ZESZYTY NAUKOWE WYŻSZEJ SZKOŁY PEDAGOGICZNEJ W BYDGOSZCZY
Problemy Matematyczne 1980 z. 2

Jerzy Browkin
Uniwersytet Warszawski

# ZNACZENIE TEORII GALOIS WE WSPÓŁCZESNEJ MATEMATYCE ORAZ ROLA TEJ TEORII W KSZTAŁCENIU MŁODYCH MATEMATYKÓW

André Weil w przedmowie do wydania rosyjskiego swej książki Basic Number Theory, Moskwa 1972, napisał m. in.

"... Był czas, gdy teorię Galois uważano za teorię trudną i abstrakcyjną, przeznaczoną wyłącznie dla specjalistów. Co więcej, znałem pewnych wybitnych matematyków należących do mojego pokolenia, którzy otwarcie przyznawali się do całkowitej niewiedzy w zakresie teorii Galois i, zdaje się, byli nawet z tego dumni. Obecnie wszyscy dobrze rozumieją, że teoria ta jest jednym z "podstawowych" działów, z którym powinien się zapoznać każdy poważnie traktujący swe studia student matematyki już podczas pierwszych lat studiów..."

Ustalmy więc najpierw, co rozumiemy przez teorię Galois. Jest to mianowicie teoria opisująca następującą sytuację.

Dane jest ciało $K$ i jego domknięcie rozdzielce $K_s$. Rozpatrujemy zbiór wszystkich ciał $L$ pośrednich między $K$ i $K_s$ oraz zbiór wszystkich $K$ - zanurzeń $\sigma : L \longrightarrow K_s$. W szczególności wyróżniamy te ciała $L$, które są rozszerzeniami Galois ciała $K$, tzn. spełniają $\sigma(L) = L$ dla każdego $K$ - zanurzenia $\sigma : L \longrightarrow K_s$. Jeżeli więc $L$ jest rozszerzeniem Galois ciała $K$, to zbiór $K$ - zanurzeń $\sigma : L \longrightarrow K_s$ jest grupą ze względu na superpozycję. Grupę tę nazywamy grupą Galois ciała $L$ względem $K$ i oznaczamy przez $G(L/K)$. W szczególności rozpatrujemy grupę $G(K_s/K)$. Na odwrót, każda podgrupa $H$ grupy $G(K_s/K)$ wyznacza pewne ciało pośrednie między $K$ i $K_s$, mianowicie - ciało elementów stałych ze względu na $K$ - zanurzenia należące do $H$. Ciało to oznaczamy przez $K_s^H$.

Podstawowymi twierdzeniami teorii Galois są:

Twierdzenie 1. O wzajemnie jednoznacznej odpowiedniości między zbiorem ciał pośrednich między K i $K_s$ oraz zbiorem podgrup grupy $G(K_s/K)$ domkniętych w topologii Krulla.

Twierdzenie 2. Jeżeli L jest rozszerzeniem Galois ciała K, to grupa $G(L/K)$ jest obrazem przy homomorfizmie kanonicznym grupy $G(K_s/K)$ polegającym na ograniczeniu K - izomorfizmów ciała $K_s$ do podciała L. Jądrem tego homomorfizmu jest grupa $G(K_s/L)$.

Jest to w istocie wniosek z twierdzenia o rozszerzaniu izomorfizmu.

Powyższe sformułowania można też ująć w języku teorii kategorii. Rozpatrujemy mianowicie kategorię $Gal_K$, której obiektami są ciała pośrednie między K i $K_s$, a morfizmami - K - izomorfizmy. Wyróżnione są w niej obiekty Galois; istnieją kanoniczne odwzorowania $Hom/K_s,K_s/ \longrightarrow Hom/L,K_s/$ polegające na ograniczaniu K - zanurzeń oraz Hom/L,L/ ma strukturę grupy.

Jeżeli M jest ustalonym ciałem pośrednim między K i $K_s$, to $Gal_M$ jest podkategorią kategorii $Gal_K$ i każdy obiekt z $Gal_M$, który był obiektem Galois w $Gal_K$ jest nadal obiektem Galois w $Gal_M$.

