0.1 Алгебарске операције и структуре

0.1.1 Дефиниција операције и основни примери

Дефиниција 0.1. Нека је A било који непразан скуп. *Операција дужине* n на скупу A је свако пресликавање $f : A^n \to A$, где је $A^n = A \times \cdots \times A$ n-ти Декартов степен скупа A, односно скуп свих уређених n-торки са компонентама из A.

Пример 0.1. $f(m, n, l) = 2mn + 7l$ је операција дужине 3 на скупу природних бројева.

Операције дужине 2 зову се *бинарне*.

Дефиниција 0.2. *Бинарна операција* на непразном скупу A је свако пресликавање $* : A^2 \to A$, којим се произвољном пару (a, b) елемената из скупа A придружује елемент тог истог скупа.

Уместо $*(a, b)$ писаћемо $a * b$.

Пример 0.2. 1) Операције сабирања и множења природних бројева су примери бинарних операција. Те операције су дефинисане и на скуповима целих, рационалних, реалних и комплексних бројева.

2) $\cup, \cap, \setminus, \triangle$ дефинисане на партитивном скупу $\mathcal{P}(X)$ непразног скупа X

3) Сабирање и множење полинома са реалним (рационалним, комплексним) коефицијентима 4) Сабирање и множење квадратних матрица са реалним (рационалним, комплексним) компонентама

5) Нека је n фиксиран природан број. Означимо са $\mathbb{Z}_n$ скуп свих остатака при еуклидском дељењу са n: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. На овом скупу уводимо две бинарне операције, сабирање и множење по модулу n:

$$r +_n s = rest(r + s, n), \quad r \cdot_n s = rest(r \cdot s, n),$$

при чему је $rest(m, n)$ остатак који број m даје при еуклидском дељењу са n.

Операције дужине 1 зову се *унарне*.

Дефиниција 0.3. *Унарна операција* на непразном скупу A је свако пресликавање $A \to A$.

Унарне операције најчешће означавамо са $-a$, a^{-1} или a'.

Пример 0.3. $a \mapsto -a$ је операција дужине 1 на скупу $\mathbb{Z}$;
$a \mapsto \frac{1}{a}$ је операција дужине 1 на скупу $\mathbb{Q} \setminus \{0\}$.

Дефиниција 0.4. *Нуларна операција* или операција дужине 0 на непразном скупу A је издвајање неког елемента скупа A.

Операције дужине 0 често се зову *константе*.

Пример 0.4. 0 је операција дужине 0 (константа) на скупу $\mathbb{Z}$;
1 је операција дужине 0 на скупу $\mathbb{Q} \setminus \{0\}$.

Алгебарски закони

Алгебарски закон или идентитет је једнакост два алгебарска израза (који се праве помоћу симбола промењивих, константи и операцијских знакова неког алгебарског језика). На пример, закони асоцијативности и комутативности за бинарну операцију $*$ гласе:
асоцијативност $(a * b) * c = a * (b * c)$ за свако $a, b, c \in A$;
комутативност $a * b = b * a$, $a, b \in A$.
(Алгебарска теорија неког алгебарског језика је сваки скуп идентитета тог језика, а алгебарски варијетет те теорије је класа свих алгебри тог језика које задовољавају све законе те теорије.)

Ако су на скупу A дефинисане две бинарне операције које ћемо означити са $+$ и $\cdot$, за $\cdot$ кажемо да је *дистрибутивна* у односу на $+$ ако важи
$(a + b) \cdot c = a \cdot c + b \cdot c$ и $c \cdot (a + b) = c \cdot a + c \cdot b$ за свако $a, b, c \in A$.

Пример 0.5. Сва сабирања која смо навели као примере бинарних операција су асоцијативна, а то важи и за сва множења. Од скуповних операција асоцијативне су унија, пресек и симетрична разлика, док обична разлика није.

Пример 0.6. Сва сабирања која смо навели као примере бинарних операција су комутативна. Такође, сва множења, осим множења квадратних матрица, су комутативна. Од скуповних операција комутативне су унија, пресек и симетрична разлика, док обична разлика није.

Пример 0.7. Операција $a \circ b = b$ дефинисана у скупу природних бројева јесте асоцијативна, а није комутативна. $m * n = m^3 + n^3$ дефинисана у скупу природних бројева јесте комутативна, а није асоцијативна.

Пример 0.8. Сва множења која смо навели су дистрибутивна у односу на одговарајућа сабирања (у скуповима природних, целих, рационалних, реалних и комплексних бројева; у скупу остатака по модулу n; у скуповима полинома са целим, рационалним, реалним и комплексним коефицијентима; у скупу квадратних матрица са целим, рационалним, реалним и комплексним компонентама). Такође, пресек је дистрибутиван у односу на унију, а важи и обрнуто.

Пример 0.9. Ако су $m * n = m + 7n$, а $m \circ n = 7mn$ операције у скупу природних бројева, $\circ$ је дистрибутиван према $*$.

Подоперације

Дужина неке операције зове се њен *тип*.

Дефиниција 0.5. За операцију g на скупу B кажемо да је *подоперација* операције f на скупу A ако важи: 1) $B \subset A$ 2) операције f и g су истог типа 3) операције f и g се подударају на скупу B.

Посебно, подоперација бинарне операције $* : A^2 \to A$ је операција $\circ : B^2 \to B$ за коју је $B \subset A$ и $a \circ b = a * b$, за све $a, b \in B$. То значи да њен скуп носач B задовољава услов: $a, b \in B \Rightarrow a * b \in B$. Тада за подскуп B кажемо да је затворен у односу на ту операцију. Подперације једне операције означавамо истим симболом као и саму ту операцију.

Пример 0.10. Сабирање целих бројева је подоперација операције сабирања рационалних или реалних бројева.

Сабирање по модулу природног броја n није подоперација операције сабирања целих бројева, иако је $\mathbb{Z}_n \subset \mathbb{Z}$, јер, на пример $4 +_7 9 = 6$ у $\mathbb{Z}_7$, док је $4 + 9 = 13$ у $\mathbb{Z}$. Исто важи и за множење по модулу n и обично множнење.

Сагласност пресликавања

Дефиниција 0.6. Нека су на скуповима A и B дефинисане редом операције f и g, обе дужине n. За пресликавање $\phi : A \to B$ кажемо да је *сагласно* са паром операција f и g ако важи $\phi(f(a_1, a_2, ..., a_n)) = g(\phi(a_1), ..., \phi(a_n))$ (то јест ако је слика резултата операције у A над неким елементима једнака резултату операције над њиховим сликама у B).

Тада кажемо да је ϕ један *хомоморфизам* пара (A, f) у пар (B, g).

Посебно, за пресликавање $\phi : A \to B$ кажемо да је сагласно са паром бинарних операција $*$ и $\circ$ дефинисаних редом на скуповима A и B ако је $\phi(a * b) = \phi(a) \circ \phi(b)$.

Исто као горе, кажемо да је f један хомоморфизам пара $(A, *)$ у пар $(B, \circ)$.

Аналогно, сагласност са паром унарних операција $a \mapsto a^{-1}$ и $b \mapsto b'$ значи да је $\phi(a^{-1}) = (\phi(a))'$, а сагласност са паром нуларних (константи) $e \in A$ и $\varepsilon \in B$ да је $\phi(e) = \varepsilon$.

Као што ћемо се (или смо се, у Линеарној алгебри) ограничавати на посматрање подскупова затворених за операције, занимаће нас и слике скупова са операцијама у односу на пресликавања сагласна са њима. Важи да "Хомоморфне слике чувају алгебарске законе". Пробајте за вежбу да докажете следеће тврђење

Т: Ако је бинарна операција $\star$ у скупу A асоцијативна и ако постоји хомоморфизам пара $(A, \star)$ у пар $(B, \circ)$ који је сурјекција, тада је и операција $\circ$ асоцијативна. Слично и за комутативност.

Пример 0.11. Пресликавање $\rho : \mathbb{Z} \to \mathbb{Z}_n$ дефинисано са $\rho(m) = rest(m, n)$ је сагласно са паром операција $+$ и $+_n$ (остатак збира је збир остатака - проверите!). Ово пресликавање је очигледно "на", па по претходном тврђењу асоцијативност сабирања целих бројева повлачи асоцијативност сабирања по модулу n. На исти начин добијамо да је $+_n$ и комутативна операција. Такође, пресликавање ρ је сагласно и са паром $\cdot$ и $\cdot_n$ (остатак производа при дељењу са n једнак је производу остатака чинилаца - проверите!), па добијамо да је $\cdot_n$ асоцијативна и комутативна операција.

Конгруенције

Нека је на скупу A задата операција f дужине n и релација еквиваленције $\sim$. Кажемо да је $\sim$ једна *конгруенција* на скупу A ако је сагласна са операцијом f, односно ако из $a_1 \sim b_1 \wedge a_2 \sim b_2 \wedge \cdots \wedge a_n \sim b_n$ следи $(f(a_1, a_2, ..., a_n)) \sim (f(b_1, b_2, ..., b_n))$.

Посебно, ако на скупу A имамо бинарну операцију $*$, релација еквиваленције $\sim$ је конгруенција дате бинарне операције ако важи $a \sim c \wedge b \sim d \ \Rightarrow \ a * b \sim c * d$. Ако је C_a класа елемента a, ово значи да $C_a = C_c \wedge C_b = C_d \Longrightarrow C_{a*b} = C_{c*d}$. Другим речима, то знаци да је тада са $C_a \bullet C_b = C_{a*b}$ добро дефинисана једна бинарна операција у скупу $A/\sim$ свих класа уочене еквиваленције. Зовемо је *количничком операцијом* дате бинарне операције $*$ у скупу A по њеној конгруенцији $\sim$. Пошто је пресликавање $\pi : A \to A/\sim$ које елементу додељује његову класу еквиваленције, $\pi(a) = C_a$ хомоморфизам који је на (ово непосредно следи из претходне дефиниције операције на класама), следи да је количничка структура хомоморфна слика од A. То ће даље повлачити да у њој важе исти алгебарски закони као у A.

0.1.2 Алгебарска структура

Дефиниција 0.7. Алгебарска структура (или алгебра) је скуп A са алгебарским операцијама дефинисаним на њему, $A = (A, f_1, f_2, ..., f_k)$.

A је *скуп-носач* алгебарске структуре, а дужине операција одређују *тип алгебарске структуре*.

Пример 0.12. $(\mathbb{Z}, +)$ је алгебарска структура типа 2, $(\mathbb{Z}, +, \cdot)$ је типа $(2, 2)$, док је $(\mathbb{Z}, +, \cdot, 0)$ типа $(2, 2, 0)$.

Дефиниција 0.8. За алгебарску структуру $B = (B, g_1, g_2, ..., g_k)$ кажемо да је *подструктура* структуре $A = (A, f_1, f_2, ..., f_k)$ ако важи:
1) Структуре B и A су истог типа; 2) за свако $i \in 1, \ldots, n$ операција g_i је подоперација операције f_i.

Из дефиниције одмах следи да је тада $B \subseteq A$, као и да је скуп B затворен за све операције дефинисане на A.

Пример 0.13. $(\mathbb{Z}, +, \cdot, 0)$ је подструктура структуре $(\mathbb{Q}, +, \cdot, 0)$

Даље, ако су $A = (A, f_1, ..., f_k)$ и $B = (B, g_1, ..., g_k)$ било које алгебарске структуре истог типа, интересују нас само она пресликавања скупа A у скуп B $\phi : A \to B$ која су сагласна са сваким од парова њихових одговарајућих операција. То су *хомоморфизми структуре* A у структуру B.
Инјективни хомоморфизми зову се и мономорфизми, сурјективни хомоморфизми су епиморфизми, док су бијективни изоморфизми.
За алгебарску структуру A кажемо да је *изоморфна* структури B ако постоји бар један изоморфизам структуре A у структуру B. Тада пишемо $A \cong B$.

Ми ћемо проучавати само алгебарске структуре одређених типова (на пример типа (2), $(2, 0)$, $(2, 1, 0)$, $(2, 2)$) и то оне чије операције задовољавају неки систем унапред задатих услова или аксиома (на пример услове асоцијативности или комутативности). Заједно са њима проучаваћемо њихове подструктуре, хомоморфизме и конгруенције. То су уједно и три основна начина у алгебри да од једне структуре добијемо структуре исте врсте - узимање подскупова затворених за операције или *подструктура*, затим

посматрање *хомоморфних слика* и на крају, узимање класа еквиваленције сагласне са операцијама или *сечење по конгруенцији*. Видећемо (на примерима група и прстена) да су ове три конструкције увек нераскидиво повезане.

0.2 Семигрупе и моноиди

0.2.1 Семигрупе

Дефиниција 0.9. Ако је $*$ било која бинарна операција у скупу A, тада уређен пар $(A, *)$ зовемо *групоид* са операцијом $*$ и скупом-носачем A.

Пример 0.14. Сви скупови и бинарне операције дефиниисане на њима које смо навели у претходном поглављу су примери групоида: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{Z}_n, +_n)$, $(\mathbb{Z}_n, \cdot_n)$, $(\mathbb{R}[X], +)$, $(\mathbb{R}[X], \cdot)$, $(M_{mn}(\mathbb{R}), +)$, $(M_n(\mathbb{R}), \cdot)$, $(\mathcal{P}(X), \cup)$, $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \triangle)$.

Групоид је комутативан ако је таква његова операција. Сви претходно наведени групоиди су комутативни, осим $(M_n(\mathbb{R}), \cdot)$. Такође, групоид $(\mathcal{P}(X), \setminus)$ није комутативан.

Оно што је важније и што нам омогућава да правимо даље сложеније алгебарске структуре је асоцијативност бинарне операције групоида. Асоцијативне групоиде зовемо полугрупе или семигрупе. Прецизније

Дефиниција 0.10. Ако је $*$ било која бинарна операција у скупу A, тада уређен пар $(A, *)$ зовемо *семигрупа* или *полугрупа* ако важи $(a * b) * c = a * (b * c)$ за свако $a, b, c \in A$.

Пример 0.15. Сви скупови и бинарне операције дефинисане на њима које смо навели у претходном поглављу су примери семигрупа: $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{Z}_n, +_n)$, $(\mathbb{Z}_n, \cdot_n)$, $(\mathbb{R}[X], +)$, $(\mathbb{R}[X], \cdot)$, $(M_{mn}(\mathbb{R}), +)$, $(M_n(\mathbb{R}), \cdot)$, $(\mathcal{P}(X), \cup)$, $(\mathcal{P}(X), \cap)$, $(\mathcal{P}(X), \triangle)$.
Даље, скуп свих функција $f : X \to X$ дефинисаних на непразном скупу X је семигрупа у односу на операцију њиховог слагања (композиције), $(X^X, \circ)$, јер важи $(f \circ g) \circ h = f \circ (g \circ h)$.

Пример 0.16. $(\mathbb{Z}, -)$ није семигрупа, као, на пример, ни $(\mathcal{P}(X), \setminus)$.

У семигрупи можемо индуктивно дефинисати и композицију више елемената: $(a) = a$, или $a * b$ је стандардна вредност бинарне операције на a и b, док композицију $n + 1$ елемената дефинишемо преко композиције n елемената на следећи начин:

$$a_1 * \cdots * a_n * a_{n+1} = (a_1 * \cdots * a_n) * a_{n+1}.$$

Одавде следи да је, на пример, $a*b*c = (a*b)*c$ или $a*b*c*d = ((a*b)*c)*d$. Међутим, асоцијативност нам даје да је први производ једнак $a * (b * c)$, па претпостављамо да исто важи за било какво здруживање елемената, наравно без мењања редоследа.

Теорема 0.1. (Уопштена асоцијативност) *Ако је $(A, *)$ било која семигрупа, n природан број и $a_1, \ldots, a_n$ произвољни елементи из A, тада за свако $i < n$ важи*

$$a_1 * a_2 \cdots * a_n = (a_1 * \cdots * a_i) * (a_{i+1} * \cdots * a_n).$$

Доказ. Прво, ако је $i = n-1$, ово се своди на дефиницију композиције више елемената. Ако је $i < n-1$, означимо $a_1 * \cdots * a_i = x$ и $a_{i+1} * \cdots * a_{n-1} = y$. Десна страна је сада $x*(y*a_n)$, а то је због асоцијативности једнако $(x*y)*a_n$. По индуктивној претпоставци је $x * y = a_1 * \cdots * a_{n-1}$, и онда је по дефиницији композиције n елемената ово тачно $a_1 * a_2 \cdots * a_n$. □

Дакле, елементе можемо груписати по вољи, без нарушавања њиховог редоследа

Када је операција семигрупе означена мултипликативно, на пример са $\cdot$, зовемо је множење, а композицију n елемената зовемо њихов производ. Производ n истих фактора означавамо са a^n , n-ти степен елемента a. Из претходног тврђења следи да за природне бројеве m и n важи:

$$a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

Ако елементи a и b комутирају, тада је $(a \cdot b)^n = a^n \cdot b^n$.

Ако је операција означена адитивно, на пример са $+$, елемент $a_1 + \cdots + a_n$ зовемо збир елемената $a_1, \ldots, a_n$. Такође, n-ти степен елемента a у тој семигрупи означавамо са $na = a + \cdots + a$, и онда је $(m+n)a = ma + na$, $m(na) = (mn)a$. Ако елементи a и b комутирају, односно ако је $a + b = b + a$, тада је $n(a + b) = na + nb$.

На крају дајемо дефиницију једног веома важног појма, који смо прошле године имали код матрица.

Дефиниција 0.11. За елемент a семигрупе A кажемо да је *регуларан слева* (односно *здесна*), ако за свако $x, y \in A$ важи
$a * x = a * y \Rightarrow x = y$ (односно $x * a = y * a \Rightarrow x = y$).
За a кажемо да је *регуларан* ако је регуларан и слева и здесна.

Пример 0.17. У семигрупама $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}_n, +_n)$, $(\mathbb{R}[X], +)$, $(M_{mn}(\mathbb{R}), +)$ сви елементи су регуларни.

У семигрупи $(\mathbb{N}, \cdot)$ такође су сви елементи регуларни, док су у $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ и $(\mathbb{R}[X], \cdot)$ регуларни сви осим нуле. У $(\mathbb{Z}_n, \cdot_n)$ регуларност елемента зависи од његовог односа са n: у $\mathbb{Z}_8$ из $3 \cdot_8 x = 3 \cdot_8 y$ следи $x = y$, док из $4 \cdot_8 2 = 4 \cdot_8 6 (= 0)$ не следи $2 = 6$ у $\mathbb{Z}_8$. Још један пример семигрупе у којој нису сви елементи регуларни су матрице, $(M_n(\mathbb{R}), \cdot)$ (поновите кад је квадратна матрица регуларна!)

