Jest to zapis odczytu wygłoszonego podczas XIX Szkoły Matematyki Poglądowej, *Ważne przykłady*, Siedlce, sierpień 1997

Ważny przykład w teorii grup: grupa prosta rzędu 168

Kazimierz SZYMICZEK, Katowice

Grupa G jest grupą *prostą*, jeśli nie ma właściwych podgrup normalnych, to znaczy, jeśli jej jedynymi podgrupami normalnymi są podgrupa jednostkowa $\{1\}$ oraz cała grupa G. Najprostszymi grupami prostymi są grupy skończone, których rzędy są liczbami pierwszymi. Takie grupy nie mają bowiem w ogóle podgrup właściwych, w związku z czym nie mają też właściwych podgrup normalnych. Jest to pierwsza nieskończona seria skończonych grup prostych: grupy cykliczne $\mathbf{C}_p$, gdzie p przebiega wszystkie liczby pierwsze.

Drugą nieskończoną serię skończonych grup prostych tworzą grupy alternujące (grupy permutacji parzystych) $\mathbf{A}(n)$ dla $n \geq 5$. Ich prostoty dowodzi się w kursowym wykładzie algebry i nie jest to najprostszy dowód w tym wykładzie.

Do początku lat sześćdziesiątych problem znalezienia wszystkich skończonych grup prostych był traktowany, podobnie jak Wielkie Twierdzenie Fermata, jako zagadnienie egzotyczne, leżące poza zasięgiem istniejących metod matematycznych.

Przełom nastąpił w 1963 roku, kiedy to ukazała się praca Feita i Thompsona o rozwiązalności grup skończonych rzędów nieparzystych. W szczególności z głównego twierdzenia tej pracy wynika, że każda nieabelowa grupa prosta ma rząd parzysty. Praca Feita i Thompsona wprowadziła nowe metody do teorii grup skończonych i rozpoczęła okres wytężonej pracy licznej grupy ekspertów, którego kulminacyjnym punktem było ustalenie w roku 1981 kompletnej listy wszystkich skończonych grup prostych.

Wśród grup nieabelowych rzędów ≤ 1000 jest – z dokładnością do izomorfizmu – tylko 5 grup prostych. Są to grupy

$$\mathbf{PSL}_2(\mathbf{F}_5) \cong \mathbf{A}(5),\quad \mathbf{PSL}_2(\mathbf{F}_7),\quad \mathbf{PSL}_2(\mathbf{F}_9) \cong \mathbf{A}(6),\quad \mathbf{PSL}_2(\mathbf{F}_8),\quad \mathbf{PSL}_2(\mathbf{F}_{11}),$$

których rzędy są odpowiednio

$$60,\quad 168,\quad 360,\quad 504,\quad 660.$$

Jak widzimy, każdą grupę prostą rzędu ≤ 1000 można przedstawić jako rzutową grupę liniową, z tym, że grupy rzędów 60 i 360 są także izomorficzne z grupami alternującymi, nie należą więc bezspornie do nowej serii grup prostych. Na specjalną uwagę zasługuje najmniejsza grupa prosta nie będąca ani grupą cykliczną, ani też grupą alternującą. Jest to grupa prosta rzędu 168. Otwiera ona listę kilku nieskończonych serii skończonych grup prostych prezentowanych jako grupy macierzy nad ciałami skończonymi. W tym artykule objaśniamy niektóre zagadnienia związane z rzutowymi grupami liniowymi $\mathbf{PSL}_n(\mathbf{F}_q)$ i dowodzimy prostoty wszystkich grup $\mathbf{PSL}_2(\mathbf{F}_q)$ dla $q \geq 7$. Grupa $\mathbf{PSL}_2(\mathbf{F}_7)$, której poświęcamy najwięcej uwagi, ma ważną interpretację geometryczną. Czytelnika zainteresowanego aspektem geometrycznym odsyłamy do szkicu historycznego J. Graya (From the history of a simple group, *Math. Intellig.* 4 (1982), 59–67). My natomiast skupimy się na algebraicznym opisie niektórych własności tej grupy.

Grupy macierzowe

Przypomnijmy podstawowe pojęcia i fakty o grupach liniowych. Grupę wszystkich odwracalnych macierzy stopnia n o elementach z ciała K oznaczamy $\mathbf{GL}_n(K)$ i nazywamy ją *pełną grupą liniową* stopnia n nad ciałem K. Podgrupa $\mathbf{SL}_n(K)$ tej grupy złożona z wszystkich macierzy o wyznaczniku 1 jest jądrem homomorfizmu $\det\colon \mathbf{GL}_n(K) \to K^*$ i w związku z tym jest podgrupą normalną pełnej grupy liniowej. Nazywamy ją *specjalną* grupą liniową stopnia n nad ciałem K.

Grupy liniowe mają naturalną interpretację geometryczną. Jeśli V jest n–wymiarową przestrzenią wektorową nad ciałem K, to zbiór wszystkich automorfizmów przestrzeni V tworzy grupę ze względu na składanie odwzorowań. Grupę tę oznacza się $\mathbf{GL}_n(V)$. Ma ona podgrupę $\mathbf{SL}_n(V)$ złożoną z automorfizmów o wyznaczniku 1.

