Spis treści

1. **Wprowadzenie**

Rozwiązywanie równań wielomianowych ma długą historię. Znane są wzory na rozwiązania równań:

- $ax + b = 0$ — wzór ma postać $x = \dfrac{-b}{a}$;
- $ax^2 + bx + c = 0$ — wzór ma postać $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ (o ile $b^2 - 4ac \geq 0$);
- $ax^3 + bx^2 + cx + d = 0$;
- $ax^4 + bx^3 + cx^2 + dx + e = 0$.

Ostatnie dwa wzory, zbyt skomplikowane, by je tu przytaczać, mają fascynującą historię. Scipione del Ferro (1465–1526) zapewne jako pierwszy umiał rozwiązać równania $x^3 = cx + d$. Stąd bardzo łatwo już przejść do ogólnych równań, ale w owych czasach nie stosowano jeszcze liczb ujemnych! Uczeń del Ferro, Antonio Fiore (14??–1557), poznał tę metodę w sekrecie, pod koniec życia del Ferro. Niezależnie ogólną metodę rozwiązywania równań stopnia trzeciego odkrył Niccoló Fontana Tartaglia (1499/1500–1557), który wygrał pojedynek na zadania z del Fiore. Informację o swoim odkryciu przekazał w sekrecie Gerolamo Cardano (1501–76), który badał je wraz ze swoim uczniem, Lodovico Ferrari (1522-65). Cardano i Ferrari dowiedzieli się jednak o wcześniejszym odkryciu del Ferro i w książce *Ars Magna* Cardano zamieścił opis (wierszem!) metody rozwiązywania równań trzeciego stopnia (przypisując autorstwo del Ferro), a także równań stopnia czwartego (które odkrył Ferrari). Wywołało to długotrwały spór między Cardanem i Tartaglią. Spór ten doprowadził do kolejnego pojedynku na zadania między Tartaglią i Ferrarim, wygranym przez tego drugiego. Niezależnie powyższe wzory otrzymał również François Viète (1540–1603). Swoje dołożył później Kartezjusz.

Powyższe wzory wymagały wyciągania pierwiastków kwadratowych z liczb ujemnych! Zwrócił na to uwagę już Cardano, ale dopiero Rafael Bombelli (1526–72) zajął się tym tematem dokładniej. Dlatego czasem to jemu przypisuje się odkrycie liczb zespolonych.

Ogólną teorię równań wielomianowych opracował dopiero Évariste Galois (1811–32), matematyk, który stracił życie w pojedynku (niematematycznym). Równolegle problem badał Niels Henrik Abel (1802–29). Obaj udowodnili, że wzory na rozwiązania równań piątego i wyższych stopni... nie istnieją! Błędny dowód tego twierdzenia podał wcześniej Paolo Ruffini (1765–1822). Z kolei dowód Galois został opublikowany dopiero po jego śmierci — z powodów, które nie są do końca jasne.

TWIERDZENIE 1.1 (Abela–Ruffiniego, nieformalnie). Nie istnieje wzór, który wyraża pierwiastki ogólnego wielomianu stopnia co najmniej 5 przy pomocy współczynników, stałych liczbowych, czterech operacji arytmetycznych i symboli pierwiastka.

Znane są inne wzory, wykorzystujące granice (np. metoda Newtona) czy funkcje specjalne (np. funkcję hipergeometryczną dla równań stopnia 5).

Niniejszy kurs zawiera (prawie całkiem formalny) dowód zasadniczego twierdzenia algebry i twierdzenia Abela–Ruffiniego: wprowadzenie do liczb zespolonych i wielomianów zespolonych, dowód twierdzeń oraz dalsze informacje o permutacjach i grupach.

2. Liczby zespolone: definicje

Rozważmy wpierw $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ (gdzie $\mathbb{Q}$ to zbiór liczb wymiernych). Zbiór ten ma następujące dwie własności.

- Jeśli $a + b\sqrt{2} = c + d\sqrt{2}$, to $a = c$ i $b = d$, bowiem w przeciwnym razie $\sqrt{2}$ byłby liczbą wymierną: jeśli $b = d$, to $a = c$, zaś jeśli $b \neq d$, to $\sqrt{2} = (a - c)/(b - d)$.
- Zbiór $\mathbb{Q}(\sqrt{2})$ jest zamknięty na cztery operacje arytmetyczne, na przykład

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{-ad + bc}{c^2 - 2d^2}\sqrt{2}.$$

Analogiczne własności ma $\mathbb{Q}(r)$ dla dowolnego $r \in \mathbb{R}$ ($\mathbb{R}$ to zbiór liczb rzeczywistych) takiego, że $r \notin \mathbb{Q}$, ala $r^2 \in \mathbb{Q}$.

Formalnie można analogicznie zdefiniować $\mathbb{Q}(\sqrt{-1})$, czyli $\mathbb{Q}(i)$, gdzie i jest (nierzeczywistą) liczbą taką, że $i^2 = -1$. Działania w tym zbiorze są łatwe:

$$(a + bi) + (c + di) = (a + c) + (b + di), \qquad (a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$
$$(a + bi) - (c + di) = (a - c) + (b - di), \qquad \frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} + \frac{-ad + bc}{c^2 + d^2}\, i.$$

Co więcej, jednoznaczność: $a + bi = c + di$ wtedy i tylko wtedy, gdy $a = c$ i $b = d$, zachodzi nie tylko dla $a, b, c, d \in \mathbb{Q}$, lecz $a, b, c, d \in \mathbb{R}$. W istocie, niech $a + bi = c + di$. Jeśli $b = d$, to $a = c$, gdyby zaś $b \neq d$, to $i = (a - c)/(b - d)$ byłoby liczbą rzeczywistą.

Definicja 2.1. Symbol i oznacza *jednostkę urojoną*, czyli obiekt (na pewno nie liczbę rzeczywistą) o własności $i^2 = -1$. *Liczbą zespoloną* nazywany jest dowolny obiekt postaci $a + bi$, gdzie a, b są liczbami rzeczywistymi. Postać taką nazywa się *postacią algebraiczną*, liczbę a — *częścią rzeczywistą* liczby $a + bi$, zaś liczbę b — *częścią urojoną* liczby $a + bi$; oznaczenia: $a = \mathrm{Re}(a + bi)$, $b = \mathrm{Im}(a + bi)$. Zbiór liczb zespolonych oznaczany będzie przez $\mathbb{C}$. Operacje arytmetyczne na liczbach zespolonych zdefiniowane są powyższymi wzorami, przy czym dzielenie jest poprawnie określone, o ile dzielnik nie jest liczbą zerową, czyli $0 + 0i$.

Liczbę rzeczywistą a utożsamia się z liczbą zespoloną $a + 0i$. Jest to dopuszczalne, bowiem definicje działań na liczbach zespolonych zgadzają się z definicjami na liczbach rzeczywistych. Liczby zespolone oznaczać będziemy zwykle literami z, w.

TWIERDZENIE 2.2. Liczby zespolone tworzą *ciało liczbowe* dla wszystkich liczb zespolonych x, y, z:

$$x + y = y + x, \qquad (x + y) + z = x + (y + z), \qquad 0 + x = x,$$
$$xy = yx, \qquad (xy)z = x(yz), \qquad 1 \cdot x = x,$$
$$x(y + z) = xy + xz;$$

ponadto dla każdej liczby zespolonej x istnieje liczba y taka, że $x + y = 0$ (oznaczana $-x$) oraz, jeśli $x \neq 0$, liczba zespolona z taka, że $xz = 1$ (oznaczana x^{-1}).

Dowód. Jest do dość żmudne, ale w sumie proste ćwiczenie. □

Warto dodać, że $-(a + bi) = (-a) + (-b)i$ oraz $(a + bi)^{-1} = \dfrac{a}{a^2 + b^2} + \dfrac{-b}{a^2 + b^2}i$.

3. **Liczby zespolone: postać trygonometryczna**

Dodawanie i odejmowanie liczb zespolonych $z = a + bi$ oraz $w = c + di$ odpowiada dodawaniu i odejmowaniu wektorów $[a, b]$ oraz $[c, d]$ (w tym rozdziale $a, b, c, d, \varphi, \psi$ to liczby rzeczywiste, zaś r, s to nieujemne liczby rzeczywiste). Można zaobserwować następującą interpretację mnożenia liczb zespolonych z i w: trójkąty o wierzchołach 0, 1, z oraz 0, w, zw są do siebie podobne. [[rysunek]]

Aby powyższą własność uzasadnić formalnie, można wykorzystać własności podobieństwa trójkątów i definicję. Lepiej jednak wprowadzić nową postać liczb zespolonych, odpowiadającą *współrzędnym biegunowym*.

Definicja 3.1. *Cosinus* i *sinus* kąta φ to współrzędne wektora $[1, 0]$ obróconego o kąt φ w lewo (lub o kąt $-\varphi$ w prawo). Jeśli $r \geq 0$ oraz $z = r(\cos\varphi + i\sin\varphi)$, to r nazywane jest *modułem* liczby zespolonej z (oznaczenie: $|z|$), zaś φ — *argumentem* liczby zespolonej z, a omawiane przedstawienie to *postać trygonometryczna* liczby zespolonej z. [[rysunek]]

TWIERDZENIE 3.2. Każda liczba zespolona ma postać trygonometryczną. Ponadto moduł liczby zespolonej jest wyznaczony jednoznacznie: $|a + bi| = \sqrt{a^2 + b^2}$, zaś dla niezerowych liczb zespolonych argument jest wyznaczony z dokładnością do wielokrotności 2π: liczba φ jest argumentem liczby $a + bi \neq 0$ wtedy i tylko wtedy, gdy $\varphi + 2n\pi$ jest argumentem liczby $a + bi$ dla dowolnego $n \in \mathbb{Z}$ ($\mathbb{Z}$ to zbiór liczb całkowitych). [[rysunek]]

Dowód. Najprościej udowodnić to twiedzenie geometrycznie: jeśli r to długość wektora $[a, b]$, zaś φ to kąt między wektorami $[1, 0]$ i $[a, b]$, mierzony w kierunku przeciwnym do ruchu wskazówek zegara, to z definicji funkcji cosinus i sinus oraz podobieństwa odpowiednich figur zachodzi $a = r\cos\varphi$, $b = r\sin\varphi$. [[rysunek]] Wobec tego $a + bi = r(\cos\varphi + i\sin\varphi)$. Wzór $r = \sqrt{a^2 + b^2}$ to twierdzenie Pitagorasa — wzór na

długość wektora. Ponadto jeśli $a+bi \neq 0$, to kąt $\varphi \in [0, 2\pi)$ jest wyznaczony jednoznacznie i oczywiście można do niego dodać dowolną wielokrotność 2π. □

TWIERDZENIE 3.3. Zachodzi $(\cos\varphi+i\sin\varphi)(\cos\psi+i\sin\psi) = \cos(\varphi+\psi)+i\sin(\varphi+\psi)$.

