O ordynkach

Beata Rothkegel

Letnia Szkoła Instytutu Matematyki
Brenna, 2018

Pierścień całkowity R nazywamy *pierścieniem Dedekinda*, jeśli

- R jest pierścieniem noetherowskim,
- $\dim R = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest pierścieniem całkowicie domkniętym.

- R jest skończenie generowanym R-modułem

Pierścień całkowity R nazywamy *pierścieniem Dedekinda*, jeśli

- R jest pierścieniem noetherowskim,
- $\dim R = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest pierścieniem całkowicie domkniętym.

- R jest skończenie generowanym R-modułem

Pierścień całkowity R nazywamy *pierścieniem Dedekinda*, jeśli

- R jest pierścieniem noetherowskim,
- $\dim R = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest pierścieniem całkowicie domkniętym.

- R jest skończenie generowanym R-modułem

Pierścień całkowity R nazywamy *pierścieniem Dedekinda*, jeśli

- R jest pierścieniem noetherowskim,
- $\dim R = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest pierścieniem całkowicie domkniętym.

- R jest skończenie generowanym R-modułem

Pierścień całkowity R nazywamy *pierścieniem Dedekinda*, jeśli

- R jest pierścieniem noetherowskim,
- $\dim R = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest pierścieniem całkowicie domkniętym.

- R jest skończenie generowanym R-modułem

R – pierścień Dedekinda

$\mathcal{O} < R$

- $\mathcal{O}$ jest pierścieniem noetherowskim,
- $\dim \mathcal{O} = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest pierścieniem całkowicie domkniętym (R jest całkowitym domknięciem R w ciele ułamków R),

R – pierścień Dedekinda

$\mathcal{O} < R$

- $\mathcal{O}$ jest pierścieniem noetherowskim,
- $\dim \mathcal{O} = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest pierścieniem całkowicie domkniętym (R jest całkowitym domknięciem R w ciele ułamków R),

R – pierścień Dedekinda

$\mathcal{O} < R$

- $\mathcal{O}$ jest pierścieniem noetherowskim,
- $\dim \mathcal{O} = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest pierścieniem całkowicie domkniętym (R jest całkowitym domknięciem R w ciele ułamków R),

R – pierścień Dedekinda

$\mathcal{O} < R$

- $\mathcal{O}$ jest pierścieniem noetherowskim,
- $\dim \mathcal{O} = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest pierścieniem całkowicie domkniętym (R jest całkowitym domknięciem R w ciele ułamków R),

R – pierścień Dedekinda

$\mathcal{O} < R$

- $\mathcal{O}$ jest pierścieniem noetherowskim,
- $\dim \mathcal{O} = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest całkowitym domknięciem $\mathcal{O}$ w ciele ułamków $\mathcal{O}$,
- R jest skończenie generowanym R-modułem

R – pierścień Dedekinda

$\mathcal{O} < R$

- $\mathcal{O}$ jest pierścieniem noetherowskim,
- $\dim \mathcal{O} = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest całkowitym domknięciem $\mathcal{O}$ w ciele ułamków $\mathcal{O}$,
- R jest skończenie generowanym R-modułem

R – pierścień Dedekinda

$\mathcal{O} < R$

- $\mathcal{O}$ jest pierścieniem noetherowskim,
- $\dim \mathcal{O} = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest całkowitym domknięciem $\mathcal{O}$ w ciele ułamków $\mathcal{O}$,
- R jest skończenie generowanym $\mathcal{O}$-modułem

R – pierścień Dedekinda

$\mathcal{O} < R$

- $\mathcal{O}$ jest pierścieniem noetherowskim,
- $\dim \mathcal{O} = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest całkowitym domknięciem $\mathcal{O}$ w ciele ułamków $\mathcal{O}$,
- R jest skończenie generowanym $\mathcal{O}$-modułem

$\mathcal{O}$ nazywamy *ordynkiem* (w pierścieniu R).

Pierścień Dedekinda R jest ordynkiem i nazywamy go *ordynkiem maksymalnym*.

