S. KNAPOWSKI (Poznań)

O pewnych kryteriach nierozkładalności wielomianów

Celem niniejszego artykułu jest udowodnienie kilku kryteriów pozwalających stwierdzić nierozkładalność wielomianu, jeżeli znany jest rząd jego grupy Galois. Zakładam, że czytelnik zna podstawy teorii Galois, np. w zakresie książki B. L. van der Waerdena [1].

Na wstępie udowodnię twierdzenia pomocnicze.

Niech K będzie ciałem komutatywnym i doskonałym (tzn. takim, że każdy wielomian nierozkładalny w K ma tylko pojedyncze pierwiastki), a $f(x)$ wielomianem o współczynnikach z K. Niech w tym ciele zachodzi rozkład

$$f(x) = f_1(x) f_2(x) \tag{1}$$

(pierwiastki $f_1(x)$: $\alpha_1, \alpha_2, \ldots, \alpha_k$; pierwiastki $f_2(x)$: $\alpha_{k+1}, \alpha_{k+2}, \ldots, \alpha_n$); wtedy

$$\Sigma = K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Wiadomo, że grupą wielomianu $f(x)=0$ w ciele K jest grupa $\mathfrak{G}(\Sigma, K)$ (grupa ciała Σ względem ciała K). Podobnie, grupą wielomianu $f_1(x)=0$ w ciele K jest grupa $\mathfrak{G}(\Delta, K)$ (gdzie $\Delta = K(\alpha_1, \alpha_2, \ldots, \alpha_k)$). Wobec tego mamy $K \subset \Delta \subset \Sigma$.

Z zasadniczego twierdzenia teorii Galois wynika

$$\mathfrak{G}(\Delta, K) \simeq \mathfrak{G}(\Sigma, K)/\mathfrak{G}(\Sigma, \Delta).$$

Grupa $\mathfrak{G}(\Sigma, \Delta)$ jest grupą Galois wielomianu $f_2(x)=0$ w ciele Δ[1]). Stąd wynika

TWIERDZENIE 1. *Grupa Galois czynnika $f_1(x)$ rozkładu (1) jest izomorficzna z grupą ilorazową grupy Galois wielomianu $f(x)$ przez grupę Galois czynnika $f_2(x)$ w ciele rozszerzonym o pierwiastki czynnika $f_1(x)$.*

Przypuśćmy teraz, że pierwiastki wielomianu $f_2(x)=0$ wyrażają się jako funkcje wymierne pierwiastków wielomianu $f_1(x)=0$. Wtedy $\Delta = \Sigma$, zatem $\mathfrak{G}(\Delta, K) \simeq \mathfrak{G}(\Sigma, K)$.

Jeżeli na odwrót, $\mathfrak{G}(\Delta, K) \simeq \mathfrak{G}(\Sigma, K)$, to $\mathfrak{G}(\Sigma, \Delta)$ jest grupą jednostkową, skąd $\Delta = \Sigma$. Zatem pierwiastki wielomianu $f_2(x)=0$ wyrażają się wymiernie przez pierwiastki wielomianu $f_1(x)=0$.

[1]) Por. [1], str. 151.

Stąd wynika

TWIERDZENIE 2. *Warunkiem koniecznym i dostatecznym, by grupa Galois* $f_1(x)=0$ *czynnika rozkładu* (1) *była izomorficzna z grupą Galois wielomianu* $f(x)=0$ *jest, by każdy pierwiastek* $f_2(x)=0$ *wyrażał się wymiernie przez pierwiastki* $f_1(x)=0$.

Podane twierdzenia pozwalają dać kryteria nierozkładalności wielomianów.

KRYTERIUM I. *Jeżeli wielomian* $f(x)=0$ *o współczynnikach z* K, *stopnia* n, *nie ma żadnego pierwiastka należącego do* K *oraz jeżeli każdy jego pierwiastek wyraża się jako funkcja wymierna dowolnych dwu pierwiastków* $f(x)=0$, *to w przypadku gdy* m^2 *nie dzieli* $n!$ (m *jest rzędem grupy Galois* $\mathfrak{G}$ *wielomianu*) *wielomian jest nierozkładalny.*

Dowód. Przypuśćmy, że wielomian rozkłada się w sposób następujący:

$$f(x)=f_1(x)f_2(x) \qquad (f_i(x) \text{ ma stopień } k_i \geqslant 2,\ i=1,2).$$

Grupy Galois obu czynników rozkładu byłyby izomorficzne z grupą $\mathfrak{G}$. W szczególności obie miałyby rząd m.

Oznaczmy

$$km=n!, \qquad l_1 m=k_1!, \qquad l_2 m=k_2! \qquad (k_1+k_2=n).$$

Niech $n!/k_1!k_2!=c$. Jak wiadomo, c jest liczbą naturalną. Wobec tego $km/l_1 l_2 m^2=c$, czyli $k=l_1 l_2 mc$, zatem byłoby $m|k$, skąd $m^2|n!$, co jest sprzeczne z założeniem.

Uwaga. Zupełnie analogicznie można wypowiedzieć kryterium dla wielomianów normalnych[2]), których każdy pierwiastek jest generujący. Tu jednak mamy mocniejsze kryterium. Warunkiem koniecznym i dostatecznym nierozkładalności takich wielomianów jest $m=n$. Jest to twierdzenie prawie oczywiste.

