5. Wykład 5: Grupy proste.

Definicja 5.1. *Grupę $(G, \cdot)$ nazywamy* **grupą prostą,** *gdy G nie zawiera właściwych podgrup normalnych.*

Przeprowadzimy obecnie skróconą klasyfikację skończonych grup prostych.

5.1. **(C1): Grupy cykliczne rzędu będącego liczbą pierwszą.** Są to, jak sama nazwa wskazuje, grupy rzędu p, gdzie p jest liczbą pierwszą.

Uwaga 5.1. *Niech $(G, \cdot)$ będzie grupą abelową. Jeżeli G zawiera podgrupę właściwą, to G nie jest prosta.*

Twierdzenie 5.1 (o klasyfikacji grup abelowych prostych)**.** *Niech $(G, \cdot)$ będzie grupą abelową. Następujące warunki są równoważne:*

(1) *G jest prosta,*
(2) *G jest grupą cykliczną rzędu będącego liczbą pierwszą,*
(3) *$G \cong \mathbb{Z}_p$, gdzie p jest liczbą pierwszą.*

Dowód. Równoważność (2) $\Leftrightarrow$ (3) jest treścią twierdzenia Cayley o klasyfikacji skończonych grup cyklicznych, zaś implikacja (2) $\Rightarrow$ (1) jest oczywista. Dla dowodu implikacji (1) $\Rightarrow$ (2) ustalmy $a \in G \setminus \{1\}$ i niech $H = \langle a \rangle$. Ponieważ G jest abelowa, więc $H \lhd G$, a ponieważ G jest prosta, więc $H = G$ i tym samym G jest cykliczna.

Pokażemy, że G jest skończona. Przypuśćmy na odwrót, że $r(a) = \infty$, czyli

$$\forall n \in \mathbb{N}(a^n \neq 1).$$

Niech $K = \langle a^2 \rangle$. Oczywiście $K \neq \{1\}$ i ponieważ G jest abelowa, więc $K \lhd G$. Zauważmy, że $a \notin K$: istotnie, gdyby $a \in K$, to wówczas $a = a^{2k}$ dla pewnego $k \in \mathbb{N}$, a wtedy $a^{2k-1} = 1$, co dałoby sprzeczność. Zatem $K \subsetneq G$, ale G jest prosta, co daje sprzeczność.

Pokażemy, że $|G|$ jest liczbą pierwszą. Przypuśćmy bowiem, że $|G| = r(a) = nm$ dla pewnych liczb naturalnych $n, m > 1$. Wówczas $r(a^m) = n$. Ponieważ G jest abelowa, więc $\langle a^m \rangle \lhd G$ i $|\langle a^m \rangle| = n < nm$, więc $\langle a^m \rangle \subsetneq G$, co daje sprzeczność. □

Uwaga 5.2. *Niech $(G, \cdot)$ będzie grupą prostą. Jeżeli G nie jest abelowa, to G nie jest rozwiązalna.*

Dowód. Niech G będzie grupą nieabelową prostą. Jedynym ciągiem podnormalnym jest

$$\{1\} \lhd G.$$

Faktor $G/\{1\} \cong G$ nie jest wszakże abelowy. □

5.2. **(C2): Grupy alternujące $A(n)$ dla $n \geq 5$.** Są to grupy rzędu $\frac{1}{2}n!$.

Lemat 5.1. *Niech $n \geq 2$ i niech $\tau \in S(n)$. Wówczas:*

(1) *dla wszystkich cykli $(a_1, \ldots, a_k) \in S(n)$:*

$$\tau \circ (a_1, \ldots, a_k) = (\tau(a_1), \ldots, \tau(a_k));$$

(2) *dla wszystkich permutacji $\sigma \in S(n)$ będących iloczynem m cykli rozłącznych o długościach $k_1, \ldots, k_m$, odpowiednio, permutacja*

$$\tau \circ \sigma \circ \tau^{-1}$$

jest iloczynem m cykli rozłącznych o długościach $k_1, \ldots, k_m$, odpowiednio.