R – pierścień Dedekinda

$\mathcal{O} < R$

- $\mathcal{O}$ jest pierścieniem noetherowskim,
- $\dim \mathcal{O} = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
- R jest całkowitym domknięciem $\mathcal{O}$ w ciele ułamków $\mathcal{O}$,
- R jest skończenie generowanym $\mathcal{O}$-modułem

$\mathcal{O}$ nazywamy *ordynkiem* (w pierścieniu R).

Pierścień Dedekinda R jest ordynkiem i nazywamy go *ordynkiem maksymalnym*.

A. Geroldinger and F. Halter-Koch and J. Kaczorowski, ***Non-unique factorizations in orders of global fields***, J. Reine Angew. Math. 459 (1995), 89–118.

Definicja

Niech R będzie pierścieniem Dedekinda. Ordynkiem w R nazywamy taki podpierścień $\mathcal{O}$ pierścienia R, że $\mathcal{O}$-moduł ilorazowy $R/\mathcal{O}$ jest skończenie generowanym $\mathcal{O}$-modułem torsyjnym.

K – ciało liczbowe (skończone rozszerzenie $\mathbb{Q}$)

R – pierścień wszystkich liczb algebraicznych całkowitych w K

J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, New York, Berlin, Heidelberg, 1999.

Definicja

Ordynkiem $\mathcal{O}$ w ciele K nazywamy podpierścień pierścienia R, który jest wolną grupą abelową rangi $[K : \mathbb{Q}]$.

K – ciało liczbowe (skończone rozszerzenie $\mathbb{Q}$)

R – pierścień wszystkich liczb algebraicznych całkowitych w K

J. Neukirch, ***Algebraic Number Theory***, Springer-Verlag, New York, Berlin, Heidelberg, 1999.

Definicja

Ordynkiem $\mathcal{O}$ w ciele K nazywamy podpierścień pierścienia R, który jest wolną grupą abelową rangi $[K : \mathbb{Q}]$.

K – ciało liczbowe (skończone rozszerzenie $\mathbb{Q}$)

R – pierścień wszystkich liczb algebraicznych całkowitych w K

J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, New York, Berlin, Heidelberg, 1999.

Definicja

Ordynkiem $\mathcal{O}$ w ciele K nazywamy podpierścień pierścienia R, który jest wolną grupą abelową rangi $[K : \mathbb{Q}]$.

Przykłady ordynków

$K = \mathbb{Q}(\sqrt{d})$, gdzie $d \neq 1$ jest bezkwadratową liczbą całkowitą

Wtedy $R = \mathbb{Z}[\omega]$, gdzie

$$\omega = \begin{cases} \sqrt{d}, & \text{gdy } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{gdy } d \equiv 1 \pmod 4. \end{cases}$$

Każdy ordynek w K jest postaci $\mathcal{O} = \mathbb{Z}[f\omega]$ dla pewnej liczby naturalnej f.

Przykłady ordynków

$K = \mathbb{Q}(\sqrt{d})$, gdzie $d \neq 1$ jest bezkwadratową liczbą całkowitą

Wtedy $R = \mathbb{Z}[\omega]$, gdzie

$$\omega = \begin{cases} \sqrt{d}, & \text{gdy } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{gdy } d \equiv 1 \pmod 4. \end{cases}$$

Każdy ordynek w K jest postaci $\mathcal{O} = \mathbb{Z}[f\omega]$ dla pewnej liczby naturalnej f.

Przykłady ordynków

$K = \mathbb{Q}(\sqrt{d})$, gdzie $d \neq 1$ jest bezkwadratową liczbą całkowitą

Wtedy $R = \mathbb{Z}[\omega]$, gdzie

$$\omega = \begin{cases} \sqrt{d}, & \text{gdy } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{gdy } d \equiv 1 \pmod 4. \end{cases}$$

Każdy ordynek w K jest postaci $\mathcal{O} = \mathbb{Z}[f\omega]$ dla pewnej liczby naturalnej f.

Przykład zastosowania ordynków

Poszukiwanie kryteriów rozwiązalności równań diofantycznych, na przykład:

D. Cox, ***Primes of the form*** $x^2 + ny^2$***: Fermat, class field theory, and complex multiplication***, John Wiley & Sons, 1989.

