АЛГЕБРА 1

Групе

Групе пермутација

Зоран Петровић

30. октобар 2012.

У овој лекцији обрађујемо веома значајан пример групе — групу пермутација (групу симетрија).

Дефиниција 1 Нека је X непразан скуп. Посматрајмо скуп S_X задат са:

$$S_X = \{\pi \colon X \to X \mid \pi \text{ је бијекција } \}.$$

Тада је $\mathbb{S}_X = (S_X, \circ)$, где је са $\circ$ означена операција композиције функција, једна група и зовемо је групом пермутација скупа X.

Елементе групе $\mathbb{S}_X$ зовемо и пермутацијама скупа X. Ако постоји бијекција између X и Y, онда су одговарајуће групе пермутација изоморфне.

Став 2 Ако постоји бијекција између X и Y, онда је $\mathbb{S}_X \cong \mathbb{S}_Y$.

Доказ. Нека је $g \colon X \to Y$ бијекција. Дефинишимо $f \colon S_X \to S_Y$ са:

$$f(\pi) := g \circ \pi \circ g^{-1}.$$

Јасно је да је $g \circ \pi \circ g^{-1}$ једна пермутација скупа Y уколико је π пермутација скупа X. Осим тога, ако је $\sigma \in S_Y$, онда је $f(g^{-1} \circ \sigma \circ g) = \sigma$, те је f „на". Јасно је да је f и „1–1". Треба само проверити да је $f(\rho \circ \pi) = f(\rho) \circ f(\pi)$, уколико $\rho, \pi \in S_X$. Учинимо то:

$$f(\rho \circ \pi) = g \circ (\rho \circ \pi) \circ g^{-1} = (g \circ \rho \circ g^{-1}) \circ (g \circ \pi \circ g^{-1}) = f(\rho) \circ f(\pi).$$

Дакле, f заиста успоставља изоморфизам између $\mathbb{S}_X$ и $\mathbb{S}_Y$. □

Уколико је $X = \{1, 2, \ldots, n\}$, онда уместо $\mathbb{S}_{\{1,2,\ldots,n\}}$ пишемо краће $\mathbb{S}_n$. На основу претходног става, свака коначна група пермутација неког скупа изоморфна је једној од група $\mathbb{S}_n$. Стога се сада концентришемо на групу $\mathbb{S}_n$.

Почнимо једним примером. Нека је $n = 9$ и пермутација $\sigma \in \mathbb{S}_9$ задата је са:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 3 & 8 & 2 & 7 & 1 & 6 & 9 \end{pmatrix}.$$

Можемо ли ову пермутацију некако једноставније записати? Елемент 1 слика се у 4, 4 у 8, 8 у 6, 6 у 7, а 7 у 1. Некако смо „затворили круг":

$$1 \mapsto 4 \mapsto 8 \mapsto 6 \mapsto 7 \mapsto 1.$$

Запишимо то овако: (14867). Прецизније, (14867) означава пермутацију скупа $\{1, 2, \ldots, 9\}$ у којој се 1 слика у 4, 4 у 8, 8 у 6, 6 у 7, а 7 у 1, док се остали елементи сликају сами у себе. Како се остали елементи не појављују у овом запису, а сликају се сами у себе, то се (14867) може видети и као елемент групе S_n за ма које $n \geqslant 8$. Оваква пермутација назива се циклус или цикл дужине 5. Пермутација у којој

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_{k-1} \mapsto a_k \mapsto a_1,$$

при чему су елементи a_i различити, означава се са $(a_1 a_2 \ldots a_k)$, зове се циклус дужине k (или k-цикл).

Вратимо се пермутацији σ. Први елемент који нисмо „покупили" до сада је елемент 2. Видимо да

$$2 \mapsto 5 \mapsto 2.$$

Дакле, добијамо нови цикл (25), који је дужине 2. Цикли дужине 2 зову се и транспозиције (само два елемента замене своја места). Видимо да се преостали елементи 3 и 9 не померају при пермутацији σ: $3 \mapsto$, односно $9 \mapsto 9$. То се може записати и у облику циклуса дужине 1: (3), односно (9). Но, то су, по нашој дефиницији, заправо идентичне пермутације (3 се слика у 3, а остали такође сами у себе!), те их често и не пишемо. Проверимо да ли је

