FEJEZETEK A SZÁMELMÉLETBŐL ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

2021. május 11.

$\{x\} > \frac{1}{2} \Rightarrow t^3(x) = t^2(-x)$

ΑΛΜΝΤΡΗ. $\frac{1}{2} < x < 1$ $\quad x = [0; 1, a_2, \dots]$

$[x] = 0, \quad \{x\} = x, \quad t(x) = \frac{1}{x}$

$\left[\frac{1}{x}\right] = 1, \quad \left\{\frac{1}{x}\right\} = \frac{1}{x} - 1 = \frac{1-x}{x}, \quad t^2(x) = \frac{x}{1-x} \quad \left[\frac{x}{1-x}\right] = a_2$

$-x = [-1; a_2+1\,?, \dots]$

$[-x] = -1, \quad \{-x\} = -x+1, \quad t(-x) = \frac{1}{1-x}$

$t(-x) = t^2(x) + 1$

$\Downarrow$

$\{t(-x)\} = \{t^2(x)\}$

$\Downarrow$

$t^2(-x) = t^3(x)$

$\left[\frac{1}{1-x}\right] \overset{?}{=} a_2 + 1$

$\frac{x-1+1}{1-x} = -1 + \frac{1}{1-x} \qquad \frac{1}{1-x} = \frac{x}{1-x} + 1 \Rightarrow \left[\frac{1}{1-x}\right] = \left[\frac{x}{1-x}\right] + 1 = a_2 + 1$

Definíció

- $\alpha \in \mathbb{C}$ algebrai szám $\iff \exists f \in \mathbb{Q}[x], f \neq 0: \quad f(\alpha) = 0$

  $\iff \exists f \in \mathbb{Q}[x]$ főpolinom: $\quad f(\alpha) = 0$

  $\iff \exists f \in \mathbb{Z}[x], f \neq 0: \quad f(\alpha) = 0$

- $\alpha \in \mathbb{C}$ algebrai egész $\iff \exists f \in \mathbb{Z}[x]$ főpolinom: $\quad f(\alpha) = 0$

$\iff m_\alpha \in \mathbb{Z}[x]$

Emlék. $\nexists f \in \mathbb{Z}[x]$ főpol.: $f(\frac{1}{\sqrt{2}}) = 0$

HF 33

Példa

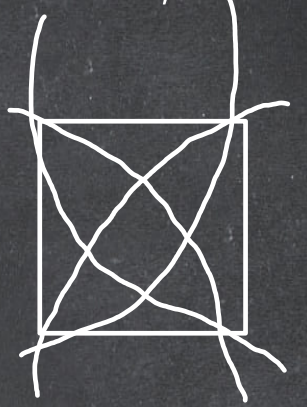
- $\sqrt{2}$ algebrai egész: $m_{\sqrt{2}} = x^2 - 2$
- $\frac{1}{\sqrt{2}}$ algebrai szám, de nem algebrai egész: $m_{\frac{1}{\sqrt{2}}} = x^2 - \frac{1}{2}$
- $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$ algebrai egész: $m_{\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}i} = x^4 + 1$

Tétel

α algebrai szám $\iff \alpha = \frac{\beta}{n}$, ahol β algebrai egész és $n \in \mathbb{N}$.

