Групно напоље

Душан Драгутиновић

dusandragutinovic1@gmail.com

1. мај 2018.

Преглед

Алгебарска структура

Алгебарска структура за нас

Алгебарском структуром $\mathbb{A} = (A, \#, \times, *, ...)$ сматрамо скуп A и на њему задане неке бинарне операције $\#, \times, *... : A^2 \to A$. Нама занимљиве биће:

- Групе
- Прстени (Комутативни прстени са јединицом)
- Поља

Алгебарска структура

Алгебарска структура за стварно

Алгебарска структура $\mathbb{A}$ је уређен пар $\mathbb{A} = (A, S)$, где је A неки скуп, а S неки коначан скуп операција. Те операције могу бити и различитих дужина. Операцијом дужине n на скупу A сматрамо пресликавање $w : A^n \to A$.

Пример операција:

- Унарне: Истакнути елемент
- Бинарне: $+(a, b) := a + b, \quad a, b, a + b \in A$
- n - арне: $w(a_1, ..., a_n) = b, \quad a_1, ..., a_n, b \in A$

Група

Алгебарску структуру $(G, *)$ називамо *групом*, ако задовољава наредне услове:

0. (добра дефинисаност) Ако $x, y \in G$ тада и $x * y \in G$
1. (асоцијативност) За све $x, y, z \in G$ важи

$$x * (y * z) = (x * y) * z$$

2. (постојање неутрала) Постоји $e \in G$ такав да за све $x \in G$ важи

$$x * e = e * x = x$$

3. (постојање инверза) За свако $x \in G$ постоји неко $y \in G$ тако да важи

$$x * y = y * x = e$$

Абелова група

Нека поред ставки 0, 1, 2, 3 важи и ставка:

4. (комутативност) За све $x, y \in G$ важи

$$x * y = y * x$$

Такву групу називамо Абеловом групом.

Примери: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Примери

Пример

1. Нека је $G = \{3k + 1 | k \in \mathbb{Z}\}$ *и нека је на* G *задата операција уобичајног множења* $\cdot$.

Пример

2. Нека је $G = \mathbb{R}$ *и нека је операција задата са* $x * y = 1 - x \cdot y$.

Да ли су $(G, \cdot)$, $(\mathbb{R}, *)$ групе?

Примери

Пример

3. Нека је G скуп свих квадратних матрица и нека је на G задата операција множења матрица $\cdot$.

Пример

4. Нека је $GL_2(\mathbb{R})$ скуп свих реалних квадратних матрица облика $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ таквих да је $ad - bc \neq 0$ и на $GL_2(\mathbb{R})$ задата операција множења матрица $\cdot$.

Да ли су $(G, \cdot)$, $(GL_2(\mathbb{R}), \cdot)$ групе?

Рачунање у групи

Нека је $(G, *)$ група и $a, b, c \in G$

- Из $a * b = c * a$ не можемо закључити $b = c$, то је случај само Абелове групе G
- Из $a * b * a * b = a * c * b$ можемо закључити $b * a = c$
- $(a * b)^{-1} = b^{-1} * a^{-1}$
- Пишемо $a^n = a * \ldots * a$
- Није тачно $(a * b)^n = a^n * b^n$, сем за Абелове групе G

Примери, још једном

Пример

5. Нека је $\mathbb{Z}$ скуп целих бројева, а $n\mathbb{Z} = \{n \cdot k | k \in \mathbb{Z}\}$. Покажимо да су $(\mathbb{Z}, +)$ и $(n\mathbb{Z}, +)$ групе.

Дакле, $(n\mathbb{Z}, +)$ је група и садржана је у групи $(\mathbb{Z}, +)$.

Подгрупе

Подгрупа

Нека је $(G, *)$ група, нека је $H \subseteq G$ и нека је $(H, *)$ група. Тада H називамо *подгрупом* групе G, у ознаци $H \leqslant G$.

За испитивање да ли је нешто подгрупа од значаја нам је највише следећа теорема.

Теорема

Нека је $(G, *)$ група, $H \subseteq G$, $H \neq \emptyset$. Тада су следеће ствари еквивалентне:

1. $H \leqslant G$
2. *За све* $a, b \in H$ $a^{-1} * b \in H$
3. *За све* $a, b \in H$ $a * b, a^{-1} \in H$

Циклична група

Циклична група

За групу G кажемо да је циклична ако постоји $a \in G$ тако да је $G = \{a^m | m \in \mathbb{Z}\}$. Пишемо $G =< a >$.

