj}(A))^2 = O_n$.

Second proof of Theorem 2. If $\mathrm{rank}(A) \leq n-2$, then $\mathrm{adj}(A) = O_n$, so $(\mathrm{adj}(A))^2 = O_n$. If $\mathrm{rank}(A) = n-1$, then $\det(A) = 0$ and by Sylvester rank inequality we have

$$0 = \mathrm{rank}(\det(A) \cdot I_n) = \mathrm{rank}(A\,\mathrm{adj}(A)) \geq \mathrm{rank}(A) + \mathrm{rank}(\mathrm{adj}(A)) - n,$$

so $\operatorname{rank}(\operatorname{adj}(A)) \in \{0, 1\}$. Since $\operatorname{rank}(\operatorname{adj}(A)) = 0$ is not the case, we have $\operatorname{rank}(\operatorname{adj}(A)) = 1$. Now, by Lemma 7 we have $(\operatorname{adj}(A))^2 = \lambda \operatorname{adj}(A)$. Since $0 = \operatorname{tr}([A, B]) = \operatorname{tr}(\operatorname{adj}(A))$, from $(\operatorname{adj}(A))^2 = \lambda \operatorname{adj}(A)$ it follows that $\operatorname{tr}((\operatorname{adj}(A))^2) = 0$ and inductively we have $\operatorname{tr}(\operatorname{adj}(A))^k) = 0$, for all $k \geq 1$. By Lemma 6 and Lemma 8 we have $(\operatorname{adj}(A))^2 = O_n$.

Third proof of Theorem 2. If $\operatorname{rank}(A) \leq n - 2$, then $\operatorname{adj}(A) = O_n$, so $(\operatorname{adj}(A))^2 = O_n$. If $\operatorname{rank}(A) = n - 1$, then $\det(A) = 0$.

From $AB - BA = \operatorname{adj}(A)$, by multiplying with $\operatorname{adj}(A)$ on left, we have

$$\det(A)B - \operatorname{adj}(A)BA = (\operatorname{adj}(A))^2$$

Now, by multiplying the above equality right with $\operatorname{adj}(A)$, we obtain

$$\det(A)B \operatorname{adj}(A) - \det(A) \operatorname{adj}(A)B = (\operatorname{adj}(A))^3.$$

We have $(\operatorname{adj}(A))^3 = O_n$ which shows that $\operatorname{adj}(A)$ is nilpotent and by Lemma 8 we obtain $(\operatorname{adj}(A))^2 = O_n$.

Fourth proof of Theorem 2. Like in the third proof, if $\operatorname{rank}(A) \leq n - 2$ there is nothing to prove. If $\operatorname{rank}(A) = n - 1$, then $\operatorname{rank}(\operatorname{adj}(A)) = 1$. Now the problem reduces to the fact that if $\operatorname{rank}(AB - BA) = 1$, then $(AB - BA)^2 = O_n$. Since $\operatorname{rank}([A, B]) = 1$ there exists $P \in M_{1,n}(\mathbb{C})$ and $Q \in M_{n,1}(\mathbb{C})$ such that $[A, B] = PQ$. From here, it follows that $[A, B]^2 = = \alpha[A, B]$, where $\alpha = QP \in \mathbb{C}$. It follows that the minimal polynomial of $[A, B]$ is $\min_{[A,B]}(X) = X^2 - \alpha X$. On the other hand, we have $0 = \operatorname{tr}([A, B]) = k\alpha$, where k is the algebraic multiplicity of α. So $\alpha = 0$ and $\min_{[A,B]}(X) = X^2$ and we have that $[A, B]^2 = (\operatorname{adj}(A))^2 = O_n$. □

Remark. Let $J_k(0)$ be the Jordan block of size k. If A is nilpotent and has rank $n - 1$, then A is similar to $J_n(0)$. For any $k > 1$, $\operatorname{adj}(J_k(0))$ is similar to $J_2(0) \oplus O_{k-1}$, so $\operatorname{adj}(J_k(0))$ is nilpotent and it has nilpotency index 2. Thus, if A is nilpotent, then $\operatorname{adj}(A)$ is nilpotent and from Lemma 8 we finally obtain $\operatorname{adj}^2(A) = O_n$.

Proof of Theorem 4. (a) It follows immediately from Theorem 1 and Lemma 8.

(b) Since $A \cdot \operatorname{adj}(A) = \operatorname{adj}(A) \cdot A = \det(A) \cdot I_n$, we obtain that $\operatorname{adj}(A)$ commutes with $[\operatorname{adj}(A), B]$, so by applying Theorem 3 we have that the commutator $[\operatorname{adj}(A), B]$ is nilpotent, so A is nilpotent as desired. □

Proof of Theorem 5. (a) We have

$$[A, B]_{\operatorname{adj}} = [\operatorname{adj}(A), \operatorname{adj}(B)] = \operatorname{adj}(BA) - \operatorname{adj}(AB) =$$

$$= \operatorname{adj}(BA - AB) = -\operatorname{adj}([A, B]).$$

Now, by the hypothesis and Theorem 3 it follows that $[A, B]_{\operatorname{adj}}$ is nilpotent, and by the identity above it follows that $\operatorname{adj}([A, B])$ is nilpotent and by Lemma 8 we have $(\operatorname{adj}([A, B]))^2 = O_n$;

(b) Since $\operatorname{adj}(A)$ commutes with A by (a) the conclusion follows immediately. □

Remark. The 3×3 matrices below show that the Jacobson-type condition of the form $[\mathrm{adj}(A), [A, B]] = O_n$ is not enough for $[A, B]$ to be nilpotent,

$$A = \begin{pmatrix} J_2(0) & 0 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} J_2(0)^T & 0 \\ 0 & 0 \end{pmatrix}.$$

Acknowledgement. The author feels deeply indebted to Benjamin Bogoşel, Radu Gologan, Călin Popescu, Marius & Speranţa Vlădoiu for their interest and also for the fruitful conversations which were of great benefit to the paper during its preparation.

REFERENCES

[1] C. Apostol, D. Voiculescu, *On a problem of Halmos*, Rev. Roum. Math. Purres et Appl. **19**(1974), 273–274.
[2] K. Dickson, T. Selle, *Eigenvectors of arrowhead matrices via the adjugate*, preprint.
[3] K. Erdman & M.J. Wildon, *An Introduction to Lie algebras*, Springer Verlag, 2006.
[4] P. Halmos, *A Hilbert space problem book*, Springer Verlag, 1982.
[5] R. Horn, C. Johnson, *Matrix Analysis*, Cambridge University Press, 1990.
[6] N. Jacosbson, *Rational methods in the theory of Lie algebras*, Ann. Math. **36**(1935), 875–881.
[7] R. Horn & C. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, 1991.
[8] W. Kahan, *Only commutators have zero trace*, preprint `http://www.eecs.berkeley.edu/wkahan/MathH110/trace0.pdf`.
[9] D.C. Kleinecke, *On operator commutators*, Proc. Amer. Math. Soc. **8**(1957), 535–536.
[10] L. Mirsky, *An Introduction to Linear Algebra*, Clarendon Press(Oxford), 1961.
[11] L. Mirsky, *The norms of adjugates and inverse matrices*, Arch. der Math. **7**(1956), 276–277.
[12] V. Prasolov, *Problems and Theorems in Linear Algebra*, American Mathematical Society Press, 1999.
[13] D.W. Robinson, *A note on matrix commutators*, Michigan Math. J. **7**(1959), 31–33.
[14] D.W. Robinson, *A matrix application of Newton's identities*, American Math. Mon. **68**(1961), 367–369.
[15] W. Rudin, *Functional Analysis* (second edition), McGraw-Hill Science Engineering, 1991.
[16] H. Schwerdtfeger, *On the adjugate of a matrix*, Portugaliae Matematica **20**(1961), 39–41.
[17] F.V. Shirokov, *Proof of a conjecture of Kaplansky*, Uspekhi Math. Nauk **11**(1956), 167–168.
[18] R. Sinkhorn, *The range of the adjugate of a matrix*, Math. Magazine **66**(1993), 109–113.
[19] G. W. Stewart, *On the adjugate matrix*, Linear Alg. & Appl. **283**(1998), 151–164.
[20] O. Taussky, *The factorization of the adjugate of a finite matrix*, Linear Alg & Appl. **1**(1968), 39–41.
[21] R.C. Thompson, *Matrices with zero trace*, Israel J. Math. **4**(1966), 33–42.
[22] R.C. Thompson, *A note on matrix commutators*, Amer. Math. Monthly **74**(1967), 276–278.

Barbălat and his Lemma

C. Corduneanu[1)]

Abstract. A key result in mathematical analysis, very useful in the qualitative theory of differential equations, which is quite elementary, is known as the Barbălat lemma. The paper is devoted to some comentaries and some mathematical perspectives on the Barbălat lemma.

Keywords: Barbălat lemma, qualitative theory, differential equations.
MSC: 01A70, 34CXX

1. Introduction

Ioan Barbălat (1907–1988) was a Romanian mathematician who had contributed, mostly, within the Seminar of „Qualitative Theory of Differential Equations", organized under the leadership of the late Professor *Aristide Halanay*, at the Institute of Mathematics of the Romanian Academy (1952-1997). His academic affiliation was with the „Institute of Civil Engineering" from Bucharest, where he held the chairmanship of the Mathematics Department. Before occupying this position, he worked as a high-school teacher, in insurance–actuarial companies or as an Assistant Professor, then Professor.

He was born in the city of Bârlad, studied in Romania and in France. In particular, he spent several years in Paris, where he acquired mathematical skills, under distinguished French professors at Sorbonne.

One of his major contributions to Mathematical Analysis/Differential Equations is, likely, his result known in the mathematical literature under his name: *Barbălat's Lemma*. It is a very simple, but handy result, which carried his name, along the last half-a-century, being quoted/used by hundreds of researchers and authors, in numerous journal papers and books. Wikipedia has also included reference to the Lemma.

This paper is aimed to pay a homage to the memory of a colleague, who distinguished himself by special amiability and refined personality.

We shall first present one of the variants of his Lemma, as it appears in the recent book [3] of Ivan Tyukin, published by Cambridge University Press.

Then, we shall consider similar results interesting the applications to the Theory of Dynamical Systems.

2. Barbălat's Lemma (1959)

The statement of the Lemma:

A real valued function, $f : \mathbb{R}_+ \to \mathbb{R}$, which is uniformly continuous and such that

[1)]University of Texas, Arlington, Romanian Academy

$$\lim_{t\to\infty}\int_0^t f(s)\mathrm{d}s = a \in \mathbb{R} \tag{1}$$

satisfies

$$\lim_{t\to\infty} f(t) = 0. \tag{2}$$

Proof. (see [3]) If (2) does not hold, there exists a sequence $\{t_n;\ n \geq 1\} \subset \mathbb{R}_+$, such that

$$|f(t_n)| > \varepsilon_0 > 0, \quad n \geq 1. \tag{3}$$

The uniform continuity of $f(t)$ on $\mathbb{R}_+$ allows us to write

$$|f(t)| \geq \frac{\varepsilon_0}{2}, \quad |t - t_n| < \delta, \quad n \geq 1, \tag{4}$$

for some $\delta = \delta(\varepsilon_0) > 0$, while (4) implies

$$f(t) \geq \frac{\varepsilon_0}{2}, \quad |t - t_n| < \delta, \tag{5}$$

for infinitely many $n \geq 1$. Without loss of generality, we can assume that (5) holds for any $n \geq 1$. Since (1) holds true when $f(t)$ is substituted by $-f(t)$, we still can rely on (5), which must be verified for either $f(t)$, or $-f(t)$.

Therefore, we derive from (3) and (5) the inequalities

$$\int_{t_n-\delta}^{t_n+\delta} f(t)\mathrm{d}t \geq 2\delta\varepsilon_0, \quad n \geq 1, \tag{6}$$

which are incompatible with (1). Indeed, condition (1) implies, on behalf of *Cauchy*'s criterion for existence of the limit, as $t \to \infty$, the inequality

$$\left|\int_t^{\bar{t}} f(s)\mathrm{d}s\right| < \varepsilon, \quad t, \bar{t} \geq T(\varepsilon), \tag{7}$$

with arbitrary $\varepsilon > 0$. In particular, for $\varepsilon < 2\delta\varepsilon_0$, (7) becomes impossible, which proves that our assumption (3) leads to a contradiction.

The Lemma is, thereby, proven.

Remark. Several variants of this Lemma can be found in various sources. In our book [2], there are basically the same conditions, but (1) is substituted by

$$\int_0^\infty f(t)\mathrm{d}t < \infty, \quad f(t) \geq 0, \tag{8}$$

somewhat stronger. Obviously, (1) is the consequence of

$$\int_0^t f(s)\mathrm{d}s \to \int_0^\infty f(s)\mathrm{d}s, \quad \text{as } t \to \infty. \tag{9}$$

Let us point out the fact that Barbălat's Lemma is of current use in stability theory, for which the space $C_0(\mathbb{R}_+, \mathbb{R}^n)$, consisting of all continuous functions from $\mathbb{R}_+$ into $\mathbb{R}^n$, tending to zero at ∞, is the natural choice.

Sometimes, the Lemma is stated in a slightly different form: $f \in L_1(0,\infty)$, $f'(t)$ uniformly continuous on $[0,\infty)$ imply $f'(t) \to 0$ as $t \to \infty$.

The dynamical interpretation is the following: the motion described by the function $f(t)$ leads to an equilibrium point (because the velocity $f'(t) \to 0$ as $t \to \infty$).

3. A boundedness result

As seen in case of Barbălat's Lemma, the assumption of *uniform continuity* has important implications on the global behavior of the function involved.