Jeśli $\mathcal{B}$ jest jakąkolwiek bazą przestrzeni V, to przyporządkowanie $\mathbf{GL}_n(V) \to \mathbf{GL}_n(K)$, które każdemu automorfizmowi α przestrzeni V przyporządkowuje macierz automorfizmu α względem bazy $\mathcal{B}$, jest izomorfizmem grup.

Izomorfizm ten przeprowadza $\mathbf{SL}_n(V)$ na $\mathbf{SL}_n(K)$. W ten sposób pełna i specjalna grupa liniowa mogą być interpretowane jako grupy automorfizmów przestrzeni wektorowych.

Łatwo sprawdzić, że grupa $\mathbf{SL}_n(K)$ jest generowana przez *transwekcje* $t_{ij}(a)$, gdzie $1 \leq i, j \leq n$, $i \neq j$ oraz $a \in K^*$ (zob. [2], str. 28). Transwekcja $t_{ij}(a)$ powstaje z macierzy jednostkowej przez zastąpienie zera na miejscu (i, j) elementem $a \in K$.

Grupy liniowe są w wysokim stopniu nieprzemienne. Badając macierze przemienne z transwekcjami stwierdza się, że centrum specjalnej grupy liniowej składa się tylko z macierzy *skalarnych* należących do tej grupy. A więc

$$Z(\mathbf{SL}_n(K)) = \{aI : a \in K,\ a^n = 1\}$$

(zob. [3], str. 40). Centrum grupy jest jej podgrupą normalną. Grupa $\mathbf{SL}_n(K)$ nie jest więc na ogół prosta. Szczególnie interesująca jest grupa ilorazowa

$$\mathbf{PSL}_n(K) := \mathbf{SL}_n(K)/Z(\mathbf{SL}_n(K))$$

nazywana *specjalną grupą rzutową* stopnia n nad ciałem K. Jej elementy zapisujemy zwykle jako macierze $A \in \mathbf{SL}_n(K)$, z tym, że dla $a \in K$ będącego pierwiastkiem stopnia n z jedynki (to znaczy spełniającego $a^n = 1$) utożsamiamy macierze A oraz aA.

Jeśli K jest q–elementowym ciałem skończonym $\mathbf{F}_q$ (gdzie q jest potęgą liczby pierwszej), to grupy liniowe są grupami skończonymi. Grupę $\mathbf{PSL}_n(\mathbf{F}_q)$ oznacza się też prościej $\mathbf{L}_n(q)$. Będziemy korzystać z tego uproszczenia symboliki zwłaszcza w przypadku grupy $\mathbf{L}_2(7)$.

Można wskazać wyraźny wzór na rząd każdej grupy liniowej w zależności od n i q. Dla przykładu, wyznaczymy rzędy grup liniowych dla $n = 2$ i $q = 7$. Zaczniemy od $\mathbf{GL}_2(\mathbf{F}_7)$. W pierwszej kolumnie macierzy należącej do tej grupy może wystąpić każdy niezerowy wektor przestrzeni $\mathbf{F}_7^2$, zatem mamy $7^2 - 1 = 48$ możliwości. Jeśli już pierwsza kolumna jest ustalona, to druga kolumna nie może być proporcjonalna do pierwszej, zatem mamy $7^2 - 7 = 42$ możliwości wyboru drugiej kolumny, gdy ustalona jest pierwsza kolumna. Razem zatem mamy $48 \cdot 42 = 2016$ macierzy. Ponieważ $|\mathbf{GL}_2(\mathbf{F}_7)/\mathbf{SL}_2(\mathbf{F}_7)| = |\mathbf{F}_7^*| = 6$, więc $|\mathbf{SL}_2(\mathbf{F}_7)| = 2016/6 = 336$. Dalej, centrum grupy $\mathbf{SL}_2(\mathbf{F}_7)$ składa się tylko z macierzy $I, -I$. Zatem

$$|\mathbf{GL}_2(\mathbf{F}_7)| = 2016 = 2^5 \cdot 3^2 \cdot 7,$$
$$|\mathbf{SL}_2(\mathbf{F}_7)| = 336 = 2^4 \cdot 3 \cdot 7,$$
$$|\mathbf{PSL}_2(\mathbf{F}_7)| = 168 = 2^3 \cdot 3 \cdot 7.$$

Podobnie dowodzi się, że dla dowolnej liczby naturalnej n i dla ciała q–elementowego $\mathbf{F}_q$ mamy

$$|\mathbf{GL}_n(\mathbf{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}),$$
$$|\mathbf{SL}_n(\mathbf{F}_q)| = \frac{1}{q-1}(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$$

oraz

$$|\mathbf{PSL}_n(\mathbf{F}_q)| = \frac{1}{d(q-1)}(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}),$$

gdzie d oznacza $\mathrm{NWD}(n, q-1)$.

