

Andrzej Mostowski

ZARYS TEORII GALOIS

OZĘŚĆ I

GRUPA GALOIS

§ 1. Grupy podstawień. Pojęcie symetrii. Niech A oznacza dowolny zbiór.

Podstawieniem zbioru A nazywamy każdą funkcję φ , odwzorowującą zbiór A na samego siebie w sposób wzajemnie jednoznaczny.

Iloczynem dwu podstawień φ i ψ nazywamy podstawienie $\vartheta = \varphi\psi$, dane wzorem $\vartheta(x) = \varphi(\psi(x))$ ¹.

Jeśli zbiór G podstawień zbioru A jest grupą ze względu na tak określone pojęcie iloczynu (por. Rozdział XIX, § 1, str. 309, przykład 17), to mówimy, że G jest *grupą podstawień*.

Jednością 1 takiej grupy jest podstawienie *tożsamościowe*: $1(x) = x$ dla każdego elementu x zbioru A . Elementem odwrotnym do φ jest podstawienie φ^{-1} , odwrotne do φ .

Łość elementów zbioru A nazywamy *stopniem* grupy G .

Pojęcie grupy podstawień zjawia się wszędzie tam, gdzie jest mowa o niezmienniczości pewnych relacji.

Założmy, że w zbiorze A określone są pewne relacje między elementami: $R(x, y, z, \dots)$, $S(x, y, z, \dots)$, ...

Mówimy, że relacje te są *niezmiennicze*, albo *symetryczne*, ze względu na podstawienie φ , jeśli z zachodzenia ich między elementami $x, y, z, \dots$ wynika zawsze zachodzenie ich między elementami $\varphi(x), \varphi(y), \varphi(z), \dots$:

$$R(x, y, z, \dots) \rightarrow R(\varphi(x), \varphi(y), \varphi(z), \dots), \quad S(x, y, z, \dots) \rightarrow S(\varphi(x), \varphi(y), \varphi(z), \dots).$$

¹) Podstawienie to oznacza się też często przez $\psi\varphi$ (por. Rozdział XVIII, § 2, str. 301), aby zaznaczyć porządek, w jakim wykonywane są podstawienia. Symbolika taka nie jest jednak konsekwentna, jeśli podstawienia chcemy traktować jako funkcje. Najwłaściwszym wydaje się pisać: $\vartheta = \varphi\psi$, lecz czytać ten wzór: „ ϑ jest równe ψ razy φ “.

Każda relacja jest, oczywiście, symetryczna ze względu na podstawienie tożsamościowe. Łatwo dalej sprawdzić, że relacja symetryczna ze względu na podstawienie φ jest też symetryczna ze względu na podstawienie φ^{-1} , a relacja symetryczna ze względu na podstawienia φ i ψ jest też symetryczna ze względu na podstawienie $\varphi\psi$.

Utwórzmy zbiór G wszystkich podstawień φ , ze względu na które relacje $R, S, \dots$ są symetryczne. Zbiór G zawiera więc podstawienie tożsamościowe 1; jeśli φ i ψ należą do G , to φ^{-1} i $\varphi\psi$ też należą do G . Zbiór G tworzy więc grupę podstawień.

Nazywamy ją *grupą symetrii relacji* $R, S, \dots$

PRZYKŁADY. 1. Niech A oznacza zbiór punktów płaszczyzny lub przestrzeni. Dla dowolnej liczby rzeczywistej $\lambda \geq 0$ określmy relację $R_\lambda(x, y)$ przez warunek, że zachodzi ona między dwoma punktami x i y wtedy i tylko wtedy, gdy ich odległość równa się λ . Grupa symetrii wszystkich tych relacji R_λ (których ilość jest tu nieskończona, a nawet nieprzeliczalna) składa się z takich przekształceń¹⁾ płaszczyzny lub przestrzeni, które nie zmieniają odległości. Są to t. zw. *przekształcenia izometryczne*.

2. Niech F oznacza dowolny podzbiór zbioru A . Uzupełnijmy relację $R_\lambda(x, y)$ z przykładu 1 jeszcze jedną relacją: punkt x należy do zbioru F . Grupa symetrii składa się teraz nie ze wszystkich przekształceń izometrycznych, lecz tylko z tych spośród nich, które odwzorowują zbiór F w siebie. W szczególności, biorąc za F wielokąt lub wielościany foremne, otrzymujemy interesujące przykłady grup skończonych.

Przykład 2 ilustruje ważny fakt, że *zwiększenie ilości relacji powoduje redukcję (zmniejszenie) grupy symetrii*.

3. Niech p będzie liczbą pierwszą, zaś A zbiorem liczb $0, 1, 2, \dots, p-1$. Dla $\lambda = 0, 1, 2, \dots, p-1$ określmy relację $R_\lambda(x, y, z, t)$, przyjmując, że zachodzi ona między liczbami x, y, z, t zbioru A wtedy i tylko wtedy, gdy $x - y \equiv \lambda(z - t) \pmod{p}$.

Wykażemy, że grupa symetrii relacji $R_0, R_1, \dots, R_{p-1}$ składa się ze wszystkich podstawień π , dla których istnieją takie liczby a i b zbioru A , że

$$(1) \quad \pi(j) \equiv aj + b \pmod{p} \quad \text{dla } j = 0, 1, 2, \dots, p-1.$$

Istotnie, jeśli spełniony jest warunek (1) i między liczbami x, y, z, t zachodzi relacja R_λ , to

$$x - y \equiv \lambda(z - t) \pmod{p},$$

skąd wynika, że

$$a(x - y) \equiv \lambda a(z - t) \pmod{p},$$

t. j.

$$[(ax + b) - (ay + b)] \equiv \lambda[(az + b) - (at + b)] \pmod{p},$$

¹⁾ Podstawienia zbiorów nieskończonych nazywamy zazwyczaj *przekształceniami (transformacjami)* tych zbiorów.

czyli

$$\pi(x) - \pi(y) \equiv \lambda[\pi(z) - \pi(t)] \pmod{p},$$

co stwierdza, że relacja R_λ zachodzi między liczbami $\pi(x), \pi(y), \pi(z), \pi(t)$. Relacja R_λ jest więc symetryczna względem podstawienia π .

Załóżmy na odwrót, że relacje R_λ są symetryczne względem podstawienia π . Ponieważ wzór $R_\lambda(\lambda, 0, 1, 0)$ jest słuszny dla każdego λ należącego do A , więc otrzymujemy stąd wzór $R_\lambda(\pi(\lambda), \pi(0), \pi(1), \pi(0))$, t. j.

$$\pi(\lambda) - \pi(0) \equiv \lambda[\pi(1) - \pi(0)] \pmod{p},$$

co dowodzi, że podstawienie π spełnia warunek (1), przy czym $b = \pi(0)$, zaś a jest tą liczbą zbioru A , dla której $a \equiv \pi(1) - \pi(0) \pmod{p}$.

Podstawienia π , spełniające warunek (1), nazywamy *podstawieniami liniowymi*, a grupę ich — *pełną grupą liniową* (albo *metacykliczną*) stopnia p .

Zwróćmy jeszcze uwagę na to, że jeśli p nie jest liczbą pierwszą, to wzór (1) określa podstawienie zbioru A tylko dla takich a , które są względnie pierwsze z p .

Inne przykłady o treści algebraicznej podane są w Rozdziale XIX (§§ 18 i 19).

Niektóre pojęcia ogólne Teorii grup nabierają wyrazistszej treści w przypadku grup podstawień.

Powróćmy np. do przykładu 2 i rozważmy prócz zbioru F jeszcze drugi zbiór E , zawarty w A . Niech G oznacza grupę tych przekształceń izometrycznych, które przekształcają F w siebie, H zaś grupę tych φ należących do G , które ponadto przekształcają E w siebie. H jest więc podgrupą grupy G . Jeśli zastosujemy do E przekształcenia φ grupy G , to otrzymamy zbiory $\varphi(E)$, które pokrywają się z E tylko wtedy, gdy φ należy do grupy H .

Zbiory te nazywamy *sprzężonymi z E*.

Rozkład

$$(2) \quad G = \varphi_1 H + \varphi_2 H + \dots$$

(por. Rozdział XIX, § 10, wzór (16), str. 327) ma teraz następującą interpretację: dwa przekształcenia φ i ψ grupy G należą wtedy i tylko wtedy do tego samego składnika rozkładu (2), gdy przekształcają one E na ten sam zbiór sprzężony, t. j. gdy $\varphi(E) = \psi(E)$.

Składniki rozkładu (2) nazywamy *warstwami lewostronnymi* grupy G względem H , a ilość warstw nazywa się *wskaźnikiem grupy H w G*.

Grupa $\varphi H \varphi^{-1}$ sprzężona z H (por. Rozdział XIX, § 9, str. 326) ma interpretację następującą: jest to grupa tych przekształceń ψ należących do G , które przekształcają $\varphi(E)$ w siebie. Jeśli wszystkie grupy sprzężone z H są równe H , to H jest dzielnikiem normalnym.

Analogiczne uwagi stosują się nie tylko do specjalnego przypadku, omawianego w przykładzie 2, ale i do ogólnego pojęcia grupy symetrii relacji $R, S, \dots$. Należy tylko zamiast zbiorów sprzężonych rozważać relacje $R_\varphi, S_\varphi, \dots$ sprzężone z $R, S, \dots$ i określone równoważnością $R_\varphi(x, y, z, \dots) = R(\varphi(x), \varphi(y), \varphi(z), \dots)$ ¹⁾.

ĆWICZENIE. Zbadaj grupy powstające w sposób opisany w przykładzie 2, gdy:

- (a) A jest płaszczyzną, zaś F trójkątem równobocznym;
- (b) A jest przestrzenią, zaś F czworoscianem foremnym;
- (c) A jest przestrzenią, zaś F sześcianiem.

Wykazać, że w przypadku (a) otrzymuje się grupę izomorficzną z grupą symetryczną stopnia 3 (t. j. grupą wszystkich podstawień trzech przedmiotów), w przypadku (b) grupę izomorficzną z grupą naprzemienną stopnia 4, zaś w przypadku (c) grupę izomorficzną z grupą symetryczną stopnia 4.

§ 2. Grupa Galois²⁾. Będziemy oznaczali przez K dowolne, lecz obrane raz na zawsze ciało liczbowe. Rozpatrywać będziemy wielomian $f(x)$ stopnia n o współczynnikach należących do ciała K , nie posiadający pierwiastków wielokrotnych (por. Rozdział VIII, § 10, str. 122). Przez $x_1, x_2, \dots, x_n$ oznaczać będziemy stale pierwiastki wielomianu $f(x)$.

Będziemy mówili, że między pierwiastkami $x_1, x_2, \dots, x_n$ zachodzi relacja wymierna w K , jeżeli istnieje wielomian $W(\xi_1, \xi_2, \dots, \xi_n)$ n zmiennych $\xi_1, \xi_2, \dots, \xi_n$ o współczynnikach należących do K , taki że $W(x_1, x_2, \dots, x_n) = 0$.

¹⁾ Czytelnik, którego interesują zagadnienia, poruszone w § 1, znajdzie wiele ciekawego materiału w książce A. Speiser, *Theorie der Gruppen von endlicher Ordnung*, Wyd. 2-e, Berlin 1927, Rozdziały VI i VII.

