$P\oplus Q$ je definováno ~~tak~~, že $\underline{[P+Q] = [P\oplus Q + O]}$

$$[P-O]+[Q-O] = [P+Q-2O] = [P\oplus Q - O]$$

$\mathrm{Div}^{(1)}(E)$ je podgrupa $\mathrm{Div}(E)$ ~~ra~~ nad místy stupně 1

$$\deg : \mathrm{Div}^{(1)}(E) \longrightarrow \mathbb{Z} \qquad \deg\left(\sum a_i P_i\right) = \sum a_i$$

$$\mathrm{sum} : \mathrm{Div}^{(1)}(E) \longrightarrow \mathbb{Z} \qquad \mathrm{sum}\left(\sum a_i P_i\right) = \bigoplus [a_i] P_i$$

$[P - Q] = [P\ominus Q - O]$ homomorfismus?

$\Uparrow$

$[Q + (P\ominus Q)] = [P + O]$

PLATÍ

$$\mathrm{sum}\left(\sum a_i P_i + \sum b_i P_i\right) =$$
$$= \mathrm{sum}\left(\sum (a_i+b_i) P_i\right) = \bigoplus [a_i+b_i] P_i$$
$$= \bigoplus \left([a_i] P_i \oplus [b_i] P_i\right) = \mathrm{sum}\left(\sum a_i P_i\right) \oplus \mathrm{sum}\left(\sum b_i P_i\right)$$

Když v divisoru A nahradíš $P+Q \to P \oplus Q + O$

$P-Q \to P \ominus Q - O$

tak se nezmění ani $\deg(A)$ ani $\mathrm{sum}(A)$

Iterací takových náhrad dostaneme

$P - \ell O \quad P \neq O$

$-P - \ell O \quad$ NIKDY

$\ell \in \mathbb{Z} \qquad \ell O \qquad \ell = 0$

A je hlavní pokud se nahradí takto hlavní

$P \oplus Q + O - P - Q$ hlavní

$\mathrm{sum}(P - \ell O) = P$

$\mathrm{sum}(-P - \ell O) = \ominus P \neq O$

$\deg(\ell O) = \ell$

divisor $A \in \mathrm{Div}^{0}(E/K)$ je hlavní $\iff \mathrm{sum}(A) = O$, $\deg(A) = 0$

$K(E)$

$O \to \mathbb{Z}$

Základní pojmy, se kterými se pracuje

$K(E)$ funkční těleso $\qquad E(K)$ je grupa

$E[n]$

$\mathrm{End}(E)$ endomorfismy E

isogenie $\sigma : E \to E$ je možno chápat jako $\sigma^* : K(E) \to K(E)$

$$\sigma^*(\tau) = \tau\sigma$$

σ^* převádí místo z $K(E)$ na místo $\mathrm{Im}(\sigma^*)$

$\mathrm{Im}(\sigma^*)$ je alg. (·) těleso obsažené v $K(E)$

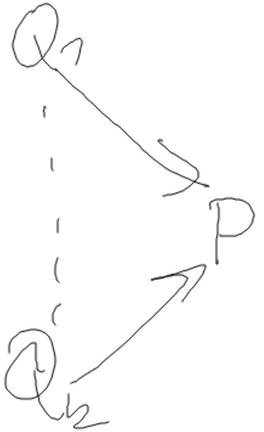
$$Q \supseteq \sigma^*(P) \iff \sigma(Q) = P$$

st 1 $\qquad$ st 1

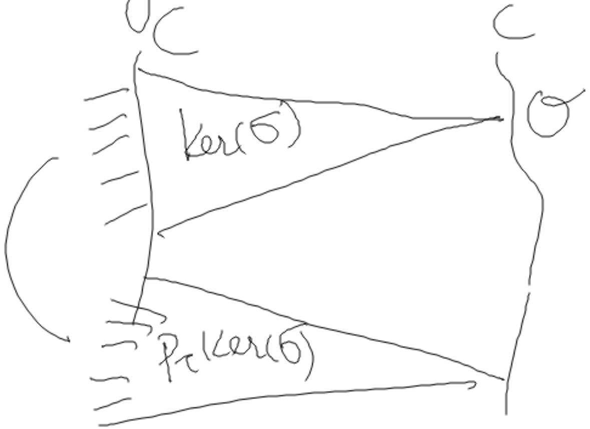
identifikovat body

$$e_\sigma(P) = e(\sigma) \qquad \sum_{\sigma(Q)=P} Q$$

stupeň neseparability $= 1$



σ je surjektívny endomorfizmus $E(\bar{K})$



$\sigma = [m]$ $\quad char(K) \nmid m$

m prevratiteľné $\quad Con([m]) = Con[m]$

$P \in E[m]$ $\exists$ presne m^2 bodov $P' \in E[m^2]$ $\cong \mathbb{Z}_{m^2} \times \mathbb{Z}_{m^2}$