Prosty dowód tego lematu pozostawiamy jako ćwiczenie.

Twierdzenie 5.2 (Galois)**.** *Dla $n \geq 5$ grupa alternująca $A(n)$ jest prosta.*

Dowód. Ustalmy $n \geq 5$ i niech $\{1\} \neq N \lhd A(n)$. Pokażemy, że $N = A(n)$. Ustalmy $\sigma \in N \setminus \{1\}$. Możemy założyć, że

$$|supp\sigma| = \min\{|supp\tau| : \tau \in N \setminus \{1\}\}.$$

Pokażemy, że $|supp\sigma| = 3$. Istotnie, przypuśćmy, że $|supp\sigma| \geq 4$. Dowód poprowadzimy równolegle w dwóch przypadkach:

(A): Załóżmy, że w rozkładzie σ na iloczyn cykli parami rozłącznych występuje cykl o długości ≥ 3. Zauważmy, że σ nie może być cyklem o długości 3, bo $|supp\sigma| \geq 4$. Zauważmy też, że σ nie może być cyklem o długości 4, bo $\sigma \in A(n)$. Zatem σ porusza przynajmniej 5 elementów. Możemy założyć, że $1, 2, 3, 4, 5 \in supp\sigma$.

(B): Załóżmy, że w rozkładzie σ na iloczyn cykli parami rozłącznych występują cykle o długości 2. Zauważmy, że σ jest iloczynem parzystej liczby transpozycji. Możemy założyć, że $1, 2, 3, 4 \in supp\sigma$. Możemy też założyć, że jeśli σ porusza więcej niż 4 elementy, to $5 \in supp\sigma$.

Niech $\tau = (3, 4, 5)$, $\tau \in A(n)$. Ponieważ N jest normalna, więc

$$\sigma_1 = \tau\sigma\tau^{-1} \in N.$$

Mamy zatem

$$\sigma_1 = \begin{cases} (1, 2, 3, \ldots)\ldots & \text{w przypadku } \mathbf{(A)}, \\ (1, 2)(4, 5)\ldots & \text{w przypadku } \mathbf{(B)}. \end{cases}$$

Zauważmy, że $\sigma_1 \neq \sigma$. Zatem

$$(1) \neq \sigma_1\sigma \in N.$$

Pokażemy, że $|supp\sigma_1\sigma^{-1}| < |supp\sigma|$. Załóżmy najpierw, że $5 \in supp\sigma$. Ustalmy $x \notin supp\sigma$. Wówczas $x \notin \{1, 2, 3, 4, 5\}$. Zatem $\tau(x) = x$. Wobec tego

$$\sigma_1\sigma^{-1}(x) = \tau\sigma\tau^{-1}\sigma^{-1}(x) = x,$$

czyli $x \notin supp\sigma_1\sigma^{-1}$. Zatem $supp\sigma_1\sigma^{-1} \subset supp\sigma$. Ponadto $\sigma_1\sigma^{-1}(2) = \sigma_1(1) = 2$, więc $2 \notin supp\sigma_1\sigma^{-1}$. Zatem $supp\sigma_1\sigma^{-1} \subsetneq supp\sigma$.

Załóżmy teraz, że $5 \notin supp\sigma$. Wówczas $\sigma = (1, 2)(3, 4)\ldots$ oraz $\sigma_1 = (1, 2)(4, 5)$, więc

$$\sigma_1\sigma^{-1} = (3, 4)(4, 5) = (3, 4, 5).$$

Zatem $|supp\sigma_1\sigma^{-1}| = 3 < |supp\sigma|$.

Tym samym $\sigma_1\sigma^{-1} \in N\setminus\{1\}$ oraz $|supp\sigma_1\sigma^{-1}| < |supp\sigma|$, ale wobec wyboru σ, $|supp\sigma| = \min\{|supp\tau| : \tau \in N \setminus \{1\}\}$, co jest sprzecznością. A zatem istotnie pokazaliśmy, że $|supp\sigma| = 3$ i możemy założyć, że $\sigma = (1, 2, 3)$.

