ISSN 2075-9827 **e-ISSN 2313-0210**
Carpathian Math. Publ. 2023, **15** (1), 150–157
doi:10.15330/cmp.15.1.150-157

https://journals.pnu.edu.ua/index.php/cmp
Карпатські матем. публ. 2023, Т.15, №1, С.150–157

Polynomial composites and certain types of fields extensions

Matysiak Ł.

In this paper, we consider polynomial composites with the coefficients from $K \subset L$. We already know many properties, but we do not know the answer to the question of whether there is a relationship between composites and field extensions. We present the characterization of some known field extensions in terms of polynomial composites. This paper contains the open problem of characterization of ideals in polynomial composites with respect to various field extensions. We also present the full possible characterization of certain field extensions. Moreover, in this paper we show that any finite group is a Galois group of some field extensions and present the inverse Galois problem solved.

Key words and phrases: field extension, polynomial, finite field extension, Noetherian ring, Galois group.

Kazimierz Wielki University, 2 Powstancow Wielkopolskich ave., Bydgoszcz, Poland
E-mail: `lukmat@ukw.edu.pl`

Introduction

By a ring R we mean a commutative ring with unity. Denote by R^* the group of all invertible elements of R. By $\operatorname{Irr} R$ we denote the set of all irreducible elements of R. A Noetherian ring is a ring that satisfies the ascending chain condition on ideals, that is, given any increasing sequence of ideals $I_1 \subset I_2 \subset \dots$, there exists a natural number (positive integer) n such that $I_n = I_{n+1} = \dots$. There are other, equivalent, definitions: every ideal $I \subset R$ is finitely generated, every non-empty set of ideals of R has a maximal element.

Let $K \subset L$ be a field extension. Let us denote by $[L\colon K]$ the degree of field extension $K \subset L$. In this paper, we will use the following extensions and let us recall their definitions:

(a) a finite extension – the extension that has a finite degree;

(b) an algebraic extension – the extension such that every element of L is algebraic over K, i.e. every element of L is a root of some non-zero polynomial with coefficients in K;

(c) a separable extension – the algebraic extension such that the minimal polynomial of every element of L over K is separable, i.e. has no repeated roots in an algebraic closure over K;

(d) a normal extension – the algebraic extension such that every irreducible polynomial in $K[X]$ that has a root in L completely factors into linear factors over L;

(e) a Galois extension – the algebraic extension such that is both separable and normal.

УДК 512.623.2
2020 *Mathematics Subject Classification:* 12F99, 12F12, 12F10.

If $K \subset L$ is a Galois extension, then $Aut_K L$ is called the Galois group of $K \subset L$ and denoted by $G(L \mid K)$. For any subgroup H of $G(L \mid K)$ by L^H we denote the corresponding fixed field, i.e. the set of those elements of L which are fixed by every automorphism in H. The algebraic closure of field K is denoted by $a(K)$.

A field K is called perfect if every finite extension of K is separable. For example, $\mathbb{Q}$ and $\mathbb{C}$ are algebraically closed fields.

D.D. Anderson, D.F. Anderson and M. Zafrullah in [1] called object $A + XB[X]$ as a composite for $A \subset B$ fields. There are a lot of manuscripts where composites are used as examples to show some properties. But the most important are presented below.

In [2], authors considered the structures in the form $D + M$, where D is a domain and M is a maximal ideal of ring R, where $D \subset R$. Later (in [7]), it was proved that in composite of the form $D + XK[X]$, where D is a domain, K is a field with $D \subset K$, such that $XK[X]$ is a maximal ideal of $K[X]$. Next, D. Costa, J.L. Mott and M. Zafrullah [4] considered composites of the form $D + XD_S[X]$, where D is a domain and D_S is a localization of D relative to the multiplicative subset S. In [8], M. Zafrullah continued research on structure $D + XD_S[X]$ but he showed that if D is a GCD-domain, then the behaviour of

$$D^{(S)} = \left\{ a_0 + \sum a_i X^i \mid a_0 \in D, a_i \in D_S \right\} = D + XD_S[X]$$

depends upon the relationship between S and the prime ideals P of D such that D_P is a valuation domain (see [8, Theorem 1]). In 1991, there was the article [1], that collected all previous composites and the authors began to create a theory about composites creating results. In that paper, the structures under consideration were officially called as composites. After this article, various minor results appeared. But the most important thing is that composites have been used in many theories as examples. We have researched many properties of composites in [7].