Dowód. Wystarczy dowieść, że zachodzą wzory $\cos(\varphi+\psi) = \cos\varphi\cos\psi - \sin\varphi\sin\psi$ oraz $\sin(\varphi+\psi) = \cos\varphi\sin\psi + \sin\varphi\cos\psi$. W tym celu zauważmy, że zachodzi $[\cos\psi, \sin\psi] = \cos\psi \cdot [1,0] + \sin\psi \cdot [0,1]$. Współrzędne tego wektora obróconego dodatkowo o kąt φ to wobec tego z jednej strony $[\cos(\varphi+\psi), \sin(\varphi+\psi)]$ (obrót $[1,0]$ o ψ, a następnie o φ, to obrót o $\varphi+\psi$), a z drugiej strony — $\cos\psi \cdot [\cos\varphi, \sin\varphi] + \sin\psi \cdot [-\sin\varphi, \cos\varphi]$ (obrót wektorów jest operacją *liniową* — to wymaga uzasadnienia! — zaś obrót o $\frac{\pi}{2}$ odwzorowuje $[x,y]$ w $[-y,x]$). □

TWIERDZENIE 3.4. Zachodzi:

$$r(\cos\varphi + i\sin\varphi) \cdot s(\cos\psi + i\sin\psi) = rs(\cos(\varphi+\psi) + i\sin(\varphi+\psi)),$$

a jeśli $s > 0$, to również

$$\frac{r(\cos\varphi + i\sin\varphi)}{s(\cos\psi + i\sin\psi)} = \frac{r}{s}(\cos(\varphi-\psi) + i\sin(\varphi-\psi)).$$

Innymi słowy przy mnożeniu/dzieleniu liczb zespolonych ich moduły się mnożą/dzielą, zaś argumenty — dodają/odejmują.

Dowód. Pierwszy wzór to bezpośredni wniosek z poprzedniego twierdzenia. Drugi wynika łatwo z pierwszego i następującej definicji dzielenia: z/w to jedyna taka liczba zespolone, że $(z/w)\cdot w = z$. (Własność tę można udowodnić następująco: jeśli $x\cdot w = z$ oraz $y\cdot w = z$, to $(x-y)\cdot w = x\cdot w - y\cdot w = z - z = 0$, zatem $x - y = (x-y)\cdot w \cdot w^{-1} = 0 \cdot w^{-1} = 0$, skąd $x = y$). □

WNIOSEK 3.5 (wzór de Moivre'a). Dla $n \in \mathbb{Z}$, $n \neq 0$, zachodzi:

$$(r(\cos\varphi + i\sin\varphi))^n = r^n(\cos(n\varphi) + i\sin(n\varphi)).$$

a jeśli $s > 0$, to również

$$\frac{r(\cos\varphi + i\sin\varphi)}{s(\cos\psi + i\sin\psi)} = \frac{r}{s}(\cos(\varphi-\psi) + i\sin(\varphi-\psi)).$$

Innymi słowy przy mnożeniu/dzieleniu liczb zespolonych ich moduły się mnożą/dzielą, zaś argumenty — dodają/odejmują.

Dowód. Dla $n \geq 1$ dowód polega na n-krotnym zastosowaniu twierdzenia o iloczynie liczb zespolonych w postaci trygonometrycznej. Gdy $n \leq -1$, należy zapisać $z^n = 1/z^{-n}$, zastosować wzór de Moivre'a dla $-n$ i twierdzenie o ilorazie liczb zespolonych w postaci trygonometrycznej. □

Na zakończenie bardzo użyteczna definicja, która jednak nie będzie tu potrzebna.

Definicja 3.6. *Sprzężeniem* liczby zespolonej $z = a + bi$ nazywa się liczbę zespoloną $\bar{z} = a - bi$.

Warto odnotować, że $|z|^2 = a^2 + b^2 = z\bar{z}$. Ponadto jeśli $z = r(\cos\varphi + i\sin\varphi)$, to $\bar{z} = r(\cos(-\varphi) + i\sin(-\varphi))$, zaś $1/z = (1/r)(\cos(-\varphi) + i\sin(-\varphi))$.

4. **Liczby zespolone: pierwiastki zespolone**

Oprócz czterech działań arytmetycznych na liczbach zespolonych do formalnego sformułowania twierdzenia Abela–Ruffiniego potrzebne jest pojęcie pierwiastków zespolonych.

Definicja 4.1. *Pierwiastkiem zespolonym* liczby zespolonej w stopnia $n \in \mathbb{N}$ ($\mathbb{N}$ to zbiór dodatnich liczb całkowitych) nazywa się dowolną liczbę zespoloną z taką, że $z^n = w$.

TWIERDZENIE 4.2. Jeśli $w \neq 0$, to w ma dokładnie n pierwiastków zespolonych stopnia $n \in \mathbb{N}$. Jeśli $w = r(\cos\varphi + i\sin\varphi)$, gdzie $r > 0$, to pierwiastki zespolone stopnia n są dane wzorami

$$z_j = \sqrt[n]{r}\left(\cos\frac{\varphi + 2j\pi}{n} + i\sin\frac{\varphi + 2j\pi}{n}\right),$$

gdzie $j \in \mathbb{Z}$, przy czym wszystkich n pierwiastków można uzyskać, wybierając dowolnych n kolejnych wartości j, na przykład $j = 0, 1, \ldots, n-1$.

Dowód. Sprawdzenie, że $(z_j)^n = w$ sprowadza się do zastosowania wzoru de Moivre'a. Ponadto $z_j = z_k$ wtedy i tylko wtedy, gdy argumenty tych liczb różnią się o wielokrotność 2π, czyli gdy $(k-j)/n$ jest liczbą całkowitą. Stąd łatwo wynika druga część twierdzenia. □

W twierdzeniu $\sqrt[n]{r}$ oznacza *pierwiastek arytmetyczny*, czyli jedyną nieujemną liczbę rzeczywistą, której n-ta potęga wynosi r. Ten sam symbol $\sqrt[n]{z}$ będzie też często oznaczał *dowolny* pierwiastek zespolony liczby z.

TWIERDZENIE 4.3. Pierwiastki kwadratowe liczby zespolonej danej w postaci algebraicznej $a + bi$ są dane wzorami:

$$\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}+a)} + \sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}-a)}\,i,$$
$$-\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}+a)} - \sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}-a)}\,i$$

gdy $b \geq 0$ oraz wzorami

$$\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}+a)} - \sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}-a)}\,i,$$
$$-\sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}+a)} + \sqrt{\tfrac{1}{2}(\sqrt{a^2+b^2}-a)}\,i$$

gdy $b < 0$.

Dowód. Równanie $(x + yi)^2 = a + bi$ można przedstawić równoważnie w postaci układu równań $x^2 - y^2 = a$, $2xy = b$. Stąd $x^4 - \frac{1}{4}b^2 = ax^2$, czyli $(x^2 - \frac{a}{2})^2 = \frac{1}{4}(a^2 + b^2)$. Skoro $x^2 > 0$, zachodzi $x^2 = \frac{1}{2}(\sqrt{a^2+b^2} + a)$. Stąd łatwo $y^2 = x^2 - a = \frac{1}{2}(\sqrt{a^2+b^2} - a)$.

Ostatecznie otrzymujemy cztery możliwości, które po sprawdzeniu dają dwie odpowiedzi podane w treści twierdzenia. □

Pierwiastki zespolone stopnia 2 można zatem wyrazić przy pomocy pierwiastków arytmetycznych stopnia 2. Analogiczne stwierdzenie nie jest jednak prawdziwe dla pierwiastków zespolonych stopnia 3 — nie istnieje na przykład reprezentacja żadnej z trzech liczb $\sqrt[3]{2+i}$ (pierwiastków zespolonych stopnia trzy z $2+i$) przy pomocy stałych liczbowych, operacji arytmetycznych i pierwiastków arytmetycznych! Dowód tego faktu jest jednak skomplikowany — twierdzenie to nazywane jest *casus irreducibilis*.

5. **Wielomiany zespolone**

Wielomiany zespolone to wielomiany zmiennej zespolonej, o współczynnikach zespolonych.

Definicja 5.1. *Wielomian zespolony* to funkcja P zmiennej zespolonej dana wzorem

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_2 z^2 + a_1 z + a_0$$

dla pewnego $n \in \mathbb{N}_0$ ($\mathbb{N}_0$ to zbiór nieujemnych liczb całkowitych) i pewnych liczb zespolonych a_0, a_1, …, a_n, nazywanych *współczynnikami* wielomianu P. Jeśli $a_n \neq 0$, to n nazywane jest *stopniem* wielomianu P. Wielomian stale równy zero nie ma stopnia. *Pierwiastek* (zespolony) wielomianu P to liczba zespolona z_0 taka, że $P(z_0) = 0$.

Twierdzenie 5.2. Jeśli P jest wielomianem stopnia n, to dla dowolnej ustalonej liczby zespolonej z_0 funkcja $Q(z) = P(z + z_0)$ też jest wielomianem stopnia n.

Dowód. Wystarczy zauważyć, że funkcja $(z+z_0)^k$ jest wielomianem stopnia k dla każdego $k \in \mathbb{N}_0$. □

Twierdzenie 5.3 (Bézouta). Jeśli z_0 jest pierwiastkiem wielomianu P stopnia $n \in \mathbb{N}_0$, to istnieje wielomian $\tilde{P}$ stopnia $n-1$ taki, że $P(z) = (z - z_0)\tilde{P}(z)$.

Dowód. Niech $Q(z) = P(z + z_0)$ i niech $Q(z) = b_n z^n + b_{n-1} z^{n-1} + \ldots + b_2 z^2 + b_1 z + b_0$. Skoro $b_0 = Q(0) = P(z_0) = 0$, zachodzi $Q(z) = z\tilde{Q}(z)$ dla wielomianu $\tilde{Q}(z) = b_n z^{n-1} + b_{n-1} z^{n-2} + \ldots + b_2 z + b_1$ stopnia $n-1$. Stąd $P(z) = Q(z - z_0) = (z - z_0)\tilde{Q}(z - z_0)$. □

Wniosek 5.4. Wielomian zespolony stopnia $n \in \mathbb{N}_0$ ma co najwyżej n pierwiastków.

Dowód. Jeśli $n = 0$, twierdzenie jest prawdziwe. Ponadto jeśli z_0 jest pierwiastkiem wielomianu stopnia $n \geq 1$, to $P(z) = (z - z_0)\tilde{P}(z)$ dla pewnego wielomianu $\tilde{P}$ stopnia $n-1$. Zatem liczba pierwiastków P nie przekracza liczby pierwiastków $\tilde{P}$ powiększonej o 1. Wystarczy n-krotnie powtórzyć to rozumowanie. □

WNIOSEK 5.5. Jeśli P jest wielomianem stopnia n o współczynniku przy najwyższej potędze zmiennej a_n oraz o pierwiastkach $z_1, z_2, \ldots, z_n$, to $P(z) = a_n(z - z_1)(z - z_2)\ldots(z - z_n)$.

Dowód. Jeśli $n = 0$, twierdzenie jest prawdziwe. Ponadto jeśli z_n jest pierwiastkiem wielomianu stopnia $n \geq 1$, to $P(z) = (z - z_n)\tilde{P}(z)$ dla pewnego wielomianu $\tilde{P}$ stopnia $n - 1$. Wystarczy n-krotnie powtórzyć to rozumowanie. □

6. Ciągłość

Ciągłość to skomplikowane pojęcie, niezwykle ważne w dowodzie twierdzenia Abela–Ruffiniego. W niniejszych notatkach temat ten traktowany jest w nieco uproszczony sposób.