У семигрупи X^X регуларне су све бијекције, док се елементи регуларни слева и здесна разликују: функција f је регуларна слева акко је "1-1", док је регуларна здесна акко је "на'.

0.2.2 Моноиди

За елемент $e \in A$ кажемо да је неутрални елемент или *неутрал* за бинарну операцију $*$ дефинисану на скупу A ако за свако $a \in A$ важи:

$a * e = a, \quad e * a = a.$
Неутрал дате операције је увек јединствен: ако би и e и $\widehat{e}$ били неутрали операције $*$, из $e * \widehat{e} = e$ (јер је $\widehat{e}$ неутрал) и $e * \widehat{e} = \widehat{e}$ (јер је e неутрал) следи да је $e = \widehat{e}$.

Напомена 0.18. Можемо да дефинишемо леви и десни неутрал неке операције, и онда не можемо да применимо горњи аргумент за јединственост. Ми се овде нећемо бавити тиме.

Пример 0.19. Сабирање у скупу природних бројева нема неутрал, док је 1 неутрал за множење у том скупу. У скупу целих бројева нула је неутрал за сабирање. Празан скуп је неутрал за унију, док је цео скуп X неутрал за пресек у $\mathcal{P}(X)$. Идентично пресликавање на скупу X је неутрал за композицију пресликавања у X^X.

Полугрупе са неутралом зову се моноиди.

Дефиниција 0.12. *Моноид* је алгебарска структура $(A, *, e)$ типа $(2, 0)$ у којој важи:
1) $(a * b) * c = a * (b * c)$ за свако $a, b, c \in A$
2) $a * e = a, \quad e * a = a.$

Пример 0.20. Структуре $(\mathbb{N}, \cdot, 1)$, $(\mathbb{Z}, \cdot, 1)$, $(\mathbb{Q}, \cdot, 1)$, $(\mathbb{R}, \cdot, 1)$ и $(\mathbb{C}, \cdot, 1)$ су моноиди, као и $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{C}, +, 0)$. Моноиди су и $(\mathbb{Z}_n, +_n, 0)$ и $(\mathbb{Z}_n, \cdot_n, 1)$, затим $(\mathbb{R}[X], +, 0)$, $(\mathbb{R}[X], \cdot, 1)$, $(M_{mn}(\mathbb{R}), +, \mathbf{0}_{mn})$, $(M_n(\mathbb{R}), \cdot, E_n)$, такође и $(\mathcal{P}(X), \cup, \emptyset)$, $(\mathcal{P}(X), \cap, X)$, $(\mathcal{P}(X), \triangle, \emptyset)$. За сваки непразан скуп X, семигрупа свих пресликавања на њему је моноид чији је неутрал идентично пресликавање , $(X^X, \circ, id_X)$.

Дефиниција 0.13. За елемент a моноида $(A, *, e)$ кажемо да је *инверзибилан слева*, ако једначина $x * a = e$ има бар једно решење у A, а да је *инверзибилан здесна* ако једначина $a * x = e$ има решење у A. Свако решење прве једначине зове се леви инверз елемента a, а друге десни инверз елемента a.

Теорема 0.2. *Сваки слева инверзибилан елемент моноида је и регуларан слева. Такође, ако једначине*

$$a * x = e, \quad y * a = e$$

имају бар по једно решење, тада су њихова решења једнака и јединствена.

Доказ. Нека је a елемент који је инверзибилан слева и нека важи $a * x = a * y$. Ако је b елемент за који је $b * a = e$, помножићемо претходну једнакост слева са b. Добијамо $b*(a*x) = b*(a*y)$, а онда нам асоцијативност даје $(b*a)*x = (b*a)*y$, то јест $e*x = e*y$ и коначно $x = y$. То значи да је a регуларан слева, али смо успут доказали и да не може да има два различита десна инверза, јер из $a * x = a * y = e$ следи $x = y$. Даље, ако је $a*c = e$ и $b*a = e$ за неке b и c, помножићемо прву од ових једнакости слева са b, искористити асоцијативност и добити $(b * a) * c = b * e$, односно $e * c = b * e$, то јест $c = b$. Ово значи да су леви и десни инверз елемента a једнаки. □

Дефиниција 0.14. Елемент моноида је *инверзибилан* ако је инверзибилан и слева и здесна.

Из претходне теореме следи да ако елемент a има и леви и десни инверз, они морају да буду једнаки. Тај јединствен елемент (који је и леви и десни инверз датог) зовемо *инверз* елемента a и означавамао са a^{-1}. Дакле, инверз елемента a је елемент a^- за који важи

$$a * a^- = a^- * a = e$$

.
Последица доказане теореме је и да ако је елемент инверзибилан, он је регуларан.

Пример 0.21. У моноиду $(\mathbb{Z}, +, 0)$ сви елементи су инверзибилни, инверз елемента a је $-a$. У $(\mathbb{Z}, \cdot, 1)$ инверзибилни су само 1 и -1. У $(\mathbb{Q}, +, 0)$ су такође сви елементи инверзибилни, инверз елемента a је $-a$, а у $(\mathbb{Q}, \cdot, 1)$ инверзибилни су сви осим 0, инвер елемента a је $\frac{1}{a}$.
У моноиду $(\mathbb{Z}_n, +_n, 0)$ сви елементи су инверзибилни, инверз елемента $r \neq 0$ је $n - r$, док је нула сама себи инверз. У $(\mathbb{Z}_n, \cdot_n, 1)$ инверзибилни су они елементи који су узајамно прости са n. У $(\mathbb{R}[X], +, 0)$ сви су инверзибилни, док су у $(\mathbb{R}[X], \cdot, 1)$ инверзибилни елементи само скалари различити од 0 (полином има инверз само ако је ненула константа!). У $(M_{mn}(\mathbb{R}), +, \mathbf{0}_{mn})$ су поново сви инверзибилни, док су у $(M_n(\mathbb{R}), \cdot, E_n)$ инверзибилни елементи матрице чија је детерминанта различита од нуле (или чији је ранг n). У $(\mathcal{P}(X), \cup, \emptyset)$ инверзибилан је само $\emptyset$, у $(\mathcal{P}(X), \cap, X)$ само цео скуп X, док су у $(\mathcal{P}(X), \triangle, \emptyset)$ инверзибилни сви елементи, инверз од A је поново A. За сваки непразан скуп X, у моноиду $(X^X, \circ, id_X)$ инверзибилни елементи су бијекције.

Теорема 0.3. *Ако су у моноиду два елемента инверзибилна, такви су и њихови инверзи, као и композиција. Важи*

$$(a * b)^- = b^- * a^-, \quad (a^-)^- = a.$$

Доказ. Непосредно проверавамо да је $(a * b) * (b^- * a^-) = a * (b * b^-) * a^- = a * e * a^- = a * a^- = e$, па је заиста $(a * b)^- = b^- * a^-$. Друга једнакост следи из саме аксиоме инверза: $a * a^- = a^- * a = e$ значи да елемент a^- помножен било слева било здесна са a даје неутрал, па је по дефиницији његов инверз управо a, тј. $(a^-)^- = a$. □

Напомена 0.22. Ако је операција моноида A означена мултипликативно (неко множење), скуп инверзибилних елемената тог моноида обично означавамо са A^*, неутрал са 1 и зовемо јединица моноида, док инверз елемента a означавамо са a^{-1}.

Ако је операција моноида означена адитивно (неко сабирање), његов неутрал означавамо са 0 и зовемо нула моноида, а инверз елемента a са $-a$ и зовемо супротан елемент елемента a (понекад и опозит од a).

Пример 0.23. Из претходног примера је $\mathbb{Z}^* = \{-1, 1\}$,
$\mathbb{Z}_n^* = \{r \in \mathbb{Z}_n : (r, n) = 1\}$,
$\mathbb{R}[X]^* = \mathbb{R} \setminus 0$,
$M_n(\mathbb{R})^* = \{A \in M_n(\mathbb{R}) : detA \neq 0\}$,
$(X^X)^* = \{f : X \to X \mid f$ је "$1-1$" и "на" $\}$.

0.3 Групе

0.3.1 Дефиниција и примери група

Моноиди у којима су сви елементи инверзибилни зову се групе.

Дефиниција 0.15. *Група* је алгебарска структура $(G, *, ^-, e)$ типа $(2, 1, 0)$ (непразан скуп G на ком је дата једна бинарна операција $*$, једна унарна $^-$ и једна константа e) таква да за свако $a, b, c \in G$ важи:
1) $(a * b) * c = a * (b * c)$
2) $a * e = a, \quad e * a = a$
3) $a * a^- = e, \quad a^- * a = e$.

(Пошто се често истиче само бинарна операција, можемо да кажемо и: Група је скуп G са бинарном операцијом $*$ дефинисаном на њему, за коју важи да је асоцијативна, има неутрал и сваки елемент има инверз, то јест:
1) за свако $a, b, c \in G$ је $(a * b) * c = a * (b * c)$
2) постоји $e \in G$ такво да је за све $a \in G$ $a * e = e * a = a$
3) за свако $a \in G$ постоји $a^- \in G$ такво да је $a * a^- = a^- * a = e$.)

Операцију групе ћемо обично означавати са $+$ или са $\cdot$, у зависности од тога и неутрал и инверз (погледајте напомену у претходној лекцији). Такође, из последњег тврдјења у претходној лекцији, следи да је скуп инверзибилних елемената сваког моноида затворен за множење и инвертовање (производ два инверзибилна елемента је инверзибилан, инверз сваког инверзибилног елемента је инверзибилан), па како му неутрал увек припада (инверз неутрала је он сам), следи да је скуп инверзибилних елемената произвољног моноида једна група. (То је и начин на који конструишемо разне групе - избацимо из моноида оно што није инверзибилно.)

Дефиниција 0.16. За групу $(G, *, ^-, e)$ кажемо да је *комутативна* (или *Абелова*) ако је таква њена бинарна операција, то јест ако је за све $a, b \in G$ испуњено $a * b = b * a$.

Дефиниција 0.17. Ако је $(G, *, ^-, e)$ група, број елемената скупа G зовемо *ред групе* G.

Природно, кажемо да је група G коначна ако је такав њен ред $|G|$ и слично за бесконачну.

Примери група

1) Скуп целих бројева је комутативна група у односу на сабирање, са неутралом 0, и инверзом елемента m (супротним елементом) $-m$: $(\mathbb{Z}, +, 0, -)$.
Исто важи за $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

2) Скуп остатака при еуклидском дељењу са n је комутативна група у односу на сабирање по модулу n, чији је неутрал поново 0, а $-_n r = n - r$ за $r > 0$ и $-_n 0 = 0$: $(\mathbb{Z}_n, +_n, 0, -_n)$. Приметимо да ово значи да за сваки природан број n постоји бар једна група реда n.

3) Скуп свих рационалних бројева различитих од нуле је комутативна група у односу на њихово множење, чији је неутрал 1, а инверз елемента a једнак $\frac{1}{a}$: $(\mathbb{Q} \setminus \{0\}, \cdot, 1, ^{-1})$. Исто важи и за скуп позитивних рационалних бројева, $(\mathbb{Q}^+, \cdot)$, као и за $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$ и $(\mathbb{C} \setminus 0, \cdot)$.

4) Знамо да у моноиду $(\mathbb{Z}_n, \cdot_n, 1)$ нису сви елементи инверзибилни, али ако издвојимо инверзибилне, добићемо групу (комутативну): $(\mathbb{Z}_n^*, \cdot_n)$.
Поновимо да је $\mathbb{Z}_n^* = \{r \in \mathbb{Z}_n : (r, n) = 1\}$.
Групу инверзибилних елемената моноида $\mathbb{Z}_n$ зовемо и *Ојлерова група* и означавамо са Φ_n. Дакле, $\Phi_n = \mathbb{Z}_n^*$ је група у односу на множење по модулу n.

5) Група пресликавања

Ако је $(G, +_G, 0_G, -_G)$ било која група и $S \neq \emptyset$ тада је скуп G^S свих пресликавања из S у G група у односу на операцију индуковану операцијом у G (као код векторских простора што смо имали). Ако су f и g два пресликавања из S у G, њихов збир дефинишемо са

$$(f + g)(x) := f(x) +_G g(x)$$

за све $x \in S$. Неутрал или нула ове групе ће бити нула-пресликавање дато са

$$\mathbf{0}(x) := 0_G$$

за све $x \in S$, док је инверз (супротан елемент) пресликавања $f \in G^S$ пресликавање $-f$ одређено са

$$(-f)(x) := -_G f(x), \quad x \in S.$$

Ако је група G комутативна, таква ће бити и G^S.

6) Симетрична група

Видели смо већ да је скуп свих пресликавања непразног скупа X у самог себе један моноид. Његови инверзибилни елементи чине групу у односу на композицију пресликавања, $(X^X)^*$. Знамо да је пресликавање инверзибилно акко је бијекција. Такође, (требало би да) знамо да се бијекција $f : X \to X$ зове и *пермутација* скупа X. Скуп свих бијекција, односно пермутација, непразног скупа X ћемо надаље означавати са $\mathbb{S}_X$ и звати *симетрична група скупа* X. Дакле, $\mathbb{S}_X = (X^X)^*$. Знамо да ова група није комутативна (композиција пресликавања није комутативна, $f \circ g \neq g \circ f$) ако је скуп X бар трочлан.
Такође, ако је $X = \{1, 2, \ldots, n\}$, $\mathbb{S}_X$ означавамо са $\mathbb{S}_n$ и зовемо *симетрична група степена* n. Она је реда $n!$ и за $n \geq 3$ није комутативна.

7) Линеарна група

Скуп свих матрица реда n са компонентама из неког поља је моноид у односу на њихово множење. Група иверзибилних елемената тог моноида зове се *линеарна група степена* n над тим пољем. Дакле, $\mathbb{GL}(n, \mathbb{R}) = M_n(\mathbb{R})^* = \{A \in M_n(\mathbb{R}) : detA \neq 0\}$.

Знамо (из Линеарне алгебре) да ова група није комутативна. Она је бесконачног реда у горњем случају, али кад је поље из ког су компоненте матрице коначно, и она је коначног реда.

8) Група изометрија еуклидске равни

Изометрија еуклидске равни је свако пресликавање $\phi : \mathbb{E} \to \mathbb{E}$ које чува растојање, тј. такво да је за произвољне тачке A и B дуж AB подударна дужи $\phi(A)\phi(B)$. Ако имамо две изометрије, и њихова композиција је такође изометрија, као и идентична трансформација и њихови инверзи. Дакле, скуп свих изометрија еуклидске равни је група у односу на њихову композицију, коју зовемо *група изометрија еуклидске равни* и означавамо са $\mathbb{GI}(\mathbb{E})$.

9) Група симетрија

Изометрије еуклидског простора које дати скуп тачака (неку фигуру) пресликавају на њега самог зовемо симетрије тог скупа. Скуп свих таквих изометрија је група у односу на њихово слагање, јер ако две изометрије пресликавају фигуру у њу саму, и њихова композиција ће имати ту особину, као и идентична трансформација и њихови инверзи. Дакле, скуп симетрија неког скупа тачака је *група симетрија тог скупа.*

10) Диедарска група

Група симетрија правилног n-тоугла зове се и *диедарска група степена* n и означава се са $\mathbb{D}_n$. Она је реда $2n$ и није комутативна (операција у њој је композиција пресликавања). Чини је n ротација и n осних симетрија. Ако са ρ означимо ротацију правилног n-тоугла око његовог средишта (центра описане кружнице) за угао $\frac{2\pi}{n}$, јасно је да све остале ротације можемо изразити као њене степене. Даље, ако са σ означимо било коју осну симетрију (рефлексију) тог n-тоугла, лако се провери да су све остале осне симетрије производи (композиције) те фиксиране и неке ротације (сетите се да је композиција две рефлексије једнака ротацији око пресечне тачке њихових оса за двоструки угао који те праве заклапају - нацртајте!). Добићемо да је

$$\mathbb{D}_n = \{id, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}\}.$$

Кажемо и да је диедарска група степена n *генерисана* са два елемента ρ и σ за које важе *релације* $\rho^n = \sigma^2 = id,\ \rho\sigma = \sigma\rho^{n-1}$.
(Детаљније о томе како смо добили представљање свих ротација и рефлексија, као и овај однос између њих, прочитајте код Николе у скрипти на 20. страни, где је све лепо објашњено на примеру групе $\mathbb{D}_4$. Ова група ће нам често бити пример којим ћемо илустровати нове појмове, јер је некомутативна и коначна, па би било добро да је лепо разумете и "видите" и алгебарски и геометријски.)

11) Клајнова четворна група

Посматрајмо скуп са четири елемента $\{1, a, b, c\}$ на ком је структура групе задата следећим релацијама:

$$a^2 = b^2 = c^2 = 1,$$

$$ab = ba = c,\ bc = cb = a,\ ca = ac = b.$$

Јасно је да смо добили комутативну групу, у којој је сваки елемент једнак свом инверзу (1 је наравно неутрал - јединица). Ова група се зове *Клајнова четворна група* $\mathbb{V}_4$. Приметимо да ова група има и геометријску интерпретацију - то је група симетрија правоугаоника који није квадрат! Заиста, ако је 1 идентична трансформација, a и b осне рефлексије у односу на праве које пролазе кроз средишта наспрамних страница, а c централна симетрија у односу на центар правоугаоника, лако се провери да су задовољене горње релације.

12) Група кватерниона

Скуп $\mathbb{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$ је група у односу на множење, при чему је $ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -1,\ ik = -j$, као и $i^2 = j^2 = k^2 = -1$ (наравно, $(-1)^2 = 1$ и $(-1)x = x(-1) = -x$). Ова група зове се *група кватерниона* $\mathbb{Q}_8$. (Открио ју је Хамилтон, покушавајући безуспешно прво да дефинише тродимензионо уопштење комплексне равни, а затим тек четвородимензионо - приметите да се i, j и k понашају сви као имагинарна јединица i у пољу $\mathbb{C}$; њихове линеарне комбинације $a + bi + cj + dk$ чине алгебру кватерниона.)

0.3.2 Подгрупе

Дефиниција 0.18. За групу $(H, \circ, \tilde{}, \varepsilon)$ кажемо да је *подгрупа* групе $(G, *, \bar{}, e)$ ако су њене операције подоперације операција групе G, то јест ако је $H \subset G$, $\varepsilon = e$, $a \circ b = a * b$ и $\tilde{a} = \bar{a}$ за све $a, b \in H$.

У том случају кажемо и да је сам скуп H једна подгрупа групе G и пишемо $H \leq G$.