²⁾ Pojęcie to wprowadził do algebry Évariste Galois (1811-1832). Mimo, iż Galois żył zaledwie 21 lat i napisał tylko kilka prac (zbiorowe wydanie jego dzieł obejmuje zaledwie 61 stron), twórczość jego wywarła głęboki wpływ na rozwój wielu dziedzin matematyki. W szczególności stworzone przez Galois pojęcie grupy okazało się podstawowym pojęciem w różnych gałęziach wiedzy.

Sama postać Galois jest równie niezwykła jak jego teoria. Jego namiętny i gwałtowny charakter powodował, że pozostawał on stale w niezgodzie z współczesnymi sobie przedstawicielami nauki, którymi pogardzał, gdyż nie rozumieli jego koncepcyj. Szkodziło mu to też w nauce szkolnej i akademickiej: dwukrotnie przepadał przy egzaminach. Brał czynny udział w życiu politycznym, krytykując ostro rządy Ludwika Filipa, co ściągnęło na niego karę więzienia. Zginął w pojedynku, którego powody nie są znane. W przeddzień śmierci napisał obszerny list do swego przyjaciela, komunikując mu o swych najważniejszych odkryciach matematycznych. List ten jest jednym z głównych źródeł naszych wiadomości o twórczości Galois. Por. *Oeuvres d'Évariste Galois*, Paryż 1897, z przedmową E. Picarda oraz pracę P. Dupuy, *La vie d'Évariste Galois*, Annales de l'École Normale Supérieure, Tom 13 (1896).

Grupę podstawień zbioru $\{x_1, x_2, \dots, x_n\}$, względem których wszystkie relacje wymierne w K są niezmiennicze, nazywamy grupą Galois równania $f(x) = 0$ w ciele K .

Pojęcie to jest więc szczególnym przypadkiem omawianych w § 1 grup symetrii.

Grupę Galois równania $f(x) = 0$ w ciele K oznaczać będziemy w dalszym ciągu stale przez G .

Z definicji wynika, że G jest zespołem podstawień

$$\pi = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \pi(x_1) & \pi(x_2) & \dots & \pi(x_n) \end{pmatrix}$$

o następującej własności: jeśli $W(\xi_1, \xi_2, \dots, \xi_n)$ jest wielomianem n zmiennych o współczynnikach należących do K i jeśli

$$W(x_1, x_2, \dots, x_n) = 0,$$

to

$$W(\pi(x_1), \pi(x_2), \dots, \pi(x_n)) = 0.$$

Zadanie, jakie stawia sobie Teoria Galois, polega na zbadaniu własności równania $f(x) = 0$ na podstawie własności przyporządkowanej mu grupy Galois. W geometrii odpowiadałoby to badaniu własności figur na podstawie ich symetrii.

Pojęcie grupy Galois można uogólnić na przypadek dowolnego ciała K , niekoniecznie utworzonego z liczb. Główna trudność, na jaką napotykamy, pragnąc sformułować definicję, polega na określeniu pierwiastków wielomianu $f(x)$ i na dowodzie ich istnienia; rzecz bowiem jasna, że nie możemy się powoływać na zasadnicze twierdzenie algebry, jeśli współczynniki równania $f(x) = 0$ nie są liczbami. Problemy te należą do t. zw. Algebry abstrakcyjnej¹⁾.

PRZYKŁAD. Wyznamy grupę Galois równania $x^4 + x^3 + x^2 + x + 1 = 0$ w ciele $\mathcal{R}$ liczb wymiernych. Pierwiastkami tego równania są liczby $x_k = e^{2\pi i k/5}$, gdzie $k = 1, 2, 3, 4$. Między liczbami tymi zachodzą następujące zależności wymierne w $\mathcal{R}$:

$$(3) \quad x_1^2 - x_2 = 0, \quad x_2^2 - x_4 = 0, \quad x_4^2 - x_3 = 0.$$

Ponieważ $x_2^2 - x_3 \neq 0$, więc wynika stąd np., że podstawienie

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_1 \end{pmatrix} = (x_1, x_2, x_3, x_4)$$

¹⁾ Wykład Teorii Galois w ramach Algebry abstrakcyjnej znaleźć można w pięknej książce: B. L. van der Waerden, *Moderne Algebra*, Wyd. 2-e, Tom 1, Berlin 1937. Por. też H. Hasse, *Höhere Algebra*, Tom 2, Sammlung Göschel, 1927 oraz Rozdział XX niniejszej książki, § 2, przykłady 8 i 9 (str. 354-359). Zob. też A. A. Albert, *Modern higher algebra*, The University of Chicago, Science Series, Wyd. 4-e (1944).

nie należy do grupy Galois rozważanego równania. W podobny sposób wykazemy, że spośród 24 podstawień liczb x_1, x_2, x_3, x_4 tylko podstawienia

$$(4) \quad 1, \quad (x_1, x_2, x_4, x_3), \quad (x_1, x_4)(x_2, x_3), \quad (x_1, x_3, x_4, x_2)$$

mogą należeć do grupy Galois. Relacje (3) są, istotnie, symetryczne ze względu na podstawienia (4); nie możemy stąd jednak jeszcze wnosić, że podstawienia te tworzą grupę Galois, gdyż nie wiemy, czy każda relacja wymierna w $\mathcal{R}$, zachodząca między liczbami x_1, x_2, x_3, x_4 , jest też symetryczna ze względu na podstawienia (4). Następujące rozumowanie wykazuje, że tak jest istotnie.

Dla dowolnego wielomianu $W(\xi, \eta, \zeta, \tau)$ czterech zmiennych przyjmijmy $V(\xi) = W(\xi, \xi^2, \xi^3, \xi^4)$. Jeśli $W(x_1, x_2, x_3, x_4) = 0$, to $V(x_1) = 0$, gdyż $x_2 = x_1^2$, $x_3 = x_1^3$ i $x_4 = x_1^4$. Wielomiany $V(x)$ i $\varphi(x) = x^4 + x^3 + x^2 + x + 1$ mają więc wspólny pierwiastek x_1 , a że $\varphi(x)$ jest wielomianem nieprzywiedlnym w $\mathcal{R}$ (por. Rozdział VIII, § 14, wniosek 2, str. 134), więc $V(x)$ jest podzielne przez $\varphi(x)$ (por. Rozdział XIII, § 3, str. 228). Wynika stąd, że $V(x_2) = 0$, co wobec $x_2^2 = x_4$, $x_2^3 = x_1$ i $x_2^4 = x_3$ daje równość $W(x_2, x_4, x_1, x_3) = 0$. Podstawienie (x_1, x_2, x_4, x_3) należy więc do grupy Galois równania $\varphi(x) = 0$ w ciele $\mathcal{R}$. Potęgi tego podstawienia muszą zatem też należeć do tej grupy, co dowodzi, iż składa się ona z podstawień (4).

Możność wyznaczenia grupy Galois w tym przykładzie zawdzięczamy faktowi, że wszystkie pierwiastki są potęgą jednego z nich. W ogólnym przypadku definicja grupy Galois nie daje żadnego sposobu rozstrzygnięcia w skończonej liczbie kroków, czy dane podstawienie należy do G , czy nie. W § 6 poznamy taki sposób dla przypadku, gdy K jest ciałem $\mathcal{R}$ liczb wymiernych (ob. str. 387).

ĆWICZENIA. 1. Wyznaczyć grupę Galois równania

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

w ciele $\mathcal{R}$ liczb wymiernych.

2. Jeśli K jest podciałem ciała A , to grupa Galois równania $f(x) = 0$ w ciele A jest podgrupą grupy G .

[Każda relacja wymierna w A jest też wymierna w K].

§ 3. Grupy symetrii funkcji wymiernych pierwiastków równania. Oznaczać będziemy przez $\Sigma = K(x_1, x_2, \dots, x_n)$ ciało, powstające z K przez dołączenie liczb $x_1, x_2, \dots, x_n$ (por. Rozdział XIII, § 2, str. 226). Ciało Σ składa się więc z liczb, dających się przedstawić w postaci ułamka

$$(5) \quad \Theta = \frac{P(x_1, x_2, \dots, x_n)}{Q(x_1, x_2, \dots, x_n)},$$

gdzie P i Q są symbolami wielomianów n zmiennych o współczynnikach należących do ciała K , przy czym $Q(x_1, x_2, \dots, x_n) \neq 0$.

Dla krótkości oznaczać będziemy zespół liczb $x_1, x_2, \dots, x_n$ jedną literą x .

Jeśli π jest dowolnym podstawieniem liczb $x_1, x_2, \dots, x_n$, to zespół liczb $\pi(x_1), \pi(x_2), \dots, \pi(x_n)$ oznaczać będziemy symbolem $\pi(x)$.

Wzór (5) zapiszemy więc krótko jako $\Theta = \frac{P(x)}{Q(x)}$.

Zespół wszystkich podstawień grupy G , względem których relacja (5) jest symetryczna, tworzy podgrupę G . Jest to mianowicie grupa symetrii relacji wymiernych w K i relacji (5).

Grupę tę nazywać będziemy *grupą symetrii liczby Θ* i oznaczać przez H_Θ .

Na to więc, aby podstawienie π grupy G należało do H_Θ , potrzeba i wystarcza, by zachodziła równość

$$(6) \quad \Theta = \frac{P(\pi(x))}{Q(\pi(x))}.$$

Należy tu zauważyć, że $Q(\pi(x)) \neq 0$ dla każdego podstawienia π , należącego do grupy G . Istotnie, związek $Q(\pi(x)) = 0$ przedstawia pewną zależność wymierną w K , zachodzącą między pierwiastkami $x_1, x_2, \dots, x_n$ ($\pi(x)$ jest pewną permutacją ciągu x). Z definicji grupy G wnosimy więc, że jeśli $Q(\pi(x)) = 0$, to $Q(\pi^{-1}(\pi(x))) = 0$, t. j. $Q(x) = 0$, wbrew założeniu.

Grupa H_Θ pozornie zależy od sposobu, w jaki liczba Θ została przedstawiona w postaci (5). Łatwo jednak pokazać, że H_Θ w rzeczywistości zależy tylko od liczby Θ . Udowodnimy mianowicie, że jeśli P_1 i Q_1 są takimi wielomianami n zmiennych o współczynnikach należących do K , że

$$(7) \quad \Theta = \frac{P_1(x)}{Q_1(x)},$$

to dla każdego podstawienia π grupy G warunek

$$(8) \quad \Theta = \frac{P_1(\pi(x))}{Q_1(\pi(x))}$$

jest równoważny z (6).

Istotnie, między $x_1, x_2, \dots, x_n$ zachodzi na mocy (5) i (7) zależność wymierna w K

$$P(x) \cdot Q_1(x) - P_1(x) \cdot Q(x) = 0,$$

skąd wynika, że dla każdego podstawienia π , należącego do grupy G , zachodzi równość $P(\pi(x)) \cdot Q_1(\pi(x)) - P_1(\pi(x)) \cdot Q(\pi(x)) = 0$. Wobec $Q(\pi(x)) \neq 0 \neq Q_1(\pi(x))$ otrzymujemy stąd

$$(9) \quad \frac{P(\pi(x))}{Q(\pi(x))} = \frac{P_1(\pi(x))}{Q_1(\pi(x))},$$

skąd od razu wynika równoważność warunków (6) i (8). Otrzymamy więc tę samą grupę H_Θ , wychodząc z przedstawienia (5) liczby Θ , co wychodząc z przedstawienia (7).