Definicja 6.1. Funkcja f, określona na pewnym zbiorze liczb rzeczywistych lub zespolonych, jest *ciągła* w punkcie x_0, jeśli dla dowolnie zadanej liczby $\varepsilon > 0$ istnieje odpowiednio mała liczba $\delta > 0$ taka, że z warunku $|x - x_0| < \delta$ wynika warunek $|f(x) - f(x_0)| < \varepsilon$. Funkcja jest *ciągła* jeśli jest ciągła w każdym punkcie swojej dziedziny.

Oczywiście funkcje $f(z) = a$ (funkcja stała) oraz $f(z) = z$ są ciągłe.

TWIERDZENIE 6.2. Dla dowolnych liczb zespolonych z, w zachodzi $|z+w| \leq |z|+|w|$.

Dowód. Najprostszy jest dowód geometryczny: jest to po prostu nierówność trójkąta. Analitycznie nierówność sprowadza się do postaci:

$$\sqrt{(a+c)^2 + (b+d)^2} \leq \sqrt{a^2+b^2} + \sqrt{c^2+d^2},$$

która po podniesieniu obu stron nierówności do kwadratu i redukcji wyrazów podobnych przyjmuje równoważną postać

$$ac + bd \leq \sqrt{a^2+b^2} \cdot \sqrt{c^2+d^2}.$$

Ponowne podniesienie do kwadratu i redukcja wyrazów podobnych prowadzi do mocniejszej nierówności

$$2abcd \leq a^2d^2 + b^2c^2,$$

równoważnej prawdziwej nierówności $(ad - bc)^2 \geq 0$. □

WNIOSEK 6.3. Dla dowolnych liczb zespolonych z, w zachodzi $||z| - |w|| \leq |z - w| \leq |z| + |w|$.

Dowód. Zachodzi $|z - w| \leq |z| + |-w|$, $|z| \leq |z - w| + |w|$ oraz $|w| \leq |w - z| + |z|$. □

Z nierówności $||z| - |w|| \leq |z - w|$ natychmiast wynika ciągłość funkcji $f(z) = |z|$.

TWIERDZENIE 6.4. Suma funkcji ciągłych jest ciągła.

Dowód. Jeśli $\varepsilon > 0$, $|f(x) - f(x_0)| < \frac{1}{2}\varepsilon$ gdy $|x - x_0| < \delta_1$ oraz $|g(x) - g(x_0)| < \frac{1}{2}\varepsilon$ gdy $|x - x_0| < \delta_2$, to $|(f+g)(x) - (f+g)(x_0)| \leq |f(x) - f(x_0)| + |g(x) - g(x_0)| < \varepsilon$ gdy $|x - x_0| < \min(\delta_1, \delta_2)$. □

TWIERDZENIE 6.5. Iloczyn funkcji ciągłych jest ciągły. Iloraz funkcji ciągłych jest ciągły (tam, gdzie jest określony, czyli gdzie mianownik się nie zeruje).

Dowód. Jeśli $\eta > 0$, $|f(x) - f(x_0)| < \eta$ gdy $|x - x_0| < \delta_1$ oraz $|g(x) - g(x_0)| < \eta$ gdy $|x - x_0| < \delta_2$, to

$$\begin{aligned}
&|(f \cdot g)(x) - (f \cdot g)(x_0)| \\
&= |(f(x) - f(x_0))(g(x) - g(x_0)) + f(x_0)(g(x) - g(x_0)) + (f(x) - f(x_0))g(x_0)| \\
&\leq |f(x) - f(x_0)||g(x) - g(x_0)| + |f(x_0)||g(x) - g(x_0)| + |f(x) - f(x_0)||g(x_0)| \\
&< \eta^2 + |f(x_0)|\eta + \eta|g(x_0)| = \eta(\eta + |f(x_0)| + |g(x_0)|)
\end{aligned}$$

gdy $|x - x_0| < \min(\delta_1, \delta_2)$. Należy na początku obrać $\eta = \min(1, \varepsilon/(1 + |f(x_0)| + |g(x_0)|))$ dla pewnego $\varepsilon > 0$: wtedy $|(f \cdot g)(x) - (f \cdot g)(x_0)| < \varepsilon$ gdy $|x - x_0| < \min(\delta_1, \delta_2)$, co oznacza ciągłość $f \cdot g$ w x_0.

Analogicznie jeśli $g(x_0) \neq 0$, $\eta > 0$ oraz $|g(x) - g(x_0)| < \eta$ gdy $|x - x_0| < \delta$, to $|g(x)| = |g(x_0) - (g(x_0) - g(x))| \geq |g(x_0)| - |g(x_0) - g(x)| > |g(x_0)| - \eta$, zatem jeśli $\eta < |g(x_0)|$, to

$$\left|\frac{1}{g(x)} - \frac{1}{g(x_0)}\right| = \frac{|g(x_0) - g(x)|}{|g(x)|\,|g(x_0)|} \leq \frac{\eta}{(|g(x_0)| - \eta)|g(x_0)|}\,.$$

Jeśli więc na początku obrać $\eta = \min(\frac{1}{2}|g(x_0)|, \frac{1}{2}\varepsilon|g(x_0)|^2)$, to $|1/g(x) - 1/g(x_0)| < \varepsilon$ gdy $|x - x_0| < \delta$. Oznacza to ciągłość $1/g$ w x_0. Ostatecznie $f/g = f \cdot (1/g)$ jest ciągła w x_0. □

TWIERDZENIE 6.6. Wielomiany są ciągłe.

Dowód. Wystarczy zastosować odpowiednio wiele razy poprzednie twierdzenia i własności funkcji stałych oraz $f(z) = z$. □

TWIERDZENIE 6.7. Złożenie funkcji ciągłych jest ciągłe.

Dowód. Niech $y_0 = g(x_0)$. Jeśli $|f(y) - f(y_0)| < \varepsilon$ gdy $|y - y_0| < \eta$ oraz $|g(x) - g(x_0)| < \eta$ gdy $|x - x_0| < \delta$, to $|f(g(x)) - f(g(x_0))| < \varepsilon$ gdy $|x - x_0| < \delta$. □

Funkcja f jest *ograniczona z góry*, jeśli dla pewnej liczby rzeczywistej M zachodzi $f(z) \leq M$ dla wszystkich z z dziedziny funkcji f. Liczbę taką nazywa się *ograniczeniem z góry*. Analogicznie określa się ograniczenia z dołu.

TWIERDZENIE 6.8 (Bolzano–Weierstrassa). Funkcja o wartościach rzeczywistych, określona na ograniczonym zbiorze liczb zespolonych z brzegiem (np. w kole z brzegiem) i ciągła w tym zbiorze, osiąga wartość największą i wartość najmniejszą.

Szkic dowodu. Wystarczy udowodnić, że rozważana funkcja f osiąga wartość największą — dowód drugiej części jest analogiczny.

Wpierw dowodzi się, że f jest ograniczona z góry. Gdyby tak nie było, możliwa byłaby konstrukcja liczby $a+bi$ o następującej własności: dla dowolnego $n \in \mathbb{N}$ funkcja f jest nieograniczona z góry na kwadracie o boku 10^{-n}, złożonym z liczb zespolonych $w = c+di$ takich, że c i a oraz d i b mają jednakowe cyfry do n-tego miejsca po przecinku (w każdym kroku taki kwadrat dzielony jest na sto mniejszych kwadratów — w co najmniej jednym z nich funkcja musi być nieograniczona z góry!). Istnienie takiej liczby z przeczy jednak definicji ciągłości f w z.

Zbiór liczb, które są ograniczeniami z góry f, jest przedziałem. Niech M będzie jego lewym końcem. Gdyby $f(z) < M$ dla wszystkich z, powyższe rozumowanie można by przeprowadzić dla (ciągłej!) funkcji $g(z) = 1/(M - f(z))$. Funkcja ta byłaby więc ograniczona z góry przez pewną liczbę K (i oczywiście $K > 0$), co by z kolei oznaczało, że $f(z) < M - 1/K$ dla wszystkich z. Ale liczby mniejsze od M nie są ograniczeniami z góry, bowiem M jest lewym końcem przedziału złożonego z tych liczb! Uzyskana sprzeczność kończy dowód. □

7. Zasadnicze twierdzenie algebry

Poniżej przedstawiony jest (niemal formalny) dowód najważniejszego twierdzenia w algebrze.

> Twierdzenie 7.1 (zasadnicze twierdzenie algebry). Każdy wielomian zespolony stopnia $n \in \mathbb{N}$ ma pierwiastek.

Dowód wykorzystuje kilka pomocniczych twierdzeń.

> Lemat 7.2. Jeśli P jest wielomianem stopnia $n \in \mathbb{N}$ oraz $P(z_0) \neq 0$, to $|P(z_1)| < |P(z_0)|$ dla pewnej liczby zespolonej z_1.

[[dowód na przykładzie]]

Dowód. Bez utraty ogólności można przyjąć, że $z_0 = 0$ (rozważając w razie potrzeby wielomian $P(z_0 + z)$). Niech $P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_2 z^2 + a_1 z + a_0$, gdzie $a_0 = P(0) \neq 0$. Bez utraty ogólności można przyjąć, że $a_0 = 1$ (rozważając w razie potrzeby wielomian $P(z)/a_0$). Niech $k \in \mathbb{N}$ będzie taką liczbą, że $a_1 = a_2 = \ldots a_{k-1} = 0$, lecz $a_k \neq 0$. Niech ponadto $Q(z) = a_n z^{n-k-1} + a_{n-1} z^{n-k-2} + \ldots + a_{k+2} z + a_{k+1}$ i niech w będzie pierwiastkiem zespolonym stopnia k z $-1/a_k$. Wówczas dla $t \in (0,1)$ zachodzi:

$$\begin{aligned} |P(tw)| &= |1 + a_k (tw)^k + (tw)^{k+1} Q(tw)| \\ &= |1 - t^k + (tw)^{k+1} Q(tw)| \leq 1 - t^k + t^{k+1} |w^{k+1} Q(tw)|. \end{aligned}$$

Funkcja $|Q(tw)|$, określona dla $t \in [0,1]$ (liczba w jest ustalona), jest ograniczona z góry przez $M = (|a_n| + |a_{n-1}| + \ldots + |a_{k+1}|)(1 + |w|)^{n-k-1}$, bowiem

$$\begin{aligned} |Q(tw)| &\leq |a_n| t^{n-k-1} |w|^{n-k-1} + |a_{n-1}| t^{n-k-2} |w|^{n-k-2} + \ldots + |a_{k+2}| t |w| + |a_{k+1}| \\ &\leq (|a_n| + |a_{n-1}| + \ldots + |a_{k+2}| + |a_{k+1}|)(1 + |w|)^{n-k-1}. \end{aligned}$$

Niech $t \in (0,1)$ spełnia warunek $|w^{k+1}| M t < \frac{1}{2}$. Wtedy

$$|P(tw)| \leq 1 - t^k + \tfrac{1}{2} t^k < 1 = |P(0)|.$$

□

LEMAT 7.3. Jeśli P jest wielomianem stopnia $n \in \mathbb{N}$ to dla każdej liczby M istnieje liczba K taka, że $|P(z)| > M$ gdy $|z| > K$.

Dowód. Niech $P(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0$ i niech $Q(w) = a_0 w^n + a_1 w^{n-1} + \ldots + a_{n-1} w + a_0$. Wówczas dla $z \neq 0$ zachodzi $P(z) = z^n Q(1/z)$.