Rozpatrzmy jeszcze kilka przykładów rzutowych grup liniowych małych rzędów. Można udowodnić następujące fakty (zob. [3]):

$\mathbf{PSL}_2(\mathbf{F}_2) \cong \mathbf{S}(3)$ grupa rzędu 6, ma podgrupę normalną $\mathbf{A}(3)$,
$\mathbf{PSL}_2(\mathbf{F}_3) \cong \mathbf{A}(4)$ grupa rzędu 12, ma podgrupę normalną $\mathbf{V}(4)$, zwaną grupą czwórkową Kleina.

Natomiast wszystkie pozostałe grupy $\mathbf{PSL}_n(\mathbf{F}_q)$ są proste. Wśród nich są:
$\mathbf{PSL}_2(\mathbf{F}_4) \cong \mathbf{PSL}_2(\mathbf{F}_5) \cong \mathbf{A}(5)$ grupa rzędu 60,
$\mathbf{PSL}_2(\mathbf{F}_7) \cong \mathbf{PSL}_3(\mathbf{F}_2)$ grupa rzędu 168,
$\mathbf{PSL}_2(\mathbf{F}_9) \cong \mathbf{A}(6)$ grupa rzędu 360,
$\mathbf{PSL}_4(\mathbf{F}_2) \cong \mathbf{A}(8)$ grupa rzędu 20 160,
$\mathbf{PSL}_3(\mathbf{F}_4)$ grupa prosta rzędu 20 160 nieizomorficzna z $\mathbf{A}(8)$.

Ostatnie dwa fakty są szczególnie interesujące, gdyż wskazują one najmniejszą liczbę naturalną m taką, że istnieją dwie nieizomorficzne grupy proste rzędu m (jest nią liczba $m = 20\,160$).

Fakt, że grupy $\mathbf{PSL}_4(\mathbf{F}_2)$ oraz $\mathbf{PSL}_3(\mathbf{F}_4)$ nie są izomorficzne można uzasadnić na co najmniej dwa sposoby. Po pierwsze, okazuje się, że w grupie $\mathbf{PSL}_4(\mathbf{F}_2)$ elementy rzędu 2 tworzą co najmniej dwie klasy elementów sprzężonych, podczas gdy w grupie $\mathbf{PSL}_3(\mathbf{F}_4)$ elementy rzędu 2 tworzą tylko jedną klasę elementów sprzężonych (zob. [1], Ch. IV). Po drugie, zakładając, że wiemy, iż $\mathbf{PSL}_4(\mathbf{F}_2) \cong \mathbf{A}(8)$ można zauważyć, że w grupie $\mathbf{A}(8)$ istnieje element rzędu 15, na przykład (12345)(678), podczas gdy w grupie $\mathbf{PSL}_3(\mathbf{F}_4)$ nie ma elementów rzędu 15 (co nie jest trywialne).

Prostota grupy $\mathbf{PSL}_2(\mathbf{F}_7)$

Z elementarnej teorii grup wiemy, że homomorfizm kanoniczny $G \to G/H$ ustala wzajemnie jednoznaczną odpowiedniość pomiędzy podgrupami normalnymi grupy G zawierającymi ustaloną podgrupę normalną H tej grupy a podgrupami normalnymi grupy ilorazowej G/H. Zatem ewentualne właściwe podgrupy normalne grupy $\mathbf{PSL}_n(K)$ byłyby przeciwobrazami właściwych podgrup normalnych grupy $\mathbf{SL}_n(K)$ (zawierających centrum tej grupy) w homomorfizmie kanonicznym $\mathbf{SL}_n(K) \to \mathbf{PSL}_n(K)$. Okazuje się, że specjalna grupa liniowa tylko w bardzo specjalnych przypadkach ($n = 2$ i $|K| = 2$ lub 3) zawiera właściwe podgrupy normalne ostro zawierające centrum. Zatem grupy $\mathbf{PSL}_n(K)$ są proste (z wyjątkiem przypadków $n = 2$ i $|K| = 2$ lub 3). Jest to tzw. twierdzenie Jordana-Dicksona, którego dowód nie jest zbyt trudny, ale angażuje jednak dość znaczny aparat teorio-grupowy (zob. [2], str. 125–126).

Dowód prostoty grupy $\mathbf{L}_2(7) = \mathbf{PSL}_2(\mathbf{F}_7)$ można byłoby przeprowadzić sporządzając kompletną listę podgrup tej grupy i pokazując *explicite*, że nie ma wśród nich podgrup normalnych. Punktem wyjścia byłoby tutaj twierdzenie Sylowa. Jednakże to podejście ma dwa istotne mankamenty. Po pierwsze, jest bardzo żmudne, i po drugie, dowodzi prostoty tylko tej jednej grupy, którą rozważamy. Okazuje się, że istnieje prosty i elementarny dowód prostoty **wszystkich** grup $\mathbf{PSL}_2(K)$ dla dowolnego ciała K (niekoniecznie skończonego), które ma co najmniej 4 elementy. Ten dowód reprodukujemy poniżej (por. [3], str. 23–25).