Jeśli podstawienie π grupy G nie należy do H_Θ , to liczba $\frac{P(\pi(x))}{Q(\pi(x))}$ jest różna od Θ .

Nazywamy ją *liczbą sprzężoną z Θ* i oznaczamy przez $\pi(\Theta)$. Samo Θ zaliczamy też do liczb sprzężonych z Θ .

Wzór (9) dowodzi, że $\pi(\Theta)$ zależy tylko od Θ i od π , nie zależy zaś od sposobu, w jaki Θ zostało przedstawione w postaci (5).

Z definicji liczb sprzężonych wynikają łatwo następujące twierdzenia:

Twierdzenie 1. Jeśli π jest podstawieniem, należącym do grupy G , a liczby Θ i Z należą do ciała Σ , to

$$\pi(\Theta + Z) = \pi(\Theta) + \pi(Z), \quad \pi(\Theta - Z) = \pi(\Theta) - \pi(Z) \quad \text{i} \quad \pi(\Theta \cdot Z) = \pi(\Theta) \cdot \pi(Z).$$

Jeśli przy tym $Z \neq 0$, to

$$\pi(Z) \neq 0 \quad \text{i} \quad \pi(\Theta : Z) = \pi(\Theta) : \pi(Z).$$

Dowód. Załóżmy, że $\Theta = \frac{P(x)}{Q(x)}$ i $Z = \frac{R(x)}{S(x)}$, gdzie P, Q, R i S są symbolami wielomianów n zmiennych o współczynnikach należących do K , przy czym $Q(x) \neq 0$ i $S(x) \neq 0$. Otrzymujemy stąd

$$\Theta \pm Z = \frac{P(x) \cdot S(x) \pm Q(x) \cdot R(x)}{Q(x) \cdot S(x)}, \quad \Theta \cdot Z = \frac{P(x) \cdot R(x)}{Q(x) \cdot S(x)}.$$

Stosując definicję liczb sprzężonych, wnosimy z tych równości, że

$$\begin{aligned} \pi(\Theta \pm Z) &= \frac{P(\pi(x)) \cdot S(\pi(x)) \pm Q(\pi(x)) \cdot R(\pi(x))}{Q(\pi(x)) \cdot S(\pi(x))} = \\ &= \frac{P(\pi(x))}{Q(\pi(x))} \pm \frac{R(\pi(x))}{S(\pi(x))} = \pi(\Theta) \pm \pi(Z) \end{aligned}$$

i podobnie

$$\pi(\Theta \cdot Z) = \frac{P(\pi(x)) \cdot R(\pi(x))}{Q(\pi(x)) \cdot S(\pi(x))} = \frac{P(\pi(x))}{Q(\pi(x))} \cdot \frac{R(\pi(x))}{S(\pi(x))} = \pi(\Theta) \cdot \pi(Z).$$

Jeśli $Z \neq 0$, to — jak wiemy — $\pi(Z) \neq 0$, a zatem

$$\pi(\Theta : Z) = \pi\left(\frac{P(x) \cdot S(x)}{Q(x) \cdot R(x)}\right) = \frac{P(\pi(x))}{Q(\pi(x))} \cdot \frac{S(\pi(x))}{R(\pi(x))} = \pi(\Theta) : \pi(Z).$$

Twierdzenie 1 jest w ten sposób udowodnione całkowicie.

Twierdzenie 2. Jeśli Θ należy do ciała K , to dla każdego podstawienia π , należącego do grupy G , zachodzi wzór $\pi(\Theta) = \Theta$.

Istotnie, we wzorze (5) możemy obrać za P wielomian stopnia 0 równy stałe Θ , a za Q — wielomian stopnia 0 równy stałe 1. Wzór $\pi(\Theta) = \Theta$ jest wtedy oczywisty.

Z twierdzeń 1 i 2 wynika przez indukcję

Twierdzenie 3. Jeśli W jest wielomianem k zmiennych o współczynnikach należących do ciała K , zaś liczby $\Theta_1, \Theta_2, \dots, \Theta_k$ należą do ciała Σ , to dla każdego podstawienia π , należącego do grupy G , zachodzi równość

$$\pi(W(\Theta_1, \Theta_2, \dots, \Theta_k)) = W(\pi(\Theta_1), \pi(\Theta_2), \dots, \pi(\Theta_k)).$$

Twierdzenie 4. Jeśli podstawienia π i σ należą do grupy G , a Θ jest liczbą należącą do ciała Σ , to

$$\pi(\sigma(\Theta)) = \pi\sigma(\Theta).$$

Dowód. Z (5) otrzymujemy wobec wzoru $\pi\sigma(x) = \pi(\sigma(x))$

$$\pi\sigma(\Theta) = \frac{P(\pi\sigma(x))}{Q(\pi\sigma(x))} = \pi\left(\frac{P(\sigma(x))}{Q(\sigma(x))}\right) = \pi\left(\sigma\left(\frac{P(x)}{Q(x)}\right)\right) = \pi(\sigma(\Theta)).$$

Jeśli F jest funkcją odwzorowującą ciało Σ samo w siebie wzajemnie jednoznacznie (czyli podstawieniem ciała Σ) i jeśli spełnione są wzory

$$F(\Theta + Z) = F(\Theta) + F(Z), \quad F(\Theta \cdot Z) = F(\Theta) \cdot F(Z),$$

to mówimy, że F jest *automorfizmem ciała Σ* .

Twierdzenia 1 i 2 stwierdzają, że jeśli π należy do grupy G , to funkcja $F(\Theta) = \pi(\Theta)$ jest automorfizmem ciała Σ , który każdy element ciała K przekształca sam w siebie. Można wykazać, że dla każdego automorfizmu F ciała Σ , który każdy element ciała K przekształca sam w siebie, istnieje w grupie G takie podstawienie π , że $F(\Theta) = \pi(\Theta)$. Wynika stąd, że grupę Galois można zdefiniować przy pomocy pojęcia automorfizmu.

ĆWICZENIA. 1. Grupą symetrii liczby $\pi(\Theta)$ jest $\pi H_\Theta \pi^{-1}$.

2. Jeśli między liczbami $\Theta_1, \Theta_2, \dots, \Theta_k$ ciała Σ zachodzi zależność $W(\Theta_1, \Theta_2, \dots, \Theta_k) = 0$ wymierna w K , to dla każdego podstawienia π grupy G zachodzi wzór $W(\pi(\Theta_1), \pi(\Theta_2), \dots, \pi(\Theta_k)) = 0$.

Wskazówka: powołać się na twierdzenia 3 i 2.

3. Jeśli F jest automorfizmem ciała Σ , który każdy element ciała K przekształca sam w siebie, i Θ jest pierwiastkiem równania $g(x) = 0$ o współczynnikach należących do K , to $F(\Theta)$ jest też pierwiastkiem tego równania.

§ 4. Istnienie liczb o danej grupie symetrii. W § 3 pokazaliśmy, że każdej liczbie θ ciała Σ odpowiada pewna podgrupa H_θ grupy G . Narzuca się teraz pytanie, czy dla każdej grupy H zawartej w G istnieje liczba θ ciała Σ taka, że $H_\theta = H$. Obecnie odpowiemy na to pytanie i udowodnimy jednocześnie pewne ogólniejsze twierdzenia, z których skorzystamy później.

Lemat 1. *Jeśli $W(\xi_1, \xi_2, \dots, \xi_k)$ jest różnym od 0 wielomianem k zmiennych o współczynnikach należących do ciała Σ , to istnieją takie liczby naturalne $m_1, m_2, \dots, m_k$, że $W(m_1, m_2, \dots, m_k) \neq 0$.*

Dowód. Dla $k=0$ twierdzenie jest oczywiste. Założmy jego słuszność dla pewnego k i rozważmy wielomian $W(\xi_1, \xi_2, \dots, \xi_{k+1})$ $k+1$ zmiennych, nie równy tożsamościowo zeru. Porządkując ten wielomian względem potęg zmiennej ξ_{k+1} , przedstawimy go w postaci

$$W_0(\xi_1, \xi_2, \dots, \xi_k) \cdot \xi_{k+1}^l + W_1(\xi_1, \xi_2, \dots, \xi_k) \cdot \xi_{k+1}^{l-1} + \dots + W_l(\xi_1, \xi_2, \dots, \xi_k),$$

przy czym co najmniej jeden z wielomianów $W_0, W_1, \dots, W_l$, np. wielomian W_j , nie jest tożsamościowo zerem. W myśl założenia istnieją takie $m_1, m_2, \dots, m_k$, że $W_j(m_1, m_2, \dots, m_k) \neq 0$. Za m_{k+1} wystarcza teraz wziąć dowolną liczbę różną od pierwiastków równania

$$W_0(m_1, m_2, \dots, m_k) \cdot t^l + W_1(m_1, m_2, \dots, m_k) \cdot t^{l-1} + \dots + W_l(m_1, m_2, \dots, m_k) = 0.$$

Z lematu 1 wynika łatwo

Lemat 2. *Jeśli wielomiany $W_j(\xi_1, \xi_2, \dots, \xi_{k_j})$ o k_j zmiennych ($j=1, 2, \dots, p$) i o współczynnikach, należących do ciała Σ , nie znikają tożsamościowo, to istnieją takie liczby naturalne $m_1, m_2, \dots, m_k$ ($j=1, 2, \dots, p$), że $W_j(m_1, m_2, \dots, m_{k_j}) \neq 0$ dla $j=1, 2, \dots, p$.*

Dla dowodu wystarczy zastosować lemat 1 do iloczynu $W_1 W_2 \dots W_p$.

Twierdzenie 5. *Istnieje taki wielomian n zmiennych o współczynnikach naturalnych $W(\xi_1, \xi_2, \dots, \xi_n)$, że dla dowolnych dwu podstawień π i σ równość*

$$(10) \quad W(\pi(x)) = W(\sigma(x))$$

zachodzi wtedy i tylko wtedy, gdy $\pi = \sigma$.

Liczba $\theta = W(x)$ należy do ciała Σ i jej grupa symetrii zawiera tylko podstawienie tożsamościowe.

Dowód. Rozważmy $\frac{n!}{2}(n!-1)$ wielomianów pierwszego stopnia zmiennych $\xi_1, \xi_2, \dots, \xi_n$

$$\sum_{j=1}^n \xi_j [\pi(x_j) - \sigma(x_j)],$$

gdzie π i σ oznaczają dwa jakiegokolwiek różne podstawienia liczb $x_1, x_2, \dots, x_n$. Zgodnie z lematem 2 istnieją takie liczby naturalne $m_1, m_2, \dots, m_n$, że $\sum_{j=1}^n m_j [\pi(x_j) - \sigma(x_j)] \neq 0$ dla każdego dwu różnych podstawień π i σ . Wielomian $W(\xi_1, \xi_2, \dots, \xi_n) = \sum_{j=1}^n m_j \xi_j$ spełnia żądany warunek. Istotnie, jeśli π i σ oznaczają dwa różne podstawienia, to

$$W(\pi(x)) = \sum_{j=1}^n m_j \pi(x_j) \quad \text{ i } \quad W(\sigma(x)) = \sum_{j=1}^n m_j \sigma(x_j),$$

a więc równość (10) nie zachodzi.