Funkcja $f(w) = |Q(w)|$ jest ciągła w punkcie 0 (złożenie wielomianu i modułu, funkcji ciągłych), zatem dla $\varepsilon = \frac{1}{2}|a_n|$ istnieje $\delta > 0$ taka, że jeśli $|w| < \delta$, to $|f(w) - f(0)| < \varepsilon$. Skoro $f(0) = a_n$, zachodzi

$$|f(w)| = |f(0) - (f(0) - f(w))| \geq |f(0)| - |f(w) - f(0)| > |f(0)| - \varepsilon = \tfrac{1}{2}|a_n|.$$

Wobec tego gdy $|z| > 1/\delta$, zachodzi

$$|P(z)| = |z|^n f(1/z) > \tfrac{1}{2}|a_n||z|^n.$$

Jeśli przy tym $|z| > \sqrt[n]{2M/|a_n|}$, to $|P(z)| > M$. Teza lematu zatem zachodzi, jeśli $K = \max(1/\delta, \sqrt[n]{2M/|a_n|})$. □

Dowód zasadniczego twierdzenia algebry. Niech $M = |P(0)|$. Na mocy drugiego lematu istnieje liczba K taka, że jeśli $|z| > K$, to $|P(z)| > M$. Ponadto funkcja $f(z) = |P(z)|$, określona w kole $|z| \leq K$, jest ciągła, a więc przyjmuje wartość najmniejszą. Niech z_0 będzie punktem, w którym f osiąga wartość njamniejszą. Wówczas $|P(z_0)| \leq |P(z)|$ dla wszystkich z: gdy $|z| \leq K$, wynika to z definicji z_0, gdy zaś $|z| > K$ jest to konsekwencją nierówności $|P(z)| > |P(0)| \geq P(z_0)$. Z pierwszego lematu wynika, że $|P(z_0)| = 0$, czyli wielomian P ma pierwiastek. □

8. **Wzory Viète'y**

Z zasadniczego twierdzenia algebry i twierdzenia Bézouta natychmiast wynika, że każdy wielomian zespolony jest postaci

$$P(z) = a_n(z - z_1)(z - z_2)\ldots(z - z_n), \tag{8.1}$$

gdzie z_1, z_2, …, z_n to pierwiastki P, powtórzone odpowiednią liczbę razy. W większości przypadków można przyjąć, że $a_n = 1$ — takie wielomiany nazywa się *monicznymi*.

TWIERDZENIE 8.1. Współczynniki wielomianu są ciągłymi funkcjami pierwiastków, danymi wzorami:

$$\begin{aligned}
a_{n-1} &= -(z_1 + z_2 + \ldots + z_n),\\
a_{n-2} &= z_1 z_2 + z_1 z_3 + \ldots + z_{n-1} z_n,\\
a_{n-3} &= -(z_1 z_2 z_3 + z_1 z_2 z_4 + \ldots + z_{n-2} z_{n-1} z_n),\\
&\vdots\\
a_1 &= (-1)^{n-1}(z_1 z_2 \ldots z_{n-1} + z_1 z_2 \ldots z_{n-2} z_n + \ldots + z_2 z_3 \ldots z_n),\\
a_0 &= (-1)^n z_1 z_2 \ldots z_n.
\end{aligned}$$

Dowód. Wystarczy otworzyć nawiasy we wzorze (8.1). Ciągłość oznacza następującą własność: jeśli z_1, z_2, …, z_n zależą w sposób ciągły od parametru t, to również a_0, a_1, …, a_{n-1} zależą w sposób ciągły od t — wynika to z twierdzeń o iloczynie i sumie funkcji ciągłych. □

Zależność współczynników od pierwiastków jest *symetryczna*: dowolna zamiana kolejności pierwiastków nie zmienia wartości współczynników.

9. **Krzywe**

W dowodzie twierdzenia Abela–Ruffiniego kluczową rolę odgrywają krzywe.

Definicja 9.1. *Krzywa* na płaszczyźnie zespolonej to ciągła funkcja Z o wartościach zespolonych, określona na pewnym przedziale $[a,b]$. *Pętla* lub *krzywa zamknięta* to krzywa o tym samym początku i końcu, czyli spełniająca równanie $Z(a) = Z(b)$. *Krzywa przeciwna*, oznaczana symbolem $\hat{Z}$, to krzywa z odwóconym czasem: $\hat{Z}(t) = Z(-t)$ dla $t \in [-b,-a]$.

Przykładem krzywej jest odcinek: $Z(t) = z_0 + t(z_1 - z_0)$ (gdzie $t \in [0,1]$), przykładem pętli — okrąg: $Z(t) = z_0 + r(\cos t + i \sin t)$ (gdzie $t \in [0, 2\pi]$).

Utożsamiamy krzywe, które różnią się wyłącznie parametryzacją: każda krzywa Z określona na $[a,b]$ jest więc równoważna krzywej określonej na $[0,1]$, danej wzorem $Z(a + t(b-a))$.

Twierdzenie 9.2. Jeśli Z jest krzywą nieprzecinającą zera, to istnieją ciągłe funkcje R i Φ takie, że $R(t) = |Z(t)|$ i $\Phi(t)$ jest argumentem $Z(t)$, czyli

$$Z(t) = R(t)(\cos \Phi(t) + i \sin \Phi(t)) \tag{9.1}$$

dla $t \in [a,b]$. Co więcej, funkcja Φ jest wyznaczona jednoznacznie, z dokładnością do wielokrotności 2π, zaś każda para ciągłych funkcji R i Φ odpowiada pewnej krzywej, danej wzorem (9.1).

Szkic dowodu. Funkcja $R(t) = |Z(t)|$ jest ciągła, bo jest złożeniem funkcji ciągłych. Ponadto dla dowolnego $t_0 \in [a,b]$ istnieje $\delta > 0$ o następującej własności: jeśli $|t - t_0| < \delta$ (i oczywiście $t \in [a,b]$), to $|Z(t) - Z(t_0)| < |Z(t_0)|$, czyli $|Z(t)/Z(t_0) - 1| < 1$, a co za tym idzie, $\operatorname{Re}(Z(t)/Z(t_0)) > 0$. Wobec tego w przedziale $(t_0 - \delta, t_0 + \delta)$ funkcja $\varphi(t) = \operatorname{arctg}(\operatorname{Im}(Z(t)/Z(t_0))/\operatorname{Re}(Z(t)/Z(t_0)))$ jest poprawnie określona i ciągła. Niech I będzie maksymalnym przedziałem, na którym można określić ciągłą funkcją $\Phi(t)$ o omawianych własnościach (dlaczego taki maksymalny przedział istnieje?) i niech t_0 będzie końcem I. Niech ponadto t_1 będzie wspólnym punktem przedziałów I oraz $(t_0 - \delta, t_0 + \delta)$. Wtedy $\Phi(t) - \Phi(t_1) = \varphi(t) - \varphi(t_1)$ dla wszystkich $t \in I \cap (t_0 - \delta, t_0 + \delta)$ (dlaczego?), co pozwala rozszerzyć definicję Φ do funkcji ciągłej na sumie przedziałów I oraz $(t_0 - \delta, t_0 + \delta) \cap [a,b]$. Stąd łatwo wynika, że $I = [a,b]$. □

Twierdzenie 9.3. Jeśli Z jest krzywą nieprzecinającą zera daną wzorem (9.1) oraz $n \in \mathbb{N}$, $j \in \mathbb{Z}$, to krzywe

$$W_j(t) = \sqrt[j]{R(t)} \left(\cos \frac{\Phi(t) + 2j\pi}{n} + i \sin \frac{\Phi(t) + 2j\pi}{n} \right) \tag{9.2}$$

(nazywane *ciągłymi pierwiastkami zespolonymi* krzywej Z) spełniają warunek $(W_j(t))^n = Z(t)$. Rodzina ta składa się z dokładnie n różnych krzywych.

Jeśli Z jest pętlą, to W_j nie muszą być pętlami — istnieje jednak liczba $\omega \in \mathbb{Z}$ (nazywana *liczbą obrotu* Z) taka, że $\Phi(b) = \Phi(a) + 2\pi\omega$, i w związku z tym $W_j(b) = W_{j+\omega}(a)$.

Dowód. Wystarczy zastosować poprzednie twierdzenie. □

Definicja 9.4. *Złączeniem* dwóch krzywych Z_1 i Z_2 nazywa się krzywą $W = Z_1 \oplus Z_2$, która najpierw przebiega Z_1, a następnie Z_2, przy czym zakłada się, że koniec Z_1 jest równy początkowi Z_2. Bez utraty ogólności można przyjąć, że Z_1 i Z_2 są określone na $[0, 1]$; wtedy $W(t) = Z_1(2t)$ dla $t \in [0, \frac{1}{2}]$ oraz $W(t) = Z_2(2t - 1)$ dla $t \in [\frac{1}{2}, 1]$ (przy czym $Z_1(1) = Z_2(0)$). *Komutatorem* dwóch krzywych Z_1 i Z_2 nazywa się krzywą $Z_1 \oplus Z_2 \oplus \hat{Z}_1 \oplus \hat{Z}_2$.

Twierdzenie 9.5 (o pierwiastkowaniu komutatora). Jeśli Z i Z' są pętlami nieprzecinającymi zera, o tym samym początku (i końcu), to złączenia odpowiednich ciągłych pierwiastków zespolonych stopnia $n \in \mathbb{N}$ z Z, Z', $\hat{Z}$ i $\hat{Z}'$ są pętlami. Ściślej, jeśli ω i ω' to liczby obrotu Z i Z' oraz W_j i W'_j są dane wzorami takimi, jak (9.1), to $W_j \oplus W'_{j+\omega} \oplus \hat{W}_{j+\omega+\omega'} \oplus \hat{W}'_{j+\omega'}$ jest pętlą, której n-ta potęga zespolona to $Z \oplus Z' \oplus \hat{Z} \oplus \hat{Z}'$.

Dowód. Wystarczy zastosować poprzednie twierdzenie (i sprawdzić, że odpowiednie początki i końce kolejnych krzywych są zgodne). □

10. **Twierdzenie Abela–Ruffiniego**

Formalne sformułowanie twierdzenia Abela–Ruffiniego wykorzystuje następującą definicję.

Definicja 10.1. Niech $a_0, a_1, \ldots, a_{n-1}$ będą współczynnikami wielomianu monicznego. Wyrażenie rzędu 0 to dowolna funkcja $f(a_0, a_1, \ldots, a_{n-1})$, która dana jest wzorem, wykorzystującym wyłącznie stałe liczbowe, współczynniki a_0, a_1, …, a_{n-1} i operacje arytmetyczne. Wyrażenie rzędu 1 to wielkość dana wzorem, w którym dodatkowo mogą się pojawić pierwiastki zespolone (dowolnego stopnia) wyrażeń rzędu 0. Wyrażenie rzędu $r \in \mathbb{N}$ jest dane w analogiczny sposób, ale może uwzględniać pierwiastki zespolone wyrażeń rzędu mniejszego niż r.

Wyrażenie rzędu $r \in \mathbb{N}$ może mieć wiele wartości: przy każdym pierwiastku zespolonym stopnia k jest k możliwości wyboru, a pierwiastki zespolone mogą dodatkowo się zagnieżdżać. Bez utraty ogólności będziemy pomijać w wyrażeniach człony stale równe zero.

Przykład. Wyrażenie rzędu 0: $-a_0$ opisuje pierwiastek wielomianu $z + a_0$.

