Krzywe i ich symetrie

Jędrzej Garnek

Analogia

Rozważmy liczby Fibonacciego:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n$$

Są to kolejno:

$$0, 1, 1, 2, 3, 5, 8, 13, \quad \ldots$$

Pytanie

Czy to możliwe, że wszystkie te liczby są postaci:

$$2^a \cdot 3^b \cdot 5^c \cdot 13^d?$$

(tzw. liczby 13-gładkie)

Analogia

Rozważmy liczby Fibonacciego:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n$$

Są to kolejno:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

Pytanie

Czy to możliwe, że wszystkie te liczby są postaci:

$$2^a \cdot 3^b \cdot 5^c \cdot 13^d?$$

(tzw. liczby 13-gładkie)

Analogia

Rozważmy liczby Fibonacciego:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n$$

Są to kolejno:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

Pytanie

Czy zbiór:

$$\mathrm{CEGIEŁKI}((F_n)_n) := \{p \in \mathbb{P} : p | F_n \text{ dla pewnego } n\}$$

jest skończony?

Analogia

Rozważmy liczby Fibonacciego:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_{n+1} + F_n$$

Są to kolejno:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

Pytanie

Czy zbiór:

$$\mathrm{CEGIEŁKI}((F_n)_n) := \{p \in \mathbb{P} : p | F_n \text{ dla pewnego } n\}$$

jest skończony?

Twierdzenie Carmichaela (1913): NIE!

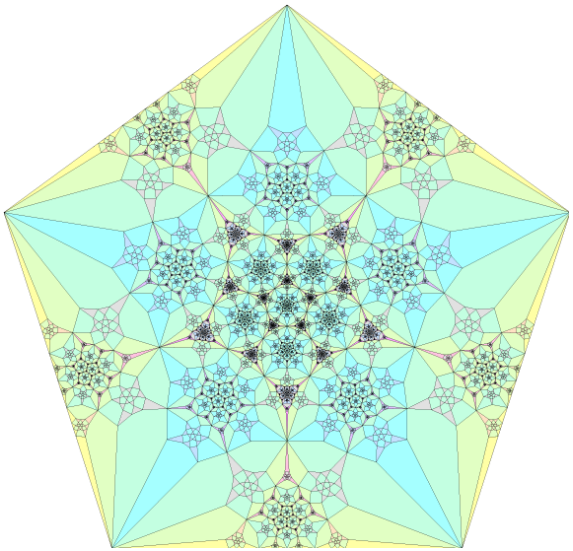
Co będziemy potrzebować do zrozumienia właściwego problemu?

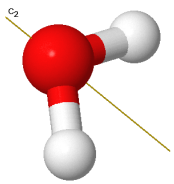
- reprezentacja grupy,
- krzywa algebraiczna,
- kohomologie.

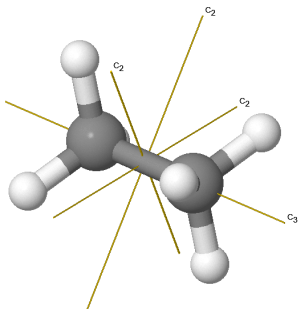
Symetrie

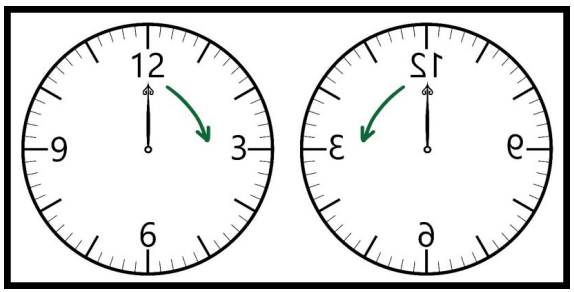
W wielu dziedzinach nauki badamy rozmaite obiekty, uwzględniając ich symetrie jako ważną część ich struktury. Filozofia ta znajduje zastosowanie np. gdy rozważamy cząsteczkę chemiczną lub układ fizyczny.

W matematyce takie podejście formalizuje się, używając takich pojęć jak **grupa**, **działanie grupy na zbiorze** lub **reprezentacja grupy**.









Działanie grupy na zbiorze

$$G \times X \to X, \qquad (g, x) \mapsto g \cdot x,$$

gdzie:

- $g \cdot (h \cdot x) = (g \cdot h) \cdot x$,
- $e \cdot x = x$.

Przykłady:

- D_{2n} działa na zbiorze wierzchołków n-kąta foremnego,
- S_n działa na zbiorze $\{1, \ldots, n\}$,
- grupa macierzy odwracalnych $\mathrm{Gl}_n(\mathbb{R})$ działa na $\mathbb{R}^n$.