Пример 0.24. Свака група G има бар две подгрупе које зовемо *тривијалне подгрупе* те групе - то су цела група G и њен неутрал $\{e\}$. (Остале подгрупе, ако их има, зову се *праве.*)

$(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$, $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$, али $(\mathbb{Z}_n, +_n)$ није подгрупа групе $(\mathbb{Z}, +)$ јер немају исту операцију;

$(\mathbb{Q} \setminus \{0\}, \cdot) \leq (\mathbb{R} \setminus \{0\}, \cdot)$;

$\mathbb{S}_n \leq \mathbb{S}_m$ за $n \leq m$ - ово закључујемо јер сваку пермутацију од n елемената можемо видети и као пермутацију од m елемената при чему фиксирамо елементе $n{+}1, n{+}2, \ldots, m$;

$\mathbb{SL}(n, \mathbb{R}) \leq \mathbb{GL}(n, \mathbb{R})$ где је $\mathbb{SL}(n, \mathbb{R})$ специјална линеарна група степена n коју чине матрице детерминанте 1

Скуп свих ротација $\{id, \rho, \rho^2, \ldots, \rho^{n-1}\}$ чини једну подгрупу диедарске групе $\mathbb{D}_n$;

$\{1, -1, i, -i\} \leq \mathbb{Q}_8$.

Теорема 0.4. *Ако је $(G, \cdot, ^{-1}, e)$ било која група, за сваки непразан подскуп H скупа G следећа три услова су еквивалентна:*
1) $H \leq G$,
2) $a, b \in H \ \Rightarrow\ a^{-1}b \in H$,

3) $a, b \in H \ \Rightarrow \ ab, a^{-1} \in H$.

(Приметите да смо променили ознаке из почетне дефиниције, да би одговарале стандардној мултипликативној нотацији, у којој $\cdot$ скоро увек изостављамо.)
Доказ. Доказаћемо ово тврђење као ланац импликација.
1) $\Rightarrow$ 2) Према претходној дефиницији, ако је $H \leq G$, скуп H је затворен за операције групе G, па ако су $a, b \in H$ имамо прво да $a^{-1} \in H$, а онда и $a^{-1}b \in H$.
2) $\Rightarrow$ 3) Овде је претпоставка да скуп H са сваким паром елемената садржи производ инверза првог и другог, па је прво $a^{-1}a = e \in H$, даље из тога $a^{-1}e = a^{-1} \in H$ и на крају, $(a^{-1})^{-1}b = ab \in H$.
3) $\Rightarrow$ 1) Пошто је H непразан, посматрајмо неко $a \in H$. Из услова 3) имамо да је онда и $a^{-1} \in H$, и поново из 3), производ $aa^{-1} = e$ такође припада H. Значи, H садржи неутрал групе G, као и производе и инверзе свих својих елемената (то је баш услов 3)), па је, по дефиницији, подгрупа групе G. □

Дакле, непразан подскуп H скупа G, где је G група, је подгрупа акко задовољава један од еквивалентних услова 2) или 3) претходног тврђења, односно ако је затворен за множење и инвертовање (у проверама ћете користити један од њих, по вољи). Јасно је да ако је операција групе означена адитивно, услов 2) гласи

$$a, b \in H \ \Rightarrow \ a - b \in H,$$

а услов 3)

$$a, b \in H \ \Rightarrow \ a + b, -a \in H.$$

Приметимо да је, на нивоу скупова, услов 3) еквивалентан са $HH \subseteq H$, $H^{-1} \subseteq H$, а пошто се лако види да обрнуте инклузије важе, биће $HH = H$, $H^{-1} = H$.

Сетимо се из Линеарне алгебре да је пресек два потпростора увек потпростор. Штавише, то важи за пресек било колико (коначно или бесконачно) потпростора (пресеци никад нису "проблематични" - ако су неки елементи у пресеку, они су у свим скуповима, односно алгебарским структурама које учествују - извршимо операцију унутар тих структура, резултат је у свакој од њих, и коначно, у пресеку!) Аналогно, важи:

Ако су H и K подгрупе групе $(G, \cdot)$, онда је то и њихов пресек $H \cap K$. Исто важи и за пресек произвољне фамилије подгрупа групе G.

- проверите за вежбу, има код Николе

С друге стране, у Линеарној алгебри смо такође имали да унија два потпростора није потпростор у општем случају. Штавише, то важи само ако је један од њих садржан у другом, односно када је унија једнака већем од њих. Исто важи и за подгрупе:
Ако су H и K подгрупе групе $(G, \cdot)$, онда је то и њихова унија $H \cup K$ ако и само ако је $H \subseteq K$ или $K \subseteq H$

- проверите за вежбу, има код Николе

Зато дефинишемо производ подгрупа као најмању подгрупу која садржи обе. (И ово смо имали у Линеарној алгебри, дефинисали смо суму два потпростора и то је био најмањи потпростор који је садржао оба.) Дакле, ако су H и K подгрупе групе G (која је овде, као и у претходном тврђењу, означена мултипликативно, при чему знак операције $\cdot$ изостављамо) *производ* подгрупа H и K дефинишемо као

$$HK = \{hk : h \in H, k \in K\}.$$

Теорема 0.5. *Ако су H и K подгрупе групе $(G,\cdot)$, онда је то и њихов производ HK акко те подгрупе комутирају, то јест ако је $HK = KH$.*

Доказ. Нека подгрупе H и K комутирају. Докажимо да је онда HK једна подгрупа групе G. Нека су hk и $h'k'$ произвољни елементи из HK. Тада је $hkh'k' = h\hat{h}\hat{k}k' \in HK$ јер је $h\hat{h} \in H$ и $\hat{k}k' \in K$ (искористили смо $HK = KH$ да елемент $kh' \in KH$ заменимо елементом $\hat{h}\hat{k} \in HK$). Даље, за $hk \in HK$ је $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$ (овде смо искористили да $h \in H \Rightarrow h^{-1} \in H$, као и $k \in K \Rightarrow k^{-1} \in K$).
Нека је сада производ HK подгрупа групе G. То повлачи да је затворен за инвертовање, то јест да је $(HK)^{-1} = HK$, односно $K^{-1}H^{-1} = HK$. Међутим, H и K су подгрупе, па је $H^{-1} = H$ и $K^{-1} = K$, а онда и $KH = HK$. □

Лагранжова теорема

Свака подгрупа H групе G индукује једну релацију еквиваленције на скупу G дефинисану са

$$a \sim_H b \Leftrightarrow a^{-1}b \in H.$$

Проверимо да је ово тачно:

рефлексивност: $a \sim_H a \Leftrightarrow a^{-1}a = e \in H$, што је тачно јер је H подгрупа и садржи неутрал

симетричност: $a \sim_H b \Leftrightarrow a^{-1}b \in H \Leftrightarrow (a^{-1}b)^{-1} = b^{-1}a \in H \Leftrightarrow b \sim_H a$

транзитивност: $a \sim_H b \wedge b \sim_H c \Leftrightarrow a^{-1}b \in H \wedge b^{-1}c \in H \Rightarrow a^{-1}bb^{-1}c \in H \Rightarrow a^{-1}c \in H \Rightarrow a \sim_H c$

Дакле, $\sim_H$ јесте једна еквиваленција. Шта су њене класе?

$$C_a = a/\sim_H = \{b \in G : b \sim_H a\} = \{b \in G : a^{-1}b \in H\} = \{b \in G : b \in aH\} = aH.$$

Скуп $aH = \{ah : h \in H\}$ зове се *леви положај* или *леви косет* подгрупе H у групи G који садржи дати елемент a. Знамо да за класе било које еквиваленције важи или да су једнаке или да су дисјунктне. При том су једнаке акко су њихови представници у релацији, одакле добијамо потребан и довољан услов за једнакост два косета:

$$aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow b \in aH.$$

Дакле, два лева косета подгрупе H су једнака акко се њихови представници разликују до на елемент из H. Посебно је $aH = H \Leftrightarrow a \in H$. Ако су два косета различита, они су и дисјунктни, и група G је једнака дисјунктној унији свих различитих левих положаја било које њене подгрупе H. Количнички скуп $G/\sim_H$ ћемо означавати са $G_L(H)$.

Слично дефинишемо и десне косете, само што полазимо од релације

$$a \sim b \Leftrightarrow ba^{-1} \in H.$$

Количнички скуп $G/\sim$ ћемо овде означавати са $G_D(H) = \{Ha : a \in G\}$.

Приметимо да важи

$$Ha = Hb \Leftrightarrow a^{-1}H = b^{-1}H,$$

па је са $f(Ha) = a^{-1}H$ дефинисана бијекција скупа свих десних положаја $G_D(H)$ подгрупе H на скуп свих левих положаја $G_L(H)$. Дакле, ова два скупа су исте кардиналности.

Ако су ти скупови коначни, број елемената било ког од њих зовемо *индекс* подгрупе H у групи G и означавамо $[G : H]$. Дакле,

$$[G : H] = |G_L(H)| = |G_D(H)|.$$

У супротном за подгрупу H кажемо да је *бесконачног индекса* у групи G. На пример, $[\mathbb{Z} : 2\mathbb{Z}] = 2$, док је $SL(n, \mathbb{R})$ бесконачног индекса у $GL(n, \mathbb{R})$.

Теорема 0.6. *(***Лагранжова теорема***) Ред било које подгрупе H коначне групе G дели ред те групе и важи*

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

Доказ. Констатовали смо већ да је група G дисјунктна унија свих различитих левих положаја дате подгрупе H. Приметимо да су сви скупови aH истобројни и њихова кардиналност једнака је кардиналности саме подгрупе H. То је јасно јер је пресликавање $f : H \to aH$ дато са $f(x) = ax$ бијекција ($f(x) = f(y) \Rightarrow ax = ay$ и помножимо слева иверзом елемента a да добијемо $x = y$ - f је '1-1'; за дато $ax \in aH$, елемент x се слика у њега помоћу f, па је f и 'на'. Дакле, број левих положаја подгрупе H је $[G : H]$, а у сваком од њих има $|H|$ елемената, па је $|G| = |H| \cdot [G : H]$. □

Претходна теорема не тврди да за сваки број који дели ред коначне групе, она има подгрупу датог реда, већ само даје кандидате за ред те подгрупе. На пример, група реда 40 сигурно нема подгрупу реда 7, док подгрупу реда 8 може, али не мора да има (видећемо да за неке посебне класе група важи и тај "обрнути Лагранж").

Лагранжову теорему користимо да одредимо индекс дате подгрупе. На пример, индекс подгрупе $\mathcal{R}_n$ сачињене од ротација, у групи $\mathbb{D}_n$ је $[\mathbb{D}_n : \mathcal{R}_n] = \frac{2n}{n} = 2$.

0.3.3 Ред елемента у групи

Нека је G група и a произвољан елемент из G. Питамо се шта је минимална подгрупа од G која садржи тај елемент?

Напомена 0.25. Ако је S било који подскуп групе G (то јест њеног скупа носача), питамо се да ли постоји минимална подгрупа од G која садржи S. Нека је Π_S фамилија свих подгрупа од G које садрже тај скуп S. Тражена подгрупа ће управо бити пресек фамилије Π_S. Означићемо је са $H =< S >$. Сви елементи из H ће бити тачно облика $a = a_1 a_2 \cdots a_n$, где је $n \in \mathbb{N}$, $a_i \in S \cup S^{-1}$ (a_i је из S или је његов инверз из S). За подгрупу H кажемо да је *генерисана уоченим скупом* S и пишемо $H = \langle S \rangle$. Ако је скуп

S коначан, $S = \{a_1, a_2, \ldots, a_m\}$ и, додатно, његови елементи комутирају, сваки елемент из $\langle S\rangle$ је облика

$$a = a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}, \quad k_i \in \mathbb{Z}.$$

(Можемо да их групишемо јер је $a_i a_j = a_j a_i$, а допуштамо да се неки не појављује у конкретном елементу тиме сто његов експонент буде 0). Ако је операција у групи означена адитивно, претходни услов гласи

$$a = k_1 a_1 + k_2 a_2 + \cdots + k_m a_m, \quad (k_i \in \mathbb{Z}).$$

(Ово нас, свакако, подсећа на линеарну комбинацију над векторима $a_1, a_2, \ldots, a_m$ коју смо прошле године имали у Линеарној алгебри).

Пример 0.26. $\mathbb{Z} = \langle 1\rangle$, $\mathbb{Z}_n = \langle 1\rangle$, док $\mathbb{Q}$ нема ниједан коначан скуп генератора (проверите - могу ли се сви разломци добити као линеарне комбинације коначно њих, са целобројним коефицијентима?)

$\mathbb{D}_n = \langle \rho, \sigma\rangle$; $\mathbb{V}_4 = \langle a, b\rangle$, $\mathbb{Q}_8 = \langle i, j, k\rangle$.

Вратимо се на почетно питање. Дакле, за задати елемент $a \in G$, тражимо $\langle a\rangle$. Из дефиниције је

$$\langle a\rangle = \{a^m : m \in \mathbb{Z}\}.$$

Питамо се да ли је ова подгрупа коначна или бесконачна, заправо разликујемо та два случаја.

Јасно је да ако међу степенима елемента a нема једнаких, подгрупа $\langle a\rangle$ је бесконачна.

Да видимо шта се дешава ако је $a^r = a^s$ за бар један пар различитих целих бројева r, s. Ако је $r > s$, односно $r - s > 0$, из $a^{r-s} = e$ следи да постоји и најмањи природан број k за који је $a^k = e$. У том случају ће k бити управо ред подгрупе $\langle a\rangle$, а тиме и

$$\langle a\rangle = \{e, a, a^2, \ldots, a^{k-1}\}.$$

Зашто ово важи? -Узмимо произвољан $a^m \in \langle a\rangle$. Ту је $m \in \mathbb{Z}$, па га можемо еуклидски поделити са k. Добићемо $m = kq + r$, при чему је $0 \leq r < k$. Пошто је $a^k = e$, имамо следећи низ једнакости

$$a^m = a^{kq+r} = a^{kq} a^r = (a^k)^q a^r = e^q a^r = a^r,$$

што значи да је сваки степен елемента a једнак неком од првих k, одакле је $\langle a\rangle = \{e, a, a^2, \ldots, a^{k-1}\}$. Приметимо такође и да међу овим елементима нема једнаких, јер ако би важило да је $a^i = a^j$ за неке $0 \leq i, j < k$, $i \neq j$ онда бисмо добили да је $a^l = e$ и за неко $0 < l < k$ ($l = i - j$ или $l = j - i$), што је у супротности са условом да је k најмањи такав број.

Значи, ако је $\langle a\rangle$ коначна, њен ред је најмањи природан број k за који је $a^k = e$. Тај број зовемо *ред* самог елемента a у групи G и означавамо са $\omega(a)$.

Дефиниција 0.19. *Ред елемента* a у групи G је најмањи природан број k за који је $a^k = e$. Ако такав број не постоји, кажемо да је a *бесконачног реда* у групи G.

Из горњих извођења је јасно да важи

$$a^m = e \;\Leftrightarrow\; \omega(a) \mid m.$$

-Јасно је да ако је $k = \omega(a)$ и $m = kq$, онда је $a^m = a^{kq} = (a^k)^q = e$. С друге стране, ако је $a^m = e$, поделићемо опет m еуклидски са $k = \omega(a)$ и добити $e = a^m = a^{kq+r} = (a^k)^q a^r = a^r$, где је $0 \leq r < k$. Опет из дефиниције реда елемента, закључујемо да је ово могуће само за $r = 0$, односно за $m = kq$.

Очигледно је да ако је сама група G коначног реда, онда је то и сваки од њених елемената. Такође, пошто је ред групе дељив редом подгрупе $\langle a\rangle$ који је по дефиницији једнак реду елемента a, из Лагранжове теореме следи да ред елемента дели ред групе, односно

$$|G| = n \;\Rightarrow\; \omega(a) \mid n,$$

као и $a^n = e$ за свако $a \in G$. (Посебно, ако је ред групе прост број, то важи и за ред сваког њеног елемента осим неутрала, па је $\langle a\rangle = G$.)

На крају, повезаћемо ред производа два елемента са њиховим редовима. Јасно је, из правила о степену производа ($(ab)^n = a^n b^n$ ако је $ab = ba$, иначе је $(ab)^n = abab\cdots ab$), да је то могуће само ако ти елементи комутирају.

Теорема 0.7. *Ако су a и b било који елементи групе G и e њен неутрал. Ако је $ab = ba$ и $\langle a\rangle \cap \langle b\rangle = \{e\}$, онда је $\omega(ab) = NZS(\omega(a), \omega(b))$.*

Доказ. Нека је $\omega(ab) = k$, $\omega(a) = m$, $\omega(b) = n$ и $NZS(\omega(a), \omega(b)) = s$. Треба показати да је $k = s$. Прво, из $ab = ba$ следи $(ab)^s = a^s b^s$, а како је најмањи заједнички садржалац два броја дељив сваким од њих, биће $(ab)^s = a^s b^s = (a^m)^{\frac{s}{m}} (b^n)^{\frac{s}{n}} = e^{\frac{s}{m}} e^{\frac{s}{n}} = e$, одакле следи да $k \mid s$. Треба показати да важи и обрнуто.
Имамо $(ab)^k = e$ (јер је $k = \omega(ab)$), односно $a^k b^k = e$ (јер комутирају), а ово је даље еквивалентно са $a^k = b^{-k}$. Тако смо добили елемент који је у пресеку подгрупа генерисаних са a и b ($a^k \in \langle a\rangle$, а $b^{-k} \in \langle b\rangle$), па је $a^k = b^{-k} = e$, односно $a^k = e$ и $b^k = e$ (из $b^{-k} = e$ следи да је и његов инверз једнак неутралу, $b^k = (b^{-k})^{-1}$). Сада, из $a^k = e$ следи да $m \mid k$, из $b^k = e$ следи да $n \mid k$, па онда и најмањи број у ком су садржани m и n дели k, то јест $s \mid k$.
На крају, из $k \mid s$ и $s \mid k$ и тога што су оба природни бројеви, закључујемо $k = s$. □

Последица: Ако су a и b било који елементи групе G који комутирају и чији су редови узајамно прости, онда је $\omega(ab) = \omega(a)\omega(b)$.

0.3.4 Хомоморфизми група

Имали смо већ у уводној лекцији да је хомоморфизам једне алгебарске структуре у другу која је истог типа, свако пресликавање њихових скупова-носача које се слаже са свим паровима одговарајућих операција тих структура. У складу са тим имамо следећу дефиницију:

Дефиниција 0.20. *Хомоморфизам* групе $(G, *, ^{-1}, e)$ у групу $(K, \circ, ^{\sim}, \varepsilon)$ је свако пресликавање $f : G \to K$ које задовољава услове:
1) $f(a * b) = f(a) \circ f(b)$,
2) $f(e) = \varepsilon$,
3) $f(a^{-1}) = f(a)^{\sim}$.