Liczba $\theta = W(x)$ należy oczywiście do ciała Σ . Jeśli podstawienie π należy do grupy G , to równość $\pi(\theta) = \theta$ znaczy to samo, co $W(\pi(x)) = W(x)$, a więc spełniona jest tylko dla $\pi = 1$.

Twierdzenie 5 jest w ten sposób udowodnione całkowicie.

Liczbę θ ciała Σ , dla której H_θ jest grupą jednostkową, nazywamy liczbą pierwotną ciała Σ .

Twierdzenie 5 orzeka zatem, że istnieją liczby pierwotne. Problem postawiony na początku § jest więc rozwiązany dla przypadku, gdy H_θ jest grupą jednostkową.

Udowodnimy teraz następujące uogólnienie twierdzenia 5:

Twierdzenie 6. *Dla każdej grupy H podstawień liczb $x_1, x_2, \dots, x_n$ istnieje taki wielomian $V(\xi_1, \xi_2, \dots, \xi_n)$ o współczynnikach całkowitych, że równość $V(\pi(x)) = V(\sigma(x))$ zachodzi dla dwu podstawień π i σ wtedy i tylko wtedy, gdy $\pi^{-1}\sigma$ należy do grupy H .*

Dowód. Oznaczmy przez S_n grupę wszystkich podstawień liczb $x_1, x_2, \dots, x_n$ i niech

$$S_n = \pi_1 H + \pi_2 H + \dots + \pi_k H$$

oznacza rozkład S_n na warstwy lewostronne względem H (p. § 1, str. 373). Możemy założyć, że π_1 jest permutacją tożsamościową.

Będziemy oznaczali podstawienia liczb $x_1, x_2, \dots, x_n$ tymi samymi literami co podstawienia zmiennych $\xi_1, \xi_2, \dots, \xi_n$. Jeśli więc $\tau = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{k_1} & x_{k_2} & \dots & x_{k_n} \end{pmatrix}$, to przyjmiemy $\tau(\xi_j) = \xi_{k_j}$. Zespół zmiennych

$\xi_1, \xi_2, \dots, \xi_n$ oznaczmy jedną literą $\mathfrak{X}$, zespół zaś zmiennych $\tau(\xi_1), \tau(\xi_2), \dots, \tau(\xi_n)$ symbolem $\tau(\mathfrak{X})$.

Niech $W(\mathfrak{X})$ będzie wielomianem, czyniącym zadość warunkom twierdzenia 5. Przyjmijmy dla $j=1, 2, \dots, k$

$$Q_j(t; \mathfrak{X}) = \prod_{\sigma \in H} [t - W(\pi_j \sigma(\mathfrak{X}))],$$

gdzie symbol $\prod_{\sigma \in H}$ oznacza iloczyn, rozciągnięty na wszystkie permutacje σ , należące do grupy H .

Wielomiany (jednej zmiennej t)

$$Q_j(t; \mathfrak{x}) = \prod_{\sigma \in H} [t - W(\pi_j \sigma(\mathfrak{x}))]$$

są różne między sobą. Istotnie, gdyby wielomiany $Q_j(t; \mathfrak{x})$ i $Q_l(t; \mathfrak{x})$ były identyczne, to $W(\pi_j(\mathfrak{x}))$ byłoby pierwiastkiem wielomianu $Q_l(t; \mathfrak{x})$, a więc istniałoby podstawienie σ , należące do grupy H i takie, że $W(\pi_j(\mathfrak{x})) = W(\pi_l \sigma(\mathfrak{x}))$. Ponieważ wielomian W spełnia twierdzenie 5, więc wynikałoby stąd, że $\pi_j = \pi_l \sigma$, co dla $j \neq l$ jest niemożliwe.

Wielomiany $Q_j(t; \mathfrak{x})$ są więc istotnie różne między sobą. Stosując lemat 2, wnosimy stąd z łatwością, że istnieje liczba naturalna m , dla której liczby

$$Q_1(m; \mathfrak{x}), Q_2(m; \mathfrak{x}), \dots, Q_k(m; \mathfrak{x})$$

są wszystkie różne.

Wykażemy teraz, że wielomian $V(\mathfrak{X}) = Q_1(m; \mathfrak{X})$ posiada żądane własności.

Przede wszystkim współczynniki tego wielomianu są liczbami całkowitymi, gdyż jest on iloczynem skończonej liczby wielomianów o współczynnikach całkowitych.

Żałóżmy, że π jest podstawieniem, należącym do grupy S_n ; istnieje więc liczba $j \leq k$ taka, że π należy do warstwy $\pi_j H$, a zatem $\pi = \pi_j \tau$, gdzie τ należy do H . Otrzymujemy stąd

$$V(\pi(\mathfrak{x})) = \prod_{\sigma \in H} [m - W(\pi_j \tau \sigma(\mathfrak{x}))].$$

Jeśli σ przebiega podstawienia grupy H , to $\tau \sigma$ też przebiega wszystkie te podstawienia, tylko w zmienionym porządku, co dowodzi, że

$$V(\pi(\mathfrak{x})) = \prod_{\sigma \in H} [m - W(\pi_j \sigma(\mathfrak{x}))] = Q_j(m; \mathfrak{x}).$$

Jeśli σ należy do warstwy $\pi_l H$, to wyprowadzimy podobnie

$$V(\sigma(\mathfrak{x})) = Q_l(m; \mathfrak{x}).$$

Równość $V(\pi(\mathfrak{x})) = V(\sigma(\mathfrak{x}))$ zachodzi więc wtedy i tylko wtedy, gdy $j=l$, t. j. gdy π i σ należą do tej samej warstwy $\pi_j H$. Jeśli warunek ten jest spełniony, to $\pi = \pi_j \tau$ i $\sigma = \pi_j \rho$, gdzie τ i ρ oznaczają podstawienia, należące do H , a więc

$$\pi^{-1} \sigma = \tau^{-1} \pi_j^{-1} \pi_j \rho = \tau^{-1} \rho,$$

co dowodzi, że $\pi^{-1} \sigma$ należy do H . Na odwrót, jeśli $\pi^{-1} \sigma$ należy do H i $\pi = \pi_j \tau$, gdzie τ oznacza podstawienie grupy H , to

$$\sigma = \pi \pi^{-1} \sigma = \pi_j \tau (\pi^{-1} \sigma),$$

co dowodzi, że σ należy do warstwy $\pi_j H$, gdyż $\tau(\pi^{-1} \sigma)$ należy do H . Podstawienia π i σ należą więc do tej samej warstwy wtedy i tylko wtedy, gdy $\pi^{-1} \sigma$ należy do H , co dowodzi, że równość $V(\pi(\mathfrak{x})) = V(\sigma(\mathfrak{x}))$ zachodzi wtedy i tylko wtedy, gdy $\pi^{-1} \sigma$ należy do H , c. b. d. o.

Z twierdzenia 6 łatwo już wysnujemy odpowiedź na pytanie, postawione na początku §:

Twierdzenie 7. Dla każdej grupy H zawartej w G istnieje liczba Θ ciała Σ , której grupą symetrii jest H .

Dowód. Niech $V(\xi_1, \xi_2, \dots, \xi_n)$ oznacza wielomian spełniający warunki twierdzenia 6. Przyjmijmy $\Theta = V(\mathfrak{x})$. Liczba ta należy oczywiście do ciała Σ . Warunek $\pi(\Theta) = \Theta$ orzeka to samo, co $V(\pi(\mathfrak{x})) = V(\mathfrak{x})$, a więc zachodzi wtedy i tylko wtedy, gdy π należy do grupy H , c. b. d. o.

Należy dobrze zdać sobie sprawę z tego, że nie miałoby sensu mówić o liczbach, których grupa symetrii nie jest zawarta w G . Jeśli bowiem π nie należy do G , to $\pi(\Theta)$ zależy nie tylko od Θ , ale i od sposobu, w jaki Θ jest przedstawione jako funkcja wymierna pierwiastków (por. dalej ćwiczenie 4).

Zauważmy jeszcze, że liczba Θ o grupie symetrii H może nieraz być konstruowana na prostszej drodze niż na podstawie twierdzenia 7. W szczególności może się nieraz okazać, że niektóre współczynniki wielomianu $Q_1(t; \mathfrak{X})$, którego używaliśmy w dowodzie twierdzenia 6, dają takie liczby Θ .

ĆWICZENIA. 1. Rozważyć ciało Σ dla równania $x^4 + x^3 + x^2 + x + 1 = 0$ i ciała $\mathcal{R}$ liczb wymiernych; wskazać liczbę pierwotną tego ciała oraz liczby należące do różnych podgrup grupy Galois (por. § 2, przykład).

[Ta grupa G ma 3 podgrupy: grupę jednostkową, grupę $\{1, (x_1, x_4)(x_2, x_3)\}$ i G . Odpowiadającymi im liczbami są np. $x_1 = e^{\frac{2\pi i}{5}}$, $x_1 + x_4 = e^{\frac{2\pi i}{5}} + e^{-\frac{2\pi i}{5}} = 2 \cos \frac{2\pi}{5}$ i 1].

2. To samo zadanie rozwiązać dla równania $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$ w ciele $\mathcal{R}$ liczb wymiernych.

3. Jeśli wielomian $Q_1(t; x)$ napisać w postaci $t^k + \theta_1 t^{k-1} + \theta_2 t^{k-2} + \dots + \theta_k$, to grupy symetrii liczb $\theta_1, \theta_2, \dots, \theta_k$ zawierają H .

4. Zachowując oznaczenia, wprowadzone w przykładzie z § 2, wykazać, że jeśli $\pi = (x_1, x_2, x_3, x_4)$, to $\pi(x_1^2) \neq \pi\left(\frac{1}{x_1 \cdot x_2 \cdot x_3}\right)$, mimo że $x_1^2 = \frac{1}{x_1 \cdot x_2 \cdot x_3}$.

§ 5. Uogólnienie twierdzenia o funkcjach symetrycznych. Zbadamy obecnie, które liczby ciała Σ mają jako grupę symetrii całą grupę G . W tym celu udowodnimy najpierw

Lemat 3. Jeśli wielomian W spełnia warunki twierdzenia 5 i $Z = W(x)$, to dla każdej liczby Θ ciała Σ istnieje taki wielomian $U(\xi)$ jednej zmiennej o współczynnikach należących do ciała K , że $\Theta = U(Z)$.

Dowód. Liczbę Θ przedstawiamy jakkolwiek w postaci (5) i określamy $\pi(\Theta)$ jako $P(\pi(x)):Q(\pi(x))$ bez względu na to, czy podstawienie π należy, czy nie należy do G . Przyjmujemy dalej:

$$R(t) = \prod_{\pi} [t - W(\pi(x))], \quad S(t) = \sum_{\pi} \frac{\pi(\Theta)}{t - W(\pi(x))},$$

gdzie iloczyn i suma rozciągają się na wszystkie podstawienia π pierwiastków $x_1, x_2, \dots, x_n$. $R(t)$ jest więc funkcją symetryczną pierwiastków $x_1, x_2, \dots, x_n$, a zatem współczynniki wielomianu $R(t)$ należą do K . To samo dotyczy wielomianu $T(t) = R(t) \cdot S(t)$. Zgodnie z definicją wielomianu W wszystkie pierwiastki wielomianu $R(t)$ są jednokrotne, a więc w szczególności $R'(Z) \neq 0$. Ponieważ $T(Z) = \Theta \cdot R'(Z)$, więc otrzymujemy stąd $\Theta = T(Z):R'(Z)$. Przedstawiliśmy w ten sposób Θ jako funkcję wymierną względem Z ; stosując teraz twierdzenie 8 Rozdziału XIII (§ 3, str. 229), możemy wyrazić Θ jako wielomian względem Z ¹⁾.

