<u>Tétel</u> $(a_i)_{i\in I} \subset \mathbb{Q}^\times$, $(\varepsilon_{i,v})_{i\in I, v\in V} = \pm 1$

(véges)

$\exists\, x \in \mathbb{Q}^\times : (a_i, x)_v = \varepsilon_{i,v}$ acsa.

(1) véges sok kivétellel $\varepsilon_{i,v} = 1$

(2) $\forall i \in I \ \prod_v \varepsilon_{i,v} = 1$

(3) $\forall v \in V \ \exists\, x_v \in \mathbb{Q}_v^\times : (a_i, x_v)_v = \varepsilon_{i,v} \ \forall i \in I$.

<u>Biz.:</u> $S := \{\infty, 2\} \cup \{a_i\text{-k prímosztói}\} \subset V$ ✓

a_i négyzetmentes

$T := \{v \in V \mid \exists i \ \varepsilon_{i,v} = -1\}$. $S \cap T = \emptyset$ ✓

Ált. eset: $S \cap T \neq \emptyset$

először $x' \in \mathbb{Q}^\times$: $\quad (a_i, x')_v = \varepsilon_{i,v} \quad \forall v \in S.$

$$x = y x' \Rightarrow (a_i, x)_v = \underbrace{(a_i, y)_v}_{\substack{\parallel \\ 1}} \underbrace{(a_i, x')_v}_{\varepsilon_{i,v} \quad v \in S}$$

$w \notin S$ / $w \in S$

$$(a_i, y)_w = \varepsilon_{i,w} \cdot (a_i, x')_w = \eta_{i,w}$$

$\eta_{i,w}$-re feltételek:

(1): kivétel: $\varepsilon_{i,w} = -1$ vagy $(a_i, x')_w = -1$

(2) $\forall i \in I \qquad \prod \eta_{i,w} = \prod \varepsilon_{i,w} \cdot \prod (a_i, x')_w = 1 \cdot 1 = 1$ ✓

(3) $v \in V \quad y_v := x' \cdot x_v$ jó: $(a_i, y_v)_v = \underbrace{(a_i, x')_v}_{} \cdot \underbrace{(a_i, x_v)_v}_{\varepsilon_{i,v}} = \eta_{i,v}$

x' konstrukciója:

$\forall\, v \in S \quad x_v \in \mathbb{Q}_v^\times \quad (a_i, x_v) = \varepsilon_{i,v}$

kell: $x' \in \mathbb{Q}^\times \qquad \dfrac{x'}{x_v} \in \left(\mathbb{Q}_v^\times\right)^2$

$$x' \in \underbrace{x_v \cdot \left(\mathbb{Q}_v^\times\right)^2}_{} \quad \text{nyílt.}$$

Approx. lemma: $\exists\, x' \in \mathbb{Q}^\times$. $\quad 1 + p\mathbb{Z}_p, \quad 1 + 8\mathbb{Z}_2$

$\square$

Általában szv. alakról:

Def.: β: szimm. bilin. fv. $K^n \times K^n \to K \longleftrightarrow q: K^n \to K$

$q(v) = \beta(v,v)$.

$\mathrm{char}(K) \neq 2$. **izotróp**, ha $\exists\, v \neq 0$, $v \in K^n$: $\beta(v,v) = 0$.

β nemelfajuló: $\forall\, 0 \neq v \in K^n\ \exists\, w \in K^n: \beta(v,w) \neq 0$.

$\Longleftrightarrow \det[\beta] \neq 0$.

Lemma Tfh. β nemelfajuló, izotróp. $\Rightarrow \forall a \in K$ $\exists\, v_0 \in K^n: \beta(v_0, v_0) = a$. (mindent előáll)

$\mathrm{char}(K) \neq 2$.

Biz.: $\exists\, 0 \neq v \in K^n$ $\beta(v,v) = 0$. $\exists\, w \in K^n$.

$\beta(v,w) \neq 0$. $\beta(cv + w, cv + w) =$

$v_0 = cv + w$

$c \in K$

$= \cancel{c^2 \beta(v,v)} + 2c \underbrace{\beta(v,w)}_{\neq 0} + \beta(w,w)$

megválasztható:

$$c = \frac{a - \beta(w,w)}{2\beta(v,w)} \qquad \square$$

Áll.: $f(x_1, \dots, x_n)$ (nemelfajuló) $\forall$ ev. alak előállítja $a \in K - 0$

$\Leftrightarrow f(x_1, \dots, x_n) - ay^2$ izotróp.

Biz.: $\boxed{\Rightarrow}$ $f(x_1, \dots, x_n) = a$ $y = 1$. mutatja, hogy van izotróp vektor.

$\boxed{\Leftarrow}$

$$f(x_1, \dots, x_n) - ay^2 = 0$$ $y \neq 0$

$\Rightarrow$ leosztunk, f előállítja a-t.