Definíció

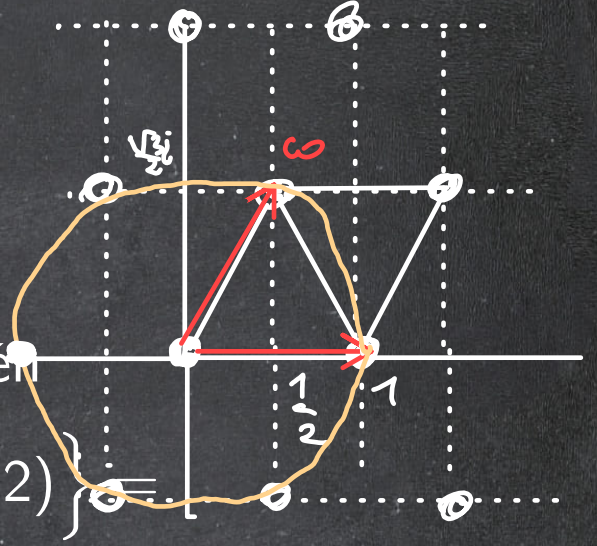
Algebrai számtesten $\mathbb{Q}$ végesfokú testbővítését értjük: $\mathbb{Q} \leq K \leq \mathbb{C}$, ahol $[K : \mathbb{Q}] < \infty$. A K-beli algebrai egészek gyűrűt alkotnak, ezt $\mathcal{O}_K$ jelöli.



Példák

- $K = \mathbb{Q}$ esetén $\mathcal{O}_K = \mathbb{Z}$

- $K = \mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ esetén
  $\mathcal{O}_K = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ (Gauss-egészek)



- $K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ esetén
  $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$

- $K = \mathbb{Q}(\sqrt{3}i) = \{a + b\sqrt{3}i : a, b \in \mathbb{Q}\}$ esetén
  $\mathcal{O}_K = \left\{\frac{a}{2} + \frac{b}{2}\sqrt{3}i : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\}$
  $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, ahol $\omega = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ (Euler-egészek)

Az $\mathcal{O}_K$ gyűrűkben lehet definiálni oszthatóságot, asszociáltságot, egységeket, legnagyobb közös osztót, irreducibilis és prím elemeket, de ezek sajnos nem mindig viselkednek olyan szépen, mint $\mathbb{Z}$-ben.

Például $K = \mathbb{Q}(\sqrt{-5})$ esetén $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$, és itt nincs bármely két elemnek legnagyobb közös osztója, az irreducibilis és a prím elemek nem ugyanazok, nincs minden elemnek egyértelmű irreducibilis faktorizációja.

Definíció

Az R gyűrű egységcsoportja: $R^* = \{a \in R : a \mid 1\} = \{a \in R : \exists a^{-1} \in R\}$.

Példák

- $K = \mathbb{Q}$ esetén $\mathcal{O}_K^* = \{1, -1\}$ (második egységgyökök)
- $K = \mathbb{Q}(i)$ esetén $\mathcal{O}_K^* = \{1, -1, i, -i\}$ (negyedik egységgyökök)
- $K = \mathbb{Q}(\sqrt{2})$ esetén $\mathcal{O}_K^* =$? (végtelen!)
- $K = \mathbb{Q}(\sqrt{3}i)$ esetén $\mathcal{O}_K^* = \left\{ \pm 1, \pm\frac{1}{2} \pm \frac{\sqrt{3}}{2} i \right\}$ (hatodik egységgyökök)

Definíció

Az $\alpha = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ elem konjugáltja $\overline{\alpha} = a - b\sqrt{2}$.

Tétel

Tetszőleges $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ esetén $\overline{\alpha \pm \beta} = \overline{\alpha} \pm \overline{\beta}$ és $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$.

Definíció

Az $\alpha = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ elem normája $N(\alpha) = \alpha\overline{\alpha} = a^2 - 2b^2 \in \mathbb{Z}$.