In concise formulation, the Barbălat's Lemma can be expressed as

$$\left\{ f;\ \int_0^t f(s)\mathrm{d}s \in C_\ell(\mathbb{R}_+, \mathbb{R}) \right\} \cap \{ f;\ f' \in C_u(\mathbb{R}_+, \mathbb{R}) \} \in C_0(\mathbb{R}_+, \mathbb{R}). \tag{10}$$

The meaning of the notations are the following

- $C_\ell(\mathbb{R}_+, \mathbb{R})$ is the Banach space of continuous maps from $\mathbb{R}_+$ into $\mathbb{R}$, with the supremum norm on $\mathbb{R}_+$, each function being such that $\lim\limits_{t\to\infty} f(t)$ exists and is finite;
- $C_u(\mathbb{R}_+, \mathbb{R})$ stands for the set of uniformly continuous maps from $\mathbb{R}_+$ into $\mathbb{R}$;
- $C_0(\mathbb{R}_+, \mathbb{R})$ is the (closed) subspace of $C_\ell(\mathbb{R}_+, \mathbb{R})$, for which the limits of functions at infinity are zero.

It is also a Banach space with the supremum norm on $\mathbb{R}_+$.

We shall state and prove a result which provides a boundedness criterion on $\mathbb{R}_+$.

Again, using concise formulation, this result can be stated as follows:

Theorem 1. *Let $M(\mathbb{R}_+, \mathbb{R})$ be the Banach space of maps from $\mathbb{R}_+$ into $\mathbb{R}$, locally integrable and such that*

$$\sup_{t\in R_+} \int_t^{t+1} |f(s)|\mathrm{d}s = |f|_M < \infty. \tag{11}$$

(*The functions of this space are called bounded in the mean.*)

By $BC(\mathbb{R}_+, \mathbb{R})$, one denotes the Banach space of all continuous and bounded maps from $\mathbb{R}_+$ into $\mathbb{R}$, with the supremum norm.

Then, the following relationship takes place:

$$M(\mathbb{R}_+, \mathbb{R}) \cap C_u(\mathbb{R}_+, \mathbb{R}) \subset BC(\mathbb{R}_+, \mathbb{R}). \tag{12}$$

Proof. One has to show that a uniformly continuous function on $\mathbb{R}_+$, with values in R, which is bounded in the mean, is actually bounded in usual sense, i.e., $|f(t)| \leq K < +\infty$, $t \in \mathbb{R}_+$, for some $K > 0$.

One proceeds by contradicting the boundedness. This fact implies the existence of a sequence $t_n \to \infty$, as $n \to \infty$, such that

$$|f(t_n)| \to \infty, \quad \text{as } n \to \infty. \tag{13}$$

The uniform continuity of f implies the property: for each $\varepsilon > 0$, there exists $\delta > 0$, such that

$$|f(t)| - |f(t_n)| \leq |f(t) - f(t_n)| < \varepsilon, \ |t - t_n| < \delta. \tag{14}$$

From (14) one derives

$$|f(t_n)| - \varepsilon < |f(t)| < |f(t_n)| + \varepsilon, \quad |t - t_n| < \delta, \tag{15}$$

and furthermore, by integration

$$\int_{t_n-\delta}^{t_n+\delta} |f(s)| \mathrm{d}s \geq 2\delta(|f(t_n)| - \varepsilon). \tag{16}$$

It is not restrictive to assume $2\delta < 1$, which means that the length of the interval of integration in (16) is less than 1. Hence, one can find $\tau_n < t_n$, $n > 1$, such that $[\tau_n, \tau_n + 1] \supset [t_n - \delta, t_n + \delta]$. Therefore, from (16) one obtains

$$\int_{\tau_n}^{\tau_n+1} |f(s)| \mathrm{d}s \geq \int_{t_n-\delta}^{t_n+\delta} |f(s)| \mathrm{d}s \geq 2\delta(|f(t_n)| - \varepsilon), \quad n \geq 1. \tag{17}$$

Now, if one takes (13) into account, one finds that

$$\sup_{t \in \mathbb{R}_+} \int_{t}^{t+1} |f(s)| \mathrm{d}s = \infty, \tag{18}$$

which contradicts the definition of the space $M(\mathbb{R}_+, \mathbb{R})$, according to (11).

Theorem 1 is thereby proven.

4. Another kind of Barbălat's Lemma

In order to state a criterion, for a function to belong to the space $C_0(\mathbb{R}_+,\mathbb{R})$, we shall consider a subspace of the space $M(\mathbb{R}_+,\mathbb{R})$, defined by (11), namely

$$M_0(\mathbb{R}_+,\mathbb{R})=\left\{f;\ f\in L^1_{\rm loc}(\mathbb{R}_+,\mathbb{R}),\int\limits_t^{t+1}|f(s)|{\rm d}s\to 0 \text{ as } t\to\infty\right\}. \tag{19}$$

It is obvious that the integral condition in (19) is equivalent to

$$F(t)=\int\limits_t^{t+1}|f(s)|{\rm d}s\in C_0(\mathbb{R}_+,\mathbb{R}).$$

The result can be stated as follows:

Theorem 2. *The following relationship is valid:*

$$M_0(\mathbb{R}_+,\mathbb{R})\cap C_u(\mathbb{R}_+,\mathbb{R})\subset C_0(\mathbb{R}_+,\mathbb{R}). \tag{20}$$

Proof. The inclusion (20) means that a function $f:\mathbb{R}_+\to\mathbb{R}$, belonging to both $M_0(\mathbb{R}_+,\mathbb{R})$ and $C_u(\mathbb{R}_+,\mathbb{R})$, must be in the space $C_0(\mathbb{R}_+,\mathbb{R})$. Let us consider such a function and observe that, in case it would not be in $C_0(\mathbb{R}_+,\mathbb{R})$, one can find a sequence $\{t_k;\ k\geq 1\}\subset\mathbb{R}_+$, such that

$$|f(t_k)|\to\ell,\quad \text{as } k\to\infty. \tag{21}$$

From the uniform continuity of f on $\mathbb{R}_+$, there results the property: to each $\varepsilon>0$, one can find $\delta>0$, such that

$$|f(t)|-|f(t_k)|\leq|f(t)-f(t_k)|\leq\varepsilon,\ |t-t_k|<\delta,\ k\geq 1. \tag{22}$$

Let us point out the fact that the existence of $\delta=\delta(\varepsilon)$ is guaranteed as the maximum possible value for δ, such that (22) holds.

We can diminish δ, as much as we want, keeping it positive, and (22) remains valid. More precisely, we shall always choose δ in (22), with $2\delta<1$.

From (22), one derives

$$|f(t)|\geq|f(t_k)|-\varepsilon,\ |t-t_k|<\delta,\ k\geq 1, \tag{23}$$

and, taking into account (21), with a sufficiently small $\varepsilon>0$ in (23), one obtains by integrating in (23), from $t_k-\delta$ to $t_k+\delta$,

$$\int\limits_{t_k-\delta}^{t_k+\delta}|f(t)|{\rm d}t\geq 2\delta(|f(t_k)|-\varepsilon),\ k\geq 1. \tag{24}$$

Taking into account our assumption $2\delta < 1$, there results the existence of a number $\tau_k \in R$, such that $[\tau_k, \tau_k + 1] \supset [t_k - \delta, t_k + \delta]$, which implies

$$\int_{\tau_k}^{\tau_k+1} |f(s)|\mathrm{d}s \geq \int_{t_k-\delta}^{t_k+\delta} |f(s)|\mathrm{d}s \geq 2\delta(|f(t_k)| - \varepsilon),\ t \geq 1. \tag{25}$$

Letting $k \to \infty$ in both sides of (25), one obtains the impossibility:

$$0 \geq 2\delta(\ell - \varepsilon), \tag{26}$$

due to the fact that both factors in the right hand side are strictly positive. Of course, from the beginning we chosen $\varepsilon < \ell$, while $\delta > 0$.

This ends the proof of Theorem 2.

Remark. Theorem 2 will be compared with the *Barbălat*'s Lemma, which we shall rephrase in the form

$$\{f;\ f \in C_\ell(\mathbb{R}_+, \mathbb{R})\} \cap \left\{f;\ f' \in C_u(\mathbb{R}_+, \mathbb{R})\right\} \subset C_0(\mathbb{R}_+, \mathbb{R}),$$

where $C_\ell(\mathbb{R}_+, \mathbb{R})$ denotes the *Banach* space of maps from $\mathbb{R}_+$ into $\mathbb{R}$, such that $\lim\limits_{t\to\infty} f(t)$ exists.

We shall now prove that the spaces $C_\ell(\mathbb{R}_+, \mathbb{R})$ and $M_0(\mathbb{R}_+, \mathbb{R})$ are distinct, though they contain both the space $C_0(\mathbb{R}_+, \mathbb{R})$.

First, it is almost obvious that a function $f \in C_\ell(\mathbb{R}_+, \mathbb{R})$, with $\lim\limits_{t\to\infty} f(t) \neq 0$, cannot be in $M_0(\mathbb{R}_+, \mathbb{R})$.

Second, the space $M_0(\mathbb{R}_+, \mathbb{R})$ contains also functions which do not belong to $C_\ell(\mathbb{R}_+, \mathbb{R}^n)$. It is rather elementary to prove that the function $f(t) = 0$ on $[0, 1]$, and

$$f(t) = \begin{cases} 0, & t \subset [k, k + 1 - k^{-1}], \\ k(t - k - 1 + k^{-1}), & t \in [k + 1 - k^{-1}, k + 1], \end{cases} \qquad k \geq 1,$$

is in $M_0(\mathbb{R}_+, \mathbb{R})$, but not in $C_\ell(\mathbb{R}_+, \mathbb{R})$. This $f(t)$ is not continuous but it is possible to construct even continuous examples.

We invite the reader to obtain such examples and get similar results to the Barbălat's Lemma.

REFERENCES

[1] I. Barbălat, Systèmes d'équations différentielles d'oscillations non linéaires, *Revue Roumaine d'Electrotechnique et Energétique,* IV (1959), 267-270.

[2] C. Corduneanu, *Integral Equations and Stability of Feedback Systems*, Academic Press, New York, 1973.

[3] Ivan Tyukin, *Adaptation in Dynamical Systems*, Cambridge University Press, 2010.

NOTE MATEMATICE

A property of the bidimensional sphere

Marius Cavachi[1)],

Abstract. It is natural to ask for a reasonable constant k having the property that any open set of area greater than k on a bidimensional sphere of area 1 always contains the vertices of a regular tetrahedron. We shall prove that it is sufficient to take $k = \frac{3}{4}$. In fact we shall prove a more general result. The interested reader will not have any problem in establishing that $\frac{3}{4}$ is the best constant with this property.

Keywords: area; open set; Haar measure; rotation group of the sphere.
MSC: 97G40

Our result is the following:

Theorem 1. *Let n be a positive integer, and let S be a bidimensional sphere of area 1. If $M \subset S$ is an open set of area greater than $\frac{n-1}{n}$ and $X \subset S$ is a finite set with n elements, then there exists a rotation ρ of the sphere such that $\rho(X) \subset M$.*

In the proof, we use the following result whose proof we postpone:

Lemma 2. *Let $M, M' \subset S$ be open sets such that $\mathcal{A}(M) > \mathcal{A}(M')$[2)]. Then there exists a finite number of mutually disjoint spherical caps U_α and rotations ρ_α such that:*

(i) $\bigcup_\alpha U_\alpha \subset M$;

(ii) $M' \subset \bigcup_\alpha \rho_\alpha(U_\alpha)$;

(iii) $M \setminus \bigcup_\alpha U_\alpha$ *has non-empty interior.*

Proof of the Theorem. Let μ be a Haar measure on $SO(3)$ such that $\mu(SO(3)) = 1$.

For any $A \subset S$, let Φ_A be the characteristic function of A.

Fix $a \in S$ and let $I_a^A \in \mathbb{R}$ be $I_a^A = \int\limits_{SO(3)} \Phi_A \circ x(a) \mathrm{d}\mu(x)$.

[1)] „Ovidius“ University of Constanţa, Constanţa, Romania, mcavachi@yahoo.com

[2)] For any $A \subset S$, $\mathcal{A}(A)$ denotes its area.

Remark 1. *Note that if b is an arbitrary point on S, then $I_a^A = I_b^A$. Indeed if $\rho \in SO(3)$ is such that $\rho(a) = b$ (and such a ρ always exists), then:*

$$I_b^A = \int\limits_{SO(3)} \Phi_A \circ x(\rho(a))\mathrm{d}\mu(x) = \int\limits_{SO(3)} \Phi_A \circ (x \circ \rho)(a))\mathrm{d}\mu(x \circ \rho) =$$
$$= \int\limits_{SO(3)} \Phi_A \circ x(a)\mathrm{d}\mu(x),$$

since $\mathrm{d}\mu(x \circ \rho) = \mathrm{d}\mu(x)$, the Haar measure being rotation invariant.

