GLASNIK MATEMATIČKI
Vol. 43(63)(2008), 7 – 12

ON DECOMPOSITION OF POLYNOMIALS OVER RINGS

Ivica Gusić
University of Zagreb, Croatia

Abstract. We discuss the behavior of decomposability of polynomials under ring extension. Also, we state two open problems.

1. Introduction

Let K and M be fields of characteristic 0 with $K \subseteq M$ and let f be a polynomial over K. We say that f is decomposable over M if there exist polynomials g, h over M of degrees at least 2 such that $f = g \circ h$.
We say that a decomposition of f is equivalent to the decomposition $f = g \circ h$ if it is of the form

$$f = (g \circ L^{-1}) \circ (L \circ h)$$

for a linear polynomial L. It is well known that decomposability over an extension of K implies decomposability over K (see [4, Theorem 6.]). Here we present a proof of a slightly more complete result (see [2, Theorem 7.]). The proof is based on elementary properties of Galois group that can be found in [3]. By the sake of simplicity we work in zero characteristic, although in most cases analogous results are valid over arbitrary fields, under assumption that the characteristic does not divide the degree of f.

Theorem 1.1. *Let f be a polynomial over K and let $f = g \circ h$ be a decomposition over M. Then:*

(a) *The decomposition $f = g \circ h$ is equivalent to a decomposition $f = (g \circ L^{-1}) \circ (L \circ h)$ over K.*
(b) *The following statements are equivalent:*
  (i) *g and h are defined over K.*
  (ii) *L is defined over K.*

2000 *Mathematics Subject Classification.* 13B25, 11C08, 13B22, 13F15.
Key words and phrases. Composition of polynomials, Galois group, discrete valuation.

(iii) *h is defined over K.*
(iv) *$c_0 \in K$ and $c_i \in K \setminus \{0\}$ for an index $i \in \{1, \dots, r\}$, where $h(X) := c_r X^r + \cdots + c_0$.*

PROOF. (a) Put $L(X) := \frac{X}{c_r} - \frac{c_0}{c_r}$, $\tilde{h} := L \circ h$, $\tilde{g} = g \circ L^{-1}$. Then $g \circ h = \tilde{g} \circ \tilde{h}$. Note that $\tilde{h}$ is monic (i.e. with leading coefficient 1) and that $\tilde{h}(0) = 0$. Let us fix a Galois closure M' of M and let σ be arbitrary automorphism of M' over K. Then from

$$f = \tilde{g} \circ \tilde{h}$$

we get

$$\sigma(f) = \sigma(\tilde{g}) \circ \sigma(\tilde{h}).$$

Here σ acts on polynomials over M' by acting on the coefficients. Since $\sigma(f) = f$, we get

$$f = \tilde{g} \circ \tilde{h} = \sigma(\tilde{g}) \circ \sigma(\tilde{h})$$

By [4, Theorem 5.], we see that $\sigma(\tilde{h}) = a\tilde{h} + b$ for suitable $a, b \in M'$. Since $\tilde{h}$ is monic, we get $a = 1$, and since $\tilde{h}(0) = 0$, we get $b = 0$. It is valid for all automorphisms σ of M' over K, and so $\tilde{h}$ is defined over K.

Now we get

$$\sigma(\tilde{g}) \circ \tilde{h} = \tilde{g} \circ \tilde{h}$$

for all σ, hence

$$\sigma(\tilde{g}) = \tilde{g}$$

for all σ, which implies that $\tilde{g}$ is defined over K, too.