Tétel

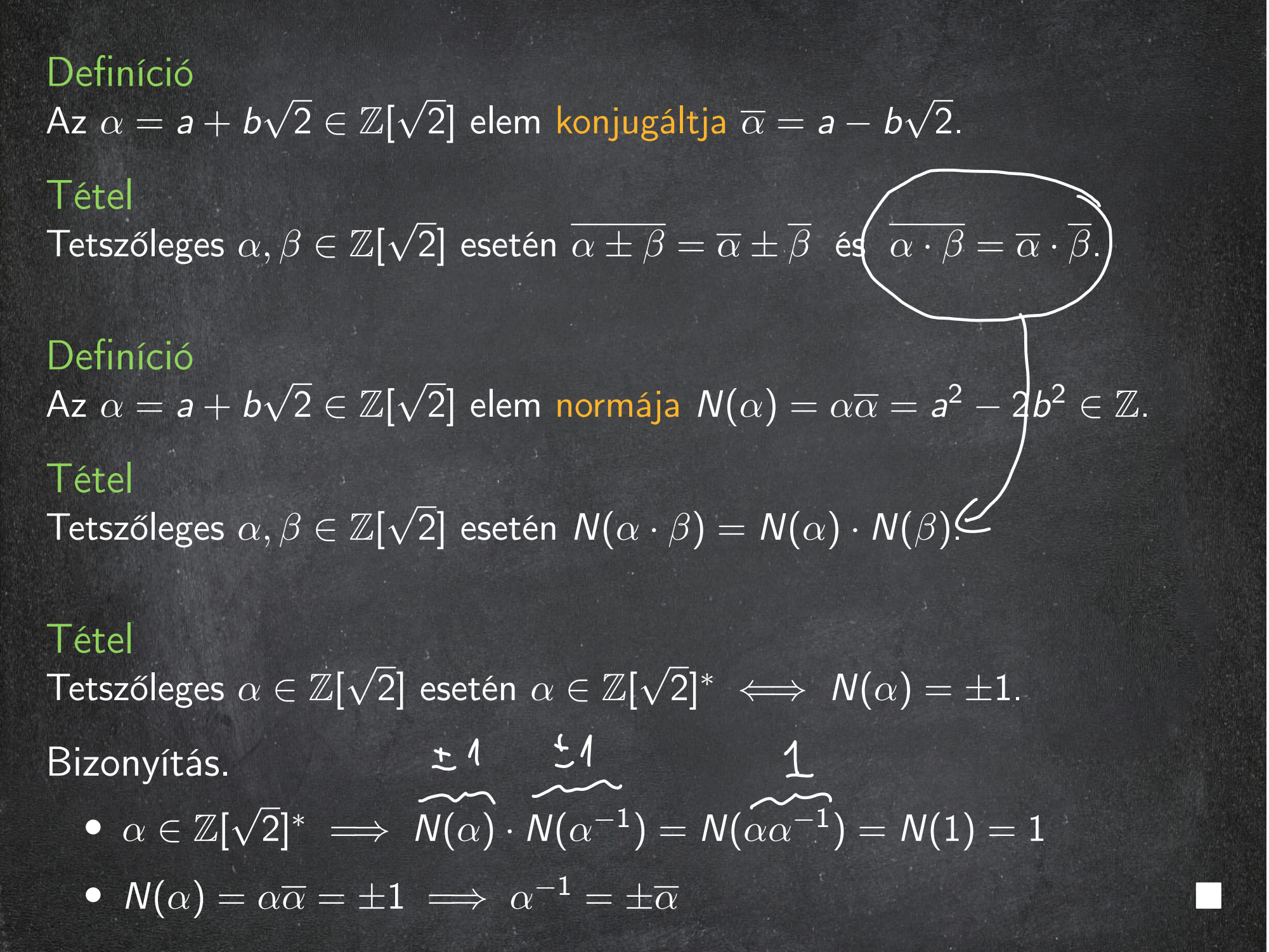
Tetszőleges $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ esetén $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

Tétel

Tetszőleges $\alpha \in \mathbb{Z}[\sqrt{2}]$ esetén $\alpha \in \mathbb{Z}[\sqrt{2}]^* \iff N(\alpha) = \pm 1$.

Bizonyítás.

