Lemat Iwasawy

Karol Janowicz

Notatki z wykładu 9 maja 2019 roku

1 Wstęp

Lemat Iwasawy stanowi efektywne narzędzie służące do badania prostoty grup. Przypomnijmy, że grupa nazywa się **prosta**, jeśli nie posiada ona nietrywialnych podgrup normalnych. Jest jasne, że każda grupa rzędu p, gdzie p jest liczbą pierwszą, jest prosta. Standardowym rezultatem w teorii grup jest także fakt, iż grupa alternująca A_n, dla $n \geq 5$ jest prosta. Udowodnimy ten fakt, korzystając z lematu Iwasawy, a ponadto dowiedziemy, że grupa rzutowa $PSL(n, \mathbb{F})$ jest prosta, dla $n > 2$ i dla ciała $\mathbb{F}$ skończonego o mocy większej niż 3.

Przypomnijmy podstawowe definicje i fakty z teorii grup. Fundamentalnym dla nas pojęciem będzie działanie grupy na zbiorze. Na prolegomenie przypomniałem pewne rzeczy (m. in. komutant, działania, podgrupy normalne); w tych notatkach nie umieszczam jednak tego, o czym tam mówiłem.

Definicja 1.1. *Niech G będzie dowolną grupą i niech X będzie dowolnym zbiorem. Wtedy homomorfizm grup $G \longrightarrow \Sigma_X$ nazywamy* ***działaniem grupy*** *G na zbiorze X.*

Przykłady:

1. Niech $G = S^1$ i $X = \mathbb{C}$. Wtedy grupa G działa na X w naturalny sposób:
$$g(z) := g \cdot z$$
dla dowolnego $g \in S^1$, $z \in \mathbb{C}$. Geometrycznie, grupa S^1 działa na płaszczyznę zepoloną poprzez izometrie niezmieniejące orientacji (obroty).

2. Niech $G = \mathbb{Z}_2$, $X = S^2$. Dla $1 \neq g \in G$ definiujemy:
$$g(x) = -x$$
dla dowolnego punktu $x \in S^2$. Grupa $\mathbb{Z}_2$ działa więc na sferze przez antypodyzm.

3. Grupa addytywna $\mathbb{R}^2$ działa na płaszczyźnie $\mathbb{R}^2$; dla $v \in \mathbb{R}^2$ definiujemy przekształcenie $T_v : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$:

$$T_v(w) := w + v$$

Definicja 1.2. *Załóżmy,że grupa G działa na zbiorze X.*

1. ***Orbitą** punktu $x \in X$ nazywamy zbiór:*

$$G(x) = \{g(x) : g \in G\}$$

2. ***Stabilizatorem** punktu $x \in X$ nazywamy zbiór:*

$$G_x = \{g \in G : g(x) = x\}$$

Przypomnijmy, że stabilizator punktu $x \in X$ jest podgrupą w grupie G; co więcej zbiory ${}^{G}/_{G_x}$ i $G(x)$ są izomorficzne jako G-zbiory; w szczególności wynika stąd natychmiast, że indeks stabilizatora jest równy mocy orbity.

Definicja 1.3. *Mówimy, że grupa G działa **tranzytywnie** na zbiorze X, jeśli $G(x) = X$ dla pewnego $x \in X$.*

Przykłady:

1. Grupa A_n działa tranzytywnie na zbiorze $\{1, \ldots, n\}$, o ile $n \geq 3$. Grupa A_2 nie działa tranzytywnie na $\{1, 2\}$.
2. Grupa liniowa $GL(2, \mathbb{R})$ działa tranzytywnie na $\mathbb{R}^2 \setminus \{0\}$, lecz nie działa tranzytywnie na $\mathbb{R}^2$ (dlaczego?)
3. Grupa izometrii n-kąta foremnego D_n działa tranzytywnie na zbiorze jego wierzchołków, $n \geq 3$ (dlaczego?)