Reprezentacja grupy

Trzy definicje o różnym stopniu trudności ☺

Reprezentacja grupy

Trzy definicje o różnym stopniu trudności ☺

- zakodowanie każdego elementu grupy jako pewną macierz,

Reprezentacja grupy

Trzy definicje o różnym stopniu trudności ☺

- zakodowanie każdego elementu grupy jako pewną macierz,
- działanie G na $\mathbb{R}^n$ takie, że dla $v, v_1, v_2 \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$:

$$g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2, \quad g \cdot (\alpha v) = \alpha \cdot (g \cdot v)$$

Reprezentacja grupy

Trzy definicje o różnym stopniu trudności ☺

- zakodowanie każdego elementu grupy jako pewną macierz,
- działanie G na $\mathbb{R}^n$ takie, że dla $v, v_1, v_2 \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$:

$$g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2, \quad g \cdot (\alpha v) = \alpha \cdot (g \cdot v)$$

- homomorfizm $f : G \to \mathrm{Gl}_n(\mathbb{R})$.

Reprezentacja grupy

Trzy definicje o różnym stopniu trudności ☺

- zakodowanie każdego elementu grupy jako pewną macierz,
- działanie G na $\mathbb{R}^n$ takie, że dla $v, v_1, v_2 \in \mathbb{R}^n$, $\alpha \in \mathbb{R}$:

$$g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2, \quad g \cdot (\alpha v) = \alpha \cdot (g \cdot v)$$

- homomorfizm $f : G \to \mathrm{Gl}_n(\mathbb{R})$.

Współczynniki macierzy mogą należeć np. do $\mathbb{C}, \mathbb{F}_p$ lub $\overline{\mathbb{F}}_p$.

Przykład:
dla $G = \mathbb{Z}/n$ reprezentacja jest wyznaczona przez dowolną macierz $A \in M_d(\mathbb{C})$ taka, że

$$A^n = I_d.$$

Przykładowo:

$$A = \mathrm{diag}(\zeta_n^{k_1}, \ldots, \zeta_n^{k_d}).$$

Przykład:

$$G = D_{2n} = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$
$$= \langle s, r : r^n = e, s^2 = e, \quad srs = r^{-1} \rangle$$

Reprezentacja:

$$s \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$r \mapsto \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix}.$$

Przykład:

$$G = S_3$$

Reprezentacja V:

$$(1,2,3) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

$$(1,2) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

(tzn. $\sigma \cdot (x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)})$)

Po co nam reprezentacje

- pomagają lepiej zrozumieć badany obiekt, uwzględniając jego symetrie,
- pomagają lepiej zrozumieć grupę.

Reprezentacje można jednoznacznie rozłożyć na „cegiełki”
– reprezentacje nierozkładalne.

Przykład: dla $G = S_3$, $V = \mathbb{R}^3$:

$$\begin{aligned} V &= \{(a,a,a) : a \in \mathbb{R}\} \oplus \{(x_1,x_2,x_3) \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\} \\ &= V_1 \oplus V_2, \end{aligned}$$

Reprezentacje można jednoznacznie rozłożyć na „cegiełki”
– reprezentacje nierozkładalne.

Przykład: dla $G = S_3$, $V = \mathbb{R}^3$:

$$\begin{aligned} V &= \{(a,a,a) : a \in \mathbb{R}\} \oplus \{(x_1,x_2,x_3) \in \mathbb{R}^3 : x_1 + x_2 + x_3 = 0\} \\ &= V_1 \oplus V_2, \end{aligned}$$

gdzie $\dim V_1 = 1$, $\dim V_2 = 2$.

Reprezentacje można jednoznacznie rozłożyć na „cegiełki”
– reprezentacje nierozkładalne.

Przykład:
dla $G = \mathbb{Z}/n$ istnieje n reprezentacji nierozkładalnych nad $\mathbb{C}$. Są one wymiaru 1. Mają postać:

$$V_k : \quad \mathbb{Z}/n \ni \qquad 1 \mapsto [\zeta_n^k] \qquad \in M_1(\mathbb{C})$$

dla $k = 0, \ldots, n$.
Reprezentacja zadana przez $A = \mathrm{diag}(\zeta_n^{k_1}, \ldots, \zeta_n^{k_d})$ rozkłada się na:

$$V_{k_1} \oplus \ldots \oplus V_{k_d}.$$

Reprezentacje można jednoznacznie rozłożyć na „cegiełki”
– reprezentacje nierozkładalne.

Przykład:
dla $G = \mathbb{Z}/p$ istnieje p reprezentacji nierozkładalnych nad $\mathbb{F}_p$. Mają postać:

$$\mathbb{Z}/p \ni \qquad 1 \mapsto \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \in M_k(\mathbb{F}_p)$$

dla $k = 0, \ldots, p$.

Reprezentacje można jednoznacznie rozłożyć na „cegiełki”
– reprezentacje nierozkładalne.

Przykład:
dla $G = \mathbb{Z}/p \times \mathbb{Z}/p$ istnieje nieskończenie wiele reprezentacji nad $\mathbb{F}_p$.
Wiadomo, że

Reprezentacje można jednoznacznie rozłożyć na „cegiełki”
– reprezentacje nierozkładalne.