- $\alpha \in \mathbb{Z}[\sqrt{2}]^* \implies \underbrace{N(\alpha)}_{\pm 1} \cdot \underbrace{N(\alpha^{-1})}_{\pm 1} = N(\underbrace{\alpha\alpha^{-1}}_{1}) = N(1) = 1$
- $N(\alpha) = \alpha\overline{\alpha} = \pm 1 \implies \alpha^{-1} = \pm\overline{\alpha}$



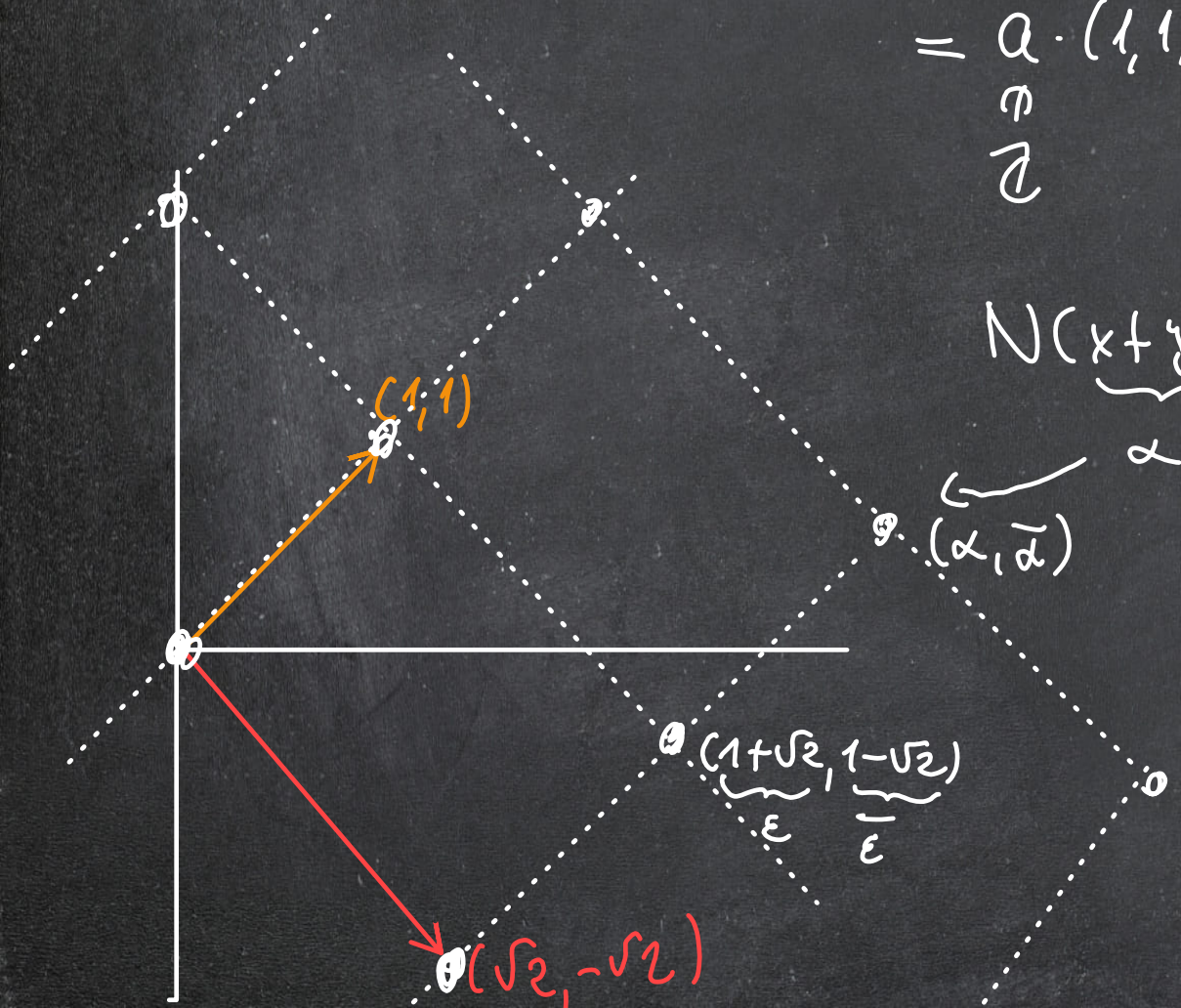
$\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ sim

