Prošli put: $G \circlearrowleft X$ notacija: $g \in G$, $x \in X$ $g \cdot x$

$Gx = \{ g \cdot x \mid g \in G \}$ (ORBITA od x)

$G_x = \{ g \in G \mid g \cdot x = x \}$ (STABILIZATOR od x) $\leq G$.

$X^g := \{ x \in X \mid g \cdot x = x \}$ (FIKSNE TOČKE od g)

$X/G = \{ Gx \mid x \in X \}$ (SKUP ORBITA)

<u>BURNSIDEOVA LEMMA</u> $$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

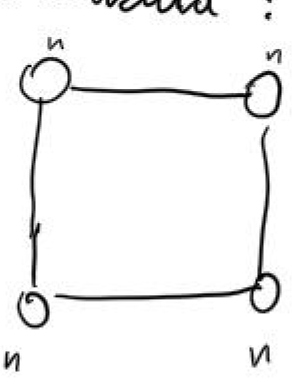
<u>Dokaz</u>: $$\sum_{g \in G} |X^g| = \sum_{g \in G} |\{ x \in X : g \cdot x = x \}|$$

$$= |\{ (g,x) : g \in G, x \in X, g \cdot x = x \}| = \sum_{x \in X} |\{ g \in G \mid gx = x \}|$$

$$= \sum_{x \in X} |G_x| \overset{TOS}{=} \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|}$$

$$= |G| \cdot |X/G| \Rightarrow |X/G| = \frac{1}{|G|} \cdot \sum_{g \in G} |X^g|$$ ∎

<u>Primjer</u> Bojanje četverokuta: bojimo vrhove kvadrata u n boja



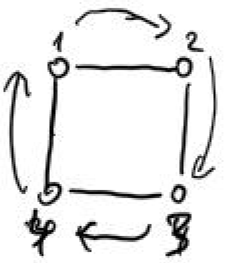
- koliko ima različitih "do na rotaciju" (90°, 180°, 270°)
- 2 bojanja su isto ako rotacijom možemo iz 1 dobiti 2.

$G \circlearrowright X$ $\quad$ G = grupa rotacija kvadrata $\cong \mathbb{Z}/4\mathbb{Z}$ $(\cong C_4)$ $= \langle \text{rot } 90° \rangle$.

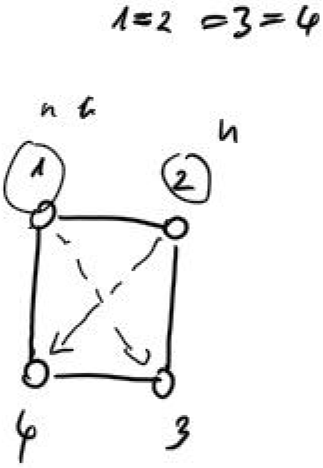
X = skup svih bojanja kvadrata (uređene 4orke $(a_1, a_2, a_3, a_4) \in \{1, \dots, n\}^4$)

$|X/G| = ?$ koristimo BURNSIDEOVU LEMU

rot $90° =: g$.



$$|X^g| = n$$



$$|X^{g^2}| = n^2$$

$$|X^{g^3}| = |X^g| = n$$

$$|X^{id}| = n^4.$$

$$\Rightarrow |X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| = \frac{1}{4}\left(n^4 + n^2 + 2n\right)$$

DZ* Koliko ima bojanja stranica kocke s n boja do na rotacije? $\underline{G \cong S_4}$

Djelovanje grupe daje homomorfizam iz grupe G u grupu bijekcija $X \to X$

Def. Reprezentacija grupe G na vektorskom prostoru V je homomorfizam grupe G u $GL(V)$.

tj. reprezentacija je preslikavanje

$\rho : G \to GL(V)$ takvo da je $\rho(g_1 g_2) = \rho(g_1) \cdot \rho(g_2)$

$\forall g_1, g_2 \in G$.

Neka je E/K. Sjetimo se $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

K je PRAB.

Imamo da $G_K := Gal(\overline{K}/K)$ djelovanje od G_K ČUVA RED ELEMENTA od $E(\overline{K})$

Dakle preslikavanje

$\rho_n : G_K \to Aut(E[n]) \simeq GL_2(\mathbb{Z}/n\mathbb{Z})$

- to je homomorfizam, te nam daje "reprezentaciju" grupe G_K.

Međutim po definiciji ovo nije reprezentacija, jer $\mathbb{Z}/n\mathbb{Z}$ nije VP ako n nije prost.

Ovaj homomorfizam grupa se zove MOD N REPREZENTACIJA PRIDRUŽENA ELIPTIČKOJ KRIVULJI E.