Wniosek 1.1. *Jeśli grupa skończona G działa tranzytywnie na zbiorze X, to $|X| \,|\, |G|$*

Twierdzenie 1.1 (Frattini)**.** *Niech grupa G działa na zbiorze X oraz niech $H \leq G$ będzie podgurpą G. Następujące warunki są równoważne:*

1. *H działa tranzytywnie na X,*
2. *G działa tranzytywnie na H oraz $G = HG_x$ dla pewnego $x \in X$*

Dowód. Implikacja z 1. do 2. jest oczywista. Załóżmy, że $G = HG_x$ dla pewnego $x \in X$ i niech G działa tranzytywnie na X. W szczególności $G(x) = X$, więc dla dowolnego punktu $x' \in X$ mamy: $g(x) = x'$ dla pewnego $g \in G$; piszemy $g = hg'$ dla $h \in H$ i $g' \in G_x$, skąd od razu $h(x) = x'$. ■

Wniosek 1.2 (lemat Frattini)**.** *Niech G będzie grupą skończoną. Jeśli $N \triangleleft G$ oraz P jest p-podgrupą Sylowa w N, to $G = NN_G(P)$.*

Dowód. Grupa G działa na zbiorze p-podgrup Sylowa grupy N przez automorfizmy wewnętrzne; podgrupa N działa nań tranzytywnie, skąd teza. ■

2 Działania 2-przechodnie

Definicja 2.1. *Grupa G działa **podwójnie traznytywnie** na zbiorze X, jeśli dla wszystkich par $(x_1, x_2), (y_1, y_2) \in X^2 \setminus \{(x, x) : x \in X\}$ istnieje $g \in G$ taki, że $gx_1 = y_1$ i $gx_2 = y_2$.*

O działaniu podwójnie przechodnim (2-przechodnim, 2-tranzytywnym) możemy myśleć następująco; działanie grupy G na zbiorze X indukuje w naturalny sposób działanie tej grupy na zbiorze $X \times X$; co więcej przekątna: $\Delta = \{(x, x) : x \in X\}$ jest podzbiorem G-niezmienniczym, skąd wynika że zbiór $X^2 \setminus \Delta$ jest także G-niezmienniczy. Zatem mamy indukowane działanie grupy G na $X^2 \setminus \Delta$. Definicja 1.2 mówi, że grupa G działa podwójnie tranzytywnie na X, wtedy i tylko wtedy, gdy G działa tranzytywnie na $X^2 \setminus \Delta$. Oczywiście jeśli grupa G działa 2-przechodznio na zbiorze X, to działa też przechodnio.

Przykłady:

- Grupa A_n działa 2-przechodnio na $\{1, \ldots, n\}$ dla $n \geq 4$; grupa A_3 nie działa 2-przechodnio na zbiorze $\{1, 2, 3\}$ (dlaczego?)
- Grupa $GL(2, \mathbb{R})$ nie działa 2-przechodnio na $\mathbb{R}^2 \setminus \{0\}$, bo operator liniowy przeprowadza wektory zależne liniowo na wektory liniowo zależne

Udowodnimy obecnie bardzo ważne twierdzenia, opisujące własności działań podwójnie tranzytywnych, będące kluczowe w dowodzie lematu Iwasawy.

Twierdzenie 2.1. *Przypuśćmy, że grupa G działa podwójnie tranzytywnie na zbiorze X. Wtedy podgrupa normalna $N \triangleleft G$ działa na X albo trywialnie albo przechodnio.*

Dowód. Załóżmy, że $nx \neq x$ dla pewnego $n \in N$ i $x \in X$. Weźmy dowolne $x_1, x_2 \in X$. Wiemy, że istnieje $g \in G$ takie, że $gx = x_1$ i $g(nx) = x_2$. Ale wtedy $x_2 = (gn)x = (gn)g^{-1}x_1 = (gng^{-1})x_1$. ■

Twierdzenie 2.2. *Grupa G działa na X, $|X| \geq 3$. To działanie jest 2-przechodnie tylko wtedy, gdy dla każdego $x \in X$ stabilizator G_x działa przechodnio na $X \setminus \{x\}$.*

Dowód. Niech $x_1, x_2 \in X \setminus \{x\}$. Wtedy istnieje $g \in G$ taki, że $g \in G_x$ i $gx_1 = x_2$. ■