Przykład. Wyrażenie rzędu 1: $\frac{1}{2}(-a_1 + \sqrt{a_1^2 - 4a_0})$ opisuje *oba* pierwiastki wielomianu $z^2 + a_1 z + a_0$.

Definicja 10.2. *Operacja* na pierwiastkach z_1, z_2, …, z_n wielomianu stopnia $n \in \mathbb{N}$ to dowolny układ krzywych Z_1, Z_2, …, Z_n określonych na tym samym przedziale — dla ustalenia uwagi $[0,1]$ — o następujących własnościach: układ liczb $(Z_1(1), Z_2(1), \ldots, Z_n(1))$ jest przestawieniem układu liczb $(Z_1(0), Z_2(0), \ldots, Z_n(0))$. Operacja *przeciwna* to operacja składająca się z przeciwnych krzywych. *Złączenie* operacji to złączenie odpowiednich krzywych (tak, aby koniec pierwszej był równy początkowi drugiej). *Komutator* dwóch operacji to układ komutatorów odpowiednich krzywych. Dowolną operację nazywa się 0-*krotnym komutatorem*. Komutator operacji, które same są $(n-1)$-krotnymi komutatorami, nazywa n-*krotnym komutatorem*.

> Twierdzenie 10.3. Jeśli pierwiastki wielomianu poddawane są operacji, to odpowiadające im współczynniki wielomianu zataczają pętle. Złączenie operacji odpowiada złączeniu pętli zataczanych przez współczynniki.

Dowód. Współczynniki $A_0(t)$, $A_1(t)$, …, $A_{n-1}(t)$ wielomianu P_t o pierwiastkach $Z_1(t)$, $Z_2(t)$, …, $Z_n(t)$ dane są wzorami Viète'y, są więc ciągłymi funkcjami t — czyli krzywymi. Ponadto wielomiany P_0 i P_1 mają te same pierwiastki (uporządkowane być może w innej kolejności), zatem współczynniki zataczają pętle. □

[[przykłady, rysunki, animacje]]

Plan dowodu twierdzenia Abela–Ruffiniego jest następujący: wykonana będzie odpowiednia operacja na pierwiastkach wielomianu, opisana przez krzywe Z_1, Z_2, …, Z_n. Współczynniki wielomianu zakreślą pętle A_0, A_1, …, A_{n-1}. Wszystkie wartości ustalonego wyrażenia zatoczą zatem pewne krzywe. Operacja będzie tak dobrana, by na końcu wartości wyrażenia powróciły do punktu wyjścia (czyli zatoczyły pętle), natomiast pierwiastki — nie.

> Twierdzenie 10.4. Dla dowolnego wyrażenia istnieje układ parami różnych pierwiastków $(z_1, z_2, \ldots, z_n)$ o następującej własności: dla dowolnego układu $(\tilde{z}_1, \tilde{z}_2, \ldots, \tilde{z}_n)$, który jest przestawieniem układu $(z_1, z_2, \ldots, z_n)$, istnieje operacja spełniająca warunki $Z_j(0) = z_j$, $Z_j(1) = \tilde{z}_j$ i taka, że przy obliczaniu dowolnej wartości zadanego wyrażenia nie występuje dzielenie przez zero ani pierwiastkowanie zera oraz wszystkie pierwiastki w każdej chwili są parami różne.

Słowo o dowodzie. Dowód tego twierdzenia wymaga wiedzy o miejscach zerowych funkcji zespolonych wielu zmiennych i zdecydowanie przekracza zakres tego kursu. Idea jest następująca: rozważmy dowolny układ parami różnych pierwiastków $(z_1, z_2, \ldots, z_n)$, dla którego obliczanie rozważanego wyrażenia nie wiąże się z dzieleniem przez zero czy pierwiastkowaniem zera. Rozważmy dowolne przestawienie tego układu $(\tilde{z}_1, \tilde{z}_2, \ldots, \tilde{z}_n)$ i operację $Z_j(0) = (1-t)z_j + t\tilde{z}_j$. Jeśli dla pewnego t_0 obliczenie którejś z wartości zadanego wyrażenia wiąże się z dzieleniem przez zero czy pierwiastkowaniem zera lub też pewne dwa pierwiastki są sobie równe, należy odpowiednio zmodyfikować operację w pewnym otoczeniu t_0. Dzięki własnościom funkcji zespolonych wiadomo, że takich punktów t_0 będzie skończenie wiele, zaś dla każdego z nich odpowiednia modyfikacja jest możliwa. □

> Twierdzenie 10.5. Dla dowolnego $r \in \mathbb{N}_0$, wartości dowolnego wyrażenia rzędu r zataczają pętle jeśli pierwiastki wielomianu są poddane r-krotnemu komutatorowi operacji (takich, przy których w wyrażeniu nie występuje pierwiastkowanie zera).

Dowód. Teza jest oczywiście prawdziwa dla $r = 0$: jeśli pierwiastki poddane są operacji, to współczynniki zataczają pętle, a więc i wyrażenia rzędu 0 (ciągłe funkcje współczynników) zataczają pętle.

Przypuśćmy, że wszystkie wyrażenia ustalonego rzędu r zataczają pętle gdy pierwiastki wielomianu poddawane są r-krotnym komutatorom operacji. Na mocy twierdzenia o pierwiastkowaniu komutatora pierwiastki zespolone z wyrażeń rzędu r zataczają pętle gdy pierwiastki wielomianu poddawane są $(r+1)$-krotnym komutatorom operacji. Oznacza to, że pętle zataczają też wyrażenia rzędu $r + 1$.

Teza twierdzenia wynika z zastosowania powyższego rozumowania odpowiednią liczbę razy. □

TWIERDZENIE 10.6 (Abela–Ruffiniego). Nie istnieje wyrażenie rzędu $r \in \mathbb{N}$, które opisuje pierwiastki zespolone dowolnego wielomianu monicznego przy pomocy jego współczynników.

Dowód. Przypuśćmy, że takie wyrażenie istnieje. Dobierzmy pierwiastki wielomianu zgodnie z twierdzeniem 10.4. Zgodnie z twierdzeniem 10.5, pierwiastki wielomianu poddane r-krotnemu komutatorowi operacji (takich, jak w twierdzeniu 10.4) muszą wrócić do punktu wyjścia (są bowiem stale opisane przez wartości wyrażenia). Jeśli jednak $n \geq 5$, to istnieje r-krotny komutator operacji, który istotnie zamienia pierwiastki — mówi o tym kolejny wynik. □

LEMAT 10.7. Jeśli pierwsza operacja zamienia cyklicznie pierwiastki z_1, z_2 i z_4, zaś druga — z_5, z_3 i z_2, to ich komutator zamienia cyklicznie pierwiastki z_1, z_2, z_3. Jeśli zatem $n \geq 5$, to istnieje r-krotny komutator operacji (zgodnych z twierdzeniem 10.4), który zamienia cyklicznie pierwiastki z_1, z_2 i z_3.

Dowód. Wystarczy sprawdzić, że z_1 przejdzie kolejno na: z_2, z_5, z_5 i z_2; z_2 — na z_4, z_4, z_2, z_3; z_3 — na z_3, z_2, z_1, z_1; z_4 — na z_1, z_1, z_4, z_4; wreszcie z_5 — na z_5, z_3, z_3, z_5. □

11. **Permutacje**

W dowodzie twierdzenia Abela–Ruffiniego, podobnie jak i w teorii Galois istnienia wzorów na pierwiastki wielomianów, ważną rolę odgrywają *permutacje* pierwiastków. Pojęcie permutacji jest doskonałym wprowadzeniem do teorii grup.

Definicja 11.1. *Permutacja* zbioru skończonego A to wzajemnie jednoznaczna funkcja σ określona na A i o wartościach w A. Najczęściej zakłada się, że $A = \{1, 2, 3, \ldots, n\}$ dla pewnej liczby naturalnej n. W tej sytuacji permutacje zapisuje się w postaci:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix};$$

aby odnaleźć wartość permutacji $\sigma(j)$ dla zadanego argumentu j, należy odnaleźć j w górnym rzędzie i odczytać odpowiadającą mu wartość $\sigma(j)$ w dolnym rzędzie

(wyrazy w górnym rzędzie nie muszą być uporządkowane, ale zwykle wygodniej jest pisać właśnie w ten sposób).

Permutacje można mnożyć.

Definicja 11.2. *Iloczynem* (lub *złożeniem*) permutacji σ i τ nazywa się permutację $\sigma\cdot\tau$ (lub $\sigma\tau$) określoną wzorem $(\sigma\cdot\tau)(j)=\tau(\sigma(j))$. (Stosowana jest często odwrotna konwencja, w której tak określona permutacja jest oznaczana $\tau\cdot\sigma$).

Permutacją jednostkową (lub *permutacją stałą*, *permutacją identycznościową*) nazywa się permutację I daną wzorem $I(j)=j$. *Permutacja odwrotna* do permutacji σ to permutacja $\hat\sigma$ (oznaczana też σ^{-1}) taka, że $\hat\sigma(j)=k$ wtedy i tylko wtedy, gdy $\sigma(k)=j$.

Twierdzenie 11.3. Permutacja odwrotna jest poprawnie określona oraz $\sigma\cdot\hat\sigma=I=\hat\sigma\cdot\sigma$. Ponadto każda z tych równości charakteryzuje permutację odwrotną do σ.

Mnożenie permutacji jest łączne: $\sigma\cdot(\tau\cdot\pi)=(\sigma\cdot\tau)\cdot\pi$. Zachodzi $I\cdot\sigma=\sigma=\sigma\cdot I$. Ponadto permutacją odwrotną do $\sigma\cdot\tau$ jest $\hat\tau\cdot\hat\sigma$.

Dowód. Dla dowolnego j istnieje jedyne k takie, że $\sigma(k)=j$, zatem $\hat\sigma$ jest poprawnie określoną funkcją. Jest też wzajemnie jednoznaczna, bowiem różnym wartościom j odpowiadają oczywiście różne wartości k.

Jeśli $\sigma(j)=k$, to $\hat\sigma(\sigma(j))=\hat\sigma(k)=j$ oraz $\sigma(\hat\sigma(k))=\sigma(j)=k$, zatem $\sigma\cdot\hat\sigma=I$ oraz $\hat\sigma\cdot\sigma=I$. Ponadto jeśli $\sigma\cdot\tau=I$, to z warunku $\sigma(j)=k$ wynika, że $\tau(k)=j$, czyli $\tau=\hat\sigma$. Analogicznie jeśli $\tau\cdot\sigma=I$, to z warunku $\sigma(j)=k$ wynika, że $\tau(k)=j$, czyli $\tau=\hat\sigma$.

Zachodzi $((\sigma\cdot\tau)\cdot\pi)(j)=\pi((\sigma\cdot\tau)(j))=\pi(\tau(\sigma(j)))=(\tau\cdot\pi)(\sigma(j))=(\sigma\cdot(\tau\cdot\pi))(j)$, skąd wynika łączność mnożenia permutacji.

Skoro $I(\sigma(j))=\sigma(j)=\sigma(I(j))$, zachodzi $\sigma\cdot I=\sigma=I\cdot\sigma$. Ponadto $(\sigma\cdot\tau)\cdot(\hat\tau\cdot\hat\sigma)=\sigma\cdot(\tau\cdot\hat\tau)\cdot\hat\sigma=\sigma\cdot I\cdot\hat\sigma=\sigma\cdot\hat\sigma=I$. □

Zbiór wszystkich permutacji jest więc *grupą*: zbiorem z łącznym działaniem, w którym istnieje element neutralny (I) oraz do każdego elementu istnieje element odwrotny ($\hat\sigma$) — jest to tzw. *grupa symetryczna* $\mathbb{S}_n$.

