

АЛГЕБРА 1

Групе

Директан производ група; Лагранжова теорема

Зоран Петровић

16. новембар 2011.

Један од начина на који од већ постојећих група можемо формирати нове групе је *директан производ група*.

Дефиниција 1 Нека су $(G_1, *_1), (G_2, *_2), \dots, (G_n, *_n)$ групе. Дефинишемо директан производ $(P, *)$ ових група са:

- $P := G_1 \times G_2 \times \dots \times G_n$;
- $(g_1, g_2, \dots, g_n) * (g'_1, g'_2, \dots, g'_n) := (g_1 *_1 g'_1, g_2 *_2 g'_2, \dots, g_n *_n g'_n)$.

Није тешко проверити да је $(P, *)$ заиста група. Наиме, асоцијативност се лако проверава, док је неутрални елемент $e \in P$ дат са:

$$e = (e_1, e_2, \dots, e_n),$$

где је e_i неутрални елемент у групи G_i . Такође је јасно шта је инверзни елемент:

$$(x_1, x_2, \dots, x_n)^{-1} = (x_1^{-1}, x_2^{-1}, \dots, x_n^{-1}).$$

Погледајмо за почетак неке једноставне примере.

Пример 2 Група $\mathbb{Z}_2 \times \mathbb{Z}_3$ је циклична група.

Приметимо најпре да је скуп носач структуре $\mathbb{Z}_2 \times \mathbb{Z}_3$, скуп

$$\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$

Да бисмо показали да је група циклична, морамо наћи елемент, који је генерише, тј. елемент реда 6. Није тешко уверити се да је један такав елемент, елемент $(1, 1)$:

$$\begin{aligned}(1, 1) + (1, 1) &= (1 +_2 1, 1 +_3 1) = (0, 2); \\(1, 1) + (1, 1) + (1, 1) &= (1 +_2 0, 1 +_3 2) = (1, 0); \\(1, 1) + (1, 1) + (1, 1) + (1, 1) &= (1 +_2 1, 1 +_3 0) = (0, 1); \\(1, 1) + (1, 1) + (1, 1) + (1, 1) + (1, 1) &= (1 +_2 0, 1 +_3 1) = (1, 2); \\(1, 1) + (1, 1) + (1, 1) + (1, 1) + (1, 1) + (1, 1) &= (1 +_2 1, 1 +_3 2) = (0, 0).\end{aligned}$$

Остављамо читаоцима да провере да ли је још неки елемент генератор ове групе. ♣

Пример 3 Група $\mathbb{Z}_2 \times \mathbb{Z}_2$ није циклична група.

Скуп носач је скуп $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$. Но, није тешко уверити се да је сваки елемент у овом скупу, осим неутрала, реда 2:

$$\begin{aligned}(0, 1) + (0, 1) &= (0 +_2 0, 1 +_2 1) = (0, 0); \\(1, 0) + (1, 0) &= (1 +_2 1, 0 +_2 0) = (0, 0); \\(1, 1) + (1, 1) &= (1 +_2 1, 1 +_2 1) = (0, 0).\end{aligned}$$

Природно се поставља питање: за које $m, n \geq 2$ је група $\mathbb{Z}_m \times \mathbb{Z}_n$ циклична група? Одговор на ово питање даје следећи став. ♣

Став 4 Група $\mathbb{Z}_m \times \mathbb{Z}_n$ је циклична ако и само ако је $\text{NZD}(m, n) = 1$.

Доказ.

\implies : Претпоставимо да је $\text{NZD}(m, n) = d > 1$. Покажимо да тада група $\mathbb{Z}_m \times \mathbb{Z}_n$ не може бити циклична. Нека је $r = \frac{mn}{d} < mn$. Покажимо да је

$$\underbrace{x + \cdots + x}_r = 0,$$

за све $x \in \mathbb{Z}_m \times \mathbb{Z}_n$. Нека је $x = (s, t)$, произвољан елемент групе $\mathbb{Z}_m \times \mathbb{Z}_n$. Дакле, знамо да је $s \in \{0, 1, \dots, m-1\}$ и $t \in \{0, 1, \dots, n-1\}$ и да важи:

$$\underbrace{s + \cdots + s}_m = 0, \quad \underbrace{t + \cdots + t}_n = 0.$$

Но, тада је

$$\underbrace{s + \cdots + s}_r = \underbrace{\underbrace{(s + \cdots + s)}_m + \cdots + \underbrace{(s + \cdots + s)}_m}_{\frac{n}{d}} = \underbrace{0 + \cdots + 0}_{\frac{n}{d}} = 0,$$