Wniosek 2.1. *Jeśli G działa 2-przechodnio na zbiorze X, to $2 \,|\, |G|$ (zakładamy rzecz jasna, że G jest grupą skończoną).*

Dowód. Weźmy $x_1 \in X$ i $x_2 \in X \setminus \{x_1\}$. Wiemy, że $|G : G_{x_1}| = |X|$. Bez straty ogólności możemy zakładać, że $|X| \geq 3$. Wiemy, że $H := G_{x_1}$ działa przechodnio na $X \setminus \{x_1\}$. Niech $K := H \cap G_{x_2}$. Wówczas:

$$|H : K| = |X \setminus \{x_1\}| = |X| - 1$$

skąd $|G| = |G : H| \cdot |H : K| \cdot |K| = |X| \cdot (|X| - 1) \cdot |K|$. ■

3 Finał, czyli lemat Iwasawy

Twierdzenie 3.1 (Iwasawa)**.** *Załóżmy, że grupa G działa podwójnie tranzytywnie na zbiorze X. Ponadto dla pewnego $x \in X$ podgrupa iztropii G_x zawiera abelową, normalną podgrupę, której sprzężenia generują grupę G. Jeśli grupa G jest doskonała, to grupa ilorazowa G/K jest prosta, gdzie K jest jądrem homomorfizmu $\varphi : G \to \Sigma_X$.*

Nim przejdziemy do dowodu tego twierdzenia, pokażemy pomocniczy lemat.

Lemat 3.1. *G działa 2-przechodnio na zbiorze X. Wówczas G_x jest podgrupą maksymalną w G.*

Dowód. Załóżmy, że $G_x \leq K \leq G$, przy czym $G_x \neq K$. Zaobserwujmy po pierwsze, że zachodzi równość: $G = G_x \cup G_x g G_x$, dla pewnego $g \in G$, $g \notin G_x$. Jeśli $|X| = 2$ to jest to jasne, bowiem $G_x g G_x = g G_x$. Niech więc $|X| \geq 3$. Wtedy zaś podgrupa G_x działa przechodnio na $X \setminus \{x\}$. Stąd też $G_x(gx) = X \setminus \{x\}$ dla dowolnie wybranego $g \notin G_x$. Jeśli więc $g' \notin G_x$, to $g'x = hgx$ dla pewnego $h \in G_x$. Stąd od razu $g' = hgh'$ dla pewnego $h' \in G_x$. Suma $G_x \cup G_x g G_x$ jest oczywiście rozłączna. Wybierzmy teraz $g \notin G_x$ i $g \in K$. Na mocy naszej obserwacji zachodzi równość $G = G_x \cup G_x g G_x = K$. ■

Możemy wreszcie udowodnić tytułowe twierdzenie.

Dowód lematu Iwasawy. Przypuśćmy, że $K \leq N \leq G$, gdzie $N \lhd G$. Niech też $H := G_x$ i niech $U \lhd H$ będzie normalną podgrupą abelową w H, której sprzężenia generują G. Mamy $NH = H$ lub $NH = G$ z powyższego lematu. Wiemy jednak, z twierdzenia 2.1, że grupa N działa trywialnie lub przechodnio

na X. W pierwszym przypadku $N \leq K$, to znaczy $K = N$. W przeciwnym wypadku mamy $NH = G$. Załóżmy więc, że $NH = G$. Mamy $NU \triangleleft NH$ (dzięki $N \triangleleft G$ i $U \triangleleft H$). Stąd, jeśli $g \in G$, to mamy

$$gUg^{-1} \subset g(NU)g^{-1} = NU$$

czyli NU zawiera wszystkie podgrupy sprzężone z U, a więc z założeń lematu jest $NU = G$. Stąd zaś

$$G/N = NU/N \simeq U/U \cap N$$

jest przemienna, co oznacza że $[G, G] \leq N$. Z doskonałości G wynika teza. ■

Korzystając z lematu Iwasawy jesteśmy w stanie efektywnie dowieść, że grupa alternująca A_5 jest prosta. Najpierw prosta obserwacja:

Lemat 3.2. *Grupa A_5 jest doskonała.*

Dowód. Weźmy dowolny element $(a\,b)(c\,d) \in A_5$ (wiemy, że permutacje typu $(2, 2)$ generują A_5); pokażemy, że jest on komutatorem w A_5. Mamy:

$$(a\,b\,c)(a\,b\,d)(a\,b\,c)^{-1}(a\,b\,d)^{-1} = (c\,a)(b\,d)(c\,b)(a\,d) = (a\,b)(c\,d)$$

czyli permutacja $(a\,b)(c\,d)$ jest równa $[(a\,b\,c), (a\,b\,d)]$. ■

Na wykładzie w tym miejscu nastąpiła pomyłka; próbowałem oszukać publikę, iż z tego, że $[\Sigma_5, \Sigma_5] = A_5$ wynika już doskonałość grupy A_5, a tak można gdy się już wie, że A_5 jest prosta, a tego właśnie dowodzimy! Nie wolno mi było więc brać komutatorów transpozycji, lecz tak jak to zauważył Jakub Różycki - należało brać 3-cykle (za tę uwagę bardzo mu dziękuje).

Lemat 3.3. *Grupa A_n, gdzie $n \geq 5$, działa 2-przechodnio i wiernie na zbiorze $\{1, \ldots, n\}$.*

Dowód. To jest naprawdę oczywiste; tutaj jest niesłychanie ważne, że $n \geq 5$ i należy w tej obserwacji z tego skorzystać! ■

Wniosek 3.1. *Grupa A_5 jest prosta.*

Dowód. Zauważmy, że stabilizator punktu $1 \in \{1, 2, 3, 4, 5\}$ w działaniu grupy A_5 jest grupą izomorficzną z A_4. Ta zaś ma abelową podgrupę, której sprzężenia generują A_5 (jest to grupa Kleina izomorficzna z $\mathbb{Z}_2 \times \mathbb{Z}_2$). ■

Rozważmy teraz specjalną grupę liniową $SL(2, \mathbb{F})$ nad ciałem $\mathbb{F}$. Działa ona naturalnie na prostej rzutowej $\mathbb{P}^1(\mathbb{F})$: $A(\mathbb{F}v) = \mathbb{F}(Av)$ (dobra określoność wynika z liniowości). Ponieważ $A \in SL(2, \mathbb{F})$ jest autmorfizmem płaszczyzny $\mathbb{F}^2$, $A : \mathbb{P}^1(\mathbb{F}) \longrightarrow \mathbb{P}^1(\mathbb{F})$ jest bijekcją zbiorów.

Lemat 3.4. *Jądrem działania $SL(2,\mathbb{F})$ na $\mathbb{P}^1(\mathbb{F})$ jest centrum grupy $SL(2,\mathbb{F})$.*

Dowód. Niech $A \in SL(2,\mathbb{F})$ będzie identycznością na $\mathbb{P}^1(\mathbb{F})$; w szczególności A zachowuje proste $\mathbb{F}(1,0)$ i $\mathbb{F}(0,1)$, więc

$$A = \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$$

Ale A zachowuje też prostą $\mathbb{F}(1,1)$, więc $a = \frac{1}{a}$, skąd musi być $a = 1$ lub $a = -1$.

■

Grupę ilorazową: ${}^{SL(2,\mathbb{F})}/_{Z(SL(2,\mathbb{F}))}$ nazywamy specjalną grupą rzutową i oznaczamy $PSL(2,\mathbb{F})$.

Lemat 3.5. *Niech:*

$$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F} \right\} \subset G := SL(2,\mathbb{F})$$

Wówczas U jest normalną, abelową podgrupą w stabilizatorze $G_{\mathbb{F}(1,0)}$, której sprzężenia generują $SL(2,\mathbb{F})$

Dowód. Zauważmy, że

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}$$

Dalej rozważamy trzy przypadki; $b \neq 0$, $c \neq 0$ i $b = c = 0$, pokazując, że w każdym z nich macierz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{F})$$

jest iloczynem macierzy dolno- i górnotrójkątnych z jedynkami na przekątnej.