(b) $(i) \Rightarrow (ii)$, $(ii) \Rightarrow (iii)$, and $(iii) \Rightarrow (iv)$ are obvious. It remains to prove $(iv) \Rightarrow (i)$. As in (a) we get $\sigma(h) = Ah + B$ for some $A, B \in M'$, where σ is a fixed K-automorphism of M'. Then from $c_i \in K \setminus \{0\}$ for an index $i \in \{1, \dots, r\}$, we get $c_i = Ac_i$, hence $A = 1$. Now from $c_0 \in K$ we get $B = 0$. Since it is valid for arbitrary σ, we see that h is defined over K, which implies, as in (a), that g is defined over K, too. □

REMARK 1.2. In the proof of Theorem 1.1, we infer from [4, Theorem 5.] that the relation $g \circ h = G \circ H$ for nonconstant polynomials over a field k of zero characteristic, with $\deg h = \deg H$, implies $H = ah + b$ for some $a, b \in k$. Since the proof of Theorem 5 from [4] is pretty sophisticated, we present here a direct proof of the needed result.

By $g \circ h = G \circ H$ and $\deg h = \deg H$ we get $H = ah + h_0$ for $a \in k$ and a polynomial h_0 with $\deg h_0 < \deg H$. We claim that h_0 is a constant polynomial. Assume the contrary and look at the Taylor expansion:

$$g \circ h = G \circ (ah + h_0) = \sum_0^m (G^{(i)} \circ h_0) \frac{(ah)^i}{i!}$$

where m denotes the degree of G. The left side is a k-linear combination of polynomials $\{1, h, \dots, h^m\}$ while the right side is a sum of $m+1$ polynomials

with degrees $(m-i)\deg h_0 + i\deg h$ for $i = 0, 1, \ldots, m$. Especially, all members of the right side are non-constant and of different degrees. Hence, the set of degrees appearing on the left side is different from the set of degrees appearing on the right side. It is impossible, and so h_0 should be constant.

In some applications arises need for analogous results over rings (see [1]). However, we have to make some restrictions on the rings or polynomials. In this paper we consider polynomials over integral domains in characteristic 0. It occurs that the case of monic polynomials is much simpler. In that case we prove that all decompositions are essentially defined over the integral closure (see Theorem 2.1, Corollary 2.2 and Example 2.3). It is an open question if the result is optimal (see Problem 3.1).
In Example 2.4 we construct a (non-monic) polynomial over $A := \mathbf{Z}[\sqrt{-5}]$ that is decomposable over $K := \mathbf{Q}[\sqrt{-5}]$, but not over A. It seems that it is an effect of non-triviality of the ideal class group of K. In Theorem 2.5 we prove that such examples do not exist over unique factorization domains of zero characteristic. It is an open question if that condition on the ring is minimal (see Problem 3.2).

2. Decomposition of polynomials over rings

In this section we consider the problem from Section 1 for polynomials over rings. Let us recall some standard definitions and facts. A ring A is called an integral domain if it is a commutative ring with 1 (where $1 \neq 0$) without zero divisors. The field of fractions of A is the smallest field containing A (defined uniquely up to an isomorphism). If M is a field containing A and $x \in M$ then we say that x is integral over A if x is a root of a monic polynomial over A. The set of all elements from M that are integral over A form a ring (the integral closure of A in M). We say that A is integrally closed if it is integrally closed in its field of fractions.

We begin our consideration with monic polynomials. In the following theorem we simulate the proof from [1, Theorem 2.1].

Theorem 2.1. *Let A be an integral domain of zero characteristic and let f be a monic polynomial over A. Let K denote the field of fractions of A and B the integral closure of A in K. Assume that $f = g \circ h$ is a decomposition over an extension field of K. Then it is equivalent to a decomposition over B.*

Proof. By Theorem 1.1, the decomposition $f = g \circ h$ is equivalent to $f = G \circ H$, where $G, H \in K[X]$ are monic and $H(0) = 0$. We claim that G, H are defined over B.