Niech $n \in \mathbb{N}$. Używając ordynka $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ w ciele $K = \mathbb{Q}(\sqrt{-n})$

($\mathcal{O} = R$, gdy $n \not\equiv 3 \pmod 4$ i $\mathcal{O} = \mathbb{Z}\left[2\frac{1+\sqrt{-n}}{2}\right]$, gdy
$n \equiv 3 \pmod 4$),

Cox sformułował kryterium rozwiązalności równania

$$x^2 + ny^2 = p \quad \text{nad } \mathbb{Z},$$

gdzie p jest nieparzystą liczbą pierwszą.

Przykład zastosowania ordynków

Poszukiwanie kryteriów rozwiązalności równań diofantycznych, na przykład:

D. Cox, ***Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication***, John Wiley & Sons, 1989.

Niech $n \in \mathbb{N}$. Używając ordynka $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ w ciele $K = \mathbb{Q}(\sqrt{-n})$

($\mathcal{O} = R$, gdy $n \not\equiv 3 \pmod 4$ i $\mathcal{O} = \mathbb{Z}\left[2\frac{1+\sqrt{-n}}{2}\right]$, gdy
$n \equiv 3 \pmod 4$),

Cox sformułował kryterium rozwiązalności równania

$$x^2 + ny^2 = p \quad \text{nad } \mathbb{Z},$$

gdzie p jest nieparzystą liczbą pierwszą.

Przykład zastosowania ordynków

Poszukiwanie kryteriów rozwiązalności równań diofantycznych, na przykład:

D. Cox, *Primes of the form* $x^2 + ny^2$*: Fermat, class field theory, and complex multiplication*, John Wiley & Sons, 1989.

Niech $n \in \mathbb{N}$. Używając ordynka $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ w ciele $K = \mathbb{Q}(\sqrt{-n})$

($\mathcal{O} = R$, gdy $n \not\equiv 3 \pmod 4$ i $\mathcal{O} = \mathbb{Z}\left[2\frac{1+\sqrt{-n}}{2}\right]$, gdy
$n \equiv 3 \pmod 4$),

Cox sformułował kryterium rozwiązalności równania

$$x^2 + ny^2 = p \quad \text{nad } \mathbb{Z},$$

gdzie p jest nieparzystą liczbą pierwszą.

Twierdzenie

Istnieje unormowany, nierozkładalny wielomian $F_n \in \mathbb{Z}[X]$ *taki, że jeśli* p *nie dzieli* n *i nie dzieli wyróżnika* F_n*, to równanie* $x^2 + ny^2 = p$ *jest rozwiązalne nad* $\mathbb{Z}$ *wtedy i tylko wtedy, gdy*

1. $-n$ *jest kwadratem modulo* p*,*
2. *równanie* $F_n(x) = 0$ *jest rozwiązalne nad* $\mathbb{Z}_p$*.*

Uogólnienie (inne artykuły):

kryterium rozwiązalności $x^2 + ny^2 = p$ nad ordynkiem maksymalnym R w dowolnym ciele liczbowym K

Twierdzenie

Istnieje unormowany, nierozkładalny wielomian $F_n \in \mathbb{Z}[X]$ taki, że jeśli p nie dzieli n i nie dzieli wyróżnika F_n, to równanie $x^2 + ny^2 = p$ jest rozwiązalne nad $\mathbb{Z}$ wtedy i tylko wtedy, gdy

1. *$-n$ jest kwadratem modulo p,*
2. *równanie $F_n(x) = 0$ jest rozwiązalne nad $\mathbb{Z}_p$.*

Uogólnienie (inne artykuły):

kryterium rozwiązalności $x^2 + ny^2 = p$ nad ordynkiem maksymalnym R w dowolnym ciele liczbowym K

Kiedy ordynek w ciele liczbowym jest ordynkiem maksymalnym?

