PRZYPOMNIENIA.

TW. Galois $f \in \mathbb{Q}[x]$ - wielomian, $\mathbb{Q}_f$ - jego ciało rozkładu.

= pewna grupa permutacji jego pierwiastków.

Pierwiastki wielomianu f wyrażają się przez pierwiastniki $\Longleftrightarrow$ grupa Galois wielomianu f, $Gal(\mathbb{Q}_f/\mathbb{Q})$ jest rozwiązalna.

DEF. Grupa G jest rozwiązalna gdy jest abelowa lub gdy istnieją homomorfizmy

$$h_1 : G \to A_1$$
$$h_2 : ker(h_1) \to A_2$$
$$\vdots$$
$$h_n : ker(h_{n-1}) \to A_n$$

„rozkład" na grupy abelowe

takie, że grupy $A_1, \ldots, A_n$ oraz grupa $ker(h_n)$ są abelowe.

FAKT. Grupy $\overset{\text{permutacji}}{} S_3$ i S_4 są rozwiązalne.

TWIERDZENIE. Grupa A_5 (parzystych permutacji 5 elementów) nie jest rozwiązalna.

TROCHĘ PRZYGOTOWAŃ Z TEORII GRUP.

DEF. Podgrupa $N < G$ jest podgrupą <u>normalną</u> (ozn. $N \triangleleft G$) jeśli sprzężenia elementów z N za pomocą elementów z G pozostają w N, tzn. $\forall h\in N\ \forall g\in G\ \ ghg^{-1}\in N$.

PRZYKŁADY. W dowolnej grupie G zachodzi $\{1\}\triangleleft G$ oraz $G \triangleleft G$. $\{1\}$ i G są tzw. <u>trywialnymi</u> podgrupami normalnymi w G.

FAKT 1. Jeśli $\varphi: G\to H$ jest homomorfizmem grup, to jego jądro $\ker(\varphi) = \{g\in G : \varphi(g) = 1\in H\}$ jest podgrupą normalną w G.

<u>Dowód</u> Wiemy już, że $\ker(\varphi)$ jest podgrupą w G. Pokażmy zamkniętość na sprzęganie.
Niech $h\in\ker(\varphi)$, $g\in G$ dowolne. Wtedy

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\cdot 1\cdot\varphi(g^{-1}) =$$
$$= \varphi(g)\cdot\varphi(g^{-1}) = \varphi(g\cdot g^{-1}) = \varphi(1) = 1$$

Zatem $ghg^{-1}\in\ker(\varphi)$. $\square$

<u>FAKT 2</u>. Jeśli $\varphi: G\to H$ jest homomorfizmem, zaś $\ker(\varphi)=\{1\}$, to φ jest różnowartościowy.

<u>D-d</u>: Gdyby φ nie był różnowartościowy, to mielibyśmy takie $g_1\neq g_2$ że $\varphi(g_1)=\varphi(g_2)$.

Skoro $g_1\neq g_2$, to $g_1g_2^{-1} \neq g_2g_2^{-1} = 1$,

a z drugiej strony

$$\varphi(g_1g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1)\cdot(\varphi(g_2))^{-1} = \varphi(g_1)(\varphi(g_1))^{-1} = 1$$

czyli $g_1g_2^{-1}\in\ker(\varphi)=\{1\}$ — SPRZECZNOŚĆ. $\square$

<u>FAKT 3</u>. Nieabelowa grupa rozwiązalna G posiada nietrywialną podgrupę normalną.

<u>Dowód</u>: Niech

$h_1 : G \to A_1$

$h_2 : \ker(h_1) \to A_2$

$\vdots$

$h_n : \ker(h_{n-1}) \to A_n$

homomorfizmy jak w definicji rozwiązalności

($\text{tzn. } A_1, \ldots, A_n$ oraz $\ker(h_n)$ – abelowe).

- Pokażmy, że $\ker(h_1) \neq \{1\}$.

Gdyby $\ker(h_1) = \{1\}$, to h_1 byłby różnowartościowy.

Z nieabelowości G istnieją $g_1, g_2 \in G$ takie $g_1 g_2 \neq g_2 g_1$,

a wtedy $h_1(g_1 g_2) \neq h_1(g_2 g_1)$.