Moreover, if $B \subset S$ is an open set such that there exists $\rho_1 \in SO(3)$ with $\rho_1(A) = B$, then again $I_a^A = I_a^B$. Indeed,

$$I_a^B = \int\limits_{SO(3)} \Phi_{\rho(A)} \circ x(a)\mathrm{d}\mu(x) = \int\limits_{SO(3)} \Phi_A \circ \rho_1^{-1} \circ x(a))\mathrm{d}\mu(x) =$$
$$= \int\limits_{SO(3)} \Phi_A \circ (\rho_1^{-1} \circ x)(a)\mathrm{d}\mu(\rho_1^{-1} \circ x) = I_a^A.$$

Returning to the problem, if $X = \{a_1, \ldots, a_n\}$, let

$$f : SO(3) \to \mathbb{R}, \qquad f(x) = \sum_{i=1}^{n} \Phi_M \circ x(a_i).$$

Note that it is enough to find an $x \in SO(3)$ with $f(x) > n - 1$. Then, since $f(x)$ is an integer $\leq qn$, we obtain $f(x) = n$ and hence $x(a_1), \ldots, x(a_n) \in M$, which proves the Theorem. To find such an x, it is enough to show that

$$\int\limits_{SO(3)} f(x)\mathrm{d}\mu(x) > n - 1.$$

But this means that

$$\sum_{i=1}^{n} I_{a_i}^M > n - 1,$$

which is implied by

$$I_{a_i}^M > \frac{n-1}{n}$$

for each i, that is

$$I_a^M > \frac{n-1}{n}.$$

We divide the sphere S in n spherical lunes $F_1, \ldots, F_n$ of equal areas. Obviously, each F_i can be obtained as a rotation of F_1. This implies:

$$1 = I_a^S = \sum_{i=1}^{n} I_a^{F_i} = nI_a^{F_1}, \quad \text{hence} \quad I_a^{F_1} = \frac{1}{n}.$$

Let now $M' = S \setminus F_n$. Then

$$I_a^{M'} = \sum_{i=1}^{n-1} I_a^{F_i} = \frac{n-1}{n}.$$

With U_α and ρ_α as in the Lemma, we deduce:

$$I_a^M > I_a^{\cup_\alpha U_\alpha} = \sum_\alpha I_a^{U_\alpha} = \sum_\alpha I_a^{\rho_\alpha(U_\alpha)} \geq I_a^{M'} = \frac{n-1}{n},$$

and the proof is complete. □

Proof of the Lemma. Let $0 < m < 1$ and let C_i, for $i \in \{1, \ldots, k\}$, be spherical caps of diameter d such that

$$\bigcup_{i=1}^{k} C_i = S,$$

and let P_i be the plane containing the center of S and parallel to the circle bounding C_i. If $\pi_i : S \to P_i$ is the orthogonal projection on P_i, we can choose d small enough such that:

- For any open $C \subset C_i$, we have $\mathcal{A}(\pi_i(C)) > m\mathcal{A}(C)$.
- For any $A \neq B \in C_i$, we have the inequality of segment lengths:

$$|\pi_i(A)\pi_i(B)| > m \cdot |AB|.$$

Define now $M_1 = C_1 \cap M$, $M_2 = C_2 \cap (M \setminus M_1)$,
$M_3 = C_3 \cap (M \setminus M_1 \cup M_2), \ldots, M_k = C_k \cap (M \setminus M_1 \cup \cdots \cup M_{k-1})$, and similarly construct $M_1', M_2', \ldots, M_k'$.

Let $N_i = \pi_i(M_i)$, $N_i' = \pi_i(M_i')$. For $1 - m$ close enough to 0, we have:

$$\sum_{i=1}^{k} \mathcal{A}(N_i) > \sum_{i=1}^{k} \mathcal{A}(N_i').$$

In each plane P_i, we fix a side length ε square lattice. It can be proven (see [1, pag. 315,327]) that the number n_i of squares contained in N_i is

$$\frac{1}{\varepsilon^2}\mathcal{A}(N_i) + O(\frac{1}{\varepsilon}),$$

and analogously we have an approximation for the number n_i' of squares contained in N_i'. Hence, for small enough ε, we get

$$\sum_{i=1}^{k} n_i > \sum_{i=1}^{k} n_i'.$$

Therefore, we can choose an injection u from the set $\mathcal{P}'$ of squares contained in $\bigcup_{i=1}^{k} N_i'$ into the set $\mathcal{P}$ of squares contained in $\bigcup_{i=1}^{k} N_i$.

Let $P \in \mathcal{P}'$ (and hence $P \subset N_i'$ for some i), let $Q \in C_i$ be the point whose projection on P_i is the center of P, and let D_P be the spherical cap defined as the intersection of S with the ball centered in Q and of radius $\varepsilon/2$. Similarly, define $D_{u(P)}$, corresponding to $u(P)$. Clearly, $D_P = \rho_P(D_{u(P)})$ for some $\rho_P \in SO(3)$. We remove from M all the caps $D_{u(P)}$ and from M' all the caps D_P, for $P \in \mathcal{P}'$.

Define now $s = \mathcal{A}(M)$, $s' = \mathcal{A}(M')$. Since $\sum n_i'\varepsilon^2 \to \sum \mathcal{A}(N_i')$, when $\varepsilon \to 0$, we can choose ε and $1 - m$ small enough such the above procedure removes from M and M' the sets $\mathcal{M}_1$ and $\mathcal{M}_1'$ of area greater than $\frac{1}{2}s'$.

Inductively, define S_i, S_i' as follows: $S_1 = M \setminus \mathcal{M}_1$ and $S_1' = M' \setminus \mathcal{M}_1'$. By repeating the above process, obtain the sets S_2, S_2' and so on.

Obviously, $\mathcal{A}(S_t') < \left(\frac{1}{2}\right)^t \to 0$ as t grows to infinty.

Since $\mathcal{A}(S_t) > s - s' > 0$, there exists some t such that

$$\mathcal{A}(S_t) > 4 \cdot \mathcal{A}(S_t').$$

Once again, we go through the first step of the above construction applied to the sets S_t, S_t' with the difference that $\mathcal{P}'$ will be the minimal set of all squares of lattices in P_i which cover $\bigcup_{i=1}^{k} N_i'$, and $\mathcal{P}$ will contain all the squares of lattices with side length 2ε that are included in $\bigcup_{i=1}^{k} N_i$. Also, D_P will be the intersection of S with the ball centered at Q and of radius $\frac{\varepsilon}{\sqrt{2}}$, and $D_{u(P)}$ is constructed analogously. The circle with the same center as $u(P)$, of radius $\frac{\varepsilon}{\sqrt{2}}$, is included in $u(P)$.

Letting the set of U_α be the set of all $D_{u(P)}$, the conditions $(i) - (iii)$ in the Lemma are satisfied and the proof is complete. □

REFERENCES

[1] M. R. Murty, J. Esmonde, *Problems in algebraic number theory*, Springer-Verlag (2005).

PROBLEMS

Authors should submit proposed problems to gmaproblems@rms.unibuc.ro. Files should be in PDF or DVI format. Once a problem is accepted and considered for publication, the author will be asked to submit the TeX file also. The referee process will usually take between several weeks and two months. Solutions may also be submitted to the same e-mail address. For this issue, solutions should arrive before **15th of March 2012**.

PROPOSED PROBLEMS

323. If m, n are given positive integers and A, B, C are three matrices of size $m \times n$ with real entries, then

$$\sum_{cyc}(\det(AB^T))^2 \det(CC^T) \leq \prod \det(AA^T) + 2\prod_{cyc} |\det(AB^T)|.$$

Proposed by Flavian Georgescu, student, University of Bucharest, Bucharest and Cezar Lupu, Politehnica University of Bucharest, Bucharest, Romania.

324. Let p be a prime number and a, b, c, d positive integers such that $a \geq c$ and $b, d \in \{0, 1, \ldots, p-1\}$. Show that

$$\binom{ap+b}{cp+d} \equiv (a-c)\binom{a}{c}\binom{p+b}{d} + c\binom{a}{c}\binom{p+b}{p+d} - (a-1)\binom{a}{c}\binom{b}{d} \pmod{p^2}.$$

Proposed by Marian Tetiva, Gheorghe Roşca Codreanu National College, Bârlad, Romania.

325. Let p be a prime number. Show that $\displaystyle\sum_{k=1}^{p} \sqrt[p]{k + \sqrt[p]{k}}$ cannot be rational.

Proposed by Marius Cavachi, Ovidius University of Constanţa, Constanţa, Romania.

326. Let $A, B \in M_n(\mathbb{R})$ be diagonalisable in $M_n(\mathbb{R})$ such that $\exp(A) = \exp(B)$. Show that $A = B$.

Proposed by Moubinool Omarjee, Jean Lurçat High School, Paris, France.

327. Let N be the $n \times n$ matrix with all its elements equal to $\dfrac{1}{n}$ and $A \in M_n(\mathbb{R})$, $A = (a_{ij})_{1 \leq i,j \leq n}$, such that for some positive integer k one has

$A^k = N$. Show that

$$\sum_{1 \le i,j \le n} a_{ij}^2 \ge 1.$$

Proposed by Lucian Ţurea, Bucharest, Romania.

328. Given $a > 0$, let f be a real-valued continuous function on $[-a, a]$ and twice differentiable on $(-a, a)$. Show that for all $|x| < a$, there exists $|\xi| < x$ such that

$$f(x) + f(-x) - 2f(0) = x^2 f''(\xi).$$

Proposed by George Stoica, University of New Brunswick in Saint John, NB, Canada.

329. Let ABC be a triangle and let P be a point in its interior with pedal triangle DEF. Suppose that the lines DE and DF are perpendicular. Prove that the isogonal conjugate of P is the orthocenter of triangle AEF.

Proposed by Cosmin Pohoaţă, student, Princeton University, Princeton, NJ, USA.

330. It is well-known that for $p > 2$ prime, the number

$$N = \frac{2^{p-1} - 1}{p}$$

is integer. When is N a natural power of an integer?

Proposed by Ion Cucurezeanu, Ovidius University of Constanţa, Constanţa, Romania.

331. Let $f \in \mathbb{Z}[X]$ be a monic polynomial of degree $n+2$, with $f(0) \neq 0$, $n \in \mathbb{N}$, $n \ge 1$. Show that there are only finitely many positive integers a such that $f(X) + aX^n$ is reducible over $\mathbb{Z}[X]$.

Proposed by Vlad Matei, student, University of Cambridge, Cambridge, UK.

332. The cells of a rectangular $2011 \times n$ array are colored using two colors, so that for any two columns the number of pairs of cells situated on a same row and bearing the same color is less than the number of pairs of cells situated on a same row and bearing different colors.

i) Prove that $n \le 2012$ (a model for the extremal case $n = 2012$ does indeed exist, but you are not asked to exhibit one).

ii) Prove that for a square array (i.e. $n = 2011$) each of the colors appears at most $1006 \cdot 2011$ (and thus at least $1005 \cdot 2011$) times.

Proposed by Dan Schwarz, Bucharest, Romania.

333. Prove that for any m, $n \ge 3$ there is an $m \times n$ matrix of rank 2 with entries distinct primes.

Proposed by Constantin-Nicolae Beli, Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania.

334. Define $\mathcal{F} = \{f : [0,1] \to [0,1] : \exists A, B \subset [0,1],\ A \cap B = \emptyset,\ A \cup B = [0,1],\ f(A) \subset B,\ f(B) \subset A\}$. Prove that $\mathcal{F}$ contains functions with Darboux property (a function f has the Darboux property if $f(I)$ is an interval whenever I is an interval).

Proposed by Benjamin Bogoşel, student, West University of Timişoara, Timişoara, Romania.

335. Let $f\colon [0,1] \to \mathbb{R}$ be an integrable function such that $\int_0^1 f(x)\mathrm{d}x = 0$. Prove that

$$\int_0^1 f^2(x)\mathrm{d}x \geq 12\left(\int_0^1 xf(x)\mathrm{d}x\right)^2.$$

Proposed by Cezar Lupu, Politehnica University of Bucharest, Bucharest, Romania, and Tudorel Lupu, Decebal High School, Constanţa, Romania.

336. Given a function $f : \mathbb{R} \to \mathbb{R}$, denote by f^n its nth iterate. It is also given that $|f(x) - f(y)| \leq |x - y|$ for all $x, y \in \mathbb{R}$ (f is Lipschitzian, and non-expansive), and that $f^N(0) = 0$ for some $N \in \mathbb{N}^*$.

i) Prove that if N is odd, then $|f(x)| \leq |x|$ for all $x \in \mathbb{R}$.

ii) Prove that if N is even, then $|f(f(x))| \leq |x|$ for all $x \in \mathbb{R}$, but not necessarily $|f(x)| \leq |x|$.

Proposed by Dan Schwarz, Bucharest, Romania.

SOLUTIONS

309. Consider a prime p and a rational number a such that $\sqrt[p]{a} \notin \mathbb{Q}$. Define a sequence of polynomials by $f_1 = X^p - a$ and $f_{n+1} = f_n^p - a$ for all $n \geq 1$. Show that all terms of the sequence f_n are irreducible polynomials.

Proposed by Marius Cavachi, Ovidius University of Constanţa, Constanţa, Romania.

Solution by the author. We show that the conclusion holds for p odd prime. For the proof we use the following known result (see chapter *Some useful irreducibility criteria* from T. Andreescu and G. Dospinescu, *Problems from the Book*, XYZ Press, 2008).

Lemma 1. *Let K be a field of complex numbers (a subfield of $\mathbb{C}$), $a \in \mathbb{C}$, and let p be a positive prime number. Then the polynomial $X^p - a$ is reducible over K if and only if a is a pth power in K (i. e., if there exists $b \in K$ with $a = b^p$).*

It is sufficient to prove that the degree of the extension $\mathbb{Q} \subset \mathbb{Q}(a_n)$ is p^n, where $(a_n)_{n\geq 1}$ is the recurrent sequence defined by $a_0 = 0$, $a_1 = \sqrt[p]{a}$, $a_{n+1} = \sqrt[p]{a + a_n}$ $(n \geq 1)$. We shall do it by induction on n. For $n = 1$ the property follows from the lemma. It is enough to prove that the extension $\mathbb{Q}(a_n) \subset \mathbb{Q}(a_{n+1})$ has degree p (the statement we wrote previously follows by *Tower Law*), or equivalently that the polynomial $g(X) = X^p - (a + a_n)$, which has a_{n+1} among its roots, is irreducible over $\mathbb{Q}(a_n)[X]$.