као и

$$\underbrace{t + \cdots + t}_r = \underbrace{\underbrace{(t + \cdots + t)}_n + \cdots + \underbrace{(t + \cdots + t)}_n}_{\frac{m}{d}} = \underbrace{0 + \cdots + 0}_{\frac{m}{d}} = 0.$$

Одавде следи да је

$$\underbrace{(s, t) + \cdots + (s, t)}_r = 0,$$

те је ред сваког елемента у групи $\mathbb{Z}_m \times \mathbb{Z}_n$ највише r , дакле мањи од mn , те група не може бити циклична.

\Leftarrow : Претпоставимо да је $\text{NZD}(m, n) = 1$. Докажимо да је елемент $(1, 1)$ генератор групе $\mathbb{Z}_m \times \mathbb{Z}_n$, тј. да је ред тог елемента једнак mn . Означимо са r ред елемента $(1, 1)$. Дакле,

$$\underbrace{(1, 1) + \cdots + (1, 1)}_r = (0, 0).$$

То значи да је

$$\underbrace{1 + \cdots + 1}_r = 0$$

у групи \mathbb{Z}_m , из чега следи да $m \mid r$, као и

$$\underbrace{1 + \cdots + 1}_r = 0$$

у групи \mathbb{Z}_n , из чега следи да $n \mid r$. Дакле, $\text{NZS}(m, n) \mid r$. Но, како су m и n узајамно прости, то је $\text{NZS}(m, n) = mn$ и закључујемо да $mn \mid r$. Дакле, ред елемента $(1, 1)$ у групи $\mathbb{Z}_m \times \mathbb{Z}_n$ је бар mn те закључујемо да је та група циклична. \square

Напомена: У случају да је група G комутативна, тј. да за све $x, y \in G$ важи: $xy = yx$, уобичајено је за ознаку операције у групи користити ознаку $+$. У том случају ознака mx , где је $m \in \mathbb{Z}$ одговара ознаци x^m . Нпр.

$$6x = \underbrace{x + \cdots + x}_6.$$

Како је свака циклична група реда n изоморфна групи \mathbb{Z}_n , то закључујемо да је директан производ цикличне групе реда m и цикличне групе реда n циклична група (реда mn) ако и само ако су m и n узајамно прости. Приметимо да се у овом тврђењу имплицитно „крије“ следећи резултат: ако је $G \cong G'$ и $H \cong H'$, онда је $G \times H \cong G' \times H'$. Размислите како бисте ово доказали.

Индукцијом није тешко показати да важи следећи резултат. Ако су m_1, m_2, \dots, m_n пар по пар узајамно прости, онда имамо изоморфизам група

$$\mathbb{Z}_{m_1 m_2 \dots m_n} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}.$$

Осим што се конструкција директног производа може искористити за добијање нових група од старих, она се може употребити и за испитивање структуре неке дате групе. Наиме, корисно је знати да је нека група изоморфна директном производу неких других група. У ту сврху користан је следећи став.

Став 5 Нека је G група, а H и K подгрупе групе G за које важи:

1. $G = H \cdot K$;

2. за све $x \in H$ и све $y \in K$: $xy = yx$;

3. $K \cap H = \{e\}$.

Тада је $G \cong H \times K$.

Доказ. Напоменимо најпре да је $H \cdot K = \{h \cdot k : h \in H, k \in K\}$.
Дефинишемо функцију $f : H \times K \rightarrow G$ са:

$$f(h, k) := hk.$$

Докажимо да је f изоморфизам група. Пре свега, како је $G = H \cdot K$, јасно је да је f „на“. Да бисмо доказали да је хомоморфизам, морамо проверити да важи следеће:

$$\text{за све } h, h' \in H \text{ и све } k, k' \in K : f((h, k) \cdot (h', k')) = f(h, k) \cdot f(h', k'),$$

тј. да за све $h, h' \in H, k, k' \in K$:

$$hh'kk' = hkh'k'.$$

Но, како по претпоставци елементи из H и елементи из K међусобно комутирају, то наведена једнакост јесте испуњена.