Przykład:
dla $G = \mathbb{Z}/p \times \mathbb{Z}/p$ istnieje nieskończenie wiele reprezentacji nad $\mathbb{F}_p$.
Wiadomo, że NIE DA SIĘ ICH SKLASYFIKOWAĆ!

Krzywe algebraiczne

Obiektem moich badań są **krzywe algebraiczne**, tzn. jednowymiarowe obiekty zadane przez równania wielomianowe, np. $y^2 = x^3 - x$.

Będziemy rozważali krzywe:

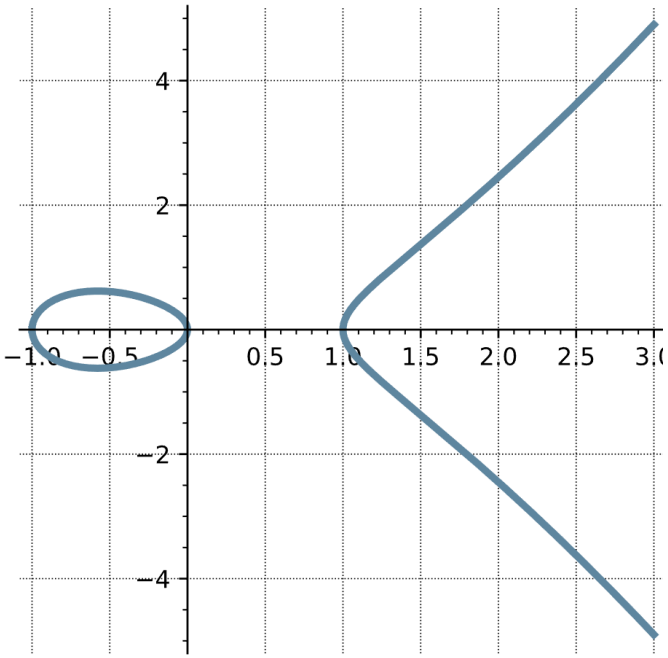
- modulo liczba pierwsza

  (= „skończone” krzywe)
- rzutowe

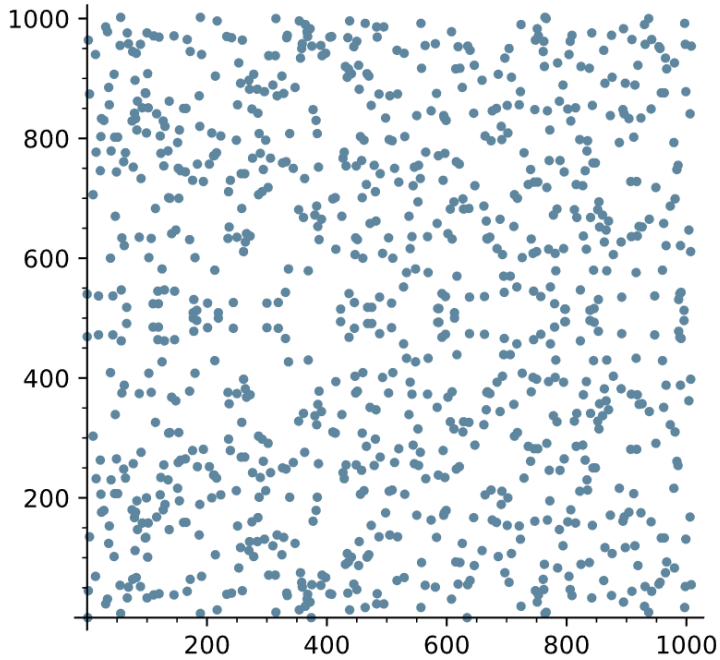
  (= krzywe, którym nie brakuje punktów)
- gładkie

  (= bez „ostrzy”)

Krzywe modulo p



"Klasyczna" krzywa $y^2 = x^3 - x$

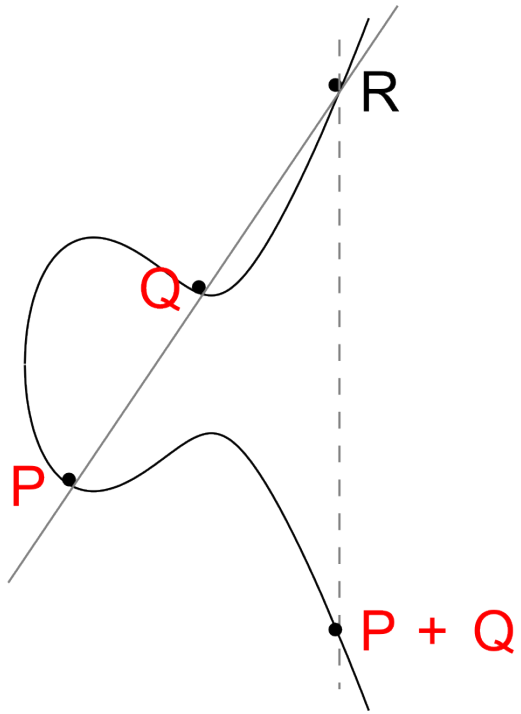


Krzywa $y^2 = x^3 - x$ modulo 1009

Krzywe modulo liczby pierwsze mają liczne zastosowania w kryptografii: zarówno przy szyfrowaniu i zapewnianiu elektronicznych podpisów, jak i przy konstrukcji kodów poprawiających błędy.