■

Wniosek 3.2. *Grupa $SL(2,\mathbb{F})$ jest doskonała, o ile $|\mathbb{F}| \geq 4$.*

Dowód. Policzyć komutator elementów:

$$\begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in SL(2,\mathbb{F})$$

i zobaczyć, że przebiega on elementy podgrupy U, gdy ustalimy $a \in \mathbb{F}^*$, $a^2 \neq 1$ i b przebiega ciało $\mathbb{F}$. ■

Potrzeba nam teraz pokazać nieco silniejszą wersję twierdzenia 2.2. Wiemy, że jeśli wszystkie stabilizatory punktów w X działają przechodnio na X bez tego punktu, to cała grupa działa 2-przechodnio na X. Zakładając dodatkowo, że grupa G działa tranzytywnie na X, można wzmocnić tezę jak następuje:

Twierdzenie 3.2. *Niech G działa tranzytywnie na zbiorze X, przy czym $|X| \geq 3$. Przypuśćmy, że dla pewnego $x_0 \in X$, grupa G_{x_0} działa przechodnio na $X \setminus \{x_0\}$. Wtedy G działa 2-przechodnio na X.*

Dowód. Stabilizatory punktów leżacych na jednej orbicie są ze sobą sprzężone; dla punktu $y \in X \setminus \{x_0\}$ napiszmy $y = gx_0$ dla pewnego $g \in G$. Wtedy $G_y = gG_{x_0}g^{-1}$. Chcemy sprawdzić, że grupa G_y działa tranzytywnie na $X \setminus \{y\}$ (to nam wystarcza!). Niech więc $x_1, x_2 \in X \setminus \{y\}$ i $x_1 \neq x_2$. Wtedy $g^{-1}x_1, g^{-1}x_2 \neq x_0$, bo $gx_0 = y$. Zatem istnieje $h \in G_{x_0}$ takie, by $hg^{-1}x_1 = g^{-1}x_2$, co kończy dowód. ■

Powracamy w tym momencie do działania grupy $G = SL(2, \mathbb{F})$ na prostej rzutowej $\mathbb{P}^1(\mathbb{F})$. Odnotujmy po pierwsze, że jest ono tranzytywne. Istotnie, prostą $\mathbb{F}(1, 0)$ przeprowadzimy na prostą $\mathbb{F}(a, b)$ gdzie $(a, b) \neq 0$ (proszę sprawdzić, że specjalna grupa liniowa działa tranzytywnie na $\mathbb{R}^2 \setminus \{0\}$). Nietrudnym ćwiczeniem jest także sprawdzenie, że grupa $G_{\mathbb{F}(1,0)}$ działa tranzytywnie na zbiorze jednowymiarowych podprzestrzeni różnych od $\mathbb{F}(1, 0)$ (jesteśmy bowiem w stanie przeprowadzić elementem z tej grupy prostą $\mathbb{F}(0, 1)$ na dowolną inną prostą $\mathbb{F}(a, b)$, przy $b \neq 0$). Stąd wniosek, że rozważane działanie jest 2-przechodnie i w konsekwencji grupa rzutowa $PSL(2, \mathbb{F})$ jest prosta z lematu Iwasawy (gdy $|\mathbb{F}| \geq 4$)!

Na koniec wykładu wspomniałem o bardzo ważnym fakcie, że grupa izomterii przestrzeni euklidesowej $\mathbb{R}^3$ (niezmieniających orientacji) $SO(3)$, jest grupą prostą. Znane mi dowody tego faktu odwołują się wprost do geometrii (każdy obrót przestrzeni $\mathbb{R}^3$ jest złożeniem symetrii względem dwu płaszczyzn itp.). Rzuciłem więc naturalnie rodzące się pytanie (w kontekście wykładu); może by próbować dowodzić prostoty grupy $SO(3)$ za pomocą lematu Iwasawy? Wiemy, że grupa $SO(3)$ działa w sposób naturalny na sferze S^2 – może warto by się mu bliżej przyjrzeć z perspektywy naszego twierdzania... Albo rozważyć inne działania grupy $SO(3)$.