Algebra and Discrete Mathematics
Volume 15 **(2013)**. Number 2. pp. 174 – 178

RESEARCH ARTICLE

On maximal and minimal linear matching property

M. Aliabadi, M. R. Darafsheh

Communicated by V. Dlab

Abstract. The matching basis in field extentions is introduced by S. Eliahou and C. Lecouvey in [2]. In this paper we define the minimal and maximal linear matching property for field extensions and prove that if K is not algebraically closed, then K has minimal linear matching property. In this paper we will prove that algebraic number fields have maximal linear matching property. We also give a shorter proof of a result established in [6] on the fundamental theorem of algebra.

1. Introduction

Throughout this paper we will consider a field extension $K \subset L$ where K is commutative and central in L. Let G be an additive group and $A, B \subset G$ be nonempty finite subsets of G. A *matching* from A to B is a map $\phi : A \to B$ which is bijective and satisfies the condition

$$a + \phi(a) \notin A$$

for all $a \in A$. This notion was introduced in [3] by Fan and Losonczy, who used matchings in $\mathbb{Z}^n$ as a tool for studying an old problem of Wakeford concerning canonical forms for symmetric tensors [7]. Eliahou

2010 MSC: 12F05.
Key words and phrases: Linear matching property, Algebraic number field, Field extension, Maximal linear matching property, Minimal linear matching property.

and Lecouvey extended this notion to subspaces in a field extension, here we will introduce a notion from [2].

Let $K \subset L$ be a field extension and A, B be n-dimensional K-subspaces of L. Let $\mathcal{A} = \{a_1, \ldots, a_n\}$, $\mathcal{B} = \{b_1, \ldots, b_n\}$ be basis of A and B respectively. It is said that $\mathcal{A}$ is *matched* to $\mathcal{B}$ if

$$a_i b \in A \quad \Rightarrow \quad b \in \langle b_1, \ldots, \hat{b_i}, \ldots, b_n \rangle$$

for all $b \in B$ and $i = 1, \ldots, n$, where $\langle b_1, \ldots, \hat{b_i}, \ldots, b_n \rangle$ is the hyperplane of B spanned by the set $\mathcal{B} \setminus \{b_i\}$. Also it is said that A is *matched* to B if every basis of A can be matched to a basis of B.

It is said that L has the *linear matching property* from K if, for every $n \geq 1$ and every n-dimensional K-subspaces A and B of L with $1 \notin B$, the subspace A is matched to B. By this we mean linear matching property for K-subspaces.

As we mentioned, the above notion was introduce by Eliahou and Lecouvey in [2], where they proved that if $K \subset L$ is a field extension and $[L : K]$ is prime, then L has linear matching property (see Theorem 5.3 in [2]). We extend this property to the family of field extensions and introduce the notions of minimal and maximal linear matching properties.

2. Definitions and the main results

Definition 2.1. Let K be a field. We say K has *minimal linear matching property* if there exists a finite field extension L of K, such that L has linear matching property from K.

Definition 2.2. Let K be a field. We say K has *maximal linear matching property* if for any positive integer n, there exists a field extension L_n of K, such that $[L_n : K]= n$ and L_n has linear matching property from K.

We shall prove the following results in section 5.

Theorem 2.3. *Let K be a field which is not algebraically closed, then K has the minimal linear matching property.*

Theorem 2.4. *Algebraic number fields have the maximal linear matching property.*

Theorem 2.5. *Suppose that K is a field and has the maximal linear matching property, then K is infinite.*

To prove our main results, we will use Theorem 3.1 which can be regarded as an improvement of the foundamental theorem of algebra.

In [6], Shipman gives an algebraic proof of the foundamental theorem of algebra in special cases, but here we present a different proof which is independent Shipman's proof.

3. An improvment of the fundamental theorem of algebra

Theorem 3.1. *Let K be a field such that every polynomial of prime degree in $K[x]$ has a root in K, then K is algebraically closed.*

Proof. First, we claim there exists a prime p such that for any non-linear irreducible polynomial $f(x) \in K[x]$, p divides the degree of $f(x)$. Suppose that this claim is false, and $p_1, \dots, p_n$ are prime divisors of the degree of $f(x)$, then there exists $g_i \in K[x]$ such that $p_i \not| \deg g_i(x)$ and $g_i(x)$ is an irreducible polynomials in $K[x]$, where $1 \leq i \leq n$.

