Časopis pro pěstování matematiky a fysiky

Štefan Schwarz

On the extension of the Jordan-Kronecker's "Principle of reduction" for inseparable polynomials“”

Časopis pro pěstování matematiky a fysiky, Vol. 72 (1947), No. 2, 61--64

Persistent URL: `http://dml.cz/dmlcz/121935`

On the extension of the Jordan-Kronecker's „Principle of reduction“ for inseparable polynomials.

Štefan Schwarz, Bratislava.

(Received January 15th, 1947.)

In this paper we shall prove two theorems concerning inseparable polynomials with coefficients in a given field P[1]).

Theorem 1. *Let* P *be a commutative field of characteristic* p, *which is not perfect. Let* $f(x)$ *and* $g(x)$ *be two eventually inseparable irreducible polynomials with coefficients in* P *of degree* m *and* n *respectively. Let* α, β *be the roots of* $f(x) = 0$ *and* $g(x) = 0$ *respectively. Let*

$$f(x) = f_1(x; \beta)^{p^{e_1}} \cdot f_2(x; \beta)^{p^{e_2}} \dots f_r(x; \beta)^{p^{e_r}}, \tag{1}$$

$$g(x) = g_1(x; \alpha)^{p^{e'_1}} \cdot g_2(x; \alpha)^{p^{e'_2}} \dots g_s(x; \alpha)^{p^{e'_s}}, \tag{2}$$

be the decompositions of $f(x)$ *and* $g(x)$ *into irreducible factors in* $P_2 = P(\beta)$ *and* $P_1 = P(\alpha)$ *respectively. Let the degrees of* $f_i(x; \beta)$ *and* $g_i(x; \alpha)$ *be* m_i $(i = 1, 2, \dots, r)$ *and* n_i $(i = 1, 2, \dots, s)$ *respectively so that the relations*

$$m_1 p^{e_1} + m_2 p^{e_2} + \dots + m_r p^{e_r} = m,$$
$$n_1 p^{e'_1} + n_2 p^{e'_2} + \dots + n_s p^{e'_s} = n,$$

are satisfied.

Under these suppositions the following relations hold:

i) it is $r = s$,

ii) by a suitable arrangement of the factors we have $\dfrac{m_i}{n_i} = \dfrac{m}{n}$ *(for every* i*),*

---

1) Following a suggestion of prof. Dr. Vl. Kořínek, I extend here the method applied in my paper „A hypercomplex proof of the Jordan-Kronecker's »Principle of reduction«“, Časopis pro pěst. mat. fys., 71 (1946), p. 17—20, to inseparable polynomials.

For another proof of these theorems see: Fr. K. Schmidt, Sitzungsberichte d. Heidelb. Akad. d. W., math. naturw. Klasse, 5. Abh., 1925.

iii) by the same arrangement of the factors we have $e_i = e'_i$ *(for every i).*

Proof. We form the hypercomplex system over P

$$\mathfrak{S} = \mathsf{P}_1 \times \mathsf{P}_2.$$

We have

$$\mathfrak{S} = \mathsf{P}_1 \times \mathsf{P}_2 = \mathsf{P}_2 + \mathsf{P}_2\alpha + \ldots + \mathsf{P}_2\alpha^{m-1} \cong \mathsf{P}_2[x] \mid (f(x)) = \\ = \mathsf{P}_2[x] \mid (f_1(x;\beta))^{p^{e_1}} \ldots (f_r(x;\beta))^{p^{e_r}}.$$

On the other hand we have the analogous decomposition

$$\mathfrak{S} = \mathsf{P}_1 \times \mathsf{P}_2 = \mathsf{P}_1 + \mathsf{P}_1\beta + \ldots + \mathsf{P}_1\beta^{n-1} \cong \mathsf{P}_1[x] \mid (g(x)) = \\ = \mathsf{P}_1[x] \mid (g_1(x;\alpha))^{p^{e'_1}} \ldots (g_s(x;\alpha))^{p^{e'_s}}.$$

The commutative ring $\mathfrak{S}$ is therefore expressible as a direct sum of primary rings[2])

$$\mathfrak{S} = \Phi_1 \oplus \Phi_2 \oplus \Phi_3 \oplus \ldots \oplus \Phi_r, \tag{3}$$

where

$$\Phi_i \cong \mathsf{P}_2[x] \mid (f_i(x;\beta))^{p^{e_i}} \quad (i = 1, 2, \ldots, r).$$

Similarly the second decomposition in primary rings has the form

$$\mathfrak{S} = \Gamma_1 \oplus \Gamma_2 \oplus \Gamma_3 \oplus \ldots \oplus \Gamma_s, \tag{4}$$

where

$$\Gamma_i \cong \mathsf{P}_1[x] \mid (g_i(x;\alpha))^{p^{e'_i}} \quad (i = 1, 2, \ldots, s).$$

Every primary commutative ring is irreducible, i. e. cannot be decomposed in the direct sum of two subrings. Further, it is well-known: The decomposition of a ring with a unity in two-sided direct irreducible components is (apart from the order of its components) uniquely determined. Comparing the decompositions (3) and (4) we have therefore:

i) $r = s$,
ii) every $\Phi_i = \Gamma_i$ if the Γ_i are properly numbered.