The main motivation of this paper is to answer the following question.

Question 1. *Is there a relationship between certain field extensions $K \subset L$ and polynomial composites $K + XL[X]$?*

In the third chapter, we present a full possible characterization of polynomial composites of the form $K + XL[X]$, where K, L are fields, with respect to a given extension with appropriate additional assumptions. We also present a full possible characterization of some extensions of fields $K \subset L$ expressed in terms of polynomial composites $K + XL[X]$ as Noetherian rings with appropriate assumptions.

In the fourth chapter, we present the consideration of ideals in polynomial composites $K + XL[X]$ assuming that $K \subset L$ is a certain field extension.

In the fifth chapter, we can found a full posible characterization of considered extensions (see Theorems 4, 5).

In Galois theory, the inverse Galois problem concerns whether or not every finite group appears as the Galois group of some Galois extension of the rational numbers $\mathbb{Q}$. This problem, first posed in the early 19th century, is unsolved. The presented results can be used as mathematical tools. All the propositions contained in this paper hold for a field of any characteristic, and therefore also for finite fields. We also have a characterization of the Galois extensions (Theorem 4, 5). The inverse Galois problem can be solved by switching to polynomial composites or to nilpotent elements.

1 Auxiliary Lemmas

Lemma 1. *Let $\varphi\colon K_1 \to K_2$ be an isomorphism of fields and $\Psi\colon K_1[X] \to K_2[X]$ be an isomorphism of polynomial rings. If polynomial $f_1 \in \operatorname{Irr} K_1[X]$, f_1 has a root a_1 in an extended L_1 of K_1 and polynomial $f_2 = \Psi(f_1)$ has a root a_2 in an extended L_2 of K_2, then there exists $\Psi'\colon K_1(a_1) \to K_2(a_2)$, which is an extension of φ and $\Psi'(a_1) = a_2$ holds.*

Proof. See [3, Lemma 2, p. 105]. □

Lemma 2. *If $\varphi\colon K \to L$ is an embedding field K to an algebraically closed field L, and K' is an algebraic extension of K, then there exists an embedding $\Psi\colon K' \to L$ which is an extension of φ.*

Proof. See [3, Lemma 4, p. 109]. □

Lemma 3. *If L is a finite field extension of K, then L is a Galois extension of K if and only if $\big|G(L|K)\big| = [L\colon K]$.*

Proof. See [3, Corollary 1, p. 126]. □

2 Characterization of field extensions in terms of polynomial composites

Let us start with an auxiliary lemma that will help us to prove the Theorem 1.

Lemma 4. *If there exists a nonzero ideal I of $L[X]$, where L is a field, that is finitely generated as a $K + XL[X]$-module, then K is a field and $[L\colon K] < \infty$.*

Proof. Clearly, I is finitely generated over $L[X]$, and hence $XL[X]I \neq I$. For otherwise,

$$XL[X]L[X]_{XL[X]} \cdot IL[X]_{XL[X]} = IL[X]_{XL[X]}$$

therefore $IL[X]_{XL[X]} = 0$, by Nakayama's lemma. This is impossible, since $0 \neq I \subseteq IL[X]_{XL[X]}$. It follows that $I/XL[X]I$ is a nonzero $\big(L[X]/XL[X] = L\big)$-module that is finitely generated as a $\big(K + XL[X]/XL[X] = K\big)$-module. Since L is a field, $I/XL[X]I$ can be written as a direct sum of copies of L. Thus, L is a finitely generated K-module. But then K is a field, since the field L is integral over K and obviously $[L\colon K] < \infty$. □

Theorem 1. *Let $K \subset L$ be a field extension. Put $T = K + XL[X]$. Then the following conditions are equivalent:*

(1) T is Noetherian;

(2) $[L\colon K] < \infty$.