Остаје да проверимо да је f „1-1“. Претпоставимо да је

$$f(h, k) = f(h', k').$$

То значи да је

$$hk = h'k',$$

односно

$$(h')^{-1}h = k'k^{-1}.$$

Но, како $(h')^{-1}h$ припада подгрупи H , а $k'k^{-1}$ подгрупи K , то смо добили елемент из $H \cap K$, а та подгрупа је тривијална. Закључујемо да мора бити $(h')^{-1}h = e$ и $k'k^{-1} = e$, те следи да је $h = h'$ и $k = k'$, тј. $(h, k) = (h', k')$. \square

Ради илустрације примене ове теореме, урадимо два примера.

Пример 6 $\mathbb{D}_6 \cong \mathbb{D}_3 \times \mathbb{Z}_2$.

Дакле, у групи D_6 треба наћи једну подгрупу изоморфну са \mathbb{D}_3 и једну изоморфну са \mathbb{Z}_2 чији је пресек тривијалан, а елементи међусобно комутирају. Група \mathbb{D}_6 је група симетрија правилног шестоугла, док је групе \mathbb{D}_3 група симетрија једнакостраничног троугла. Где се у правилном шестоуглу „крије“ једнакостранични троугао? Није тешко видети да, ако су темена правилног шестоугла A, B, C, D, E, F , дијагонале AC, CE, EA образују једнакостранични троугао. Ротација шестоугла за угао $2\pi/3$, тј. ротација ρ^2 , јесте симетрија тог троугла. Ако за σ узмемо осну рефлексију око праве која садржи дијагоналу BE ,

онда се лако можемо уверити да је подгрупа $H = \{\varepsilon, \rho^2, \rho^4, \sigma, \sigma\rho^2, \sigma\rho^4\}$, изоморфна групи \mathbb{D}_3 . Ако за групу K узмемо групу генерисану елементом ρ^3 , тј. ако је $K = \{\varepsilon, \rho^3\}$, то лако проверавамо да је $H \cdot K = \mathbb{D}_6$. Осим тога, елемент ρ^3 комутира са свим елементима из H ($\sigma\rho^3 = \rho^{-3}\sigma = \rho^3\sigma$, па заправо ρ^3 комутира са свим елементима из \mathbb{D}_6). Како је $H \cap K = \{\varepsilon\}$, на основу претходног става закључујемо да је $\mathbb{D}_6 \cong H \times K$, тј. $\mathbb{D}_6 \cong \mathbb{D}_3 \times \mathbb{Z}_2$. ♣

Пример 7 Ако је G коначна група чији је сваки елемент сем неутрала реда 2, онда је G изоморфна директном производу цикличних група реда 2.

Докажимо најпре да је група у којој је сваки елемент реда 2 комутативна. Нека су a и b произвољни елементи из G . По претпоставци је $a^2 = e$, $b^2 = e$, $(ab)^2 = e$. Одавде следи да је

$$(ab)^2 = a^2b^2,$$

тј.

$$abab = aabb,$$

што, после скраћивања даје

$$ab = ba.$$

Нека је $x_1 \neq e$ произвољан елемент групе G , различит од неутрала. Посматрајмо подгрупу H_1 генерисану тим елементом. Она је реда 2 пошто је елемент реда x_1 реда 2. Уколико је $H_1 = G$, доказ је завршен. У супротном, изаберимо елемент $x_2 \in G \setminus H_1$ и нека је $K_2 = \langle x_2 \rangle$. Тада је $H_2 = H_1 \cdot K_2 = \{e, x_1, x_2, x_1x_2\}$ једна подгрупа групе G (проверите!). Подгрупе H_1 и K_2 испуњавају услове претходног става (зашто?), те добијамо да је $H_2 \cong H_1 \times K_2$. Уколико је $H_2 = G$, доказ је завршен. У супротном, бирамо елемент $x_3 \in G \setminus H_2$ и посматрамо подгрупу $K_3 = \langle x_3 \rangle$. Као и у претходном случају $H_3 = H_2 \cdot K_3$ је подгрупа групе G и $H_3 \cong H_2 \times K_3 \cong H_1 \times K_2 \times K_3$. Овакав поступак мора се завршити пошто је група G коначна, а $|H_k| = 2^k$. Стога добијамо да је за неко n испуњено $G \cong H_1 \times K_2 \times \cdots \times K_n$, а сви ови фактори су цикличне групе реда 2. ♣

Подсетимо се да смо увели појам реда групе и реда елемента. У случају цикличне групе, ред саме групе једнак је реду елемента који генерише ту групу. Природно је поставити питање о вези између реда елемента и реда коначне групе и у случају да група није циклична. Још општије, каква је веза између реда коначне групе и реда неке њене подгрупе? Испоставља се да је одговор једноставан и сада ћемо се тиме позабавити.