It follows from the last result

$$\mathsf{P}_2[x] \mid (f_i(x;\beta))^{p^{e_i}} \cong \mathsf{P}_1[x] \mid (g_i(x;\alpha))^{p^{e'_i}}. \tag{5}$$

The ring $\mathsf{O}_i = \mathsf{P}(\beta)[x] \mid (f_i(x;\beta))^{p^{e_i}}$ is an algebra of order $nm_ip^{e_i}$ over P. The unique prime ideal of the ring O_i is the ideal $\pi_i = (f_i(x;\beta))$. The exponent of π_i is p^{e_i}, i. e. the integer p^{e_i} is the least integer e for which π_i^e is the zero ideal (0): $\pi_i^{p^{e_i}} = (0)$. The ideal π_i is the radical of O_i.

Similarly the ring $\mathsf{O}'_i = \mathsf{P}(\alpha)[x] \mid (g_i(x;\alpha))^{p^{e'_i}}$ is an algebra

[2]) See e. g.: Van der Waerden, Moderne Algebra II, 1940, p. 42 and 151.

over P of order $mn_ip^{e'_i}$. The ideal $\pi'_i = (g_i(x; \alpha))$ is his unique prime ideal and at the same time his radical. The exponent of π'_i is $p^{e'_i}$.

The rings O_i, O'_i are isomorphic (the isomorphism leaving P invariant). We have therefore

i) $nm_ip^{e_i} = mn_ip^{e'_i}$,

ii) since it is obvious that the isomorphism carries elements of the radical of O_i into elements of the radical of O'_i, we have also $p^{e_i} = p^{e'_i}$, thus $e_i = e'_i$ and $nm_i = mn_i$, q. e. d.

Theorem 2. *Let the suppositions of Theorem 1 be satisfied. Let us write $g_i(x; \alpha)$ in the form of an integral function in α of the lowest degree. Then the greatest common divisor of $f(x)$ and $g_i(\beta; x)$ is*

$$(f(x), g_i(\beta; x)) = f_i(x; \beta). \tag{6}$$

Proof. Let us transform the right side of the isomorphism

$$\mathsf{P}_2[x] \mid (f_i(x; \beta))^{p^{e_i}} \cong \mathsf{P}_1[x] \mid (g_i(x; \alpha))^{p^{e_i}}.$$

Applying the second theorem of isomorphism ($(g(x))$ is a submodul of the ideal $(f(\xi), g_i(x; \xi)^{p^{e_i}})$ of the ring $\mathsf{P}[x, \xi]$), we have

$$\mathsf{P}_1[x] \mid (g_i(x; \alpha))^{p^{e_i}} \cong \mathsf{P}[x, \xi] \mid (f(\xi), g_i(x; \xi)^{p^{e_i}}) \cong$$
$$\cong \mathsf{P}[x, \xi] \mid (g(x)) \Big| (f(\xi), g_i(x; \xi)^{p^{e_i}}) \mid (g(x)) \cong \mathsf{P}_2[\xi] \mid (f(\xi), g_i(\beta; \xi)^{p^{e_i}}) \cong$$
$$\cong \mathsf{P}_2[x] \mid (f(x), g_i(\beta; x)^{p^{e_i}}).$$

Therefore

$$\mathsf{P}_2[x] \mid (f_i(x; \beta))^{p^{e_i}} \cong \mathsf{P}_2[x] \mid (f(x), g_i(\beta; x)^{p^{e_i}}).$$

Thus we have

$$f_i(x; \beta)^{p^{e_i}} = (f(x), g_i(\beta; x)^{p^{e_i}}),$$
$$f_i(x; \beta) \quad = (f(x), g_i(\beta; x)),$$

q. e. d.

*

O rozšírení Jordan-Kroneckerovho „Principu redukcie" na inseparabilné polynomy.

(Obsah predchádzajúceho článku.)

Obsahom predchádzajúcej poznámky je dôkaz týchto viet:

Nech P je nedokonalé teleso charakteristiky p. Nech $f(x)$ a $g(x)$ sú dva ireducibilné, po prípade inseparabilné, polynomy z telesa P stupňov m resp. n. Nech α, β sú korene rovnice $f(x) = 0$ resp. $g(x) = 0$. Nech rozklady $f(x)$ a $g(x)$ v ireducibilných súčiniteľov v telese $\mathsf{P}(\beta)$ resp. $\mathsf{P}(\alpha)$ sú dané vzťahmi (1) a (2). Stupne polynomov $f_i(x; \beta)$, $g_i(x; \alpha)$ nech sú m_i resp. n_i. Potom platí:

1. $r = s$,
2. pri vhodnom usporiadaní faktorov $e_i = e'_i$, $mn_i = nm_i$,
3. ak píšeme $g_i(x; \alpha)$ ako celistvú funkciu v α najnižšieho možného stupňa je polynom $f_i(x; \beta)$ daný vzťahom (6).