Put $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$, $G(X) = (X - \beta_1) \cdots (X - \beta_m)$, for $\alpha_1, \ldots, \alpha_n$ integral over A and $\beta_1, \ldots, \beta_m$ algebraic over K. Thus,

$$f(X) = (H(X) - \beta_1) \cdots (H(x) - \beta_m).$$

The polynomials $f(X)$ and $H(X)-\beta_j$, $j=1,2,\dots,m$ have a factorization into linear polynomials over a suitable algebraic extension of K containing $\alpha_1,\dots,\alpha_n;\beta_1,\dots,\beta_m$. Since the factorization is unique,

$$H(X)-\beta_j = const\cdot\prod_{i\in I}(X-\alpha_i),$$

for a suitable set of indices $I\subset\{1,2,\dots,n\}$. But $H(X)-\beta_j$ is monic, which implies that $const=1$. Since the α_i's are integral over A and $H(0)=0$, we conclude that β_j, $j=1,\dots,m$ (the roots of $G(X)$) are integral over A and also the coefficients of H are integral over A. Since H is defined over K, we see that it is defined over B. Similarly, $G\in B[X]$. □

Corollary 2.2. *Let A be an integrally closed integral domain of zero characteristic and let f be a monic polynomial over A. Let K denote the field of fractions of A. Assume that $f=g\circ h$ is a decomposition over an extension field of K. Then it is equivalent to a decomposition over A.*

Let us notice on two restrictions in Corollary 2.2:

(i) restriction on A (closeness),
(ii) restriction on f (unitarity).

In the following example we show that the restriction on A is not superfluous.

Example 2.3. Let $A:=\mathbf{Z}[\sqrt{-3}]$. Then $K=\mathbf{Q}[\sqrt{-3}]$ and $B=\mathbf{Z}[\rho]$, where ρ is a nontrivial third root of unity. Put $f(X)=X^4+2\rho X^3-X\in A[X]$, and $f=g\circ h$, where $g(X):=X^2-\rho^2X$ and $h(X):=X^2+\rho X$, is a nontrivial decomposition over over B. This decomposition is not equivalent to a decomposition over A. However, it is sufficient to check the decompositions $f=G\circ H$ with $G(X)=X^2+aX$ and $H(X)=X^2+bX$, for which we get $b=\rho$.

In the case of non-monic polynomials we have to make wider restrictions on the rings. Namely, the following example shows that Theorem 2.1 fails generally for arbitrary polynomials even over the rings of integers of number fields (which are integrally closed).

Example 2.4. A quartic polynomial $f(X):=uX^4+vX^3+zX^2+wX$ is decomposable (over a field) if and only if there exist $a\neq 0$, $\alpha\neq 0$, b and β such that $uX^4+vX^3+zX^2+wX=a(\alpha X^2+\beta X)^2+b(\alpha X^2+\beta X)$. It is easy to see that this is satisfied if and only if the condition $z=\frac{v^3+8u^2w}{4uv}$ holds (and then should be $a=\frac{u}{\alpha^2}$, $\beta=\frac{v\alpha}{2u}$ and $b=\frac{2uw}{\alpha v}$).
Assume now that $A:=\mathbf{Z}[\sqrt{-5}]$, the ring of integers of the quadratic field $K:=\mathbf{Q}[\sqrt{-5}]$, and that

$$f(X):=3(1+\sqrt{-5})X^4+12X^3+2(4-\sqrt{-5})X^2+2(1-\sqrt{-5})X.$$

It is easy to see that f satisfies the condition of decomposability, so it is decomposable over K. Assume that it is decomposable over A. Then $a = \frac{3(1+\sqrt{-5})}{\alpha^2} \in A$, $\beta = \frac{\alpha(1-\sqrt{-5})}{3} \in A \setminus \{0\}$ and $b = \frac{6}{\alpha} \in A$ with $\alpha \in A \setminus \{0\}$. It is well known that there exist non-principal different prime ideals $\mathcal{P}$, $\mathcal{Q}$ and $\overline{\mathcal{Q}}$ (the conjugate of $\mathcal{Q}$) in A satisfying
$(2) = \mathcal{P}^2$, $(3) = \mathcal{Q}\overline{\mathcal{Q}}$, $(1+\sqrt{-5}) = \mathcal{P}\mathcal{Q}$ and $(1-\sqrt{-5}) = \mathcal{P}\overline{\mathcal{Q}}$
(here, for any $y \in A$, we denote by (y) the principal ideal in A generated by y).
Now, we get $(\beta) = (\alpha)\frac{\mathcal{P}}{\mathcal{Q}}$, and so $\mathcal{Q}|(\alpha)$. Also $(a)(\alpha)^2 = \mathcal{P}\overline{\mathcal{Q}}\mathcal{Q}^2$, hence $(\alpha) = \mathcal{Q}$, a contradiction.