We argue by contradiction, so assume the contrary. The previous lemma, it follows that $a_n + a = \alpha^p$, with $\alpha \in \mathbb{Q}(a_n)$. Applying to this equality the norm $\mathbf{N}_{\mathbb{Q}(a_n)/\mathbb{Q}}$, we obtain $\mathbf{N}_{\mathbb{Q}(a_n)/\mathbb{Q}}(a_n + a) = \mathbf{N}^p_{\mathbb{Q}(a_n)/\mathbb{Q}}(\alpha)$.

With the notation $F_k = \mathbb{Q}(a_k)$, $\mathbf{N}_k = \mathbf{N}_{F_k/F_{k-1}}$ $(k \geq 1)$, we can write

$$\begin{aligned}\mathbf{N}_{F_n/\mathbb{Q}}(a_n + a) &= \mathbf{N}_1(\mathbf{N}_2(\ldots(\mathbf{N}_n(a_n + a))\ldots)) = \\ &= \mathbf{N}_1(\mathbf{N}_2(\ldots(\mathbf{N}_n\left(\sqrt[p]{a_{n-1} + a} + a\right))\ldots)) = \\ &= \mathbf{N}_1(\mathbf{N}_2(\ldots(\mathbf{N}_{n-1}(a_{n-1} + a^p + a))\ldots)) = \ldots \\ \ldots &= ((\ldots((a^p + a)^p + a)^p \ldots + a)^p + a)^p + a = h(a).\end{aligned}$$

Letting $b = \mathbf{N}_{F_n/\mathbb{Q}}(\alpha)$, it follows that $h(a) = b^p$.

Let $a = \dfrac{r}{s}$, $r,\ s \in \mathbb{Z}$, $\gcd(r, s) = 1$. Multiplying the equality above by s^{p^n}, we get an equality of the form $rs^{p^n-1}(1 + rsc) = b^p$, $c \in \mathbb{Z}$. Since all of the terms r, s^{p^n-1} and $1 + rsc$ are pairwise coprime, it follows that each of them is a pth power, so $\sqrt[p]{a} = \sqrt[p]{\dfrac{r}{s}} \in \mathbb{Q}$, a contradiction.

Solution by Marian Tetiva, Gheorghe Roşca Codreanu National College, Bârlad, Romania. Thus stated, the problem is definitely false. Take, for example, $p = 2$ and $a = \dfrac{4}{3}$; then $f_1 = X^2 - \dfrac{4}{3}$ and

$$f_2 = \left(X^2 - \frac{4}{3}\right)^2 - \frac{4}{3} = X^4 - \frac{8}{3}X^2 + \frac{4}{9} = \left(X^2 - 2X + \frac{2}{3}\right)\left(X^2 + 2X + \frac{2}{3}\right)$$

is reducible over $\mathbb{Q}$.

However we are able to prove that the assertion is true when a is *integer*. In order to do that, we use the following auxiliary results.

Lemma 2. *For integers a, n, p with n positive and p prime, the number*

$$(\cdots(((a^p - a)^p - a)^p - a)^p \cdots)^p - a$$

(with n parentheses) is a perfect pth power if and only if either $a = 0$ (with arbitrary p and n) or $a = 1$, p is arbitrary, and $n = 1$.

The number

$$(\cdots(((a^p + a)^p + a)^p + a)^p \cdots)^p + a$$

is a pth power of an integer if and only if either $a = 0$ (with arbitrary p and n) or $a = -1$, $p = 2$, and $n = 1$.

Lemma 3. *(Capelli's theorem) Let K be a subfield of $\mathbb{C}$ and let f, g be polynomials from $K[X]$. Suppose that f is irreducible in $K[X]$ and there exists a complex root α of f such that $g-\alpha$ is irreducible in $K[\alpha][X]$. Then $f(g(X))$ is irreducible in $K[X]$.*

Lemma 1 is just an exercise in elementary arithmetics (the number from the statement is between two consecutive pth powers that are easy to write down). For a proof of Lemma 3, we refer the reader to the chapter *Some useful irreducibility criteria* from Dospinescu and Andreescu's book cited in the previous solution.

Now we solve the problem (with integer a). Put

$$f_1(X)=f(X),\quad f_{n+1}(X)=f_1(f_n(X))\quad \text{for all}\quad n\geq 1.$$

Then $f_n(X)=f_1(\cdots(f_1(X))\cdots)$ (with n appearances of f_1), therefore

$$f_{n+1}(X)=f_n(f_1(X))$$

also holds for all $n\geq 1$.

We prove the result by induction on n. For $n=1$, the irreducibility of f_1 follows by Lemma 2 (of course, we assume that it's irreducibility over $\mathbb{Q}$ of which we are talking about).

Assume further that f_n is irreducible over $\mathbb{Q}$, and let's prove that f_{n+1} is irreducible, too. We try to apply *Capelli*'s theorem, with $f=f_n$ (irreducible, according to the induction hypothesis), and $g=f_1$. So, we need to show that, for a certain root α of f_n, the polynomial $f_1-\alpha=X^p-a-\alpha$ is irreducible over $\mathbb{Q}[\alpha]$. Suppose not. Using Lemma 2 once again, this means that $a+\alpha$ is a pth power in $\mathbb{Q}[\alpha]$, that is, there are $b_0,\ldots,b_{m-1}\in\mathbb{Q}$ (with $m=p^n$, the degree of f_n and of α over $\mathbb{Q}$), such that

$$(b_0+b_1\alpha+\cdots+b_{m-1}\alpha^{m-1})^p=a+\alpha.$$

Let $\alpha_1=\alpha,\alpha_2,\ldots,\alpha_m$ be all the roots of f_n. Because the polynomial with rational coefficients

$$(b_0+b_1X+\cdots+b_{m-1}X^{m-1})^p-(a+X)$$

has the root α, it must be divisible with f_n (which, being irreducible, is the minimal polynomial of α), therefore it has all α_j as zeros. By multiplying side by side all equalities

$$(b_0+b_1\alpha_j+\cdots+b_{m-1}\alpha_j^{m-1})^p=a+\alpha_j,\ \ 1\leq j\leq m,$$

one gets

$$\prod_{j=1}^{m}(b_0+b_1\alpha_j+\cdots+b_{m-1}\alpha_j^{m-1})^p=\prod_{j=1}^{m}(a+\alpha_j)$$

or

$$b^p=\prod_{j=1}^{m}(a+\alpha_j)$$

for some b which is a rational number according to the fundamental theorem of symmetric polynomials. Actually in the right hand side we have

$$(-1)^m \prod_{j=1}^{m}(-a-\alpha_j) = (-1)^m f_n(-a) \in \mathbb{Z},$$

that is b^p needs to be an integer and, consequently, b is an integer, too.

As one can immediately see, this leads to an equality of the form

$$(\cdots((a^2-a)^2-a)^2\cdots)^2 - a = b^2$$

when $p=2$, or of the form

$$(\cdots((a^p+a)^p+a)^p\cdots)^p + a = b^p$$

when p is an odd prime, with integers a and b.

According to Lemma 1 (and because $|a| \geq 2$), such an equality is impossible, hence our assumption (that $f_1 - \alpha$ is reducible over $K[\alpha]$) is false, and the conditions to apply *Capelli*'s theorem are fulfilled, leading to the conclusion that f_{n+1} is irreducible. □

Remark. The counterexample we gave at the beginning of the solution is for $p=2$; we did not find one for odd prime p. Note that Lemma 1 is not true when $p=2$ if both a and b are assumed to be rational. If it were true for odd p, it would give us a proof for the original statement (with rational a) — but it seems hard to find an argument for that.

310. For $n \geq 4$, $1 \leq \delta < \Delta \leq n-1$, $n, \delta, \Delta \in \mathbb{N}$, consider the function

$$f(x_\delta, x_{\delta+1}, \ldots, x_\Delta) = \sum_{\delta \leq i < j \leq \Delta} \left(\frac{1}{\sqrt{i}} - \frac{1}{\sqrt{j}}\right)^2 x_i x_j$$

and the domain

$$D = \{(x_\delta, x_{\delta+1}, \ldots, x_\Delta) : x_i \in \mathbb{N} \text{ for } \delta \leq i \leq \Delta, \sum_{i=\delta}^{\Delta} x_i = n\}.$$

Show that if $(x_\delta, \ldots, x_\Delta) \in D$ then

$$f(x_\delta, \ldots, x_\Delta) \leq \left(\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{\Delta}}\right)^2 \alpha(n),$$

where $\alpha(n) = n^2/4$ for n even and $\alpha(n) = (n^2-1)/4$ for n odd. When does equality hold?

Proposed by Ioan Tomescu, University of Bucharest, Bucharest, Romania.

Solution by the author. We shall prove that all points where f is maximum in D are the following:

i) If $n \geq 4$ is even, then $\max_D f(x_\delta, \ldots, x_\Delta)$ is reached for $(n/2, 0, \ldots, 0, n/2)$;

ii) If $n \geq 5$ is odd, then $\max_D f(x_\delta, \ldots, x_\Delta)$ is attained for

$$((n-1)/2, 0, \ldots, 0, (n+1)/2) \quad \text{and} \quad ((n+1)/2, 0, \ldots, 0, (n-1)/2).$$

If $x_{\delta+1} = \ldots = x_{\Delta-1} = 0$ then

$$f(x_\delta, \ldots, x_\Delta) = (\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{\Delta}})^2 x_\delta x_\Delta$$

and the result is obvious since $x_\delta + x_\Delta = n$. Otherwise, denote by $i\,(\delta+1 \leq i \leq \Delta-1)$ the smallest index such that $x_i \geq 1$ and by $j\,(\delta+1 \leq j \leq \Delta-1)$ the greatest index such that $x_j \geq 1$; obviously $i \leq j$. Denote by α and β the operations consisting of replacing $x = (x_\delta, \ldots, x_\Delta) \in D$ by $x' = (x_\delta, 0, \ldots, 0, x_i, \ldots, x_{j-1}, x_j - 1, 0, \ldots, 0, x_\Delta + 1) \in D$ and by $x'' = (x_\delta + 1, 0, \ldots, 0, x_i - 1, x_{i+1}, \ldots, x_j, 0, \ldots, 0, x_\Delta) \in D$, respectively. We have

$$\begin{aligned} f(x') - f(x) = \left(\frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right)^2 (x_j - x_\Delta - 1) + \\ + x_\delta \left(\frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right)\left(\frac{2}{\sqrt{\delta}} - \frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right) + \\ + x_i \left(\frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right)\left(\frac{2}{\sqrt{i}} - \frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right) + \\ + x_{i+1} \left(\frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right)\left(\frac{2}{\sqrt{i+1}} - \frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right) + \\ + \cdots + x_{j-1} \left(\frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right)\left(\frac{2}{\sqrt{j-1}} - \frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right). \end{aligned}$$

Since $\frac{2}{\sqrt{k}} - \frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}} > \frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}$ for $k = \delta, i, i+1, \ldots, j-1$, we can write

$$f(x') - f(x) \geq \left(\frac{1}{\sqrt{j}} - \frac{1}{\sqrt{\Delta}}\right)^2 (x_\delta + x_i + x_{i+1} + \ldots + x_j - x_\Delta - 1), \quad (1)$$

and this inequality is strict if at least one of x_δ, x_i, $x_{i+1}, \ldots, x_{j-1}$ is different from zero. Similarly,

$$\begin{aligned} f(x'') - f(x) = \left(\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{i}}\right)^2 (x_i - x_\delta - 1) + \\ + x_{i+1} \left(\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{i}}\right)\left(\frac{1}{\sqrt{\delta}} + \frac{1}{\sqrt{i}} - \frac{2}{\sqrt{i+1}}\right) + \ldots + x_j \left(\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{i}}\right) + \\ + \left(\frac{1}{\sqrt{\delta}} + \frac{1}{\sqrt{i}} - \frac{2}{\sqrt{j}}\right) + x_\Delta \left(\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{i}}\right)\left(\frac{1}{\sqrt{\delta}} + \frac{1}{\sqrt{i}} - \frac{2}{\sqrt{\Delta}}\right), \end{aligned}$$

which implies

$$f(x'') - f(x) \geq \left(\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{i}}\right)^2 (x_i + x_{i+1} + \ldots + x_j + x_\Delta - x_\delta - 1). \quad (2)$$

This last inequality is strict if at least one of $x_{i+1}, \ldots, x_j, x_\Delta$ is different from zero.

If $i = j$ we get

$$f(x') - f(x) \geq \left(\frac{1}{\sqrt{i}} - \frac{1}{\sqrt{\Delta}}\right)^2 (x_\delta + x_i - x_\Delta - 1), \tag{3}$$

the inequality being strict if $x_\delta \geq 1$, and

$$f(x'') - f(x) \geq \left(\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{i}}\right)^2 (x_\Delta + x_i - x_\delta - 1), \tag{4}$$

this inequality being strict if $x_\Delta \geq 1$.