Ale z abelowości A_1

$$h(g_1 g_2) = h(g_1)\, h(g_2) \overset{\text{abelowość } A_1}{=} h(g_2)\, h(g_1) = h(g_2 g_1) \text{ – sprzeczność.}$$

Zatem rzeczywiście $\ker(h_1) \neq 1$.

- Gdyby G nie posiadała żadnej nietrywialnej podgrupy normalnej, to mielibyśmy

$\ker(h_1) = G$

$h_2 : \ker(h_1) \to A_2$

czyli $h_2 : G \to A_2$ i ten sam argument pokazuje że $\ker(h_2) = G$

itd.

dochodzimy do $\ker(h_n) = G$

ale G nieabelowa – sprzeczność z wymogiem z definicji rozwiązalności, że $\ker(h_n)$ abelowa. □

W świetle FAKTU 3, TWIERDZENIE jest konsekwencją następującego lematu.

LEMAT. Grupa A_5 nie posiada żadnej nietrywialnej podgrupy normalnej.

<u>Dowód LEMATU:</u>

(1) Do A_5 należą: id, oraz wszystkie
- cykle długości 5
- cykle długości 3
- pary rozłącznych transpozycji

Tak jest bo
- każda permutacja to kombinacja rozłącznych cykli
- cykle dł. parzystej są nieparzyste, i na odwrót.

(2) SPRZĘGANIE PERMUTACJI.

Jeśli $(a_1 \dots a_k)$ jest cyklem z S_n $(n \geq k)$ [czyli permutacją $a_1 \to a_2 \to a_3 \to \dots \to a_k \to a_1$]
zaś σ jest dowolną permutacją z S_n, to sprzężenie

$$\sigma \circ (a_1 \dots a_k) \circ \sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k))$$

jest cyklem tej samej długości

<u>D-d</u> pokażmy, że $\sigma(a_i)$ przechodzi na $\sigma(a_{i+1})$

$$\sigma(a_i) \xrightarrow{\sigma^{-1}} a_i \xrightarrow{(a_1 \dots a_k)} a_{i+1} \xrightarrow{\sigma} \sigma(a_{i+1});$$

jeśli natomiast $m \notin \{\sigma(a_1), \dots, \sigma(a_k)\}$, to

$$m \xrightarrow{\sigma^{-1}} \underbrace{\sigma^{-1}(m)}_{\notin \{a_1, \dots, a_k\}} \xrightarrow{(a_1 \dots a_k)} \sigma^{-1}(m) \xrightarrow{\sigma} m. \quad \square$$

(3) WNIOSEK: Jeśli $N \lhd A_5$ jest podgrupą normalną, oraz pewien 5-cykl należy do N, to wszystkie 5-cykle należą do N. Podobnie jest z 3-cyklami oraz z parami transpozycji.

4 Ilość poszczególnych rodzajów permutacji w A_5:

5-cykle	$5!/5 = 24$
3-cykle	$\binom{5}{3}\cdot 2 = 20$
pary transpozycji	$5 \cdot 3 = 15$
id	1
RAZEM	60

Zatem, z 3 wynika, że rząd podgrupy normalnej N jest sumą 1 (bo $id \in N$) oraz pewnych spośród liczb $15, 20, 24$

5 Niech $N \triangleleft A_5$.

Z Twierdzenia Lagrange'a, rząd N jest dzielnikiem rzędu A_5, czyli dzielnikiem 60.

Możliwości: $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$

Żadna z tych liczb, oprócz 1 i 60, nie jest sumą liczby 1 oraz pewnych spośród liczb $15, 20, 24$

Stąd jedyne podgrupy normalne w A_5 to

$\{1\}$ – rząd 1

A_5 – rząd 60. $\square$

WNIOSKI.

(1) S_5 oraz A_n i S_n dla $n \geq 5$ nie są rozwiązalne, (bo są nadgrupami nierozwiązalnej grupy A_5).

(2) Jeśli $f \in \mathbb{Q}[x]$ jest wielomianem stopnia 5 i jeśli jego grupa Galois to A_5 lub S_5, to nie wszystkie pierwiastki wielomianu f wyrażają się przez pierwiastniki.