Przykład: krzywe eliptyczne

Krzywa $y^2 = x^3 - x$ stanowi przykład **krzywej eliptycznej**. Punkty na tych krzywych można dodawać:



Zbiór punktów krzywej eliptycznej stanowi **grupę przemienną**. Obserwacja ta prowadzi do zastosowań w kryptografii (np. algorytm ElGamal).

Krzywe rzutowe

Krzywe, które będziemy rozważali, pochodzą ze sklejenia kilku krzywych.

Krzywa $y^2 = x^3 - x$ nie jest rzutowa – brakuje jej jednego "punktu w nieskończoności". Staje się ona rzutowa po doklejeniu do niej krzywej

$$w^2 = u - u^3$$

za pomocą utożsamień $u = 1/x$, $w = y/x^2$.
Brakujący punkt to punkt $(u, w) = (0, 0)$.

Krzywa rzutowa – krzywa sklejona z kilku krzywych, która nie ma dziur.

Symetrie krzywych

Mówiąc o działaniu grupy na krzywej, chcemy, żeby było ono algebraiczne.

Symetrie krzywych

Mówiąc o działaniu grupy na krzywej, chcemy, żeby było ono algebraiczne.

Krzywe nad $\mathbb{F}_p$ mogą mieć bardzo dużo symetrii!

Symetrie krzywych

Mówiąc o działaniu grupy na krzywej, chcemy, żeby było ono algebraiczne.

Krzywe nad $\mathbb{F}_p$ mogą mieć bardzo dużo symetrii!

Powód:

$$y^p - y = f(x)$$

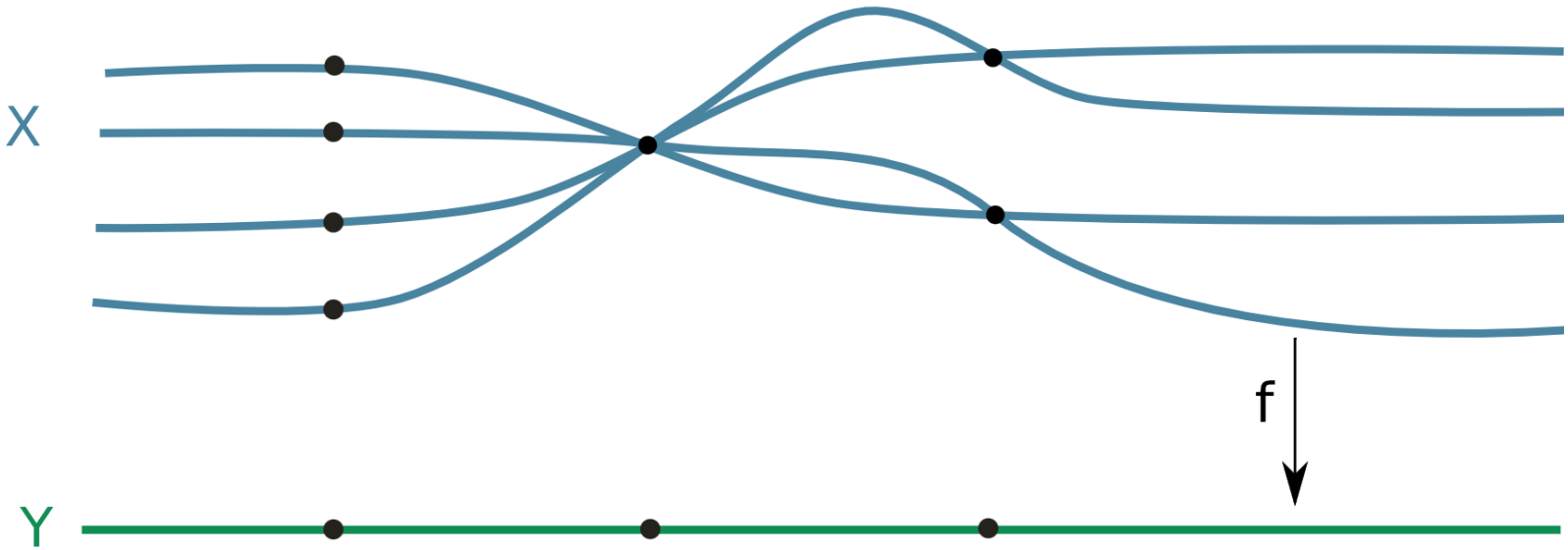
ma symetrię rzędu p:

$$(x, y) \mapsto (x, y + 1).$$

Spojrzenie geometryczne

Rozważanie krzywej X wraz z działaniem grupy G jest równoważne z rozważaniem **nakrycia krzywych** $f : X \to Y$ (gdzie $Y := X/G$).