Tak więc teoria Galois rozumiana w ten sposób jest teorią opisującą zbiór rozszerzeń rozdzielczych ciała K i wykorzystującą w tym celu własności K - zanurzeń.

Zastosowania teorii Galois polegają zwykle na tym, że określa się funktor z opisanej wyżej kategorii $Gal_K$ do odpowiedniej innej kategorii /na przykład do kategorii grup, grup abelowych, zbiorów algebraicznych lub grup algebraicznych określonych nad ciałem K/, który pozwala w naturalny sposób określić działanie grup $G(L/K)$ na obiektach tej drugiej kategorii. Obiekty te uzyskują więc bogatszą strukturę, co pozwala na dokładniejsze ich zbadanie, stosując na przykład metody algebry homologicznej.

Te uwagi ogólne wyjaśnimy na kilku przykładach o podstawowym znaczeniu.

1/ Niech G będzie grupą algebraiczną określoną nad ciałem

K, na przykład - pełną grupą liniową $GL_n$. Wtedy przyporządkowując każdemu ciału L, które jest rozszerzeniem Galois ciała K, grupę $GL_n/L/$ otrzymujemy pewien funktor. Określone jest więc działanie grupy $G(L/K)$ na grupie $GL_n/L/$. W tej sytuacji można stosować metody algebry homologicznej do badania własności grupy $GL_n/L/$. Zachodzi na przykład

Twierdzenie 3 /A. Speiser/. $H^1\left(G(L/K), GL_n/L/\right) = 0$.

Z twierdzenia tego wynika na przykład, że jeżeli macierz zespolona A spełnia $\bar{A} = A^{-1}$, to istnieje taka macierz zespolona B, że $A = \bar{B}.B^{-1}$.

2/ Przyjmując w powyższym przykładzie n = 1 otrzymujemy funktor, który ciału L przyporządkowuje jego grupę multyplikatywną $L^*$. W tej sytuacji mamy twierdzenia:

$H^0(G(L/K), L^*) = K^*$, $H^1(G(L/K), L^*) = 0$ /twierdzenie Hilberta/,

$H^2(G(L/K), L^*)$ - jest podgrupą grupy Brauera ciała K złożoną z tych klas algebr, które rozpadają się nad ciałem L.

3/ Niech E będzie rozmaitością abelową /rzutową/ określoną nad ciałem K. Wtedy przyporządkowując ciału L, które jest rozszerzeniem Galois ciała K, grupę E/L/ punktów L - wymiernych na tej rozmaitości otrzymamy pewien funktor. Określone jest więc działanie grupy G L/K na E/L/. W tej sytuacji zachodzą na przykład następujące twierdzenia:

Twierdzenie 4 /L. Mordell, A. Weil/. Jeżeli K jest ciałem globalnym, to grupa E/K/ jest skończenie generowana.

Wynika stąd oczywiście, że podgrupa torsyjna grupy E/K/ jest skończona. Ostatnio B. Mazur udowodnił

Twierdzenie 5 /B. Mazur/. Jeżeli E jest rozmaitością abelową jednowymiarowa /tzn. krzywą eliptyczną/, a Q ciałem liczb wymiernych, to podgrupa torsyjna grupy E/Q/ ma $\leq 10$ lub 12 elementów.

Jest to rozstrzygnięcie dawno postawionego problemu.

Odnotujmy jeszcze dla przykładu

Twierdzenie 6 /F.K. Schmidt/. Jeżeli E jest krzywą eliptyczn-

ną, a K - ciałem skończonym, to $H^1(G(L/K), E/L/) = 0$. dla $(L : K) < \infty$.

Z twierdzenia tego wynika, że na krzywej eliptycznej nad ciałem skończonym istnieje punkt wymierny.