Proof. *(1) ⇒ (2)* Since $XL[X]$ is a finitely generated ideal of $K + XL[X]$, it follows from Lemma 4 that $[L\colon K] < \infty$. Thus, $L[X]$ is module-finite over the Noetherian ring $K + XL[X]$.

(2) ⇒ (1) $L[X]$ is Noetherian ring and module-finite over the subring $K + XL[X]$. This is the situation covered by P.M. Eakin's theorem [5]. □

All our considerations began with the Theorem 1. This Theorem motivated us to further consider polynomial composites $K + XL[X]$ in a situation where the extension of fields $K \subset L$ is algebraic, separable, normal and Galois, respectively.

Proposition 1. *Let $K \subset L$ be a field extension such that $L^{G(L|K)} = K$. Put $T = K + XL[X]$. Then the following conditions are equivalent:*

(1) T is Noetherian;

(2) $K \subset L$ is an algebraic extension.

Proof. *(1) ⇒ (2)* Since $T = K + XL[X]$ is Noetherian, where $K \subset L$ is a field extension, then by Theorem 1 we get that $K \subset L$ is a finite extension. And every finite extension is algebraic.

(2) ⇒ (1) Assume that $K \subset L$ is an algebraic extension. Assuming $L^{G(L|K)} = K$, we get directly from the definition of the Galois extension. Since $K \subset L$ is the Galois extension, then $K \subset L$ is a normal extension. Every normal extension is finite, then by Theorem 1 we get that $K + XL[X]$ is a Noetherian. □

Proposition 2. *Let $K \subset L$ is a field extension such that K is a perfect field. Assume that any K-isomorphism $\varphi\colon M \to M$, where $\varphi(L) = L$, holds for every field M such that $L \subset M$. Put $T = K + XL[X]$. Then the following conditions are equivalent:*

(1) T is Noetherian;

(2) $K \subset L$ is a separable extension.

Proof. *(1) ⇒ (2)* By Theorem 1, $K \subset L$ is a finite extension. Every finite extension is an algebraic extension. Since K is the perfect field, then $K \subset L$ is a separable extension.

(2) ⇒ (1) First we show that if L is a separable extension of the field K, then the smallest normal extension M of the field K containing L is the Galois extension of the field K.

If L is a separable extension of the field K, and N is a normal extension of the field K containing L, then let M is the largest separable extension of K contained in N. So we have $L \subset M$ and therefore it suffices to prove that M is the normal extension of K.

Let $g \in \operatorname{Irr} K[X]$ has a root a in the field M. Because N is the normal extension of K and $a \in N$, it follows that all roots of polynomial G belong to the field N. The element a is separable relative to K, and so belongs to M. Hence polynomial g is the product of linear polynomials belonging to $M[X]$, which proves that M is the normal extension of the field K.

Since M is the normal extension of K and the Galois extension of K, then L is the normal extension of K by the assumption (see [3, Exercise 4, p. 119]).

Because L is the normal extension of K, then L is the finite extension of K. And by Theorem 1 we get that $K + XL[X]$ is Noetherian. □

Proposition 3. *Let $K \subset L$ be a field extension and let $T = K + XL[X]$. Assume that if a map $\varphi\colon L \to a(K)$ is K-embedding, then $\varphi(L) = L$. Then the following conditions are equivalent:*

(1) T is Noetherian;

(2) $K \subset L$ is a normal extension.

Proof. *(1) ⇒ (2)* By Proposition 1, $K \subset L$ is the algebraic extension.

Let c be a root of polynomial g belonging to L, and b be the arbitrary root of g belonging to $a(K)$. Because $g \in \operatorname{Irr} K[X]$, by Corollary from Lemma 1 there exists K-isomorphism $\varphi'\colon K(c) \to K(d)$. By Lemma 2 it can be extended to an embedding $\varphi\colon L \to a(K)$. Hence towards $\varphi(L) = L$ and $\varphi\big(K(c)\big) = \varphi'\big(K(c)\big) = K(d)$ we get that $K(d) \subset L$, so $b \in L$. Hence every root of polynomial g belongs to L, so polynomial g is the product of linear polynomials belonging to $L[X]$.