- Ако G има бесконачно много елемената, кажемо да је бесконачног реда. То се за цикличне групе дешава када не постоји $n \in \mathbb{Z}$ такво да је $a^n = e$.
- Иначе, ред групе је број $|G|$.
- Ако постоји најмање n такво да је $a^n = e$, кажемо да је ред елемента a једнак n и пишемо $r(a) = n$.
- Цикличне групе реда n изоморфне су са $\mathbb{Z}_n$.

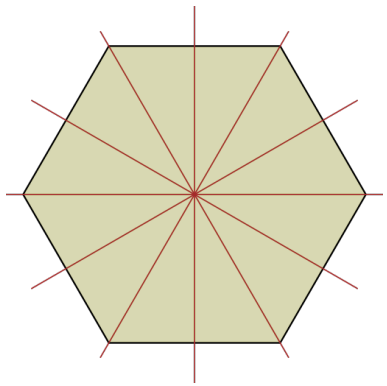
Диедарска група

Диедарска група

Диедарска група је група симетрија правилног n-тоугла. Формално, Диедарска група јесте група

$$\mathbb{D}_n = < r, s | r^n = 1, s^2 = 1, sr = r^{-1}s >$$

- Геометрију пребацујемо у алгебру
- $< r >$ је подгрупа реда n групе D_n
- $< s >, < sr >, < sr^2 >, \ldots$ су подгрупе реда 2 групе $\mathbb{D}_n$



Слика: Пример осних рефлексија $s, sr, sr^2, \ldots$

Лагранжова теорема

Лема

Нека је H подгрупа групе G и нека је a неки елемент из G. Тада постоји бијекција између скупова H и $aH := \{a * h | h \in H\}$.

Лема

Нека је H подгрупа групе G. Нека је на G задата релација $\sim$ са: $a \sim b$ акко $a^{-1} * b \in H$. Тада је $\sim$ релација еквиваленције на G и класа еквиваленције за произвољан елемент $a \in G$ је $C_a = aH$.

За H подгрупу од G са $[G : H]$ означимо број различитих aH за $a \in G$, тј. број класа еквиваленције релације $\sim$.

Теорема (Лагранж)

Нека је G коначна група и H нека њена подгрупа. Тада важи

$$[G : H] \cdot |H| = |G|$$

Специјално, важи:

$$|H| \mid |G|$$

Наизглед наивни примери

- Лагранж каже да и ред сваког елемента дели ред групе
- Ако је $r(a) = n$ и $a^m = e$ за неко m, тада $n|m$
- $(Z_p \setminus \{0\}, \cdot_p)$ чини групу, где је $\cdot_p$ множење по модулу p, где је p прост број

Простих бројева постоји бесконачно много

Теорема

Простих бројева постоји бесконачно много.

Симетрична група

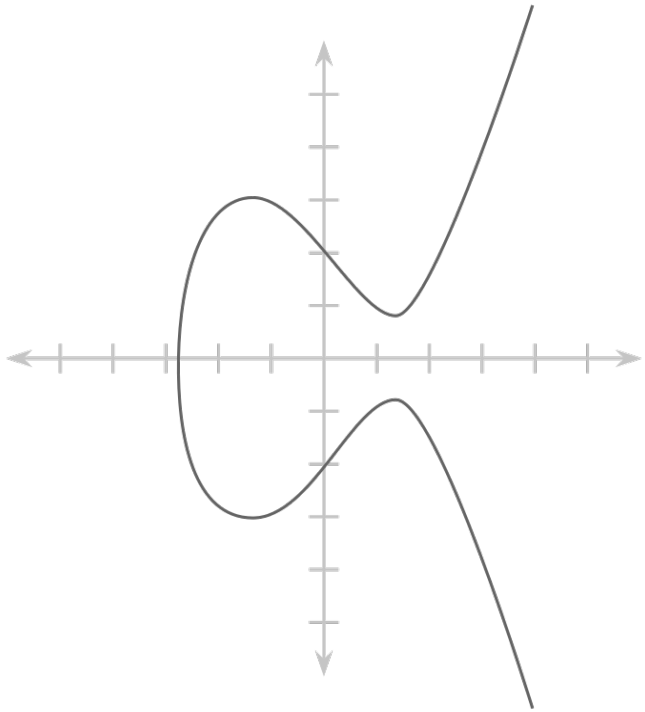
Симетрична група

Симетрична група скупа X јесте скуп свих бијекција (дакле функција!) из скупа X на самог себе са операцијом композиције пресликавања. Означавамо је са $Sym(X)$.
За коначан скуп X са n елемената користимо ознаку $\mathbb{S}_n$. Дакле, елементи групе $\mathbb{S}_n$ су пермутације ($=$ бијекције) скупа $\{1, 2, ..., n\}$.