We shall prove that at least one of the differences $f(x') - f(x)$ and $f(x'') - f(x)$ is positive, which implies that all sequences $(x_\delta, \ldots, x_\Delta) \in D$ realizing the maximum of f satisfy $x_{\delta+1} = \ldots = x_{\Delta-1} = 0$. Consider first the case when $i = j$. It is clear that if $x_\delta = x_\Delta = 0$ then $f(x_\delta, \ldots, x_\Delta) = 0$, which implies that $(0, \ldots, 0, x_i, 0, \ldots, 0)$ cannot maximize f. Otherwise, suppose that $x_\delta \geq 1$. If $x_\delta + x_i - x_\Delta - 1 \geq 0$ then inequality (3) is strict and it follows that $f(x') > f(x)$, so that x cannot maximize f on D. Otherwise, $x_\delta + x_i - x_\Delta - 1 \leq -1$. In this case $x_\Delta \geq x_\delta + x_i$, hence $x_\Delta + x_i - x_\delta - 1 \geq 2x_i - 1 \geq 1$, which implies $f(x'') > f(x)$ and x also cannot maximize f. If $x_\Delta \geq 1$ the same conclusion follows since inequality (4) is strict.

Suppose that $i < j$. In this case $x_i > 0$, $x_j > 0$ and both inequalities (1) and (2) are strict. If $x_\delta + x_i + \cdots + x_j - x_\Delta - 1 \geq 0$ then from (1) it follows that $f(x') > f(x)$. Otherwise, $x_\Delta \geq x_\delta + x_i + \cdots + x_j$ and $x_i + \cdots + x_j + x_\Delta - x_\delta - 1 \geq 2(x_i + \cdots + x_j) - 1 > 0$, which implies $f(x'') > f(x)$ from (2).

Consequently, all sequences maximizing f have the form $(n_1, 0, \ldots, 0, n_2)$, where $n_1 + n_2 = n$; in this case

$$f(n_1, 0, \ldots, 0, n_2) = \left(\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{\Delta}}\right)^2 n_1 n_2 \leq \left(\frac{1}{\sqrt{\delta}} - \frac{1}{\sqrt{\Delta}}\right)^2 \varphi(n),$$

and the conclusion follows. □

311. Show that for any matrix $A \in M_2(\mathbb{R})$ there exist X, $Y \in M_2(\mathbb{R})$ with $XY = YX$ such that $A = X^{2n+1} + Y^{2n+1}$ for all $n \geq 1$.

Proposed by Vlad Matei, student, University of Bucharest, Bucharest, Romania.

Solution by the author. We can prove easily by induction, using Hamilton-Cayley relation $A^2 - \mathrm{Tr}(A)A + \det(A)I_2 = O_2$, that there are a_k, $b_k \in \mathbb{R}$ such

that $a_kA = A^k + b_kI_2$, for all $k \geq 1$. For x real number, we therefore have

$$\begin{aligned}(A + xI_2)^{2n+1} &= \sum_{k=0}^{2n+1} x^k A^{2n+1-k}\binom{2n+1}{k} \\ &= \sum_{k=0}^{n} x^k(a_{2n+1-k}A - b_{2n+1-k}I_2)\binom{2n+1}{k} \\ &= A\sum_{k=0}^{2n+1} x^k a_{2n+1-k}\binom{2n+1}{k} - I_2\sum_{k=0}^{2n+1} x^k b_{2n+1-k}\binom{2n+1}{k}.\end{aligned}$$

Now we look at the polynomials

$$f(x) := \sum_{k=0}^{2n+1} x^k a_{2n+1-k}\binom{2n+1}{k}, \quad g(x) := \sum_{k=0}^{2n+1} x^k b_{2n+1-k}\binom{2n+1}{k}.$$

We have $a_1 = 1$, so that f is not the zero polynomial. Thus we can find $c \in \mathbb{R}$ such that $f(c) \neq 0$. We get

$$\left(\frac{A + cI_2}{\sqrt[2n+1]{f(c)}}\right)^{2n+1} + \left(\sqrt[2n+1]{\frac{g(c)}{f(c)}} \cdot I_2\right)^{2n+1} = A.$$

It is obvious that these two matrices commute. □

312. Let p_n be the nth prime number. Show that the sequence $(x_n)_{n\geq 1}$ defined by

$$x_n = \left\{\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}\right\} - \{\log\log n\}$$

is divergent. Here $\{x\}$ denotes the fractional part of the real number x.

Proposed by Cezar Lupu, Politehnica University of Bucharest, Bucharest, Romania and Cristinel Mortici, University of Valahia, Târgovişte, Romania.

Solution by the authors. Here log denotes the natural logarithm (the inverse function of exponential function).

First of all, it is well-known that there are infinitely many prime numbers. Let us denote by $\pi(x)$ the counting function of prime numbers. From the prime number theorem we infer

$$\pi(x) \sim \frac{x}{\log x} \quad \text{for} \quad x \to \infty.$$

Putting here $x = p_n$, we get $n \sim \dfrac{p_n}{\log p_n}$, and by taking the logarithm we deduce $\log n \sim \log p_n - \log\log p_n$. On the other hand, we have

$$\frac{\log n}{\log p_n} \sim 1 - \frac{\log\log p_n}{\log p_n},$$

and since $\lim\limits_{x\to\infty}\dfrac{\log\log x}{\log x}=0$, we obtain $\log n\sim\log p_n$. Combining with the fact that $n\sim\dfrac{p_n}{\log p_n}$ we thus obtain $p_n\sim n\log n$. It is obvious that the sequence $(P_n)_{n\geq 1}$ defined by

$$P_n=\frac{1}{p_1}+\frac{1}{p_2}+\cdots+\frac{1}{p_n}$$

diverges because we have $\displaystyle\sum_{n=1}^{\infty}\frac{1}{p_n}\sim\sum_{n=2}^{\infty}\frac{1}{n\log n}$, which is the celebrated Bertrand series. Now, let's prove that the sequence $(\mathcal{P}_n)_{n\geq 2}$ defined by

$$\mathcal{P}_n=P_n-\log\log n$$

is convergent. We have $\mathcal{P}_{n+1}-\mathcal{P}_n=\dfrac{1}{p_{n+1}}-(\log\log(n+1)-\log\log n)$. On the other hand, it is well-known that $p_n>n\log n$ for all $n\geq 1$, and by Lagrange's theorem applied to the function $\log\log x$ we infer the inequalities

$$\frac{1}{(n+1)\log(n+1)}<\log\log(n+1)-\log\log n<\frac{1}{n\log n},\ \text{for all } n>1.$$

From these inequalities we conclude that the sequence $\mathcal{P}_n$ is strictly decreasing. However, as it is shown in F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. reine angew. Math., 78(1874), 46–62, there exists $\lim\limits_{n\to\infty}\mathcal{P}_n=B$, where $B\simeq 0.261497$ is known as Meissel-Mertens constant. It is obvious that $\mathcal{P}_n\in[0,1]$.

Next, we prove that $x_n\in\{\mathcal{P}_n-1,\mathcal{P}_n\}$ for all $n\geq 2$. Indeed, we have

$$x_n=P_n-\log\log n-([P_n]-[\log\log n])=\mathcal{P}_n-([\log\log n+\mathcal{P}_n]-[\log\log n]).$$

Since $\mathcal{P}_n\in[0,1]$, we have $[\log\log n]\leq[\log\log n+\mathcal{P}_n]\leq[\log\log n+1]=1+[\log\log n]$, so $0\leq[\log\log n+\mathcal{P}_n]-[\log\log n]\leq 1$, and we obtain that $x_n\in\{\mathcal{P}_n-1,\mathcal{P}_n\}$ for all $n\geq 2$, as claimed.

Now we can solve the problem. We assume, for the sake of a contradiction, that the sequence x_n is convergent. This implies

$$\lim_{n\to\infty}(x_{n+1}-x_n)=\lim_{n\to\infty}\big(\mathcal{P}_{n+1}-\mathcal{P}_n-[P_{n+1}]-[\log\log n]+$$
$$+[P_n]+[\log\log(n+1)]\big)=0,$$

which is equivalent to

$$\lim_{n\to\infty}\big([P_{n+1}]-[P_n]-[\log\log(n+1)]+[\log\log n]\big)=0.$$

This means that each term of the sequence

$$y_n=[P_{n+1}]-[P_n]-[\log\log(n+1)]+[\log\log n]$$

is the integer 0 from a rank n_1 onwards. In other words, we have

$$[P_{n+1}]-[P_n]=[\log\log(n+1)]-[\log\log n]\ \text{for all } n\geq n_1.$$

Since $\lim_{n\to\infty} P_n = \infty$, there exist infinitely many positive integers $m \geq n_1$ such that $[P_m] = a_m \neq [P_{m+1}]$, $a_m \in \mathbb{N}$. Since $P_{n+1} = P_n + \dfrac{1}{p_{n+1}} < P_n + 1$, we have $[P_{m+1}] = a_m + 1$, whence $1 = [\log\log(m+1)] - [\log\log m]$. Put $b_m = [\log\log m]$, so that $b_m + 1 = [\log\log(m+1)]$. Now, if $a_m = b_m$, then it follows

$$\log\log m < P_m < a_m + 1 = [\log\log(m+1)] \leq \log\log(m+1) < P_{m+1}.$$

Then we obtain that the inequality between the extreme terms in the chain

$$\begin{aligned} B &< P_{m+1} - \log\log m < P_{m+1} - P_m + \log\log(m+1) - \log\log m \\ &< \frac{1}{(m+1)\log(m+1)} + \frac{1}{m\log m} < \frac{2}{m\log m} \end{aligned}$$

holds for infinitely many positive integers m, which is false. If $b_m < a_m$, then we have

$$\log\log m < b_m + 1 \leq a_m < \log\log(m+1) < P_{m+1},$$

whence $P_{m+1} - \log\log m > a_m - b_m \geq 1$. As $\lim_{n\to\infty}(P_n - \log\log n) = B \in (0,1)$, we again reached a contradiction. □

313. Does there exist a set M of points in the Euclidean plane such that the distance between any two of them is larger than 1 and such that there is a point in M between any two distinct parallel lines in the plane? Justify your answer.

Proposed by Marius Cavachi, Ovidius University of Constanţa, Constanţa, Romania.

Solution by the author. Such a set does indeed exist. Choose a system of coordinates and write $d:\ y = mx+n$ instead of "the equation of the line d is $y = mx+n$". According to Kronecker's density theorem, between any two parallel lines of irrational slope there exists a point of the lattice $2\mathbb{Z}\times 2\mathbb{Z}$. It remains to treat the case of parallel lines whose slope is either rational or ∞. In what follows, p, q, r are varying rational numbers. Consider the countable sets

$$\begin{aligned} A &= \{d \mid d:\ y = px + r;\ p > 0, r < 0\} \cup \{d \mid d:\ x = q;\ q > 0\}, \\ B &= \{d \mid d:\ y = px + r;\ p < 0, r < 0\} \cup \{d \mid d:\ y = q;\ q < 0\}, \\ C &= \{d \mid d:\ y = px + r;\ p > 0, r > 0\} \cup \{d \mid d:\ x = q;\ q < 0\}, \\ D &= \{d \mid d:\ y = px + r;\ p < 0, r > 0\} \cup \{d \mid d:\ y = q;\ q > 0\}. \end{aligned}$$

Write A as a sequence $(a_n)_{n\geq 1}$ and similarly for B, C and D. Then define

$$\begin{aligned} A_n &= a_n \cap \{(x, 2n+1) \mid x > 0\}, \\ B_n &= b_n \cap \{(2n+1, y) \mid y < 0\}, \\ C_n &= c_n \cap \{(x, -2n-1) \mid x < 0\}, \\ D_n &= d_n \cap \{(-2n-1, y) \mid y > 0\}. \end{aligned}$$

We show that the set $M = (2\mathbb{Z} \times 2\mathbb{Z}) \cup \{A_n, B_n, C_n, D_n \mid n \geq 1\}$ has the required properties.

The distance between any two points of M is at least one because their x or y coordinates differ by at least one. Also, between any two distinct parallel lines there exists one lying in A, B, C or D, so at least one point from $\{A_n, B_n, C_n, D_n \mid n \geq 1\}$. □

314. Let $f : [0,1] \to \mathbb{R}$ be a C^2 real-valued function on $[0,1]$ which is convex on $[0,1]$. Prove

$$\int_0^1 f(x)\mathrm{d}x \leq \frac{1}{4}\left(f(0) + f\left(\frac{1}{3}\right) + f\left(\frac{2}{3}\right) + f(1)\right).$$

Proposed by Tudorel Lupu, Decebal High School of Constanţa, Constanţa, Romania.

Solution by the editors. We shall use the following lemmas.

Lemma 4. *Any convex function $f : [a,b] \to \mathbb{R}$ is continuous on the open interval (a,b).*

Lemma 5. *(Hermite-Hadamard inequality) Let $f : [a,b] \to \mathbb{R}$ be a convex function on $[a,b]$. Then the following inequalities hold:*

$$(b-a)f\left(\frac{a+b}{2}\right) \leq \int_a^b f(x)\mathrm{d}x \leq (b-a)\frac{f(a)+f(b)}{2}.$$

Lemma 6. *(Hardy-Littlewood-Pólya) Let $f : [a,b] \to \mathbb{R}$ be a convex function on $[a,b]$. Then the inequality*

$$\frac{f(a)+f(b)}{2} - f\left(\frac{a+b}{2}\right) \geq \frac{f(c)+f(d)}{2} - f\left(\frac{c+d}{2}\right)$$

holds for any $a \leq c \leq d \leq b$.