K – ciało liczbowe

$\mathcal{O}$ – ordynek w K

$C(\mathcal{O})$ – grupa dywizorów Cartiera (multyplikatywna grupa generowana przez wszystkie ideały odwracalne w $\mathcal{O}$)

Oczywiście $C(R)$ – grupa wszystkich ideałów ułamkowych K

Kiedy ordynek w ciele liczbowym jest ordynkiem maksymalnym?

K – ciało liczbowe

$\mathcal{O}$ – ordynek w K

$C(\mathcal{O})$ – grupa dywizorów Cartiera (multyplikatywna grupa generowana przez wszystkie ideały odwracalne w $\mathcal{O}$)

Oczywiście $C(R)$ – grupa wszystkich ideałów ułamkowych K

Kiedy ordynek w ciele liczbowym jest ordynkiem maksymalnym?

K – ciało liczbowe

$\mathcal{O}$ – ordynek w K

$C(\mathcal{O})$ – grupa dywizorów Cartiera (multyplikatywna grupa generowana przez wszystkie ideały odwracalne w $\mathcal{O}$)

Oczywiście $C(R)$ – grupa wszystkich ideałów ułamkowych K

Kiedy ordynek w ciele liczbowym jest ordynkiem maksymalnym?

K – ciało liczbowe

$\mathcal{O}$ – ordynek w K

$C(\mathcal{O})$ – grupa dywizorów Cartiera (multyplikatywna grupa generowana przez wszystkie ideały odwracalne w $\mathcal{O}$)

Oczywiście $C(R)$ – grupa wszystkich ideałów ułamkowych K

Kiedy ordynek w ciele liczbowym jest ordynkiem maksymalnym?

K – ciało liczbowe

$\mathcal{O}$ – ordynek w K

$C(\mathcal{O})$ – grupa dywizorów Cartiera (multyplikatywna grupa generowana przez wszystkie ideały odwracalne w $\mathcal{O}$)

Oczywiście $C(R)$ – grupa wszystkich ideałów ułamkowych K

U_K – grupa jedności K (grupa elementów odwracalnych w R), na przykład:

$K = \mathbb{Q}(i)$, to $U_K = \{\pm 1, \pm i\}$

$K = \mathbb{Q}(\sqrt{-n})$, $n \in \mathbb{N}$, $n \neq 1, 3$, to $U_K = \{1, -1\}$

$K = \mathbb{Q}(\sqrt{-3})$, to $U_K = \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\}$

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. *$C(\mathcal{O})$ jest grupą beztorsyjną,*
2. *$U_K \subseteq \mathcal{O}$.*

U_K – grupa jedności K (grupa elementów odwracalnych w R), na przykład:

$K = \mathbb{Q}(i)$, to $U_K = \{\pm 1, \pm i\}$

$K = \mathbb{Q}(\sqrt{-n})$, $n \in \mathbb{N}$, $n \neq 1, 3$, to $U_K = \{1, -1\}$

$K = \mathbb{Q}(\sqrt{-3})$, to $U_K = \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\}$

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. *$C(\mathcal{O})$ jest grupą beztorsyjną,*
2. *$U_K \subseteq \mathcal{O}$.*

U_K – grupa jedności K (grupa elementów odwracalnych w R), na przykład:

$K = \mathbb{Q}(i)$, to $U_K = \{\pm 1, \pm i\}$

$K = \mathbb{Q}(\sqrt{-n})$, $n \in \mathbb{N}$, $n \neq 1, 3$, to $U_K = \{1, -1\}$

$K = \mathbb{Q}(\sqrt{-3})$, to $U_K = \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\}$

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. *$C(\mathcal{O})$ jest grupą beztorsyjną,*
2. *$U_K \subseteq \mathcal{O}$.*

U_K – grupa jedności K (grupa elementów odwracalnych w R), na przykład:

$K = \mathbb{Q}(i)$, to $U_K = \{\pm 1, \pm i\}$

$K = \mathbb{Q}(\sqrt{-n})$, $n \in \mathbb{N}$, $n \neq 1, 3$, to $U_K = \{1, -1\}$

$K = \mathbb{Q}(\sqrt{-3})$, to $U_K = \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\}$

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. *$C(\mathcal{O})$ jest grupą beztorsyjną,*
2. *$U_K \subseteq \mathcal{O}$.*