$\alpha \rightsquigarrow (\alpha, \bar{\alpha}) \in \mathbb{R}^2$

$a+b\sqrt{2} \rightsquigarrow (a+b\sqrt{2}, a-b\sqrt{2}) = (a,a) + (b\sqrt{2}, -b\sqrt{2}) =$

$= \underset{\uparrow}{a} \cdot (1,1) + \underset{\uparrow}{b} \cdot (\sqrt{2}, -\sqrt{2})$

$\mathbb{Z} \qquad \mathbb{Z}$



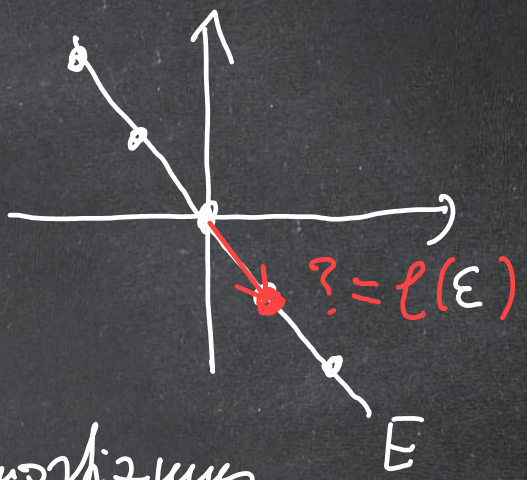
$N(\underbrace{x+y\sqrt{2}}_{\alpha}) = x^2 - 2y^2 =$

$= (\underbrace{x+\sqrt{2}y}_{\alpha}) \cdot (\underbrace{x-\sqrt{2}y}_{\bar{\alpha}}) = \pm 1$

$\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ $\quad \mathbb{R}\times\mathbb{R} \quad \mathbb{R}^+\times\mathbb{R}^+ \quad \mathbb{R}\times\mathbb{R}$

$\alpha \mapsto (\alpha, \bar{\alpha}) \mapsto (|\alpha|, |\bar{\alpha}|) \mapsto (\log|\alpha|, \log|\bar{\alpha}|) = \ell(\alpha)$

ℓ



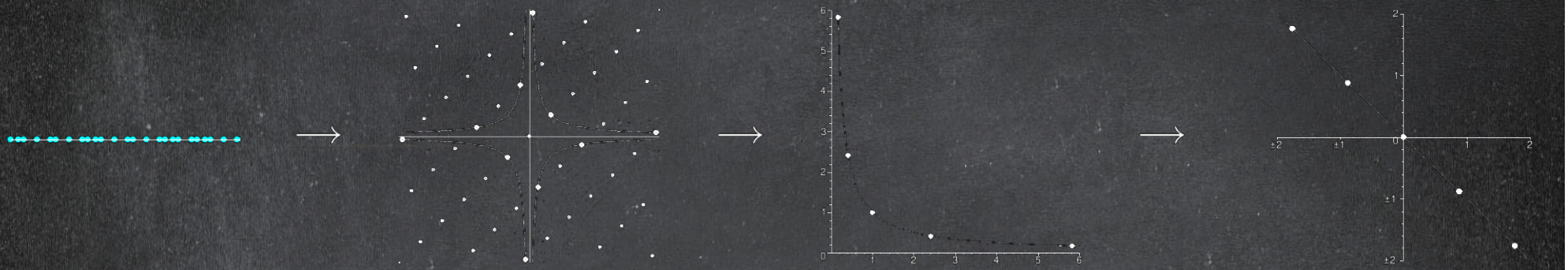
$\ell(\alpha\cdot\beta) = \ell(\alpha) + \ell(\beta)$

$(\mathbb{Z}[\sqrt{2}]; \cdot) \xrightarrow{\ell} (\mathbb{R}\times\mathbb{R}; +)$ homomorphism

