(4) b (Artin 38 – 51)

Definícia grupy

- množina S s operáciou skladania, na ktorej existujú inverzné prvky pre každý prvok množiny.

Príklady - $R^x = R \setminus \{0\}$ vzhľadom na násobenie
- množina $n \times n$ regulárnych matíc (všeobecná lineárna grupa $GL_n(R)$)

Operácia skladania (kompozičné pravidlo)

dvom prvkom $a, b \in S$ priradiť prvok $p \in S$.

(Modelom je sčítanie/násobenie reálnych čísel)

Formálne ide o zobrazenie $S \times S \to S$ (binárna operácia) priraďujúca dvojici (záleží na poradí)

$$(a, b) \longmapsto p.$$

Rôzne značenia: $p = f(a, b)$

$p = ab, a \times b, a \circ b, a + b$

v závislosti od kontextu.

Pre grupy sa najčastejšie používa značenie ab.

Príklad: 2×2 matice:

$$a = \begin{bmatrix} 1 & 3 \\ 0 & 2 \end{bmatrix}, \quad b = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \quad ab = \begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix}$$

$$ba = \begin{bmatrix} 1 & 3 \\ 2 & 8 \end{bmatrix}$$

- Dôležité: (asociatívny zákon)

$$(ab)c = a(bc)$$

pre $a, b, c \in S$

(komutatívny zákon)

$$ab = ba$$

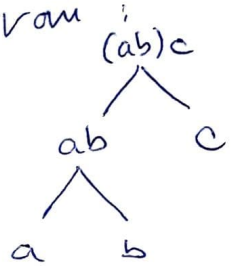
(v našom príklade matíc neplatil).

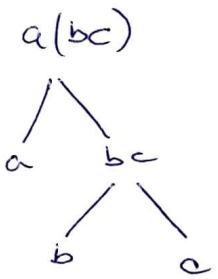
- Asociativita:
  - v aditívnom značení: $(a+b)+c = a+(b+c)$
  - vo funkčnom: $m(m(a,b),c) = m(a, m(b,c))$
  - v súčinovom $(ab)c = a(bc)$

Vo všetkých troch prípadoch ide o to isté, iné je len značenie.

---

odbočka: multiplikačný strom:





pre výraz, v ktorom je n členov by sme dostali veľa viac rôznych možností ako ho uzátvorkovať (Catalanove čísla?) – je to zaujímavý kombinatorický problém.

Asociatívny zákon ale hovorí, že na zátvorkovaní nezáleží (to ale treba dokázať – Artin Prop. 2/1.4) a všetky súčiny v stromoch sú rovnaké.

(5)

Prečo je asociatívita dôležitá?

- základným príkladom je skladanie zobrazení.

Ak je T množina ~~potom~~ a g, f sú zobrazenia $T \to T$,

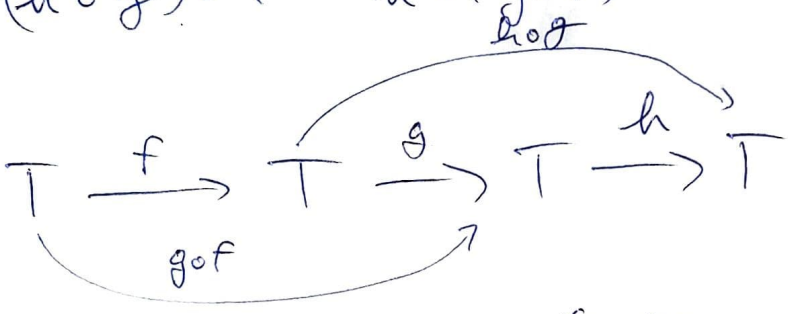
potom $g \circ f$ značíme $t \longmapsto g(f(t))$.

Teda máme pravidlo o: $g, f \longmapsto g \circ f$

$$Zobr(T,T) \times Zobr(T,T) \longrightarrow Zobr(T,T)$$

Skladanie zobrazení spĺňa asociatívny zákon:

$$(h \circ g) \circ f = h \circ (g \circ f)$$



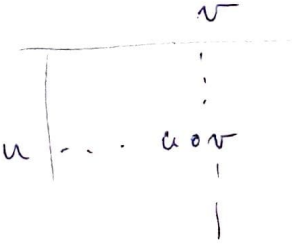
lebo obe zložlenia priraďujú t na $a(g(f(t)))$.

Príklad Nech $T = \{a, b\}$. $Zobr(T,T)$ je $2^2 = 4$

i:	identita	$i(a) = a$,	$i(b) = b$
τ:	transpozícia	$\tau(a) = b$	$\tau(b) = a$
α:	konšt. a	$\alpha(a) = a$	$\alpha(b) = a$
β:	konšt b	$\beta(a) = b$	$\beta(b) = b$

Tabuľka:

II \ I	i	τ	α	β
i	i	τ	α	β
τ	τ	i	β	α
α	α	α	α	α
β	β	β	β	β



$\tau \circ \alpha = \beta, \quad \alpha \circ \tau = \alpha$ (napr.)

Na rozdiel od tabuľky, ktorú sme videli minulý týždeň pre S_3 tu čosi nesedí

- Na jednej strane, stále máme identitu (neutrálny prvok)

$$ea = a \quad \text{a} \quad ae = a \quad \text{pre } \forall a \in S$$

V iných príkladoch:
- matice $I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, $\mathbb{R}^+$ – nula, $\mathbb{R}^\times$ – jednotka

Ale inverzný prvok, t.j. také b, že

$$ab = 1 \quad \text{a} \quad ba = 1$$

existuje len pre transpozíciu τ.

Tvrdenie jednoznačnosť inverzného prvku

– ak $ab = 1$ a $ca = 1$, potom $b = c$.

D:

$$c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b.$$

1 neut. ; b je inv. ; asoc. ; c je inv ; 1 neut.

Značenie a^{-1}.

potom: $(ab)^{-1} = b^{-1}a^{-1}$

a môžeme tiež definovať $a^n = a\,a \cdots a$

$a^0 = 1$

$a^{-n} = (a^{-1}) \cdots (a^{-1})$

platí $a^{r+s} = a^r \cdot a^s$, tiež $(a^r)^s = a^{rs}$

(pre $r, s \in \mathbb{Z}$).

Značenie $\frac{b}{a}$ je lepšie sa vyhnúť, lebo nie je jasné, či sa myslí ba^{-1}, $a^{-1}b$ (resp. niečo ešte iné).

Definícia Množina G s binárnou operáciou (skladaním, pravidlom skladania) nazývame grupou, ak táto operácia:
- je asociatívna
- má neutrálny prvok
- každé $a \in G$ má inverzný prvok.

Komutatívne (resp. Abelovské) grupy sú tie, v ktorých navyše platí aj komutatívny zákon.

Tvrdenie (pravidlo krátenia). Nech a, b, c sú prvky grupy G: zľava/sprava
ak $ab = ac$, potom $b = c$. (podobne $ba = ca \Rightarrow b = c$)

D: Prenásobíme $ab = ac$ prvkom a^{-1} zľava.

$$b = a^{-1}ab = a^{-1}ac = c.$$

Násobenie a^{-1} je dôležité – existujú príklady binárnych operácií, kde neexistencia inverzu dá neplatnosť pravidla krátenia:

Napr. $0 \cdot 1 = 0 \cdot 2$ (Nevieme deliť 0)

0^{-1} ✗

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$$

(Neexistuje $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}^{-1}$)

Alebo vo všeobecnosti: $Ax = Bx \not\Rightarrow A = B$

(matica, vektor)

keď neexistuje x^{-1}.

Takže ktoré matice majú inverz?

↳ reg. matice $GL_n(\mathbb{R})$, $GL_n(\mathbb{C})$

$T \to T$

Ktoré zobrazenia majú inverz?

↳ permutácie bijekcie → permutácie

S_3 sme videli ako príklad

Podgrupy

Dôvod prečo sú grupy permutácií S_n a všeobecné lineárne grupy $GL_n(\mathbb{R})$ $(GL_n(\mathbb{C}))$ dôležité je fakt, že obsahujú ich podgrupy ako podmnožiny, ktoré majú istú operáciu.

Tedy podobne ako sme pre vekt.-priestory definovali podpriestory, môžeme sa pozrieť na podgrupy.

Pre definíciu podgrupy je dôležité: $H \subseteq G$

a) uzavretosť ($a \in H, b \in H \rightarrow ab \in H$) (vzhľadom na operáciu)

b) identita $1 \in H$

c) inverzné prvky $a \in H \Rightarrow a^{-1} \in H$.

---

a) – znamená, že operácia skladania na H je indukovaná z G. (teda máme asociatívnu)

b), c) dávajú grupovú štruktúru.

Triviálne príklady: pre G máme $\{1\}$ a G.

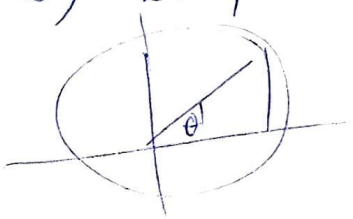
vlastná podgrupa – niečo iné, ako tieto dve.

príklad a) horné trojuholníkové matice. (reg.)

$ad \neq 0$.

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

b) komplexné čísla $\cos\theta + i\sin\theta$ –



t.j. $|z|=1$ tvoria podgrupu v $\mathbb{C}^*$.

c) príklad $b\mathbb{Z} = \{ n \in \mathbb{Z} \mid n = bk \text{ pre } k \in \mathbb{Z} \}$.

Tvrdenie $k\mathbb{Z}$ je podgrupou $\mathbb{Z}^+$, navyše každá podgrupa H grupy $\mathbb{Z}^+$ má tvar $H = b\mathbb{Z}$ pre nejaké $b \in \mathbb{N}_0$.

Pôkaz Overiť, že $k\mathbb{Z}$ je podgrupou — cvičenie.

Nech H je podgrupa $\mathbb{Z}^+$.

- Neut. prvok je 0, teda $0 \in H$, inverzný k a je $-a$.
- ak je 0 jediným prvkom H, potom $H = 0\mathbb{Z}$ ✓
- ak existuje nejaký nenulový, potom buď $a > 0$ alebo $-a > 0$.

Zoberme b ako najmenšie nenulové kladné číslo patriace do H. Potom tvrdíme, že $H = b\mathbb{Z}$.

(najprv: $b\mathbb{Z} \subset H$ → to je jasné, lebo $b \in H$ aj $bk = b+b+\dots+b$, resp. $b(-k) = -bk$.

Opačná inklúzia $H \subset b\mathbb{Z}$.

Každé celé číslo n sa dá deliť so zyškom:

$$n = bq + r, \quad 0 \le r < b.$$

Keďže n aj bq sú v H aj r tam musí patriť. $(r = n - bq)$

Lenže b bolo najmenšie kladné číslo v H, jediná možnosť je, že $r = 0$ a $n = bq \in b\mathbb{Z}$.

(odpadla kvôli chybe 1. predp.) Sem 5.3.18