$$\sigma = (14867)(25).$$

Овде треба напоменути да знак за композицију $\circ$ најче71е нећемо писати. Осим тога, подсетимо читаоца да су ово функције, те ова ознака значи да прво делује (25), а потом (14867). Није тешко проверити да горња једнакост заиста важи. Овако смо нашу пермутацију приказали о облику производа дисјунктних циклуса (циклуси $(a_1 a_2 \ldots a_k)$ и $(b_1 b_2 \ldots b_l)$ су дисјунктни уколико су $\{a_1, a_2, \ldots, a_k\}$ и $\{b_1, b_2, \ldots, b_l\}$ дисјунктни скупови). Заправо важи следећа теорема.

Теорема 3 Свака пермутација из $\mathbb{S}_n$ може се на јединствен начин, до на редослед фактора, представити у облику производа дисјунктних циклуса.

Ову теорему нећемо доказивати. Приметимо да важи следеће. Уколико су циклуси ρ и π дисјунктни, онда је $\rho\pi = \pi\rho$. То није тешко директно проверити анализирајући где се сликају поједини елементи.

Уколико пак циклуси нису дисјунктни, они не морају да комутирају:

$$(12)(23) = (123), \quad (23)(12) = (132).$$

Приметимо да је

$$(a_1 a_2 \dots a_k) = (a_2 \dots a_k a_1) = \dots = (a_k \dots a_1 a_2 \dots a_{k-1}).$$

У конкретном случају $k = 4$:

$$(a_1 a_2 a_3 a_4) = (a_2 a_3 a_4 a_1) = (a_3 a_4 a_1 a_2) = (a_4 a_1 a_2 a_3).$$

У вези са овим, природно се поставља питање колико у S_n има различитих циклуса дужине k, где је $k \leqslant n$. На то питање није тешко одговорити. Наиме, најпре је потребно из скупа од n елемената изабрати њих k. То се може извести на $\binom{n}{k}$ начина. Ти елементи се међусобно могу поређати у циклус дужине k на $k!$ начина. Но, видели смо да неке од тих пермутација заправо задају исти циклус. Прецизније, од датих k елемената може се формирати $\frac{k!}{k} = (k-1)!$ различитих циклуса. Дакле, различитих циклуса дужине k у S_n има $\binom{n}{k}(k-1)! = \frac{n(n-1)\cdots(n-k+1)}{k}$. Наравно, ово се може доказати и на друге начине. Размислите како.

Позабавимо се мало рачунањем са циклусима. Најпре, лако је проверити да је, ако су a, b, c међусобно различити, $(ab)(bc) = (abc)$. Општији резултат је следећи. Ако су $a_1, a_2, \dots, a_{k+l}$ међусобно различити онда је:

$$(a_1 a_2 \dots a_k)(a_k a_{k+1} \dots a_{k+l}) = (a_1 a_2 \dots a_{k+l}),$$

за све $k \geqslant 2, l \geqslant 1$. Користећи овај резултат, лако се показује да је сваки циклус производ транспозиција:

$$(a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k) = (a_1 a_2 \dots a_k).$$

Како је свака пермутација производ циклуса то закључујемо да важи следећи став.

Став 4 Свака пермутација из $\mathbb{S}_n$ може се представити у облику производа транспозиција.

Овде треба истаћи да представљање није јединствено. Нпр.

$$(12)(23)(34) = (14)(13)(12).$$

Оно што јесте јединствено је парност броја транспозиција које се појављују у факторизацији дате пермутације. Тај резултат такође нећемо доказивати. Укажимо само да пермутације које се могу представити у облику производа парног броја транспозиција зовемо парне пермутације, док се пермутације које се представљају у облику непарног броја транспозиција зову непарне пермутације. Скуп свих парних пермутација означава се са $\mathbb{A}_n$ и важи следећи став.

Став 5 За свако $n \geqslant 2$ је $\mathbb{A}_n \leqslant \mathbb{S}_n$ и $|\mathbb{A}_n| = \frac{n!}{2}$.

