**Kwaterniony**

# 1 Równania kwadratowe

Badamy równanie $w(x) = x^2 - (i+j)x + ij = (x-i)(x-j) = 0$

Oczywiście $w(j) = 0$ ale $w(i) = ij - ji = 2k$ jak zawsze w wielomianach o nieprzemiennych współczynnikach.

Szukamy pozostałych pierwiastków tego wielomianu.
Przyjmijmy $w(x) = x^2 + bx + c$, gdzie $b = -(i+j)$ zaś $c = ij$. Wtedy: $b \neq 0$, $\bar{b} = -b$, $\bar{c} = -c$ i $bc = -cb$.

Niech $h \in \mathbb{H}$ będzie rozwiązaniem. Wówczas $h$ jest też rozwiązaniem równania $x^2 - (h+\bar{h})x + h\bar{h}$.

Przyjmijmy $t = h + \bar{h}$ i $n = h\bar{h}$. Teraz $t, n \in \mathbb{R}$ oraz $n \geq 0$. Odejmując stronami równania $x^2 + bx + c = 0$ i $x^2 - tx + n = 0$ otrzymujemy
$(b+t)x + c - n = 0$ stąd $x = \frac{1}{b+t}(n-c) = \frac{t-b}{t^2-b^2}(n-c)$. $t^2 - b^2 \in \mathbb{R}$.
Zatem $h$ jest wyznaczone jednoznacznie przez swoją normę $n$ i ślad $t$.

Wyliczamy $t = h + \bar{h} = \frac{t-b}{t^2-b^2}(n-c) + \overline{\frac{t-b}{t^2-b^2}(n-c)} =$
$\frac{1}{t^2-b^2}(t-b)(n-c) + \frac{1}{t^2-b^2}(n+c)(t+b) = \frac{2tn}{t^2-b^2}$

$n = h\bar{h} = \frac{t-b}{t^2-b^2}(n-c)\overline{\frac{t-b}{t^2-b^2}(n-c)} = \frac{1}{(t^2-b^2)^2}(t-b)(n-c)(n+c)(t+b) =$
$\frac{(t^2-b^2)(n^2-c^2)}{(t^2-b^2)^2} = \frac{n^2-c^2}{t^2-b^2}$

Skoro $t = \frac{2tn}{t^2-b^2}$ to rozpatrzmy dwa przypadki:

1) $t = 0$. Wtedy $n = \frac{n^2-c^2}{-b^2}$ i $n$ jest pierwiastkiem równania $x^2 + b^2x - c^2 = 0$. W przypadku $b = -(i+j)$ i $c = ij$ daje to $x^2 - 2x + 1 = 0$. Zatem $n = 1$. Ponieważ $j + \bar{j} = 0$ oraz $j\bar{j} = 1$ więc $h = j$.

2) $t \neq 0$. Wtedy $1 = \frac{2n}{t^2-b^2}$ i $n = \frac{n^2-c^2}{t^2-b^2} = \frac{n^2-c^2}{2n}$. Zatem $n$ jest pierwiastkiem równania $x^2 + c^2 = 0$. W przypadku $c = ij$ daje to $x^2 - 1 = 0$. Zatem $n = \pm 1$. Ponieważ $n \geq 0$ więc $n = 1$.

Podstawiając do normy $n = 1$ otrzymujemy $1 = \frac{1-c^2}{t^2-b^2} = \frac{2}{t^2+2}$ stąd $t^2 + 2 = 2$ i $t = 0$ sprzeczność.

Podsumowując $w(x)$ ma tylko jeden pierwiastek.

**Uwaga 1** *Jeżeli $w(x) = x^2 + bx + c$, gdzie $b \neq 0$, $\bar{b} = -b$, $\bar{c} = -c$, $bc = -cb$ i $b^4 = -4c^2$ to $w(x)$ ma tylko jeden pierwiastek.*

**Stwierdzenie 2** *Wielomiany $w(x) = (x-a)^2 \in H[x]$ mają jeden pierwiastek.*

**Dowód:**
Niech $h \in H[x]$ będzie pierwiastkiem $w(x)$. Zapiszmy $h = a - b$. Teraz $0 = w(a-b) = (a-b)^2 - 2a(a-b) + a^2 = ab - ba + b^2$. Czyli $b^2 = ba - ab$.
Przedstawmy $a = r + u$ i $b = s + v$, gdzie $r, s \in \mathbb{R}$ zaś $u, v \in \mathbb{R}^3$ są urojone.