Испоставља се да су у претходној дефиницији услови 2) и 3) последица услова 1) (и наравно, аксиома групе):
прво, из $e * e = e$ и проласка f кроз бинарну операцију, добијамо $f(e) \circ f(e) = f(e)$ - ово је једнакост у групи K и знамо да њу испуњава једино неутрал те групе ($x \circ x = x$ помножимо слева инверзом од x и добијемо да је x једнак неутралу). Одавде је $f(e) = \varepsilon$. Сада, из аксиоме инверза $a * a^{-1} = e$, применом f добијамо $f(a) \circ f(a^{-1}) = f(e)$, односно $f(a) \circ f(a^{-1}) = \varepsilon$, што, по аксиоми инверза у групи K значи да је $f(a^{-1}) = (f(a))^{\sim}$.
Дакле, пресликавање $f : G \to K$ је хомоморфизам групе G у групу K акко је сагласно са паром њихових бинарних операција.

Шта можемо да кажемо о вези реда неког елемента и његове слике при хомоморфизму? Важи:

Ако је елемент a коначног реда у групи G, онда је и $f(a)$ коначног реда у групи K и $\omega(f(a)) \mid \omega(a)$ (ред слике дели ред елемента).

-Кренимо од $a^{\omega(a)} = e$ и применимо f. Добијамо $f(a^{\omega(a)}) = f(e) = \varepsilon$, односно $f(a)^{\omega(a)} = \varepsilon$ што тачно значи да $\omega(f(a)) \mid \omega(a)$.

Ако је пресликавање f инјекција, a и $f(a)$ су истог реда.

Приметимо на крају да је композиција два хомоморфизма опет хомоморфизам (имали смо прошле године у Линеарној алгебри композицију два линеарна пресликавања) и да је инверз бијективног хомоморфизма такође хомоморфизам (опет аналогно важи за операторе):

1) Ако су $f : G \to K$ и $g : K \to L$, редом, хомоморфизми групе $(G, *)$ у $(K, \star)$, односно $(K, \star)$ у $(L, \diamond)$, онда је $g \circ f : G \to L$ хомоморфизам групе G у групу L.

2) Ако је $f : G \to K$ хомоморфизам група који је инверзибилан (дакле, бијективан), онда је и његов инверз $f^{-1} : K \to G$ хомоморфизам група.

Инјективне хомоморфизме зовемо мономорфизми, сурјективне епиморфизми, бијективне изоморфизми. Ако је $f : G \to K$ било који изоморфизам групе G на групу K, тада је и његов инверз један изоморфизам групе K на групу G. За групу G кажемо да је *изоморфна* групи K и пишемо $G \cong K$ ако постоји бар један изоморфизам $f : G \to K$. Између изоморфних група нема суштинских разлика, изузимајући саме природе њихових објеката, па их често поистовећујемо.

Хомоморфизми групе G у њу саму зову се ендоморфизми, а изоморфизми групе G њени аутоморфизми. Скуп свих ендоморфизама групе G означаваћемо са $End(G)$. Приметимо да је то један моноид у односу на композицију пресликавања, $(End(G), \circ, id_G)$, док је скуп инверзибилних елемената овог моноида $End(G)^*$ управо група аутоморфизама групе G, $Aut(G)$.

Пример 0.27. Изоморфизам $S_3 \cong D_3$ добијамо тако што означимо темена правилног троугла са $1, 2, 3$ и пратимо шта се десава кад применимо све ротације и осне симетрије. С друге стране, изоморфизам $Aut(S_3) \cong S_3$ добијамо пратећи шта су могући редови

елемената приликом сликања аутоморфизмом (изоморфизам мора да чува ред сваког елемента!)

0.3.5 Цикличне групе

СВЕ ИЗ НИКОЛИНЕ СКРИПТЕ, И САМО ТО

Дефиниција 0.21. За групу G кажемо да је *циклична* ако има бар једну једночлану генератрису, то јест бар један елемент a за који је

$$G = \langle a \rangle = \{a^m : m \in \mathbb{Z}\}$$

Свака циклична група је комутативна и у случају када је коначна, њен ред је управо ред било ког од њених генератора.
Ако је група G означена адитивно, уместо a^m пишемо ma, па је онда

$$G = \langle a \rangle = \{ma : m \in \mathbb{Z}\}.$$

Пример 0.28. Адитивна група $\mathbb{Z}$ је циклична и са генератором $a = 1$. То важи и за сваку од адитивних група $\mathbb{Z}_n$, само што је $\mathbb{Z}$ бесконачна, а ове остале коначне и реда n.

Код Николе су доказана следећа тврђења:

Теорема [Задатак 19 код Николе]: Свака циклична група је изоморфна или групи $\mathbb{Z}$ или тачно једној од група $\mathbb{Z}_n$. Посебно, две цикличне групе су изоморфне ако и само ако су истог реда.

Теорема[Задатак 20 код Николе]: Свака подгрупа цикличне групе G је такође циклична.

Теорема[Задатак 21 код Николе]: Ако је G коначна циклична група реда n, тада за сваки природан број m који дели n, група G има тачно једну подгрупу реда m.

Теорема [Задатак 22 код Николе]: Ако је G циклична група реда n генерисана елементом a, онда сваки елемент a^k такође генерише групу G ако и само ако су n и k узајамно прости.

0.3.6 Симетрична група

Имали смо већ да је скуп $\mathbb{S}_X$ свих пермутација (бијекција $X \to X$) непразног скупа X група у односу на њихову композицију (слагање). Та група се зове *симетрична група*

скупа X. Уместо уобичајеним ознакама за функције, пермутације ћемо означавати грчким словима $\pi, \rho, \sigma, \tau \ldots$. Значај симетричне групе у разним областима математике је огроман, а њену важност у теорији група показује Кејлијева теорема

Теорема 0.8. *Свака група G је изоморфна некој подгрупи симетричне групе $\mathbb{S}_G$ њеног скупа-носача G.*

Доказ. Сваком елементу $g \in G$ придружићемо пермутацију $\pi_g \in \mathbb{S}_G$, одређену са $\pi_g(x) = gx$. За почетак треба проверити да смо заиста добили пермутацију, односно бијекцију скупа G: π_g је "1-1" јер $\pi_g(x) = \pi_g(y) \Leftrightarrow gx = gy \Leftrightarrow g^{-1}(gx) = g^{-1}(gy) \Leftrightarrow (g^{-1}g)x = (g^{-1}g)y \Leftrightarrow ex = ey \Leftrightarrow x = y$
π_g је "на" јер $y = \pi_g(x) \Leftrightarrow y = gx \Leftrightarrow g^{-1}y = g^{-1}(gx) \Leftrightarrow g^{-1}y = (g^{-1}g)x \Leftrightarrow g^{-1}y = ex \Leftrightarrow x = g^{-1}y$. Дакле, за свако $g \in G$ пресликавање π_g је пермутација из $\mathbb{S}_G$. Сада треба показати да је придруживање $\phi : G \to \mathbb{S}_G$ дефинисано са $\phi(g) = \pi_g$ један хомоморфизам група G и $\mathbb{S}_G$: $\phi(g_1g_2) = \pi_{g_1g_2} = \pi_{g_1} \circ \pi_{g_2} = \phi(g_1) \circ \phi(g_2)$ јер $\pi_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = \pi_{g_1}(\pi_{g_2}(x)) = (\pi_{g_1} \circ \pi_{g_2})(x)$ за све $x \in G$. □

Ако су скупови X и Y истобројни, њихове симетричне групе су изоморфне (ако је $f : X \to Y$ бијекција која потврђује исту кардиналност скупова X и Y, онда је пресликавање $F : \mathbb{S}_X \to \mathbb{S}_Y$ одређено са $F(\pi) = f \circ \pi \circ f^{-1}$ један изоморфизам ових симетричних група). Одавде следи да је симетрична група било ког коначног скупа са n елемената изоморфна симетричној групи скупа $\{1, 2, ..., n\}$. Групу $\mathbb{S}_{\{1,2,\ldots,n\}}$ означавамо са $\mathbb{S}_n$ и зовемо *симетрична група степена n*. Она је реда $n!$ и није комутативна за $n \geq 3$.

Пермутације ћемо поистовећивати са уређеним n-торкама њихових вредности, односно ако је $\pi(i) = a_i$ за $i \in \{1, 2, ..., n\}$, писаћемо $\pi = (a_1, a_2, \ldots, a_n)$. Међутим, из овог записа не видимо довољно (на пример, не можемо одмах да одредимо ред пермутације π, или да кажемо нешто више о њој). Зато посматрамо посебне врсте пермутација.

Дефиниција 0.22. Пермутација $\pi \in \mathbb{S}_n$ је *циклус дужине k* ако за k елемената $a_1, a_2, \ldots, a_k$ из $\{1, 2, ..., n\}$ важи да је $\pi(a_1) = a_2$, $\pi(a_2) = a_3, \ldots$, $\pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$, а за све $j \in \{1, 2, ..., n\} \setminus \{a_1, a_2, \ldots, a_k\}$ је $\pi(j) = j$.

Овакав циклус ћемо означавати са $\pi = \lceil a_1, a_2, \ldots, a_k \rfloor$. Приметимо такође да исти циклус можемо записати на више начина:

$$\lceil a_1, a_2, \ldots, a_k \rfloor = \lceil a_2, a_3, \ldots, a_k, a_1 \rfloor = \lceil a_3, a_4, \ldots, a_k, a_1, a_2 \rfloor = \cdots = \lceil a_k, a_1, a_2, \ldots, a_{k-1} \rfloor.$$

Скуп $\{a_1, a_2, \ldots, a_k\}$ зовемо *носач* циклуса.

Јасно је да је $\pi^k = \pi \circ \pi \circ \cdots \circ \pi = id$ и да је k најмањи такав број. Закључујемо да је дужина циклуса заправо његов ред у групи $\mathbb{S}_n$. Такође, из саме дефиниције циклуса следи да се његов инверз лако рачуна, $\pi^{-1} = \lceil a_k, a_{k-1}, \ldots, a_2, a_1 \rfloor$.

Једночлани циклуси се подударају са идентичном пермутацијом, па их не пишемо кад рачунамо са пермутацијама. Означавамо их понекад $\lceil \rfloor$ (по договору, неутрал у симетричној групи означавамо углавном са ε; дакле, $id = \lceil \rfloor = \varepsilon$). С друге стране, двочлани циклуси имају посебан значај. Зову се *транспозиције* . Сваки циклус дужине k је производ $k - 1$ транспозиција. Ово се лако провери:

$$\lceil a_1, a_2, \ldots, a_k \rfloor = \lceil a_1, a_2 \rfloor \lceil a_2, a_3 \rfloor \cdots \lceil a_{k-1}, a_k \rfloor.$$

(обратите пажњу да на десној страни треба да множите здесна улево). За тај циклус кажемо да је *паран*, односно *непаран*, ако је то и број $k - 1$ (једна транспозиција је

непарна, производ две паран итд). При том, цео број $sgn\pi = (-1)^{k-1}$ зове се *знак циклуса* (на пример, $sgn\lceil a, b\rfloor = -1$, док $sgn\lceil a, b, c\rfloor = 1$).

За два циклуса кажемо да су *дисјунктна* ако су такви и њихови носачи. Пошто се елементи које ти циклуси померају не поклапају, јасно је да дисјунктни циклуси комутирају.

Теорема 0.9. *Свака пермутација $\pi \neq \varepsilon$ из $\mathbb{S}_n$ се може разложити на производ дисјунктних циклуса, и ти циклуси су одређени једнозначно до на њихов редослед.*

Доказ. Пошто π није идентична пермутација, постоји бар један елемент a_1 за који је $\pi(a_1) \neq a_1$. Нека је $\pi(a_1) = a_2$. Започнимо циклус $\lceil a_1, a_2, \ldots\rfloor$ и у њега редом упишимо све елементе које добијамо од a_1, односно $\pi^i(a_1)$, за $i = 0, 1, 2, \ldots$. У једном тренутку ћемо поново добити a_1 јер се налазимо у коначном скупу. Ако је $\pi^k(a_1) = a_1$ и $\pi^i(a_1) = a_{i+1} \neq a_1$ за све $1 \leq i \leq k-1$, приметимо да се пермутација π поклапа са циклусом $\pi_1 = \lceil a_1, a_2, \ldots, a_{k-1}, a_k\rfloor$ на његовом носачу. Сада настављамо даље. Ако у скупу $\{1, 2, ..., n\} \setminus \{a_1, a_2, \ldots, a_{k-1}, a_k\}$ има елемената које π не фиксира, узмемо један од њих, b_1, и њиме започнемо нови циклус. Тај циклус ће сигурно бити дисјунктан са циклусом π_1 јер π_1 садржи све степене $\pi^i(a_1)$ за $i = 0, 1, 2, \ldots$ и тачно њих.
Овај процес прављења нових циклуса ће се у једном тренутку завршити због коначности скупа $\{1, 2, ..., n\}$. Ако смо добили циклусе $\pi_1, \pi_2, \ldots, \pi_m$, тврдимо да је

$$\pi = \pi_1\pi_2 \cdots \pi_m.$$

Ово је тачно јер се π са сваким од ових циклуса поклапа на његовом носачу, а ван тог носача циклус фиксира остале елементе док их неки други циклус помера исто као и π. За елементе које π не помера важи да их и производ $\pi_1\pi_2 \cdots \pi_m$ фиксира. На крају, пошто су сви циклуси у горњој декомпозицији међусобно дисјунктни, они комутирају, па њихов редослед није важан. □

Зашто је претходно разлагање тако важно? Имали смо тврђење да ако два елемента групе комутирају и при том се подгрупе генерисање њима тривијално секу, онда је ред производа тих елемената једнак најмањем заједничком садржиоцу њихових редова. Ово се индукцијом лако уопштава на производ коначно елемената. Приметимо да су ови услови испуњени за дисјунктне циклусе у декомпозицији произвољне пермутације. Дакле, ако је $\pi = \pi_1\pi_2 \cdots \pi_m$ представљање пермутације као производа дисјунктних циклуса, ред те пермутације је најмањи заједнички садржалац дужина тих циклуса.

Помоћу разлагања на дисјунктне циклусе дефинишемо и знак пермутације. Већ смо дефинисали знак циклуса дужине k као $(-1)^{k-1}$.

Дефиниција 0.23. Ако је $\pi = \pi_1\pi_2 \cdots \pi_m$ декомпозиција пермутације $\pi \in \mathbb{S}_n$ на производ дисјунктних циклуса, укључујући и једночлане, *знак пермутације* π је производ знакова свих дисјунктних циклуса π_i који учествују у овом разлагању, односно

$$sgn\pi = (-1)^{n-m}.$$

Ако је $sgn\pi = 1$, за пермутацију π кажемо да је *парна*, а ако је $sgn\pi = -1$, да је *непарна*.

Теорема 0.10. *Ако су $\pi, \sigma \in \mathbb{S}_n$ две пермутације, онда је*

$$sgn(\sigma\pi) = sgn\sigma sgn\pi.$$

Доказ. Доказаћемо прво да горња једнакост важи ако је $\sigma = \lceil a, b \rfloor$ нека транспозиција, односно да је $sgn(\lceil a, b \rfloor \pi) = -sgn\pi$. Нека је $\pi = \pi_1\pi_2 \cdots \pi_m$ декомпозиција пермутације π на производ дисјунктних циклуса, где су укључени и једночлани. Постоје две могућности:

1) ако елементи a и b припадају носачу истог циклуса из π, на пример π_1 (дисјунктни циклуси комутирају, па тај коме припадају a и b можемо довести на прво место), онда је

$$\sigma\pi_1 = \lceil a, b \rfloor \lceil a, c_1, \ldots, c_k, b, d_1, \ldots, d_l \rfloor = \lceil a, c_1, \ldots, c_k \rfloor \lceil b, d_1, \ldots, d_l \rfloor,$$

што значи да $\sigma\pi$ има укупно $m+1$ дисјунктних циклуса, за један више него π, па имају супротне знакове ($sgn(\sigma\pi) = (-1)^{n-m-1} = -(-1)^{n-m} = sgn\pi$).

2) ако елементи a и b припадају носачима различитих циклуса из π, на пример $\pi_1 = \lceil a, c_1, \ldots, c_k \rfloor$ и $\pi_2 = \lceil b, d_1, \ldots, d_l \rfloor$, онда је $\sigma\pi = \lceil a, b \rfloor \lceil a, c_1, \ldots, c_k \rfloor \lceil b, d_1, \ldots, d_l \rfloor \pi_3 \cdots \pi_m$, односно $\sigma\pi = \lceil a, c_1, \ldots, c_k, b, d_1, \ldots, d_l \rfloor \pi_3 \cdots \pi_m$ је производ $m-1$ дисјунктних циклуса, па и уовом случају има знак супротан од знака пермутације π ($sgn(\sigma\pi) = (-1)^{n-m+1} = -(-1)^{n-m} = sgn\pi$).

Ако је сада σ произвољна пермутација, написаћемо је прво као производ неких транспозиција (то можемо јер је свака пермутација производ циклуса, а сваки циклус производ транспозиција), којих има на пример r, па прво добијамо да је $sgn\sigma = (-1)^r$ (по претходном, множење једном транспозицијом једном промени знак), а онда и $sgn(\sigma\pi) = sgn\sigma sgn\pi$. □

Последица претходне теореме је да је пермутација $\pi \in \mathbb{S}_n$ парна акко је производ парног броја транспозиција. Такође, из ње следи да ако имамо две парне пермутације, и њихов производ ће бити парна пермутација. Како је идентитета парна, а инверз пермутације π има исти облик као π у смислу цикличне декомпозиције, закључујемо да скуп свих парних пермутација из $\mathbb{S}_n$ чини једну подгрупу те групе. Обележавамо је са $\mathbb{A}_n$ и зовемо *алтернирајућа група степена n*. Она је реда $\frac{n!}{2}$ јер парних и непарних пермутација у $\mathbb{S}_n$ има једнако (на пример, пресликавање $f(\pi) = \lceil a, b \rfloor \pi$ је једна бијекција $\mathbb{A}_n \to \mathbb{S}_n \setminus \mathbb{A}_n$).

На крају пар речи о конјуговању у групи $\mathbb{S}_n$. У било којој групи G за елементе a и b кажемо да су *конјуговани* ако постоји елемент $g \in G$ за који је $b = g^{-1}ag$. Конјуговани елементи су истих редова и по свему су слични (све што радимо са a радимо и са b, само допишемо g^{-1} и g са стране - сетите се сличних матрица од прошле године!). Испоставља се да се конјугат циклуса веома лако одређује. Важи

$$\rho\lceil a_1, a_2, \ldots, a_k \rfloor \rho^{-1} = \lceil \rho(a_1), \rho(a_2), \ldots, \rho(a_k) \rfloor.$$

(Ово се провери: на носачу циклуса на десној страни једнакости, лева страна прво помоћу ρ^{-1} скине то ρ, а онда "прошета" елементе како циклус $\lceil a_1, a_2, \ldots, a_k \rfloor$ налаже и на крају им дода ρ - исто што уради и лева; ван носача циклуса на десној страни, он је идентитета, а то је и пресликавање на левој страни, јер циклус $\lceil a_1, a_2, \ldots, a_k \rfloor$ помера само елементе који су у њему, то јест оне које ρ^{-1} убаци у скуп $\{a_1, a_2, \ldots, a_k\}$).