¹⁾ Lemat 3 udowodniony został przez Lagrange'a w pracy „*Réflexions sur la résolution algébrique des équations*“, która ukazała się w *Nouveaux Mémoires de l'Académie Royale de Berlin* w latach 1770 i 1771 (przedruk w „*Oeuvres de Lagrange*“, publiées par J. A. Serret“, Paryż 1869, Tom 3, str. 403).

W pracy tej Lagrange poddał analizie różne znane metody rozwiązywania równań 3-go i 4-go stopnia i stwierdził związek, zachodzący między rozwiązaniami tych równań a pewnymi grupami podstawień. Z tego względu Lagrange uważany być może za prekursora Galois. Co do wzorów dla funkcji $R(t)$ i $S(t)$, por. też wzór interpolacyjny Lagrange'a w Rozdziale VIII, § 12, str. 130.

Twierdzenie 8. Na to, żeby grupą symetrii liczby Θ , należącej do ciała Σ , była cała grupa G , potrzeba i wystarcza, by Θ należało do K .

Dowód. Dostateczność tego warunku udowodniliśmy już w twierdzeniu 2. Dla dowodu jego konieczności zachowajmy oznaczenia, wprowadzone w lemacie 3, i przypuśćmy, że $\pi(\Theta) = \Theta$ dla każdego podstawienia π grupy G . Możemy więc napisać

$$\Theta = a_0 + a_1 Z + a_2 Z^2 + \dots + a_h Z^h,$$

lub wyraźniej

$$\Theta = a_0 + a_1 \cdot W(x) + a_2 \cdot [W(x)]^2 + \dots + a_h \cdot [W(x)]^h,$$

przy czym liczby $a_0, a_1, \dots, a_h$ należą do K . Na mocy twierdzenia 3 wynika stąd, że dla dowolnego podstawienia π , należącego do grupy G , zachodzi równość

$$\Theta = \pi(\Theta) = a_0 + a_1 \cdot W(\pi(x)) + a_2 \cdot [W(\pi(x))]^2 + \dots + a_h \cdot [W(\pi(x))]^h.$$

Wypiszmy te równości dla wszystkich podstawień π grupy G i dodajmy je do siebie. Oznaczając przez m rząd grupy G , otrzymamy

$$m\Theta = m \cdot a_0 + a_1 \cdot \sum_{\pi} W(\pi(x)) + a_2 \cdot \sum_{\pi} [W(\pi(x))]^2 + \dots + a_h \cdot \sum_{\pi} [W(\pi(x))]^h.$$

Występujące tu sumy $\sum_{\pi} [W(\pi(x))]^i$ potęg pierwiastków wielomianu $R(t)$ można na mocy wzorów Newtona wyznaczyć przy pomocy współczynników tego wielomianu (por. Rozdział IX, § 5, str. 164). Sumy te należą zatem do ciała K ; dowodzi to, że $m\Theta$, a więc i Θ , są elementami tego ciała, c. b. d. o.

Twierdzenie 8 jest uogólnieniem twierdzenia o funkcjach symetrycznych. Twierdzenie to mówi bowiem, że nie tylko takie wielomiany względem $x_1, x_2, \dots, x_n$, które nie zmieniają swej wartości przy wszelkich podstawieniach liczb $x_1, x_2, \dots, x_n$, mają wartość należącą do K , ale że własność tę posiadają również wszystkie wielomiany, które nie zmieniają swej wartości przy podstawieniach należących do grupy G .

§ 6. Wyznaczanie grupy Galois. Z twierdzenia 8 wysnujemy wniosek, pozwalający w niektórych przypadkach efektywnie wyznaczyć grupę Galois danego równania.

Niech S_n oznacza grupę symetryczną, złożoną z wszystkich podstawień pierwiastków $x_1, x_2, \dots, x_n$, a H — dowolną jej podgrupę.

Założmy, że $\pi_1 H + \pi_2 H + \dots + \pi_k H$ jest rozkładem S_n na warstwy względem H . Mamy wtedy

Twierdzenie 9. *Jeśli wielomian $V(\xi_1, \xi_2, \dots, \xi_n)$ czyni zadość warunkom twierdzenia 6, to na to, by grupa G była podgrupą H lub jednej z grup sprzężonych z H , potrzeba i wystarcza, żeby choć jedna z liczb $V(\pi_j(x))$, gdzie $j=1, 2, \dots, k$, należała do ciała K .*

Dowód. Jeśli $V(\pi_j(x)) = a$ i a należy do ciała K , to między pierwiastkami równania $f(x) = 0$ zachodzi zależność wymierna w K

$$V(\pi_j(x)) - a = 0.$$

Dla dowolnej permutacji π grupy Galois G musi więc być $V(\pi\pi_j(x)) - a = 0$, co daje $V(\pi_j(x)) = V(\pi\pi_j(x))$. Ponieważ zakładamy, że wielomian V czyni zadość warunkom twierdzenia 6, więc wnosimy stąd, że $\pi_j^{-1}\pi\pi_j$ należy do grupy H , t. zn. że π należy do grupy $\pi_j H \pi_j^{-1}$, sprzężonej z H . Grupa G jest więc zawarta w $\pi_j H \pi_j^{-1}$.

Założmy na odwrót, że G jest podgrupą grupy $\tau H \tau^{-1}$, sprzężonej z H . Jeśli τ należy np. do warstwy $\pi_j H$, to istnieje w H takie podstawienie χ , że $\tau = \pi_j \chi$, a więc $\tau H \tau^{-1} = \pi_j \chi H \chi^{-1} \pi_j^{-1} = \pi_j H \pi_j^{-1}$. Wynika stąd, że każde podstawienie π grupy G ma postać $\pi_j \sigma \pi_j^{-1}$, gdzie σ jest elementem grupy H . Dla każdego więc π należącego do G iloczyn $\pi_j^{-1}(\pi\pi_j)$ należy do grupy H , co dowodzi, że $V(\pi_j(x)) = V(\pi\pi_j(x))$. Wartość wielomianu $V(\pi_j(x))$ nie ulega zatem zmianie przy żadnej permutacji π grupy G , a to w myśl twierdzenia 8 dowodzi, że liczba $V(\pi_j(x))$ należy do ciała K , c. b. d. o.

Liczby $V(\pi_1(x)), V(\pi_2(x)), \dots, V(\pi_k(x))$ są pierwiastkami wielomianu

$$F(t) = \prod_{j=1}^k [t - V(\pi_j(x))].$$

Wykażemy, że współczynniki tego wielomianu należą do ciała K . Istotnie, jeśli liczby $x_1, x_2, \dots, x_n$ poddamy dowolnej permutacji π , to otrzymamy wielomian

$$(11) \quad \prod_{j=1}^k [t - V(\pi\pi_j(x))].$$

Układ liczb $V(\pi\pi_1(x)), V(\pi\pi_2(x)), \dots, V(\pi\pi_k(x))$ różni się co najwyżej porządkiem od układu liczb $V(\pi_1(x)), V(\pi_2(x)), \dots, V(\pi_k(x))$. Istotnie, jeśli $\pi\pi_j$ należy do warstwy $\pi_c H$, to $\pi_c^{-1}\pi\pi_j$ należy do H , a więc $V(\pi\pi_j(x)) = V(\pi_c(x))$; nadto liczby $V(\pi\pi_j(x))$ i $V(\pi\pi_l(x))$ są różne dla $j \neq l$, gdyż w przeciwnym razie z twierdzenia 6 otrzymali-

byśmy wniosk, że $(\pi\pi_j)^{-1}(\pi\pi_l)$ jest elementem H , czyli, że $\pi_l^{-1}\pi_j$ należy do H , co dla $j \neq l$ nie jest możliwe. Wynika stąd, że wielomian (11) jest identyczny z wielomianem $F(t)$. Współczynniki wielomianu $F(t)$ są więc funkcjami symetrycznymi liczb $x_1, x_2, \dots, x_n$, t. zn. należą do ciała K . Na mocy twierdzenia 9 wynika stąd

Twierdzenie 10. *Jeśli istnieje metoda, pozwalająca sprawdzić, czy choć jeden z pierwiastków dowolnego wielomianu o współczynnikach należących do ciała K też do tego ciała należy, to istnieje też metoda, pozwalająca sprawdzić, czy grupa Galois dowolnego równania $f(x) = 0$ o współczynnikach należących do ciała K jest podgrupą dowolnej z górą danej grupy H , ewentualnie jednej z grup z nią sprzężonych.*

Biorąc jako H kolejno wszystkie grupy podstawień liczb $x_1, x_2, \dots, x_n$ (których ilość jest oczywiście skończona), wyznaczymy w ten sposób samą grupę G , bądź jedną z grup sprzężonych z G .

Grupa $\pi G \pi^{-1}$ różni się od G właściwie tylko sposobem ponumerowania liczb $x_1, x_2, \dots, x_n$. Istotnie, jeśli G zawiera permutację $\begin{pmatrix} x_1 & x_2 & \dots & x_n \\ x_{k_1} & x_{k_2} & \dots & x_{k_n} \end{pmatrix}$, to $\pi G \pi^{-1}$ zawiera permutację $\begin{pmatrix} \pi(x_1) & \pi(x_2) & \dots & \pi(x_n) \\ \pi(x_{k_1}) & \pi(x_{k_2}) & \dots & \pi(x_{k_n}) \end{pmatrix}$ i vice versa. Wystarczy więc przenumerać liczby $x_1, x_2, \dots, x_n$ tak, aby $\pi(x_j)$ przeszło na x_j , a wtedy $\pi G \pi^{-1}$ stanie się identyczne z G .

Większość ciał K , jakie spotykamy w zastosowaniach, spełnia założenia twierdzenia 10. W szczególności dotyczy to ciała $\mathcal{R}$ liczb wymiernych (por. dalej ćwiczenie 5) oraz — jak można wykazać¹⁾ — ciała, powstającego z $\mathcal{R}$ przez dołączenie jednej lub wielu liczb algebraicznych. Z drugiej strony, istnieją też ciała, nie spełniające założeń twierdzenia 10²⁾.

PRZYKŁAD. Niech $f(x)$ będzie wielomianem 4-go stopnia bez pierwiastków wielokrotnych:

$$f(x) = a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4.$$

Jako H obierzmy następującą grupę G_8 :

$$\{(1, x_1, x_2, x_3, x_4), (x_1, x_2)(x_3, x_4), (x_1, x_4, x_2, x_3), (x_1, x_2), (x_3, x_4), (x_1, x_3)(x_2, x_4), (x_1, x_4)(x_2, x_3)\}.$$

Rozkład S_4 na warstwy ma postać

$$S_4 = \pi_1 G_8 + \pi_2 G_8 + \pi_3 G_8,$$

gdzie $\pi_1 = 1$, $\pi_2 = (x_1, x_2, x_3, x_4)$, $\pi_3 = (x_1, x_3, x_2, x_4)$.