$ab = rs - \langle u, v \rangle + av + su + u \times v$

$ba = rs - \langle u, v \rangle + av + su + v \times u$

$b^2 = s^2 - \langle v, v \rangle + 2sv + u \times u$ co daje:

$b^2 = s^2 - \langle v, v\rangle + 2sv = 2v \times u.$

Porównując części rzeczywiste i urojone otrzymujemy:

$$\begin{cases} s^2 - \langle v, v\rangle = 0 \\ 2sv = 2v \times u \end{cases}$$

Ponieważ $v \perp (v \times u)$ więc $v = 0$, a stąd $s = 0$, $b = 0$ i $h = a$ jest jedynym pierwiastkiem.

□

## 2 Algebraiczna domkniętość.

Ponieważ w pierścieniach wielomianów nad pierścieniami z dzieleniem działa algorytm Euklidesa z normą, którą jest stopień wielomianu więc prawdziwe jest twierdzenie:

**Twierdzenie 3** *Każdy niezerowy ideał lewostronny pierścienia $H[x]$ jest generowany przez jeden wielomian unormowany.*

**Definicja 4** *Najmniejszą ( lewostronną ) wspólną wielokrotnością wielomianów $g(x)$ i $h(x)$ nazywać będziemy taki unormowany wielomian $n(x) = NWW(g, h)$, że $H[x]g(x) \cap H[x]h(x) = H[x]n(x)$.*

**Przykład 5** $NWW(x - i,\ x - j) = x^2 + 1.$

**Przykład 6** *Obliczmy teraz $NWW(x - 2i,\ x - j)$. Wspólnymi wielokrotnościami tych wielomianów są $g(x) = (x^2 + 1)(x - 2i) = x^3 - 2ix^2 + x - 2i$ oraz $h(x) = (x^2 + 4)(x - j) = x^3 - jx^2 + 4x - 4j$. Zatem najmniejszą wspólną wielokrotnością będzie największy wspólny dzielnik wielomianów $g(x)$ i $h(x)$. Uzyskujemy go normując $g(x) - h(x)$.*

$NWW(x - 2i,\ x - j) = x^2 + \frac{3}{5}(j - 2i)x + \frac{1}{5}(8 + 6k).$

*Rzeczywiście* $x^2 + \frac{3}{5}(j - 2i)x + \frac{1}{5}(8 + 6k) = \big(x + \frac{1}{5}(4i + 3j)\big)(x - 2i)$

*oraz* $x^2 + \frac{3}{5}(j - 2i)x + \frac{1}{5}(8 + 6k) = \big(x - \frac{1}{5}(6i - 8j)\big)(x - j).$

**Twierdzenie 7** *(Niven)W pierścieniu $H[x]$:*

*1) Każdy nierozkładalny wielomian ma stopień równy 1.*

*2) Każdy wielomian stopnia $\geq 1$ jest iloczynem wielomianów stopnia 1.*

*3) Każdy wielomian stopnia $\geq 1$ ma pierwiastek w $H$.*

**Dowód:**

Ad 1). Niech $p = p(x) \in H[x]$ będzie unormowanym, nierozkładalnym wielomianem. Wielomian $w(x) = \overline{p}p \in \mathbb{R}[x] \subset \mathbb{C}[x] \subset H[x]$ ma współczynniki rzeczywiste. Zatem istnieje liczba zespolona $z$ taka, że $w(z) = 0$.

a) Jeżeli $x - z$ dzieli $p$ to $p = x - z$ jest wielomianem stopnia 1.

b) Jeżeli $z \in \mathbb{R}$ to $0 = w(z) = \overline{p(z)}p(z)$, stąd $p(z) = 0$ i $p$ jest wielomianem stopnia 1.