U_K – grupa jedności K (grupa elementów odwracalnych w R), na przykład:

$K = \mathbb{Q}(i)$, to $U_K = \{\pm 1, \pm i\}$

$K = \mathbb{Q}(\sqrt{-n})$, $n \in \mathbb{N}$, $n \neq 1, 3$, to $U_K = \{1, -1\}$

$K = \mathbb{Q}(\sqrt{-3})$, to $U_K = \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\}$

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. *$C(\mathcal{O})$ jest grupą beztorsyjną,*
2. *$U_K \subseteq \mathcal{O}$.*

$P(\mathcal{O})$ – podgrupa $C(\mathcal{O})$ złożona ze wszystkich dywizorów głównych $a\mathcal{O}$, $0 \neq a \in K$

$\mathrm{Pic}(\mathcal{O}) := C(\mathcal{O})/P(\mathcal{O})$ – grupa Picarda, skończona

$\mathrm{Pic}(R)$ – grupa klas ideałów ciała K

$h_K := \#\mathrm{Pic}(R)$ – liczba klas ciała K

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. $\#\mathrm{Pic}(\mathcal{O}) = h_K$,
2. $U_K \subseteq \mathcal{O}$.

$P(\mathcal{O})$ – podgrupa $C(\mathcal{O})$ złożona ze wszystkich dywizorów głównych $a\mathcal{O}$, $0 \neq a \in K$

$\mathrm{Pic}(\mathcal{O}) := C(\mathcal{O})/P(\mathcal{O})$ – grupa Picarda, skończona

$\mathrm{Pic}(R)$ – grupa klas ideałów ciała K

$h_K := \#\mathrm{Pic}(R)$ – liczba klas ciała K

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. $\#\mathrm{Pic}(\mathcal{O}) = h_K$,
2. $U_K \subseteq \mathcal{O}$.

$P(\mathcal{O})$ – podgrupa $C(\mathcal{O})$ złożona ze wszystkich dywizorów głównych $a\mathcal{O}$, $0 \neq a \in K$

$\mathrm{Pic}(\mathcal{O}) := C(\mathcal{O})/P(\mathcal{O})$ – grupa Picarda, skończona

$\mathrm{Pic}(R)$ – grupa klas ideałów ciała K

$h_K := \#\mathrm{Pic}(R)$ – liczba klas ciała K

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. $\#\mathrm{Pic}(\mathcal{O}) = h_K$,
2. $U_K \subseteq \mathcal{O}$.

$P(\mathcal{O})$ – podgrupa $C(\mathcal{O})$ złożona ze wszystkich dywizorów głównych $a\mathcal{O}$, $0 \neq a \in K$

$\mathrm{Pic}(\mathcal{O}) := C(\mathcal{O})/P(\mathcal{O})$ – grupa Picarda, skończona

$\mathrm{Pic}(R)$ – grupa klas ideałów ciała K

$h_K := \#\mathrm{Pic}(R)$ – liczba klas ciała K

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. $\#\mathrm{Pic}(\mathcal{O}) = h_K$,
2. $U_K \subseteq \mathcal{O}$.

$P(\mathcal{O})$ – podgrupa $C(\mathcal{O})$ złożona ze wszystkich dywizorów głównych $a\mathcal{O}$, $0 \neq a \in K$

$\mathrm{Pic}(\mathcal{O}) := C(\mathcal{O})/P(\mathcal{O})$ – grupa Picarda, skończona

$\mathrm{Pic}(R)$ – grupa klas ideałów ciała K

$h_K := \#\mathrm{Pic}(R)$ – liczba klas ciała K

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. $\#\mathrm{Pic}(\mathcal{O}) = h_K$,
2. $U_K \subseteq \mathcal{O}$.