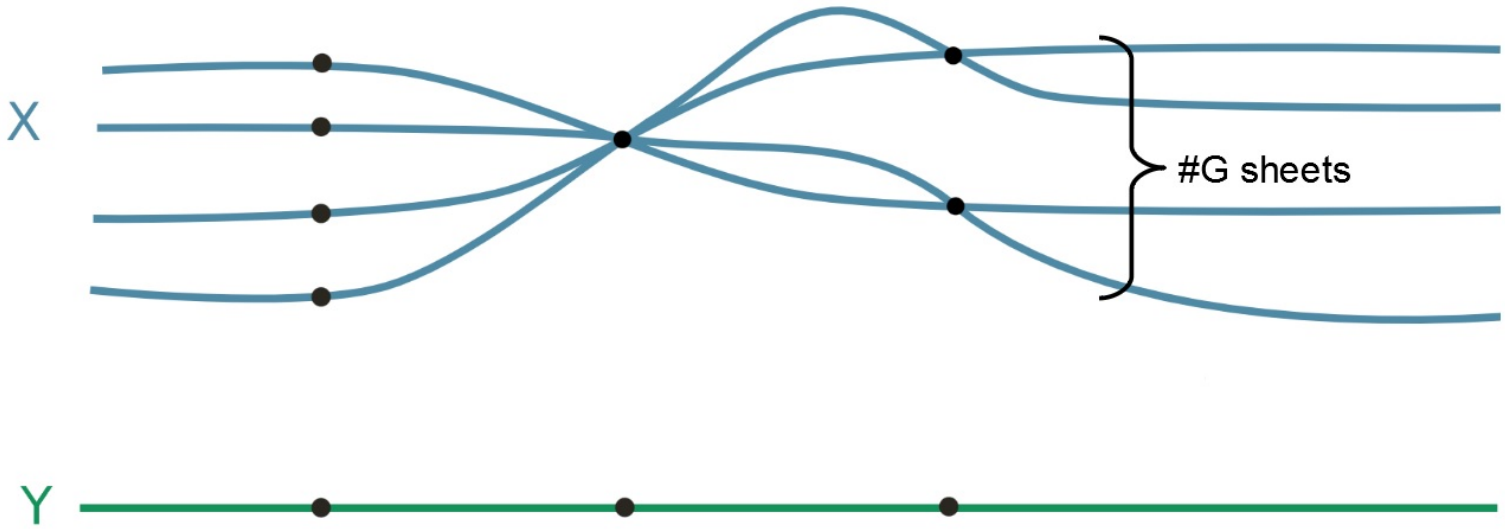
Krzywa Y jest wtedy przestrzenią orbit działania, tzn. utożsamiamy ze sobą "symetryczne punkty".



Spojrzenie geometryczne

Rozważanie krzywej X wraz z działaniem grupy G jest równoważne z rozważaniem **nakrycia krzywych** $f : X \to Y$ (gdzie $Y := X/G$).

Na obrazku widzimy przypadek $\#G = 4$.