- Покажимо да је ово стварно једна група
- Колики је ред ове групе?
- Сваку пермутацију из $\mathbb{S}_n$ можемо написати као производ *циклуса*

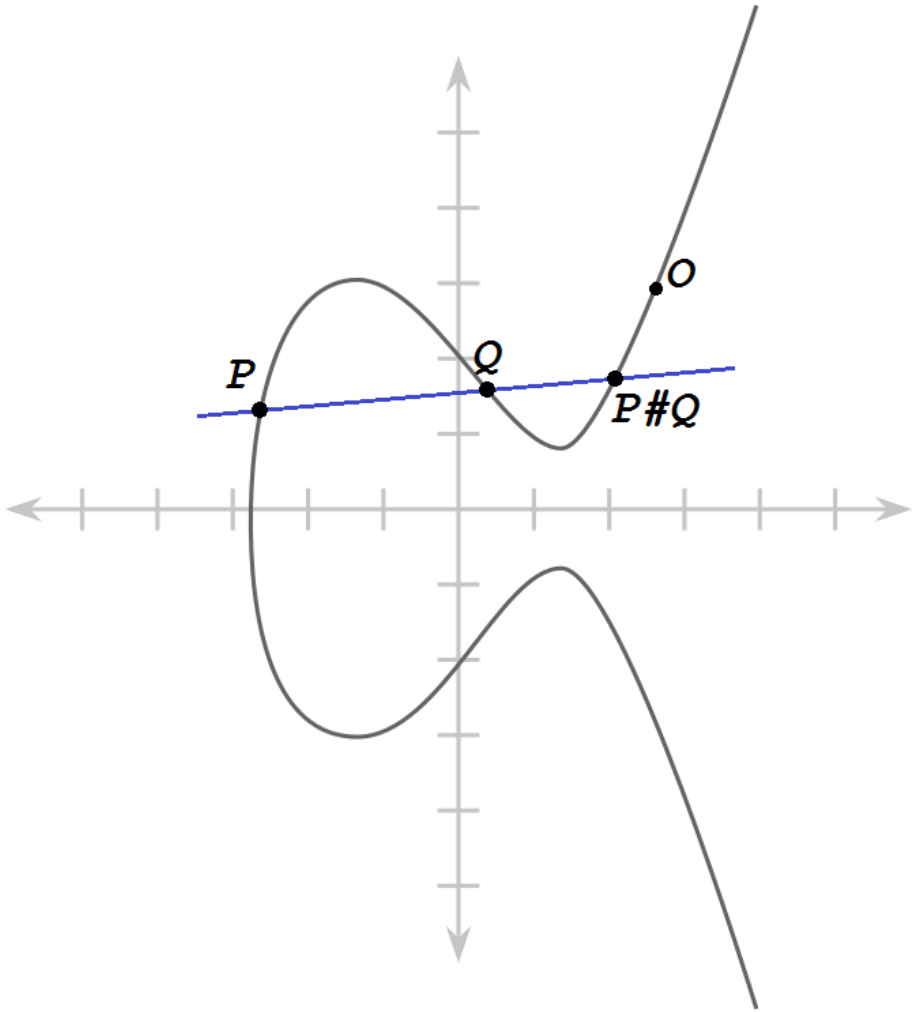
Елиптичке криве

- Посматрајмо једначине облика $y^2 = x^3 + p \cdot x + q$ и скицирајмо их у Декартовом координатном систему.