Przykład. Zachodzi $\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$ oraz $\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$, zatem mnożenie permutacji nie jest przemienne.

Przykład. Jeśli $\sigma=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$, to $\hat\sigma=\begin{pmatrix}2&3&1&4\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$.

12. **Rozkład na cykle**

Wyróżnie się kilka ważnych klas permutacji; najważniejsze to cykle, czyli permutacje, które cyklicznie zamieniają wybrane elementy. Poniżej rozważane są permutacje zbioru $\{1,2,3,\dots,n\}$ dla ustalonej wartości n.

Definicja 12.1. *Cyklem* o długości r i wyrazach $j_1, j_2, \ldots, j_r$ nazywana jest permutacja σ dana wzorami $\sigma(j_m) = j_{m+1}$ dla $m = 1, 2, \ldots, r-1$; $\sigma(j_r) = j_1$, oraz $\sigma(k) = k$ jeśli $k \in \{1, 2, \ldots, n\} \setminus \{j_1, j_2, \ldots, j_r\}$, przy czym zakłada się, że liczby $j_1, j_2, \ldots, j_r$ są parami różne. Taki cykl oznacza się $\sigma = (j_1, j_2, \ldots, j_r)$. Cykl długości 2 nazywany jest *transpozycją*; cykl długości 1 to permutacja jednostkowa.

Z zapisu $(j_1, j_2, \ldots, j_r)$ nie wynika wartość n; na szczęście niemal zawsze jest ona znana z kontekstu lub nie ma znaczenia.

Przykład. Dla $n = 5$ zachodzi $(1,2,3,4,5) = (2,3,4,5,1) = (4,5,1,2,3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, $(1,2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$, $(3,1,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$.

Każdy cykl długości $r \geq 2$ można zapisać w postaci $(j_1, j_2, \ldots, j_r)$ na dokładnie r sposobów — ten sam cykl opisany jest wzorami $(j_2, j_3, \ldots, j_r, j_1)$, $(j_3, j_4, \ldots, j_r, j_1, j_2)$ itd. Permutacją odwrotną do cyklu $(j_1, j_2, \ldots, j_r)$ jest cykl $(j_r, j_{r-1}, \ldots, j_1)$. Transpozycje są permutacjami odwrotnymi do samych siebie.

Przykład. Zachodzi $(1,2,3) \cdot (2,4) = (1,4,2,3)$ oraz $(2,4) \cdot (1,2,3) = (1,2,4,3)$, zatem mnożenie cykli nie jest przemienne. Ponadto $(1,2,3) \cdot (2,3,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1,3) \cdot (2,4) = (2,4) \cdot (1,3)$, a więc iloczyn cykli nie musi być cyklem. Warto zauważyć, że założono tu, że $n = 4$, ale równości $(1,2,3) \cdot (2,3,4) = (1,3) \cdot (2,4) = (2,4) \cdot (1,3)$ zachodzą dla dowolnego $n \geq 4$.

Definicja 12.2. Dwa cykle są *rozłączne*, jeśli ich wyrazy są parami różne.

Twierdzenie 12.3. Mnożenie cykli rozłącznych jest przemienne.

Dowód. Iloczyn $(j_1, j_2, \ldots, j_r) \cdot (i_1, i_2, \ldots, i_s)$ przekształca j_k w j_{k+1} $(k = 1, 2, \ldots, r-1)$, j_r w j_1, i_k w i_{k+1} $(k = 1, 2, \ldots, s-1)$, i_s w i_1 oraz pozostawia pozostałe liczby bez zmian. Iloczyn $(i_1, i_2, \ldots, i_s) \cdot (j_1, j_2, \ldots, j_r)$ określa tę samą permutację. □

Twierdzenie 12.4. Każda permutacja (różna od permutacji jednostkowej) jest iloczynem pewnej liczby rozłącznych cykli długości większej od jeden. Rozkład na cykle rozłączne jest jednoznaczny (jeśli wykluczyć cykle długości jeden).

Dowód. Niech $\sigma \neq I$ i niech j_1 będzie najmniejszą liczbą spełniającą warunek $\sigma(j_1) \neq j_1$. Niech $j_2 = \sigma(j_1)$, $j_3 = \sigma(j_2)$ itd. Niech wreszcie r będzie najmniejszą liczbą taką, że $j_{r+1} \in \{j_1, j_2, \ldots, j_r\}$. Gdyby $j_{r+1} \neq j_1$, to $j_{r+1} = j_k$ dla pewnego $k \in \{2, 3, \ldots, r\}$, skąd $j_r = \hat{\sigma}(j_{r+1}) = \hat{\sigma}(j_k) = j_{k-1}$, co przeczyłoby definicji r. Zatem $j_{r+1} = j_1$. Niech $\tau_1 = (j_1, j_2, \ldots, j_r)$. Wówczas σ zmienia każdą z wielkości j_1, j_2, …, j_r, zaś $\hat{\tau}_1 \cdot \sigma$ tych wartości nie zmienia.

Jeśli $\hat{\tau}_1 \cdot \sigma \neq I$, niech τ_2 będzie skonstruowane jak wyżej, ale dla permutacji $\hat{\tau}_1 \cdot \sigma$. Analogicznie konstruuje się kolejne permutacje τ_3, …, τ_p, aż uzyska się $\hat{\tau}_p \cdot \hat{\tau}_{p-1} \cdot \ldots \cdot$

$\hat{\tau}_1 \cdot \sigma = I$ (w każdym kroku liczba elementów zmianianych przez omawianą permutację się zmniejsza, zatem liczba kroków z pewnością jest skończona). Oznacza to, że $\sigma = \tau_1 \cdot \tau_2 \cdot \ldots \cdot \tau_p$. Ponadto τ_1, τ_2, $\ldots$, τ_p są cyklami, z konstrukcji wiadomo zaś, że są to cykle rozłączne. Jednoznaczność również wynika z konstrukcji: jeśli $\sigma(j) = k$ oraz $k \neq j$, to j musi pojawić się w pewnym cyklu oraz po j w tym samym cyklu musi nastąpić k (cykle są bowiem rozłączne); jeśli zaś $\sigma(j) = j$, to z tego samego powodu j nie może pojawić się w żadnym cyklu. □

TWIERDZENIE 12.5. Cykl długości r jest iloczynem $r - 1$ transpozycji: $(j_1, j_2, \ldots, j_r) = (j_1, j_2) \cdot (j_1, j_3) \cdot \ldots \cdot (j_1, j_r)$.

Dowód. Wystarczy sprawdzić, że w omawianym iloczynie j_1 przejdzie na j_2; j_2 — wpierw na j_1, a potem na j_3; j_3 — wpierw na j_1, a potem na j_4 itd.; j_{r-1} — wpierw na j_1, a potem na j_r; wreszcie j_r — na j_1. □

WNIOSEK 12.6. Każda permutacja jest iloczynem pewnej liczby transpozycji. □

13. **Znak permutacji**

Poniższa definicja jest najprostszą z możliwych, choć niekoniecznie najwygodniejszą.

Definicja 13.1. Permutacja σ jest *parzysta*, jeśli jest iloczynem parzystej liczby transpozycji, zaś *nieparzysta* — jeśli jest iloczynem nieparzystej liczby transpozycji.

Każda permutacja jest iloczynem pewnej liczby transpozycji, jest więc parzysta lub nieparzysta. Okazuje się, że żadna permutacja nie jest jednocześnie parzysta i nieparzysta. Aby to udowodnić, wygodnie zastosować inną, równoważną definicję parzystości.

Definicja 13.2. Dla permutacji σ zbioru $\{1, 2, 3, \ldots, n\}$ niech N_σ oznacza liczbę *inwersji*, czyli takich par liczb j, k, że $j < k$, lecz $\sigma(j) > \sigma(k)$. Niech ponadto $\operatorname{sign}(\sigma) = (-1)^{N_\sigma}$; wielkość ta nazywana jest *znakiem* permutacji σ.

TWIERDZENIE 13.3. Zachodzi $\operatorname{sign}(\sigma \cdot \tau) = \operatorname{sign}(\sigma) \operatorname{sign}(\tau)$.

Dowód. Niech P oznacza iloczyn wszystkich czynników postaci $(x_j - x_k)$, gdzie $1 \leq j < k \leq n$. Niech P_σ oznacza analogiczny iloczyn czynników $(x_{\sigma(j)} - x_{\sigma(k)})$. Dla dowolnych j i k takich, że $1 \leq j < k \leq n$ w iloczynie P występuje czynnik $(x_{\sigma(j)} - x_{\sigma(k)})$ (jeśli $\sigma(j) < \sigma(k)$) lub $(x_{\sigma(k)} - x_{\sigma(j)})$ (jeśli $\sigma(j) > \sigma(k)$), zatem $P = \operatorname{sign}(\sigma) P_\sigma$. Równoważnie: $P_\sigma = \operatorname{sign}(\sigma) P$. Analogicznie określone P_τ i $P_{\sigma\cdot\tau}$ spełniają podobne równania $P_\tau = \operatorname{sign}(\tau) P_{\sigma\cdot\tau} = \operatorname{sign}(\sigma \cdot \tau) P$.

Iloczyn $P_{\sigma\cdot\tau}$ można uzyskać z iloczynu P zamieniając wpierw każdy czynnik $(x_j - x_k)$ na czynnik $(x_{\sigma(j)} - x_{\sigma(\tau)})$ (co z wielomianu P czyni wielomian $P_\sigma = \operatorname{sign}(\sigma) P$), a następnie każdy czynnik $(x_J - x_K)$ na czynnik $(x_{\tau(J)} - x_{\tau(K)})$ (co z wielomianu P czyni wielomian $P_\tau = \operatorname{sign}(\tau) P$). Oznacza to, że $P_{\sigma\cdot\tau} = \operatorname{sign}(\sigma) \operatorname{sign}(\tau) P$. □

Inny dowód. Wystarczy obliczyć liczbę inwersji $\sigma \cdot \tau$. Niech M oznacza liczbę par j, k takich, że $j < k$, $\sigma(j) > \sigma(k)$ oraz $\tau(\sigma(j)) < \tau(\sigma(k))$. Równoważnie: M jest liczbą par j, k takich, że $j > k$, $\sigma(j) < \sigma(k)$ oraz $\tau(\sigma(j)) > \tau(\sigma(k))$. Podzielmy inwersje (czyli pary j, k takie, że $j < k$, $\tau(\sigma(j)) > \tau(\sigma(k))$) na dwa typy, w zależności od tego, czy $\sigma(j) > \sigma(k)$, czy $\sigma(j) < \sigma(k)$. Liczba inwersji pierwszego typu powiększona o M daje N_σ, liczbę inwersji permutacji σ. Liczba inwersji drugiego typu powiększona o M daje liczbę par j, k takich, że $\sigma(j) > \sigma(k)$ oraz $\tau(\sigma(j)) < \tau(\sigma(k))$, czyli liczbę par J, K takich, że $J > K$ oraz $\tau(J) < \tau(K)$, czyli N_τ, liczbę inwersji permutacji τ. Stąd $N_{\sigma\cdot\tau} + 2M = N_\sigma + N_\tau$. Stąd łatwo $\operatorname{sign}(\sigma \cdot \tau) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau)$. □

TWIERDZENIE 13.4. Zachodzi $\operatorname{sign}(\sigma) = \operatorname{sign}(\hat{\sigma})$.

Dowód. W istocie, $\operatorname{sign}(\sigma)\operatorname{sign}(\hat{\sigma}) = \operatorname{sign}(\sigma \cdot \hat{\sigma}) = \operatorname{sign}(I) = 1$. □

TWIERDZENIE 13.5. Jeśli σ jest transpozycją, to $\operatorname{sign}(\sigma) = -1$.

Dowód. Jeśli $\sigma = (a, b)$, gdzie $a < b$, to $N_\sigma = 1 + 2(b - a - 1)$, skąd $\operatorname{sign}(\sigma) = -1$. □

TWIERDZENIE 13.6. Znak permutacji określa jej parzystość: permutacja σ jest parzysta wtedy i tylko wtedy, gdy $\operatorname{sign}(\sigma) = 1$, σ jest zaś nieparzysta wtedy i tylko wtedy, gdy $\operatorname{sign}(\sigma) = -1$.

Dowód. Jeśli σ jest iloczynem m transpozycji, to $\operatorname{sign}(\sigma) = (-1)^m$. □

TWIERDZENIE 13.7. Jeśli σ jest cyklem długości r, to $\operatorname{sign}(\sigma) = (-1)^{r-1}$. Jeśli σ jest iloczynem m rozłącznych cykli o łącznej długości M, to $\operatorname{sign}(\sigma) = (-1)^{M-m}$.

Dowód. Cykl długości r jest iloczynem $r - 1$ transpozycji. □

Zbiór permutacji parzystych $\mathbb{A}_n$, nazywany *grupą alternującą*, jest zamknięty ze względu na mnożenie permutacji i odwracanie permutacji — jest *podgrupą* grupy symetrycznej $\mathbb{S}_n$.

TWIERDZENIE 13.8. Każda (różna od permutacji jednostkowej) permutacja parzysta jest iloczynem cykli długości 3.

Dowód. Każda taka permutacja jest iloczynem parzystej liczby transpozycji, zaś każdy iloczyn transpozycji jest albo permutacją jednostkową: $(j, k) \cdot (j, k) = I$, albo iloczynem dwóch cykli długości 3: $(j, k) \cdot (J, K) = (j, k, J) \cdot (j, K, J)$ gdy j, k, J, K są parami różne, za wyjątkiem być może $k = K$ (i analogicznie w pozostałych przypadkach). □

14. **Podgrupy normalne**

Rząd grupy permutacji G, oznaczany $|G|$, to liczba elementów tej grupy.

Przykład. Zachodzi $|\mathbb{S}_n| = n!$ i na mocy ćwiczenia — $|\mathbb{A}_n| = \frac{1}{2}n!$ dla $n \geq 2$.

Jeśli G i H są grupami permutacji i H jest podzbiorem G, to mówi się, że H jest *podgrupą* G. Czasem zapisuje się ten fakt w postaci $H < G$.

Przykład. Jeśli $k \leq n$, to permutacje zbioru $\{1, 2, \ldots, k\}$ można utożsamić z permutacjami większego zbioru $\{1, 2, \ldots, n\}$, które nie zmieniają liczb $k+1, k+2, \ldots, n$. W tym sensie $\mathbb{S}_k < \mathbb{S}_n$.

Przykład. Niech $a = (1,2) \cdot (3,4)$, $b = (1,3) \cdot (2,4)$, $c = (1,4) \cdot (2,3)$. Niech ponadto $p_1 = (2,3,4)$, $p_2 = (3,4,1)$, $p_3 = (4,1,2)$ i $p_4 = (1,2,3)$. Niech $G = A_4 = \{I, a, b, c, p_1, p_2, p_3, p_4, \hat{p}_1, \hat{p}_2, \hat{p}_3, \hat{p}_4\}$ oraz $H = \{I, a, b, c\}$. Ponieważ $a \cdot a = b \cdot b = c \cdot c = I$, $a \cdot b = c$, $a \cdot c = b$, $b \cdot c = a$, więc H jest podgrupą G.

Definicja 14.1. Jeśli $H < G$, to zbiór $\sigma \cdot H = \{\sigma \cdot h : h \in H\}$ nazywany jest *warstwą lewostronną* permutacji σ względem podgrupy H. Analogicznie $H \cdot \sigma = \{h \cdot \sigma : h \in H\}$ to *warstwa prawostronna.*

Przykład. W rozważanym wcześniej przykładzie są trzy warstwy: $H, p_1 \cdot H = \{p_1, \hat{p}_2, p_3, \hat{p}_4\}$ oraz $\hat{p}_1 \cdot H = \{\hat{p}_1, p_2, \hat{p}_3, p_4\}$ — łatwo sprawdzić, że warstwy pozostałych elementów są takie same. Co więcej, $p_1 \cdot H = H \cdot p_1$ oraz $\hat{p}_1 \cdot H = H \cdot \hat{p}_1$, zatem warstwy lewostronne i prawostronne są sobie równe.

Przykład. W $\mathbb{S}_3$ podgrupa $\mathbb{S}_2$ ma trzy warstwy: $\mathbb{S}_2 = \{I, (1,2)\}$, $(1,3) \cdot \mathbb{S}_2 = \{(1,3), (3,2,1)\}$ oraz $(2,3) \cdot \mathbb{S}_2 = \{(2,3), (1,2,3)\}$ — ponownie warstwy pozostałych elementów $\mathbb{S}_3$ są takie same. Skoro $\mathbb{S}_2 \cdot (1,3) = \{(1,3), (1,2,3)\}$, warstwy lewostronne i prawostronne nie są jednakowe.

Twierdzenie 14.2. Jeśli $\sigma \in H$, to $\sigma \cdot H = H$. Każda warstwa $\sigma \cdot H$ jest równoliczna z H. Każde dwie warstwy $\sigma \cdot H$ i $\pi \cdot H$ są albo rozłączne, albo równe.

Dowód. Jeśli $\sigma \in H$, to $\sigma \cdot h \in H$ dla $h \in H$, więc $\sigma \cdot H \subseteq H$. Ponadto dla $h \in H$ zachodzi $\hat{\sigma} \cdot h \in H$ oraz $\sigma \cdot (\hat{\sigma} \cdot h) = h$, zatem w istocie $\sigma \cdot H = H$.

Dla dowolnych $h_1, h_2 \in H$ z równości $\sigma \cdot h_1 = \sigma \cdot h_2$ wynika $h_1 = \hat{\sigma} \cdot (\sigma \cdot h_1) = \hat{\sigma} \cdot (\sigma \cdot h_2) = h_2$. Zatem $\sigma \cdot H$ ma tyle elementów, co H.

Jeśli $\sigma \cdot h_1 = \pi \cdot h_2$, to $\sigma \cdot h = (\sigma \cdot h_1) \cdot (\hat{h}_1 \cdot h) = (\pi \cdot h_2) \cdot (\hat{h}_1 \cdot h) \in \pi \cdot H$, zatem $\sigma \cdot H$ jest podzbiorem $\pi \cdot H$. Analogicznie $\pi \cdot H$ jest podzbiorem $\sigma \cdot H$, co dowodzi równości tych warstw. □

Analogiczne twierdzenie zachodzi oczywiście dla warstw prawostronnych. Skoro każdy element należy do swojej warstwy, tj. $\sigma \in \sigma \cdot H$, grupa G rozpada się na parami rozłączne, równoliczne warstwy. Liczbę warstw grupy H w grupie G nazywa się *indeksem* grupy H w grupie G i oznacza $G : H$ lub $(G : H)$.

Wniosek 14.3. Jeśli $H < G$, to $|H|$ jest dzielnikiem $|G|$ oraz $|G| = |H| \cdot (G : H)$. □

Zatem $\pi \cdot H = \sigma \cdot H$ można zapisać równoważnie na różne sposoby: $\pi \in \sigma \cdot H$, $\pi = \sigma \cdot h$ dla pewnego $h \in H$, $\pi \cdot h_1 = \sigma \cdot h_2$ dla pewnych $h_1, h_2 \in H$ itp.

Definicja 14.4. Jeśli $H < G$ i warstwy lewostronne oraz prawostronne H w G są jednakowe (tj. $\sigma \cdot H = H \cdot \sigma$ dla wszystkich $\sigma \in G$), to grupa H nazywana jest *podgrupą normalną* (inaczej: *dzielnikiem normalnym*) grupy G. Fakt ten zapisywany jest w postaci $H \lhd G$, a warstwy oznaczane są symbolem $[\sigma] = \sigma \cdot H = H \cdot \sigma$.

Przykład. W rozważanym wcześniej przykładzie H jest podgrupą normalną $G = \mathbb{A}_4$. Z drugiej strony $\mathbb{S}_2$ nie jest podgrupą normalną $\mathbb{S}_3$.

Definicja 14.5. Grupa G nazywana jest *grupą prostą*, jeśli jedynymi jej podgrupami normalnymi są $\{I\}$ oraz G.

TWIERDZENIE 14.6. Grupy $\mathbb{A}_n$ dla $n \geq 5$ są proste.

Dowód powyższego twierdzenia został rozpisany na ćwiczenia na liście zadań. Wcześniejszy przykład dowodzi, że $\mathbb{A}_4$ nie jest grupą prostą.

TWIERDZENIE 14.7. Jeśli $H \lhd G$ oraz $[\sigma_1] = [\sigma_2]$, $[\pi_1] = [\pi_2]$, to $[\sigma_1 \cdot \pi_1] = [\sigma_2 \cdot \pi_2]$.

Dowód. Skoro $\sigma_2 = \sigma_1 \cdot h_1$, $\pi_2 = \pi_1 \cdot h_2$ oraz $h_1 \cdot \pi_1 = \pi_1 \cdot h_3$ dla pewnych $h_1, h_2, h_3 \in H$ (ostatnia równość to konsekwencja równości $H \cdot \pi_1 = \pi_1 \cdot H$), zachodzi $\sigma_2 \cdot \pi_2 = \sigma_1 \cdot h_1 \cdot \pi_1 \cdot h_2 = \sigma_1 \cdot \pi_1 \cdot h_3 \cdot h_2$, skąd wynika teza. □

WNIOSEK 14.8. Jeśli $H \lhd G$, to wzór $[\sigma] \cdot [\pi] = [\sigma \cdot \pi]$ poprawnie określa mnożenie warstw grupy H w grupie G. □

Warto zauważyć, że powyższa definicja zgadza się z inną, bardziej naturalną: $[\sigma] \cdot [\pi] = \{g \cdot h : g \in [\sigma],\, h \in [\pi]\}$ — na mocy twierdzenia $[g \cdot h] = [\sigma \cdot \pi]$, czyli $g \cdot h \in [\sigma \cdot \pi]$.

TWIERDZENIE 14.9. Jeśli $H \lhd G$, to zdefiniowane wyżej mnożenie jest operacją grupową: jest łączne, ma element neutralny $[I] = H$ oraz każda warstwa $[\sigma]$ ma warstwę odwrotną $[\hat{\sigma}]$.