$|N(\alpha)| = |\alpha|\cdot|\bar{\alpha}| = 1 \Leftrightarrow \log|\alpha| + \log|\bar{\alpha}| = \log 1 = 0$

$(\mathbb{Z}[\sqrt{2}]^*; \cdot) \xrightarrow{\ell} (E; +)$ $\qquad \ell(\mathbb{Z}[\sqrt{2}]^*) \leq E$

$(z\cdot t \pm r\alpha)$



$$\begin{array}{ccccccc} \mathbb{Z}[\sqrt{2}] & \to & \mathbb{R}\times\mathbb{R} & \to & \mathbb{R}^+\times\mathbb{R}^+ & \to & \mathbb{R}\times\mathbb{R} \\ \alpha & \mapsto & (\alpha,\overline{\alpha}) & \mapsto & (|\alpha|,|\overline{\alpha}|) & \mapsto & \underbrace{(\log|\alpha|,\log|\overline{\alpha}|)}_{\ell(\alpha)} \end{array}$$

$$\ell\colon \mathbb{Z}[\sqrt{2}] \to \mathbb{R}^2,\ \alpha \mapsto (\log|\alpha|,\log|\overline{\alpha}|)$$

$$\ell(\mathbb{Z}[\sqrt{2}]^*) = \{\ldots, -\ell(\varepsilon), 0, \ell(\varepsilon), 2\ell(\varepsilon), \ldots\} \cong C_\infty$$

$$\Rightarrow \mathbb{Z}[\sqrt{2}]^* = \{\pm\varepsilon^z \mid z \in \mathbb{Z}\} \cong C_2 \times C_\infty$$

$\varepsilon = 1+\sqrt{2}$ <u>fundamentális egység</u>

$$N(\varepsilon) = (1+\sqrt{2})(1-\sqrt{2}) = -1$$

$$\varepsilon^{-1} = -\bar{\varepsilon} = -1+\sqrt{2}$$

$$(1+\sqrt{2})^n = \underset{\in\mathbb{Z}}{x_n} + \underset{\in\mathbb{Z}}{y_n}\sqrt{2}$$

$$\mathbb{Z}[\sqrt{2}]^* = \{\pm(\pm 1+\sqrt{2})^n \mid n \in \mathbb{N}_0\} =$$

$$= \{\pm x_n \pm y_n\sqrt{2} \mid n \in \mathbb{N}_0\}$$

$\uparrow$ az $x^2 - 2y^2 = \pm 1$ Pell-egyenlet megoldáshalmaza

Tétel (Dirichlet)

Legyen $d > 1$ négyzetmentes természetes szám, és legyen (x_1, y_1) a legkisebb pozitív megoldása az $x^2 - dy^2 = \pm 1$ egyenlet(ek)nek.

Legyen $\varepsilon = x_1 + y_1\sqrt{d}$ (fundamentális egység), és legyen $\varepsilon^n = x_n + y_n\sqrt{d}$. Ekkor a $\mathbb{Z}[\sqrt{d}]$ gyűrű egységcsoportja

$$\mathbb{Z}[\sqrt{d}]^* = \{ \pm \varepsilon^k : k \in \mathbb{Z} \}.$$

Következmény

1. Ha $N(\varepsilon) = 1$, akkor
   - a pozitív Pell-egyenlet összes megoldása $(\pm x_n, \pm y_n)$, ahol $n \in \mathbb{N}_0$;
   - a negatív Pell-egyenletnek nincs megoldása.

2. Ha $N(\varepsilon) = -1$, akkor
   - a pozitív Pell-egyenlet összes megoldása $(\pm x_n, \pm y_n)$, ahol $n \in \mathbb{N}_0$ ps;
   - a negatív Pell-egyenlet összes megoldása $(\pm x_n, \pm y_n)$, ahol $n \in \mathbb{N}_0$ ptl.