$y = 0 \Rightarrow f$ izotróp $\overset{\text{Lemma}}{\Rightarrow}$ a-t előállítja

$\square$

Tétel (Hasse-Minkowski) $f \in \mathbb{Q}[x_1, \dots, x_n]$ hom. 2-fokú polinom. f-nek van nemtriviális zérushelye $\mathbb{Q}$ fölött $\iff$ f-nek $\exists$ nemtrivi zérushelye $\mathbb{R}$ fölött és $\mathbb{Q}_p$ fölött $\forall p$ prímre.

Biz.: $\boxed{\Rightarrow}$ ✓

$\boxed{\Leftarrow}$ f nemelfajuló Gram-Schmidt

$\rightsquigarrow f(x_1, \dots, x_n) = a_1 x_1^2 + \dots + a_n x_n^2$ $a_i \in \mathbb{Z}$ négyzetmentes.

(1) $n=2$ $\quad f(x,y) = x^2 - ay^2$ $\quad a<0 \Rightarrow \mathbb{R}$ fölött nincs!

$a>0$.

$\mathbb{Q}_p$-ben? $\quad x_p, y_p \neq 0$ $\in \mathbb{Q}_p^\times$

$x_p^2 = a\, y_p^2$

$v_p(a)$ ps $\Rightarrow a = b^2$.

$b \in \mathbb{Q}^\times$.

$x=b,\ y=1$ ✓.

(2) $n=3$ $\quad f(x_1,x_2,x_3) = x_1^2 - a x_2^2 - b x_3^2$ $\quad a,b \in \mathbb{Z}$ négyzetmentes.

$a,b<0$ $\mathbb{R}$-ben nincs.

$a>0>b \Rightarrow$ hasonlóan b-vel ...

feltehetjük, hogy $a, b > 0$. $|a| \leq |b|$.

Indukció $m = |a| + |b|$ - re.

$m = 2$ $x_1^2 - x_2^2 - x_3^2$ $x_3 = 0$, $x_1 = x_2 = 1$ ✓.

$m > 2 \Rightarrow |b| \geq 2$ $b = p_1 \cdot \ldots \cdot p_r$.

<u>Áll</u>: $x^2 \equiv a \ (p_i)$ $i = 1, \ldots, r$ megoldható ($\left(\frac{a}{p_i}\right) = 1 \vee 0$)

<u>Biz.</u>: $p_i | a$ ✓ $p_i \nmid a$. $\Leftrightarrow x_1^2 - a x_2^2 - b x_3^2 = 0$ $\exists$ primitív mo.-a $\mathbb{Z}_{p_i}$-ben.

$(a, b)_p = 1 \Rightarrow p \nmid b \Rightarrow \left(\frac{a}{p}\right) = 1.$ $p_i | b \Rightarrow p_i | x_1^2 - a x_2^2$

$\square$

rínai maradéktétel $\Rightarrow$ $\exists\, t: \quad t^2 \equiv a \ (b)$

$$t^2 = a + b \cdot b' \qquad |t| \le \frac{|b|}{2}.$$

$$\Rightarrow \quad b' < b. \qquad t^2 - 1^2 a - 1^2 \cdot b b' = 0$$

$$(a, bb')_p = 1 \qquad \forall\, p \text{ prímre és } p = \infty\text{-re}.$$

$$\Updownarrow \qquad x^2 - a y^2 - b z^2 = 0 \text{ megoldható}$$

lokálisan $\mathbb{Q}_p$-ben

$$(a, b')_p = 1 \Leftarrow (a, b)_p = 1$$

$$|a| + |b'| < |a| + |b| = m$$

$\Rightarrow$ indukció $\quad \exists\, x_1, x_2, x_3 \in \mathbb{Q}$ nem mind 0

$$x_1^2 - a x_2^2 - b' x_3^2 = 0.$$

$$t^2 - a\cdot 1^2 - b b'\cdot 1^2 = 0$$

$bb' \in \mathbb{Q}(\sqrt{a})$-beli elem normája

(3) $n = 4$.

$$f = \underbrace{a x_1^2 + b x_2^2}_{u} - c x_3^2 - d x_4^2$$

b' is $\Rightarrow b$ is. ✓

$X_v \in \mathbb{Q}_v^\times$ $\quad ax^2+by^2$ előállítja X_v-t

$\Longleftrightarrow \quad ax^2+by^2-X_v z^2=0$ van nemtriviális mo.-a

$\Longleftrightarrow \quad \frac{a}{X_v}\cdot x^2+\frac{b}{X_v}\cdot y^2-z^2=0$

$(u,w)=(u,-uw)$

$\Longleftrightarrow \quad \left(\frac{a}{X_v},\frac{b}{X_v}\right)_v=1.$

$(u,-u)=1$

$\parallel$

$(aX_v, bX_v)_v=\left(aX_v,-abX_v^2\right)_v=(aX_v,-ab)_v=(a,-ab)_v$

$(X_v,-ab)_v=$

$=\underline{(a,b)_v}\,\underline{(X_v,-ab)_v}.$

$\forall v \in V$-re $\exists$ közös értér + ha a 0 a közös

Lemma

$\Rightarrow$ $\exists \neq 0$ közös értér: $x_v \in \mathbb{Q}_v^{\times}$.