Returning to our problem, we split the integral $\int_0^1 f$ into

$$\int_0^{1/3} f + \int_{1/3}^{2/3} f + \int_{2/3}^1 f.$$

By Lemma 5, we have

$$\int_0^1 f(x)\mathrm{d}x \le \frac{1}{3}\left(\frac{f(0)+f(1/3)}{2} + \frac{f(1/3)+f(2/3)}{2} + \frac{f(2/3)+f(1)}{2}\right),$$

so we only need to prove

$$\frac{f(0)+2f(1/3)+2f(2/3)+f(1)}{6} \le \frac{f(0)+f(1/3)+f(2/3)+f(1)}{4},$$

which is equivalent to $f\left(\frac{1}{3}\right)+f\left(\frac{2}{3}\right) \le f(0)+f(1)$. This inequality follows from Lemma 6 appplied for $a=0, b=1$ and $c=\frac{1}{3}, d=\frac{2}{3}$.

Solution by Marian Tetiva, Gheorghe Roşca Codreanu National College, Bârlad, Romania. There's no need that the function be C^2; being convex is enough to ensure for f the inequality

$$\int_0^1 f(x)\mathrm{d}x \le \frac{1}{n+1}\sum_{k=0}^{n} f\left(\frac{k}{n}\right)$$

for every positive integer n. (Note that f is Riemman integrable by Lemma 4.) Indeed, denote by x_n the right hand side of the above inequality. By convexity, we have the inequalities

$$(k+1)f\left(\frac{k}{n}\right) + (n-k)f\left(\frac{k+1}{n}\right) \ge (n+1)f\left(\frac{k+1}{n+1}\right)$$

for all $k=0,1,\ldots,n-1$. Summing them up we get (after some easy algebraic manipulations) $x_n \ge x_{n+1}$ for all $n \ge 1$; that is, the sequence (x_n) is decreasing. On the other hand,

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \frac{n}{n+1}\cdot\frac{1}{n}\sum_{k=0}^{n} f\left(\frac{k}{n}\right) = \int_0^1 f(x)\mathrm{d}x,$$

according to the definition of the Riemann integral. The well-known fact that the limit of a decreasing sequence is at most equal to each term of the sequence gives the desired inequality (and for $n=3$ one gets the inequality required by the proposer).

Remark. The monotonicity of the sequence (x_n) is also stated in problem XII.22 proposed by Ion Raşa in *Revista matematică din Timişoara*, **1**(1997), p. 53.

Solution by Angel Plaza, Las Palmas University, Las Palmas, Spain. Since f is a C^2 real-valued function on $[0,1]$ which is convex on $[0,1]$, $f(x) \leq r(x)$ for all secant lines of its graph, for x between the two abscissas of the secant points. Considering the three linear functions passing through the points of abscissas 0, $\frac{1}{3}$, $\frac{2}{3}$ and 1, it is obtained

$$\begin{aligned}\int_0^1 f(x)\mathrm{d}x &\leq \frac{1}{3}\left(\frac{f(0)+f(1/3)}{2}+\frac{f(1/3)+f(2/3)}{2}+\frac{f(2/3)+f(1)}{2}\right)\\ &= \frac{1}{6}f(0)+\frac{1}{3}f\left(\frac{1}{3}\right)+\frac{1}{3}f\left(\frac{2}{3}\right)+\frac{1}{6}f(1)\end{aligned}$$

On the other hand, since f is convex,

$$f\left(\frac{1}{3}\right) \leq \frac{1}{2}\left(f(0)+f\left(\frac{2}{3}\right)\right)$$

and

$$f\left(\frac{2}{3}\right) \leq \frac{1}{2}\left(f\left(\frac{1}{3}\right)+f(1)\right).$$

Therefore it is also obtained

$$\int_0^1 f(x)\mathrm{d}x \leq \frac{1}{3}f(0)+\frac{1}{6}f\left(\frac{1}{3}\right)+\frac{1}{6}f\left(\frac{2}{3}\right)+\frac{1}{3}f(1).$$

By summing up the two inequalities for $\int_0^1 f(x)\mathrm{d}x$, we get

$$\int_0^1 f(x)\mathrm{d}x \leq \frac{1}{4}\left(f(0)+f\left(\frac{1}{3}\right)+f\left(\frac{2}{3}\right)+f(1)\right). \qquad \square$$

Remark. The author proved that for any C^2 real-valued function f on $[0,1]$ there exists $c \in (0,1)$ such that

$$\int_0^1 f(x)\mathrm{d}x = \frac{1}{4}\left(f(0)+f(1/3)+f(2/3)+f(1)\right)-\frac{1}{36}f''(c).$$

The required inequality follows since the second derivative of a convex function is non-negative.

315. Let $f : [0; 2\pi] \to \mathbb{R}$ be such that $\int_0^{2\pi} f(x)\cos kx\mathrm{d}x = 1$ for all $k = \overline{1,n}$, where $n \geq 2$ is a fixed positive integer. Find the minimum of $\int_0^{2\pi} f^2(x)\mathrm{d}x$ over all such functions f.

Proposed by Vlad Matei, student, University of Bucharest, Bucharest, Romania.

Solution by the author. We search for a function $g(x) = \sum_{k=1}^{n} a_k \cos kx$ which satisfies the required conditions. From the hypothesis we get

$$\int_0^{2\pi} (f(x) - g(x))\cos kx\mathrm{d}x = 0,$$

for all $k = \overline{1,n}$, whence $\int_0^{2\pi} (f(x)-g(x))g(x)\mathrm{d}x = 0$. Using this, we can rewrite $\int_0^{2\pi} (f(x) - g(x))^2\mathrm{d}x \geq 0$ as $\int_0^{2\pi} f^2(x)\mathrm{d}x \geq \int_0^{2\pi} f(x)g(x)\mathrm{d}x$. Since

$$\int_0^{2\pi} f(x)g(x)\mathrm{d}x = \sum k = 1^n a_k \int_0^{2\pi} f(x)\cos kx\mathrm{d}x = \sum k = 1^n a_k,$$

we conclude that $\int_0^{2\pi} f^2(x)\mathrm{d}x \geq \sum k = 1^n a_k$.

It remains to determine a_k for $k = \overline{1,n}$.

It is known that $\int_0^{2\pi} \cos ix\cos jx\mathrm{d}x = \pi\delta_{ij}$, where δ_{ij} is the *Kronecker* symbol. Since g satisfies the initial conditions, we obtain $a_k = 1/\pi$ for all $k = \overline{1,n}$.

Puting all this together, we get $\int_0^{2\pi} f^2(x)\mathrm{d}x \geq n/\pi$. From this proof it is obvious that the equality is attained if and only if $f(x) = \frac{1}{\pi}\sum k = 1^n \cos kx$. Thus, n/π is the required minimum. □

316. Let $f : [0,1] \to [0,\infty)$ and $g : [0,1] \to [0,1]$ be two integrable functions. Prove that for any positive integers p, q, s, t with $p \neq q$, the following inequality holds

$$\int_0^1 f^p(x)g^s(x)\mathrm{d}x \cdot \int_0^1 f^q(x)g^t(x)\mathrm{d}x \leq \int_0^1 f^{p+q}(x) \cdot g^{\frac{sp-qt}{p-q}}(x)\mathrm{d}x.$$

Proposed by Andrei Deneanu, student, Oxford University, Oxford, UK and Cezar Lupu, Politehnica University of Bucharest, Romania.

Solution by the authors. Let us consider integrable functions

$$F, G : [0,1] \to [0,\infty) \quad \text{such that} \quad \int_0^1 G(x)\mathrm{d}x \leq 1.$$

We shall prove that for any positive integers p, q, s, t, the following inequality holds:

$$\int_0^1 F^p(x)G(x)\mathrm{d}x \int_0^1 F^q(x)G(x)\mathrm{d}x \leq \int_0^1 F^{p+q}(x)G(x)\mathrm{d}x. \tag{5}$$

This is trivially true if

$$\int_0^1 F(x)G(x)\mathrm{d}x = 0,$$

so below we may assume

$$\int_0^1 F(x)G(x)\mathrm{d}x \neq 0.$$

If $p = q$ the asserted inequality is an immediate consequence of the well-known *Cauchy-Buniakovski-Schwarz* inequality. We shall proceed by induction on $p + q$. Without loss of generality, we may assume that $q > p$. By applying *Cauchy-Buniakovski-Schwarz* integral inequality, we get

$$\int_0^1 \left(\sqrt{F^{p+q}(x)G(x)}\right)^2 \mathrm{d}x \cdot \int_0^1 \left(\sqrt{F^{q-p}(x)G(x)}\right)^2 \mathrm{d}x \geq \left(\int_0^1 F^q(x)G(x)\mathrm{d}x\right)^2.$$

On the other hand, by the induction hypothesis, we have the inequality

$$\int_0^1 F^q(x)G(x)\mathrm{d}x \geq \int_0^1 F^p(x)G(x)\mathrm{d}x \cdot \int_0^1 F^{q-p}(x)G(x)\mathrm{d}x.$$

Now, inequality (5) follows after simplification of $\int_0^1 F^{q-p}(x)G(x)\mathrm{d}x$ in

$$\int_0^1 F^{p+q}(x)G(x)\mathrm{d}x \int_0^1 F^{q-p}(x)G(x)\mathrm{d}x \geq$$

$$\geq \int_0^1 F^{q}(x)G(x)\mathrm{d}x \int_0^1 F^{p}(x)G(x)\mathrm{d}x \int_0^1 F^{q-p}(x)G(x)\mathrm{d}x.$$

To solve our problem, we apply inequality (5) for

$$F(x) = f(x)g^{\frac{s-t}{p-q}}(x), \quad G(x) = g^{\frac{pt-sq}{p-q}}(x). \qquad \square$$

317. For integer $n \geq 2$, determine the dimension of

$$V = \operatorname{span}\left\{ \frac{P(x)}{1-x^{\deg P+1}} \ : \ P(x) \in \mathbb{R}[x],\ 0 \leq \deg P < n-1, \deg P + 1 \mid n \right\}$$

as a subspace of the $\mathbb{R}$-linear space $\mathbb{R}(x)$.

Proposed by Dan Schwarz, Bucharest, Romania.

Solution by the author. Write the canonical factorization $n = \prod_{i=1}^{s} p_i^{e_i}$. Denote by V_i the span of the elements with $\deg P + 1 | \frac{n}{p_i}$. It is clear that every element belongs to (at least) one of these subspaces, hence

$$V = \operatorname{span}\left(\bigcup_{i=1}^{s} V_i \right).$$

Since $\dim(\operatorname{span}(A \cup B)) = \dim A + \dim B - \dim(A \cap B)$ for linear subspaces A, B, by induction one gets the inclusion/exclusion formula

$$\dim V = \sum k = 1^s(-1)^{k-1} \sum |I| = k \dim\left(\bigcap_{i\in I} V_i \right).$$

But

$$\dim\left(\bigcap_{i\in I} V_i \right) = \frac{n}{\prod_{i\in I} p_i},$$

so

$$\dim V = n \sum k = 1^s(-1)^{k-1} \sum |I| = k \frac{1}{\prod_{i\in I} p_i} =$$

$$= n\left(1 - \prod_{k=1}^{s}\left(1 - \frac{1}{p_k}\right)\right) = n - \varphi(n),$$

therefore $\dim V = n - \varphi(n)$, with $\varphi(n)$ Euler's indicator function. □

Remark. One may ask the same question in $\mathbb{R}[[x]]$ instead of $\mathbb{R}[x]$.

318. Let f be a polynomial with integer coefficients, $\deg(f) \geq 1$, and k a positive integer. Show that there are infinitely many positive integers n such that $f(n)$ can be written in the form $f(n) = d_1 d_2 \ldots d_k d_{k+1}$, where $1 \leq d_1 < d_2 < \ldots < d_k < n$.

Proposed by Marian Tetiva, Gheorghe Roşca Codreanu National College, Bârlad, Romania.

Solution by the author. We can assume, without loss of generality, that f has the leading coefficient positive, otherwise we can prove for $-f$, and this implies the result for f. Thus, $f(n)$ is positive for all n large enough.

Next, it is easy to verify through direct calculations that $f\big(X + f(X)\big)$ is divisible by $f(X)$, so $f\big(X + f(X)\big) = f(X)g(X)$, where $g \in \mathbb{Z}[X]$ has positive leading coefficient. We substitute again X with $X + f(X)$, and we obtain

$$f\left(X + f(X) + f\big(X + f(X)\big)\right) = f(X)g(X)g\big(X + f(X)\big).$$

We iterate this process, and in general, if we denote $h(X) = X + f(X)$ and $h^{[p]}(X) = h(\cdots(h(X))\cdots)$ (p times), we get by induction

$$f\big(h^{[p]}(X)\big) = f(X)g(X)g\big(h(X)\big)\cdots g\big(h^{[p-1]}(X)\big)$$

for any integer $p \geq 1$. If s is the degree of f (which is also the degree of h), the degree of $h^{[p]}$ is s^p, and the degrees of the polynomials in the right side of the equality are s, $s^2 - s, \ldots, s^p - s^{p-1}$, respectively $s^{p+1} - s^p$.

For $s \geq 2$ we have $s^2 - s < s^3 - s^2 < \cdots < s^p - s^{p-1} < s^p$, so that for m large enough we get

$$0 < g(m) < g\big(h(m)\big) < \cdots < g\big(h^{[p-2]}(m)\big) < h^{[p]}(m).$$

Thus it is sufficient to choose $p = k + 1$ and $n = h^{[k+1]}(m)$ for m large enough such that the above inequalities hold, to have that f can be written in the stated form (with $d_1 = g(m), \ldots, d_k = g\big(h^{[k-1]}(m)\big)$ and $d_{k+1} = f(m)g\big(h^{[k]}(m)\big)$.