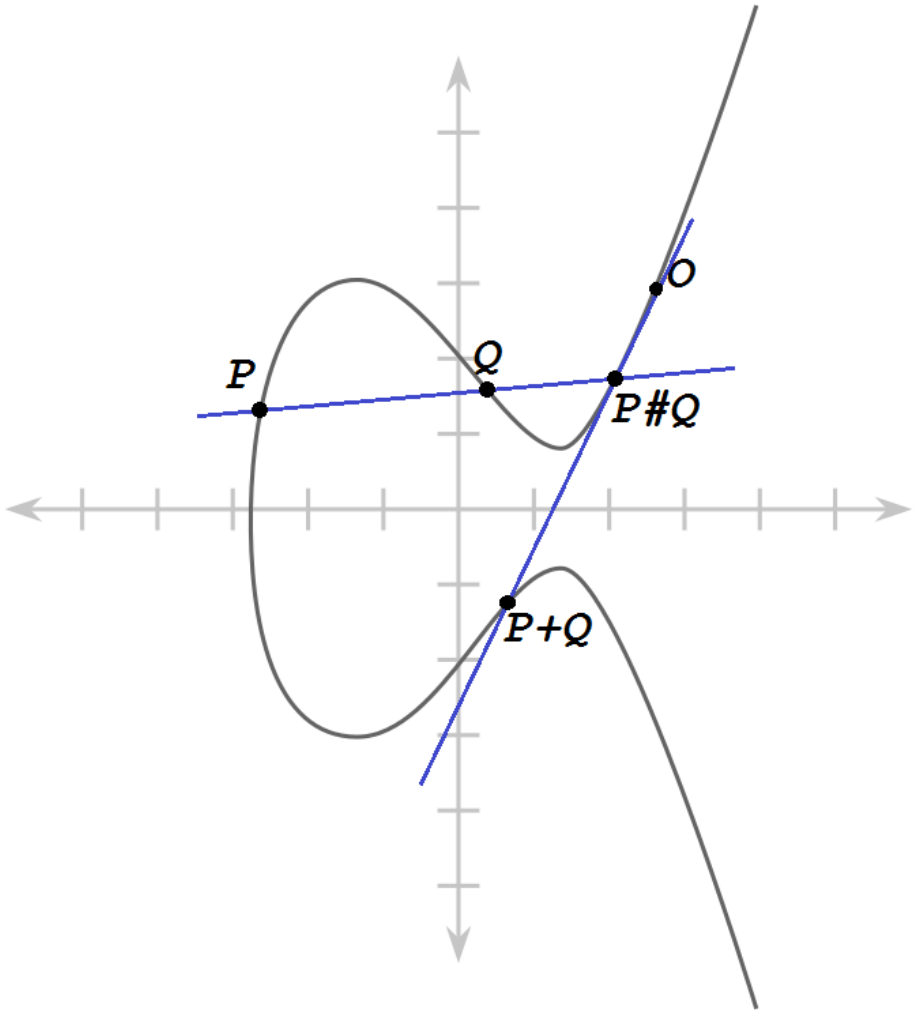


- Одаберимо произвољно неку тачку са криве и означимо је са $\mathcal{O}$. Њу ћемо прогласити неутралом групе свих тачака са елиптичке криве у односу на операцију $+$ коју ћемо касније дефинисати и та тачка $\mathcal{O}$ ће заиста бити неутрал такве групе.

- Сабирање тачака (међукорак)