For every $c \in L$, let $g_c \in \operatorname{Irr} K[X]$ satisfying $g_c(c) = 0$. From the above it follows that every root of g_c belongs to the field L. Hence L is a composition of splitting field of all polynomials g_c, where $c \in L$. Hence L is the normal extension of K.

(2) ⇒ (1) If L is a normal extension of the field K, then $K \subset L$ is the finite extension. Then by Theorem 1 we get that $K + XL[X]$ is Noetherian. □

In the above proposition we can replace the assumption "if a map $\varphi\colon L \to a(K)$ is K-embedding, then $\varphi(L) = L$" to "$L^{G(L|K)} = K$". Then we obtain the following assertion.

Proposition 4. *Let $K \subset L$ be a field extension such that $L^{G(L|K)} = K$. If $T = K + XL[X]$ is a Noetherian, then $K \subset L$ is a normal extension.*

Proof. By Proposition 1, we get that $K \subset L$ is an algebraic field extension. Assuming $L^{G(L|K)} = K$, we get directly from the definition of the Galois extension, and so normal extension. □

Proposition 5. *Let $T = K + XL[X]$ be Noetherian, where $K \subset L$ is a field. Assume $\left|G(L \mid K)\right| = [L\colon K]$ and any K-isomorphism $\varphi\colon M \to M$, where $\varphi(L) = L$, holds for every field M such that $L \subset M$. Then the following conditions are equivalent:*

(1) T is Noetherian;

(2) $K \subset L$ is a Galois extension.

Proof. *(1) ⇒ (2)* By Theorem 1, we get $K \subset L$ is the finite extension. By the assumption, we can use Lemma 3 and we get that $K \subset L$ is a Galois extension.

(2) ⇒ (1) If $K \subset L$ is a Galois field extension, then it is separable. By Proposition 2, we get that $K + XL[X]$ is Noetherian. □

In the above proposition, we can swap the assumptions "$\left|G(L \mid K)\right| = [L\colon K]$ and any K-isomorphism $\varphi\colon M \to M$, where $\varphi(L) = L$, holds for every field M such that $L \subset M$" to "$L^{G(L|K)} = K$". Then we obtain the following assertion.

Proposition 6. *Let $T = K + XL[X]$, where $K \subset L$ is a field such that $K = L^{G(L|K)}$. The following conditions are equivalent:*

(1) T is Noetherian;

(2) $K \subset L$ is a Galois extension.

Proof. *(1) ⇒ (2)* By Proposition 1, we get that $K \subset L$ is the algebraic extension. Assuming $K = L^{G(L|K)}$, we get directly from the definition of the Galois extension.

(2) ⇒ (1) If $K \subset L$ is a Galois field extension, then $K \subset L$ is a normal extension. Hence by Proposition 4 we get that $K + XL[X]$ is Noetherian. □

Proposition 7. *Let $K \subset L \subset M$ be fields such that K is a perfect field. If $K + XL[X]$ and $L + XM[X]$ are Noetherian, then $K \subset M$ is separable field extension.*

Moreover, if we assume that any K-isomorphism $\varphi\colon M' \to M'$, where $\varphi(M) = M$ holds for every field M' such that $M \subset M'$, then $K + XM[X]$ is a Noetherian.

Proof. By Proposition 2, we get $K \subset L$, $L \subset M$ are separable extensions. Then $K \subset M$ is a separable extension. Moreover, from Proposition 2 we get $K + XM[X]$ is Noetherian. □

Proposition 8. *Let $K \subset L \subset M$ be fields such that $M^{G(M|K)} = K$. If $K + XM[X]$ is Noetherian, then $L \subset M$ is a normal field extension. Moreover, $L + XM[X]$ is Noetherian.*

Proof. By Proposition 4, we have that $K \subset M$ is a normal extension. Then $L \subset M$ is the normal extension. Moreover, from Proposition 2 we get that $L + XM[X]$ is Noetherian. $\square$

Proposition 9. *Let $K \subset L$ be a field extension such that $[L\colon K] = 2$. Then $K + XL[X]$ is Noetherian. Moreover, if $L^{G(L|K)} = K$, then $K \subset L$ is normal.*

Proof. Of course, from Theorem 1 we get $K + XL[X]$ is Noetherian. By Proposition 4, we have $K \subset L$ is a normal field extension. $\square$

3 Field extensions and ideals in composites

In this chapter, let us consider how can ideals be characterized in such polynomial composites, assuming that a given field extension is a certain type.