Twierdzenie. *Niech K będzie ciałem, które ma co najmniej 4 elementy. Wtedy grupa $\mathbf{PSL}_2(K)$ jest prosta. W szczególności, wszystkie grupy $\mathbf{PSL}_2(\mathbf{F}_q)$ dla $q \geq 4$ są proste.*

Dowód. Grupa $\mathbf{PSL}_2(K)$ jest izomorficzna z grupą $\mathbf{PSL}_2(V)$, gdzie V jest płaszczyzną nad ciałem K. Wystarczy pokazać, że jeśli H jest podgrupą normalną grupy $\mathbf{SL}_2(V)$ nie zawierającą się w centrum tej grupy, to $H = \mathbf{SL}_2(V)$.

Niech $\alpha \in H$ będzie automorfizmem płaszczyzny V nie leżącym w centrum grupy $\mathbf{SL}_2(V)$. Wtedy istnieje wektor $v \in V$ taki, że $\alpha(v)$ nie leży na prostej wyznaczonej przez wektor v. Zatem wektory $v, \alpha(v)$ tworzą bazę płaszczyzny V i w tej bazie automorfizm α ma macierz

$$A = \begin{bmatrix} 0 & -1 \\ 1 & a \end{bmatrix}$$

gdzie a jest pewnym elementem ciała K. Postać pierwszej kolumny tej macierzy otrzymujemy wprost z definicji macierzy endomorfizmu przestrzeni wektorowej, natomiast postać drugiej kolumny otrzymujemy stąd, że musimy mieć $\det A = 1$. Przeniesiemy teraz nasze rozważania do grupy macierzy $\mathbf{SL}_2(K)$. Rozpatrzmy więc izomorfizm grup

$$\Phi : \mathbf{SL}_2(V) \to \mathbf{SL}_2(K),$$

który każdemu automorfizmowi $\beta \in \mathbf{SL}_2(V)$ przyporządkowuje jego macierz w bazie $\{v, \alpha(v)\}$ płaszczyzny V. Niech $\mathcal{H} = \Phi(H)$. Wtedy $\mathcal{H}$ jest podgrupą normalną grupy $\mathbf{SL}_2(K)$ oraz $\Phi(\alpha) = A \in \mathcal{H}$.

Wobec tego $BAB^{-1} \in \mathcal{H}$ dla każdej macierzy $B \in \mathbf{SL}_2(K)$, a więc także $BAB^{-1}A^{-1} \in \mathcal{H}$.

Obieramy teraz $B = \begin{bmatrix} b^{-1} & 0 \\ 0 & b \end{bmatrix}$, gdzie b jest dowolnym niezerowym elementem ciała K. Wtedy

$$C := BAB^{-1}A^{-1} = \begin{bmatrix} b^{-2} & 0 \\ a(b^2-1) & b^2 \end{bmatrix} \in \mathcal{H}.$$

Podobnie, dla dowolnego $d \in K$ oraz $D = \begin{bmatrix} 1 & 0 \\ d & 1 \end{bmatrix}$ mamy

$$E := DCD^{-1}C^{-1} = \begin{bmatrix} 1 & 0 \\ d(1-b^4) & 1 \end{bmatrix} \in \mathcal{H}$$

oraz dla $F = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$,

$$G := FEF^{-1} = \begin{bmatrix} 1 & -d(1-b^4) \\ 0 & 1 \end{bmatrix} \in \mathcal{H}.$$

Zauważmy, że macierze E i G są transwekcjami. Pokażemy, że przy odpowiednim wyborze elementów $b, d \in K$ każdą transwekcję można przedstawić w postaci macierzy E lub G. Przede wszystkim w ciele K istnieją co najwyżej 4 elementy b takie, że $b^4 - 1 = 0$.

Jeśli więc ciało K ma co najmniej 7 elementów, to istnieje element $b \in K$ taki, że $b^4 - 1 \neq 0$ i $b \neq 0$.

W ciele 4-elementowym $K = \mathbf{F}_4$ każdy niezerowy element x spełnia równanie $x^3 = 1$, zatem jeśli $x^4 = 1$, to $x = 1$. Obierając więc jako b dowolny element ciała $\mathbf{F}_4$ różny od 0 i 1 otrzymamy także $b^4 - 1 \neq 0$ i $b \neq 0$.

Pozostawiając więc na razie przypadek, gdy ciało K ma 5 elementów, widzimy, że gdy $d \in K$ przebiega elementy ciała K, to $e = d(1-b^4)$ (a także $-e$) przebiega **wszystkie** elementy ciała K. Zatem wszystkie transwekcje

$$\begin{bmatrix} 1 & 0 \\ e & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & -e \\ 0 & 1 \end{bmatrix}$$

należą do $\mathcal{H}$, a ponieważ transwekcje generują $\mathbf{SL}_2(K)$, więc $\mathcal{H} = \mathbf{SL}_2(K)$. Zatem także $H = \mathbf{SL}_2(V)$ i twierdzenie jest udowodnione dla wszystkich ciał K z wyjątkiem ciała 5-elementowego $\mathbf{F}_5$.