Дефиниција 8 Ако је $H \leq G$ и $x \in G$, скуп

$$xH = \{x \cdot h : h \in H\},$$

назива се леви косет подгрупе H у групи G . Аналогно, скуп

$$Hx = \{h \cdot x : h \in H\},$$

назива се десни косет.

Како $e \in H$, косет xH (Hx) садржи елемент x . У општем случају $xH \neq Hx$. Нпр. ако је $G = \mathbb{D}_3$ и $H = \{\varepsilon, \sigma\}$, онда је

$$H\rho = \{\rho, \sigma\rho\} \neq \{\rho, \rho\sigma\} = \rho H,$$

пошто је $\rho\sigma = \sigma\rho^2$. Скуп свих левих косета подгрупе H у G означаваћемо са G/H , а свих десних косета са $H \backslash G$. Као што смо видели, леви косет, који садржи елемент x , не мора бити једнак десном косету који садржи тај елемент, па је у општем случају $G/H \neq H \backslash G$. У наредним лекцијама видећемо када су ови скупови једнаки, али то је друга прича. За сада само можемо да закључимо да постоји бијекција између њих која левом косету xH придружује десни косет Hx .

Став 9 Важи следеће:

1. $xH = yH$ ако и само ако је $x^{-1}y \in H$;
2. ако је $xH \neq yH$, онда је $xH \cap yH = \emptyset$.

Доказ.

1. \implies : Претпоставимо да је $xH = yH$. То посебно значи да $y \in xH$, тј. постоји $h \in H$ за који је $y = xh$. Но, тада је $h = x^{-1}y$, па закључујемо да $x^{-1}y \in H$.

\impliedby : Нека $x^{-1}y \in H$. Претпоставимо да $z \in xH$. Дакле, $z = xh$, за неко $h \in H$. Тада је $z = x(x^{-1}y)(x^{-1}y)^{-1}h = y((x^{-1}y)^{-1}h)$, но, како је H подгрупа од G и $x^{-1}y \in H$, то и $(x^{-1}y)^{-1}h \in H$, па закључујемо да $z \in yH$. Обратно, ако $z \in yH$, онда постоји $h' \in H$, такав да је $z = yh'$. Тада је $z = x((x^{-1}y)h')$, а како је $x^{-1}y \in H$ и како је H подгрупа од G , то $z \in xH$. Закључујемо да је $xH = yH$ уколико $x^{-1}y \in H$.

2. Претпоставимо да је $xH \cap yH \neq \emptyset$. То значи да за неке $h, h' \in H$ важи: $xh = yh'$. Одавде следи да је $x^{-1}y = h(h')^{-1}$, а како је $H \leq G$, то $h(h')^{-1} \in H$. На основу претходно доказаног, следи да је $xH = yH$. \square

Дакле, различити леви косети ма које подгрупе H су дисјунктни. Како сваки елемент x лежи у косету xH , то закључујемо да важи следећи став.

Став 10 Нека је G група и $H \leq G$. Тада је G дисјунктна унија различитих левих косета подгрупе H .

Дефиниција 11 Уколико је скуп левих косета G/H бесконачан, кажемо да је подгрупа H бесконачног индекса у групи G . Уколико је тај скуп коначан, онда се индекс подгрупе H у групи G , у ознаци $[G : H]$, дефинише као број елемената у G/H , тј. $[G : H]$ је број различитих левих косета подгрупе H у групи G .

Напомена: Како постоји бијекција између G/H и $H \backslash G$, то је $[G : H]$ такође и број различитих десних косета H у G . Осим тога, бесконачна група може садржати подгрупе коначног индекса. На пример, подгрупа од \mathbb{Z} генерисана елементом 3 је индекса 3 (проверити ово).

Теорема 12 (Лагранжова теорема) Нека је G коначна група и $H \leq G$. Тада је

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

Посебно, ред подгрупе H , дели ред групе G .

Доказ. Како је група G коначна, то је очигледно G коначна унија левих косета подгрупе H , тј. за неке $x_1, \dots, x_k \in G$ важи:

$$G = x_1H \sqcup x_2H \sqcup \dots \sqcup x_kH,$$

при чему је $k = [G : H]$. Но, $|xH| = |yH|$ за све $x, y \in G$. Наиме, функција $f: xH \rightarrow yH$ дефинисана са: $f(xh) = yh$ задаје бијекцију између ова два скупа (проверите ово). Стога је $|G| = |H| \cdot k = |H| \cdot [G : H]$. \square

Наведимо неке последице Лагранжове теореме.