Now set $F(x) := f^{k_0}(x) g_1^{k_1}(x) \cdots g_n^{k_n}(x)$ where $k_0, k_1, \dots, k_n$ are non-negative integers. It is clear that $\gcd(\deg f(x), \deg g_1(x), \dots, \deg g_n(x)) = 1$ and $\deg F = k_0 \deg f + k_1 \deg g_1 + \cdots + k_n \deg g_n$. By Dirichlet's Theorem on primes, since the k_i's are non-negative integers, we can choose $k_0, \dots, k_n$ such that $\deg F$ becomes a prime number. So $F(x)$ has a root in K and this is a contradiction. Therefore there exists a prime p such that p divide the degree of every irreducible polynomials in $K[x]$. Now if L is a field extension of K of degree p and $\alpha \in L \setminus K$, then $L = K(\alpha)$ and if $f(x) \in K[x]$ is the minimal polynomial of α, then $\deg f(x) = p$ and $f(x)$ has a root in K and this is a contradiction, hence K has no field extension of degree p. Let L be a Galois extension of K with $[L : K] = p^r \cdot m$ where $r, m \in \mathbb{N}$, $(m, p) = 1$. By Galois fundamental theorem and Cauchy theorem, there is an intermediate field L', $K \subset L' \subset L$ such that $[L : L'] = p^r$, then $[L' : K] = m$. If $m > 1$ we can choose $\alpha \in L' \setminus K$, and assume $f(x)$ is the minimal polynomial of α over K, then $\deg f(x) | m$, also $f(x)$ is irreducible, then $p | \deg f(x)$, so $p | m$, a contradiction. Hence $m = 1$ and $[L : K] = p^r$, again by using Galois fundamental theorem and Cauchy theorem there exists an intermediate field L', $K \subseteq L' \subset L$ such that $[L : L'] = p^{r-1}$, then $[L' : K] = p$, but since we proved that K has no field extension of degree p, this is a contradiction. Thus K has no Galois extension and it is algebraically closed. □

Corollary 3.2 *Let K be a field such that every polynomial of prime degree in $K[x]$ is reducible on K. Then K is algebraically closed.*

4. Preliminary results about field extensions and linear matching property

We use the following result from [4].

Theorem 4.1. *Let L be a finite field of characteristic $p > 0$ where $\mathbb{Z}_p$ is embedded in L and $[L : \mathbb{Z}_p] = n$. Then for any divisor m of n, L has a subfield with p^m elements.*

We also use the following result from [5] which is about field extensions with no proper intermediate subfield.

Theorem 4.2. *If K is an algebraic number field, then for every positive integer n there exist infinitely many field extensions of K with degree n having no proper subfields over K.*

The following theorem was proved in [2], see also [1].

Theorem 4.3. *Let $K \subset L$ be a field extension. Then L has linear matching property if and only if $K \subset L$ has no proper intermediate subfield with finite degree over K.*

Now we are ready to prove the main results.

5. Proof of main results

Proof of Theorem 2.3

Proof. By Corollary 3.2 there exists an irreducible polynomial $f(x)$ of prime degree in $K[x]$. Now if L is the splitting field of $f(x)$ over K, then $[L : K]$ is prime and by Theorem 4.3 L has the linear matching property from K, so K has the minimal linear matching property. □

Proof of Theorem 2.4

Proof. Let K be an algebraic number field. Then by theorem 4.2 for any positive integer n, there exists an extension L_n of K with $[L_n : K] = n$ and this field extension has no proper intermediate subfield, then by Theorem 4.3, L_n has the linear matching property from K, so K has the maximal linear matching property. □

Proof of Theorem 2.5

Proof. Let K be a finite field with $|K| = p^n$ and p a prime and n a positive integer. Now let q and m be positive integers with $n < q < m$

and $q|m$. If L is an extension of K of degree m, then $[L : \mathbb{Z}_p] = mn$ and by Theorem 4.1, $\mathbb{Z}_p \subseteq L$ has an intermediate subfield K' of degree p^q. Now since finite fields with the same cardinality are isomorphic, K' is a finite proper intermediate subfield in the extension $K \subset L$ with finite degree over K, then by Theorem 4.3, L does not have linear matching property from K, hence K does not have maximal linear matching property. □

References

[1] S. Akbari, M. Aliabadi, Erratum to: Matching Subspaces in a field extension, submitted.

[2] S. Eliahou, C. Lecouvey, Mathching subspaces in a field extension, J. Algebra. 324 (2010), 3420-3430.

[3] C.K. Fan, J. Losonczy, Matchings and canonical forms in symmetric tensors, Adv. Math. 117 (1996), 228-238.

[4] D. S. Malik, Jhon N. Mordeson, M. K. Sen, Fundamentals of Abstract Algebra, Mc GrawHill (1999).

[5] H. Marksaitis, Some remarks on subfields of algebraic number fields, Lithuanian Mathematical Journal, Vol. 35. No. 2. (1995).

[6] J. Shipman, Improving of fundamental theorem of algebra, Math. Intelligencer 29 (2007), no.4, 9-14. 00-01 (12D05)

[7] E.K. Wakeford, On canonical forms, Proc. London Math. Soc. 18 (1918-1919), 403-410.

Contact information

M. Aliabadi Department of Mathematical Sciences, Sharif University of Technology, Tehran, Iran
E-Mail: mohsenmath88@gmail.com

M. R. Darafsheh School of Mathematics, Statistics and Computer Science, Colledge of Science, University of Tehran, Tehran, Iran
E-Mail: darafsheh@ut.ac.ir

Received by the editors: 03.05.2012
and in final form 15.09.2012.