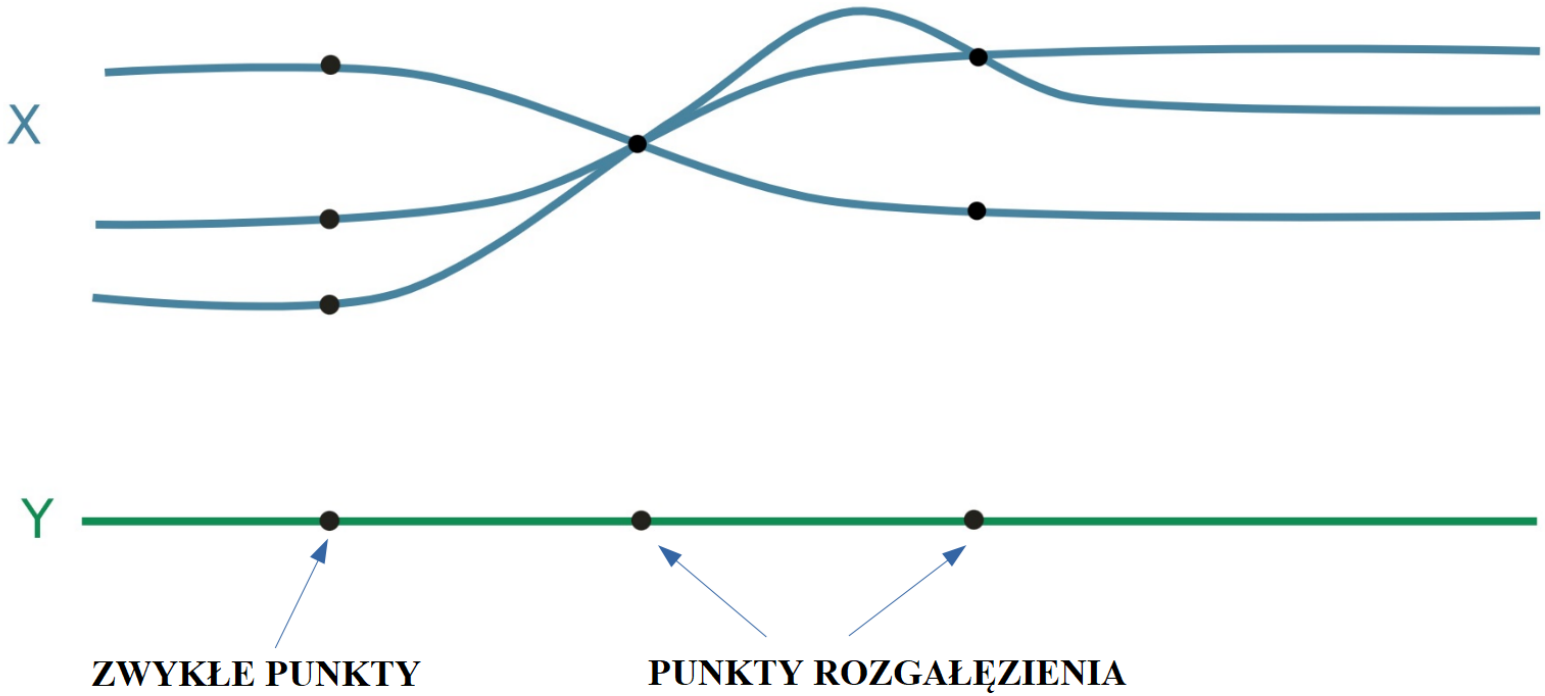


Spojrzenie geometryczne

Rozważanie krzywej X wraz z działaniem grupy G jest równoważne z rozważaniem **nakrycia krzywych** $f : X \to Y$ (gdzie $Y := X/G$).

Zauważmy, że:

- nad prawie każdym punktem Y są $\#G$ punkty X,
- pozostałe punkty to tzw. **punkty rozgałęzienia**.

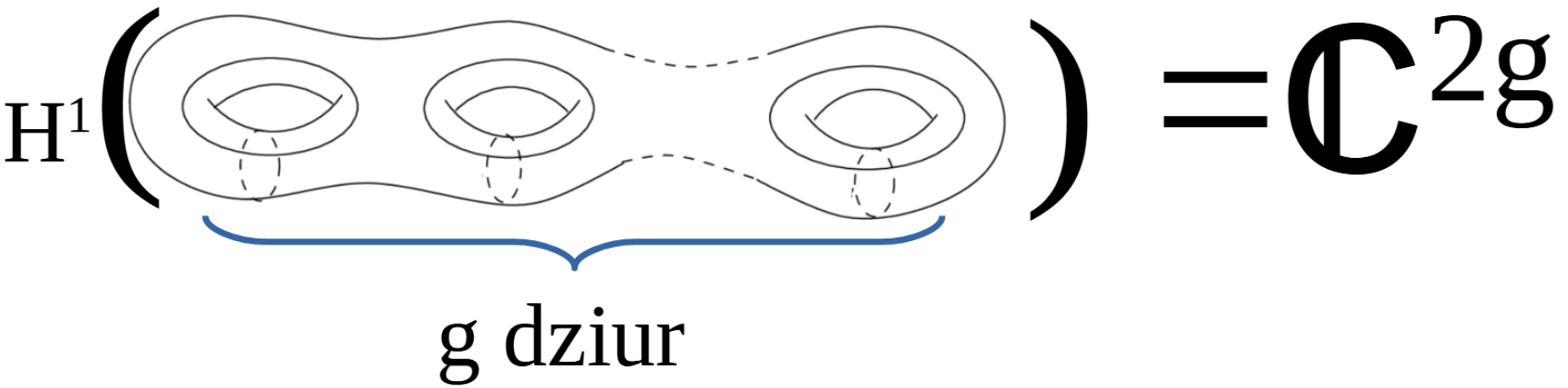


Kohomologie

Rozważmy dwa niezmienniki krzywych:

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

Obydwa niezmienniki są pewnymi przestrzeniami wektorowymi.



Kohomologie

$$\begin{array}{ll} G \circlearrowright & X - \text{krzywa algebraiczna} \\ & \downarrow \\ G \circlearrowright & H^1_{Hdg}(X), H^1_{dR}(X) - \text{niezmienniki krzywej} \end{array}$$

Problem

Zrozumieć strukturę $H^1_{dR}(X)$ oraz $H^1_{Hdg}(X)$, uwzględniając "symetrie" krzywej X.