TÉTEL Ha $(x,y)\in\mathbb{N}^2$ megoldása az $x^2-dy^2=\pm 1$ egyenletnek, akkor $\frac{x}{y}$ szerepel $\sqrt{d}$ lehetőségek konvergensei közötti.

Biz. Tfh. $x^2-dy^2=\pm 1$

$$(x-\sqrt{d}y)(x+\sqrt{d}y)=\pm 1$$

$$|x-\sqrt{d}y|\cdot|x+\sqrt{d}y|=1 \qquad /:y^2$$

$$\left|\frac{x}{y}-\sqrt{d}\right|\cdot\left|\frac{x}{y}+\sqrt{d}\right|=\frac{1}{y^2}$$

$$\left|\frac{x}{y}-\sqrt{d}\right|=\frac{1}{\left|\frac{x}{y}+\sqrt{d}\right|\cdot y^2}<\frac{1}{2y^2}$$

$\left|\frac{x}{y}+\sqrt{d}\right|$: $\frac{1}{1}$ $\to 2$

$\Rightarrow \frac{x}{y}\approx\sqrt{d}$ jobb közelítés

$\Rightarrow$ megy a konvergensek között ∎

PELL $x^2 - 2y^2 = \pm 1$ $\quad \sqrt{2} = [1; 2, 2, \dots]$

$$[a_0; a_1, \dots, a_n] = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \dots \cdot \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \cdot \infty$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \frac{ax+b}{cx+d} \cdot \infty = \frac{a}{c}$$

$$x_{n+1} = 2x_n + x_{n-1}$$

$$y_{n+1} = 2y_n + y_{n-1}$$

	$\begin{matrix}2 & 1\\ 1 & 0\end{matrix}$	$\begin{matrix}2 & 1\\ 1 & 0\end{matrix}$	$\begin{matrix}2 & 1\\ 1 & 0\end{matrix}$	…		
$\begin{matrix}1 & 1\\ 1 & 0\end{matrix}$	$\begin{matrix}3 & 1\\ 2 & 1\end{matrix}$	$\begin{matrix}7 & 3\\ 5 & 2\end{matrix}$	$\begin{matrix}17 & 7\\ 12 & 5\end{matrix}$	…	$\begin{matrix}p_n & p_{n-1}\\ q_n & q_{n-1}\end{matrix}$	

	x_0	x_1	x_2	x_3	x_4	
p_n	1	1	3	7	17	…
q_n	y_0 0	y_1 1	y_2 2	y_3 5	y_4 12	…
$p_n^2 - 2q_n^2$	1	−1	1	−1	1	…

$$x_n + y_n\sqrt{2} = (x_1 + y_1\sqrt{2})^n = (1+\sqrt{2})^n$$

$$(1+\sqrt{2})^2 = 1 + 2\sqrt{2} + 2 = \underset{\parallel}{3} + \underset{\parallel}{2}\sqrt{2}$$

$$x_2 \quad y_2$$

PÉLDA $x^2 - 14y^2 = \pm 1$ $\quad \sqrt{14} = [3; \overline{1, 2, 1, 6}]$

	1 1	2 1	1 1	6 1	1 1	2 1	...
	1 0	1 0	1 0	1 0	1 0	1 0	
3 1	4 3	11 4	15 11	101 15	116 101	333 116	..
1 0	1 1	3 1	4 3	27 4	31 27	89 31	

p_n	3	4	11	15	101	116	333	449	...
q_n	1	1	3	4	27	31	89	120	..
$p_n^2 - 14q_n^2$	-5	2	-5	1	-5	2	-5	1	

$x_1 = 15,\ y_1 = 4 \quad \varepsilon = 15 + 4\sqrt{14}$

$x_2 = 449,\ y_2 = 120 \quad (15 + 4\sqrt{14})^2 = 449 + 120\sqrt{14} \ \dots$

HF 35 $x^2 - 13y^2 = \pm 1$

$(x_1, y_1) = ?$

$(x_2, y_2) = ?$