Werk

Label: Article

Jahr: 1946

PURL: https://resolver.sub.uni-goettingen.de/purl?31311028X_0071|log8

A hypercomplex proof of the Jordan - Kronecker's „Principle of reduction".

Štefan Schwarz, Bratislava.

(Received November 1st, 1945.)

I.

This important theorem of the Galois' theory can be proved very simply by means of only elementary facts known from the theory of algebras.

Let $f(x)$ and $g(x)$ be two separable irreducible polynomials of degree m resp. n over a commutative field P. *Let α, β be the roots of $f(x) = 0$ and $g(x) = 0$ respectively. Let us denote* $\mathsf{P}_1 = \mathsf{P}(\alpha)$ *and* $\mathsf{P}_2 = \mathsf{P}(\beta)$. *Let*

$$f(x) = f_1(x) \cdot f_2(x) \ldots f_r(x), \tag{1}$$

$$g(x) = g_1(x) \cdot g_2(x) \ldots g_s(x) \tag{2}$$

be the decompositions of $f(x)$ and $g(x)$ into irreducible factors of degree m_i ($i = 1, 2, \ldots, r$) and n_i ($i = 1, 2, \ldots, s$) in P_2 and P_1 respectively. Then, the Jordan-Kronecker's Principle of reduction says: It is

i) $r = s$,

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

The proof is as follows. We form the hypercomplex system

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

over P:

We can write $\mathfrak{S}$ in two different manners.

It is first (we use the usual notation)

$$\mathfrak{S} = \mathsf{P}_{1\mathsf{P}_1} = \mathsf{P}_2 + \mathsf{P}_2\alpha + \mathsf{P}_2\alpha^2 + \ldots + \mathsf{P}_2\alpha^{m-1} \cong \mathsf{P}_2[z]/(f(z)).$$

On the other hand we have also

$$\mathfrak{S} = \mathsf{P}_{\mathsf{P}_1} = \mathsf{P}_1 + \mathsf{P}_1\beta + \mathsf{P}_1\beta^2 + \ldots + \mathsf{P}_1\beta^{n-1} \cong \mathsf{P}_1[z]/(g(z)),$$

where $\mathsf{P}_1[z]$, $\mathsf{P}_2[z]$ denote rings of polynomials in one variable z over P_1 and P_2 respectively.

The structures of the rings of remainder-classes on the right side of the last relations can be easily given. Writing the factorisation of $f(z)$ in $P_2[z]$ as above, we have

$$\mathfrak{S} \cong P_2[z]/(f(z)) = P_2[z]/(f_1 \cdot f_2 \ldots f_r).$$

But, this ring can be written as a direct sum of the fields Φ_1, $\Phi_2, \ldots, \Phi_r$ corresponding[1]) to the irreducible factors $f_1(z)$, $f_2(z)$, ..., $f_r(z)$ in $P_2[z]$.

Therefore

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

where

$$\Phi_i \cong P_2[z]/(f_i(z)), \quad i = 1, 2, \ldots, r.$$

In the same manner we treat the second equation (2) and we obtain the direct decomposition

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

where

$$\Gamma_i \cong P_1[z]/(g_i(z)), \quad i = 1, 2, \ldots, s.$$

The decomposition of a ring, possessing a unit, in two-sided direct irreducible components is uniquely determined[2]). Therefore, it is

i) $r = s$ and

ii) by a suitable arrangement $\Gamma_i = \Phi_i$ (for every i),

i. e.

$$P_1[z]/(g_i(z)) \cong P_2[z]/(f_i(z)).$$

The order of the field $P_1[z]$ $(g_i(z))$ over the field P is evidently $m \cdot n_i$. The order of $P_2[z]/(f_i(z))$ over P is $n \cdot m_i$.

From that isomorphisme follows therefore

$$m n_i = n m_i,$$

$$\frac{m}{n} = \frac{m_i}{n_i},$$

q. e. d.

II.

From the isomorphisme just proved

$$P_1[z]/(g_i(z)) \cong P_2[z]/(f_i(z))$$

---

[1]). See e. g.: Van der Waerden, Moderne Algebra II, Berlin 1931, p. 48.
[2]) See e. g.: Van der Waerden, ibid., p. 162.

follows an interesting and very easy proof of the following theorem due to A. Loewy (M. Z., 15, 1922, p. 266)).

Let — under the same suppositions as above — the explicite factorisation of $f(x)$ and $g(x)$ in P_2 and P_1 respectively be

$$f(x) = f_1(x, \beta) \cdot f_2(x, \beta) \ldots f_s(x, \beta),$$
$$g(x) = g_1(x, \alpha) \cdot g_2(x, \alpha) \ldots g_s(x, \alpha).$$

If we write $g_i(x, \alpha)$ in the form of an integral function in α of the lowest degree (what is possible because $P(\alpha) = P[\alpha]$) and replace in $g_i(x, \alpha)$ the variable x by the number β and the number α by the indeterminate x, we obtain a polynomial $g_i(\beta, x)$ possessing the following propriety: $f_i(x, \beta)$ is the greatest common divisor of $f(x)$ and $g_i(\beta, x)$.

Proof: We shall transform the left side of the isomorphisme

$$P_1[x]/(g_i(x, \alpha)) \cong P_2[x]/(f_i(x,\beta)). \qquad \cdot \qquad (*)$$

First it is evidently

$$P_1[x]/(g_i(x, \alpha)) \cong P[x, \xi]/(f(\xi), g_i(x, \xi)),$$

where $P[x, \xi]$ is the polynomial domain of all polynomials in two variables x and ξ with coefficients in the commutative field P. In fact, α satisfies the equation $f(\xi) = 0$, which is irreducible in P. Applying the transformation $x \to \xi$, $\xi \to x$ we have the further isomorphisme

$$P_1[x]/(g_i(x, \alpha)) \cong P[x, \xi]/(f(x), g_i(\xi, x)).$$

According to the second theorem of isomorphisme $((g(\xi))$ is a sub-modul of the ideal $(f(x), g_i(\xi, x)))$ we obtain

$$P[x,\xi]/(f(x), g_i(\xi, x)) \cong P[x, \xi]/(g(\xi)) \big/ (f(x), g_i(\xi, x))/(g(\xi)).$$

But the last expression is evidently isomorphic with

$$P_2[x]/(f(x), g_i(\beta, x)).$$

It is therefore

$$P_1[x]/(g_i(x, \alpha)) \cong P_2[x]/(f(x), g_i(\beta, x)).$$

Comparing it with the relation (*) we have

$$P_2[x]/(f(x), g_i(\beta, x)) \cong P_2[x]/(f_i(x, \beta)).$$

Therefore (in the sense of division!)

$$f_i(x, \beta) = (f(x), g_i(\beta, x)),$$

q. e. d.

---

[*] This theorem enables us to find the polynominal $g_i(x)$ corresponding to $f_i(x)$ and inversely.