Као последицу ове једнакости добијамо да се и конјугат пермутације која је представљена као производ дисјунктних циклуса лако рачуна:

$$\rho\pi_1\pi_2 \cdots \pi_m\rho^{-1} = \rho\pi_1\rho^{-1}\rho\pi_2\rho^{-1} \cdots \rho\pi_m\rho^{-1}$$

и онда ρ "уђе" у сваки циклус π_i.

Ово значи да су све међусобно конјуговане пермутације "истог облика" (каже се и истог типа) у смислу да имају једнак број циклуса исте дужине у својим декомпозицијама на дисјунктне циклусе. (Важи и обрнуто: ако су две пермутације истог типа, оне морају да буду конјуговане! Објаснићемо на примеру: нека су $\pi = \lceil 1,2,3,4\rfloor\lceil 5,6,7\rfloor$ и $\sigma = \lceil 2,5,7,3\rfloor\lceil 1,4,6\rfloor$; шта је ρ за које је $\rho\pi\rho^{-1} = \sigma$? Знамо да је

$$\rho\pi\rho^{-1} = \lceil \rho(1),\rho(2),\rho(3),\rho(4)\rfloor\lceil \rho(5),\rho(6),\rho(7)\rfloor$$

и онда узмемо, на пример

$$\rho(1) = 2, \rho(2) = 5, \rho(3) = 7, \rho(4) = 3, \rho(5) = 1, \rho(6) = 4, \rho(7) = 6.)$$

Дакле, две пермутације су конјуговане акко су истог типа. Тај тип често пишемо као m-торку уређену тако да буде нерастућа. На пример, ако је пермутација π представљена као производ дисјунктних циклуса π_1, π_2, π_3 и π_4 чије су дужине редом 4, 3, 3 и 2, она је типа $(4,3,3,2)$. Приметимо да овакве m-торке чине партиције броја n, тако да можемо да закључимо да свакој партицији броја n одговара једна класа конјугованости у групи $\mathbb{S}_n$.

0.3.7 Опис група малог реда

Желимо да помоћу техника које су нам до сада на располагању дамо што више информација о групама чији су редови једноцифрени бројеви. Наравно, касније ћемо имати тврђења помоћу којих ћемо то урадити много лакше.

Пре свега знамо да ред елемента дели ред саме групе. То је довољно да у потпуности опишемо све **групе чији су редови прости бројеви**. Ако је $|G| = p$, где је p прост број и $a \in G$, важиће да $\omega(a) \mid p$, односно $\omega(a) \in \{1,p\}$ па ако a није неутрал, он ће бити реда управо p. То даље даје да $|\langle a\rangle| = |G|$, односно $\langle a\rangle = G$. Дакле, свака група простог реда је циклична. За модел такве групе ћемо узети цикличну групу $\mathbb{Z}_p$.

Закључак: Свака група простог реда је изоморфна тачно једној групи $\mathbb{Z}_p$.

Идемо на најмањи једноцифрен број који није прост. Описаћемо **групе реда 4.** У групи G реда 4, елементи могу бити реда 1,2 или 4. Ако у њој постоји бар један елемент реда 4, он ће моћи да изгенерише целу ту групу. У том случају G је циклична и изоморфна групи $\mathbb{Z}_4$. Остаје могућност да су у групи G сви елементи осим неутрала реда 2. Тврдимо да је тада група G комутативна.

[Важи: Ако су у групи G сви елементи осим неутрала реда 2, група G је комутативна. - Нека су a и b било који елементи групе G. Имамо $a^2 = b^2 = e$, као и $(ab)^2 = e$. Одавде је

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

односно

$$aabb = abab.$$

Помножићемо ову једнакост слева инверзом елемента a, а здесна инверзом елемента b. Добијамо $ab = ba$, што смо и желели.]

Узмимо сада два различита елемента a и b из G. Посматрајмо подгрупе генерисане тим елементима, $H = \langle a \rangle = \{e, a\}$ и $K = \langle b \rangle = \{e, b\}$. Пошто елементи a и b комутирају, комутираће и подгрупе H и K. Знамо да из $HK = KH$ следи да је HK подгрупа групе G. Од којих елемената се она састоји?

$$HK = \{e, a, b, ab\},$$

јер су ови елементи сигурно ту и међу њима нема једнаких ($a \neq b$, $a \neq ab$ јер $b \neq e$, исто и за $b \neq ab$, док $ab \neq e$ јер a и b нису један другом инверз). Тиме смо већ добили 4 елемента, па је $HK = G$. Знамо да је ово Клајнова група, па је $G \cong \mathbb{V}_4$.

Приметимо још да се овај производ понаша исто као Декартов производ група H и K. [Декартов производ две групе $(G_1, \cdot, e_1, ^{-})$ и $(G_2, \circ, e_2, \tilde{})$ је група $G_1 \times G_2$ у којој су операције дефинисане по координатама: $(g_1, g_2) \bullet (g_1', g_2') = (g_1 \cdot g_1', g_2 \circ g_2')$, $e = (e_1, e_2)$, $(g_1, g_2)^{-1} = (\bar{g_1}, \tilde{g_2})$].
Прецизније, тврдимо да је пресликавање $(h, k) \mapsto hk$ изоморфизам група $H \times K$ и HK. Дакле, $G = HK \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Закључак: Свака група реда 4 је изоморфна или цикличној групи $\mathbb{Z}_4$ или групи $\mathbb{V}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Стигли смо до **група реда** 6. Ако је G реда 6, њени елементи могу бити реда 1,2,3 или 6. Да ли може да се деси да су сви елементи осим неутрала у G реда 2? У том случају бисмо имали исту ситуацију као у претходном примеру: постојала би два различита елемента реда 2 која би онда комутирала и дала подгрупу реда 4. Међутим, ово је у супротности са Лагранжом, јер 4 не дели 6! Такође, не могу ни сви елементи групе G да буду реда 3. Тачније, ако је a реда 3, тврдимо да у $G \setminus \{e, a, a^2\}$ нема елемената реда 3. Ако би ту постојао b који је реда 3, онда бисмо могли да направимо више од 6 различитих елемената облика $a^i b^j$ $(e, a, a^2, b, b^2, ab, a^2b, ab^2$ су сви различити - проверите). Зато нека је $b \in G \setminus \{e, a, a^2\}$ реда 2. Помоћу њега и елемента a који је реда 3 можемо да направимо следеће елементе $\{e, a, a^2, b, ab, a^2b\}$ који су сви међусобно различити (проверите!) Дакле, у овом случају је

$$G = \{e, a, a^2, b, ab, a^2b\}.$$

Али, има још елемената! Први од њих је ba. Пошто смо већ попунили целу групу, питамо се ком од наведених елемената је једнак ba. Није e јер a и b нису један другом инверзи, није a јер $b \neq e$, није a^2 јер $b \neq a$, није b јер $a \neq e$. Остају две могућности.

Прва је да је $ba = ab$. Сада имамо два елемента који комутирају и чији су редови узајамно прости, па знамо да је ред њиховог производа једнак производу њихових редова, то јест $\omega(ab) = 6$. Како у групи реда 6 постоји елемент реда 6, она ће бити циклична. Дакле, у овом случају је група G циклична.

Друга могућност је да је $ba = a^2b$. Сада у групи G имамо елемент a реда 3 и елемент b реда 2 за које важи $ba = a^2b$. Ако релације $a^3 = b^2 = e$ и $ba = a^2b$ упоредимо са релацијама које карактеришу диедарску групу $\mathbb{D}_3$: $\rho^3 = \sigma^2 = id$, $\sigma\rho = \rho^2\sigma$, закључујемо да је у овом случају група G изоморфна са $\mathbb{D}_3$.

Закључак: Свака група реда 6 је изоморфна или цикличној групи $\mathbb{Z}_6$ или диедарској групи $\mathbb{D}_3$ (односно симетричној $\mathbb{S}_3$).

Класификоваћемо сада **групе реда** 8. Ако је G реда 8, њени елементи могу бити реда 1,2,4 или 8. Ако у групи G постоји елемент реда 8, она ће бити циклична и изоморфна са $\mathbb{Z}_8$.

Ако су у групи G сви елементи осим неутрала реда 2, видели смо да она мора да буде комутативна, и на исти начин као у случају групе реда 4 показали бисмо да је тада $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Даље ћемо претпоставити да у групи G не постоји елемент реда 8, али да постоји бар један елемент реда 4. Ако је $H = \{e, a, a^2, a^3\}$ подгрупа генерисана тим елементом, за произвољан елемент из $G \setminus H$ важи да је реда 2 или реда 4.

Ако постоји бар један елемент $b \in G \setminus \{e, a, a^2, a^3\}$ који је реда 2, онда ћемо, слично као за групу реда 6, моћи да конструишемо 8 различитих елемената облика $a^i b^j$:

$$G = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Опет, на исти начин као код групе реда 6, дискутујемо ком од њих би могао да буде једнак ba. Лако елеминишемо првих 5 могућности (проверите за вежбу) и долазимо до прве која може да важи: $ba = ab$. Овде имамо два елемента која комутирају, па ће и подгрупе генерисане њима комутирати. Слично као за нецикличну групу реда 4, лако показујемо да је онда $G = HK \cong H \times K \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, при чему је $K = \{e, b\}$. Следећи случај, $ba = a^2b$, није могућ, јер је ова једнакост еквивалентна са $a = b^{-1}a^2b$, а онда би било $aa = b^{-1}a^2bb^{-1}a^2b$, односно $a^2 = b^{-1}a^4b = b^{-1}eb = e$, што није тачно јер a није реда 2. Остаје случај $ba = a^3b$. Сада имамо групу у којој важи $a^4 = b^2 = e$ и $ba = a^3b$, и препознајемо да је реч о групи симетрија квадрата, односно диедарској групи $\mathbb{D}_4$.

На крају, остаје могућност да су сви елементи из $G \setminus \{e, a, a^2, a^3\}$ реда 4. Направимо подгрупу коју генерише један од њих, $K = \{e, b, b^2, b^3\}$. Овде је кључно приметити да сви степени елемента b не могу да се налазе ван подгрупе H генерисане елементом a! Ако би то важило (ако не би било "мешања" степена a и b), могли бисмо да конструишемо више од 8 различитих елемената облика $a^i b^j$. Елемент b смо бирали тако да није у H. Ако би b^3 био у H, затвореност H за множење би имплицирала да је и подгрупа генерисана њиме цела у H, а то је K ($K = \langle b \rangle = \langle b^3 \rangle$), нетачно. Значи, $b^2 \in H$. Ком елементу је он једнак? Пошто је реда 2, мораће да важи $b^2 = a^2$. Сада се питамо шта је ba. Испостави се да је $ba = a^3b$ ($ba = a^2b$ даје $a = b^{-1}a^2b$, односно $a^2 = e$, што није тачно, док $ba = ab$ повлачи $a^{-1}b = ba^{-1}$ и даље $(a^{-1}b)(a^{-1}b) = a^{-1}bba^{-1} = a^{-1}a^2a^{-1} = e$, а претпоставили смо да у $G \setminus H$ нема елемената реда 2!)
Дакле, сада имамо $a^4 = b^4 = e$, $a^2 = b^2$ и $ba = a^3b$. Приметимо да ове услове испуњава група кватерниона, ако узмемо да је $a = i$ и $b = j$.

Закључак: Свака група реда 8 је изоморфна једној од следећих група:

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{D}_4, \quad \mathbb{Q}_8.$$

При том су прве три комутативне, а преостале две некомутативне.

Остају нам још **групе реда** 9. Ако је G реда 9, њени елементи могу бити реда 1,3 или 9. Ако у групи G постоји елемент реда 9, она ће бити циклична и изоморфна са $\mathbb{Z}_9$.

Нека су сви елементи групе G, осим неутрала, реда 3. Узмимо један од њих, a, и означимо са H подгрупу коју он генерише, $H = \{e, a, a^2\}$. Узмимо даље елемент $b \in G \setminus H$. Пошто се подгрупа $K = \{e, b, b^2\}$ генерисана са b тривијално сече са подгрупом H,

можемо да направимо 9 различитих елемената облика $a^i b^j$: $\{e, a, a^2, b, b^2, ab, a^2b, ab^2, a^2b^2\}$. Опет се питамо ком од њих је једнак ba. Лако елеминишемо првих 5 могућности. Да бисмо елиминисали последње три, кренућемо од $\omega(ab) = 3$, односно $ababab = e$. Помножићемо ову једнакост слева са a^2, а здесна са b^2 (да бисмо искористили $a^3 = b^3 = e$) и добити $baba = a^2b^2$. Ово нам је довољно да добијемо да ba не припада скупу $\{a^2b, ab^2, a^2b^2\}$ ($ba = a^2b$ би нам дало $baba = a^2ba^2b$, односно $a^2b^2 = a^2ba^2b$; скратимо слева са a^2, па здесна са b и на крају преосталим b и добијамо $a^2 = e$ што је нетачно; испитајте преостале две могућности!) Дакле, $ba = ab$. Сада у G имамо две цикличне подгрупе реда 3 чији генератори комутирају, па је $G = HK \cong H \times K \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Закључак: Свака група реда 9 је изоморфна или цикличној групи $\mathbb{Z}_9$ или групи $\mathbb{Z}_3 \times \mathbb{Z}_3$.

0.3.8 Конгруенције целих бројева и Кинеска теорема о остацима

Знамо да за сваки цео број m и природан број k постоје јединствени цели бројеви q и r такви да је $m = kq + r$ и $0 \leq r < k$. Много пута смо се ослањали на ово тврђење које се зове Лема о остатку и овде ћемо дати један његов доказ.

Лема 0.1. *За свака два броја $n \in \mathbb{N}_0$ и $k \in \mathbb{N}$ постоје јединствени бројеви $q, r \in \mathbb{N}_0$ такви да је $n = kq + r$ и $0 \leq r < k$.*

Доказ. Посматрајмо скуп $X = \{n - kl : l \in \mathbb{N}_0, n - kl \geq 0\}$, где је $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Овај скуп је непразан јер је у њему бар n. Пошто је X подскуп скупа $\mathbb{N}_0$ који је добро уређен (сваки његов непразан подскуп има најмањи елемент), и X ће имати најмањи елемент, означимо га са r. Дакле, постоји неко $q \in \mathbb{N}_0$ за које је $r = n - kq$. Јасно је да је онда $n = kq + r$. Тврдимо да важи и $0 \leq r < k$: ако би r било веће или једнако k, могло би да се представи као збир $r = k + s$ где је $s \in \mathbb{N}_0$. Одавде би следило да је и елемент $s = r - k = n - kq - k = n - k(q + 1)$ у скупу X, а он је строго мањи од r, контрадикција!

Зашто су бројеви q и r јединствени? Претпоставимо супротно, да важи $n = kq_1 + r_1$ и $n = kq_2 + r_2$ за неке $q_1, q_2 \in \mathbb{N}_0$ и $0 \leq r_1, r_2 < k$. Одузимањем ових једнакости добијамо

$$0 = k(q_1 - q_2) + (r_1 - r_2),$$

односно

$$r_2 - r_1 = k(q_1 - q_2).$$

Ако би бројеви r_1 и r_2 били различити, на пример $r_1 < r_2$, онда би важило $0 < r_2 - r_1 < k$. Сада имамо да је природан број $r_2 - r_1$ умножак природног броја k, а строго је мањи од њега, што је немогуће. Дакле, $r_1 = r_2$, па је и $q_1 - q_2 = 0$, односно $q_1 = q_2$. □

Једнозначно одређене бројеве q и r из претходног тврђења зовемо редом *количник* и *остатак* при *еуклидском дељењу* броја n природним бројем k. То да је r еуклидски остатак при дељењу броја n са k записујемо $r = rest(n, k)$ или $r = \rho(n, k)$.
Ако је у претходној леми $n = 0$, и количник и остатак при дељењу са k ће бити 0. Ако је $n > 0$ и једнакост из претходне леме помножимо са (-1), добићемо $(-n) = k(-q) - r$. Ако је овде $r = 0$, $-q$ ће бити количник, а нула остатак при еуклидском дељењу негативног целог броја $-n$ природним бројем k. Ако је $r > 0$, важиће $(-n) = k(-q - 1) + k - r$ и $0 < k - r < k$, па је овде $-q - 1$ количник, а $k - r$ остатак при еуклидском дељењу негативног целог броја $-n$ природним бројем k.

Дакле,за сваки цео број m и природан број k постоје јединствени цели бројеви q и r такви да је $m = kq + r$ и $0 \leq r < k$. Ако је овде $r = 0$, односно $m = kq$, кажемо да је цео број m *дељив* са k или да k *дели* m и пишемо $k \mid m$. Тада је k један *делилац* броја m.

Приметимо да два цела броја, m и n, дају исте остатке при еуклидском дељењу природним бројем k ако и само ако је њихова разлика дељива са k (ако дају исте остатке, јасно је да је разлика дељива са k, а за обрнути смер применимо слично разматрање као у доказу јединствености у претходној леми). У том случају кажемо да су бројеви m и n *једнаки* или *конгруентни* по *модулу* k и пишемо $m = n \ (modk)$ или $m =_k n$. Дакле,

$$m =_k n \quad \Leftrightarrow \quad \rho(m, k) = \rho(n, k) \quad \Leftrightarrow \quad k \mid m - n.$$

Лако се проверава да је $=_k$ једна релација еквиваленције у скупу целих бројева. Штавише, ова релација је сагласна и са сабирањем и са множењем целих бројева, то јест важи:

$$m =_k n \ \wedge \ m' =_k n' \quad \Rightarrow \quad m + m' =_k n + n' \ \wedge \ mm' =_k nn'.$$

(За доказ друге ћемо разлику $mm' - nn'$ трансформисати на следећи начин $mm' - nn' = mm' - mn' + mn' - nn' = m(m' - n') + (m - n)n'$ и онда искористити дељивост бројева $m - n$ и $m' - n'$ са k.)

Из уводне лекције онда знамо да смо добили једну *конгруенцију* прстена целих бројева. (Штавише, може се показати да је свака конгруенција прстена $\mathbb{Z}$ (дакле релација еквиваленције сагласна са сабирањем и множењем) облика $=_k$ за неко $k \in \mathbb{N}$).