If $s = 1$ and $f = aX + b$ we choose pairwise coprime integers $d_1, \ldots, d_k$ which are coprime with a. By Chinese Remainder Theorem, there exists a positive integer m such that $am + 1 \equiv 0 \pmod{d_i}$, $1 \leq i \leq k$. For $n = mb$ we have $f(n) = an + b = (am + 1)b$, and it is readily verified that n chosen as above satisfies the requirements of the problem. This ends the proof. □

319. Let μ be the Möbius function defined by $\mu(1) = 1$, $\mu(p_1 p_2 \dots p_k) = (-1)^k$ for all distinct primes $p_1, p_2, \dots, p_k$, and $\mu(n) = 0$ for any other positive integer n. For integers $n \geq 2$, $q \geq 1$ and $j \geq 1$ define

$$N_j = \frac{1}{j} \sum_{d/j} \mu\left(\frac{n}{d}\right) q^d.$$

Show that

$$\sum_{\substack{x_1+2x_2+\cdots+nx_n=n \\ x_i \geq 0}} \binom{N_1}{x_1} \binom{N_2}{x_2} \cdots \binom{N_n}{x_n} = q^n - q^{n-1}.$$

Proposed by Gabriel Dospinescu, École Polytechnique, Paris, France, and Marian Tetiva, Gheorghe Roşca Codreanu National College, Bârlad, Romania.

Solution by the authors. In the following, all the polynomials will be taken as monic.

Firstly, let us consider the case when q is a power of a prime number. Then it is known that N_j is the number of monic irreducible polynomials of degree j over $\mathbb{F}_q$. This is true since $X^{q^n} - X \in \mathbb{F}_q[X]$ is the product of all monic irreducible polynomials from $\mathbb{F}_q[X]$ of degree dividing n, thus the sum of the degrees of these polynomials is q^n (in other words

$$\sum_{d|n} dN_d = q^n$$

for any $n \geq 1$), hence the above formula for N_j follows from applying the *Möbius* inversion formula.

We claim that the expresion

$$\sum_{\substack{x_1+2x_2+\ldots+nx_n=n \\ x_i \geq 0}} \binom{N_1}{x_1} \binom{N_2}{x_2} \cdots \binom{N_n}{x_n}$$

counts the number of square-free polynomials (polynomials which decompose in a product of distinct irreducible polynomials) of degree n over $\mathbb{F}_q$. Indeed, any such polynomial can be uniquely written as a product of x_1 distinct irreducible polynomials of degree 1 (which can be chosen in $\binom{N_1}{x_1}$ ways), x_2 distinct irreducible polynomials of degree 2 (which can be chosen in $\binom{N_2}{x_2}$ ways), and so on, up to x_n distinct irreducible polynomials of degree n (which can be chosen in $\binom{N_n}{x_n}$ ways). Since we have also the equality of degrees, it follows that these numbers must also satisfy $x_1 + 2x_2 + \cdots + nx_n = n$. The above construction gives a bijection, so indeed the formula gives the number of square-free polynomials of degree n over $\mathbb{F}_q$.

It is sufficient to prove that the number M_n of monic square-free polynomials of degree n over $\mathbb{F}_q$ is $q^n - q^{n-1}$ (for $n \geq 2$; if $n = 1$, obviously $N_1 = M_1 = q$), and we obtain that the statement of the problem is true for q power of a prime number. Since the formula is an equality of polynomials and holds for infinitely many q, it follows that it is true for any positive integer q.

Let us finish the proof. So we can assume q is a power of a prime number. Let

$$f(x) = \frac{1}{1 - qx} = \sum_{n \geq 0} q^n x^n$$

be the generating function of the numbers q^n, which give the number of all monic polynomials of degree n over the field with q elements $\mathbb{F}_q$, and let

$$g(x) = \sum_{n \geq 0} M_n x^n$$

be the generating function of the numbers M_n (where $M_0 = 1$). The equality

$$f(x) = g(x) f(x^2)$$

is true since any polynomial can be written uniquely as a product of a square-free polynomial and the square of an arbitrary polynomial. Identifying the coefficients in the two sides of the equality $g(x) = \dfrac{f(x)}{f(x^2)} = f(x)(1 - qx^2)$, one gets $M_1 = q$ and $M_n = q^n - q^{n-1}$ for $n \geq 2$. □

320. For $n > 1$, does there exist a quadratic polynomial $f \in \mathbb{Q}[X]$ such that $f^{2^n} + 1$ is reducible over $\mathbb{Q}$?

Proposed by Gabriel Dospinescu, École Polytechnique, Paris, France, and Marian Tetiva, Gheorghe Roşca Codreanu National College, Bârlad, Romania.

Solution by the authors. There is no such polynomial! Assume that $f = aX^2 + bX + c$ has the property asked in problem and let $\Delta = b^2 - 4ac$. Let $g = X^{2^n} + 1$ and let z be a root of g. Finally, let α be a complex number such that $f(\alpha) = z$. Then α is a root of $f^{2^n} + 1$. We clearly have $z \in \mathbb{Q}[\alpha]$ and so $\mathbb{Q}[z] \subset \mathbb{Q}[\alpha]$. Moreover, since g is irreducible over $\mathbb{Q}$ (an easy consequence of *Eisenstein*'s criterion applied to the polynomial $g(X + 1)$), we have $[\mathbb{Q}[z] : \mathbb{Q}] = 2^n$. Since $f^{2^n} + 1$ is reducible of degree 2^{n+1}, the degree of the minimal polynomial of α is at most 2^n, and since

$$[\mathbb{Q}[\alpha] : \mathbb{Q}] = [\mathbb{Q}[\alpha] : \mathbb{Q}[z]] \cdot 2^n,$$

we deduce $\mathbb{Q}[\alpha] = \mathbb{Q}[z]$. This means that there exists $h \in \mathbb{Q}[X]$ such that $\alpha = h(z)$. Now, since $f(\alpha) = z$, we have

$$z + \frac{\Delta}{4a} = a \left(h(z) + \frac{b}{2a} \right)^2.$$

The irreducibility of g over $\mathbb{Q}$ implies that the previous relation holds not only for the root z of g, but for any of its roots $z_1, \ldots, z_{2^n}$. Taking the product of these relations and using the fact that $\prod_{i=1}^{2^n} \left(h(z_i) + \frac{b}{2a} \right)$ is a rational number (this is immediate using *Galois* theory or, more elementarily, from the fundamental theorem of symmetric polynomials), we deduce that $\left(\frac{\Delta}{4a} \right)^{2^n} + 1$ is the square of a rational number. But a classical result of *Fermat* ensures that the equation $a^4 + b^4 = c^2$ does not have nontrivial integer solutions, thus we must have $\Delta = 0$.

By performing a translation of the variable X, we may thus assume that $f = a^{-1}X^2$ for some nonzero rational number a. So, it remains to prove that for any such a, the polynomial $X^{2^{n+1}} + a^{2^n}$ is irreducible over $\mathbb{Q}$. By a standard theorem of *Capelli*, it is enough to check that a^{2^n} is not of the form $4x^4$ for some rational number x. Since this is trivial (just consider the exponent of 2 in the prime factorizations of both sides), the problem is solved. □

321. Find the probability that, by choosing a positive integer n, the numbers $n\sqrt{2}$ and $n\sqrt{3}$ have even integral parts both.

Proposed by Radu Gologan, Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania.

Solution by the author. The sequence defined by $a_n = \left(n\frac{\sqrt{2}}{2}, n\frac{\sqrt{3}}{2} \right)$ is uniformly distributed in $[0,1] \times [0,1]$ (mod 1) (due, by example, to the uniform ergodicity of the transformation $T : [0,1] \times [0,1] \to [0,1] \times [0,1]$, $T(x,y) = \left(x + \frac{\sqrt{2}}{2}, y + \frac{\sqrt{2}}{2} \right)$). As the problem asks for inequalities of the type $2k \leq n\sqrt{2} < 2k+1, 2r \leq \sqrt{3} < 2r+1$ with $k, r, n \in \mathbb{N}$. The answer is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$. □

322. Let K be an algebraically closed field and let $P \in K[X_1, \ldots, X_n]$, $P = aX_1^{i_1} \cdots X_n^{i_n} + bX_1^{j_1} \cdots X_n^{j_n} + cX_1^{k_1} \cdots X_n^{k_n}$, where $abc \neq 0$. Assume that $X_t \nmid P$ for all t and the points of coordinates $(i_1, \ldots, i_n)$, $(j_1, \ldots, j_n)$ and $(k_1, \ldots, k_n)$ are non-collinear (in $\mathbb{R}^n$). Prove that P is reducible if and only if $\operatorname{char} K = p$ and $p \mid \gcd(i_t, j_t, k_t)$ for all t for some prime p.

Proposed by Constantin-Nicolae Beli, Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania.

Solution by the author. Before we start our proof we first introduce some definitions and results regarding *Newton* polytopes and *Minkowski* sums of convex polytopes.

If $I \subseteq \mathbb{R}^n$ then we denote by conv I its convex hull, the smallest convex set containing I. If I is a finite set then $C = \text{conv } I$ is a bounded set and therefore a convex polytope. Convex polytopes are analogues of 0-dimensional points, 1-dimensional segments, 2-dimensional convex polygons or 3-dimensional convex polyhedra.

For any polytope C we denote by $\mathcal{V}(C)$ the set of all its vertices. Then $\mathcal{V}(C)$ is the minimal subset of $\mathbb{R}^n$ that has C as its convex hull. Hence if $C = \text{conv } I$, then $\mathcal{V}(C) \subseteq I$.

If $A, B \subseteq \mathbb{R}^n$ then $A + B := \{a + b \ : \ a \in A, b \in B\}$ is called their *Minkowski* sum. In particular, if $b \in \mathbb{R}^n$ then $A+b := A+\{b\} = \{a+b \mid a \in A\}$. If $A \subseteq \mathbb{R}^n$ and $\lambda \in \mathbb{R}$ we denote $\lambda A := \{\lambda a \ : \ a \in A\}$.

If C', C'' are polytopes their Minkowski sum $C = C' + C''$ is also a polytope. Indeed, one can write $C' = \text{conv } I'$ and $C'' = \text{conv } I''$, where $I', I'' \subset \mathbb{R}^n$ are finite, and we have $C = \text{conv } I$, where $I = I' + I''$, which is also finite.

Given a polytope C we are interested in its Minkowski decompositions $C = C' + C''$, where C', C'' are polytopes. From the definition of a convex set one easily sees that $C = \lambda C + (1-\lambda)C$ for any $\lambda \in [0,1]$. More generally, if $\alpha \in \mathbb{R}^n$ then $C = (\lambda C + \alpha) + ((1-\lambda)C - \alpha)$. Such decompositions are called homothetic as $\lambda C + \alpha$ and $(1-\lambda)C - \alpha$ are homothetic images of C. Polytopes for which there are no Minkowski decompositions other than those of this type are called homothetically indecomposable.

Lemma 7. *All triangles are homothetically indecomposable.*

Let K be a field and let $X = (X_1, \ldots, X_n)$ be a multi-variable.

Let $K[X] = K[X_1, \ldots, X_n]$. For any $i = (i_1, \ldots, i_n) \in \mathbb{N}^n$ we denote $X^i := X_1^{i_1} \cdots X_n^{i_n}$. For $P \in K[X]$ we define the suport of P as the set $I(P) \subset \mathbb{N}^n$ such that P writes as $P = \sum i \in I(P) a_i X^i$ with $a_i \in K^*$. The Newton polytope $C(P) \subseteq \mathbb{R}^n$ of P is defined by $C(P) = \text{conv } I(P)$.

Lemma 8. *(Ostrowski,* 1975*) If $P, Q \in K[X] \setminus \{0\}$ then*

$$C(P) + C(Q) = C(PQ).$$

Note that $C(P) = \{0\}$ iff $I(P) = \{0\}$, i.e., iff P is a non-zero constant polynomial.

Note that for any polynomial $P \in K[X] \setminus \{0\}$ we have $C(P) = \text{conv } I(P)$, so $\mathcal{V}(C(P)) \subseteq I(P)$. In particular, all the vertices of $C(P)$ belong to $\mathbb{N}^n$.

We denote by $(\cdot, \cdot) : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ the usual inner product, $(a, b) = a_1 b_1 + \ldots + a_n b_n$. If $S \subseteq \mathbb{R}^n$, $a \in \mathbb{R}^n$ we denote $(S, a) := \{(x, a) : x \in S\}$.

Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{R}^n$, $e_t = (0, \ldots, 1, \ldots, 0)$.

Lemma 9. *Let $P \in K[X] \setminus \{0\}$.*

(i) *We have* $\deg P = \max\left(I(P), \sum_{t=1}^{n} e_t\right) = \max\left(C(P), \sum_{t=1}^{n} e_t\right)$.

(ii) *For any t the highest power of X_t dividing P is* $\min(I(P), e_t) = \min(C(P), e_t)$. *In particular, $X_t \nmid P$ iff* $\min(C(P), e_t) = 0$.

Proof. For any $i = (i_1, \dots, i_n) \in \mathbb{N}^n$ we have

$$\deg X^i = i_1 + \cdots + i_n = \left(i, \sum_{t=1}^{n} e_t\right)$$

and the highest power of X_t dividing X^i is $i_t = (i, e_t)$.