Gdy $K = \mathbf{F}_5$ mamy $b^4 = 1$ dla każdego niezerowego elementu $b \in K$ i, wobec tego, $E = G = I$ jest macierzą jednostkową. Dla $b = 2, 3 \in K$ mamy jednak $b^2 \neq 1$ i macierz C jest odpowiednim punktem wyjścia do dowodu, że wszystkie transwekcje należą do $\mathcal{H}$. Znalezienie tego dowodu pozostawiamy Czytelnikowi jako ćwiczenie (lub też odsyłamy do [3], str. 24–25).

Uwaga. Dla $n \geq 3$ istnieje dowód prostoty grupy $\mathbf{PSL}_n(K)$ oparty na podobnym podejściu, jak przedstawiony tutaj dowód dla $n = 2$, z tym, że jest on nieco trudniejszy i mniej bezpośredni (zob. [3], str. 23–24). Z drugiej strony, istnieje także jednolity dowód ogólnego twierdzenia Jordana-Dicksona nie wyróżniający przypadku $n = 2$. Opiera się on na technice grup permutacji (zob. [2], str. 125–126 oraz [3], str. 25–27).

Inne własności grupy $\mathbf{L}_2(7) := \mathbf{PSL}_2(\mathbf{F}_7)$

(a) *Kod genetyczny*

Rozważmy dwie następujące macierze $s, t \in \mathbf{L}_2(7)$:

$$s = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad t = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Bezpośrednim rachunkiem stwierdzamy, że

(1) $$s^7 = t^2 = (st)^3 = (s^4t)^4 = 1 \in \mathbf{L}_2(7).$$

Zauważmy tutaj, że jeśli wykonamy te rachunki w $\mathbf{SL}_2(\mathbf{F}_7)$ to otrzymamy równości $s^7 = (st)^3 = I$ oraz $t^2 = (s^4t)^4 = -I$, gdzie I oznacza macierz jednostkową.

Ponadto dla $a \in \{0, 1, 2, 3, 4, 5, 6\}$ mamy

$$tst = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \qquad \text{oraz} \qquad s^a = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \qquad (tst)^a = \begin{bmatrix} 1 & 0 \\ -a & 1 \end{bmatrix}.$$

Wynika stąd, że podgrupa $\langle s, t \rangle$ grupy $\mathbf{L}_2(7)$ generowana przez macierze s, t zawiera wszystkie transwekcje, zatem jest równa grupie $\mathbf{L}_2(7)$. Można udowodnić, że faktycznie grupa $\mathbf{L}_2(7)$ ma następującą prezentację za pomocą generatorów i relacji, czyli tzw. *kod genetyczny*:

(2) $$\mathrm{s}^7 = \mathrm{t}^2 = (\mathrm{st})^3 = (\mathrm{s}^4\mathrm{t})^4 = 1.$$

Różnica pomiędzy stwierdzeniami, że grupa $\mathbf{L}_2(7)$ jest generowana przez elementy s, t spełniające relacje (1) oraz że grupa $\mathbf{L}_2(7)$ ma kod genetyczny (2) jest dość znaczna. Grupa G z kodem genetycznym (2) jest generowana przez elementy s,t spełniające relacje (2) i dla każdej grupy L generowanej przez elementy s, t spełniające relacje (1) istnieje surjektywny homomorfizm $h : G \to L$ taki, że $\mathrm{s} \mapsto s$ oraz $\mathrm{t} \mapsto t$. Fakt, że grupa $L = \mathbf{L}_2(7)$ ma kod genetyczny (2) oznacza, że gdy $L = \mathbf{L}_2(7)$, to homomorfizm h jest izomorfizmem grup. Pierwszym matematykiem, który znalazł ten kod genetyczny grupy $\mathbf{L}_2(7)$ był Walter von Dyck w 1883 roku. Dla dowodu tego faktu wystarczyłoby pokazać, że grupa G z kodem genetycznym (2) ma rząd 168. Wtedy bowiem homomorfizm $h : G \to \mathbf{L}_2(7)$ musi być izomorfizmem grup. Rezygnujemy tutaj z przedstawienia tego dowodu ze względu na jego uciążliwość. Żeby jednak dać Czytelnikowi przedsmak trudności związanych z tą pozornie elementarną sprawą przedstawimy dowód jednej z kluczowych tożsamości, niezbędnych w analizie sposobu przedstawiania elementów grupy G w postaci iloczynów potęg generatorów. Twierdzimy, że jeśli s i t spełniają relacje (2), to także