Do teorii Galois należy też następujący krąg zagadnień. Dane jest ciało K i pewna klasa grup $\mathfrak{K}$. Opisać wszystkie rozszerzenia Galois L ciała K takie, że grupa $G(L/K)$ należy do rozważanej klasy grup.

Pełne rozwiązanie tego zagadnienia jest znane tylko w przypadku, gdy $\mathfrak{K}$ jest klasą grup rozwiązalnych. Mianowicie zachodzi

Twierdzenie 7. Istnieje największe rozszerzenie L ciała K zawarte w $K_s$ i takie, że grupa $G(L/K)$ jest rozwiązalna. Ciało L jest sumą wszystkich ciał M, dla których istnieje ciąg ciał

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = M,$$

gdzie 1/ $K_{i+1}$ jest ciałem rozkładu wielomianu postaci $x^n - a$ należącego do $K_i[x]$, gdy char K = 0, 2/ $K_{i+1}$ jest ciałem rozkładu wielomianu postaci $x^n - a$ bądź $x^p - x - a$ należącego do $K_i[x]$, gdy char $K = p \neq 0$.

Dla pewnych szczególnych ciał K znane są inne twierdzenia tego typu. Na przykład:

Twierdzenie 8. Jeżeli K jest rozszerzeniem rozdzielczym ciała liczb p-adycznych $Q_p$ lub ciała szeregów formalnych $k((x))$, gdzie k jest ciałem skończonym, to grupa $G(K_s/K)$ jest rozwiązalna.

Zatem w tym przypadku największym rozszerzeniem rozwiązalnym ciała K, o którym jest mowa w poprzednim twierdzeniu, jest całe ciało $K_s$.

Twierdzenie 9. Grupa $G(Q_s/Q)$ nie jest rozwiązalna.

Nietrudno dowieść, że dla dowolnego ciała K istnieje największe rozszerzenie Galois takie, że grupa $G(L/K)$ jest abelowa. To ciało L oznaczamy przez $K_{ab}$. Dla pewnych ciał K można efektywnie opisać ciało $K_{ab}$. Na przykład:

Twierdzenie 10 /L. Kronecker, H. Weber/. Największe rozsze-

rzenie abelowe $Q_{ab}$ ciała liczb wymiernych Q powstaje z ciała Q przez dołączenie wszystkich pierwiastków z 1, tzn. $Q_{ab} = Q/A/$, gdzie $A = \{\zeta_n : n = 1,2,\ldots , \zeta_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}\}$.

Analogiczne twierdzenie jest prawdziwe w przypadku ciała liczb p - adycznych:

**Twierdzenie 11.** Największe rozszerzenie abelowe ciała $Q_p$ powstaje z ciała $Q_p$ przez dołączenie wszystkich pierwiastków z 1.

**Twierdzenie 12.** Jeżeli ciało k jest algebraicznie domknięte oraz $K = k((x))$ jest ciałem szeregów formalnych zmiennej x, to ciało $K_{ab}$ powstaje z ciała K przez dołączenie wszystkich pierwiastków z x, tzn. $K_{ab} = K/A/$, gdzie $A = \{x^{1/n} : n = 1,2,\ldots$

**Twierdzenie 13.** Jeżeli ciało K jest skończone, to $K_{ab} = K_s$ jest algebraicznym domknięciem ciała K. Ponadto $G(K_s/K) = \hat{Z} = \varprojlim Z/nZ$.

Podamy jeszcze kilka twierdzeń podobnego typu dotyczących rozszerzeń skończonych. Najpierw skończona wersja twierdzenia Kroneckera-Webera:

**Twierdzenie 10.** Jeżeli L jest skończonym rozszerzeniem Galois ciała Q i grupa G(L/Q) jest abelowa, to $L \subset Q(\zeta_n)$ dla pewnego n.

**Twierdzenie 14 /Lagrange/.** Jeżeli L jest rozszerzeniem Galois stopnia n ciała K /a w przypadku, gdy char $K = p \neq 0$ zakładamy jeszcze, że $p \nmid n$/ oraz $\zeta_n \in K$ i grupa G(L/K) jest cykliczna, to $L = K(\sqrt[n]{a})$ dla pewnego $a \in K$.