c) Niech $x-z$ nie dzieli $p$. Przyjmijmy $n(x) = NWW\big(p(x),\ x-z\big)$.
Teraz $n(x) = h(x)p(x)$ i stopień $h$ jest $\geq 1$. ($x-z$ nie dzieli $p$)

Ponieważ $w(x) = \overline{p}p$ jest zarówno wielokrotnością $x-z$ jak i $p$ to $\overline{p}p = g(x)n(x) = g(x)h(x)p(x)$. Ale $H[x]$ jest dziedziną więc możemy tą równość skrócić przez $p$ i $\overline{p} = g(x)h(x)$. Z nierozkładalności $\overline{p} = h(x)$ i $g(x) = 1$. Otrzymaliśmy $\overline{p}p = n(x)$.

Inną wspólną wielokrotnością $x-z$ jak i $p$ jest $(x-\overline{z})(x-z)p(x)$.
Stąd $\overline{p}p$ dzieli $(x-\overline{z})(x-z)p(x)$ oraz $\overline{p}$ dzieli $(x-\overline{z})(x-z)$.
Zatem $\overline{p}$ i $p$ są wielomianami stopnia 1.

Ad 2) Każdy wielomian stopnia $\geq 1$ jest iloczynem wielomianów nierozkładalnych więc na mocy 1) jest iloczynem wielomianów stopnia 1.

Ad 3) Każdy wielomian stopnia $\geq 1$ jest iloczynem
$w(x) = h(x-h_1)(x-h_2)...(x-h_2)$, stąd $w(h_n) = 0$.

$\square$

# 3 Kwaterniony uogólnione.

**Stwierdzenie 8** *Niech $K$ będzie ciałem charakterystyki różnej od 2 zaś $G = \langle g, h|\ g^4 = 1,\ h^{-1}gh = g^{-1},\ g^2 = h^2\rangle$ grupą kwaternionów. Wówczas $KG = K \times K \times K \times K \times H(K)$, gdzie $H(K)$ jest 4- wymiarową algebrą prostą izomorficzną z $KG/(1+g^2)$*

**Dowód:**
W $KG$ mamy centralne idempotenty wyznaczone przez dzielniki normalne:
$e_1 = \frac{1}{8}\widehat{G}$, $e_2 = \frac{1}{4}\widehat{\langle g\rangle}$, $e_3 = \frac{1}{4}\widehat{\langle h\rangle}$, $e_4 = \frac{1}{4}\widehat{\langle gh\rangle}$, $e_5 = \frac{1}{2}\widehat{\langle g^2\rangle}$.

Mamy następujący rozkład jedynki na ortogonalne idempotenty:

$1 = e_1 + (e_2 - e_1) + (e_3 - e_1) + (e_4 - e_1) + (1 - e_5)$.

Więcej składników być nie może bo $G$ ma tylko 5 klas sprzężoności i centrum $KG$ jest wymiaru 5. Innym argumentem jest, że nieprzemienna algebra półprosta ma wymiar $\geq 4$.

$\square$

Przypomnijmy:

**Twierdzenie 9** *Niech $K$ będzie ciałem charakterystyki $\neq 2$.
Wówczas równoważne są warunki:*

*1) Grupa $Q_8$ jest zawarta w grupie $Gl(3, K)$.*

*2) Grupa $Q_8$ jest zawarta w grupie $Gl(2, K)$.*

*3) Równanie $x^2 + y^2 + 1 = 0$ ma rozwiązanie w ciele $K$.*

**Twierdzenie 10** *Przy tych samych oznaczeniach następujące warunki są równoważne:*

*1) $K(H) \simeq M_2(K)$,*

*2) Grupa $Gl(2,k)$ zawiera podgrupę izomorficzną z grupą kwaternionów $Q_8$,*
*3) Równanie $x^2+y^2=-1$ ma rozwiązanie w ciele $K$.*

**Dowód:**
1) $\Rightarrow$ 2) Oczywiste.
2) $\Rightarrow$ 3) Niech $\phi : Q_8 \to M_2(K)$ będzie zanurzeniem zaś $\Phi : KQ_8 \to M_2(K)$ będzie przedłużeniem tego homomorfizmu. Wówczas $\Phi\big(KQ_8\big)$ jest nieprzemienną półprostą podalgebrą $M_2(K)$. Zatem $\Phi\big(KQ_8\big) = M_2(K) = H(K)$, na mocy stwierdzenia **??**.