$P(\mathcal{O})$ – podgrupa $C(\mathcal{O})$ złożona ze wszystkich dywizorów głównych $a\mathcal{O}$, $0 \neq a \in K$

$\mathrm{Pic}(\mathcal{O}) := C(\mathcal{O})/P(\mathcal{O})$ – grupa Picarda, skończona

$\mathrm{Pic}(R)$ – grupa klas ideałów ciała K

$h_K := \#\mathrm{Pic}(R)$ – liczba klas ciała K

Twierdzenie

Niech K będzie ciałem liczbowym i $\mathcal{O}$ będzie ordynkiem w K. Wówczas $\mathcal{O}$ jest ordynkiem maksymalnym wtedy i tylko wtedy, gdy

1. $\#\mathrm{Pic}(\mathcal{O}) = h_K$,
2. $U_K \subseteq \mathcal{O}$.

$$\#\mathrm{Pic}(\mathcal{O}) = \frac{h_K}{\#(U_K/U(\mathcal{O}))}\frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

$\mathfrak{f}$ – konduktor $\mathcal{O}$ (największy ideał R zawarty w $\mathcal{O}$), na przykład:

$$K = \mathbb{Q}(\sqrt{d}), \quad \mathcal{O} = \mathbb{Z}[f\omega], \quad \text{to} \quad \mathfrak{f} = fR.$$

$$\omega = \begin{cases} \sqrt{d}, & \text{gdy } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{gdy } d \equiv 1 \pmod 4. \end{cases}$$

$$\#\mathrm{Pic}(\mathcal{O}) = \frac{h_K}{\#(U_K/U(\mathcal{O}))}\frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

$\mathfrak{f}$ – konduktor $\mathcal{O}$ (największy ideał R zawarty w $\mathcal{O}$), na przykład:

$$K = \mathbb{Q}(\sqrt{d}), \quad \mathcal{O} = \mathbb{Z}[f\omega], \quad \text{to} \quad \mathfrak{f} = fR.$$

$$\omega = \begin{cases} \sqrt{d}, & \text{gdy } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{gdy } d \equiv 1 \pmod 4. \end{cases}$$

$$\#\mathrm{Pic}(\mathcal{O}) = \frac{h_K}{\#(U_K/U(\mathcal{O}))}\frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

$\mathfrak{f}$ – konduktor $\mathcal{O}$ (największy ideał R zawarty w $\mathcal{O}$), na przykład:

$$K = \mathbb{Q}(\sqrt{d}), \quad \mathcal{O} = \mathbb{Z}[f\omega], \quad \text{to} \quad \mathfrak{f} = fR.$$

$$\omega = \begin{cases} \sqrt{d}, & \text{gdy } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{gdy } d \equiv 1 \pmod 4. \end{cases}$$

Przykład

$K = \mathbb{Q}(\sqrt{-n}),\ \ 1 \neq n \in \mathbb{N},\ n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}],\ \ \mathfrak{f} = fR,\ U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n}),\ \ 1 \neq n \in \mathbb{N},\ n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}]$, $\mathfrak{f} = fR$, $U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n}),\ \ 1 \neq n \in \mathbb{N},\ n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}],\ \ \mathfrak{f} = fR$, $U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n}),\ \ 1 \neq n \in \mathbb{N},\ n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}],\ \ \mathfrak{f} = fR,\ U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n}),\ \ 1 \neq n \in \mathbb{N},\ n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}],\ \ \mathfrak{f} = fR,\ U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n})$, $1 \neq n \in \mathbb{N}$, $n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}]$, $\mathfrak{f} = fR$, $U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n}),\ \ 1 \neq n \in \mathbb{N},\ n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}],\ \ \mathfrak{f} = fR,\ U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n})$, $1 \neq n \in \mathbb{N}$, $n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}]$, $\mathfrak{f} = fR$, $U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n})$, $1 \neq n \in \mathbb{N}$, $n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}]$, $\mathfrak{f} = fR$, $U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n}),\ \ 1 \neq n \in \mathbb{N},\ n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}],\ \ \mathfrak{f} = fR,\ U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n})$, $1 \neq n \in \mathbb{N}$, $n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}]$, $\mathfrak{f} = fR$, $U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n}),\ \ 1 \neq n \in \mathbb{N},\ n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}],\ \ \mathfrak{f} = fR,\ U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n})$, $1 \neq n \in \mathbb{N}$, $n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}]$, $\mathfrak{f} = fR$, $U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład

$K = \mathbb{Q}(\sqrt{-n})$, $1 \neq n \in \mathbb{N}$, $n \not\equiv 3 \pmod 4$

$\mathcal{O} = \mathbb{Z}[f\sqrt{-n}]$ dla pewnego $f \in \mathbb{N}$

Wtedy $R = \mathbb{Z}[\sqrt{-n}]$, $\mathfrak{f} = fR$, $U_K = \{1, -1\} \subseteq \mathcal{O}$ oraz

$$\#\mathrm{Pic}(\mathcal{O}) = h_k \frac{\#U(R/\mathfrak{f})}{\#U(\mathcal{O}/\mathfrak{f})}$$

Załóżmy, że $f \neq 1$.

(1) $\mathrm{NWD}(n, f) = 1$

Istnieją $x, y \in \mathbb{Z}$ takie, że $-nx + fy = 1$. Stąd

$$-nx + \mathfrak{f} = 1 + \mathfrak{f}, \quad \text{czyli} \quad (\sqrt{-n} + \mathfrak{f})(\sqrt{-n}x + \mathfrak{f}) = 1 + \mathfrak{f}.$$

Ostatecznie $\sqrt{-n} + \mathfrak{f} \in U(R/\mathfrak{f})$.

Przypuśćmy, że $\sqrt{-n} + \mathfrak{f} \in U(\mathcal{O}/\mathfrak{f})$. Wtedy istnieje $b \in \mathcal{O}$ taki, że $\sqrt{-n} + \mathfrak{f} = b + \mathfrak{f}$. Ale $\sqrt{-n} = b + f_1$ dla pewnego $f_1 \in \mathfrak{f} \subseteq \mathcal{O}$, czyli $\sqrt{-n} \in \mathcal{O}$, sprzeczność.

Przykład (cd)

(2) p jest liczbą pierwszą taką, że $p \mid n$ i $p \mid f$

$$\Rightarrow \left(1 + \frac{f}{p}\sqrt{-n}\right) + \mathfrak{f} \in U(R/\mathfrak{f}) \setminus U(\mathcal{O}/\mathfrak{f})$$

Zatem $\#\mathrm{Pic}(\mathcal{O}) \neq h_K$.

$\mathcal{O}$ maksymalny $\Leftrightarrow \#\mathrm{Pic}(\mathcal{O}) = h_K$

Przykład (cd)

(2) p jest liczbą pierwszą taką, że $p \mid n$ i $p \mid f$
$\Rightarrow \left(1 + \frac{f}{p}\sqrt{-n}\right) + \mathfrak{f} \in U(R/\mathfrak{f}) \setminus U(\mathcal{O}/\mathfrak{f})$

Zatem $\#\mathrm{Pic}(\mathcal{O}) \neq h_K$.

$\mathcal{O}$ maksymalny $\Leftrightarrow \#\mathrm{Pic}(\mathcal{O}) = h_K$

Przykład (cd)

(2) p jest liczbą pierwszą taką, że $p \mid n$ i $p \mid f$

$$\Rightarrow \left(1 + \frac{f}{p}\sqrt{-n}\right) + \mathfrak{f} \in U(R/\mathfrak{f}) \setminus U(\mathcal{O}/\mathfrak{f})$$

Zatem $\#\mathrm{Pic}(\mathcal{O}) \neq h_K$.

$\mathcal{O}$ maksymalny $\Leftrightarrow \#\mathrm{Pic}(\mathcal{O}) = h_K$

Przykład (cd)

(2) p jest liczbą pierwszą taką, że $p \mid n$ i $p \mid f$

$$\Rightarrow \left(1 + \frac{f}{p}\sqrt{-n}\right) + \mathfrak{f} \in U(R/\mathfrak{f}) \setminus U(\mathcal{O}/\mathfrak{f})$$

Zatem $\#\mathrm{Pic}(\mathcal{O}) \neq h_K$.

$\mathcal{O}$ maksymalny $\Leftrightarrow \#\mathrm{Pic}(\mathcal{O}) = h_K$

Dziękuję za uwagę!