Podobnie jest dla wyższych stopni, o ile grupa Galois $Gal(\mathbb{Q}_f/\mathbb{Q})$ zawiera A_5 jako podgrupę.

PRZYKŁAD

Grupa Galois wielomianu $f(x) = x^5 - 6x + 3$ to nierozwiązalna grupa S_5. Zatem pierwiastki tego wielomianu nie wyrażają się przez pierwiastniki.

Dowód w Maciej Bryński „Elementy teorii Galois" Biblioteczka Delty, Wydawnictwo „Alfa", 1985. Rozdział 22

JESZCZE JEDEN PRZYDATNY REZULTAT Z TEORII GRUP

Def. Niech G - grupa, $g \in G$ - element tej grupy.

Rzędem elementu g nazywamy najmniejsze $n \geq 1$ dla którego $g^n = e$. (Jeśli dla każdego $n \geq 1$ $g^n \neq e$, to mówimy, że g ma rząd nieskończony).

PRZYKŁADY. (0) Rząd e wynosi 1, i jest to jedyny element rzędu 1 w dowolnej grupie G.

(1) Rząd cyklu $(a_1 \ldots a_k)$ w dowolnej grupie permutacji wynosi k.

(2) Rząd elementu 1 w grupie $(\mathbb{Z}, +)$ wynosi ∞.

(3) Wiadomo (i łatwo to uzasadnić), że w skończonej grupie G rzędy wszystkich elementów $g \in G$ są skończone.

Lemat 2 (Cauchy). *Jeśli liczba pierwsza p jest dzielnikiem rzędu grupy G, to do grupy G należy element rzędu p.*

Dowód. Niech $n = \text{rz}\, G$, $p|n$, p jest liczbą pierwszą.
Rozważmy wszystkie ciągi $(g_1, g_2, \ldots, g_p)$ elementów grupy G, spełniające warunek $g_1 g_2 \ldots g_p = e$. Każdy taki ciąg jest wyznaczony jednoznacznie przez podanie elementów $g_1, g_2, \ldots$ $\ldots, g_{p-1}$, wobec tego liczba tych ciągów wynosi n^{p-1}, a więc jest podzielna przez p. W zbiorze tych ciągów wprowadzamy relację wiążącą dwa ciągi wtedy i tylko wtedy, gdy jeden z nich powstaje przez cykliczne przesunięcie elementów drugiego ciągu. Jest to relacja równoważności.
Oczywiście każda klasa tej relacji zawiera nie więcej niż p ciągów. Pokażemy, że każda klasa zawiera albo jeden, albo p ciągów. Przypuśćmy, że pewna klasa zawiera k ciągów dla $1 < k < p$, przy czym $g_1, g_2, \ldots, g_p$ jest jednym z nich. Obliczmy iloraz i resztę z dzielenia p przez $k; p = qk+r$ $(r < k)$. Rozważany ciąg przekształca się na siebie po k-krotnym przesunięciu cyklicznym wyrazów. Wobec tego

$$g_1 = g_{k+1} = g_{2k+1} = g_{qk+1} = g_{r+1}$$

i analogicznie $g_2 = g_{r+2}$ itd., stąd wynika, że po r-krotnym przesunięciu cyklicznym wyrazów ciągu $(g_1, g_2, \ldots, g_p)$ otrzymujemy ten sam ciąg, to zaś oznacza, że klasa równoważności tego ciągu zawiera nie więcej niż r wyrazów. Otrzymujemy sprzeczność, bo $r < k$. Zatem każda klasa zawiera albo p ciągów, albo jeden ciąg.

Ponieważ liczba wszystkich ciągów dzieli się przez p, więc liczba klas jednoelementowych też dzieli się przez p. Oczywiście ciąg należący do klasy jednoelementowej ma wszystkie wyrazy równe. Jednym z takich ciągów jest $(e, e, \ldots, e)$. Wobec tego istnieją jeszcze inne klasy jednoelementowe, czyli istnieją takie elementy $a \in G$, $a \neq e$, że $a^p = e$. Każdy taki element jest elementem rzędu p. ∎