Jako ilustracja kryterium I może służyć przykład wielomianu x^p-a (p jest liczbą pierwszą), nierozkładalnego w ciele liczb wymiernych. Grupa Galois wielomianu w tym ciele jest izomorficzna z pełną grupą metacykliczną[3]), zatem rząd jej wynosi $p(p-1)$. Wielomian nasz spełnia założenia kryterium I oraz $p^2(p-1)^2$ nie dzieli $p!$

KRYTERIUM II. *Wielomian stopnia* p *o grupie rzędu* p (p *jest liczbą pierwszą*) *jest nierozkładalny.*

Dowód. Grupa wielomianu jest cykliczna, bo jej rząd jest liczbą pierwszą. Oznaczmy przez π podstawienie generujące. Przypuśćmy, że

[2]) Por. [1], str. 104.

[3]) Zob. [2], str. 416, ćwiczenie 5.

rozpada się ono na k cykli po $n_1, n_2, \ldots, n_k$ wyrazów. Wtedy $n_1+n_2+\ldots+n_k=p$ (niektóre n_i mogą być równe 1). Mamy $\pi^l=1$ dla $l=p$ i nie wcześniej. Zatem p jest najmniejszą wspólną wielokrotnością liczb $n_1, n_2, \ldots, n_k$. Stąd $k=1$, $n_1=p$. Grupa jest więc przechodnia, czyli wielomian jest nierozkładalny, c. b. d. u.

KRYTERIUM III. *Niech $f(x)=0$ będzie wielomianem cyklicznym stopnia p^m (p jest liczbą pierwszą). Na to, by wielomian ten był nierozkładalny, potrzeba i wystarcza, by rząd jego grupy był równy stopniowi wielomianu.*

Dowód. Konieczność warunku wypływa stąd, że wielomian jako cykliczny i nierozkładalny jest normalny. Dla dowodu dostateczności przedstawmy podstawienie generujące π grupy jako iloczyn cykli po $n_1, n_2, \ldots, n_k$ wyrazów. Wtedy $n_1+n_2+\ldots+n_k=p^m$ (niektóre n_i mogą być równe 1). Analogicznie jak w dowodzie kryterium II, p^m jest najmniejszą wspólną wielokrotnością liczb $n_1, n_2, \ldots, n_k$. W szczególności liczby n_i jako dzielniki p^m muszą być postaci p^α ($\alpha \leqslant m$). Zatem $k=1$, $n_1=p^m$. Grupa jest więc przechodnia czyli wielomian jest nierozkładalny, c. b. d. u.

Uwaga. Konieczność warunku pozostaje w mocy także dla dowolnych wielomianów abelowych. Dowód jest analogiczny do poprzedniego. Natomiast dostateczność przestaje być słuszna w przypadku ogólnym.

Prace cytowane

[1] B. L. van der Waerden, *Moderne Algebra*, tom I, Berlin 1930.

[2] A. Mostowski, *Zarys teorii Galois*, przypis do książki W. Sierpińskiego *Zasady algebry wyższej*, Warszawa-Wrocław 1946.

С. КНАПОВСКИЙ (Познань)

НЕКОТОРЫЕ ТЕОРЕМЫ О НЕПРИВОДИМОСТИ ПОЛИНОМОВ

РЕЗЮМЕ

В настоящей работе представлены теоремы, которые позволяют убедиться в неприводимости некоторых алгебраических уравнений, если известен порядок их группы Галуа.

I. *Пусть $f(x)=0$ алгебраическое уравнение n-ой степени, коэффициенты которого принадлежат к некоторому совершенному полю K, но ни один из его корней не является элементом K, и пусть порядок его группы Галуа будет m.*

Если каждый из корней уравнения $f(x)=0$ выражается в виде рациональной функции произвольной пары корней уравнения и m^2 не делит $n!$, то уравнение неприводимо.

II. *Всякое уравнение степени p с группой Галуа порядка p (p простое число) — неприводимо.*

III. *Пусть* $f(x)=0$ *— циклическое уравнение степени* p^m (p *простое число*). *Для того, чтобы оно было неприводимым, необходимо и достаточно, чтобы* $\overline{\overline{\mathfrak{G}}}=p^m$ ($\mathfrak{G}$ *группа Галуа уравнения*).

S. Knapowski (Poznań)

CERTAIN THEOREMS, CONCERNING IRREDUCIBILITY OF POLYNOMIALS

SUMMARY

In this paper I prove some theorems, which permit us to state the irreducibility of certain algebraic equations when the order of the Galois group is known.

I. *Let* $f(x)=0$ *be an equation of degree* n, *its coefficients belonging to a perfect field* K, *and none of its zeros belonging to* K.

Let $\mathfrak{G}$ *be the Galois group of this equation and* $\overline{\overline{\mathfrak{G}}}=m$.

Let every zero of the equation $f(x)=0$ *be expressed by a rational function of each pair of zeros of this equation. If* $m^2 \nmid n!$, *then the equation is irreducible.*

II. *Every equation of degree* p (p *being prime*) *whose Galois group is of order* p *is irreducible.*

III. *Let* $f(x)=0$ *be a cyclic equation of degree* p^m (p *being prime*). *The necessary and sufficient condition for the irreducibility of the equation is:* $\overline{\overline{\mathfrak{G}}}=p^m$ ($\mathfrak{G}$ *is the Galois group of the equation*).
