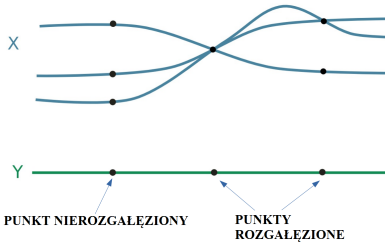
Kohomologia de Rhama nakryć p-grupowych
OPIS POPULARNONAUKOWY

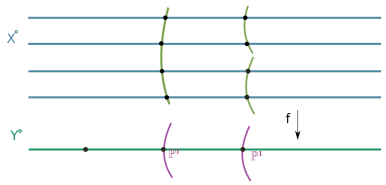
Jędrzej Garnek

Głównym tematem moich badań są *krzywe algebraiczne* (jednowymiarowe zbiory określone przez równania wielomianowe) i ich symetrie. Współczynniki wielomianów definiujących krzywą mogą należeć do zbioru liczb zespolonych, rzeczywistych lub wymiernych, ale także np. do $\mathbb{F}_p$, gdzie p jest ustaloną liczbą pierwszą. Przypomnijmy, że $\mathbb{F}_p$ jest zbiorem reszt z dzielenia przez p z działaniami dodawania i mnożenia modulo p. Krzywe określone nad $\mathbb{F}_p$ są szczególnie ważne z punktu widzenia kryptografii. Te z nich, które mają wiele symetrii, są, w zależności od sytuacji, szczególnie pożądane, albo też unikane.

Następujące pojęcia będą kluczowe do zrozumienia uzyskanych wyników: *grupa*, *reprezentacja* i *kohomologia*. Pojęcie *grupy* lub też *działania grupy* formalizuje pojęcie symetrii obiektu. Wybór zbioru symetrii krzywej X (tzn. działania grupy na X) jest równoważny z zadaniem „ładnego" odwzorowania (zwanego *nakryciem rozgałęzionym*) z X do innej krzywej Y. W nakryciu nad prawie każdym punktem krzywej Y znajduje się ta sama liczba punktów krzywej X. Pozostałe punkty nazywamy *punktami rozgałęzienia* (patrz Rysunek 1). Kolejnym ważnym pojęciem jest *reprezentacja grupy*. Reprezentacja koduje elementy grupy („symetrie") jako macierze. Mimo że reprezentacje rzeczywiste oraz zespolone są dobrze zrozumiane, reprezentacje nad $\mathbb{F}_p$ są uważane za niemożliwe do sklasyfikowania w większości przypadków. *Kohomologia* to klasyczny niezmiennik rozmaitości topologicznych oraz algebraicznych. W topologii kohomologie pozwalają na zliczanie „dziur" zadanej rozmaitości. Intuicja ta nie jest poprawna nad $\mathbb{F}_p$, jednak istnieje sposób na zdefiniowanie kohomologii krzywej modulo p. Jako że działanie dowolnej symetrii na krzywej X określa macierz działającą na kohomologii, otrzymujemy reprezentację rozpatrywanej grupy.



Rysunek 1: Nakrycie krzywych.



Rysunek 2: Nakrycie z rysunku 1 można przybliżyć za pomocą nakryć Harbatera–Katza–Gabbera (krzywe pionowe) i trywialnego nakrycia

Dwa pierwsze z uzyskanych wyników dotyczą krzywych nad $\mathbb{F}_p$. Mój główny rezultat pokazuje, że dla większości krzywych reprezentacja pochodząca od kohomologii rozkłada się na sumę części globalnej (zależącej tylko od „kształtu" nakrycia) oraz części lokalnych. Części lokalne mogą być opisane jako kohomologie *nakryć Harbatera–Katza–Gabbera*, tzn. nakryć prostej rozgałęzionych tylko nad jednym punktem, które przybliżają daną krzywą (patrz Rysunek 2). Uzyskany wynik ma wiele możliwych zastosowań. Przykładowo, mając daną grupę G, można zastanawiać się jakie reprezentacje powstają z kohomologii wszystkich możliwych krzywych z działaniem G. Pytanie to wydaje się być bardzo trudne, ale udowodniłem (korzystając z powyższych wyników), że prawie zawsze istnieje nieskończenie wiele „cegiełek" z których zbudowane są kohomologie. Sugeruje to, że świat reprezentacji pochodzących od krzywych algebraicznych jest tak bogaty, jak świat wszystkich reprezentacji nad $\mathbb{F}_p$.

By wytłumaczyć ostatni z wyników, przypomnijmy że każda krzywa zanurza się w *Jakobian*, tzn. rozmaitość której punkty można dodawać w algebraiczny sposób. Każdy Jakobian dostarcza nam reprezentacji absolutnej grupy Galois liczb wymiernych (jednego z najważniejszych obiektów w teorii liczb). Reprezentacje te grają kluczową rolę np. w dowodzie hipotezy Fermata oraz w programie Langlandsa (zbiorze daleko idących hipotez dotyczących związków między teorią liczb a geometrią). Jak przewiduje hipoteza Mumforda–Tate'a, obraz reprezentacji związanej z Jakobianem powinien być kontrolowany przez kształt krzywej. Hipoteza ta może być również postrzegana jako pomost między dwoma innymi ważnymi otwartymi problemami z geometrii arytmetycznej – hipotezą Tate'a oraz hipotezą Hodge'a (jednym z siedmiu problemów milenijnych). W trakcie projektu zajmowałem się krzywymi postaci $y^\ell = f(x)$, gdzie ℓ jest liczbą pierwszą, zaś $f(x)$ to wielomian o współczynnikach wymiernych. Udało mi się pokazać, że hipotezy Mumforda–Tate'a, Hodge'a oraz Tate'a *zazwyczaj* zachodzą dla tych krzywych.