(3) $$(\mathrm{s}^2\mathrm{ts}^4\mathrm{t})^3 = 1.$$

Najpierw zauważamy, że

$$(\mathrm{s}^2\mathrm{tst})^2 = \mathrm{s} \cdot \mathrm{st} \cdot \mathrm{st} \cdot \mathrm{s} \cdot \mathrm{st} \cdot \mathrm{st} = \mathrm{s} \cdot \mathrm{st} \cdot \mathrm{st} \cdot \mathrm{s} \cdot \mathrm{ts}^{-1} = \mathrm{s} \cdot (\mathrm{st})^3 \cdot \mathrm{s}^{-1} = 1.$$

Stąd

$$\mathrm{s}^2\mathrm{tsts}^2\mathrm{t} = \mathrm{ts}^{-1} = \mathrm{ts}^3 \cdot \mathrm{s}^3 = \mathrm{s}^4\mathrm{t} \cdot \mathrm{s}^4\mathrm{t} \cdot \mathrm{s}^4\mathrm{t} \cdot \mathrm{s}^3.$$

Tę równość mnożymy z lewej strony najpierw przez s^3, a potem przez t:

$$\mathrm{ts}^5\mathrm{t} \cdot \mathrm{s} \cdot \mathrm{ts}^2\mathrm{t} = \mathrm{s}^4\mathrm{t} \cdot \mathrm{s}^4 \cdot \mathrm{ts}^3.$$

Zastępując po lewej stronie $\mathrm{ts}^5\mathrm{t}$ przez $(\mathrm{ts}^2\mathrm{t})^{-1}$ oraz po prawej stronie ts^3 przez $(\mathrm{s}^4\mathrm{t})^{-1}$ otrzymujemy tożsamość

(4) $$(\mathrm{ts}^2\mathrm{t})^{-1} \cdot \mathrm{s} \cdot \mathrm{ts}^2\mathrm{t} = \mathrm{s}^4\mathrm{t} \cdot \mathrm{s}^4 \cdot (\mathrm{s}^4\mathrm{t})^{-1}.$$

Pokazuje ona, że w grupie G elementy s i s^4 są sprzężone. Podnosząc obie strony tożsamości (4) do potęgi czwartej otrzymujemy

$$(\mathrm{ts}^2\mathrm{t})^{-1} \cdot \mathrm{s}^4 \cdot \mathrm{ts}^2\mathrm{t} = \mathrm{s}^4\mathrm{t} \cdot \mathrm{s}^2 \cdot (\mathrm{s}^4\mathrm{t})^{-1},$$

skąd

$$\mathrm{s}^4 \cdot \mathrm{ts}^2\mathrm{t} \cdot \mathrm{s}^4\mathrm{t} = \mathrm{ts}^2\mathrm{t} \cdot \mathrm{s}^4\mathrm{t} \cdot \mathrm{s}^2,$$

oraz

$$\mathrm{t} \cdot \mathrm{s}^4 \cdot \mathrm{ts}^2\mathrm{t} \cdot \mathrm{s}^4\mathrm{t} = \mathrm{s}^2\mathrm{t} \cdot \mathrm{s}^4\mathrm{t} \cdot \mathrm{s}^2.$$

Wobec tego

$$(\mathrm{s}^2\mathrm{ts}^4\mathrm{t})^3 = \mathrm{s}^2\mathrm{ts}^4\mathrm{ts}^2 \cdot \mathrm{ts}^4\mathrm{ts}^2\mathrm{ts}^4\mathrm{t} = \mathrm{s}^2\mathrm{ts}^4\mathrm{ts}^2 \cdot \mathrm{s}^2\mathrm{ts}^4\mathrm{ts}^2$$
$$= \mathrm{s}^2\mathrm{t} \cdot (\mathrm{s}^4\mathrm{t})^3 \cdot \mathrm{s}^2 = \mathrm{s}^2\mathrm{t} \cdot \mathrm{ts}^3 \cdot \mathrm{s}^2 = 1.$$

(b) *Wyjątkowy izomorfizm* $\mathbf{L}_2(7) \cong \mathbf{SL}_3(\mathbf{F}_2)$.

Wobec prostoty grup $\mathbf{PSL}_n(K)$ jest rzeczą interesującą zbadać, czy istnieją izomorfizmy $\mathbf{PSL}_n(K) \cong \mathbf{PSL}_m(L)$ dla różnych ciał K i L oraz różnych stopni n i m. Okazuje się, że wspomniane już izomorfizmy $\mathbf{PSL}_2(\mathbf{F}_4) \cong \mathbf{PSL}_2(\mathbf{F}_5) \cong \mathbf{A}(5)$ oraz $\mathbf{PSL}_2(\mathbf{F}_7) \cong \mathbf{PSL}_3(\mathbf{F}_2)$ są tu jedynymi wyjątkami. O. Schreier i B. L. van der Waerden udowodnili bowiem w 1928 roku następujące twierdzenie klasyfikacyjne dla rzutowych specjalnych grup liniowych:

Niech K i L będą dowolnymi ciałami i niech $n \geq 2$ i $m \geq 2$ będą dowolnymi liczbami naturalnymi. Wtedy

$$\mathbf{PSL}_n(K) \cong \mathbf{PSL}_m(L) \iff n = m \text{ i } K \cong L$$

z wyjątkiem dwóch przypadków:
$\mathbf{PSL}_2(\mathbf{F}_4) \cong \mathbf{PSL}_2(\mathbf{F}_5)$ oraz $\mathbf{PSL}_2(\mathbf{F}_7) \cong \mathbf{PSL}_3(\mathbf{F}_2)$.