Доказ. Како је идентична пермутација очигледно парна (зашто?), то је $A_n \neq \emptyset$. Осим тога, ако су σ и π парне пермутације, то је и $\sigma\pi^{-1}$ парна пермутација. Наиме, ако је $\sigma = \tau_1\tau_2\cdots\tau_{2k}$, а $\pi = \phi_1\phi_2\cdots\phi_{2l}$, представљање ових пермутација у облику производа парног броја транспозиција то је $\sigma\pi^{-1} = \tau_1\tau_2\cdots\tau_{2k}\phi_{2l}\cdots\phi_2\phi_1$ представљање у облику производа парног броја транспозиција (појаснити ову последњу једнакост). Стога закључујемо да је $\mathbb{A}_n$ заиста подгрупа групе $\mathbb{S}_n$.

Да бисмо одредили ред подгрупе $\mathbb{A}_n$, изаберимо било коју транспозицију τ. Тада можемо дефинисати функцију $\Phi\colon A_n \to S_n \setminus A_n$ са: $\Phi(\pi) := \tau\pi$. Није тешко уверити се да је Φ бијекција. Резултат одавде следи (проверити да је Φ бијекција и објаснити како се добија тражени резултат). □

Ако је $\pi \in \mathbb{S}_n$ и $(a_1a_2\ldots a_k)$ један k-цикл тада је

$$\pi(a_1a_2\ldots a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)\ldots\pi(a_k)).$$

Ово се лако може проверити. Споменимо узгред да је

$$(a_1a_2\ldots a_k)^{-1} = (a_ka_{k-1}\ldots a_1).$$

Видели смо да је група $\mathbb{S}_n$ генерисана транспозицијама. То је прилично велики генераторни скуп. Заправо се могу наћи знатно једноставнији скупови генератора за $\mathbb{S}_n$.

Став 6 Група $\mathbb{S}_n$ генерисана је:

1. транспозицијама $(12), (13), \ldots, (1n)$;
2. транспозицијама $(12), (23), (34), \ldots (n-1, n)$;
3. пермутацијама (12) и $(123\ldots n)$.

Доказ.
1. Лако се може проверити да је $(ab) = (1a)(1b)(1a)$. Дакле, све транспозиције се могу добити помоћу наведених.

2. Довољно је показати да можемо да добијемо све транспозиције облика $(1a)$ за $2 \leqslant a \leqslant n$. Наравно, (12) је већ на списку! Ево како добијамо (13):

$$(13) = (12)(23)(12).$$

Сада када имамо (13) није тешко добити и (14):

$$(14) = (13)(34)(13).$$

Уочавамо правилност:

$$(1, k+1) = (1k)(k, k+1)(1k).$$

На овај начин добијамо све транспозиције за које знамо да генеришу $\mathbb{S}_n$. Стога и почетне транспозиције генеришу $\mathbb{S}_n$.

3. Подсетимо се формуле: $\pi(a_1 \dots a_k)\pi^{-1} = (\pi(a_1) \dots \pi(a_k))$ (**веома** пажљив читалац је можда приметио да се ова формула крије и у идентитету $(13) = (12)(23)(12)$). Уколико је $\pi = (12 \dots n)$ добијамо

$$(12 \dots n)(12)(12 \dots n)^{-1} = (23).$$

Када смо добили (23), није нам тешко да добијемо и (34):

$$(12 \dots n)(23)(12 \dots n)^{-1} = (34).$$

Уочавамо правилност:

$$(12 \dots n)(k, k+1)(12 \dots n)^{-1} = (k+1, k+2),$$

за $1 \leqslant k \leqslant n-2$. Тако добијамо све транспозиције за које знамо да генеришу $\mathbb{S}_n$, па према томе закључујемо да и дате две пермутације такође генеришу $\mathbb{S}_n$. □

Приметимо да парност k-цикла зависи од k. Заправо је k-цикл парна пермутација ако и само ако је k непаран (погледајте како смо k-цикл представили у облику производа транспозиција). То посебно значи да је сваки цикл дужине три (трицикл!) једна парна пермутација. Важи следећи став.

Став 7 Ако је $n \geqslant 3$, онда је $\mathbb{A}_n$ генерисана циклусима дужине 3.

Доказ. Ово заправо није тешко доказати. Уколико је $n = 3$ и немамо шта да доказујемо. Наиме, $\mathbb{S}_3 = \{(1), (12), (13), (23), (123), (132)\}$ ((1) представља идентичну пермутацију). Дакле, овде је заправо $A_3 = \{(1), (123), (132)\}$. Претпоставимо стога да је $n \geqslant 4$. Како је, према претходном ставу, скуп $\{(12), (13), \dots, (1n)\}$ један скуп генератора групе S_n, то се и сваки елемент из A_n може представити у облику производа ових елемената. Но, како је у питању елемент из A_n, он је представљен у облику производа парног броја таквих транспозиција. Групишући их две по две, добијамо да је довољно да покажемо да се пермутације облика $(1a)(1b)$, где је $a \neq b$ могу представити у облику производа циклуса дужине 3. Но, заправо је $(1a)(1b) = (a1)(1b) = (a1b)$! Дакле, то је већ циклус дужине 3. Овим је доказ завршен. □

Позабавимо се сада питањем одређивања реда елемената из S_n. Директном провером се добија да је $\omega((a_1 \dots a_k)) = k$. Како се свака пермутација може представити у облику производа дисјунктних циклуса, то би морало бити корисно за одређивање реда произвољне пермутације. Доказаћемо један општи став.

Став 8 Нека је G произвољна група и $a, b \in G$ такви да је:

1. $\omega(a) = m$, $\omega(b) = n$;
2. $ab = ba$;
3. $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Тада је $\omega(ab) = \text{NZS}(m, n)$.

Доказ. Како је $ab = ba$, то је за сваки $k \in \mathbb{N}$: $(ab)^k = a^k b^k$. То се лако доказује индукцијом (докажите то за вежбу!). Ради краћег записа уведимо ознаке: $s = \omega(ab)$, $t = \text{NZS}(m, n)$. Осим тога, $t = mt_1 = nt_2$. Како је

$$(ab)^t = a^t b^t = a^{mt_1} b^{nt_2} = (a^m)^{t_1} (b^n)^{t_2} = e^{t_1} e^{t_2} = e,$$

то добијамо $s \mid t$.

С обзиром да је $s = \omega(ab)$,

$$e = (ab)^s = a^s b^s.$$

Добијамо да је $a^s = (b^s)^{-1}$. Но, $a^s \in \langle a \rangle$, а $(b^s)^{-1} \in \langle b \rangle$ те смо добили елемент из пресека $\langle a \rangle \cap \langle b \rangle$. Како је овај пресек тривијалан, мора бити $a^s = e$ и $(b^s)^{-1} = e$, тј. $b^s = e$. Но, с обзиром на то да је $m = \omega(a)$ и $n = \omega(b)$, следи да $m \mid s$ и $n \mid s$. Имајући у виду да је $t = \text{NZS}(m, n)$, добијамо да $t \mid s$. Закључујемо да је $s = t$. □

Из овог резултата можемо добити две последице.

Последица 9 Ако су σ и τ дисјунктни циклуси из $\mathbb{S}_n$, онда је $\omega(\sigma\tau) = \text{NZS}(\omega(\tau), \omega(\sigma))$.

Доказ. Да бисмо применили претходни став, довољно је показати да је $\langle \tau \rangle \cap \langle \sigma \rangle = \{(1)\}$. Претпоставимо да је $\pi \in \langle \tau \rangle \cap \langle \sigma \rangle$. Нека је $\sigma = (a_1 \dots a_k)$, а $\tau = (b_1 \dots b_l)$. Нека је $i \in \{1, \dots, n\}$ произвољан елемент. Ако $i \notin \{a_1, \dots, a_k\}$, с обзиром да је $\pi = \sigma^s$, за неко s, мора бити $\pi(i) = i$. Ако пак $i \in \{a_1, \dots, a_k\}$, онда $i \notin \{b_1, \dots, b_l\}$, те с обзиром да је $\pi = \tau^t$, за неко t, мора бити $\pi(i) = i$. Закључујемо да је π идентична пермутација, те је пресек тривијалан. □

Следећи резултат је генерализација претходног.

Последица 10 Ако је $\pi = \sigma_1 \cdots \sigma_k$ представљање пермутације π у облику производа дисјункних циклуса, онда је $\omega(\pi) = \text{NZS}(\omega(\sigma_1), \dots, \omega(\sigma_k))$.

Искористимо управо доказано на једном примеру.

Пример 11 а) Испитати да ли у $\mathbb{S}_7$ постоји елемент реда 12.

б) Испитати да ли у $\mathbb{S}_7$ постоји елемент реда 8.