**Twierdzenie 15 /E. Artin, Schreier/.** Jeżeli char $K = p \neq 0$ oraz L jest rozszerzeniem Galois stopnia p ciała K i grupa G(L/K) jest cykliczna, to L powstaje z K przez dołączenie pierwiastka wielomianu postaci $x^p - x - a$, gdzie $a \in K$.

Wspomnijmy jeszcze o tzw. zagadnieniu odwrotnym teorii Galois. Chodzi w nim o to, by dla danego ciała K opisać grupy G(L/K), gdzie L przebiega wszystkie rozszerzenia Galois ciała K /lub wszystkie rozszerzenia Galois i skończone ciała K/. Innymi słowy, chodzi o opisanie wszystkich grup /odpowiednio:

grup skończonych/, które są obrazami przy homomorfizmach grupy $G(K_s/K)$.

Do dziś na przykład nie wiadomo, czy każda grupa skończona jest izomorficzna z grupą Galois pewnego rozszerzenia Galois ciała liczb wymiernych.

Dla niewielkiej klasy ciał K znany jest opis zbioru grup Galois skończonych rozszerzeń Galois tych ciał. Na przykład, jeżeli K jest ciałem skończonym, to ta klasa grup składa się ze wszystkich grup cyklicznych skończonych; jeżeli zaś każdy wielomian stopnia nieparzystego należący do $K[x]$ ma pierwiastek w ciele K /a więc na przykład K jest ciałem liczb rzeczywistych/, to ta klasa grup składa się z grupy jedno- i dwuelementowej, albo tylko z grupy jednoelementowej.

Trochę dokładniej odwrotne zagadnienie teorii Galois ujmuje tzw. teoria zanurzeń. Zajmuje się ona następującą sytuacją. Dane jest rozszerzenie Galois L ciała K oraz pewna grupa G wraz z homomorfizmem $\varphi : G \longrightarrow G(L/K)$. Czy istnieje takie rozszerzenie Galois M ciała K zawierające L oraz izomorfizm $\lambda : G(M/K) \longrightarrow G$, że homomorfizm $\varphi \circ \lambda : G(M/K) \longrightarrow G(L/K)$ był równy odpowiedniemu homomorfizmowi z teorii Galois polegającemu na ograniczeniu K-izomorfizmów ciała M do podciała L?

Istnieje szereg twierdzeń teorii zanurzeń, które dla odpowiednich ciał K podają warunki dostateczne dla otrzymania pozytywnej odpowiedzi na postawione pytanie. W wielu jednak przypadkach odpowiedź jest negatywna.

Znaczenie teorii Galois w nauczaniu matematyki polega, jak sądzę, nie tylko na tym, że ma ona zastosowania w różnych działach algebry /przede wszystkim w teorii ciał, lecz także w teorii modułów, teorii grup, geometrii algebraicznej, algebrze homologicznej, algebraicznej teorii liczb/, lecz również na tym, że do jej studiowania i posługiwania się nią potrzebna jest znajomość podstawowych faktów z innych działów algebry /z teorii ciał, teorii pierścieni, grup, modułów, grup topologicznych/.

Teoria Galois dostarcza więc interesujących przykładów za-

stosowań nietrywialnych faktów z teorii grup, ciał itd. Student ma więc możność przekonania się, że pozornie formalne tylko twierdzenia /ustalające pewne podstawowe zależności między pojęciami np. teorii grup/ mają zastosowania dla badania trudnych i głębokich zagadnień teorii ciał.

W teorii Galois jest też wiele otwartych problemów o podstawowym znaczeniu i różnych stopniach trudności, przy badaniu których początkujący matematyk może z pożytkiem spróbować swych sił.

Co z tego wszystkiego powinno znaleźć się w wykładzie algebry abstrakcyjnej dla matematyków i w wykładzie algebry dla nauczycieli? Uważam, że treści podawane studentom kierunku teoretycznego i nauczycielskiego mogą być te same, z tym, że w zależności od słuchaczy nieco inaczej mogą być rozłożone akcenty.