$$(x_v, -ab)_v = (a, b)_v \quad , \quad (x_v, -cd)_v = (c, d)_v .$$

Kell: $x \in \mathbb{Q}^{\times}$: $(x, -ab)_v = (a, b)_v$ és

$(x, -cd)_v = (c, d)_v$

(1), (2), (3) illesztési tételben.

$n = 3$ esét $|I| = 2$.

teljesül $\Rightarrow \exists\, x \in \mathbb{Q}^{\times}$

$\Rightarrow$ x globálisan is közös értér.

(4) $n \geq 5$ indukció n-re

$$f = \underbrace{\left(a_1 x_1^2 + a_2 x_2^2\right)}_{h} - \underbrace{\left(-a_3 x_3^2 - \dots - a_n x_n^2\right)}_{g}$$

$a_1, \dots, a_n \in \mathbb{Z}$ négyzetmentes.

$$S := \{\infty, 2\} \cup \underbrace{\{p \in V \mid \exists i \geq 3 : p \mid a_i\}}_{\text{véges}}.$$

$\forall v \in V$ és $\exists a_v \in \mathbb{Q}_v$ a_v közös értéke h-nak és g-nek.

$\exists x_i^v \in \mathbb{Q}_v$: $h(x_1^v, x_2^v) = a_v$

$g(x_3^v, \dots, x_n^v) = a_v$.

$\underset{\text{approximáció}}{\Longrightarrow}$ $\exists\ a \in \mathbb{Q}^\times : \frac{a}{a_v} \in (\mathbb{Q}_v^\times)^2 \ \forall v \in S.$

$a = h(x_1, x_2)$ megoldható $(n=3)$

$h(x_1^v, x_2^v) = a_v$ $\exists\ \underset{x_1^v \in}{U_1^v}, \underset{x_2^v \in}{U_2^v}$ nyílt;

$h(U_1^v, U_2^v) \in a_v (\mathbb{Q}_v^\times)^2$ $\exists\ x_1 \in \mathbb{Q}^\times$

$x_1 \in U_1^v$, $\exists\ x_2 \in \mathbb{Q}^\times$

$x_2 \in U_2^v$

$\forall v \in S.$

$y \in \mathbb{Q}^\times$ x_1 $a := h(x_1, x_2)$ jó.

$a \in a_v (\mathbb{Q}_v^\times)^2 \ \forall v \in S.$

$\Rightarrow$ a-t előállítja g lokálisan a $v \in S$ helyen $\forall v \in S$-re, mert a_v-t előállítja.

$\Rightarrow$ $v \notin S \Rightarrow a_3, \dots, a_n \in \mathbb{Z}_v^\times$

$n \geq 5 \Rightarrow n-2 \geq 3$

a-t előállítja g a v helyen is

$n-1$ Hasse-Minkowski $\Rightarrow$ a-t előállítja g $\mathbb{Q}$ fölött is.

$\Rightarrow$ a közös értékre h-val és g-vel. $\square$

Analitikus számelmélet.

$$n^s = e^{s \cdot \log n}$$

$$e^z = 1 + z + \frac{z^2}{2} + \dots$$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \mathrm{Re}(s) > 1 \text{ konvergál.}$$

$$e^{s \log n} = e^{\mathrm{Re}\, s \cdot \log n + i\, \mathrm{Im}(s) \log n}$$

$$(a_n)_{n \geq 1} \Rightarrow \sum_{n=1}^{\infty} \frac{a_n}{n^s} \to \text{Dirichlet-sor.}$$

$$|e^{ix}| = 1 \qquad x \in \mathbb{R}.$$

$$e^{ix} = \cos x + i \sin x$$

$$e^{ix} = 1 + ix + \frac{i^2 x^2}{2} + \dots + \frac{(ix)^n}{n!} + \dots$$

$$\cos x = 1 - \frac{x^2}{2} + \frac{x^4}{4!} - \dots$$

$$\Rightarrow |n^s| = n^{Re(s)}$$

μ

$$f(z) = \int_0^\infty e^{-zt} \mu(t)$$

Laplace

$\mu_a(t)$

$$a_1, a_2, \dots, a_n, \dots$$

$$e^{-s\cdot\log n} = n^{-s} = \frac{1}{n^s}$$

$\log n$

$$\sum \frac{a_n}{n^s} = \int_0^\infty e^{-st} \mu_a(t)$$