$\square$

Bezpośrednio otrzymujemy

**Wniosek 11** *Przy tych samych oznaczeniach następujące warunki są równoważne:*
*1) $H(K)$ jest algebrą z dzieleniem,*
*2) Grupa $Gl(2,K)$ nie zawiera podgrupy izomorficznej z grupą kwaternionów $Q_8$,*
*3) Równanie $x^2+y^2=-1$ nie ma rozwiązania w ciele $K$.*

**Dowód:**

$\square$

**Twierdzenie 12 (Gauss)** *Jeżeli $n$ jest bezkwadratową liczbą naturalną, to równoważne są warunki:*
*1) $n$ jest sumą trzech kwadratów liczb wymiernych,*
*2) $n$ jest sumą trzech kwadratów liczb naturalnych,*
*3) $n$ nie jest postaci $8k+7$.*

Jako wniosek otrzymujemy:

**Twierdzenie 13** *Jeżeli $n$ jest bezkwadratową liczbą naturalną, to równoważne są warunki:*
*1) Grupa $Gl\Big(2, Q(i\sqrt{n})\Big)$ zawiera grupę $Q_8$.*
*2) Grupa $Gl\Big(3, Q(i\sqrt{n})\Big)$ zawiera grupę $Q_8$.*
*3) $n$ nie jest postaci $8k+7$.*

**Twierdzenie 14 (Moser)** *Niech $K = Q(\xi_n)$ będzie ciałem cyklotomicznym, gdzie $\xi_m$ jest pierwiastkiem pierwotnym stopnia $n$ z 1. Wówczas równanie $x^2+y^2=-1$ ma rozwiązanie w ciele $K$ wtedy i tylko wtedy gdy rząd $1+1$ w grupie multyplikatywnej ciała $Z_n$ jest liczbą parzystą.*

Jako wniosek otrzymujemy:

**Twierdzenie 15** *Niech* $K = Q(\xi_n)$ *będzie ciałem cyklotomicznym, gdzie* $\xi_m$ *jest pierwiastkiem pierwotnym stopnia n z 1. Wówczas równoważne są warunki:*

*1) Grupa* $Gl\Big(2, Q(\xi_n)\Big)$ *zawiera grupę* $Q_8$.

*2) Grupa* $Gl\Big(3, Q(\xi_n)\Big)$ *zawiera grupę* $Q_8$.

*3) Rząd* $1+1$ *w grupie multyplikatywnej ciała* $Z_n$ *jest liczbą parzystą.*

**Twierdzenie 16** *Jeżeli* $K$ *jest ciałem nierzeczywistym to nie istnieje zanurzenie algebry* $H(K)$ *w pierścień kwaternionów.*

**Dowód:**
Niech $K$ będzie ciałem nierzeczywistym i $f : H(K) \to H$ będzie zanurzeniem algebry $H(K)$ w pierścień kwaternionów. Ponieważ $f(K)$ nie jest ciałem rzeczywistym więc $f(K) \not\subset \mathbb{R}$. Niech $T = C_H\big(f(K)\big)$. Skoro $\mathbb{R}$ jest centrum $H$ to $T = C_H\big(f(K)\big) = C_H\big(f(K)\mathbb{R}\big) \simeq \mathbb{C}$ jest maksymalnym podciałem $H$. Dalej $g, h \in C_H\big(K\big)$ więc $f(g), f(h) \in C_H\big(f(K)\big) = f(K)\mathbb{R}$. Otrzymaliśmy przemienność $f(g), f(h)$ co jest niemożliwe.

$\square$

5) NIE, poniewaz istnieja ciala o dowolnie duzym Štufe "Teoria Pfistera. Lacze pozdrowienia, J.Browkin