¹⁾ Por. np. B. L. van der Waerden, *Moderne Algebra*, Wyd. 2-e, Tom I, Berlin 1937, str. 142-144.

²⁾ Por. B. L. van der Waerden, *Mathematische Annalen*, Tom 102 (1930), str. 738.

Przyjmijmy

$$V(\xi_1, \xi_2, \xi_3, \xi_4) = \xi_1 \xi_2 + \xi_3 \xi_4.$$

Dla każdego podstawienia π z grupy G_8 jest $V(\pi(x)) = V(x)$, ale:

$$V(\pi_2(x)) = x_1 x_4 + x_2 x_3 \quad \text{ i } \quad V(\pi_3(x)) = x_1 x_3 + x_2 x_4.$$

Trzy te liczby są różne między sobą, gdyż np. z równości

$$x_1 x_3 + x_2 x_4 = x_1 x_2 + x_3 x_4$$

wynikłoby, że $(x_1 - x_4)(x_2 - x_3) = 0$, wbrew założeniu, że $f(x)$ nie ma pierwiastków wielokrotnych. Równość $V(\pi(x)) = V(x)$ zachodzi więc wtedy i tylko wtedy, gdy podstawienia π i σ należą do tej samej warstwy.

Liczby:

$$\Theta_1 = V(x) = x_1 x_2 + x_3 x_4, \quad \Theta_2 = V(\pi_2(x)) = x_1 x_4 + x_2 x_3 \quad \text{ i } \quad \Theta_3 = V(\pi_3(x)) = x_1 x_3 + x_2 x_4.$$

są pierwiastkami wielomianu

$$F(t) = a_0^3(t - \Theta_1)(t - \Theta_2)(t - \Theta_3) = \\ = a_0^3 t^3 - a_0^2 a_2 t^2 + a_0(a_1 a_3 - 4a_0 a_4)t - (a_1^2 a_4 - 4a_0 a_2 a_4 + a_0 a_3^2).$$

Na to więc, by grupa Galois równania $f(x) = 0$ była zawarta w G_8 lub w jednej z grup sprzężonych z G_8 , potrzeba i wystarcza, żeby równanie $F(t) = 0$ miało choć jeden pierwiastek należący do K .

ĆWICZENIA. 1. Grupa równania symetrycznego $x^4 + ax^3 + bx^2 + ax + 1 = 0$ w dowolnym ciele zawierającym a i b jest sprzężona z G_8 lub z jedną z podgrup G_8 .

[$F(t)$ ma pierwiastek 2].

2. Jeśli wyróżnik D równania $f(x) = 0$ jest kwadratem liczby należącej do K , to grupa G składa się wyłącznie z podstawień parzystych, t. zn. takich, które są iloczynami parzystej liczby transpozycji.

$[D = \prod_{j=2}^n \prod_{k=1}^{j-1} (x_j - x_k)^2]$, w myśl więc założenia istnieje w K liczba a taka, że $\prod_{j=2}^n \prod_{k=1}^{j-1} (x_j - x_k) = a$, zaś ta zależność jest niezmiennicza tylko względem podstawień parzystych].

3. Kiedy grupa równania z ćwiczenia 1 jest zawarta w grupie $\{1, (x_1 x_2)(x_3 x_4), (x_1 x_3)(x_2 x_4), (x_1 x_4)(x_2 x_3)\}$ lub w jednej z grup z nią sprzężonych?

[Wtedy, gdy pierwiastek kwadratowy z wyróżnika równania należy do K lub — co na jedno wychodzi — gdy wszystkie pierwiastki równania $F(t) = 0$ należą do K].

4. Wyróżnik równania $a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = 0$ równy jest wyróżnikowi równania $F(t) = 0$. Obliczyć wyróżnik równania stopnia 4.

[Oprzeć się na tożsamościach:

$$\Theta_1 - \Theta_2 = (x_1 - x_3)(x_2 - x_4), \quad \Theta_2 - \Theta_3 = (x_1 - x_2)(x_4 - x_3) \quad \text{ i } \quad \Theta_3 - \Theta_1 = (x_1 - x_4)(x_3 - x_2).]$$

5. Jeśli równanie o współczynnikach całkowitych $a_0 x^n + a_1 x^{n-1} + \dots + a_n = 0$ ma pierwiastek wymierny, to $w = p \cdot a_0$, gdzie p jest dzielnikiem liczby $a_0^{n-1} a_n$.

[Por. Rozdział VIII, § 15, str. 137].

§ 7. Własności liczb ciała Σ . W § 5 badaliśmy liczby, których grupą symetrii jest cała grupa G . Obecnie zbadamy liczby Θ ciała Σ , których grupą symetrii jest dowolna podgrupa grupy G . Udowodnimy najpierw

Twierdzenie 11. Jeśli H jest grupą symetrii liczby Θ i $G = \pi_1 H + \pi_2 H + \dots + \pi_k H$ oznacza rozkład grupy G na warstwy lewostronne względem H , to liczby $\pi_1(\Theta), \pi_2(\Theta), \dots, \pi_k(\Theta)$ są wszystkimi liczbami sprzężonymi z Θ i są wszystkie różne.

Liczby te są pierwiastkami równania $P(t) = 0$ stopnia k o współczynnikach należących do K , nieprzywiedlnego w ciele K .

Dowód. Liczby $\pi_j(\Theta)$ są dla $j = 1, 2, 3, \dots, k$ sprzężone z Θ . Gdyby było $\pi_j(\Theta) = \pi_l(\Theta)$, to mielibyśmy $\pi_l^{-1} \pi_j(\Theta) = \Theta$, a więc $\pi_l^{-1} \pi_j$ należałoby do H , t. zn. że π_j należałoby do $\pi_l H$, co dla $j \neq l$ nie jest możliwe. Każda liczba sprzężona z Θ ma postać $\pi(\Theta)$, gdzie π jest dowolnym podstawieniem z grupy G ; istnieje więc $j \leq k$ takie, że π należy do warstwy $\pi_j H$, t. j. zachodzi równość postaci $\pi = \pi_j \sigma$, gdzie σ oznacza podstawienie należące do H . Stąd

$$\pi(\Theta) = \pi_j(\sigma(\Theta)) = \pi_j(\Theta),$$

gdyż $\sigma(\Theta) = \Theta$.

Liczby $\pi_1(\Theta), \pi_2(\Theta), \dots, \pi_k(\Theta)$ są pierwiastkami wielomianu $P(t) = \prod_{j=1}^k [t - \pi_j(\Theta)]$ stopnia k . Jeżeli zastosujemy do liczb $x_1, x_2, \dots, x_n$

podstawienie π grupy G , to otrzymamy wielomian $\prod_{j=1}^k [t - \pi \pi_j(\Theta)]$,

który pokrywa się z $P(t)$, gdyż liczby $\pi \pi_j(\Theta)$ są też sprzężone z Θ i też są różne między sobą. Współczynniki wielomianu $P(t)$ nie ulegają więc zmianie, gdy liczby $x_1, x_2, \dots, x_n$ poddamy dowolnemu podstawieniu należącemu do grupy G ; w myśl zatem twierdzenia 8 należą one do K .

Wreszcie, wielomian $P(t)$ jest nieprzywiedlny w K . Istotnie, jeśli $Q(t)$ jest wielomianem, którego współczynniki są elementami ciała K , i takim, że $Q(\pi_1(\Theta)) = 0$, to dla każdego podstawienia π z grupy G musi być $Q(\pi \pi_1(\Theta)) = 0$ (por. twierdzenie 3). Przyjmując tu $\pi = \pi_1 \pi_i^{-1}$ dojdziemy do wniosku, że wszystkie pierwiastki wielomianu $P(t)$ są też pierwiastkami wielomianu $Q(t)$. Wielomian $P(t)$ nie może więc mieć czynnika $Q(t)$, którego współczynniki należą do K i który ani nie jest stałą, ani nie różni się od $P(t)$ tylko czynnikiem stałym.

Twierdzenie 11 jest w ten sposób udowodnione całkowicie.

Jeśli w szczególności założymy, że Θ jest liczbą pierwotną ciała Σ , to H będzie grupą jednostkową i permutacje $\pi_1, \pi_2, \dots, \pi_k$ wypełnią całą grupę G . Iloczyn $\prod_{\pi \in G} [t - \pi(\Theta)]$, rozciągnięty na wszystkie permutacje π grupy G , jest więc wielomianem nieprzywiedlnym w K o współczynnikach należących do K , posiadającym współczynnik 1 przy najwyższej potędze t i równym 0 dla $t = \Theta$. Jak wiemy (por. Rozdział XII, § 1, twierdzenie 2, str. 211), własności te wyznaczają jednoznacznie wielomian; możemy więc wypowiedzieć

Twierdzenie 12. *Jeśli Θ jest liczbą pierwotną ciała Σ , to iloczyn $R(t) = \prod_{\pi \in G} [t - \pi(\Theta)]$ jest jedynym wielomianem nieprzywiedlnym w K o współczynnikach należących do K , równym 0 dla $t = \Theta$ i mającym współczynnik równy 1 przy najwyższej potędze t .*

Wielomian $R(t)$ nazywa się *rozwiązującą Galois*. Każdej liczbie pierwotnej odpowiada więc pewna rozwiązująca.

W związku z twierdzeniem 11 wprowadzimy pewne nazwy.

Każdy pierwiastek Θ wielomianu $P(t)$ o współczynnikach należących do K , nazywamy *liczbą algebraiczną względem K* .

Stopniem liczby Θ algebraicznej względem K nazywamy stopień wielomianu nieprzywiedlnego w K , którego pierwiastkiem jest Θ .

Z twierdzenia 11 wynika zatem

Twierdzenie 13. *Jeśli H jest grupą symetrii liczby Θ , to Θ jest liczbą algebraiczną względem K , której stopień równa się wskaźnikowi grupy H w G .*

PRZYKŁAD. Niech $f(x) = a_0x^3 + a_1x^2 + a_2x + a_3$. Grupa G równania $f(x) = 0$ jest zawarta w grupie wszystkich podstawień pierwiastków x_1, x_2, x_3 . Przypuśćmy, że grupa G zawiera wszystkie te podstawienia. Liczba $\Theta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ ciała Σ ma jako grupę symetrii grupę cykliczną $O = \{1, (x_1, x_2, x_3), (x_1, x_3, x_2)\}$ o wskaźniku 2, czyni więc zadość równaniu stopnia 2 o współczynnikach należących do K . Istotnie, $a_0^4\Theta^2 = a_2^2a_3^2 + 18a_0a_1a_2a_3 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2$, gdyż $a_0^4\Theta^2$ jest wyróżnikiem wielomianu $f(x)$. Drugim pierwiastkiem równania dla Θ jest liczba $(x_2 - x_1)(x_2 - x_3)(x_3 - x_1)$, sprzężona z Θ (por. tu też równanie $F(t) = 0$, podane w przykładzie z § 6, str. 388).

Z twierdzeń 8 i 11 wynika dalej łatwo następujące uogólnienie lematu 3:

Twierdzenie 14. *Jeśli H jest grupą symetrii liczby Θ , a grupa symetrii liczby Z zawiera H , to istnieje taki wielomian $R(\xi)$ jednej zmiennej o współczynnikach należących do ciała K , że $Z = R(\Theta)$.*

Dowód. Zachowujemy oznaczenia wprowadzone w twierdzeniu 11 i przyjmujemy:

$$P(t) = \prod_{j=1}^k [t - \pi_j(\Theta)], \quad Q(t) = \sum_{j=1}^k \frac{\pi_j(Z)}{t - \pi_j(\Theta)}.$$

$P(t)$ ma — jak wiemy z twierdzenia 11 — współczynniki, należące do ciała K . To samo dotyczy wielomianu $P(t) \cdot Q(t)$, gdyż nie ulega on zmianie, jeśli liczby $x_1, x_2, \dots, x_n$ poddamy jakimkolwiek podstawieniu π grupy G (por. twierdzenie 8). Wystarczy teraz zauważyć, że wielomian $P(t) \cdot Q(t)$ przyjmuje dla $t = \Theta$ wartość $Z \cdot P'(\Theta)$, i zastosować to samo rozumowanie, co w dowodzie lematu 3.

Twierdzenie 14 nazywane jest często *twierdzeniem Lagrange'a*.

Jako prosty wniosek otrzymamy jeszcze

Twierdzenie 15. *Jeśli Θ jest liczbą pierwotną ciała Σ , to każda inna liczba tego ciała może być przedstawiona jako wielomian $c_0 + c_1\Theta + c_2\Theta^2 + \dots + c_h\Theta^h$, gdzie $c_0, c_1, \dots, c_h$ są liczbami ciała K .*

Twierdzenie 15 jest znacznie ogólniejsze od lematu 3. Występująca w tym lemacie liczba $Z = W(\mathfrak{x})$ jest niewątpliwie liczbą pierwotną ciała Σ ; twierdzenie 15 mówi nam, że możemy każdą inną liczbę pierwotną ciała Σ użyć do tego samego celu, choćby nawet liczba ta nie dawała się przedstawić w postaci $W(\mathfrak{x})$, gdzie W spełnia założenia lematu 3.

ĆWICZENIA. 1. Oznaczając przez $\varepsilon, \varepsilon^2, \varepsilon^3$ i ε^4 pierwiastki równania $x^4 + x^3 + x^2 + x + 1 = 0$, podać równanie, któreinu czyni zadość liczba $\Theta = \varepsilon + \varepsilon^4$. [Wprowadzając oznaczenie $\Theta' = \varepsilon^2 + \varepsilon^3$, mamy $\Theta + \Theta' = -1$ i $\Theta\Theta' = -1$].

2. Korzystając z wyników ćwiczenia 1, rozwiązać równanie

$$x^4 + x^3 + x^2 + x + 1 = 0.$$

§ 8. Kryterium nieprzywiedlności wielomianu. Zastosujmy twierdzenie 11 do przypadku $\Theta = x_1$. Grupą symetrii tej liczby jest grupa H tych podstawień π należących do grupy G , dla których $\pi(x_1) = x_1$. Wynika stąd, że w rozkładzie grupy G na warstwy względem H :

$$G = \pi_1 H + \pi_2 H + \dots + \pi_h H$$

kompleks $\pi_j H$ składa się z wszystkich π należących do G , dla których $\pi(x_1) = \pi_j(x_1)$. Istotnie, jeśli π należy do kompleksu $\pi_j H$, to $\pi = \pi_j \sigma$, gdzie σ należy do H , a więc $\pi(x_1) = \pi_j(\sigma(x_1)) = \pi_j(x_1)$. Na odwrót, jeśli $\pi(x_1) = \pi_j(x_1)$, to $\pi_j^{-1}\pi(x_1) = x_1$, a więc $\pi_j^{-1}\pi$ należy do grupy H , t. j. π należy do kompleksu $\pi_j H$. Liczby $\pi_j(x_1)$ i $\pi_l(x_1)$ są różne dla $j \neq l$, gdyż warstwy $\pi_j H$ i $\pi_l H$ są rozłączne.

Możliwe są teraz dwa przypadki:

1° Dla każdego $j \leq n$ istnieje w grupie G takie podstawienie π , że $\pi(x_1) = x_j$.

Grupa G nazywa się wtedy *przechodnią* i wskaźnik k grupy H w G musi być równy n .

2° Istnieje $j \leq n$ takie, że dla żadnego π należącego do G nie zachodzi równość $\pi(x_1) = x_j$.

Grupa G nazywa się wtedy *nieprzechodnią* i k jest mniejsze od n .

Jeżeli grupa G jest przechodnią, to wielomian

$$P(t) = (t - \pi_1(x_1)) (t - \pi_2(x_1)) \dots (t - \pi_n(x_1))$$

różni się od $f(t)$ co najwyżej czynnikiem stałym, gdyż oba te wielomiany stają się równe 0 dla t równych $x_1, x_2, \dots, x_n$ i tylko dla tych t . Jeśli natomiast grupa G jest nieprzechodnią, to $P(t)$ jest dzielnikiem właściwym $f(t)$. Otrzymujemy w ten sposób

Twierdzenie 16. *Na to, aby wielomian $f(x)$ był nieprzywiedlny w ciele K , potrzeba i wystarcza, by grupa równania $f(x) = 0$ w ciele K była przechodnią.*

PRZYKŁAD. Obliczanie grupy równania stopnia 3. Grupa wszystkich podstawień trzech przedmiotów ma tylko jedną podgrupę właściwą przechodnią, mianowicie grupę cykliczną C (por. przykład z § 7). Grupą równania nieprzywiedlnego stopnia 3 jest więc albo grupa symetryczna S_3 , składająca się ze wszystkich podstawień liczb x_1, x_2, x_3 , albo grupa cykliczna. Drugi przypadek zachodzi wtedy i tylko wtedy, gdy w ciele K istnieje liczba, której kwadrat równa się wyróżnikowi równania.

Z faktu, że wskaźnik grupy H w G jest równy n , o ile G jest grupą przechodnią, wynika od razu następujące twierdzenie z Teorii grup:

Twierdzenie 17. *Rząd¹⁾ grupy przechodniej jest podzielny przez jej stopień.*

Istotnie, rząd każdej grupy jest podzielny przez wskaźnik dowolnej jej podgrupy (por. Rozdział XIX, § 10, tw. 13, str. 327).

ĆWICZENIA. 1. Wyznaczyć grupy równań $x^3 - 2 = 0$ i $x^3 + 2x + 1 = 0$ w ciele $\mathcal{R}$ liczb wymiernych.

2. Jeśli posiadamy sposób, pozwalający rozstrzygnąć, czy dowolne równanie o współczynnikach należących do K ma choć jeden pierwiastek należący do K , to posiadamy też sposób, pozwalający rozłożyć dowolny wielomian o współczynnikach należących do K na czynniki nieprzywiedlne.

[Zgodnie z § 6 możemy wyznaczyć grupę G lub jedną z grup sprzężonych z G . Jeśli grupa ta jest przechodnią, to $f(x)$ jest wielomianem nieprzywiedlnym. W przeciwnym razie zbiór $\{x_1, x_2, \dots, x_n\}$ rozpada się na zbiory nie mające

¹⁾ Rzędem grupy (skończonej) nazywamy liczbę jej elementów.

elementów wspólnych, w obrębie których grupa ta jest przechodnią. Jeśli np. $x_1, x_2, \dots, x_k$ ($k < n$) jest takim zbiorem, to iloczyn $(x - x_1)(x - x_2) \dots (x - x_k)$ jest czynnikiem nieprzywiedlnym wielomianu $f(x)$.

3. Rząd grupy przemiennej i przechodniej jest równy jej stopniowi.

[Oznaczając przez H grupę tych π , dla których $\pi(x_1) = x_1$, wnosimy, że $\pi_j H \pi_j^{-1}$ jest grupą tych π , dla których $\pi(\pi_j(x_1)) = \pi_j(x_1)$. Ponieważ grupa G jest przemienne, więc $\pi_j H \pi_j^{-1} = H$, co dowodzi, że podstawienia z grupy H przekształcają każdą z liczb $x_1, x_2, \dots, x_n$ w samą siebie (gdyż każde x_i może być przedstawione jako $\pi_j(x_1)$). H jest więc grupą jednostkową i wskaźnik jej w G jest równy rządowi grupy G].

§ 9. Równania o grupie symetrycznej. Zastosujemy twierdzenie 16 do dowodu istnienia równań stopnia p , będącego liczbą pierwszą, których grupa jest *symetryczna*, t. j. składa się z wszystkich podstawień pierwiastków.

Potrzebny nam będzie następujący

Lemat 4. *Jeśli p jest liczbą pierwszą, a G jakąkolwiek grupą podstawień zbioru $A = \{x_1, x_2, \dots, x_p\}$ przechodnią i zawierającą choć jedną transpozycję, to G zawiera wszystkie podstawienia zbioru A .*

Dowód. Podzbiór N zbioru A nazwiemy *spójnym*, jeśli dla dowolnych dwu jego elementów a, b transpozycja (a, b) należy do G .

Zbiór spójny nazywa się *maksymalnym*, jeśli nie jest częścią żadnego innego zbioru spójnego.

Jest jasne, że

(i) *Dla każdego a , należącego do A , istnieje maksymalny zbiór spójny, zawierający a .*

Pokażemy następnie, że

(ii) *Jeśli $N = \{a_1, a_2, \dots, a_k\}$ jest maksymalnym zbiorem spójnym, a π permutacją należącą do G , to i zbiór $\pi(N) = \{\pi(a_1), \pi(a_2), \dots, \pi(a_k)\}$ jest maksymalnym zbiorem spójnym.*

Istotnie, jeśli a i b należą do N , to transpozycja (a, b) należy do G . Grupa G zawiera zatem transpozycję $(\pi(a), \pi(b)) = \pi(a, b)\pi^{-1}$, t. zn. że zbiór $\pi(N)$ jest spójny. Gdyby zbiór ten nie był maksymalny, to istniałby poza $\pi(N)$ element b taki, że dla każdego a , należącego do N , transpozycje $(\pi(a), b)$ należałyby do G . Wynika stąd, że i transpozycje $(a, \pi^{-1}(b)) = \pi^{-1}(\pi(a), b)\pi$ należałyby do G , mimo że $\pi^{-1}(b)$ nie należy do N . Zbiór N nie byłby więc maksymalnym zbiorem spójnym.

(iii) *Różne maksymalne zbiory spójne M i N nie mają elementu wspólnego.*

Wystarczy pokazać, że jeśli M i N mają element wspólny c , to suma zbiorów M i N jest spójna. Do tego celu zaś wystarczy zauważyć, że jeśli dwa elementy a i b należą jednocześnie do M lub jednocześnie do N , to transpozycja (a, b) należy do G w myśl założenia, jeśli zaś a należy do M , a b do N , to transpozycje (a, c) i (b, c) należą do G , skąd wynika, że i transpozycja $(a, b) = (a, c)(b, c)(a, c)$ należy do G .

Z (iii) wynika łatwo, że

(iv) Dwa maksymalne zbiory spójne M i N mają zawsze tę samą liczbę elementów.

Istotnie, przypuśćmy, że a jest elementem M , zaś b — elementem N . Grupa G — jako przechodnia — zawiera podstawienie π , dla którego $\pi(a)=b$. Zbiory $\pi(M)$ i N mają więc element wspólny b , a że oba są w myśl (ii) maksymalnymi zbiorami spójnymi, więc zgodnie z (iii) muszą być identyczne. To dowodzi, że M i N mają po tyleż elementów.

