KOHOMOLOGIA DE RHAMA NAKRYć p-GRUPOWYCH OPIS POPULARNONAUKOWY (WYDŁUŻONY)

JĘDRZEJ GARNEK

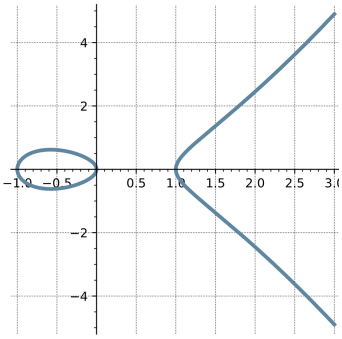
1. „Symetrie” krzywych

W wielu dziedzinach nauki badamy rozmaite obiekty, uwzględniając ich symetrie jako ważną część ich struktury. Filozofia ta znajduje zastosowanie np. gdy rozważamy cząsteczkę chemiczną lub układ fizyczny. W wielu przypadkach pozwala to na lepsze zrozumienie badanych obiektów. W matematyce takie podejście formalizuje się, używając takich pojęć jak **grupa**, **działanie grupy na zbiorze** lub **reprezentacja grupy**.

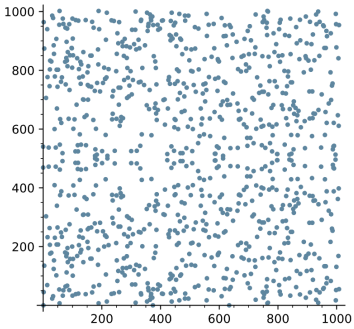
Projekt ten dotyczyć będzie symetrii krzywych algebraicznych, tzn. jednowymiarowych obiektów zadanych równaniami wielomianowymi, np.

$$(*) \qquad y^2 = x^3 - x.$$

W projekcie będę się jednak zajmował krzywymi modulo p, gdzie p jest pewną liczbą pierwszą. Oznacza to, że równanie ma być spełnione tylko z dokładnością do pewnej wielokrotności liczby p. Przykładowo, punkt $(x, y) = (662, 578)$ należy do krzywej o równaniu $(*)$ modulo 1009, jako że $578^2 = 662^3 - 662 + 287198 \cdot 1009$.



“Klasyczna” krzywa $y^2 = x^3 - x$



Krzywa $y^2 = x^3 - x$ modulo 1009

Na lewym rysunku widzimy krzywą klasyczną, zaś na prawym – krzywą z tym samym równaniem modulo 1009. Zauważmy, że obie krzywe mają pewną symetrię (i w tym przypadku jest to dosłownie symetria odpowiadającego obrazka – symetria wg osi poziomej).

Krzywe modulo p mają duże znaczenie w matematyce – przykładowo słynna hipoteza Riemanna, wciąż nie rozwiązana w klasycznym przypadku, jest znana dla krzywych modulo p. Krzywe modulo liczby pierwsze mają również

liczne zastosowania w kryptografii – służą one m.in. do szyfrowania wiadomości, do konstrukcji kodów poprawiających błędy, a także zapewniają metodę cyfrowego podpisu plików.

2. Kohomologie

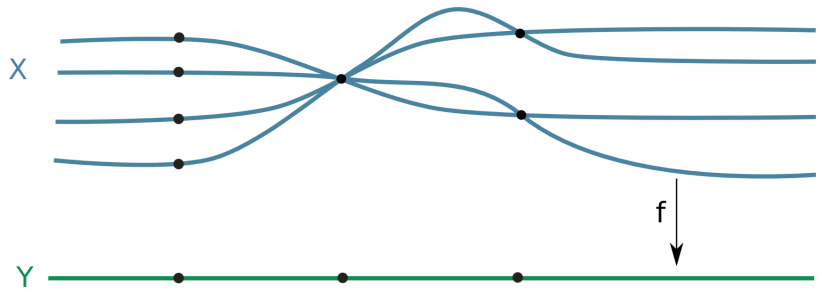
Istnieją wiele niezmienników krzywych, które pozwalają je rozróżnić i dostarczają informacji o krzywych. Projekt dotyczy dwóch takich niezmienników:

- **kohomologii de Rhama**: $H^1_{dR}(X)$,
- **kohomologii Hodge'a**: $H^1_{Hdg}(X)$.