Последица 13 Ред сваког елемента коначне групе дели ред те групе.

Доказ. Нека је G коначна група и $x \in G$. Јасно је да ред елемента x мора бити коначан. Осим тога, $\omega(x) = |\langle x \rangle|$, а према Лагранжовој теореме $|\langle x \rangle| \mid |G|$. \square

Последица 14 Свака група простог реда је циклична.

Доказ. Нека је $|G| = p$, где је p прост број. Ако је x било који елемент из G различит од неутрала, онда је $\omega(x) \neq 1$ и $\omega(x) \mid p$. Закључујемо да је $\omega(x) = p$, те је $\langle x \rangle = G$. \square

Последица 15 Ако је G коначна група и $x \in G$, онда је $x^{|G|} = e$.

Доказ. Присетимо се да је $x^m = e$ ако и само ако $\omega(x) \mid m$. Како $\omega(x) \mid |G|$, резултат следи. \square

У скупу $Z_n = \{0, 1, \dots, n-1\}$, где је $n \geq 2$ можемо увести операцију \cdot_n (множење по модулу n). Наравно, у односу на ову операцију Z_n не чини групу. Посматрајмо стога следећи скуп.

$$\Phi(n) := \{k : 1 \leq k < n, \text{NZD}(k, n) = 1\}.$$

Важи следећи став.

Став 16 За све $n \geq 2$, $(\Phi(n), \cdot_n)$ је комутативна група.

Доказ. Најпре треба проверити да ли множење по модулу n заиста задаје бинарну операцију на скупу $\Phi(n)$, тј. да ли је испуњено следеће:

ако $x, y \in \Phi(n)$ онда $x \cdot_n y \in \Phi(n)$.

Уколико је $\text{NZD}(x, n) = 1 = \text{NZD}(y, n)$, онда је и $\text{NZD}(x \cdot y, n) = 1$. Наиме, добро нам је познато следеће:

$\text{NZD}(a, b) = 1$ **ако** постоје $p, q \in \mathbb{Z}$ тако да је $ap + bq = 1$.

Дакле, постоје $p, q \in \mathbb{Z}$ за које је $xp + nq = 1$, као и $p', q' \in \mathbb{Z}$ за које је $yp' + nq' = 1$. Множењем ове две релације, добијамо да је

$$xy(pp') + n(qyp' + xpq' + nqq') = 1,$$

те мора бити $\text{NZD}(x \cdot y, n) = 1$. С обзиром да је

$$x \cdot y \equiv x \cdot_n y \pmod{n},$$

то је и $\text{NZD}(x \cdot_n y, n) = 1$.

Познато нам је да је операција \cdot_n асоцијативна и комутативна. Осим тога, $1 \in \Phi(n)$, па постоји и неутрални елемент за ову операцију. Но, сваки елемент из $\Phi(n)$ заиста има инверз. Наиме, ако $x \in \Phi(n)$, онда постоје $p, q \in \mathbb{Z}$ за које је $xp + nq = 1$. Ако са \bar{p} означимо елемент из Z_n , који је конгруентан елементу p по модулу n , онда је $\bar{p} \in \Phi(n)$ и осим тога је $x \cdot_n \bar{p} = 1$. \square

Ред групе $\Phi(n)$ означавамо са $\varphi(n)$. Ова функција φ зове се Ојлерова функција.

Последица 17 (Ојлерова теорема) Нека је $n \geq 2$ и x цео број, узајамно прост са n , онда је

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Доказ. Како је x узајамно прост са n , то је x конгруентан по модулу n неком броју $\bar{x} \in \Phi(n)$. Но, $|\Phi(n)| = \varphi(n)$ и на основу Последице ?? знамо да у групи $\Phi(n)$ важи једнакост $\bar{x}^{\varphi(n)} = 1$. То заправо значи да је $x^{\varphi(n)}$ конгруентно са 1 по модулу n . \square

У случају да је p прост број, очигледно је да је $\varphi(p) = p - 1$. Стога добијамо још једну последицу Лагранжове теореме.

Последица 18 (Мала Фермаова теорема) Ако је p прост број, који не дели цео број x , онда је

$$x^{p-1} \equiv 1 \pmod{p}.$$