Evo – trebali bi naći !

1. E/k $\underline{E[m]} := \{ P \in E(\bar{k}) : [m]P = 0 \} = \ker [m]$.

Kako izgleda $E[m]$ kao grupa?

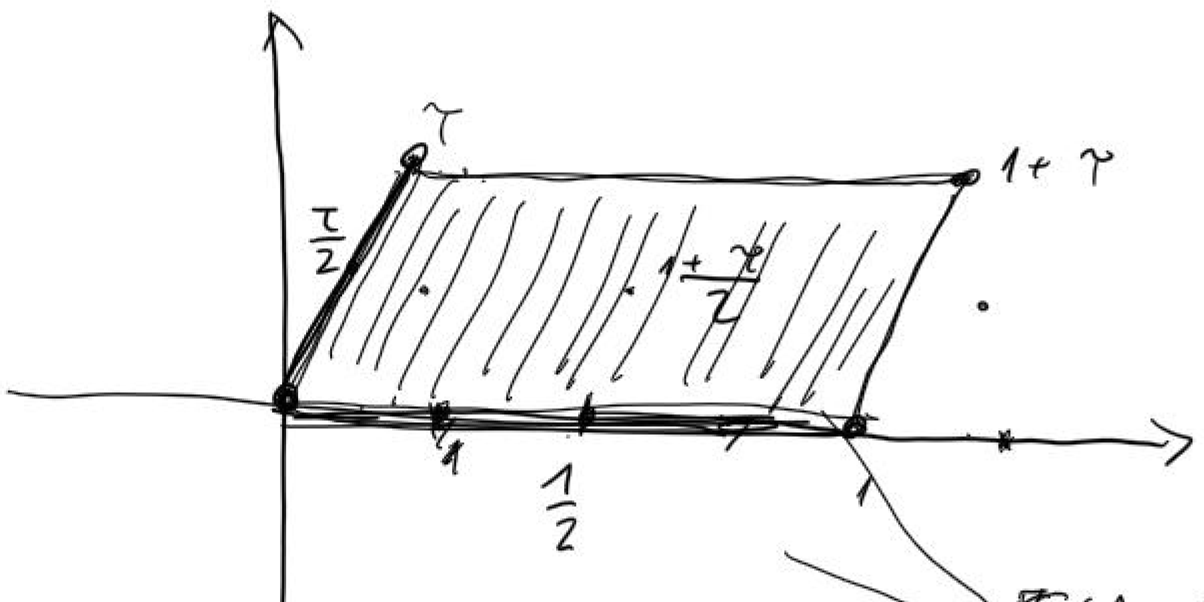
$E(k)[m] := \{ P \in E(k) : mP = 0 \}$.

__Tm__ $\forall\, E/\mathbb{C}$ $\exists!$ (do na homotetiju) rešetka $\Lambda \subseteq \mathbb{C}$ i izomorfizam (kompleksnih Liejevih) grupa $\phi : \mathbb{C}/\Lambda \to E$.

$\mathbb{C}/\Lambda \simeq E(\mathbb{C})$

Λ_1 je homotetična s Λ_2 ako $\exists\, \alpha \in \mathbb{C}^*$ t.d. $\alpha \Lambda_1 = \Lambda_2$ (pišem $\Lambda_1 \simeq \Lambda_2$)

$\Lambda = \mathbb{Z} w_1 + \mathbb{Z} w_2$. Npr. $\Lambda \simeq \mathbb{Z} + \mathbb{Z}\tau$



$\mathbb{C}/\Lambda \simeq E(\mathbb{C})$

$E(\mathbb{C})[2]$

$E(\mathbb{C})[n] = \{ (a \cdot \frac{1}{n} + b \cdot \frac{\tau}{n}) + \Lambda \}$ ($a, b \in \mathbb{Z}/n\mathbb{Z}$) $\simeq (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$

Imamo $E(\mathbb{C})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$

E/k, k PAB $\quad E(\bar{k})[n]$. $\quad [n]P = (f_1(P) : f_2(P) : f_3(P))$

$E(\bar{k})[n] = E(\mathbb{C})[n]$ $\quad$ f_1, f_2, f_3 nacrtalno

$f_1(P) = 0$, $f_2(P) \neq 0$, $f_3(P) = 0$

rješenja od ovoga sistemi su algebarski!

$\Rightarrow E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 \quad \forall n \in \mathbb{N}.$

Oznaka $G_k := Gal(\bar{k}/k) = \{ f \in Aut\ \bar{k}$ t.d. $f|_k = id \}$

Definicija Neka je G grupa, a X skup. Tada je (desno) djelovanje grupe od G na X funkcija $G \times X \longrightarrow X \quad (g, x) \mapsto x^g$ gdje vrijedi asocijativnost, $x^{gh} = (x^g)^h \quad \forall x \in X, \forall g, h \in G$, te $x^e = x \quad \forall x \in X$.

Npr. S_n djeluje kanonski $\{1, \ldots, n\}$, $\forall$ grupa G djeluje na sebe množenjem, $Gal(K/\mathbb{Q})$ djeluje na K, ...

Def. Označavamo s $G \circlearrowright X$ da G djeluje na X.

ORBITA Gx od nekog $x \in X$ je $Gx := \{ x^g \mid g \in G \}$

Def. Ako $g \in G$ i $x \in X$ t.d. $x^g = x$ kažemo da je x fiksna točka od g, tj. da g fiksira x.

Za $\forall x \in X$ definiramo <u>stabilizatorsku podgrupu</u> od x (IZOTROPSKA PODGRUPA od x) $G_x := \{g \in G \mid x^g = x\}$.

Nap: $G_x \leq G$. $Gx \subseteq X$

Teorem (Teorem o orbiti i stabilizatoru).

Neka su G i X konačni i $G \circlearrowright X$.

Tada vrijedi $|Gx| = [G : G_x] = \dfrac{|G|}{|G_x|}$.

Korisno za primjenje: Koliko ima rotacijskih simetrija kocke?

1) fiksiramo npr. 1 stranu – G orbiju, 4 moguće rotacije.

2) 1. točka.

– 8 mjesta, 3 mjesta za rotaciju $\Rightarrow 24$.

$= 24$.

X = strane kocke

G

x = 1. strana.

$|Gx| = 6$

$|G_x| = 4$

$\Big\}$ 24

$G_k \circlearrowright E[n]$ $\rightsquigarrow$ $\rho_{E,n}$ mod n reprezentacija.