It follows that $\deg P = \max\left(I(P), \sum_{t=1}^{n} e_t\right)$ and the highest power of X_t dividing P is $\min(I(P), e_t)$. We still have to prove that

$$\max\left(I(P), \sum_{t=1}^{n} e_t\right) = \max\left(C(P), \sum_{t=1}^{n} e_t\right)$$

and

$$\min(I(P), e_t) = \min(C(P), e_t).$$

We prove more generally that if $C = \operatorname{conv} I$ and $a \in \mathbb{R}^n$ then $\max(I, a) = \max(C, a)$ and $\min(I, a) = \min(C, a)$. We have $I \subseteq C$ so $\max(I, a) \leq \max(C, a)$. For the reverse inequality let $M = \max(I, a)$. Then $I \subseteq H^- := \{x \in \mathbb{R}^n : (x, a) \leq M\}$, one of the two halfspaces bounded by the hyperplane $H = \{x \in \mathbb{R}^n : (x, a) = M\}$. But $I \subseteq H^-$ and H^- is convex so $C = \operatorname{conv} I \subseteq H^-$. It follows that $\max(C, a) \leq M$. Similarly for $\min(I, a) = \min(C, a)$. □

Before starting our proof we need one more result.

Lemma 10. *If K is algebraically closed, i, $j \in \mathbb{Z}^n$ are linearly independent and $\varepsilon, \eta \in K^*$ then there is $x \in (K^*)^n$ with $x^i = \varepsilon$, $x^i = \eta$.*

Proof. First we show that if s_1, t_1, s_2, $t_2 \in \mathbb{Z}$ with $s_1 t_2 - s_2 t_1 \neq 0$ and ε_1, $\varepsilon_2 \in K^*$ then the system $x^{s_1} y^{t_1} = \varepsilon_1$, $x^{s_2} y^{t_2} = \varepsilon_2$ has a solution with x, $y \in K^*$. If $t_2 \neq 0$ we note that for any $q \in \mathbb{Z}$ our system is equivalent to the system $x^{s_2} y^{t_2} = \varepsilon_2$, $x^{s_1} y^{t_1} (x^{s_2} y^{t_2})^{-q} = \varepsilon_1 \varepsilon_2^{-q}$. The second equation may be written as $x^{s_3} y^{t_3} = \varepsilon_3$, where $\varepsilon_3 = \mathrm{e}_1 \varepsilon_2^{-q}$, $s_3 = s_1 - q s_2$ and $t_3 = t_1 - q t_2$. We choose q such that $|t_3| < |t_2|$. Note that $s_2 t_3 - s_3 t_2 = -(s_1 t_2 - s_2 t_1) \neq 0$. We repeat the procedure and obtain new equivalent systems $x^{s_l} y^{t_l} = \mathrm{e}_l$, $x^{s_{l+1}} y^{t_{l+1}} = \mathrm{e}_{l+1}$ with $s_l t_{l+1} - s_{l+1} t_l \neq 0$ and $|t_2| > \ldots > |t_{l+1}|$ until we get an index l with $t_{l+1} = 0$. We have $0 \neq s_l t_{l+1} - s_{l+1} t_l = -s_{l+1} t_l$, so $s_{l+1}, t_l \neq 0$ and our system writes as $x^{s_l} y^{t_l} = \varepsilon_l$, $x^{s_{l+1}} = \varepsilon_{l+1}$, which obviously has solutions. (Take x with $x^{s_{l+1}} = \varepsilon_{l+1}$ and then take y with $y^{t_l} = \varepsilon_l x^{-s_l}$.)

Let $i = (i_1, \dots, i_n)$, $j = (j_1, \dots, j_n)$. Since i, j are linearly independent, the $2 \times n$ matrix $\begin{pmatrix} i \\ j \end{pmatrix}$ has rank 2, so there are $1 \leq \alpha < \beta \leq n$ such that $i_\alpha j_\beta - i_\beta j_\alpha \neq 0$. Then as seen above there are y, $z \in K^*$ such that $y^{i_\alpha} z^{i_\beta} = \varepsilon$

and $y^{j_\alpha} z^{j_\beta} = \eta$. Then we simply take $x = (x_1, \dots, x_n)$ with $x_\alpha = y$, $x_\beta = z$, and $x_t = 1$ for $t \neq \alpha, \beta$ and we have $x^i = \varepsilon$, $x^j = \eta$. □

We now start our proof. Note that our statement can be re-written as follows:

If K is algebraically closed, $P \in K[X]$, $I(P) = \{i, j, k\}$, where $i, j, k \in \mathbb{N}^n$ are non-collinear and $X_t \nmid P$ $\forall t$ then P is reducible iff car $K = p$ and i, j, $k \in p\mathbb{N}^n$ for some prime p.

We will write $P = a_i X^i + a_j X^j + a_k X^k$. If car $K = p$ and $i, j, k \in p\mathbb{N}^n$ then $P = \left(a_i^{1/p} X^{i/p} + a_j^{1/p} X^{j/p} + a_i^{1/p} X^{k/p}\right)^p$, so P is reducible.

Conversely, assume that P is reducible but there is no prime p such that car $K = p$ and i, j, $k \in p\mathbb{N}^n$. Then $P = QR$, where Q, $R \in K[X] \setminus K$ and Q is irreducible. Since i, j, k are non-colinear, $C(P) = \operatorname{conv} I(P)$ is the triangle of vertices i, j, k. By Lemma 8, $C(P) = C(Q) + C(R)$. Since $C(P)$ is a triangle, by Lemma 7 we get $C(Q) = lC(P) + \alpha$ and $C(R) = (1 - \lambda)C(P) - \alpha$ for some $\lambda \in [0, 1]$ and $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n$.

For any t we have $X_t \nmid P$, whence $X_t \nmid Q$, and by Lemma 9 (ii) we have $0 = \min(C(P), e_t)$ and

$$0 = \min(C(Q), e_t) = \min(\lambda C(P) + \alpha, e_t) = \lambda \min(C(P), e_t) + (\alpha, e_t) = \alpha_t.$$

So $\alpha = 0$ and therefore $C(Q) = \lambda C(P)$, $C(R) = (1 - \lambda)C(P)$. By Lemma 9 (i) this implies

$$\deg Q = \max\left(C(Q), \sum_{i=1}^n e_t\right) = \lambda \max\left(C(P), \sum_{i=1}^n e_t\right) = \lambda \deg P.$$

Note that we cannot have $\lambda = 0$ or 1 since this would imply either $C(Q) = \{0\}$ or $C(R) = \{0\}$, whence either Q or R is a constant polynomial. Thus $\lambda \in (0, 1)$.

Since $C(P)$ is the triangle of vertices i, j, k, $C(Q)$ is the triangle of vertices λi, λj, λk. So $\{\lambda i, \lambda j, \lambda k\} = \mathcal{V}(C(Q)) \subseteq I(Q) \subset \mathbb{N}^n$. It follows that $\lambda \in \mathbb{Q}$, i.e. $\lambda = \dfrac{\alpha}{d}$, with $\gcd(\alpha, d) = 1$, and $i, j, k \in d\mathbb{N}^n$. Since $0 < \lambda < 1$ we have $0 < \alpha < d$. In particular, $d > 1$.

Since i, j, k are non-colinear, $\dfrac{1}{d}(j - i)$ and $\dfrac{1}{d}(k - i)$ are linearly independent. By Lemma 10, for any ε, $\eta \in \mu_d$ there is

$$\gamma(\varepsilon, \eta) = (\gamma_1(\varepsilon, \eta), \dots, \gamma_n(\varepsilon, \eta)) \in (K^*)^n$$

such that

$$\gamma(\varepsilon, \eta)^{\frac{1}{d}(j-i)} = \varepsilon \text{ and } \gamma(\varepsilon, \eta)^{\frac{1}{d}(k-i)} = \eta.$$

By $\mu_d = \mu_d(K)$ we denote the group of the d-roots of unity in K, i.e., the roots in K of $f(x) = x^d - 1$. Since K is algebraically closed, all d roots of $f(x)$ are in K. Note that they are distinct since

$$\gcd(f(x), f'(x)) = \gcd(x^d - 1, dx^{d-1}) = 1.$$

Here we use the fact that $d \neq 0$ in K. If $d = 0$ in K then char $K = p \mid d$, so i, j, $k \in d\mathbb{N}^n \subseteq p\mathbb{N}^n$ for some prime p, contradicting our hypothesis. So $|\mu_d| = d$.

We denote $\gamma(\varepsilon, \eta)X = (\gamma_1(\varepsilon, \eta)X_1, \ldots, \gamma_n(\varepsilon, \eta)X_n)$.

Thus $(\gamma(\varepsilon, \eta)X)^h = \gamma(\varepsilon, \eta)^h X^h$ for any $h \in \mathbb{Z}^n$.

We define $P_{\varepsilon,\eta}(X) := P(\gamma(\varepsilon, \eta)X)$ and $Q_{\varepsilon,\eta}(X) := Q(\gamma(\varepsilon, \eta)X)$. Since Q divides P, we have $Q_{\varepsilon,\eta} \mid P_{\varepsilon,\eta}$, and since Q is irreducible, so is $Q_{\varepsilon,\eta}$.

We have $P_{\varepsilon,\eta} = a_i\gamma(\varepsilon, \eta)^i X^i + a_j\gamma(\varepsilon, \eta)^j X^j + a_k\gamma(\varepsilon, \eta)^k X^k$ and if $Q = \sum h \in I(Q) b_h X^h$ then $Q_{\varepsilon,\eta} = \sum h \in I(Q) b_h \gamma(\varepsilon, \eta)^h X^h$.

Note that $P_{\varepsilon,\eta} = \gamma(\varepsilon, \eta)^i (a_i X^i + a_j\gamma(\varepsilon, \eta)^{j-i} X^j + a_k\gamma(\varepsilon, \eta)^{k-i} X^k)$. But $\gamma(\varepsilon, \eta)^{j-i} = \mathrm{e}^d = 1$ and $\gamma(\varepsilon, \eta)^{k-i} = \eta^d = 1$, so $P_{\varepsilon,\eta} = \gamma(\varepsilon, \eta)^i P \sim P$. (Here by $\sim$ we mean that the two polynomials are associates in $K[X]$.) Since $Q_{\varepsilon,\eta} \mid P_{\varepsilon,\eta}$ we have $Q_{\varepsilon,\eta} \mid P \ \forall \varepsilon, \eta \in \mu_d$.

Assume now that $Q_{\varepsilon,\eta} \sim Q_{\varepsilon',\eta'}$, that is, $Q_{\varepsilon',\eta'} = tQ_{\varepsilon,\eta}$ for some $t \in K^*$. We have λi, λj, $\lambda k \in I(Q)$, and by considering the coefficients of $X^{\lambda i}$, $X^{\lambda j}$, $X^{\lambda k}$ we get

$$t = \frac{b_i\gamma(\varepsilon', \eta')^{\lambda i}}{b_i\gamma(\varepsilon, \eta)^{\lambda i}} = \frac{b_j\gamma(\varepsilon', \eta')^{\lambda j}}{b_j\gamma(\varepsilon, \eta)^{\lambda j}} = \frac{b_l\gamma(\varepsilon', \eta')^{\lambda k}}{b_l\gamma(\varepsilon, \eta)^{\lambda k}}.$$

It follows that $\gamma(\varepsilon, \eta)^{\lambda(j-i)} = \gamma(\varepsilon', \eta')^{\lambda(j-i)}$ and $\gamma(\varepsilon, \eta)^{\lambda(k-i)} = \gamma(\varepsilon', \eta')^{\lambda(k-i)}$, so $\varepsilon^\alpha = \varepsilon'^\alpha$ and $\eta^\alpha = \eta'^\alpha$. (Recall, $\lambda = \dfrac{\alpha}{d}$.) But ε, ε', η, $\eta' \in \mu_d$ and $\gcd(\alpha, d) = 1$ imply $\varepsilon = \varepsilon'$ and $\eta = \eta'$.

Since $Q_{\varepsilon,\eta} \mid P \ \forall\, \varepsilon, \eta \in \mu_d$ and $Q_{\varepsilon,\eta} \not\sim Q_{\varepsilon',\eta'}$ if $(\varepsilon, \eta) \neq (\varepsilon', \eta')$, we have $\prod_{\varepsilon,\eta\in\mu_d} Q_{\varepsilon,\eta} \mid P$. It follows that $\deg P \geq \deg \prod_{\varepsilon,\eta\in\mu_d} Q_{\varepsilon,\eta} = |\mu_d|^2 \deg Q$. But $\deg Q = l \deg P \geq \dfrac{1}{d} \deg P$ and $|\mu_d| = d$, so $|\mu_d|^2 \deg Q \geq d \deg P > \deg P$, contradiction. Hence P is irreducible. □

SOCIETATEA DE ŞTIINŢE MATEMATICE DIN ROMÂNIA

organizează în a doua jumătate a lunii iulie 2012

ŞCOALA DE VARĂ A S.S.M.R
(Program de formare continuă)

pentru profesorii de matematică şi informatică din învăţământul preuniversitar

Şcoala este acreditată de Ministerul Educaţiei, Cercetării, Tineretului şi Sportului, oferind un număr de 15 credite profesionale transferabile.

Cursurile se vor desfăşura la Buşteni în a doua jumătate a lunii iulie 2012. Data exactă va fi comunicată pe pagina de web a S.S.M.R.: www/ssmr.ro

Pot participa la cursuri profesorii din România şi Republica Moldova, membri sau nemembri ai S.S.M.R.

Înscrierile la cursuri se pot face începând cu data de 01 noiembrie 2011 la sediul S.S.M.R. din Bucureşti sau prin e-mail la adresa office@rms.unibuc.ro.

Candidaţii vor fi admişi în funcţie de data depunerii banilor şi în limita locurilor disponibile.

În limita locurilor disponibile, participanţii la cursuri pot fi însoţiţi de membri ai familiei.

Pentru informaţii suplimentare, vă rugăm să vă adresaţi la sediul centralal S.S.M.R.

Directorul cursurilor
Dan Radu