[Знамо да су онда и на скупу класа ове конгруенције дефинисане операције које тај количнички скуп претварају у нови прстен. Шта је класа елемента m?

$$C_m = \{n \in \mathbb{Z} : m =_k n\} = \{n \in \mathbb{Z} : \ k \mid m - n\} = \{m + kl : l \in \mathbb{Z}\} = m + k\mathbb{Z}.$$

Онда је структура прстена дефинисана на скупу класа

$$\mathbb{Z}/ =_k \ = \{m + k\mathbb{Z} : m \in \mathbb{Z}\} = \{kq + r + k\mathbb{Z} : 0 \leq r < k\} = \{r + k\mathbb{Z} : 0 \leq r < k\}$$

односно,

$$\mathbb{Z}/ =_k \ = \{k\mathbb{Z}, 1 + k\mathbb{Z}, \ldots, (k-1) + k\mathbb{Z}\}.$$

Операције у њему су

$$(r + k\mathbb{Z}) + (s + k\mathbb{Z}) = (r +_k s) + k\mathbb{Z} \text{ и}$$

$$(r + k\mathbb{Z}) \cdot (s + k\mathbb{Z}) = (r \cdot_k s) + k\mathbb{Z},$$

а нула и јединица, редом, $k\mathbb{Z}$ и $1 + k\mathbb{Z}$. Приметимо да је овај прстен изоморфан прстену $\mathbb{Z}_k$.]

О овоме у угластим заградама ћемо учити више и општије у другом семестру, али приметимо сада да једнакост по модулу k можемо свести на једнакост у скупу $\mathbb{Z}_k$:

$$m =_k n \quad \Leftrightarrow \quad \rho(m, k) = \rho(n, k) \quad \Leftrightarrow \quad m = n \text{ у } \mathbb{Z}_k.$$

Пошто умемо да рачунамо у $\mathbb{Z}_k$ (нећемо говорити у прстену $\mathbb{Z}_k$ јер још увек нисмо изучавали прстене, него мислимо првенствено на његов мултипликативни моноид), применићемо то на конгруенције. На пример, осим што је $=_k$ сагласна са сабирањем и множењем, неке конгруенције можемо и да скратимо. Али пре свега, рећи ћемо пар речи о највећем заједничком делиоцу два броја и Безуовој релацији.

Нека су $m, n \in \mathbb{Z}$. Сваки од њих је сигурно дељив бројем 1 (и самим собом). То значи да можемо да посматрамо скуп $D(m, n)$ свих њихових заједничких делилаца, који није празан. Ако је овај скуп једночлан, то јест $D(m, n) = \{1\}$, за бројеве m и n кажемо да су *узајамно прости*. Овај скуп ће имати и максималан елемент у односу на релацију дељивости. Ако тај елемент означимо са d, он је одређен следећим условима:

$$d \mid m \ \ \wedge \ \ d \mid n \ \ \wedge \ (d' \mid m \ \wedge \ d' \mid n \ \Rightarrow \ d' \mid d).$$

Зовемо га *највећи заједнички делилац* бројева m и n и пишемо $d = NZD(m, n)$.

Важи: Ако је $d = NZD(m, n)$, онда постоје $x, y \in \mathbb{Z}$ тако да је $d = mx + ny$.

-Ове бројеве одређујемо применом *Еуклидовог алгоритма* за тражење највећег заједничког делиоца бројева m и n. Еуклидов алгоритам се заснива на чињеници да приликом еуклидског дељења са остатком чувамо највећи заједнички делилац. Наиме, ако је $m = nq + r$ $(m \in \mathbb{Z},\ n \in \mathbb{N})$, онда је $NZD(m,n) = NZD(n,r)$, Зашто ово важи? -Пре свега, јасно је да из $m = nq + r$ следи да сваки број који дели m и n мора да дели и r, јер је $r = m - nq$, а онда добијамо $d' \mid m \ \wedge\ d' \mid n \ \Rightarrow\ d' \mid n \ \wedge\ d' \mid r \ \Rightarrow\ d' \mid NZD(n,r)$, па и $NZD(m,n) \mid NZD(n,r)$. Слично и за обрнуто, јер сваки заједнички делилац од n и r мора да буде и заједнички делилац од m и n, па добијамо и $NZD(n,r) \mid NZD(m,n)$.

Како ово користимо да нађемо највећи заједнички делилац два броја? -Настављамо поступак еуклидског дељења, и у следећем кораку делимо n са r: $n = rq_1 + r_1$. Пошто је у $m = nq + r$ испуњено $0 \le r < n$, а сада имамо и $0 \le r_1 < r$, ако наставимо даље на исти начин, добићемо строго опадајући низ остатака: $r = r_1q_2 + r_2$, $r_1 = r_2q_3 + r_3$, ..., $r_i = r_{i+1}q_{i+2} + r_{i+2}$, ... и $r > r_1 > r_2 > \cdots \ge 0$. Овај процес се мора завршити у коначно корака, односно добијамо да је у једном тренутку остатак нула. Ако је $r_{k-2} = r_{k-1}q_k + r_k$ и $r_{k-1} = r_kq_{k+1} + 0$, тврдимо да је последњи остатак различит од нуле, то јест r_k, управо $NZD(m,n)$. Ово следи из следећег низа једнакости

$$NZD(m,n) = NZD(n,r) = NZD(r,r_1) = NZD(r_1,r_2) = \ldots = NZD(r_{k-1},r_k) = r_k.$$

Оно што нам је још важније у наставку је да идући уназад, највећи заједнички делилац бројева m и n можемо да изразимо као њихову "линеарну комбинацију" са целобројним коефицијетима. Изразићемо прво r_k преко r_{k-2} и r_{k-1} користећи претпоследњу једнакост у горњим еуклидским дељењима: $r_k = r_{k-2} - r_{k-1}q_k$. Даље, из оне пре ње, r_{k-1} изражавамо преко r_{k-2} и r_{k-3} и замењујемо у израз за r_k. Тако, ходом уназад, стижемо до n и r, и на крају, до m и n. Коефицијенти уз m и n ће бити неки цели бројеви добијени у овом рачуну.

Сама веза $d = mx + ny$, где је $d = NZD(m,n)$, а $x, y \in \mathbb{Z}$ зове се *Безуова релација.*

Последица: У случају узајамно простих бројева добијамо: Ако су m и n узајамно прости цели бројеви, онда постоје $x, y \in \mathbb{Z}$ за које је $mx + ny = 1$.

Приметимо још ово: у горњем тврђењу важи еквиваленција. Тачније: m и n су узајамно прости ако и само ако постоје $x, y \in \mathbb{Z}$ такви да је $mx + ny = 1$.

-Смер који нисмо показали следи из чињенице да сваки број који дели m и n мора да дели и $mx + ny$ за било које $x, y \in \mathbb{Z}$, а то је у нашем случају 1, па је то и једини заједнички делилац бројева m и n.

Сада се коначно враћамо на конгруенције и најављено "скраћивање".

Лема 0.2. *Ако је цео број l узајамно прост са природним бројем k, онда*

$$ml =_k nl \quad \Rightarrow \quad m =_k n.$$

Доказ. $NZD(l,k) = 1 \quad \Rightarrow \quad (\exists x, y \in \mathbb{Z})\ kx + ly = 1 \ \Rightarrow\ ly =_k 1$
Сада ћемо конгруенцију $ml =_k nl$ помножити са y (тачније помножићемо леве и десне стране конгруенција $ml =_k nl$ и $y =_k y$) и добити $mly =_k nly$. Кад искористимо $ly =_k 1$, добијамо тражену једнакост $m =_k n$. □

Теорема 0.11. *Конгруенција $mx =_k 1$ има бар једно решење (по x) ако и само ако су бројеви m и k узајамно прости. У том случају и свака од конгруенција $mx =_k n$ има решење и оно је одређено једнозначно по модулу k (односно, јединствено у скупу $\mathbb{Z}_k$).*

Доказ. Конгруенција $mx =_k 1$ је еквивалентна са $k \mid mx - 1$, а ово даље са $mx + ky = 1$ за неко $y \in \mathbb{Z}$, што значи да је $NZD(m, k) = 1$.

Нека је l једно решење ове конгруенције (на пример, оно које нам даје Еуклидов алгоритам, то јест број за који је $ml + kp = 1$). Како је $ml =_k 1$ и $n =_k n$, множењем добијамо $mln =_k n$, то јест $x = ln$ је решење конгруенције $mx =_k n$. Оно је одређено једнозначно по модулу k, јер ако би важило $mr =_k n =_k ms$, из тога што су m и k узајамно прости и претходног тврђења бисмо имали $r =_k s$. Дакле, решење сваке конгруенције $mx =_k n$ је јединствено у $\mathbb{Z}_k$. □

У случају када је k прост број који не дели m, једно конкретно решење претходне конгруенције даје следећа теорема.

Теорема 0.12. (Мала Фермаова теорема) *Ако прост број p не дели цео број m, онда је*

$$m^{p-1} =_p 1.$$

Доказ. За сваки цео број m постоји $r \in \mathbb{Z}_p$ за које је $m =_p r$ (то је његов еуклидски остатак при дељењу са p). Ако p не дели m, биће $r \neq 0$, па r припада скупу $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$. Међутим, знамо да је овај скуп група (група инверзибилних елемената моноида $(\mathbb{Z}_p, \cdot_p, 1)$, имали смо већ)! Сада просто применимо "ред елемента дели ред групе": $|\mathbb{Z}_p^*| = p - 1$, па за свако $r \in \mathbb{Z}_p^*$ важи $\omega(r) \mid p - 1$, односно $r^{p-1} = 1$ у $\mathbb{Z}_p$.
Сада је $m^{p-1} =_p r^{p-1} =_p 1$. □

Дакле, ако је p прост број који не дели m, једно решење конгруенције $mx =_p 1$ је $x = m^{p-2}$, а ако треба да решимо конгруенцију $mx =_p n$, из $m^{p-1} =_p 1$ добијамо $m^{p-1}n =_p n$, односно $m \cdot m^{p-1}n =_p n$, што значи да је једно њено решење $\bar{x} = m^{p-1}n$ (а сва $x =_p m^{p-1}n$).

Размотримо сада односе између различитих конгруенција у скупу целих бројева, односно конгруенција по различитим модулима.

Теорема 0.13. (Кинеска теорема о остацима) *Ако су r и s произвољни и m и n узајамно прости цели бројеви, тада конгруенције*

$$x =_m r \quad и \quad x =_n s$$

имају тачно једно заједничко решење по модулу mn, то јест постоји цео број $k \in \{0, 1, \ldots, mn - 1\}$ за који су са $x =_{mn} k$ одређена сва њихова заједничка решења.

Доказ. Из $x =_m r$ следи да је x облика $x = r + my$ за неко $y \in \mathbb{Z}$. Уврстимо ово сада у другу конгруенцију. Добијамо $r + my =_n s$, односно $my =_n s - r$. Овде су бројеви m и n узајамно прости, па, по претходном тврђењу, ова конгруенција има бар једно решење, $y = t$. Онда је $x = r + mt$ заједничко решење ових конгруенција. Покажимо и да је решење овог система конгруенција јединствено у $\mathbb{Z}_{mn}$. Нека су k и l била која заједничка решења ових конгруенција. Тада важи: $k =_m r$, $k =_n s$, као и $l =_m r$ и $l =_n s$. Из $k =_m r$ и $l =_m r$ добијамо да $m \mid k - l$, а из $k =_n s$ и $l =_n s$ да $n \mid k - l$. Одавде следи да $mn \mid k - l$, јер су бројеви m и n узајамно прости. То тачно значи да је $k =_{mn} l$, односно сва заједничка решења ових конгруенција једнака су по модулу mn (разликују се до на умножак броја mn). Онда су сва облика $k + t(mn)$, где је $t \in \mathbb{Z}$, а k јединствено решење из скупа $\mathbb{Z}_{mn}$. □

0.3.9 Ојлерова функција и теорема

У претходној лекцији смо знање из теорије група применили да добијемо доказ познатог тврђења из елементарне теорије бројева - Мале Фермаове теореме. Сада ћемо урадити исто, само што нећемо посматрати групу инверзибилних елемената моноида $\mathbb{Z}_p$, него произвољног $\mathbb{Z}_n$ за $n \in \mathbb{N}$. Имали смо већ у примерима група да та група има посебан назив, *Ојлерова група*, $\Phi_n = \mathbb{Z}_n^*$.

[**Напомена** Сада можемо да покажемо да је елемент $r \in \mathbb{Z}_n$ инверзибилан ако и само ако је узајамно прост са n без ослањања на друге изворе. Имали смо у прошлој лекцији да су два броја узајамно проста ако и само ако постоји њихова целобројна линеарна комбинација која је једнака 1. Дакле, r и n су узајамно прости ако и само ако постоје $x, y \in \mathbb{Z}$ такви да је $rx + ny = 1$. Ова релација је даље еквивалентна са $rx =_n 1$, односно са $r \cdot_n x = 1$ што значи да r има инверз у моноиду $\mathbb{Z}_n$ (тај инверз је еуклидски остатак који x даје при дељењу са n).]

Дакле,

$$\Phi_n = \{r \in \mathbb{Z}_n : NZD(r, n) = 1\}.$$

Ред ове групе је онда

$$|\Phi_n| = |\{1 \leq r \leq n : NZD(r, n) = 1\}|,$$

а то је управо вредност *Ојлерове функције* $\varphi(n)$. На пример, $|\Phi_1| = \varphi(1) = 1$, $|\Phi_2| = \varphi(2) = 1$, $|\Phi_3| = \varphi(3) = 2$, $|\Phi_4| = \varphi(4) = 2$ и тако даље. Приметимо да за сваки прост број p важи $\varphi(p) = p - 1$, а лако се показује да је на степенима простих бројева вредност Ојлерове функције $\varphi(p^n) = p^n - p^{n-1}$: који бројеви у низу $1, 2, \ldots, p, p+1, \ldots, 2p, \ldots, 3p, p^2, \ldots, p^3, \ldots, p^n - 1$ нису узајамно прости са p^n? -То су сви бројеви који имају бар једно p као фактор, односно сваки p-ти, па оних који јесу узајамно прости са p^n има $p^n - \frac{p^n}{p}$. Ово можемо искористити да израчунамо вредност Ојлерове функције

на сваком природном броју, јер је Ојлерова функција *мултипликативна аритметичка функција*. То значи да је $\varphi(1) = 1$ и $\varphi(mn) = \varphi(m)\varphi(n)$ кад год су природни бројеви mи n узајамно прости. Ово се доказује тако што се посматра Декартов производ прстена $\mathbb{Z}_m$ и $\mathbb{Z}_n$, који је за узајамно просте m и n изоморфан прстену $\mathbb{Z}_{mn}$ (ми нисмо радили још ни директан производ група, али лако се провери да је, за операције дефинисане по компонентама, Декартов производ два прстена поново прстен). Елемент из Декартовог производа је инверзибилан акко су његове компоненте инверзибилне у одговарајућим прстенима, па је $|\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^*||\mathbb{Z}_n^*|$.

Важи: Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација природног броја n на производ простих, онда је

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Доказ: Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, где су p_i прости. Онда су и њихови степени узајамно прости, па из мултипликативности Ојлерове функције следи

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) =$$

$$\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) =$$

$$(p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k-1}) =$$
$$p_1^{\alpha_1}(1 - \frac{1}{p_1})p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdots p_k^{\alpha_k}(1 - \frac{1}{p_k}) =$$
$$n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}) =$$
$$n \prod_{p|n} (1 - \frac{1}{p}).$$

-Поново ћемо знање о групама и редовима елемената искористити да докажемо познато тврђење из елементарне теорије бројева.

Теорема 0.14. (Ојлерова теорема) *За сваки цео број m који је узајамно прост са n важи*

$$m^{\varphi(n)} =_n 1.$$

Доказ. Као и у доказу Мале Фермаове теореме, опет ћемо применити "ред елемента дели ред групе", само овог пута у Ојлеровој групи Φ_n. Пошто је m узајамно прост са n, важиће да $m \in \mathbb{Z}_n^* = \Phi_n$. Прецизније, $m =_n r$ за неко $r \in \mathbb{Z}_n^* = \Phi_n$ јер ако је $m = nq + r$ и m и n немају заједничких делилаца осим 1, онда и $r = m - nq$ и n немају заједничких делилаца различитих од 1. Пошто је $r \in \Phi_n$, а ред елемента дели ред групе, биће $r \cdot_n r \cdot_n \cdots \cdot_n r = 1$, при чему смо r множили са собом $|\Phi_n| = \varphi(n)$ пута, односно $r^{\varphi(n)} =_n r^{|\Phi_n|} =_n 1$. Зато је

$$m^{\varphi(n)} =_n r^{\varphi(n)} =_n 1.$$

□

-Приметимо да је Мала Фермаова теорема специјалан случај Ојлерове, за $n = p$ прост. Ојлерова теорема има широку примену при рачунању са конгруенцијама.

0.3.10 Вилсонова теорема

Теорема 0.15. (Вилсонова теорема) *Број p је прост ако и само ако важи $p \mid 1 + (p-1)!$.*

Доказ. -Нека је p прост број. Ако је $p = 2$, важи $2 \mid 1 + (2-1)!$. Нека је сада p прост број већи од 2. То значи да је p непаран. Желимо поново да искористимо оно што знамо о реду елемента и групе, зато ћемо посматрати групу инверзибилних елемената моноида $\mathbb{Z}_p^*$. Пошто је p прост, са њим су узајамно прости сви природни бројеви мањи од њега, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$. Дакле, за свако $r \in \mathbb{Z}_p^*$ важи $r^{|\mathbb{Z}_p^*|} = r^{p-1} =_p 1$ или $r^{p-1} - 1 =_p 0$. То значи да свако $r \in \mathbb{Z}_p^*$ поништава полином $a(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$. Ово је полином степена $p-1$ и у неком пољу он може да има највише $p-1$ различиту нулу. Закључујемо да су све нуле полинома $a(x)$ тачно $1, 2, \ldots, p-1$, па се он факторише на следећи начин у $\mathbb{Z}_p$:

$$a(x) = x^{p-1} - 1 = (x-1)(x-2) \cdots (x-(p-1)).$$

Заменимо $x = 0$ (израчунајмо вредност и леве и десне стране у нули):

$$a(0) = (0-1)(0-2)\cdots(0-(p-1)),$$

односно,

$$-1 = (-1)(-2)\cdots(-(p-1)).$$

Ово је једнакост у пољу $\mathbb{Z}_p$, па је у $\mathbb{Z}$ она еквивалентна са:

$$-1 =_p (-1)(-2)\cdots(-(p-1)) =_p (-1)^{p-1}1\cdot 2\cdots(p-1).$$

Како је p непаран, биће $(-1)^{p-1} = 1$, па коначно добијамо

$$-1 =_p (p-1)!,$$

што смо и желели.