Pokażemy, że $\forall i \in \{3, \ldots, n\}((1, 2, i) \in N)$. Pokazaliśmy to już w przypadku $i = 3$, ustalmy więc $i \in \{4, \ldots, n\}$. Niech $\rho_1 = (1, 2)(3, i)$, $\rho_1 \in A(n)$. Ponieważ N jest normalna, więc

$$\gamma = \rho_1\sigma\rho_1^{-1} \in N.$$

Mamy:

$$\gamma = (2, 1, i).$$

Ustalmy $k, l \in \{1, 2, i\}$, przy czym $k \neq l$. Niech $\rho_2 = (1, 2)(k, l)$, $\rho_2 \in A(n)$. Ponieważ N jest normalna, więc

$$\delta = \rho_2\gamma\rho_2^{-1} \in N.$$

Mamy:

$$\delta = (1, 2, i).$$

Ponieważ grupa $A(n)$ jest generowana przez zbiór $\{(1,2,i) : i \in \{3,\dots,n\}\}$, więc $N = A(n)$. □

Uwaga 5.3. *Dla $n \geq A(n)$ (a więc także $S(n)$) nie jest rozwiązalna.*

Dowód. Wystarczy zauważyć, że $A(n)$ jest nieabelową grupą prostą. □

5.3. **(C3): Skończone odpowiedniki $A_n(q)$ grup Liego $A_n(\mathbb{C})$, $n > 1$.** Są to grupy rzędu $\frac{1}{q-1}\prod_{i=0}^{n}(q^{n+1}-q^i)$. Grupy te zawierają grupy proste o indeksie $NWD(n+1, q-1)$.

Definicja 5.2. *Niech $n \in \mathbb{N}$, niech F będzie ciałem. Grupę*

$$SL(n,F)/Z(SL(n,F))$$

nazywamy **specjalną grupą rzutową** *stopnia n nad ciałem F i oznaczamy $PSL(n,F)$.*

W przypadku, gdy F jest ciałem q-elementowym piszemy:

$$SL(n,q) = SL(n,F) \text{ oraz } PSL(n,q) = PSL(n,F).$$

Uwaga 5.4. *Specjalna grupa liniowa $SL(n+1,q)$ jest skończonym odpowiednikiem $A_n(q)$ grupy Liego $A_n(\mathbb{C})$, izomorficznej z $SL(n+1,\mathbb{C})$.*

Twierdzenie 5.3 (Jordana-Dicksona)**.** [13] *Niech $n \in \mathbb{N}$, niech F będzie ciałem q-elementowym. Wówczas:*

(1) *grupa $PSL(2,q)$ jest prosta dla $q \geq 4$,*
(2) *grupa $PSL(n,q)$ jest prosta dla $n \geq 3$ i $q \geq 2$.*

5.4. **(C4): Skończone odpowiedniki $B_n(q)$ grup Liego $B_n(\mathbb{C})$.** Są to grupy rzędu $q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$. Grupy te zawierają grupy proste o indeksie $NWD(2, q-1)$.

Definicja 5.3. *Niech $n \in \mathbb{N}$, niech V będzie przestrzenią liniową wymiaru n nad ciałem F, niech $q : V \to F$ będzie niezdegenerowaną formą kwadratową. Grupę*

$$\{f : V \to V : f \text{ jest izomorfizmem ortogonalnym względem formy } q \text{ oraz } \det f = 1\}$$

nazywamy **specjalną grupą ortogonalną** *formy q i oznaczamy $SO(q)$.*

W przypadku, gdy $F = \mathbb{C}$, $V = \mathbb{C}^n$ oraz q jest formą kanoniczną piszemy:

$$SO(n,\mathbb{C}) = SO(q);$$

w przypadku, gdy F jest ciałem q-elementowym oraz $V = F^n$ piszemy:

$$SO(n,q) = SO(q).$$

Uwaga 5.5. *Specjalna grupa ortogonalna $SO(2n+1,q)$ jest skończonym odpowiednikiem $B_n(q)$ grupy Liego $B_n(\mathbb{C})$ izomorficznej z $SO(2n+1,\mathbb{C})$.*