$[m]P' = P$ $\qquad |E[m]| = m^2$

$$Con([m])(P - O) = \sum_{Q \in E[m]} (P' \oplus Q - Q)$$

$mP - mO$ hlavný

$Con[m](P - Q)$ tiež hlavný

$sum(mP) = [m]P = O$

$sum(P' \oplus Q - Q)$

$= P' \oplus Q \ominus Q = P'$

Q prebieha $E[m^2]$ $\quad sum(Con[m]) = [m^2]P' = O$

$mP - mO$ linear $= \mathrm{div}(r_p)$

$\mathrm{Car}[m](P-O)$ linear $= \mathrm{div}(\Delta_p)$

$$\mathrm{div}(\Delta_p^m) = \mathrm{div}\big(\underbrace{[m]^*(r_p)}_{r_p \circ [m]}\big)$$

$$\mathrm{div}([m]^*(r_p)) = \mathrm{Car}([m])(\mathrm{div}(r_p))$$

$$= \mathrm{Car}[m](mP - mO) = m\,\mathrm{Car}[m](P-Q) = m\,\mathrm{div}(s_p)$$

$$= \mathrm{div}(s_p^m)$$

$$\Delta_p^m = [m^*](r_p)$$

Obecně platí

$$\mathrm{div}(\sigma^*(z)) =$$

$$\mathrm{div}(z \circ \sigma) =$$

$$\mathrm{Car}(\sigma)(\mathrm{div}[z])$$

Lemma Ať $S,T \in E[m]$. Pak $\mathrm{div}(\Delta_T) = \mathrm{div}(\tau_S^*(\Delta_T))$ $\quad // \; S_T \circ \tau_S$

$\tau_S : R \to R \oplus S$ mapa $E \to E$

$$\mathrm{div}(\tau_S^*(S_T)) = \mathrm{Cau}(\tau_S)(\mathrm{div}(S_T)) =$$

$$= \mathrm{Cau}(\tau_S)\Big(\sum_{Q \in E[m]} ((T \oplus Q) - Q)\Big)$$

$$= \sum_Q \big((T \oplus Q \ominus S) - (Q \ominus S)\big) = \sum \big((T \oplus Q) - Q\big) = \mathrm{div}(S_T)$$

$$\boxed{\tau_S^*(\Delta_T)/\Delta_T \in K^*} \qquad e_m(S,T) = \frac{\tau_S^*(\Delta_T)}{\Delta_T}$$

$\in \mu_m$ tedy m-té odmocniny z jedné

Chiave dorata $\quad e_m(S,T)$ $\quad \boxed{\Delta_0 = 1}$ $\quad K^*$

$T=O$

$$\left(\frac{\tau_S^*(\Delta_T)}{S_T}\right)^m = 1 \qquad (\tau_S^*(\Delta_T))^m = \Delta_T^m$$

$$\Delta_T^m = [m]^* r_T = r_T \circ [m] = \underbrace{r_T \circ [m]}_{S_T^m = [m]^*(r_T)} \circ \tau_S = \Delta_T^m \circ \tau_S = \tau_S^*(\Delta_T^m)$$

$$[m] \circ \tau_S = [m]$$

$S \in E[m]$

$$P \xrightarrow{[m]} [m]P$$

$$P \downarrow P \oplus S$$

$$[m](P \oplus S) = [m]P \oplus \underbrace{[m]S}_{O} = [m]P$$

$$e_m(S,T) = \frac{\tau^*_S(\Delta_T)}{\Delta_T} \qquad \tau^*_0 = \mathrm{id}$$

$$\tau^*_T(\Delta_0) = \tau^*_T(1) = 1$$

$$e_m(0,T) = e_m(T,0) = 1$$

$$[m]T' = T$$

$$e_m(T,1) = 1$$

$$G = \Delta_T \cdot \tau^*_{T'}(\Delta_T) \cdot \tau^*_{[2]T'}(\Delta_T) \cdots \tau^*_{[m-1]T'}(\Delta_T) \qquad \tau^*_{[m]T'}(S_T)$$

$$\mathrm{div}(G) \qquad \mathrm{div}\left(\tau^*_{[i]T'}(\Delta_T)\right) = \mathrm{Cu}(\tau_{[i]T'}) \cdot (\mathrm{div}(\Delta_T)) \to \sum (T \oplus P) - P$$

P-Etino

$$\mathrm{div}(G) = \sum_{i=0,\dots,m-1} P \oplus [i-1]T' - P \ominus [i]T'$$

$$= \sum \underbrace{T' \oplus P \ominus [i]T'}_{P \oplus [i-1]T'} - P \ominus [i]T'$$

$$\boxed{\mathrm{div}(G) = 0}$$ — G je konstantne

$$\Delta_T = \tau^*_T(\Delta_T) \qquad \tau^*_{T'}(G) = G$$

$$e_m(S \oplus R, T) = e_m(S, T)\, e_m(R, T)$$

$$e_m(S, T \oplus R) = e_m(S, T)\, e_m(S, R)$$

$$e_m(S, T)^{-1} = e_m(T, S)$$

Alternative

$$e_m(S, T) = (-1)^m \frac{g_T(S)}{g_S(T)} \frac{g_S(O)}{g_T(O)}$$

$$\mathrm{div}(g_T) = mT - mO$$

$$\mathrm{div}(g_S) = mS - mO$$

$\parallel$

1

$\mathrm{char}(K) \mid m$