(czyli zrozumieć $H^1_{dR}(X)$ oraz $H^1_{Hdg}(X)$ jako reprezentacje grupy G)

Funkcje i formy na krzywej

- funkcje (z biegunami): $\mathbb{C}(x, y)$, gdzie $y^2 = x^3 - x$,
- funkcje regularne poza punktem w nieskończoności: $\mathbb{C}[x, y]$,
- funkcja y/x^3 jest regularna w punkcie w nieskończoności, bo

$$\frac{y}{x^3} = uw$$

Funkcje i formy na krzywej

- funkcje (z biegunami): $\mathbb{C}(x, y)$, gdzie $y^2 = x^3 - x$,
- funkcje regularne poza punktem w nieskończoności: $\mathbb{C}[x, y]$,
- funkcja y/x^3 jest regularna w punkcie w nieskończoności, bo

$$\frac{y}{x^3} = uw = -t^3 + 2 \cdot t^7 - 5 \cdot t^{11} + 14 \cdot t^{15} - 42 \cdot t^{19} + 132 \cdot t^{23} + O(t^{25}),$$

Funkcje i formy na krzywej

- funkcje (z biegunami): $\mathbb{C}(x, y)$, gdzie $y^2 = x^3 - x$,
- funkcje regularne poza punktem w nieskończoności: $\mathbb{C}[x, y]$,
- funkcja y/x^3 jest regularna w punkcie w nieskończoności, bo

$$\frac{y}{x^3} = uw = -t^3 + 2 \cdot t^7 - 5 \cdot t^{11} + 14 \cdot t^{15} - 42 \cdot t^{19} + 132 \cdot t^{23} + O(t^{25}),$$

- formy różniczkowe: wyrażenia postaci $f\,dx$.

Czym właściwie są te kohomologie?

```
sage: AS = as_cover(P1, [P1.x^2, 1/2*P1.x^3], prec=1000)
sage: AS
(Z/p)^2-cover of Superelliptic curve with the equation y^1 = x over Finite Field of size 7 with the equations:
z0^7 - z0 = x^2
z1^7 - z1 = -3*x^3
sage: AS.de_rham_basis()
[( (1) * dx, 0 ),
 ( (z1) * dx, 0 ),
 ( (z1^2) * dx, 0 ),
 ( (z1^3) * dx, 0 ),
 ( (z1^4) * dx, 0 ),
 ( (3*x*z0^4 + z1^5 + x*z0*z1^2) * dx, 0 ),
 ( (-2*z0^6*z1^2 - 2*x*z0^4*z1 + z1^6 + x*z0*z1^3 + 3*x^2*z0^2) * dx, 0 ),
 ( (z0) * dx, 0 ),
 ( (z0*z1) * dx, 0 ),
 ( (z0*z1^2) * dx, 0 ),
 ( (z0*z1^3) * dx, 0 ),
 ( (z0*z1^4 + 3*x^2) * dx, 0 ),
 ( (2*x*z0^5 + z0*z1^5 - 3*x*z0^2*z1^2 - 3*x^2*z1) * dx, 0 ),
 ( (-2*z0^4*z1^4 - x*z0^5*z1 + z0*z1^6 - 2*x*z0^2*z1^3 + 2*x^2*z0^3 + 2*x^2*z1^2) * dx, 0 ),
 ( (z0^2) * dx, 0 ),
 ( (z0^2*z1) * dx, 0 ),
 ( (z0^2*z1^2) * dx, 0 ),
 ( (z0^2*z1^3 - x*z0^3) * dx, 0 ),
 ( (z0^2*z1^4 + 3*x*z0^3*z1 - 2*x^2*z0) * dx, 0 ),
 ( (3*x*z0^6 + z0^2*z1^5 - 2*x*z0^3*z1^2 - 3*x*z1^4 + x^2*z0*z1) * dx, 0 ),
 ( (2*z0^5*z1^4 + 2*x*z0^6*z1 + z0^2*z1^6 + x*z0^3*z1^3 + x^2*z0^4 - 3*x*z1^5 - 3*x^2*z0*z1^2) * dx, 0 ),
```

Rozważmy zbiory:

$$\text{CEGIEŁKI}^{dR}(G) := \{M : M \text{ jest nierozkładalnym składnikiem } H^1_{dR}(X) \text{ dla pewnej krzywej } X \text{ nad } \mathbb{F}_p\}$$

$$\text{CEGIEŁKI}^{Hdg}(G) := \{M : M \text{ jest nierozkładalnym składnikiem } H^1_{Hdg}(X) \text{ dla pewnej krzywej } X \text{ nad } \mathbb{F}_p\}.$$

Rozważmy zbiory:

$$\text{CEGIEŁKI}^{dR}(G) := \{M : M \text{ jest nierozkładalnym składnikiem } H^1_{dR}(X) \text{ dla pewnej krzywej } X \text{ nad } \mathbb{F}_p\}$$

$$\text{CEGIEŁKI}^{Hdg}(G) := \{M : M \text{ jest nierozkładalnym składnikiem } H^1_{Hdg}(X) \text{ dla pewnej krzywej } X \text{ nad } \mathbb{F}_p\}.$$

Jeżeli te zbiory są niemożliwe do opisania, to kohomologie krzywych też!

Rozważmy zbiory:

$$\text{CEGIEŁKI}^{dR}(G) := \{M : M \text{ jest nierozkładalnym składnikiem } H^1_{dR}(X) \text{ dla pewnej krzywej } X \text{ nad } \mathbb{F}_p\}$$

$$\text{CEGIEŁKI}^{Hdg}(G) := \{M : M \text{ jest nierozkładalnym składnikiem } H^1_{Hdg}(X) \text{ dla pewnej krzywej } X \text{ nad } \mathbb{F}_p\}.$$

Jeżeli te zbiory są niemożliwe do opisania, to kohomologie krzywych też!