Udowodnimy wreszcie, że

(v) A jest zbiorem spójnym.

Istotnie, w myśl założenia istnieje w G co najmniej jedna transpozycja (a, b) . Maksymalny zbiór spójny N , zawierający a , ma więc co najmniej dwa elementy. Gdyby zbiór N nie wypełniał całego A , to istniałby w A element a_1 , nie należący do N . Niech π_1 oznacza takie podstawienie, należące do grupy G , że $\pi_1(a)=a_1$. Zbiór $N_1=\pi_1(N)$ ma tyleż elementów co N i nie ma z N żadnego elementu wspólnego. Jeśli zbiory N_1 i N nie wyczerpują jeszcze całego zbioru A , to istnieje w A element a_2 , nie należący ani do N , ani do N_1 . Oznaczmy przez π_2 podstawienie, należące do G , dla którego $\pi_2(a)=a_2$, i przyjmijmy $N_2=\pi_2(N)$. Zbiór N_2 ma tyleż elementów co N i nie ma ani z N , ani z N_1 żadnego elementu wspólnego. Kontynuując to rozumowanie, dojdziemy do wniosku, że zbiór A rozkłada się na sumę skończonej liczby zbiorów, które mają tę samą liczbę elementów i nie mają między sobą żadnego elementu wspólnego. Wniosek ten jest niemożliwy, gdyż ilość elementów zbioru A jest liczbą pierwszą. Zatem N musi być równe A , t. j. zbiór A jest spójny.

Z (v) wynika, że grupa G zawiera każdą transpozycję (a, b) dla dowolnych a i b , należących do A . Wynika stąd, że G jest grupą symetryczną rzędu $p!$, gdyż każde podstawienie zbioru A jest iloczynem skończonej liczby transpozycji.

Opierając się na udowodnionym lemacie, wyprowadzimy

Twierdzenie 18. Jeśli równanie $h(x)=0$ o współczynnikach wymiernych, którego stopień p jest liczbą pierwszą, jest nieprzywiedlne w ciele $\mathcal{R}$ liczb wymiernych i ma dokładnie $p-2$ pierwiastki rzeczywiste, to jego grupą G w ciele $\mathcal{R}$ jest grupa symetryczna rzędu $p!$.

Dowód. Załóżmy, że pierwiastki $x_1, x_2, \dots, x_{p-2}$ równania $h(x)=0$ są rzeczywiste, a x_{p-1} i x_{p-2} — zespolone sprzężone. W ciele $\mathcal{R}(x_1, x_2, \dots, x_{p-2})$ wielomian $h(x)$ rozpada się na iloczyn $p-2$ czynników pierwszego stopnia i na czynnik drugiego stopnia $g(x)$, którego pierwiastkami są x_{p-1} i x_p :

$$h(x) = (x - x_1)(x - x_2) \dots (x - x_{p-2}) \cdot g(x).$$

Wielomian $g(x)$ jest nieprzywiedlny w ciele $\mathcal{R}(x_1, x_2, \dots, x_{p-2})$, gdyż w przeciwnym razie liczby x_{p-1} i x_p byłyby rzeczywiste. Grupa równania $h(x)=0$ w ciele $\mathcal{R}(x_1, x_2, \dots, x_{p-2})$ zawiera więc podstawienie (x_{p-1}, x_p) , a ponieważ grupa ta jest zawarta w G (por. § 2, ćwiczenie 2), więc G zawiera transpozycję (x_{p-1}, x_p) . W myśl twierdzenia 16 grupa G jest przechodnią, na mocy zatem lematu 4 G zawiera wszystkie podstawienia pierwiastków $x_1, x_2, \dots, x_p$, c. b. d. o.

Twierdzenie 18 wiąże się z następującym zagadnieniem:

(Z) Mając daną grupę podstawień n liczb oraz ciało liczbowe K , skonstruować równanie stopnia n o współczynnikach należących do K , którego grupa w ciele K jest izomorficzna z G .

Dla ciała liczb wymiernych i grupy G symetrycznej lub naprzemiennej zagadnienie to rozwiązał Hilbert¹⁾. Twierdzenie 18 pozwala rozwiązać zagadnienie (Z) dla przypadku ciała liczb wymiernych i grupy symetrycznej przy założeniu, że n jest liczbą pierwszą. Dla dowolnego G zagadnienie (Z) nie jest dotąd rozwiązane nawet w przypadku, gdy K jest ciałem liczb wymiernych²⁾.

ĆWICZENIA. 1. Grupa równania $x^5 - 10x + 2 = 0$ w ciele liczb wymiernych zawiera wszystkie podstawienia pierwiastków.

[Nieprzywiedlność tego równania ustalić można na podstawie kryterium Eisensteina (Rozdział VIII, § 26, str. 133, twierdzenie 14). Ilość pierwiastków rzeczywistych obliczamy, badając znak wielomianu $x^5 - 10x + 2$ i jego pochodnej w przedziałach $(-\infty, -\sqrt[4]{2})$, $(-\sqrt[4]{2}, +\sqrt[4]{2})$ i $(+\sqrt[4]{2}, +\infty)$].

2. Podać przykłady równań o współczynnikach całkowitych stopnia p , gdzie p jest liczbą pierwszą, których grupa G względem ciała liczb wymiernych jest symetryczna rzędu p .

§ 10. Wyznaczenie wszystkich ciał między K i Σ .

Pokażemy obecnie, w jaki sposób Teoria Galois pozwala rozklasyfikować wszystkie ciała zawarte w Σ i zawierające K . Udowodnimy mianowicie, że między takimi ciałami a podgrupami grupy Galois zachodzi odpowiedniość wzajemnie jednoznaczna.

Twierdzenie 19. (1) Jeśli H jest podgrupą grupy G , to zbiór Δ_H tych liczb ciała Σ , których grupa symetrii zawiera H , jest ciałem zawartym w Σ i zawierającym K .

(2) Jeśli grupą symetrii liczby θ jest H , to $\Delta_H = K(\theta)$.

(3) Każde ciało zawarte między K i Σ jest jednym z ciał Δ_H .

¹⁾ D. Hilbert, Crelle's Journal für Mathematik, Tom 110 (1892), str. 104.

²⁾ O zagadnieniu (Z) poinformować się można dokładnie w książce N. Czebotaiew, *Osnovy teorii Galois* (po rosyjsku), Leningrad-Moskwa 1934, Rozdział V; Wyd. 2-e (1936), Rozdział III. W książce tej podana jest też obszerna literatura.

Dowód. (1) Jeśli $\pi(\Theta) = \Theta$ i $\pi(Z) = Z$ dla każdego podstawienia π należącego do grupy H , to

$$\pi(\Theta \pm Z) = \Theta \pm Z, \quad \pi(\Theta \cdot Z) = \Theta \cdot Z \quad \text{ i } \quad \pi(\Theta : Z) = \Theta : Z \quad (\text{o ile } Z \neq 0).$$

Ze wzorów tych wynika, że Δ_H jest ciałem liczbowym. Ciało to jest oczywiście zawarte w Σ , zawiera zaś ono K na mocy twierdzenia 2.

(2) wynika bezpośrednio z twierdzenia 14.

Wreszcie, aby udowodnić (3), założmy, że Δ jest ciałem zawartym między K a Σ , i oznaczmy przez H część wspólną grup symetrii wszystkich liczb ciała Δ . Δ jest więc zawarte w Δ_H , gdyż grupa symetrii każdej liczby ciała Δ zawiera H .

Ponieważ ilość wszystkich podgrup G jest skończona, więc H jest częścią wspólną skończonej liczby grup $H_1, H_2, \dots, H_r$, przy czym H_j jest grupą symetrii pewnej liczby Θ_j ciała Δ ($j=1, 2, \dots, r$). Rozważmy teraz wielomiany liniowe r zmiennych $\zeta_1, \zeta_2, \dots, \zeta_r$

$$W_\pi(\zeta_1, \zeta_2, \dots, \zeta_r) = \zeta_1[\pi(\Theta_1) - \Theta_1] + \zeta_2[\pi(\Theta_2) - \Theta_2] + \dots + \zeta_r[\pi(\Theta_r) - \Theta_r],$$

gdzie π jest dowolnym podstawieniem grupy G , nie należącym do H . Wielomiany te nie są tożsamościowo równe 0, gdyż w przeciwnym razie zachodziłyby równości $\pi(\Theta_j) = \Theta_j$ dla $j=1, 2, \dots, r$, a więc π należałoby do wszystkich grup H_j ($j=1, 2, \dots, r$), t. j. do grupy H . Zgodnie z lematem 2 z § 4 (str. 380) istnieją więc liczby naturalne $n_1, n_2, \dots, n_r$ takie, że $W_\pi(n_1, n_2, \dots, n_r) \neq 0$ dla każdego podstawienia π grupy G , nie należącego do H . Przyjmijmy

$$\Theta = n_1\Theta_1 + n_2\Theta_2 + \dots + n_r\Theta_r.$$

Dla π nie należących do H będzie więc $\pi(\Theta) \neq \Theta$, podczas gdy dla π należących do H jest $\pi(\Theta_j) = \Theta_j$ dla $j=1, 2, \dots, r$, a więc $\pi(\Theta) = \Theta$. Grupą symetrii liczby Θ jest więc H , skąd w myśl twierdzenia 14 wnosimy, że każda liczba ciała Δ_H daje się przedstawić jako wielomian względem Θ o współczynnikach z K . Ponieważ liczby $\Theta_1, \Theta_2, \dots, \Theta_r$ należą do Δ , więc i Θ należy do Δ , co dowodzi, że ciało Δ_H zawiera się w Δ . Ciała Δ i Δ_H są zatem identyczne, c. b. d. o.

Z twierdzenia 19 wynika kilka ważnych wniosków.

Wniosek 1. Każde ciało zawarte między K i Σ powstaje z K przez dołączenie pewnej liczby należącej do Σ .

Istotnie, jeśli Θ jest liczbą, której grupą symetrii jest H , to $\Delta_H = K(\Theta)$ w myśl twierdzenia 19.

Wniosek 2. Jeśli Z należy do ciała $K(\Theta)$, a Θ do ciała Σ , to stopień liczby Z jest dzielnikiem stopnia liczby Θ .

Istotnie, jeśli H_Z i H_Θ oznaczają grupy symetrii liczb Z i Θ , to H_Z zawiera grupę H_Θ , skąd wynika, że rząd grupy H_Z jest wielokrotnością rzędu grupy H_Θ . Wskaźnik H_Z w G jest więc dzielnikiem wskaźnika H_Θ , wskaźniki te zaś są równe stopniom liczb Z i Θ (por. twierdzenie 13).

Wniosek 3. Jeśli Z należy do ciała $K(\Theta)$, a Θ do ciała Σ , oraz stopnie liczb Θ i Z są równe, to $K(\Theta) = K(Z)$.

Istotnie, z założenia wynika, że wskaźniki grup H_Θ i H_Z są równe, a więc i rzędy ich są równe. Ponieważ zaś H_Θ jest podgrupą grupy H_Z , więc $H_\Theta = H_Z$, co daje $K(\Theta) = K(Z)$.

ĆWICZENIE. Jeśli H' jest podgrupą grupy H'' , to ciało $\Delta_{H'}$ zawiera ciało $\Delta_{H''}$ i na odwrót.