Dowód. Sprawdzenie łączności jest elementarne:

$$\begin{aligned}([\sigma_1] \cdot [\sigma_2]) \cdot [\sigma_3] &= [\sigma_1 \cdot \sigma_2] \cdot [\sigma_3] = [(\sigma_1 \cdot \sigma_2) \cdot \sigma_3] \\ &= [\sigma_1 \cdot (\sigma_2 \cdot \sigma_3)] = [\sigma_1] \cdot [\sigma_2 \cdot \sigma_3] = [\sigma_1] \cdot ([\sigma_2] \cdot [\sigma_3]).\end{aligned}$$

Podobnie $[\sigma] \cdot [I] = [\sigma \cdot I] = [\sigma]$ oraz $[I] \cdot [\sigma] = [I \cdot \sigma] = [\sigma]$, a także $[\sigma] \cdot [\hat{\sigma}] = [\sigma \cdot \hat{\sigma}] = [I]$ oraz $[\hat{\sigma}] \cdot [\sigma] = [\hat{\sigma} \cdot \sigma] = [I]$. □

Definicja 14.10. Jeśli $H \lhd G$, to zbiór warstw, wraz ze zdefiniowanym wyżej mnożeniem, nazywany jest *grupą ilorazową* i oznaczany G/H.

Działanie w grupie o stosunkowo małej liczbie elementów można przedstawić przy pomocy *tabliczki mnożenia*, w której „numer" wiersza mnożony jest przez „numer kolumny". Przydaje się to do obliczeń.

Przykład. Tabliczka mnożenia w grupie $\mathbb{S}_3$ to:

	I	(1,2,3)	(3,2,1)	(1,2)	(1,3)	(2,3)
I	I	(1,2,3)	(3,2,1)	(1,2)	(1,3)	(2,3)
(1,2,3)	(1,2,3)	(3,2,1)	I	(2,3)	(1,2)	(1,3)
(3,2,1)	(3,2,1)	I	(1,2,3)	(1,3)	(2,3)	(1,2)
(1,2)	(1,2)	(1,3)	(2,3)	I	(1,2,3)	(3,2,1)
(1,3)	(1,3)	(2,3)	(1,2)	(3,2,1)	I	(1,2,3)
(2,3)	(2,3)	(1,2)	(1,3)	(1,2,3)	(3,2,1)	I

Z tabliczki tej łatwo odczytać, że $\mathbb{A}_3$ jest normalną podgrupą $\mathbb{S}_3$ o dwóch warstwach: $[I] = \mathbb{A}_3$ oraz $[(1,2)] = \{(1,2),(1,3),(2,3)\}$. Ponadto tabliczka mnożenia tych warstw wygląda następująco:

	[I]	[(1,2)]
[I]	[I]	[(1,2)]
[(1,2)]	[(1,2)]	[I]

Grupy często reprezentuje się w inny, nieco wygodniejszy w rachunkach sposób: poprzez *generatory* i *reguły upraszczania*. Grupa $\mathbb{S}_3$ jest generowana przez permutacje $\sigma = (1,2,3)$ oraz $\tau = (1,2)$, które spełniają równości $\sigma \cdot \sigma \cdot \sigma = I$, $\tau \cdot \tau = I$ oraz $\tau \cdot \sigma = \sigma \cdot \tau \cdot \tau$.

TWIERDZENIE 14.11. Jeśli $H < G$ oraz $G : H = 2$, to $H \lhd G$.

Dowód. Jedną warstwą (obustronną) jest $I \cdot H = H \cdot I = H$. Drugą w takim razie musi być $G \setminus H$. Oznacza to równość warstw lewo- i prawostronnych. □

WNIOSEK 14.12. Dla $n \geq 2$ zachodzi $\mathbb{A}_n \lhd \mathbb{S}_n$.

15. **Grupy rozwiązalne**

Teoria Galoisa pozwala z każdym wielomianem o współczynnikach wymiernych (a także w ogólniejszych przypadkach) związać pewną grupę permutacji, nazywaną *grupą Galoisa* wielomianu. Jeśli wielomian jest stopnia n, jego grupa Galoisa jest podgrupą $\mathbb{S}_n$. Pierwiastki wielomianu można wyrazić wzorem (przy pomocy operacji arytmetycznych i pierwiastków) wtedy i tylko wtedy, gdy grupa Galoisa tego wielomianu spełnia warunek poniższej definicji.

Definicja 15.1. Grupa permutacji G jest *rozwiązalna*, jeśli isnieje ciąg H_0, H_1, …, H_n jej podgrup o następujących własnościach:
(a) $G = H_0 \rhd H_1 \rhd H_2 \rhd \ldots \rhd H_{n-1} \rhd H_n = \{I\}$;
(b) grupy ilorazowe H_0/H_1, H_1/H_2, …, H_{n-1}/H_n są przemienne.

Przemienność $H_{n-1}/H_n = H_{n-1}/\{I\}$ jest oczywiście równoważna przemienności H_{n-1} (bowiem w $H_{n-1}/\{I\}$ warstwy są jednoelementowe: $[\sigma] = \{\sigma\}$).

Przykład. Grupa $\mathbb{S}_3$ jest rozwiązalna, bowiem $\mathbb{S}_3 \rhd \mathbb{A}_3 \rhd \{I\}$ oraz $\mathbb{S}_3/\mathbb{A}_3$ jest przemienna (jako grupa dwuelementowa) oraz $\mathbb{A}_3/\{I\}$ jest przemienna (bo $\mathbb{A}_3$ jest przemienna, albo dlatego, że każda trzyelementowa jest przemienna — jest to ćwiczenie na liście zadań).

Systematyczna metoda badania rozwiązalności grup wykorzystuje następujące pojęcie.

Definicja 15.2. Jeśli G jest grupą permutacji, to *komutantem* grupy G nazywamy podgrupę G' grupy G, która składa się z iloczynów (dowolnie wielu) komutatorów, czyli permutacji postaci $\sigma \cdot \tau \cdot \hat{\sigma} \cdot \hat{\tau}$, gdzie $\sigma, \tau \in G$.

Iloczyn komutatorów nie musi sam być komutatorem, dlatego komutant G' nie musi być równy zbiorowi wszystkich komutatorów (może być od niego większy; najmniejsza taka grupa liczy jednak aż 92 elementy). Warto zauważyć, że iloczyn σ i τ jest przemienny (czyli $\sigma \cdot \tau = \tau \cdot \sigma$) wtedy i tylko wtedy, gdy $\sigma \cdot \tau \cdot \hat{\sigma} \cdot \hat{\tau} = I$. Wobec tego G jest przemienna wtedy i tylko wtedy, gdy $G' = \{I\}$.

Twierdzenie 15.3. Podgrupa H grupy permutacji G zawiera G' wtedy i tylko wtedy, gdy jest podgrupą normalną oraz G/H jest przemienna.

Dowód. Niech H będzie podgrupą G zawierającą G'. Dla dowolnego $\sigma \in G$ oraz $h_1 \in H$ permutacja $h_2 = \sigma \cdot h \cdot \hat{\sigma} \cdot \hat{h}$ należy do G', a więc także do H. Oznacza to, że $\sigma \cdot h = h_2 \cdot h \cdot \sigma$, czyli $\sigma \cdot h \in H \cdot \sigma$. Oznacza to, że $\sigma \cdot H$ jest podzbiorem $H \cdot \sigma$. Analogicznie dowodzi się przeciwnego zawierania. Wynika stąd, że H jest podgrupą normalną G. Ponadto $[\sigma] \cdot [\tau] \cdot [\hat{\sigma}] \cdot [\hat{\tau}] = [\sigma \cdot \tau \cdot \hat{\sigma} \cdot \hat{\tau}] = [I]$, bowiem $\sigma \cdot \tau \cdot \hat{\sigma} \cdot \hat{\tau}$ należy do G', a więc i do H. Oznacza to, że $[\sigma] \cdot [\tau] = [\tau] \cdot [\sigma]$.

Jeśli zaś H jest podgrupą normalną G oraz G/H jest przemienna, to dla dowolnych $\sigma, \tau \in G$ zachodzi $[\sigma \cdot \tau \cdot \hat{\sigma} \cdot \hat{\tau}] = [\sigma] \cdot [\tau] \cdot [\hat{\sigma}] \cdot [\hat{\tau}] = [I]$, czyli $\sigma \cdot \tau \cdot \hat{\sigma} \cdot \hat{\tau}$ należy do H. Stąd wynika, że H zawiera G'. □

Wniosek 15.4. Komutant grupy permutacji jest jej podgrupą normalną. □

Wprost z definicji wynika, że jeśli H jest podgrupą G, to H' jest podgrupą G'.

Twierdzenie 15.5. Grupy permutacji G jest rozwiązalna wtedy i tylko wtedy, gdy ciąg kolejnych komutantów: G, G', G'', G''', ...jest od pewnego miejsca równy $\{I\}$ (tu G'' oznacza komutant grupy G' itd.).

Dowód. Jeśli n-ty komutant $G^{(n)}$ jest równy $\{I\}$, to ciąg podgrup $G_0 = G$, $G_1 = G'$, $G_2 = G''$, ..., $G_n = G^{(n)}$ spełnia warunek z definicji grupy rozwiązalnej. Przeciwnie, jeśli $G_0, G_1, \ldots, G_n$ jest ciągiem spełniającym ów warunek, to G_1 zawiera G'; G_2 zawiera G_1', a więc tym bardziej G''; analogicznie G_n zawiera n-ty komutant $G^{(n)}$. Skoro jednak $G_n = \{I\}$, zachodzi $G^{(n)} = \{I\}$. □

Powyższy argument jest ściśle związany z rozważaniem komutatorów wyższych rzędów w dowodzie twierdzenia Abela–Ruffiniego.

Wniosek 15.6. Wszystkie podgrupy grupy rozwiązalnej są rozwiązalne. □

Poniższy wynik jest słabszą (i łatwiejszą do udowodnienia) wersją twierdzenia o tym, że $\mathbb{A}_n$ jest grupą prostą gdy $n \geq 5$.

Twierdzenie 15.7. Grupy $\mathbb{S}_n$ oraz $\mathbb{A}_n$ są rozwiązalne wtedy i tylko wtedy, gdy $n \leq 4$.

Dowód. Grupy $\mathbb{A}_n$ dla $n \leq 3$ są przemienne, więc rozwiązalne. Rozwiązalność $\mathbb{A}_4$ jest ćwiczeniem na liście zadań. Rozwiązalność $\mathbb{S}_n$ dla $n \leq 3$ wynika z przemienności grupy $\mathbb{S}_n/\mathbb{A}_n$.

Gdy $n \geq 5$, to komutant $\mathbb{A}'_n$ zawiera każdy cykl (j_1, j_2, j_3) długości 3: istnieją bowiem liczby j_4 i j_5 takie, że j_1, j_2, j_3, j_4 i j_5 są parami różne i wtedy $(j_1, j_2, j_3) = (j_1, j_2, j_4) \cdot (j_2, j_5, j_3) \cdot (j_4, j_2, j_1) \cdot (j_3, j_5, j_2)$ jest komutatorem. Stąd jednak wynika, że $\mathbb{A}'_n$ zawiera wszystkie permutacje parzyste, czyli $\mathbb{A}'_n = \mathbb{A}_n$.

Ponieważ grupa rozwiązalna nie może zawierać nierozwiązalnej podgrupy, grupy $\mathbb{S}_n$ również nie są rozwiązalne dla $n \geq 5$. $\square$