Twierdzenie (JG, 2024)

Zbiory te są nieskończone, o ile $p > 2$ oraz G zawiera $\mathbb{Z}/p \times \mathbb{Z}/p$.

Rozważmy zbiory:

$$\text{CEGIEŁKI}^{dR}(G) := \{M : M \text{ jest nierozkładalnym składnikiem } H^1_{dR}(X) \text{ dla pewnej krzywej } X \text{ nad } \mathbb{F}_p\}$$
$$\text{CEGIEŁKI}^{Hdg}(G) := \{M : M \text{ jest nierozkładalnym składnikiem } H^1_{Hdg}(X) \text{ dla pewnej krzywej } X \text{ nad } \mathbb{F}_p\}.$$

Jeżeli te zbiory są niemożliwe do opisania, to kohomologie krzywych też!

Twierdzenie (JG, 2024)

Zbiory te są nieskończone, o ile $p > 2$ oraz G zawiera $\mathbb{Z}/p \times \mathbb{Z}/p$.

Pytanie: czy zbiory:

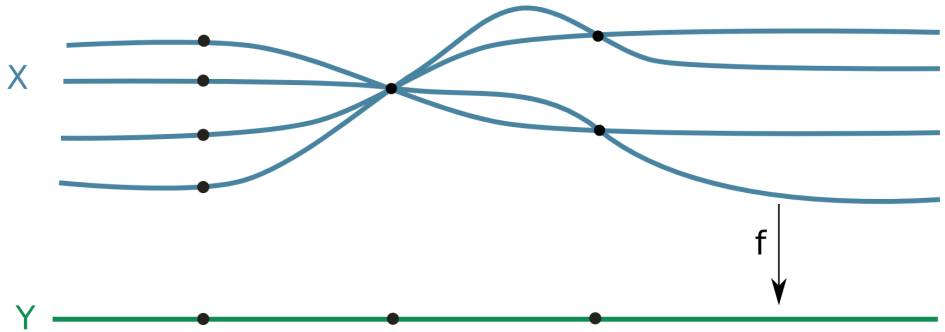
$$\{\dim M : M \in \text{CEGIEŁKI}^{dR}(G)\}, \quad \{\dim M : M \in \text{CEGIEŁKI}^{Hdg}(G)\}$$

są skończone?

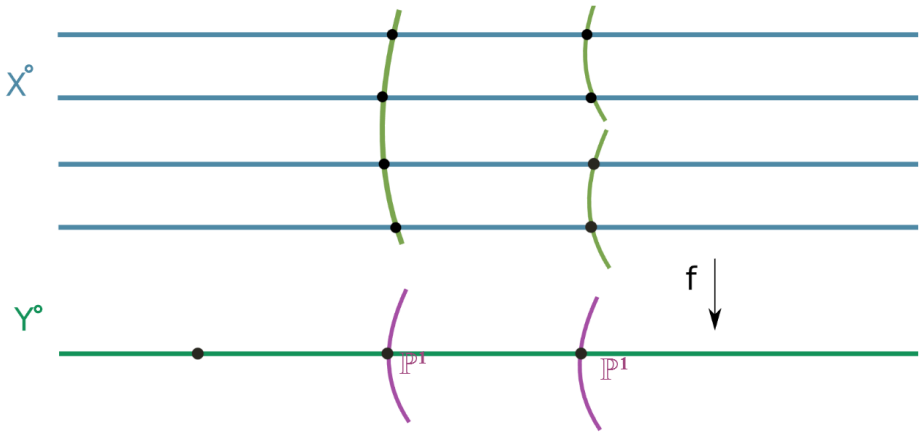
Dziękuję za uwagę!

Hipoteza o rozkładzie – wersja obrazkowa

kohomologie nakrycia:



powinny być takie same, jak kohomologie zdegenerowanego nakrycia przybliżającego je:



Hipoteza o rozkładzie – wersja na znaczkach

$$H^1_{dR}(X) \cong \text{część globalna} \oplus \bigoplus_{\substack{Q - \text{punkty} \\ \text{rozg.}}} H^1_{dR,Q},$$

$$H^1_{Hdg}(X) \cong \text{część globalna} \oplus \bigoplus_{\substack{Q - \text{punkty} \\ \text{rozg.}}} H^1_{Hdg,Q},$$

gdzie:

- część globalna zależy tylko od "obrazka" nakrycia i jest taka sama dla obu kohomologii,
- $H^1_{dR,Q}$ oraz $H^1_{Hdg,Q}$ są pewnymi częściami lokalnymi które zależą tylko od "infinitezymalnego otoczenia" punktu Q.

SLOGAN:
kohomologie Hodge'a oraz de Rham'a różnią się o części lokalne!