$$(1 - d\alpha_1\alpha_2\beta_1\beta_2)(\alpha_1\alpha_2 - \beta_1\beta_2)$$

$$= (\alpha_1\beta_2 - \alpha_2\beta_1)(\alpha_2\beta_2 - a\alpha_1\beta_1)$$

$$a\alpha_1^2 + \alpha_2^2 = 1 + d\alpha_1^2\alpha_2^2 \qquad a\beta_1^2 + \beta_2^2 = 1 + d\beta_1^2\beta_2^2$$

$$\alpha_1\alpha_2 - \beta_1\beta_2 - d\alpha_1^2\alpha_2^2\beta_1\beta_2 + d\alpha_1\alpha_2\beta_1^2\beta_2^2 =$$

$$= \alpha_1\alpha_2(1 + d\beta_1^2\beta_2^2) - \beta_1\beta_2(1 + d\alpha_1^2\alpha_2^2)$$

$$\alpha_1\alpha_2\beta_2^2 - a\alpha_1^2\beta_1\beta_2 - \alpha_2^2\beta_1\beta_2 + a\alpha_1\beta_1^2\alpha_2$$

$$= \alpha_1\alpha_2(a\beta_1^2 + \beta_2^2) - \beta_1\beta_2(a\alpha_1^2 + \alpha_2^2)$$

$$(1+d\alpha_1\alpha_2\beta_1\beta_2)(\alpha_1\alpha_2+\beta_1\beta_2)$$

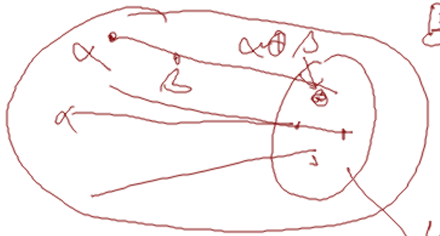
$$=(\alpha_2\beta_2+a\alpha_1\beta_1)(\alpha_1\beta_2+\alpha_2\beta_1)$$

$$\alpha_1\alpha_2(1+d\beta_1^2\beta_2^2)+\beta_1\beta_2(1+d\alpha_1^2\alpha_2^2)$$

$$=\alpha_1\alpha_2(a\beta_1^2+\beta_2^2)+\beta_1\beta_2(a\alpha_1^2+\alpha_2^2)$$

$$\alpha_1\alpha_2\beta_2^2+\beta_1\beta_2\alpha_2^2+a\alpha_1^2\beta_1\beta_2+a\alpha_1\beta_1^2\alpha_2$$

d ad nečtverec
vzorec vůbec funguje



BODY GRUPY

LHS = 0

$(1-d\ldots)(\quad)$

$=(\alpha_1\beta_2-\alpha_2\beta_1)$

$(\alpha_2\beta_2-a\alpha_1\beta_1)$

mohou a nemohou existovat α_1^2

$$1-d\alpha_1\alpha_2\beta_1\beta_2=0$$

$\alpha_1\beta_2=\alpha_2\beta_1$

$\alpha_2\beta_2=a\alpha_1\beta_1.$

$\cancel{1}=d\alpha_1\alpha_2\beta_1\beta_2=d\alpha_1^2\beta_2^2$

ROVNO MŮŽE PLATIT
JENOM KDYŽ d ČTVERCE

$da\alpha_1^2\beta_1^2$ da čtverec

$$1+d\alpha_1\alpha_2\beta_1\beta_2=0$$

$\alpha_2\beta_2=-a\alpha_1\beta_1$

$\alpha_1\beta_2=-\alpha_2\beta_1$ $\quad 1=-d\alpha_1\alpha_2\beta_1\beta_2$

$da\alpha_1^2\beta_1^2$

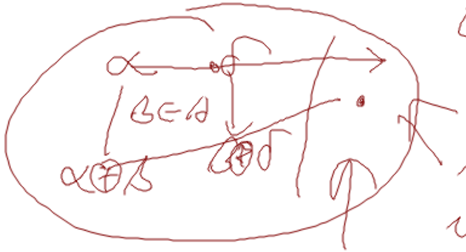
$d\alpha_1^2\beta_2^2$

POKUD d, a nejsou čtverce, tak vůbec nejsou
afinní body možné
kromě základního vzorce.

Edwardsova křivka

$A = \{(0,1),(1,0),(0,-1),(-1,0)\}$

kde je $\cong \mathbb{Z}_4$



EDW

body grupy v nekonečnu

pokud je γ bod v ∞

tak ∀ β∈A je β⊕γ opět bod v ∞

body v ∞ řád nekonečna

nebo základová třída grupy A

jejich počet je tedy řád 0 nebo 4

$\alpha_2^2 \; \alpha_1^2$ 4 SITUACE $\alpha_1^2 \alpha_2^2 \beta_1^2 \beta_2^2 = 1/d^2$

$\alpha_1^2 \beta_2^2 = \alpha_2^2 \beta_1^2$ $\alpha_2^2 \beta_2^2 = \alpha_1^2 \beta_1^2$

ROVNICE S $\alpha_2^2 \beta_2^2$ může platit obě situace

NEBO 2 NÁ IZOLOVANÉ ROZLIŠITÉ BODY

$(\alpha_1, \alpha_2)(\beta_1, -\beta_2)$

$$d\alpha_1\alpha_2\beta_1\beta_2 = 1 \qquad \alpha_1\beta_2 = \alpha_2\beta_1 \qquad \alpha_1/\beta_1 = \alpha_2/\beta_2$$

$$d\alpha_1^2 \cdot \beta_2^2 = 1 :$$

$1 + d\alpha_1^2\alpha_2^2 = a\alpha_1^2 + \alpha_2^2$ Bre Ƒ $1 + 1/\beta_2^2 = a\alpha_1^2 + \alpha_2^2$

$1 + 1/\alpha_2^2 = a\beta_1^2 + \beta_2^2$

$$\left.\begin{aligned} d\alpha_1^2\alpha_2^2 &= a\alpha_1^2 + \alpha_2^2 - 1 \\ d\beta_1^2\beta_2^2 &= a\beta_1^2 + \beta_2^2 - 1 \end{aligned}\right\} \quad 1 = (a\alpha_1^2 + \alpha_2^2 - 1)(a\beta_1^2 + \beta_2^2 - 1)$$

$$0 = a^2\alpha_1^2\beta_1^2 + \alpha_2^2\beta_2^2 + 2a/d \cancel{=} (a\alpha_1^2 + \alpha_2^2 + a\beta_1^2 + \beta_2^2)$$

$$2 + 1/\alpha_2^2 + 1/\beta_2^2$$

$$0 = (a/d)^2 + \alpha_2^4\beta_2^4 + 2(a/d)\alpha_2^2\beta_2^2 - 2\alpha_2^2\beta_2^2 + \alpha_2^2 + \beta_2^2$$

$$0 = (a/d)^2 + x^2y^2 + 2(a/d - 1)xy + x + y \qquad x = \alpha_2^2 \quad y = \beta_2^2$$

KVADRATICKO ROVNICI $\beta_2^2 < \alpha_2^2$