[13] Camille Jordan (1838-1922) – matematyk francuski, zajmował się algebrą, topologią i analizą z jej zastosowaniami; wyjaśnił idee Ewarysta Galois; od jego nazwiska pochodzą pojęcia krzywej Jordana i miary Jordana. Twierdzenie pochodzi z 1870 roku. Niedokładności w dowodzie usunął Dickson w 1958 roku

5.5. **(C5): Skończone odpowiedniki $C_n(q)$ grup Liego $C_n(\mathbb{C})$, $n > 2$.** Są to grupy rzędu $q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$. Grupy te zawierają grupy proste o indeksie $NWD(2, q-1)$.

Definicja 5.4. *Niech $n \in \mathbb{N}$, niech V będzie przestrzenią liniową wymiaru $2n$ nad ciałem F, niech $B : V \times V \to F$ będzie niezdegenerowaną i antysymetryczną formą dwuliniową. Grupę*

$$\{f : V \to V : \forall u, v \in V(B(f(u), f(v)) = B(u, v)) \text{ oraz } f \text{ jest izomorfizmem}\}$$

nazywamy **grupą symplektyczną** *formy B i oznaczamy $Sp(B)$.*

W przypadku, gdy $F = \mathbb{C}$, $V = \mathbb{C}^{2n}$ oraz B jest formą kanoniczną piszemy:

$$Sp(2n, \mathbb{C}) = Sp(B);$$

w przypadku, gdy F jest ciałem q-elementowym, $V = F^{2n}$ oraz B jest formą kanoniczną piszemy:

$$Sp(2n, q) = Sp(B).$$

Uwaga 5.6. *Grupa symplektyczna $Sp(2n, q)$ jest skończonym odpowiednikiem $C_n(q)$ grupy Liego $C_n(\mathbb{C})$ izomorficznej z $Sp(2n, \mathbb{C})$.*

5.6. **(C6): Skończone odpowiedniki $D_n(q)$ grup Liego $D_n(\mathbb{C})$, $n > 3$.** Są to grupy rzędu $q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1)$. Grupy te zawierają grupy proste o indeksie $NWD(4, q^n-1)$.

Uwaga 5.7. *Specjalna grupa ortogonalna $SO(2n, q)$ jest skończonym odpowiednikiem $D_n(q)$ grupy Liego $D_n(\mathbb{C})$ izomorficznej z $SO(2n, \mathbb{C})$.*

5.7. **(C7): Skończone odpowiedniki $G_2(q)$ grup Liego $G_2(\mathbb{C})$.** Są to grupy rzędu $q^6(q^6-1)(q^2-1)$.

5.8. **(C8): Skończone odpowiedniki $F_4(q)$ grup Liego $F_4(\mathbb{C})$.** Są to grupy rzędu $q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$.

5.9. **(C9): Skończone odpowiedniki $E_6(q)$ grup Liego $E_6(\mathbb{C})$.** Są to grupy rzędu $q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$. Grupy te zawierają grupy proste o indeksie $NWD(3, q-1)$.

5.10. **(C10): Skończone odpowiedniki $E_7(q)$ grup Liego $E_7(\mathbb{C})$.** Są to grupy rzędu $q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^6-1)(q^2-1)$. Grupy te zawierają grupy proste o indeksie $NWD(2, q-1)$.

5.11. **(C11): Skończone odpowiedniki $E_8(q)$ grup Liego $E_8(\mathbb{C})$.** Są to grupy rzędu $q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$.

5.12. **(C12): Skończone odpowiedniki ${}^2A_n(q)$ grup Liego ${}^2A_n(\mathbb{C})$, $n > 1$.** Są to grupy rzędu $q^{\frac{1}{2}n(n-1)}\prod_{i=1}^{n}(q^{i+1}-(-1)^{i+1})$. Grupy te zawierają grupy proste o indeksie $NWD(n+1, q+1)$.