,

$G_K \curvearrowright E[n]$

$n(P^\sigma) = (nP)^\sigma = O$

$[n]$ je def nad K

$[n] : E \to E$

$(x, y) \to (f_1(x,y), f_2(x,y))$

$f_1, f_2 \in K(x)$

Oprez

$f \in K(x) \mid \sigma \in G_K$

$f(x)^\sigma = f(x^\sigma)$

$(a_n x^n + a_{n-1} x^{n-1} + \dots + a_0)$

Pretpostavimo da za E/K, $E[n] \subseteq E(\overline{K})$ jer

je $[n]$ zakon, svi funkcija

pa su njegove nultočke

pa su ~~E[n]~~ sve koordinate

od $E[n]$ algebarske.

$\mathbb{Q}(E[n]) :=$ polje definirano tako da polju $\mathbb{Q}$ pridružimo x i y koordinate nultočaka iz $E[n]$.

$E/\mathbb{Q}$ (može se umjesto $\mathbb{Q}$ uzeti bilo koji DAB K)

$[\mathbb{Q}(E[n]) : \mathbb{Q}] < +\infty.$

$\forall \sigma \in Gal(\overline{\mathbb{Q}} / \mathbb{Q}(E[n])) \iff \rho_n(\sigma) = I$ (identiteta)

$\Rightarrow Gal(\overline{\mathbb{Q}} / \mathbb{Q}(E[n])) = \ker \rho_n$

Dakle

$$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) / Gal(\overline{\mathbb{Q}} / \mathbb{Q}(E[n])) \simeq Gal(\mathbb{Q}(E[n])/\mathbb{Q})$$

$Gal(\overline{\mathbb{Q}} / \mathbb{Q}(E[n])) = \ker \rho_n$, $Gal(\mathbb{Q}(E[n])/\mathbb{Q}) = \operatorname{Im} \rho_n$

$$\Rightarrow \boxed{\operatorname{Im} \rho_n = Gal(\mathbb{Q}(E[n])/\mathbb{Q})}$$

Promatrat ćemo dosta ove slike.

Pogledajmo kako eksplicitno izračunati $\rho_n(\sigma)$. $\sigma \in G_{\mathbb{Q}}$

Neka je $\{P, Q\}$ baza za $E[n]$ ($E[n] = \mathbb{Z}/n\mathbb{Z} \cdot P + \mathbb{Z}/n\mathbb{Z} \cdot Q$)

$P^\sigma \in E[n] \Rightarrow P^\sigma = \alpha P + \beta Q$ za neke $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$.

$Q^6 = \gamma P + \delta Q$ za $\gamma, \delta \in \mathbb{Z}/n\mathbb{Z}$.

$$\rho_n(G) = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in GL_2(\mathbb{Z}/n\mathbb{Z})$$

$$\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} \lambda \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \checkmark$$

Nap. Slika od ρ_n ovisi o izboru baze od $E[n]$!

Nap. Promjenom baze čemo dobiti konjugiranu (u $GL_2(\mathbb{Z}/n\mathbb{Z})$) matricu!

Primjer Mod 2 reprezentacija.

$E: y^2 = x^3 + ax + b$ $a, b \in \mathbb{Q}$ $E/\mathbb{Q}$.

Slika mod 2. reprezentacije ? $y^2 = x^3 + ax + b = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

$E[2] = \{O, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\}$ $\alpha_1, \alpha_2, \alpha_3 \in \overline{\mathbb{Q}}$.

Želimo za $\mathrm{Im}\,\rho_2 \cong G_{al}(\mathbb{Q}(E[2])/\mathbb{Q})$

$= G_{al}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)/\mathbb{Q})$.

Mogućnosti za $\mathrm{Im}\,\rho_2(G_{\mathbb{Q}})$ = mogućnosti za Galoisove grupe polinoma stupnja 3.

$= \{S_3, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \{id\}\}$

$\alpha_1, \alpha_2, \alpha_3 \notin \mathbb{Q}$	$\alpha_1, \alpha_2, \alpha_3 \notin \mathbb{Q}$	$\alpha_1 \in \mathbb{Q}$	$\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$.
$\Delta_E \neq \square$	$\Delta_E \neq \square$	$\alpha_2 \alpha_3 \notin \mathbb{Q}$	

Primjer $E\ y^2 = x^3 - 2$.

$$E[2] = \{O, (\sqrt[3]{2}, 0), (\zeta_3\sqrt[3]{2}, 0), (\zeta_3^2\sqrt[3]{2}, 0)\}$$

$\zeta_3 = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$ – primitivni 3. korijen iz 1.

Općenito $\zeta_n :=$ primitivni n-ti korijen iz 1.

$$\mathbb{Q}(E[2]) := \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$$

$$Gal(\mathbb{Q}(E[2])/\mathbb{Q}) = \langle \sigma, \tau \rangle \simeq S_3$$

$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ $\quad \sigma(\sqrt{-3}) = -\sqrt{-3}$ (kompleksno konjugiranje)

$\tau(\sqrt[3]{2}) = \zeta_3\sqrt[3]{2}$ $\quad \tau(\sqrt{-3}) = \sqrt{-3}$ $\quad \sigma(\zeta_3) = \zeta_3^2$

$\tau(\zeta_3) = \zeta_3$.

$P_1 := (\sqrt[3]{2}, 0)$

$P_2 = (\zeta_3\sqrt[3]{2}, 0)$

$P_3 = (\zeta_3^2\sqrt[3]{2}, 0) = P_1 + P_2$

Označimo skup $\{P_1, P_2\}$

$\rho_2(\sigma) = ?$

$P_1^{\sigma} = P_1$

$P_2^{\sigma} = (\zeta_3^2\sqrt[3]{2}, 0) = P_3 = P_1 + P_2$

$$\Rightarrow \rho_2(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$\rho_2(\tau) = ?$

$$P_1^\tau = (\zeta_3 \sqrt[3]{2}, 0) = P_2$$

$$P_2^\tau = (\zeta_3^2 \sqrt[3]{2}, 0) = P_1 + P_2$$

$$\rho_2(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

<u>Par definicija u vezi djelovanja grupa:</u>

<u>Def</u> Ako grupa G djeluje na X, te je $|X/G| = 1$ tada kažemo da je djelovanje TRANZITIVNO.

Ako $\forall g, h \in G$, ako $\exists x \in X$ t.d. vrijedi da $x^g = x^h \Rightarrow g = h$ kažemo da G djeluje VJERNO na X.

To je $\Leftrightarrow$ ($x^g = x$ za neki $x \in X \Rightarrow g = id$)

$Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \hookrightarrow E[n]$ (djeluje vjerno!)

VJERNO

MOD N REPREZENTACIJA ✓

P - ADSKI (CIJELI) BROJEVI

<u>Def</u> INVERZNI SISTEM je niz objekata (~~sk~~ SKUPOVA / GRUPA / PRSTENA)

(A_n) zajedno sa nizom morfizama (funkcija / HOMOMORFIZAMA)

(f_n)

$$\cdots \xrightarrow{f_3} A_3 \xrightarrow{f_2} A_2 \xrightarrow{f_1} A_1.$$

Def INVERZNI LIMES $A = \varprojlim_n A_n$ inverznog sistema $(A_n), (f_n)$ definiramo kao pnoji je objekt A čiji elementi su beskonačni nizovi (a_n), gdje je $a_n \in A_n$ $\forall n \geq 1$ i vrijedi ~~$f_n(a_{n+1})$~~ $f_n(a_{n+1}) = a_n$ $\forall n \geq 1$.

Def Neka je p fiksan prost broj. PRSTEN CIJELIH p-ADSKIH BROJEVA $\mathbb{Z}_p$ je inverzni limes

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

inverznog sistema prstena $(\mathbb{Z}/p^n\mathbb{Z})$, f_n je redukcija modulo p^n.

Nap Ako su A_n grupe i f_n homomorfizmi grupa $\Rightarrow A = \varprojlim A_n$ je grupa, analogno za prstene.

$\Rightarrow \mathbb{Z}_p$ je prsten.

Nap $\mathbb{Z}_p$ je prsten s $1. = (\bar{1}, \bar{1}, \ldots\ldots)$

$$\begin{array}{cc} \shortparallel & \shortparallel \\ a_1 & a_2 \\ \shortparallel & \shortparallel \\ 1+\mathbb{Z}/p\mathbb{Z} & 1+\mathbb{Z}/p^2\mathbb{Z} \ldots \end{array}$$

char $\mathbb{Z}_p = 0$. $\quad n \cdot 1 = (n \bmod p, n \bmod p^2, n \bmod p^3, \ldots) \neq 0$

$n \neq 0$.

$\mathbb{Z} \hookrightarrow \mathbb{Z}_p$

$a \mapsto (\bar{a}, \bar{a}, \ldots)$

$(a_1, a_2$

$a_1 \in \{0, \ldots, p-1\}$

$a_2 \bmod p = a_1$

$a_2 \in \{a_1 + p \cdot k \, ; \, k \in \{0, \ldots, p-1\}\})$

$\mathbb{Z}_p$ je neprebojen.

Primer $2 = (2, 2, 2, 2, \ldots)$

$2002 = (0, 42, 287, 2002, 2002, \ldots)$

$-2 = (5, 47, 341, 2399, \ldots)$

$\frac{1}{2} = (4, 25, 172, \ldots)$

$\sqrt{2} = \begin{cases} (3, 10, 108, 2100, \ldots) \\ (2, 39, \ldots) \end{cases}$

$\vdots$

Def. Naj je ℓ fiksno prast broj. Premisljam da $\exists$ pravilni homomorfizam $E[\ell^{n+1}] \xrightarrow{\ell} E[\ell^n]$, tj $[\ell]$

INVERZNI SISTEM

$$\ldots \to E[\ell^3] \xrightarrow{[\ell]} E[\ell^2] \xrightarrow{[\ell]} E[\ell].$$

SE ZOVE TATEOV MODUL $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$.