Proposition 10. *Let $K \subset L$ be fields and algebraic extension such that $K = L^{G(L|K)}$. Then every ideal of $K + XL[X]$ is finite generated.*

Proof. By Propositon 1, we have that $K + XL[X]$ is Noetherian. Hence every ideal of $K + XL[X]$ is finite generated. $\square$

Corollary 1. *Let $K \subset L$ be fields and finite extension. Then every ideal of $K + XL[X]$ is finite generated.*

Unfortunately, the following questions have arisen at the moment.

Question 2. *What is the additional argument of the Proposition 10 if we assume that field extension is separable?*

Question 3. *What is the additional argument of the Propostion 10 if we assume that field extension is normal?*

4 Full characterization

In this section, we present the full possible characterization of field extensions. Combining the A.R. Magid's results and from this paper, we get the following two theorems.

Theorem 2 ([6, Theorem 1.2.]). *Let M be an algebraically closed field algebraic over K, and let L such that $K \subseteq L \subseteq M$ be an intermediate field. Then the following are equivalent:*

(a) L is separable over K;

(b) $M \otimes_K L$ has no nonzero nilpotent elements;

(c) every element of $M \otimes_K L$ is a unit times an idempotent;

(d) as an M-algebra $M \otimes_K L$ is generated by idempotents.

Theorem 3 ([6, Theorem 1.3]). *Let M be an algebraically closed field containing K, and let L be a field algebraic over K. Then the following are equivalent:*

(a) L is separable over K;

(b) $M \otimes_K L$ has no nonzero nilpotent elements;

(c) every element of $M \otimes_K L$ is a unit times an idempotent;

(d) as an M-algebra $M \otimes_K L$ is generated by idempotents.

Below we have conclusions from the above results.

Theorem 4. *If we assume $L^{G(L|K)} = K$ in Theorems 2 and 3, then the conditions (a) – (d) are equivalent to*

(e) $K + XL[X]$ *is Noetherian;*

(f) $[L\colon K] < \infty$*;*

(g) $K \subset L$ *is an algebraic extension;*

(h) $K \subset L$ *is a Galois extension.*

Proof. *(h) ⇒ (a)* It is obvious.

(a) ⇒ (g) ⇒ (e)⇒ (h) If $K \subset L$ is a separable extension, then it is an algebraic extension. By Proposition 1, $K + XL[X]$ is a Noetherian. By Proposition 6, $K \subset L$ is a Galois extension.

(e) ⇒ (f) It is Theorem 1. □

Theorem 5. *If we assume that K is a perfect field and $L^{G(L|K)} = K$ in Theorem 4, then the conditions (a) – (h) are equivalent to the following:*

(g) $K \subset L$ *is a normal extension.*

Proof. *(g) ⇒ (a)* If $K \subset L$ is a normal extension, then it is an algebraic extension. By definition, perfect field $K \subset L$ is a separable extension.

(h) ⇒ (g) It is obvious. □

Proposition 6, Theorems 4 and 5 can be used to solve the inverse Galois problem. There is a lot of work and it is enough to solve the problem for nonabelian groups. Thus, the following question arises.

Question 4. *Can all the statements in this paper operate in noncommutative structures?*

And another question also arises regarding polynomial composites.

Question 5. *Under certain assumptions for any type of $K \subset L$, we get that $K + XL[X]$ is a Noetherian ring. When can $K + XL[X]$ be isomorphic to any Noetherian ring?*

5 The inverse Galois problem

Let us start from the following assertion.