In the following theorem (which is a generalization and an extension of [1, Theorem 2.1]) we show that the restriction on f in Corollary 2.2 may be omitted provided A is a unique factorization domain.

THEOREM 2.5. *Let A be a unique factorization domain of zero characteristic and let f be a polynomial over A. Let K denote the field of fractions of A. Assume that $f = g \circ h$ is a decomposition over an extension field of K. Then it is equivalent to a decomposition over A.*

PROOF. It is sufficient to prove the theorem for primitive polynomials f, i.e. polynomials satisfying: if $f = cg$ for $c \in A$, and $g \in A[X]$, then c is invertible (in A). According to Theorem 1.1, the decomposition $f = g \circ h$ is equivalent to a decomposition $f = \tilde{g} \circ \tilde{h}$ over K with $\tilde{h}(0) = 0$. Further, it is equivalent to a decomposition

$$f = \epsilon G \circ H$$

with G, H over A primitive, $H(0) = 0$ and $\epsilon \in K$. We claim that ϵ is invertible (in A). To see this, assume that $v_p(\epsilon) > 0$ for a prime $p \in A$. Then $\bar{f} = 0$, where $\bar{f}$ denotes the reduction of f modulo p. It contradicts the fact that f is primitive. Namely, a polynomial over A is primitive if and only if its reductions modulo p are non-zero for all primes p of A. Assume now that $v_p(\epsilon) < 0$ for a prime p. Then $\overline{\frac{1}{\epsilon}f} = 0$, and so, since the reduction modulo p is a homomorphism, $\bar{G} \circ \bar{H} = 0$. Since G, H are primitive we see that $\bar{H}$ is constant, and since $H(0) = 0$, we see that $\bar{H} = 0$, a contradiction. Therefore, $v_p(\epsilon) = 0$ for all primes p, hence ϵ is invertible. □

REMARK 2.6. The fact that the product of primitive polynomials (over a unique factorization domain) is a primitive polynomial is known as the Gauss lemma, and it is a direct consequence of the fact that the reduction modulo p is a homomorphism. The composition of primitive polynomials is not a primitive polynomial, generally. To formulate a more precise result, let us say that a polynomial f is super-primitive if the polynomial $f(X) - f(0)$ is primitive. However, if f is super-primitive, then it is primitive. It is easy

to see that the following is valid: if g, h are primitive polynomials, and h is super-primitive, then $g \circ h$ is primitive.

Note that Example 2.4 shows that Theorem 2.5 is not valid for Dedekind domains, generally.

3. Open problems

Problem 3.1. *Prove or disprove. Let A be an integral domain of zero characteristic. Let B denote the integral closure of A in the field of fractions of A. Assume that $B \neq A$. Then there exists a monic polynomial f over A that is decomposable over B but not over A.*

Problem 3.2. *Prove or disprove. Let A be the ring of integers of a number field K. Assume that A is not a unique factorization domain. Then there exists a polynomial f over A that is decomposable over K but not over A.*

References

[1] A. Dujella and I. Gusić, *Indecomposability of polynomials and related diophantine equations*, Quart. J. Math. Oxford Ser. **498** (2005), 173-199.
[2] A. Horwitz, *Composition of polynomials with coefficients in a given field*, J. Math. Anal. Appl. **267** (2002), 489-500.
[3] S. Lang, Algebra, Addison-Wesley 1993.
[4] A. Schinzel, Polynomials with special regard to reducibility, Cambridge University Press, 2000.

I. Gusić
Faculty of Chemical Engin. and Techn.
University of Zagreb
Marulićev trg 19
10000 Zagreb
Croatia
E-mail: igusic@fkit.hr

Received: 24.8.2007.
Revised: 9.10.2007.