а) Елемент $(1234)(567)$ је на основу претходних резултата реда 12.
б) Питање се своди на следеће. Да ли број 8 може бити најмањи заједнички садржалац бројева мањих од њега? Да то није могуће, може се проверити једноставном анализом. Остављамо читаоцима да се у то убеде.

Ми смо се до сада бавили цикличним, диедарским и групама пермутација. Да ли се можда неке од ових група подударају? Није тешко видети да су групе $\mathbb{S}_2$ и $\mathbb{A}_3$ цикличне групе (реда 2 односно 3). Много је занимљивија следећа чињеница:

$$\mathbb{D}_3 \cong \mathbb{S}_3.$$

Наиме, група $\mathbb{D}_3$ је група симетрија једнакостраничног троугла. Означимо темена тог троугла бројевима 1, 2 и 3. Свака симетрија троугла индукује једну пермутацију скупа свих темена, а тиме и скупа $\{1, 2, 3\}$. Није тешко уверити се која пермутација одговара којој симетрији троугла. Препоручујемо читаоцима да нацртају цртеж и сами одреде наведене симетрије. Такође за вежбу остављамо да читаоци сами покажу да ниједна од група $\mathbb{S}_n$, $\mathbb{D}_n$, за $n \geqslant 3$, није циклична.

Размотримо два занимљива примера из геометрије.

Пример 12 Група ротационих симетрија правилног тетраедра изоморфна је групи $\mathbb{A}_4$.

И овде је добро темена тетраедра нумерисати бројевима од 1 до 4. Свака ротациона симетрија индукује пермутацију скупа темена. Тако добијамо функцију из групе симетрија тетраедра у групу $\mathbb{A}_4$ (уверите се да добијамо само парне пермутације). Но, та функција не само да је бијекција, него је и изоморфизам, пошто је у оба случаја операција у групи заправо композиција пресликавања. ♣

Пример 13 Група ротационих симетрија коцке изоморфна је групи $\mathbb{S}_4$.

Размотримо најпре колико има ротационих симетрија коцке. Како коцка има 6 страна, то за сваки пар страна постоје по три нетривијалне ротације коцке око оса које пролазе кроз центре наспрамних страна. Ротације су за $\pi/2$, π и $3\pi/2$. Тако добијамо 9 ротација.

Коцка има и 4 дијагонале и око сваке дијагонале постоје две нетривијалне ротације — за углове од $2\pi/3$ и $4\pi/3$. Дакле, добијамо још 8 ротација.

Коцка има и 12 ивица. Постоји 6 ротација за π око оса које пролазе кроз средишта наспрамних ивица коцке.

Укупно смо добили $9+8+6+1 = 24$ ротације (додали смо и идентичну трансформацију).

Свака од ротација пермутује дијагонале коцке. Тако се свака ротација може видети и као пермутација скупа од 4 елемента. Све оне

су различите, а има их 24 колико и елемената групе $\mathbb{S}_4$. С обзиром да су у оба случаја групне операције композиција функција добијамо да је тражена група симетрија изоморфна групи $\mathbb{S}_4$. Препоручујемо читаоцима да детаљније проуче овај пример и провере које ротације одговарају којим елементима из $\mathbb{S}_4$. ♣

За крај ове лекције докажимо једну једноставну, али веома важну теорему, која показује зашто групе пермутација имају значајно место у теорији група.

Теорема 14 (Кејлијева теорема) Свака група G изоморфна је некој подгрупи групе $\mathbb{S}_G$.

Доказ. Ако је $g \in G$, са $L_g: G \to G$ означимо бијекцију дефинисану са:

$$L_g(x) := g \cdot x.$$

Јасно је да је L_g бијекција пошто је $L_g \circ L_{g^{-1}} = \mathrm{id}_G (= L_e)$. Дакле, $(L_g)^{-1} = L_{g^{-1}}$. Осим тога:

$$L_g \circ L_h = L_{g \cdot h}.$$

Дакле, видимо да је $G' = \{L_g : g \in G\}$ једна подгрупа групе $\mathbb{S}_G$.

Функција $f: G \to G'$ дефинисана са $f(g) = L_g$ остварује изоморфизам између G и G'. □

У случају да је група коначна добијамо следећу последицу.

Последица 15 Свака коначна група реда n изоморфна је некој подгрупи групе $\mathbb{S}_n$.