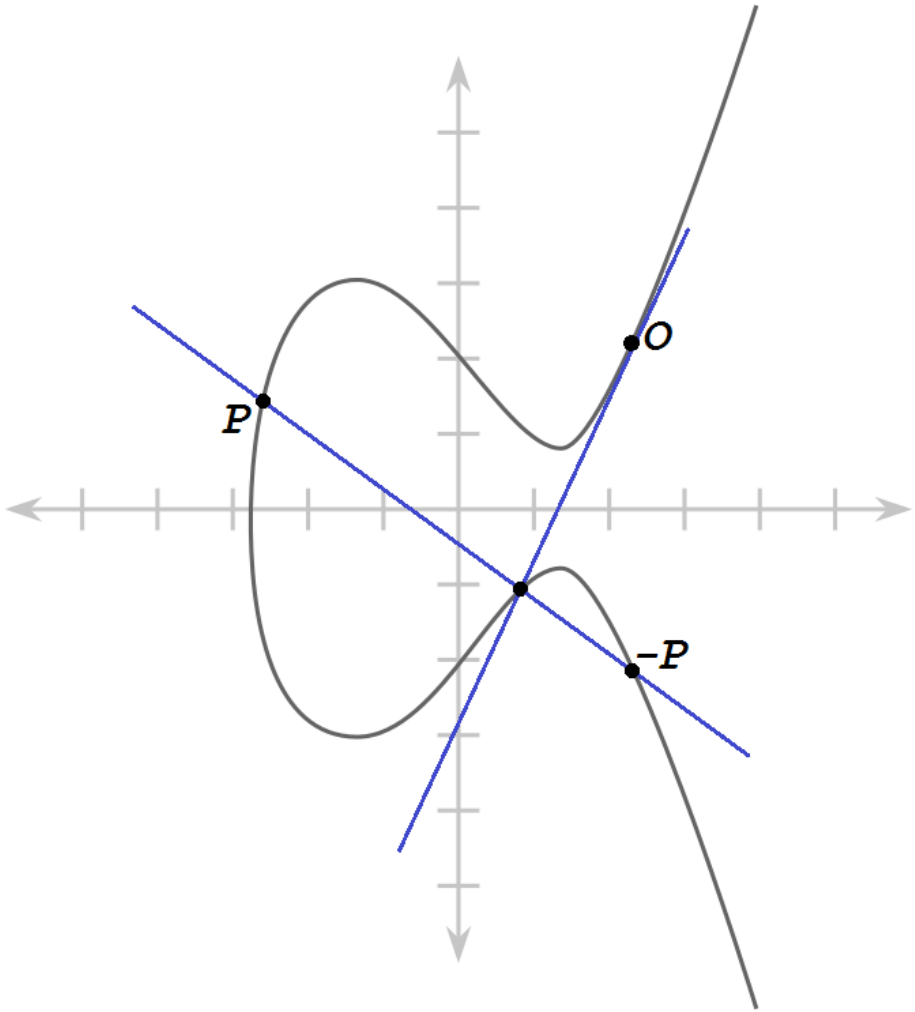


- Сабирање тачака



Слика: Сабирање тачака на кривој

- Тражење инверзног елемента



Слика: Тражење инверзног елемента

Производ група

Директан производ група $(G, *)$ и $(H, \#)$ јесте група $(G \times H, \cdot)$ где је операција $\cdot$ задата координатно, тј. $(a, b) \cdot (c, d) := (a * c, b \# d)$, за $(a, b), (c, d) \in G \times H$.

- Ова дефиниција је добра, тј. $(G \times H, \cdot)$ је заиста група
- Примери: $\mathbb{D}_8 \times \mathbb{S}_{93}$, Клајнова група $V = \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_8 \times \mathbb{Z}_{15} \times \mathbb{Z}_{15}$

Прстени

Дефиниција (Прстен)

Алгебарску структуру $(R, +, \cdot)$ *називамо прстеном ако је:*

- $(R, +)$ *Абелова група*
- $(R \setminus \{e\}, \cdot)$ *асоцијативна (*e *је неутрал за* $+$*)*
- *За све* $a, b, c \in R$ *важи* $(a + b) \cdot c = a \cdot c + b \cdot c$ *и* $c \cdot (a + b) = c \cdot a + c \cdot b$

Ако притом постоји неутрални елемент за $\cdot$ *и* $(R \setminus \{e\}, \cdot)$ *је комутативна, прстен* $(R, +, \cdot)$ *називамо комутативним прстеном са јединицом.*

Примери:

- $(\mathbb{Z}, +, \cdot)$
- $(\mathbb{Z}_n, +_n, \cdot_n)$
- $(\mathbb{Z}_n \times \mathbb{Z}_m, +, \cdot)$

Поља

Дефиниција (Поље)

Алгебарску структуру $(F, +, \cdot)$ *називамо пољем ако је:*

- $(F, +)$ *Абелова група*
- $(F \setminus \{e\}, \cdot)$ *Абелова група (*e *је неутрал за* $+$*)*
- *За све* $a, b, c \in F$ *важи* $(a + b) \cdot c = a \cdot c + b \cdot c$

Еквивалентно, поље је комутативни прстен са јединицом у ком сваки елемент има инверзни у односу на операцију $\cdot$*.*

- Нису примери: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_n, +_n, \cdot_n)$, $(\mathbb{Z}_n \times \mathbb{Z}_m, +, \cdot)$
- Јесу примери: $(\mathbb{Z}_p, +_p, \cdot_p)$, $(\mathbb{Q}, +, \cdot)$, ...

Хвала на пажњи!