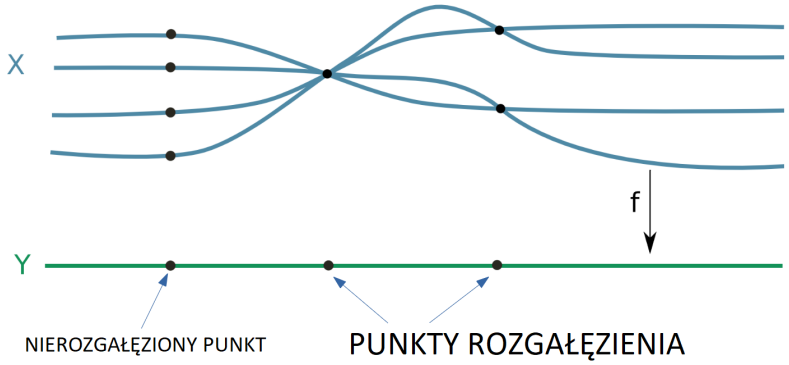
Obydwa niezmienniki są pewnymi przestrzeniami wektorowymi. Dla klasycznych krzywych obie teorie kohomologii pokrywają się, ale dla krzywych modulo p nie jest to prawda. Jeżeli rozpatrywana krzywa ma symetrie, to działają one również na kohomologiach. Celem projektu jest zrozumienie tych niezmienników, uwzględniając działanie symetrii na nich.

3. Punkty rozgałęzienia

Aby wytłumaczyć hipotezę związaną z kohomologiami, muszę opowiedzieć o pojęciu **punktu rozgałęzienia**. Zamiast rozważać krzywą X z pewnym zbiorem symetrii, możemy równoważnie badać **nakrycie krzywych** $f : X \to Y$. Krzywa Y jest wówczas przestrzenią orbit, tzn. powstaje z krzywej X przez utożsamienie symetrycznych punktów. Na rysunku widzimy przykładową sytuację, gdy rozpatrujemy krzywą X wraz z czterema symetriami.



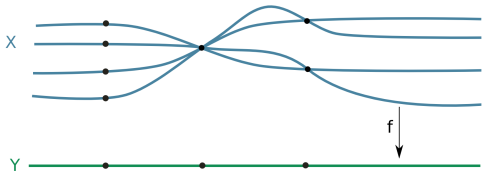
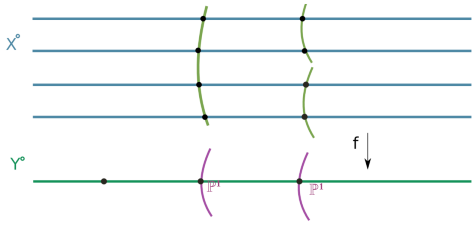
Zauważmy, że nad prawie każdym punktem Y znajdują się cztery punkty krzywej X. Pozostałe, „wyjątkowe" punkty nazywamy **punktami rozgałęzienia**. W taki sam sposób definiuje się punkty rozgałęzienia, gdy symetrii jest więcej.



4. Hipoteza

Moje poprzednie wyniki sugerują, że kohomologia de Rhama rozkłada się na sumę pewnych części globalnych i lokalnych. Część globalna powinna zależeć tylko od „topologii" nakrycia (tzn. od rysunku nakrycia – takiego, jaki przedstawiłem powyżej), podczas gdy części lokalne powinny zależeć tylko od małego otoczenia punktów rozgałęzienia nakrycia. Ponadto, części globalne kohomologii de Rhama i kohomologii Hodge'a powinny być takie same. Mówiąc krótko, kohomologie te powinny różnić się tylko częściami lokalnymi! Hipotetycznie części lokalne można opisać za pomocą nakryć Harbatera-Katza-Gabbera, tzn. nakryć prostej które są rozgałęzione tylko w jednym punkcie.

Hipoteza ta ma przyjemną interpretację geometryczną. Mianowicie, oznacza ona, że kohomologia nakrycia:



powinna być taka sama jak kohomologia zdegenerowanego nakrycia przybliżającego je: