PIERŚCIENIE I CIAŁA
Wykład 4

Pierścienie

Przypomnijmy podstawowe definicje dotyczące pierścieni.

Definicja 1. ***Pierścieniem*** nazywamy zbiór P z określonymi w nim dwoma działaniami $+, \cdot$ spełniającymi warunki:

(1) $\bigwedge\limits_{x,y,z\in P} (x+y)+z = x+(y+z)$ (łączność dodawania)
(2) $\bigwedge\limits_{x,y\in P} x+y = y+x$ (przemienność dodawania)
(3) $\bigvee\limits_{e\in P} \bigwedge\limits_{x\in P} e+x = x$ (istnienie elementu neutralnego dodawania)
(4) $\bigwedge\limits_{x\in P} \bigvee\limits_{y\in P} x+y = e$ (istnienie elementu przeciwnego)
(5) $\bigwedge\limits_{x,y,z\in P} (x\cdot y)\cdot z = x\cdot(y\cdot z)$ (łączność mnożenia)
(6) $\bigwedge\limits_{x,y,z\in P} (x+y)\cdot z = x\cdot z + y\cdot z$ (rozdzielność mnożenia względem dodawania)
(7) $\bigwedge\limits_{x,y,z\in P} z\cdot(x+y) = z\cdot x + z\cdot y$ (rozdzielność mnożenia względem dodawania).

Element neutralny dodawania e z warunku (3) nazywamy zerem pierścienia P i oznaczamy przez 0. Element y z warunku (4) nazywamy elementem przeciwnym do x i oznaczmy przez $-x$. Aby uniknąć nieporozumień co do działań często pierścień zapisuje się jako trójkę $(P, +, \cdot)$ złożoną ze zbioru i rozważanych działań.

Warunki od (1)–(4) oznaczają że $(P, +)$ jest grupą przemienną.

Mówimy, że pierścień P jest przemienny, jeśli mnożenie $\cdot$ jest przemienne, czyli

$$\bigwedge_{x,y\in P} x\cdot y = y\cdot x.$$

Jeżeli istnieje element neutralny mnożenia $\cdot$, to nazywamy go jedynką pierścienia P i oznaczamy przez 1. Zwykle dla uproszczenia zapisów pomijamy znak mnożenia $\cdot$ i zamiast $x\cdot y$ piszemy xy.

Przykłady

1. Zbiór liczb całkowitych $\mathbb{Z}$ ze zwykłym dodawaniem i mnożeniem jest pierścieniem przemiennym.
2. Niech $\mathbb{Z}'$ oznacza zbiór liczb całkowitych $\mathbb{Z}$ ze zwykłym dodawaniem, ale z mnożeniem określonym wzorem

$$a \star b = -ab$$

dla $a, b \in \mathbb{Z}$. Jest to pierścień przemienny z jedynką, ale jego jedynką jest liczba -1.
3. Zbiór $\mathbb{Z}[x]$ wszystkich wielomianów o współczynnikach całkowitych ze zwykłymi działaniami jest pierścieniem przemiennym. Podobnie pierścieniami przemiennymi są:
$\mathbb{Q}[x]$ – zbiór wszystkich wielomianów o współczynnikach wymiernych,
$\mathbb{R}[x]$ – zbiór wszystkich wielomianów o współczynnikach rzeczywistych,
$\mathbb{C}[x]$ – zbiór wszystkich wielomianów o współczynnikach zespolonych.

3. Dla zbioru niepustego X niech $M(X)$ oznacza zbiór wszystkich funkcji $f : X \to \mathbb{R}$. zbiór $M(X)$ ze zwykłymi działaniami:

$$(f+g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x)$$

jest pierścieniem przemiennym. Jego elementem zerowym jest funkcja stale równa 0, zaś jedynką jest funkcja stale równa 1.
4. Niech $d \in \mathbb{Z}$, $d \neq 0$. Jeśli $d > 0$, to przez $\sqrt{d}$ rozumiemy dodatni pierwiastek z d, a jeśli $d < 0$, to przez $\sqrt{d}$ rozumiemy liczbę zespoloną $i\sqrt{|d|}$. W obu przypadkach $\left(\sqrt{d}\right)^2 = d$. W drugim przypadku wynika to ze wzoru

$$\left(i\sqrt{|d|}\right)^2 = -|d| = d.$$

Oznaczamy

$$\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\}.$$

Rozpatrując ten zbiór ze zwykłym dodawaniem i mnożeniem otrzymujemy pierścień przemienny. Ponieważ działania w tym zbiorze są zwykłymi działaniami na liczbach zespolonych, więc oczywiście spełniają one warunki z definicji pierścienia przemiennego. Należy jednak sprawdzić, że są to działania wewnętrzne. Bierzemy w tym celu dwa dowolne elementy: $u = a + b\sqrt{d}$, $v = a_1 + b_1\sqrt{d}$, gdzie $a, b, a_1, b_1 \in \mathbb{Z}$. Mamy

$$u + v = a + b\sqrt{d} + a_1 + b_1\sqrt{d} = a + a_1 + (b + b_1)\sqrt{d}$$

i ponieważ $a + a_1 \in \mathbb{Z}$ oraz $b + b_1 \in \mathbb{Z}$, więc $u + v \in \mathbb{Z}[\sqrt{d}]$. Ponadto

$$\begin{aligned} uv &= \left(a + b\sqrt{d}\right)\left(a_1 + b_1\sqrt{d}\right) = aa_1 + ab_1\sqrt{d} + a_1b\sqrt{d} + bb_1\left(\sqrt{d}\right)^2 = \\ &= aa_1 + bb_1d + (ab_1 + a_1b)\sqrt{d} \end{aligned}$$

i ponieważ $aa_1 + bb_1d \in \mathbb{Z}$ oraz $ab_1 + a_1b \in \mathbb{Z}$, więc $uv \in \mathbb{Z}[\sqrt{d}]$.
5. Niech $n \in \mathbb{N}$, $n > 1$. Dla $a \in \mathbb{Z}$ przez $r_n(a)$ oznaczamy (nieujemną) resztę z dzielenia a przez n. Zbiór $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ z ***działaniami modulo*** n:

$$x \oplus_n y = r_n(x + y), \quad x \odot_n y = r_n(xy)$$

dla $x, y \in \mathbb{Z}_n$ jest pierścieniem przemiennym. Elementem przeciwnym do 0 jest 0. Dla $x \in \mathbb{Z}_n$, elementem przeciwnym do x w $\mathbb{Z}_n$ jest $n - x$, gdyż $n - x \in \mathbb{Z}_n$ i

$$x \oplus_n (n - x) = r_n(x + (n - x)) = r_n(n) = 0.$$

6. Niech $n \in \mathbb{N}$, $n > 1$. Zbiór $M_n(\mathbb{C})$ wszystkich macierzy kwadratowych stopnia n o wyrazach zespolonych ze zwykłymi działaniami dodawania i mnożenia macierzy jest pierścieniem. Pierścień ten nie jest przemienny, gdyż np.

$$\begin{bmatrix} 0, & 1 \\ 0, & 0 \end{bmatrix}\begin{bmatrix} 0, & 0 \\ 0, & 1 \end{bmatrix} = \begin{bmatrix} 0, & 1 \\ 0, & 0 \end{bmatrix}, \quad \begin{bmatrix} 0, & 0 \\ 0, & 1 \end{bmatrix}\begin{bmatrix} 0, & 1 \\ 0, & 0 \end{bmatrix} = \begin{bmatrix} 0, & 0 \\ 0, & 0 \end{bmatrix}.$$

Elementem zerowym $M_n(\mathbb{C})$ jest macierz samych zer, a jedynką jest macierz jednostkowa

$$I_n = \begin{bmatrix} 1, & 0, & \dots & 0, & 0 \\ 0 & 1, & \dots & 0, & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0, & 0, & \dots & 1, & 0 \\ 0, & 0, & \dots & 0, & 1 \end{bmatrix}$$

Element x pierścienia P jest ***dzielnikiem zera***, jeśli istnieje $y \in P$, $y \neq 0$ taki, że $xy = 0$ lub $yx = 0$. Oczywiście 0 jest dzielnikiem zera.

Przykłady

1. Liczba 2 jest dzielnikiem zera w pierścieniu $\mathbb{Z}_4$. Rzeczywiście

$$2 \odot_4 2 = r_4(4) = 0.$$

Ogólnie jeśli $n \in \mathbb{N}$ nie jest liczbą pierwszą, to $n = kl$, gdzie $1 < k, l < n$, a więc

$$k \odot_n l = r_n(n) = 0.$$

Zatem k, l są dzielnikami zera w $\mathbb{Z}_n$.

2. Funkcja

$$g(x) = \begin{cases} 0, & \text{dla } x < 0, \\ 1, & \text{dla } x \geqslant 0 \end{cases}$$

jest dzielnikiem zera w pierścieniu $M(\mathbb{R})$ wszystkich funkcji $f : \mathbb{R} \to \mathbb{R}$. Rzeczywiście, dla

$$h(x) = \begin{cases} 1, & \text{dla } x < 0, \\ 0, & \text{dla } x \geqslant 0 \end{cases}$$

mamy $(gh)(x) = g(x)h(x) = 0$ dla każdego $x \in \mathbb{R}$.

Ogólnie, jeśli funkcja g zeruje się na pewnym niepustym podzbiorze $A \subset \mathbb{R}$, to g jest dzielnikiem zera w $M(\mathbb{R})$.

3. W pierścieniu macierzy $M_2(\mathbb{C})$ mamy

$$\begin{bmatrix} 0, & 0 \\ 0, & 1 \end{bmatrix} \begin{bmatrix} 0, & 1 \\ 0, & 0 \end{bmatrix} = \begin{bmatrix} 0, & 0 \\ 0, & 0 \end{bmatrix},$$

więc macierze

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

są dzielnikami zera.

Dla elementów, które nie są dzielnikami zera mamy następującą regułę skracania.

Twierdzenie 1. *Jeżeli $x \in P$ nie jest dzielnikiem zera i $ax = bx$ lub $xa = xb$ dla pewnych $a, b \in P$, to $a = b$.*

Dowód. Jeżeli $ax = bx$, to $(a - b)x = 0$ i ponieważ x nie jest dzielnikiem zera, więc $a - b = 0$, czyli $a = b$. □

Definicja 2. Mówimy, że P jest ***pierścieniem całkowitym*** (albo dziedziną całkowitości), jeśli P jest pierścieniem przemiennym z $1 \neq 0$ i P nie ma niezerowych dzielników zera. Warunek $1 \neq 0$ oznacza po prostu, że $P \neq \{0\}$.

Definicja 3. Pierścień P nazywamy ***ciałem***, jeśli P jest pierścieniem przemiennym z $1 \neq 0$, w którym każdy element $x \neq 0$ jest odwracalny, czyli

$$\bigwedge_{x \in P \setminus \{0\}} \bigvee_{y \in P} xy = 1.$$

Element y nazywamy elementem odwrotnym do x i oznaczmy przez x^{-1}.

Jeśli P jest ciałem, to nie tylko $(P, +)$ jest grupą przemienną, ale również $(P \setminus \{0\}, \cdot)$ jest grupą przemienną.

Twierdzenie 2. *Jeżeli element x pierścienia P jest odwracalny, to x nie jest dzielnikiem zera.*

Dowód. Załóżmy, że $xy = 0$ dla pewnego $y \in P$. Wtedy

$$y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0$$

i podobnie jeśli $yx = 0$, to $y = 0$. □

Wniosek 1. *Każde ciało P jest pierścieniem całkowitym.*

Przykład 1.
1. Pierścień $\mathbb{Z}$ ze zwykłym dodawaniem i mnożeniem jest pierścieniem całkowitym. Pierścienie liczb wymiernych $\mathbb{Q}$, liczb rzeczywistych $\mathbb{R}$ i liczb zespolonych $\mathbb{C}$ ze zwykłymi działaniami są ciałami.
2. Pierścień $\mathbb{Z}[\sqrt{d}]$ jest pierścieniem całkowitym, zaś

$$\mathbb{Q}[\sqrt{d}] = \left\{a + b\sqrt{d} : a, b \in \mathbb{Q}\right\}$$

ze zwykłym dodawaniem i mnożeniem jest ciałem.
3. Niech $n \in \mathbb{N}$, $n > 1$. Dla pierścienia $\mathbb{Z}_n$ następujące warunki są równoważne:

$$\mathbb{Z}_n \text{ jest ciałem} \Leftrightarrow \mathbb{Z}_n \text{ jest pierścieniem całkowitym} \Leftrightarrow n \text{ jest liczbą pierwszą.}$$

Podpierścienie i ideały

Niepusty podzbiór A pierścienia P nazywamy ***podpierścieniem***, jeśli

(1) $\bigwedge_{a,b \in A} a - b \in A$

(2) $\bigwedge_{a,b \in A} ab \in A.$

Warunek (1) oznacza, że $(A, +)$ jest podgrupą grupy $(P, +)$.

Niepusty podzbiór A ciała P nazywamy ***podciałem***, jeśli

(1) $\bigwedge_{a,b \in A} a - b \in A$

(2) $\bigwedge_{a,b \in A,\, b \neq 0} ab^{-1} \in A.$

Oznacza to, że A jest podpierścieniem P i A jest ciałem. Wtedy $(A \setminus \{0\}, \cdot)$ jest podgrupą grupy $(P \setminus \{0\}, \cdot)$.

Jeśli A jest podciałem ciała P, to mówimy, że P jest ***rozszerzeniem ciała*** A.

Przykład 2. Ciało $\mathbb{R}$ jest rozszerzeniem ciała $\mathbb{Q}$, zaś $\mathbb{C}$ jest rozszerzeniem ciała $\mathbb{R}$.

Ciało $\mathbb{Q}[\sqrt{d}]$ jest rozszerzeniem ciała $\mathbb{Q}$. Jeśli $d > 0$ i $\sqrt{d} \notin \mathbb{Q}$, to $\mathbb{Q}[\sqrt{d}]$ jest podciałem ciała $\mathbb{R}$, zaś jeśli $d < 0$, to $\mathbb{Q}[\sqrt{d}]$ jest podciałem ciała $\mathbb{C}$. Np. dla $d = -1$ mamy $\sqrt{d} = i$, a więc $\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[i]$ jest ciałem liczb zespolonych, których część rzeczywista i część urojona są liczbami wymiernymi.

Definicja 4. ***Ideałem*** pierścienia P nazywamy niepusty zbiór I zawarty w P taki, że

(1) $\bigwedge\limits_{a,b\in I} a - b \in I$

(2) $\bigwedge\limits_{a\in I}\bigwedge\limits_{x\in P} ax \in I,\ xa \in I.$

Zbiory $\{0\}$ i P są ideałami. Ideał I różny od $\{0\}$ i P nazywamy ***ideałem właściwym***.

Uwaga 1. Ideał I pierścienia z jedynką jest właściwy wtedy i tylko wtedy, gdy 1 nie należy do I.

Dowód. Oczywiście, jeśli $I = P$, to $1 \in I$. Na odwrót, jeśli $1 \in I$, to dla dowolnego $x \in P$ mamy $x = 1 \cdot x \in I$ i stąd $I = P$. □

Wniosek 2. *Jeżeli P jest ciałem, to jedynymi ideałami w P są $\{0\}$ i P.*

Dowód. Jeżeli $I \neq \{0\}$ jest ideałem ciała P, to istnieje $a \in I$, $a \neq 0$. Zatem $1 = aa^{-1} \in I$, a więc $I = P$. □

Każdy ideał jest podpierścieniem, ale nie każdy podpierścień jest ideałem.

Przykład 3. Pierścień liczb całkowitych $\mathbb{Z}$ jest podpierścieniem ciała $\mathbb{R}$. Nie jest to ideał, gdyż np. $1 \in \mathbb{Z}$, ale $\frac{1}{2} = 1 \cdot \frac{1}{2} \notin \mathbb{Z}$. Fakt, że $\mathbb{Z}$ nie jest ideałem ciała $\mathbb{R}$ wynika także z ostatniego wniosku.

Dla ideału I pierścienia P definiujemy ***relację równoważności*** $\equiv$ wzorem:

$$x \equiv y \pmod{I} \Leftrightarrow x - y \in I, \tag{1}$$

gdzie $x, y \in P$. Relację tę nazywamy relacją ***przystawania modulo*** I. Przez $[x]$ lub $x + I$ oznaczmy klasę abstrakcji elementu $x \in P$ względem tej relacji, czyli

$$[x] = x + I = \{a \in P : a \equiv x \pmod{I}\}.$$

Relacja $\equiv$ jest zgodna z działaniami w pierścieniu P, co oznacza, że jeśli $a \equiv b \pmod{I}$ i $x \equiv y \pmod{I}$, to $(a + x) \equiv (b + y) \pmod{I}$ i $ax \equiv by \pmod{I}$. Dzięki temu w zbiorze P/I wszystkich klas abstrakcji względem relacji $\equiv$ możemy określić działania wzorami

$$[a] + [b] = [a + b], \quad [a][b] = [ab],$$

gdzie $a, b \in P$. Zbiór P/I z tymi działaniami jest pierścieniem. Nazywamy go ***pierścieniem ilorazowym***.

Homomorfizmy pierścieni

Niech P_1, P_2 będą pierścieniami z jedynkami. Funkcję $f : P_1 \to P_2$ nazywamy ***homomorfizmem***, jeśli

(1) $\bigwedge\limits_{x,y\in P_1} f(x+y) = f(x) + f(y)$
(2) $\bigwedge\limits_{x,y\in P_1} f(xy) = f(x)f(y)$
(3) $f(1) = 1$.

Jądro homomorfizmu

$$\operatorname{Ker} f = \{x \in P_1 : f(x) = 0\}$$

jest ideałem pierścienia P_1, zaś obraz $f(P_1)$ jest podpierścieniem pierścienia P_2.

Homomorfizm $f : P_1 \to P_2$ nazywamy ***izomorfizmem*** jeśli f jest różnowartościowy i $f(P_1) = P_2$. Mówimy, że pierścienie P_1, P_2 są ***izomorficzne*** jeśli istnieje izomorfizm przekształcający P_1 na P_2. Piszemy wtedy $P_1 \cong P_2$.

Twierdzenie 3. *Niech $f : P_1 \to P_2$ będzie homomorfizmem pierścieni. Wtedy pierścienie $f(P_1)$ i $P_1/\operatorname{Ker} f$ są izomorficzne.*

Przykład 4. Niech $n \in \mathbb{N}$, $n > 1$. Dla $a \in \mathbb{Z}$ przez $r_n(a)$ oznaczamy nieujemną resztę z dzielenia a przez n. Dla dowolnych $a, b \in \mathbb{Z}$ mamy

$$r_n(a+b) = r_n(r_n(a) + r_n(b)) = r_n(a) \oplus r_n(b), \quad r_n(ab) = r_n(r_n(a)r_n(b)) = r_n(a) \odot r_n(b),$$

co oznacza, że funkcja $r_n : \mathbb{Z} \to \mathbb{Z}_n$ jest homomorfizmem. Ponadto $r_n(\mathbb{Z}) = \mathbb{Z}_n$, a więc pierścień $\mathbb{Z}/\operatorname{Ker} r_n$ jest izomorficzny z $\mathbb{Z}_n$. Zauważmy, że

$$\operatorname{Ker} r_n = \{a \in \mathbb{Z} : r_n(a) = 0\} = \{mn : m \in \mathbb{Z}\}$$

i ideał ten oznaczamy przez (n). Stąd $\mathbb{Z}_n \cong \mathbb{Z}/(n)$.

Kwaterniony

William Rowan Hamilton był irlandzkim matematykiem i fizykiem. Zajmował się m.in. problemem, czy można skonstruować rozszerzenie ciała liczb zespolonych, co doprowadziło go do konstrukcji kwaternionów.

Rysunek 1. Sir William Rowan Hamilton (1805–1865)

Już jako dziecko Hamilton miał nadzwyczajną pamięć. Z początku wykorzystał to do nauki martwych bądź egzotycznych języków: łaciny, greki i hebrajskiego w wieku pięciu lat, do tego w wieku lat dziewięciu doszły: perski, arabski, sanskryt, chaldejski, syryjski, hindi, bengalski, malajski itd. Tak przynajmniej twierdził jego ojciec, który go zresztą nie wychowywał, od trzeciego roku życia chłopiec mieszkał bowiem i uczył się u swojego wujka pastora (rodzice zmarli, zanim William dorósł).

Hamilton potrafił również wykonywać w pamięci skomplikowane obliczenia matematyczne. We wrześniu 1813 r. uczestniczył w konkursie pamięciowych obliczeń, w którym jego przeciwnikiem był dziewięcioletni Amerykanin Zerah Colburn, reklamowany jako „American calculating boy". Hamilton przegrał te zawody i być może urażone ambicje spowodowały, że zajął się bardziej intensywnie matematyką i fizyką matematyczną.

Konstrukcja kwaternionów jest analogiczna do konstrukcji liczb zespolonych. Przypomnijmy, że liczby zespolone to uporządkowane pary (a, b) liczb rzeczywistych. Parę postaci $(a, 0)$ utożsamiamy z liczbą $a \in \mathbb{R}$ i w ten sposób zbiór liczb rzeczywistych $\mathbb{R}$ uważamy za podzbiór zbioru liczb zespolonych. Oznaczając $i = (0, 1)$ zapisujemy liczbę zespoloną w postaci $a + bi$. Dodawanie w zbiorze $\mathbb{C}$ definiujemy zgodnie ze wzorem na dodawanie wektorów:

$$(a, b) + (a_1, b_1) = (a + a_1, b + b_1).$$

Mnożenie można zdefiniować przyjmując, że $i^2 = -1$ i stosując zwykłe reguły działań. W ten sposób

$$(a + bi)(a_1 + b_1 i) = aa_1 + ab_1 i + a_1 bi + bb_1 i^2 = aa_1 - bb_1 + (ab_1 + a_1 b)i.$$

Inny model ciała liczb zespolonych $\mathbb{C}$ to model macierzowy. Niech M będzie zbiorem wszystkich macierzy postaci

$$\begin{bmatrix} a, & b \\ -b, & a \end{bmatrix}$$

gdzie $a, b \in \mathbb{R}$. Funkcja F, która liczbie zespolonej $a + bi$ przyporządkowuje taką macierz jest wzajemnie jednoznacznym odwzorowaniem zbioru $\mathbb{C}$ na M. Jest ona homomorfizmem ciała $\mathbb{C}$ na zbiór M rozpatrywany ze zwykłymi działaniami na macierzach. Rzeczywiście jeśli $z = a + bi$, $z_1 = a_1 + b_1 i$, to

$$F(z + z_1) = \begin{bmatrix} a + a_1, & b + b_1 \\ -b - b_1, & a + a_1 \end{bmatrix} = \begin{bmatrix} a, & b \\ -b, & a \end{bmatrix} + \begin{bmatrix} a_1, & b_1 \\ -b_1, & a_1 \end{bmatrix} = F(z) + F(z_1).$$

Ponadto

$$F(i)^2 = F(i)F(i) = \begin{bmatrix} 0, & 1 \\ -1, & 0 \end{bmatrix} \begin{bmatrix} 0, & 1 \\ -1, & 0 \end{bmatrix} = \begin{bmatrix} -1, & 0 \\ 0, & -1 \end{bmatrix} = - \begin{bmatrix} 1, & 0 \\ 0, & 1 \end{bmatrix}$$

przy czym

$$I_2 = \begin{bmatrix} 1, & 0 \\ 0, & 1 \end{bmatrix}$$

jest jedynką mnożenia w M. W M mamy więc wzór $F(i)^2 = -I_2$ analogiczny do wzoru $i^2 = -1$. Stąd i ze wzoru

$$F(z) = \begin{bmatrix} a, & b \\ -b, & a \end{bmatrix} = \begin{bmatrix} a, & 0 \\ 0, & a \end{bmatrix} + \begin{bmatrix} 0, & b \\ -b, & 0 \end{bmatrix} = aI_2 + bF(i),$$

wynika, że

$$F(zz_1) = F(z)F(z_1).$$

Zatem M jest ciałem izomorficznym z $\mathbb{C}$.

Zauważmy ponadto, że

$$\det F(z) = \det \begin{bmatrix} a, & b \\ -b, & a \end{bmatrix} = a^2 + b^2 = |z|^2.$$

Analogicznie kwaterniony definiujemy jako uporządkowane czwórki liczb rzeczywistych (a, b, c, d). Zbiór wszystkich takich czwórek oznaczamy przez $\mathbb{H}$. Czwórkę postaci $(a, 0, 0, 0)$ utożsamiamy z liczbą a. Oznaczając $\mathbf{i} = (0, 1, 0, 0)$, $\mathbf{j} = (0, 0, 1, 0)$, $\mathbf{k} = (0, 0, 0, 1)$ otrzymujemy zapis

$$(a, b, c, d) = a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}.$$

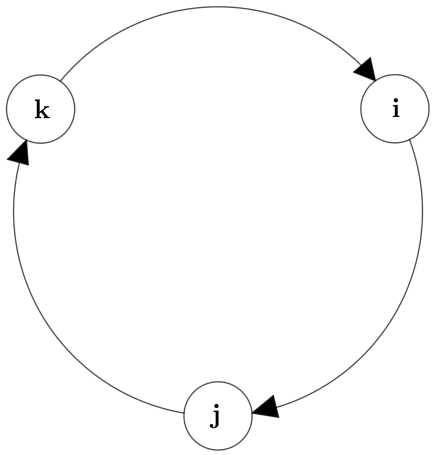
Dodawanie w zbiorze $\mathbb{H}$ definiujemy wzorem

$$(a + b\,\mathbf{i} + c\,\mathbf{j} + d\,\mathbf{k}) + (a_1 + b_1\,\mathbf{i} + c_1\,\mathbf{j} + d_1\,\mathbf{k}) = a + a_1 + (b + b_1)\mathbf{i} + (c + c_1)\mathbf{j} + (d + d_1)\mathbf{k}.$$

Mnożenie jednostek $\mathbf{i}, \mathbf{j}, \mathbf{k}$ definiujemy wzorami

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Do zobrazowania tych wzorów stosujemy następujący diagram.



Rysunek 2. Mnożenie kwaternionów

Stosując te wzory i zwykłe reguły działań możemy wykonywać mnożenie dowolnych kwaternionów, np.

$$(1 + \mathbf{i})(2 + \mathbf{k}) = 2 + \mathbf{k} + \mathbf{i} \cdot 2 + \mathbf{ik} = 2 + \mathbf{k} + 2\mathbf{i} + (-\mathbf{j}) = 2 + 2\mathbf{i} - \mathbf{j} + \mathbf{k}.$$

Zbiór $\mathbb{H}$ z tak zdefiniowanymi działaniami jest pierścieniem. Zerem tego pierścienia jest liczba 0, zaś jedynką liczba 1. Pierścień $\mathbb{H}$ nie jest przemienny, gdyż np.

$$\mathbf{ik} = -\mathbf{j} \neq \mathbf{j} = \mathbf{ki}.$$