-Докажимо и други смер тражене еквиваленције. Нека је p број за који важи $p \mid 1 + (p-1)!$. Претпоставимо да p није прост, односно да има праву факторизацију. Нека је $p = r \cdot s$ за неке $1 < r, s < p$. Сада добијамо

$$r \cdot s \mid 1 + 1\cdot 2\cdots r\cdots s\cdots(p-1).$$

Пошто r (или s, свеједно) дели $(p-1)!$, а дели и збир на десној страни, следи да $r \mid 1$. Ово је у супротности са нашом претпоставком да је r прави фактор броја p. Дакле, p нема растав на производ бројева мањих од њега, па је прост. □

0.3.11 Нормалне подгрупе и количничка група

Дефиниција 0.24. За подгрупу H групе G кажемо да је *нормална* у G ако за сваки елемент $a \in G$ важи $aH = Ha$, или, еквивалентно, $a^{-1}Ha = H$.

Пишемо $H \lhd G$.

Први услов се односи на једнакост одговарајућих левих и десних косета, а други на једнакост подгрупе H и свих њених конјугата, то јест, њену инваријантност у односу на унутрашње аутоморфизме $\pi_a : G \to G$ одређене са $\pi_a(x) = a^{-1}xa$, због чега се нормалне подгрупе зову и *инваријантне*. У ствари, да би H била нормална подгрупа групе G довољно је да важи $a^{-1}Ha \subseteq H$ за свако $a \in G$, односно $\pi_a(H) \subseteq H$ за свако $a \in H$. То је зато што из ове релације следи $\pi_{a^{-1}}(\pi_a(H)) \subseteq \pi_{a^{-1}}(H)$ за свако $a \in H$, односно $H \subseteq \pi_{a^{-1}}(H)$ за свако $a \in H$, што је $H \subseteq aHa^{-1}$ за свако $a \in H$, а то је управо обрнута инклузија.

Пример 0.29. 1) Тривијалне подгрупе групе G су њене нормалне подгрупе, $\{e\}$, $G \lhd G$. Ако група G нема праве нормалне подгрупе (подгрупе различите од $\{e\}$ и G), кажемо да је она *проста*.

2) У Абеловој групи све подгрупе су нормалне.

3) Језгро било ког хомоморфизма $f : G \to K$, дефинисано са

$$Kerf = \{g \in G : \ f(g) = \varepsilon_K\},$$

где је ε_K неутрал групе K, је увек нормална подгрупа групе G: прво, језгро јесте подгрупа групе G јер за $g, h \in Kerf$ следи $f(g^{-1}h) = f(g)^{-1}f(h) = \varepsilon_K$, односно $g^{-1}h \in Kerf$; даље, за $a \in G$ и $g \in Kerf$ важи $f(a^{-1}ga) = f(a^{-1})f(g)f(a) = f(a)^{-1}\varepsilon_K f(a) = \varepsilon_K$, па и $a^{-1}ga$ припада језгру, што даје $a^{-1}Kerfa \subseteq Kerf$.

4) Ако је релација $\sim$ једна конгруенција групе G (еквиваленција која је сагласна са операцијом у G: $a \sim b \ \wedge \ c \sim d \ \Rightarrow \ ac \sim bd$), онда је класа неутрала једна нормална подгрупа групе G : $C_e = \{g \in G : g \sim e\} \lhd G$.
-Нека је $g \in C_e$, $a \in G$. Онда из $g \sim e$ и $a^{-1} \sim a^{-1}$ следи $a^{-1}g \sim a^{-1}e = a^{-1}$, а из ове релације и $a \sim a$ је даље $a^{-1}ga \sim a^{-1}a = e$, па и $a^{-1}ga \in C_e$, што значи $a^{-1}C_e a \subseteq C_e$.

5) Свака подгрупа индекса 2 је нормална.
-Нека је $[G : H] = 2$. То значи да постоје укупно 2 лева косета, H и aH. Први је одређен било којим представником из H ($aH = H$ само за $a \in H$), а други било којим a које не припада H. То важи и за десне косете. Дакле $G = H \sqcup aH = H \sqcup Ha$ за било које a које није у H. Ово даје $aH = Ha = G \setminus H$ за свако a које није у H. Наравно, за $a \in H$ је $aH = Ha = H$, па су и овде једнаки леви и десни косет одређен истим елементом.

Последица: $\mathcal{R}_n \lhd D_n$ ($\mathcal{R}_n$ је подгрупа ротација у диедарској групи степена n);
$A_n \lhd S_n$ (A_n је алтернирајућа група степена n)

Пример 0.30. 1) $H \lhd G, \ K \leq G \ \Rightarrow \ HK \leq G$
Знамо да је $HK \leq G$ акко је $HK = KH$. Ако је H нормална подгрупа групе G, онда је $kH = Hk$ и за свако $k \in K$, па је

$$KH = \bigcup_{k \in K} kH = \bigcup_{k \in K} Hk = HK.$$

2) $H \lhd G,\ K \lhd G \ \Rightarrow\ HK \lhd G$

Да би производ био подгрупа, по управо доказаном, довољно је да је једна од ових подгрупа нормална. Остаје да проверимо нормалност производа:

$$a^{-1}HKa = (a^{-1}Ha)(a^{-1}Ka) = HK.$$

Зашто су нам важне нормалне подгрупе? -Зато што помоћу њих можемо да направимо нове групе. Подсетимо се релације $\sim_H$ из доказа Лагранжове теореме, одређене датом подгрупом H: $a \sim_H b \ \Leftrightarrow\ a^{-1}b \in H$. Она је релација еквиваленције и њене класе су управо леви косети подгрупе H у групи G. Међутим, ако је подгрупа H и нормална у групи G, ова релација постаје сагласна са операцијом у G:

$$a \sim_H b \ \wedge\ c \sim_H d \ \Rightarrow\ aH = bH \ \wedge\ cH = dH \ \Rightarrow\ aHcH = bHdH,$$

и сада искористимо једнакост одговарајућих левих и десних косета подгрупе H да заменимо $Hc = cH$ и $Hd = dH$, па је даље

$$acHH = bdHH \ \Rightarrow\ acH = bdH \ \Rightarrow\ ac \sim_H bd.$$

Дакле, добили смо једну конгруенцију и онда знамо да скуп њених класа такође једна група. У њој је операција дефинисана тако да је "производ класа једнак класи производа", то јест

$$aH \bullet bH = abH.$$

(Могли смо и без помињања речи конгруенција, просто из горњег низа импликација издвојимо $aH = bH \ \wedge\ cH = dH \ \Rightarrow\ acH = bdH$ и то управо значи да је на скупу класа добро дефинисана операција $aH \bullet bH = abH$.) Неутрал у овој групи је класа неутрала у групи G, а то је $eH = H$, док је инверз косета aH косет инверза елемента a: $(aH)^{-1} = a^{-1}H$. Дакле, скуп косета нормалне подгрупе H је једна група, која се зове *количничка група* групе G по њеној нормалној подгрупи H. Пошто су код нормалне подгрупе десни косети једнаки одговарајућим левим, више не наглашавамо да ли је у питању скуп једних или других, и количничку групу означавамо G/H.

Још једном: $H \lhd G$ повлачи да је $G/H = \{aH : a \in G\}$ група са операцијама

$$aH \bullet bH = abH$$
$$aH \bullet H = aH$$
$$(aH)^{-1} = a^{-1}H,$$

и она се зове количничка или фактор група дате групе G по њеној нормалној подгрупи H.

Пресликавање $\pi : G \to G/H$ које елементу групе додељује његов косет, $\pi(a) = aH$, је у овом случају и један хомоморфизам група, који је очигледно и "на":

$$\pi(ab) = abH = aH \bullet bH = \pi(a) \bullet \pi(b).$$

То значи да је количничка група хомоморфна слика почетне групе. Шта ће она бити зависи од групе од које полазимо и подгрупе по којој је "сечемо". Приметимо такође

да је језгро епиморфизма π управо сама подгрупа H: $Ker\pi = \{a \in G : \pi(a) = H\} = \{a \in G : aH = H\} = \{a \in G : a \in H\} = H$.

Напомена Појмови нормалне подгрупе, хомоморфизма и конгруенције су еквивалентни:

1) Свака нормална подгрупа индукује један хомоморфизам и једну конгруенцију (то смо управо описали):
$H \lhd G \ \Rightarrow \sim_H$ је конгруенција и $\pi : G \to G/H$ је хомоморфизам

2) Сваки хомоморфизам индукује једну нормалну подгрупу и једну конгруенцију:
$f : G \to K$ хомоморфизам група $\Rightarrow \ Kerf \lhd G$ и релација $\sim$ дефинисана са

$$a \sim b \ \Leftrightarrow \ f(a) = f(b)$$

је конгруенција групе G (ово једино нисмо доказали, проверите!)

3) Свака конгруенција индукује једну нормалну подгрупу и један хомоморфизам:
$\sim$ конгруенција групе $G \Rightarrow \ C_e \lhd G$ и пресликавање $\pi : G \to G/\sim$ које елементу додељује његову класу еквиваленције је хомоморфизам група

Пример 0.31. 1) За било који подскуп S групе G дефинисана је подгрупа $N_S = \{a \in G : aS = Sa\}$ која се зове *нормализатор* скупа S у групи G. Посебно, ако је H нека подгрупа групе G, њен нормализатор је највећа подгрупа групе G у којој је H нормална (ово следи из саме дефиниције, $H \lhd N_H = \{a \in G : aH = Ha\}$), па је $H \lhd G \ \Leftrightarrow \ N_H = G$.

2) За било који подскуп S групе G дефинисана је подгрупа $C_S = \{a \in G : (\forall s \in S)\ as = sa\}$ која се зове *централизатор* скупа S у групи G. Посебно, централизатор саме групе G се зове *центар групе* G: $C_G = \{a \in G : (\forall g \in G)\ ag = ga\}$. Јасно је да је група комутативна ако и само ако је $C_G = G$. Центар је нормална подгрупа групе G, само што не мора да буде права (групе у којима је центар тривијалан, $C_G = \{e\}$ зову се и групе без центра). Оно што увек важи је да *индекс центра не може да буде прост број.* *

Доказ *: Прво ћемо доказати да важи

Ако је C_G центар групе G, група G/C_G је циклична ако и само ако је група G Абелова.

$\Rightarrow$ Нека је група G/C_G генерисана елементом aC_G. То значи да су за произвољне $g_1, g_2 \in G$ косети одређени њима неки степени косета aC_G у количничкој групи: $g_1C_G = (aC_G)^m$ и $g_2C_G = (aC_G)^n$, односно $g_1C_G = a^mC_G$ и $g_2C_G = a^nC_G$. Сада из једнакости два косета добијамо $g_1 = a^mc_1$ и $g_2 = a^nc_2$ за неке $c_1, c_2 \in C_G$. Пошто елементи из центра комутирају са свим осталим елементима, а степени елемента a међусобно, коначно имамо

$$g_1g_2 = a^mc_1a^nc_2 = a^{m+n}c_1c_2 = a^nc_2a^mc_1 = g_2g_1.$$

$\Leftarrow$ Ако је група G комутативна, њен центар је једнак целој групи, па је $G/C_G = G/G = \{G\} \cong \{e\}$ једночлана група, која је и циклична.

Претпоставимо сада да је $[G : C_G] = p$, где је p прост број. То значи да је $|G/C_G| = p$. Пошто је свака група простог реда циклична, G/C_G је циклична, а онда је, по претходно доказаном, G Абелова. Међутим, онда је њен центар цела група, па није индекса p!

0.3.12 Теореме о изоморфизмима

Нека је $f : G \to K$ било који хомоморфизам група. Њиме су одређене две подгрупе, једна групе G, а друга групе K. Прва је *слика хомоморфизма*, подскуп који се природно дефинише као скуп слика свих елемената групе G:

$$Imf = \{f(g) : \ g \in G\}.$$

Ово је једна подгрупа групе K: ако су $k_1, k_2 \in Imf$, постоје $g_1, g_2 \in G$ такви да је $k_1 = f(g_1)$ и $k_2 = f(g_2)$, па је $k_1k_2 = f(g_1)f(g_2) = f(g_1g_2) \in Imf$, као и $k_i^{-1} = f(g_i)^{-1} = f(g_i^{-1}) \in Imf$, за $i \in \{1, 2\}$.
Друга је *језгро хомоморфизма* дефинисано са

$$Kerf = \{g \in G : \ f(g) = \varepsilon_K\},$$

и већ смо показали да је ово једна нормална подгрупа групе G.

Као што смо имали код векторских простора, и код група слика "мери" сурјективност пресликавања f, а језгро инјективност, односно важи:

$$f \text{ је 'на' ако и само ако је } Imf = K,$$

$$f \text{ је '1-1' ако и само ако је } Kerf = \{e_G\}.$$

Прва еквиваленција је јасна, док друга следи из $f(g_1) = f(g_2) \ \Leftrightarrow \ f(g_1^{-1}g_2) = \varepsilon_K \ \Leftrightarrow \ g_1^{-1}g_2 \in Kerf$, па ако је $Kerf = \{e_G\}$, из $f(g_1) = f(g_2)$ ће следити $g_1 = g_2$.
Однос између ових подгрупа даје следећа теорема, која се још зове *Теорема о хомоморфизму* или *Теорема о разлагању хомоморфизма.*

Теорема 0.16. (Прва теорема о изоморфизму) *Нека је $f : G \to K$ хомоморфизам група. Тада је*

$$G/Kerf \cong Imf.$$

Доказ. Дефинисаћемо пресликавање $\Phi : G/Kerf \to Imf$ са $\Phi(gKerf) = f(g)$. Пошто је Φ дефинисано на косетима подгрупе $Kerf$ треба прво показати да је добро дефинисано, то јест да не зависи од избора представника класе еквиваленције.

$$g_1Kerf = g_2Kerf \ \Leftrightarrow \ g_1^{-1}g_2 \in Kerf \ \Leftrightarrow \ f(g_1^{-1}g_2) = \varepsilon_K \ \Leftrightarrow \ f(g_1)^{-1}g_2 = \varepsilon_K \ \Leftrightarrow \ f(g_1) = f(g_2).$$

Овим смо показали не само да је Φ добро дефинисано, већ и да из $\Phi(g_1Kerf) = \Phi(g_2Kerf)$, то јест $f(g_1) = f(g_2)$ следи $g_1Kerf = g_2Kerf$ (свуда су важиле еквиваленције, па претходни низ читамо здесна улево), односно да је Φ '1-1'. Ово пресликавање је јасно и 'на', јер је сваки елемент из $k \in Imf$ облика $k = f(g)$ за неко $g \in G$, а самим тим и $k = \Phi(gKerf)$.
Остаје да покажемо да је Φ хомоморфизам, што ће следити из дефиниције множења у количничкој групи и тога што је f хомоморфизам:

$$\Phi(g_1Kerf \bullet g_2Kerf) = \Phi(g_1g_2Kerf) = f(g_1g_2) = f(g_1)f(g_2) = \Phi(g_1Kerf)\Phi(g_1Kerf).$$

Дакле, пресликавање Φ је бијекција и хомоморфизам, па је и један изоморфизам група $G/Kerf$ и Imf. $\square$

-Претходна теорема се зове теорема о разлагању хомоморфизма, јер се f заправо разлаже на композицију епиморфизма $\pi : G \to G/Kerf$, управо дефинисаног пресликавања Φ и инклузије $\sigma : Imf \to K$ (дефинисане са $\sigma(k) = k$ за $k \in Imf$):

$$f = \sigma \circ \Phi \circ \pi.$$

Однос између пресека и производа две подгрупе исте групе, при чему је једна од њих и нормална, даје следећа теорема.

Теорема 0.17. (Друга теорема о изоморфизму) *Нека су H и K подгрупе групе G, при чему је подгрупа H нормална. Тада је $H \cap K \lhd K$ и важи*

$$HK/H \cong K/H \cap K.$$

Доказ. Пошто је $H \lhd G$, можемо да направимо количничку групу G/H. Посматраћемо пресликавање $f : K \to G/H$ дефинисано са $f(k) = kH$. Приметимо да је ово рестрикција природног епиморфизма $\pi : G \to G/H$, па је и f хомоморфизам. Наћи ћемо његово језгро и слику и применити претходну теорему. За елемент $k \in K$ важи да је у језгру пресликавања f ако је $f(k)$ неутрал у групи G/H, а то је H. Дакле, $k \in Kerf \Leftrightarrow kH = H$, а ово значи да је $k \in H$. Сада имамо $k \in K$ и $k \in H$, па је $Kerf = H \cap K$. Остаје да одредимо слику. Из саме дефиниције пресликавања је $Imf = \{kH : k \in K\}$, али не можемо писати да је то K/H јер није $H \subseteq K$ па та група и не постоји. Међутим, сваки елемент из подгрупе HK (која постоји јер је $H \lhd G$ и $K \leq G$) је облика hk за неке $h \in H,\ k \in K$. Пошто је $HK = KH$ (имали смо $HK \leq G$ акко $HK = KH$, а следи и из нормалности H), постоје и $h' \in H, k' \in K$ за које је дато hk једнако $k'h'$. Дакле, ако узмемо потпуно произвољно $k \in K$ и $h \in H$, онда је $kH = khh^{-1}H = khH$, па је скуп свих kH, за $k \in K$, једнак KH/H (ова група постоји, јер $H \lhd G$ повлачи $H \lhd KH$), односно $Imf = KH/H$. Кад применимо Прву теорему и једнакост $HK = KH$, добијамо

$$K/H \cap K \cong HK/H.$$

$\square$

Ако је сада $H \lhd G$, питамо се какав је однос између подгрупа групе G и подгрупа количника G/H. Одговор на ово питање даје последња теорема о изоморфизму.