Lemma 5. *Let K be a field and G be a finite group of field automorphism of K, then K is a Galois extension of the fixed field K^G with Galois group G, moreover $[K\colon K^G] = |G|$.*

Proof. Pick any $\alpha \in K$ and consider a maximal subset $\{\sigma_1, \dots, \sigma_n\} \subseteq G$ for which all $\sigma_i\alpha$ are distinct. Now any $\tau \in G$ must permute the $\sigma_i\alpha$ as it is an automorphism. If some $\tau\sigma_i\alpha \neq \sigma_j\alpha$ for all j, then we could extend our set of σ's by adding this $\tau\sigma_i$.

So, α is a root of

$$f_\alpha(X) = \prod_{i=1}^{n}(X - \sigma_i\alpha).$$

Note that f_α is fixed by τ by the above. So, all the coefficients of f_α are in K^G. By construction, f_α is a separable polynomial as the $\sigma_i\alpha$ were chosen distinct, note that f_α also splits into linear factors in K.

The above was true for arbitrary $\alpha \in K$. So we must show directly that K is a separable and normal extension of K^G, which is the definition of Galois extension. As every element of K^G is a root of a polynomial of degree n, we can not have the extension of degree $[K\colon K^G] > n$. But we also have a group of n automorphisms of K that fix K^G, so $[K\colon K^G] \geqslant n$ and hence $[K\colon K^G] = n$. □

Theorem 6. *Every finite group is a Galois group.*

Proof. Let K be an arbitrary field, G any finite group. Now take $L = K(g'\colon g \in G)$ (i.e. adjoin all elements of G to K as indeterminates, denoted by g'). Now we have a natural action of G on L defined via $h \cdot g' = (hg)'$ and extending K-linearly. Now L and G satisfy Lemma 5 and hence $L^G \subset L$ is a Galois extension with Galois group G. □

From proof we get the inverse Galois problem in the classic form.

Corollary 2. *Let G be a finite group. Then there exists a field extension L of $\mathbb{Q}$ such that G is a Galois group of this extension.*

References

[1] Anderson D.D., Anderson D.F., Zafrullah M. *Rings between D[X] and K[X]*. Houston J. Math. 1991, **17**, 109–129.

[2] Brewer J.M., Rutter E.A. *D+M construction with general overrings*. Michigan Math. J. 1976, **23** (1), 33–42. doi:10.1307/mmj/1029001619

[3] Browkin J. Theory of Fields. PWN, Warszawa, 1977.

[4] Costa D., Mott J.L., Zafrullah M. *The construction $D + XD_S[X]$*. J. Algebra 1978, **53**, 423–439.

[5] Eakin Jr.P.M. *The converse to a well known theorem on Noetherian rings*. Math. Ann. 1968, **177**, 278–282. doi: 10.1007/BF01350720

[6] Magid A.R. The Separable Galois Theory of Commutative Rings. (2nd ed.) Chapman and Hall/CRC, Boca Raton, 2014. doi:10.1201/b17145

[7] Matysiak Ł. *On properties of composites and monoid domains*. Ital. J. Pure Appl. Math. 2022, **47**, 796–811.

[8] Zafrullah M. *The $D + XD_S[X]$ construction from GCD-domains*. J. Pure Appl. Algebra 1988, **50** (1), 93–107.

Received 05.01.2022
Revised 22.03.2022

Матисяк Л. *Поліноміальні композити та деякі типи розширень полів* // Карпатські матем. публ. — 2023. — Т.15, №1. — С. 150–157.

У цій статті ми розглядаємо поліноміальні композити з коефіцієнтами з $K \subset L$. Нам відомо багато властивостей, але ми не знаємо відповіді на питання про існування взаємозв'язку між композитами та розширеннями полів. Ми даємо характеризацію деяких відомих розширень полів в термінах поліноміальних композитів. Ця стаття містить відкриту проблему про характеризацію ідеалів в поліноміальних композитах у відношенні до різних розширень полів. Ми також подаємо повну можливу характеризацію деяких розширень полів. Більше того, у цій статті ми показуємо, що кожна скінченна група є групою Галуа деякого розширення поля і представляємо розв'язану обернену проблему Галуа.

Ключові слова і фрази: розширення поля, поліном, розширення скінченного поля, кільце Нетер, група Галуа.