Podobne twierdzenia klasyfikacyjne (i to bez żadnych wyjątków) są prawdziwe także dla pełnej i dla specjalnej grupy liniowej (zob. [3], str. 76).

Istnienie izomorfizmu $\mathbf{PSL}_2(\mathbf{F}_7) \cong \mathbf{PSL}_3(\mathbf{F}_2)$ ma też interpretację geometryczną w zagadnieniu kolorowania płaszczyzny hiperbolicznej podzielonej na trójkąty równoboczne, których każdy wierzchołek jest wspólny dla dokładnie siedmiu trójkątów. Problem polega na wskazaniu metody kolorowania za pomocą siedmiu kolorów w taki sposób, że żadne dwa trójkąty tego samegu koloru nie mają wspólnego wierzchołka (a więc tym bardziej boku). Istnienie przynajmniej dwóch odmiennych metod rozstrzygnięcia tego zagadnienia jest związane z istnieniem izomorfizmu $\mathbf{PSL}_2(\mathbf{F}_7) \cong \mathbf{PSL}_3(\mathbf{F}_2)$ (zob. D. Mackenzie, A hyperbolic plane coloring and the simple group of order 168, *Amer. Math. Monthly* **102** (1995), 706–715). Podamy tutaj inny, dowód tego faktu, wykorzystujący prostotę i kod genetyczny grupy $\mathbf{L}_2(7)$.

Weźmy dwie następujące macierze $S, T \in \mathbf{PSL}_3(\mathbf{F}_2) = \mathbf{SL}_3(\mathbf{F}_2)$:

$$S = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \qquad T = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Macierze te spełniają następujące relacje:

$$S^7 = T^2 = (ST)^3 = (S^4T)^4 = 1 \in \mathbf{SL}_3(\mathbf{F}_2).$$

Generatory podgrupy $\langle S, T \rangle$ grupy $\mathbf{SL}_3(\mathbf{F}_2)$ spełniają więc relacje z kodu genetycznego grupy $\mathbf{L}_2(7)$. Istnieje zatem surjektywny homomorfizm h : $\mathbf{L}_2(7) \to \langle S, T \rangle$ taki, że $s \mapsto S$ oraz $t \mapsto T$. Jądro tego homomorfizmu jest podgrupą normalną grupy $\mathbf{L}_2(7)$, zatem wobec prostoty tej grupy, jest grupą jednoelementową. A więc h jest izomorfizmem grup.

Ponieważ grupy $\mathbf{L}_2(7)$ i $\mathbf{SL}_3(\mathbf{F}_2)$ mają ten sam rząd 168, wynika stąd, że

$$\mathbf{L}_2(7) \cong \langle S, T \rangle = \mathbf{SL}_3(\mathbf{F}_2).$$

(c) *Realizacja* $\mathbf{L}_2(7)$ *jako grupy Galois nad* $\mathbf{Q}$

Już w 1877 roku F. Klein pisał, że znalezienie wielomianu f o współczynnikach wymiernych, którego grupą Galois jest $\mathbf{L}_2(7) := \mathbf{PSL}_2(\mathbf{F}_7)$ jest *starym* problemem. Jednak problem ten pozostawał otwarty jeszcze przez następnych sto lat! Pierwszy przykład wielomianu $f \in \mathbf{Q}[X]$ takiego, że $\mathrm{Gal}(f, \mathbf{Q}) = \mathbf{L}_2(7)$ został znaleziony dopiero w 1968 roku za pomocą komputera w pracy dyplomowej W. Trinksa na uniwersytetcie w Karlsruhe:

$$f = X^7 - 7X + 3.$$

Innym przykładem takiego wielomianu jest $P_7 = X^7 - 154X + 99$ wskazany w 1979 roku przez Erbacha, Fischera i McKaya (w *Journal of Number Theory*). Tutaj podany został dowód, że wielomian ten ma grupę Galois $\mathbf{L}_2(7)$, a ponadto udowodniono, że f i P_7 mają nieizomorficzne ciała rozkładu. Tak więc f i P_7 są istotnie różnymi przykładami wielomianów z tą samą grupą Galois $\mathbf{L}_2(7)$. Potem znalezione zostały jedno- a nawet dwuparametrowe rodziny takich wielomianów (zob. G. Malle und B. H. Matzat, Realisierung von Gruppen $\mathbf{PSL}_2(\mathbf{F}_p)$ als

Galoisgruppen uber $\mathbf{Q}$. *Math. Annalen* **272** (1985), 549–565 i cytowaną tam literaturę).