Wiadomości z algebry, które student powinien opanować przez studiowaniem teorii Galois:

Z teorii grup: Wiadomości podstawowe aż do teorii grup rozwiązalnych, włączając twierdzenia Sylowa, własności komutanta. informacje o budowie grup abelowych skończenie generowanych.

Z teorii pierścieni: Własności podstawowe włączając własności ideałów maksymalnych i pierwszych oraz własności pierścienia wielomianów jednej zmiennej o współczynnikach w ciele.

Z teorii ciał: Wiadomości podstawowe, rozszerzenie o pierwiastek wielomianu, ciało rozkładu, własności elementów algebraicznych, elementy rozdzielcze. Domknięcie algebraiczne i domknięcie rozdzielcze. Przykłady ciał: Ciała skończone, skończone rozszerzenia ciała liczb wymiernych, ciała funkcji wymiernych, ciało szeregów formalnych, ewentualnie ciało liczb p-adycznych, ciało liczb rzeczywistych i ciało liczb zespolonych, algebraiczna domkniętość tego ostatniego ciała.

Wykład teorii Galois powinien obejmować następujące tematy:

1. Własności automorfizmów ciał - twierdzenie o niezależności automorfizmów, związki między liczbą automorfizmów a stop-

niem rozszerzenia.

2. Rozszerzenia normalne a rozszerzenia Galois. Automorfizmy a permutacje zbioru pierwiastków wielomianu.

3. Zasadnicze twierdzenia teorii Galois podane w wersji skończonej lub nieskończonej.

4. Zastosowania do badania rozwiązalności równań w pierwiastnikach tzn. charakteryzacja rozszerzeń skończonych Galois o rozwiązalnej grupie Galois.

5. Informacje o innych wynikach i zagadnieniach tej teorii.

Wykład ten powinien być bogato ilustrowany nietrywialnymi przykładami, o co w tej teorii nietrudno.

Uważam też, że ograniczanie wykładu teorii Galois do przypadku ciał charakterystyki zero jest sztuczne i niczym nie uzasadnione. Z drugiej strony, by nie wdawać się w trudności techniczne lub zjawiska patologiczne można

a/ W wykładzie zasadniczych twierdzeń teorii Galois przyjąć założenie, że każdy wielomian nierozkładalny ma pierwiastki jednokrotne i zauważyć, że wiele ciał spełnia ten warunek,

b/ W wykładzie rozwiązalności równań w pierwiastnikach ograniczyć się do ciał charakterystyki zero.

Jeżeli chodzi o podręczniki zawierające wykład teorii Galois, to przede wszystkim należy polecić piękną i zwięzłą książkę E. Artina "Galois Theory". W języku polskim oprócz dodatku A. Mostowskiego do książki W. Sierpińskiego "Zasady algebry wyższej" trzeci tom "Algebry wyższej" A. Mostowskiego i M. Starka zawiera wykład teorii Galois. Również tę tematykę obejmuje podręcznik Langa "Algebra". Wreszcie w pierwszych trzech rozdziałach mojej "Teorii ciał" przedstawiona jest teoria Galois w nieco ulepszonej wersji w stosunku do ujęcia podanego w "Wybranych zagadnieniach algebry". Istnieje też skrypt W. Więsława wydany przez Uniwersytet Wrocławski.

# THE MEANING OF GALOIS THEORY IN MODERN MATHEMATICS AND ITS ROLE IN THE EDUCATION OF YOUNG MATHEMATICIANS

**Summary**

**In the paper there are mentioned some applications of the Galois theory in several branches of algebra.**

# ЗНАЧЕНИЕ ТЕОРИИ ГАЛУА В СОВРЕМЕННОЙ МАТЕМАТИКЕ И ЕЕ РОЛЬ В ОБУЧЕНИИ СТУДЕНТОВ

Резюме

В работе приведены некоторые примеры приложений теории Галуа разных областях алгебры.