5.13. **(C13): Skończone odpowiedniki ${}^2B_2(q)$ grup Liego ${}^2B_2(\mathbb{C})$, $q = 2^{2m+1}$.** Są to grupy rzędu $q^2(q^2+1)(q^2-1)$.

5.14. **(C14): Skończone odpowiedniki ${}^2D_n(q)$ grup Liego ${}^2D_n(\mathbb{C})$, $n > 3$.** Są to grupy rzędu $q^{n(n-1)}(q^n+1)\prod_{i=1}^{n-1}(q^{2i}-1)$. Grupy te zawierają grupy proste o indeksie $NWD(4, q^n+1)$.

5.15. **(C15): Skończone odpowiedniki ${}^3D_4(q)$ grup Liego ${}^3D_4(\mathbb{C})$.** Są to grupy rzędu $q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$.

5.16. **(C16): Skończone odpowiedniki ${}^2G_2(q)$ grup Liego ${}^2G_2(\mathbb{C})$, $q = 3^{2m+1}$.** Są to grupy rzędu $q^3(q^3+1)(q-1)$.

5.17. **(C17): Skończone odpowiedniki ${}^2F_4(q)$ grup Liego ${}^2F_4(\mathbb{C})$, $q = 2^{2m+1}$.** Są to grupy rzędu $q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$.

5.18. **(C18): Skończone odpowiedniki ${}^2E_6(q)$ grup Liego ${}^2E_6(\mathbb{C})$.** Są to grupy rzędu $q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)$. Grupy te zawierają grupy proste o indeksie $NWD(3, q+1)$.

5.19. **(S1): Grupa Mathieu M_{11}.** [14] Jest to grupa rzędu $2^4 \cdot 3^2 \cdot 5 \cdot 11 = 7920$.

Uwaga 5.8. *$M_{11} < S(11)$ przy czym $M_{11} = \langle A, B\rangle$, gdzie*

$$A = (1,2,3,4,5,6,7,8,9,10,11)$$

oraz

$$B = (5,6,4,10)(11,8,3,7).$$

5.20. **(S2): Grupa Mathieu M_{12}.** Jest to grupa rzędu $2^6 \cdot 3^3 \cdot 5 \cdot 11 = 95040$.

Uwaga 5.9. *$M_{12} < S(12)$ przy czym $M_{12} = \langle A, B, C\rangle$, gdzie permutacje A i B dane są tymi samymi wzorami co w Uwadze 5.8 oraz*

$$C = (1,12)(2,11)(3,6)(4,8)(5,9)(7,10).$$

5.21. **(S3): Grupa Mathieu M_{22}.** Jest to grupa rzędu $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 443520$.

Uwaga 5.10. *$M_{22} < S(22)$ przy czym $M_{22} = \langle D, E, F\rangle$, gdzie*

$$D = (1,2,3,4,5,6,7,8,9,10,11)(12,13,14,15,16,17,18,19,20,21,22),$$

$$E = (1,4,5,9,3)(2,8,10,7,6)(12,15,16,20,14)(13,19,21,18,17)$$

oraz

$$F = (11,22)(1,21)(2,10,8,6)(12,14,16,20)(4,7,3,13)(5,19,9,18).$$

5.22. **(S4): Grupa Mathieu M_{23}.** Jest to grupa rzędu $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 10200960$.

Uwaga 5.11. *$M_{23} < S(23)$ przy czym $M_{23} = \langle G, H\rangle$, gdzie*

$$G = (1,2,3,4,5,6,7,8,9,10,11)(12,13,14,15,16,17,18,19,20,21,22,23)$$

oraz

$$H = (3,17,10,7,9)(5,4,13,14,19)(11,12,23,8,18)(21,16,15,20,22).$$

5.23. **(S5): Grupa Mathieu M_{24}.** Jest to grupa rzędu $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040$.