(d) *Reprezentacja* $\mathbf{L}_2(7)$ *w grupach permutacji*

Łatwo stwierdzić, że grupy $\mathbf{L}_2(7) := \mathbf{PSL}_2(\mathbf{F}_7)$ nie można zanurzyć w grupę $\mathbf{S}(6)$. Gdyby bowiem takie zanurzenie istniało, to rząd grupy $\mathbf{L}_2(7)$ równy $168 = 2^3 \cdot 3 \cdot 7$ musiałby dzielić rząd grupy $\mathbf{S}(6)$, czyli liczbę $6!$, co oczywiście nie ma miejsca.

Używając standardowych metod można natomiast stwierdzić, że grupa $\mathbf{L}_2(7)$ ma zanurzenie w grupę $\mathbf{S}(8)$. Niech bowiem s_7 oznacza liczbę podgrup rzędu 7 w grupie $\mathbf{L}_2(7)$ (jest to liczba sylowowskich 7-podgrup tej grupy). Wtedy na podstawie twierdzenia Sylowa mamy

$$s_7 \equiv 1 \pmod 7 \qquad \text{oraz} \qquad s_7 | 2^3 \cdot 3 \cdot 7.$$

W takim razie $s_7 = 1 + 7k$ dla pewnej liczby naturalnej k. Zauważmy, że $k \geq 1$, gdyż gdyby było $k = 0$, to byłoby również $s_7 = 1$ skąd wynika, że grupa prosta $\mathbf{L}_2(7)$ ma podgrupę **normalną** rzędu 7. Liczba s_7 nie dzieli się przez 7 i wobec tego s_7 dzieli $2^3 \cdot 3 = 24$. Stąd wynika już, że $s_7 = 8$. Z twierdzenia Sylowa wiadomo także, że jeśli H jest p–podgrupą Sylowa grupy G oraz $N(H)$ jest normalizatorem podgrupy H w G, to $s_p = |G : N(H)|$. Zatem jeśli H jest 7-podgrupą Sylowa grupy $\mathbf{L}_2(7)$, to

$$8 = s_7 = |\mathbf{L}_2(7) : N(H)|.$$

Nasza grupa ma więc podgrupę $N = N(H)$ o indeksie 8. Rozpatrując teraz regularną reprezentację grupy $\mathbf{L}_2(7)$ w grupie permutacji zbioru warstw $\mathbf{L}_2(7) : N$ otrzymujemy zanurzenie grupy $\mathbf{L}_2(7)$ w grupę $\mathbf{S}(8)$. Mówiąc bardziej szczegółowo, rozpatrujemy homomorfizm grup

$$\mathbf{L}_2(7) \to \mathbf{S}(\mathbf{L}_2(7) : N) \cong \mathbf{S}(8), \quad g \mapsto \varphi_g,$$

gdzie $\varphi_g(aN) = gaN$ dla wszystkich $a \in G$. Ponieważ grupa $\mathbf{L}_2(7)$ jest prosta, homomorfizm ten jest odwzorowaniem różnowartościowym, a więc zanurzeniem w grupę permutacji zbioru 8–elementowego.

Ale grupa $\mathbf{L}_2(7)$ ma też reprezentację w grupie $\mathbf{S}(7)$. Udowodnimy mianowicie, że $\mathbf{L}_2(7) \cong \langle (1234567), (23)(47) \rangle \subset \mathbf{S}(7)$. Rozważmy permutacje

$$\sigma = (1234567), \quad \tau = (23)(47).$$

Bezpośrednim rachunkiem stwierdzamy, że

$$\sigma^7 = \tau^2 = (\sigma\tau)^3 = (\sigma^4\tau)^4 = 1.$$

A więc σ i τ spełniają te same relacje co generatory s, t w kodzie genetycznym grupy $\mathbf{L}_2(7)$. Wynika stąd, że podgrupa $\langle \sigma, \tau \rangle$ grupy $\mathbf{S}(7)$ jest homomorficznym obrazem grupy $\mathbf{L}_2(7)$. Mianowicie istnieje surjektywny homomorfizm

$$\mathbf{L}_2(7) \to \langle \sigma, \tau \rangle \qquad \text{taki, że} \qquad s \mapsto \sigma, \quad t \mapsto \tau.$$

Faktycznie, wobec prostoty grupy $\mathbf{L}_2(7)$, homomorfizm ten ma trywialne jądro, jest zatem izomorfizmem.

Można także udowodnić, że grupa $\mathbf{L}_2(11)$ ma reprezentację w grupie $\mathbf{S}(11)$. Natomiast już Galois wiedział, że dla żadnej liczby pierwszej $p > 11$ grupy $\mathbf{L}_2(p)$ nie można zanurzyć w grupę symetryczną $\mathbf{S}(p)$.

Literatura

[1] E. Artin. *Geometric Algebra*. Interscience, New York 1957.

[2] M. I. Kargapołow i J. I. Mierzlakow. *Podstawy teorii grup*. PWN, Warszawa 1989.

[3] O. T. O'Meara. *Lectures on Linear Groups*. CBMS Series No. 22, AMS, Providence, RI, 1974.