Uwaga 5.12. *$M_{24} < S(24)$ przy czym $M_{24} = \langle G, H, I\rangle$, gdzie permutacje G i H dane są tymi samymi wzorami co w Uwadze 5.11 oraz*

$$I = (1,24)(2,23)(3,12)(4,16)(5,18)(6,10)(7,20)(8,14)(9,21)(11,17)(13,22)(19,15).$$

[14] Odkryta około 1860 roku.

5.24. **(S6): Grupa Janko J_1.** Jest to grupa rzędu $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 = 175560$.

Uwaga 5.13. *$J_1 < GL(7, 11)$ przy czym $J_1 = \langle Y, Z \rangle$, gdzie*

$$Y = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \text{oraz } Z = \begin{bmatrix} -3 & 2 & -1 & -1 & -3 & -1 & -3 \\ -2 & 1 & 1 & 3 & 1 & 3 & 3 \\ -1 & -1 & -3 & -1 & -3 & -3 & 2 \\ -1 & -3 & -1 & -3 & -3 & 2 & -1 \\ -3 & -1 & -3 & -3 & 2 & -1 & -1 \\ 1 & 3 & 3 & -2 & 1 & 1 & 3 \\ 3 & 3 & -2 & 1 & 1 & 3 & 1 \end{bmatrix}.$$

5.25. **(S7): Grupa Janko J_2.** Jest to grupa rzędu $2^7 \cdot 3^3 \cdot 5^2 \cdot 7$.

5.26. **(S8): Grupa Janko J_3.** Jest to grupa rzędu $2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$.

5.27. **(S9): Grupa Janko J_4.** Jest to grupa rzędu $2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$.

5.28. **(S10): Grupa Highmana-Sims'a HS.** Jest to grupa rzędu $2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$.

5.29. **(S11): Grupa McLauglin'a Mc.** Jest to grupa rzędu $2^7 \cdot 3^6 \cdot 5^3 \cdot 11$.

5.30. **(S12): Grupa Suzuki Suz.** Jest to grupa rzędu $2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$.

5.31. **(S13): Grupa Rudvalisa Ru.** Jest to grupa rzędu $2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$.

5.32. **(S14): Grupa Helda He.** Jest to grupa rzędu $2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$.

5.33. **(S15): Grupa Lyona Ly.** Jest to grupa rzędu $2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$.

5.34. **(S16): Grupa O'Nan'a ON.** Jest to grupa rzędu $2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$.

5.35. **(S17): Grupa Conway'a .1.** Jest to grupa rzędu $2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$.

5.36. **(S18): Grupa Conway'a .2.** Jest to grupa rzędu $2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$.

5.37. **(S19): Grupa Conway'a .3.** Jest to grupa rzędu $2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$.

5.38. **(S20): Grupa Fishera $M(22)$.** Jest to grupa rzędu $2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$.

5.39. **(S21): Grupa Fishera $M(23)$.** Jest to grupa rzędu $2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$.

5.40. **(S22): Grupa Fishera $M(24)'$.** Jest to grupa rzędu $2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 23 \cdot 29$.

5.41. **(S23): Grupa Harady F_5.** Jest to grupa rzędu $2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$.

5.42. **(S24): Grupa Thompson'a F_3.** Jest to grupa rzędu $2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$.

5.43. **(S25): Grupa Fishera F_2.** Jest to grupa rzędu $2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$.

5.44. **(S26): Grupa Fishera-Greiss'a F_1.** Grupa ta zwana jest też pieszczotliwie "The Monster". Jest to grupa rzędu $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$.

Twierdzenie 5.4. *(główne twierdzenie klasyfikacyjne)* [15] *Każda skończona grupa prosta jest izomorficzna z jedną z grup z serii* **(C1)** – **(C18)** *lub z jedną ze sporadycznych grup prostych* **(S1)** – **(S26)**.

[15] Dowód tego twierdzenia zakończono w lutym 1981; jego opracowanie trwało około 30 lat, pełen zapis dowodu zajmuje około 300-500 prac o objętości 5-10 tysięcy stron.