Теорема 0.18. (Трећа теорема о изоморфизму) *Нека је H нормална подгрупа групе G. Тада свакој подгрупи групе G која садржи H одговара тачно једна подгрупа групе G/H, и обрнуто. Такође, ако је K нормална подгрупа групе G која садржи дату H, биће и $K/H \lhd G/H$, и још важи*

$$(G/H)/(K/H) \cong G/K.$$

Доказ. Нека је K било која подгрупа групе G која садржи дату нормалну подгрупу H. Тврдимо да је тада K/H једна подгрупа групе G/H. Ово се лако провери захваљујући томе што је $K \leq G$: ако $k_1H, k_2H \in K/H$ онда је $k_1H \bullet k_2H = k_1k_2H \in K/H$ јер $k_1k_2 \in K$,

а за $kH \in K/H$ је и $(kH)^{-1} = k^{-1}H \in K/H$ јер $k \in K \Rightarrow k^{-1} \in K$. Међутим, важи и обрнуто: сваку подгрупу групе G/H можемо да "вратимо" у подгрупу групе G која садржи H. Нека је $\mathcal{K}$ једна таква подгрупа количника G/H. Дефинишимо $K = \{k \in G : kH \in \mathcal{K}\}$. Тврдимо да је ово једна подгрупа од G. Нека $k_1, k_2 \in K$, то значи да $k_1H, k_2H \in \mathcal{K}$ па је и њихов производ k_1k_2H у $\mathcal{K}$, што из начина на који смо дефинисали K повлачи да $k_1k_2 \in K$. На исти начин, из $k \in K$ следи $kH \in \mathcal{K}$, а онда подгрупа $\mathcal{K}$ садржи и инверз $(kH)^{-1} = k^{-1}H$, што тачно значи да $k^{-1} \in K$. Дакле, $K \leq G$, и остаје само да констатујемо да она свакако садржи H, јер за било које $h \in H$ важи $hH = H$, а то припада $\mathcal{K}$ као неутрал групе G/H. Значи, у ствари је $\mathcal{K} = K/H$ и придруживање $K \mapsto K/H$ је једна бијекција скупа свих подгрупа групе G које садрже H на скуп свих подгрупа групе G/H.

Нека је сада K нормална подгрупа групе G која садржи дату нормалну подгрупу H. Треба показати да додатно важи $K/H \lhd G/H$. Узмимо произвољан елемент $aH \in G/H$ и конјугујмо њиме произвољно $kH \in K/H$. Добијамо $(aH)^{-1}kH(aH) = a^{-1}kaH$, па како је $K \lhd G$, биће $a^{-1}ka \in K$, а самим тим и $(aH)^{-1}kH(aH) \in K/H$. (Јасно је да важи и обрнуто, ако је $\mathcal{K} = K/H$ нормална подгрупа групе G/H, онда из $(aH)^{-1}kH(aH) = a^{-1}kaH \in K/H$ следи да $a^{-1}ka \in K$.) Да бисмо показали да важи тражени изоморфизам (наравно, и даље под условом да је K нормална подгрупа групе G која садржи дату H), посматраћемо пресликавање $f : G/H \to G/K$ дефинисано са $f(gH) = gK$. Оно је пре свега добро дефинисано јер из $g_1H = g_2H$ следи $(g_1)^{-1}g_2 \in H$, али како је $H \subseteq K$ важиће и $(g_1)^{-1}g_2 \in K$, па је $g_1K = g_2K$. Јасно је да је ово пресликавање 'на'. Наћи ћемо му језгро: $Kerf = \{gH \in G/H : f(gH) = K\} = \{gH \in G/H : gK = K\} = \{gH \in G/H : g \in K\} = K/H$. Сада из $(G/H)/Kerf \cong Imf$ добијамо

$$(G/H)/(K/H) \cong G/K.$$

□

0.3.13 Разлагања групе

Декартов производ група $(G_1, \cdot, e_1, ^-)$ и $(G_2, \circ, e_2, \tilde{})$ је група $G_1 \times G_2$ у којој су операције дефинисане по координатама: $(g_1, g_2)\bullet(g_1', g_2') = (g_1 \cdot g_1', g_2 \circ g_2')$, $e_{G_1 \times G_2} = (e_1, e_2)$, $(g_1, g_2)^{-1} = (\bar{g_1}, \tilde{g_2})$.

На пример, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}_n \times \mathbb{Z}$, $\mathbb{Z}_m \times \mathbb{Z}_n$ су групе које су Декартови производи нама познатих група.

Пример 0.32. Важи:

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \quad \Leftrightarrow \quad NZD(m, n) = 1.$$

-Доказ имате код Николе, задаци 63. и 64.

Ако је група G Декартов производ група G_1 и G_2, оне нису формално подгрупе од G. Међутим, постоје њихове "копије" које јесу подгрупе групе G. Зашто уопште

желимо да представимо G као Декартов производ неких група? -Зато што онда можемо да искористимо оно што знамо о њима да бисмо добили информације о G, јер оне задржавају своје особине у Декартовом производу, међу њима "нема мешања". На пример, $G = G_1 \times G_2$ је комутативна ако и само ако су G_1 и G_2 комутативне. Ускоро ће се испоставити да је свака комутативна група производ неких цикличних, а о њима знамо све.
Вратимо се на део "ако је $G = G_1 \times G_2$, онда постоје подгрупе групе G изоморфне групама G_1 и G_2". Шта су те подгрупе? Посматрајмо пресликавања $\pi_1 : G_1 \times G_2 \to G_1$ и $\pi_2 : G_1 \times G_2 \to G_2$ дефинисана са $\pi_1(g_1, g_2) = g_1$ и $\pi_2(g_1, g_2) = g_2$. Она се зову *пројекције* и на основу дефиниције операција у Декартовом производу јасно је да су то епиморфизми (прва координата производа једнака је производу првих координата, и исто за другу). Шта су њихова језгра, односно шта се слика са π_1 у e_1 (или са π_2 у e_2)? То ће бити елементи Декартовог производа чија је прва координата e_1 (односно e_2). Дакле, $Ker\pi_1 = \{e_1\} \times G_2$ и $Ker\pi_2 = G_1 \times \{e_2\}$. Знамо да су језгра хомоморфизама нормалне подгрупе, па онда група G која је Декартов производ група G_1 и G_2 има нормалне подгрупе H и K изоморфне тим групама G_1 и G_2, $H = \{e_1\} \times G_2 \cong G_2$ и $K = G_1 \times \{e_2\} \cong G_1$. Приметимо да је једини заједнички елемент тих подгрупа неутрал групе G, $H \cap K = \{(e_1, e_2)\} = e_G$. Такође, важи и

$$(g_1, g_2) = (e_1, g_2) \bullet (g_1, e_2) = (g_1, e_2) \bullet (e_1, g_2)$$

за свако $(g_1, g_2) \in G$, па добијамо $G = HK (= KH)$, као и то да подгрупе H и K комутирају члан по члан. Приметимо да претходна једнакост значи и да сваки елемент из G има јединствени растав као производ једног елемента из H и једног из K!

Да резимирамо, ако је $G = G_1 \times G_2$, онда у групи G постоје подгрупе H и K за које важи $H \cong G_2$, $K \cong G_1$ и

$$H, K \lhd G,\ G = HK,\ H \cap K = \{e_G\},$$

као и

$$(\forall h \in H, k \in K)\ hk = kh\ \wedge\ (\forall g \in G)(\exists_1 h \in H, k \in K)\ g = hk.$$

Сада се питамо следеће: да ли за произвољну групу G постоје њене (праве) подгрупе H и K за које је $G \cong H \times K$? Оне су онда мањих редова од G и вероватно једноставније. Видели смо да $G = G_1 \times G_2$ значи читав низ услова за њене подгрупе H и K изоморфне са G_1 и G_2, па је тако очекивано и следеће тврђење.

Теорема 0.19. *За групу G и њене подгрупе H и K следећи услови су еквивалентни:*
1) *$G \cong H \times K$ и $\pi : (h, k) \mapsto hk$ је један изоморфизам групе $H \times K$ на групу G;*
2) *$H, K \lhd G,\ G = HK,\ H \cap K = \{e\}$;*
3) *$hk = kh$ за све $h \in H,\ k \in K$ и свако $g \in G$ се на јединствен начин представља као производ једног елемента из H и једног из K.*

Доказ. Еквивалентност наведених услова ћемо доказати као ланац импликација.

1) $\Rightarrow$ 2) Нека је $G \cong H \times K$ и $\pi : H \times K \to G$ изоморфизам. Посматрајмо подгрупе $\widetilde{K} = \{e\} \times K$ и $\widetilde{H} = H \times \{e\}$ групе $H \times K$. Управо смо видели (у коментару испред теореме) да су то две нормалне подгрупе од $H \times K$ које се секу по неутралу (e, e) те групе и као производ дају целу групу: $\widetilde{H}\widetilde{K} = H \times K$. Онда исто важи и за њихове слике при изоморфизму π (изоморфизам чува све особине и подструктуре). Дакле,

за $H = \pi(\widetilde{H})$ и $K = \pi(\widetilde{K})$ у групи G важи све исто што за $\widetilde{H}$ и $\widetilde{K}$ важи у $H \times K$: $H, K \lhd G,\ G = HK,\ H \cap K = \{e\}$.

2) $\Rightarrow$ 3) Нека су $h \in H$ и $k \in K$ произвољни елементи. Приметимо да је $hk = kh$ акко је $h^{-1}k^{-1}hk = e$. Зато ћемо посматрати елемент $h^{-1}k^{-1}hk$. Пошто је $H \lhd G$, $k^{-1}hk$ припада H као конјугат елемента из H. Подгрупа H је затворена и за инвертовање и множење, па је онда и цео производ $h^{-1}(k^{-1}hk)$ у H. Истим аргументима показујемо да је $h^{-1}k^{-1}hk$ у K: $K \lhd G$, $k^{-1} \in K$, па $h^{-1}k^{-1}h \in K$, а онда и $(h^{-1}k^{-1}h)k \in K$. То значи да је $h^{-1}k^{-1}hk \in H \cap K$, а тај пресек је по претпоставци једночлан, па је $h^{-1}k^{-1}hk = e$, односно $hk = kh$. Даље, услов $G = HK$ даје да се сваки елемент $g \in G$ може представити као производ једног из H и једног из K. Треба још доказати да је то разлагање јединствено. Претпоставимо зато да је $g = hk = h'k'$ где $h, h' \in H$, $k, k' \in K$. Опет, множењем слева елементом h^{-1}, а здесна елементом $(k')^{-1}$, једнакост $hk = h'k'$ трансформишемо у $k(k')^{-1} = h^{-1}h'$. Овим смо добили да је на левој страни производ елемената из K, а на десној производ елемената из H. То значи да је $k(k')^{-1} = h^{-1}h' \in H \cap K$ и опет искористимо да је тај пресек само неутрал, па је $k(k')^{-1} = h^{-1}h' = e$, што тачно даје $h = h'$ и $k = k'$.

3) $\Rightarrow$ 1) Треба показати да је пресликавање $\pi : (h, k) \mapsto hk$ изоморфизам групе $H \times K$ на групу G ако знамо да важе услови под 3). Прво ћемо проверити да је π хомоморфизам ових група:

$$\pi((h,k)(h',k')) = \pi(hh', kk') = hh'kk' = hkh'k' = \pi((h,k))\pi((h',k')).$$

Овде смо искористили да подгрупе H и K комутирају члан по члан и заменили $h'k$ са kh'.

Даље проверавамо да је π '1-1': $\pi((h,k)) = \pi((h',k')) \ \Rightarrow\ hk = h'k'$, а због јединствености представљања сваког елемента као производа једног из H и једног из K следи $h = h'$ и $k = k'$, односно $(h,k) = (h',k')$.

Остаје да се уверимо да је π и 'на' пресликавање: ово следи из тога што свако $g \in G$ има растав на производ једног елемента h из H и једног k из K, па је $g = \pi(h,k)$. $\square$

Услове претходне теореме увек задовољавају тривијалне подгрупе групе G. Ако постоје праве подгрупе H и K које задовољавају неки од наведених услова (а то значи и све), за групу G кажемо да је *разложива*. Тада поистовећујемо групе $H \times K$ и G у смислу да је (h,k) исто што и hk.
(Производ $G = HK$ под условима $H, K \lhd G,\ H \cap K = \{e_G\}$ зовемо *унутрашњи директан производ*, док $H \times K$ зовемо *спољашњи директан производ*. Претходна теорема тврди да су ова два појма еквивалентна.)

Индукцијом по n претходно тврђење се уопштава на коначно подгрупа.

Теорема 0.20. *За групу G и њене подгрупе $H_1, H_2, \ldots, H_n$ следећи услови су еквивалентни:*

1) *Са $\pi : (h_1, h_2, \ldots, h_n) \mapsto h_1h_2\cdots h_n$ је дефинисан један изоморфизам групе $H_1 \times H_2 \times \cdots \times H_n$ на групу G;*
2) *$H_i \lhd G,\ G = H_1H_2\cdots H_n,\ (H_1H_2\cdots H_{i-1}) \cap H_i = \{e\}$ за све $i \in \{2, \ldots, n\}$;*
3) *За $i \neq j$ подгрупе H_i и H_j комутирају члан по члан и свако $g \in G$ има тачно један растав облика $g = h_1h_2\cdots h_n$.*

□

За групу G кажемо да је *директан производ* својих подгрупа $H_1, H_2, \ldots, H_n$ ако те подгрупе задовољавају бар један од услова претходне теореме. Ако је операција у групи G означена адитивно, кажемо да је G *директна сума* тих подгрупа и пишемо

$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_n.$$

Често се дешава да је нека група производ (унутрашњи) својих подгрупа које се тривијално секу и од којих је само једна нормална.
За групу G кажемо да је *полудиректан или семидиректан производ* својих подгрупа H и K ако важе следећи услови: $G = HK,\ H \lhd G,\ H \cap K = \{e\}$. То записујемо $G = H \rtimes K$.
(Ово је опет полудиректан унутрашњи производ, а постоји и спољашњи - нећемо овом приликом о њему, али и овде важи да је спољашњи исто што и унутрашњи.)

Пример 0.33. У диедарској групи $\mathbb{D}_n$ природно се издвајају подгрупе генерисане са ρ и σ, $H = \langle\rho\rangle$ и $K = \langle\sigma\rangle$. Прва од њих је нормална јер је индекса 2, а јасно је да су сви елементи диедарске групе производи неког степена ρ и σ. Зато је $\mathbb{D}_n = HK$. Једини заједнички елемент ових подгрупа је неутрал диедарске групе, па важи $\mathbb{D}_n = H \rtimes K \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$. Слично се показује да важи $\mathbb{S}_n \cong \mathbb{A}_n \rtimes \mathbb{Z}_2$, при чему је овде $\mathbb{Z}_2$ подгрупа генерисана било којом транспозицијом.

0.3.14 Комутативне групе

Желимо да опишемо све комутативне групе до на изоморфизам. Испоставиће се да је то могуће, а технике које ћемо користити су углавном из Линеарне алгебре. По договору, комутативне групе означавамо адитивно.

Слободне комутативне групе

Нека је $(G, +, 0, -)$ комутативна група. Као и у свакој групи, за дати елемент $g \in G$ су дефинисани његови степени, у овом случају адитивни (ако је група G означена мултипликативно, за $n \in \mathbb{N}$ имамо: $g^n = g \cdot g \cdots g$, где примењујемо операцију n пута, $g^0 = e$, док је $g^{-n} = g^{-1} \cdot g^{-1} \cdots g^{-1}$, такође n пута):

за $n \in \mathbb{N}$ је $ng = g + g + \cdots + g$, n пута, а $(-n)g = (-g) + (-g) + \cdots + (-g)$, исто n пута, док је $0g = 0 = 0_G$.

Дакле, за свако $m \in \mathbb{Z}$ је дефинисан адитивни m-ти степен било ког елемента $g \in G$. Ово можемо посматрати као операцију $(m, g) \mapsto mg$, односно пресликавање $\mathbb{Z} \times G \to G$. Сада из аксиома групе и комутативности која овде важи добијамо:

$(m + n)g = mg + ng$ (ово је особина степеновања која у мултипликативним ознакама гласи $g^{m+n} = g^m g^n$)

$m(ng) = (mn)g$ (ово је особина степеновања која у мултипликативним ознакама гласи $(g^n)^m = g^{mn}$)

$m(g_1 + g_2) = mg_1 + mg_2$ (ово следи из комутативности и у мултипликативним ознакама гласи $(g_1 g_2)^m = g_1^m g_2^m$)

$1g = g$ (из дефиниције степена, у мултипликативним ознакама гласи $g^1 = g$)

Погледајмо све претходно написано "очима" Линеарне алгебре: имамо комутативну групу $(G, +)$ са њене четири аксиоме и додатно, једну спољну $\mathbb{Z}$-операцију у групи G, $(m, g) \mapsto mg$, за коју важи

1) $(m + n)g = mg + ng$

2) $m(g_1 + g_2) = mg_1 + mg_2$

3) $m(ng) = (mn)g$

4) $1g = g$

за све $m, n \in \mathbb{Z}$ и $g, g_1, g_2 \in G$.

Дакле, свака комутативна група је један $\mathbb{Z}$-*модул* (модул над прстеном је исто што и векторски простор над пољем - важе потпуно исте аксиоме, али то што скалари немају инверзе додводи до различитих последица тих аксиома). То нам даје могућност да применимо све што знамо о векторским просторима - да посматрамо линеарне комбинације, генератрисе, говоримо о линеарној независности, бази и димензији. Наравно, мислимо на одговарајуће појмове у $\mathbb{Z}$-модулу G, али ћемо дефиниције формулисати тако да се односе на саму групу G. Прва од њих (аналогна дефиницији коначнодимензионог векторског простора) је следећа:

Дефиниција 0.25. За комутативну групу G кажемо да је *коначног типа* ако има бар једну коначну генератрису.

То значи да постоје елементи $e_1, e_2, \ldots, e_n$ групе G такви да се сваки $g \in G$ може представити у облику

$$g = k_1 e_1 + k_2 e_2 + \cdots + k_n e_n,$$

где су k_i неки цели бројеви. Пошто сваки e_i генерише своју цикличну групу $\langle e_i \rangle$, група G је сума коначно цикличних подгрупа

$$G = \langle e_1 \rangle + \langle e_2 \rangle + \cdots + \langle e_n \rangle = e_1\mathbb{Z} + e_2\mathbb{Z} + \cdots + e_n\mathbb{Z}.$$

Оно што не знамо је да ли су ове цикличне подгрупе коначне или бесконачне. Ако важи да су $e_1, e_2, \ldots, e_n$ линеарно независни, прво добијамо да је $e_i\mathbb{Z} \cong \mathbb{Z}$ (у супротном, тј. ако неки e_i генерише коначну цикличну групу $\mathbb{Z}_{k_i}$, из $k_i e_i = 0$ следи да је e_i линеарно зависан (сам са собом), па је онда и цео систем линеарно зависан), а затим и да је $G = e_1\mathbb{Z} \oplus e_2\mathbb{Z} \oplus \cdots \oplus e_n\mathbb{Z}$ (сума је директна јер су испуњени услови за то - све подгрупе у комутативној групи су нормалне, а сви пресеци који се појављују у услову за директност суме су $\{0\}$ опет због линеарне независности).

Дакле, ако је систем $[e_1, e_2, \ldots, e_n]$ линеарно независан, важи

$$G \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} = \mathbb{Z}^n.$$

То значи да је свака група G која има коначну линеарно независну генератрису изоморфна групи $\mathbb{Z}^n$ за неко n.

Дефиниција 0.26. За комутативну групу G кажемо да је *слободна* ако има бар једну базу, то јест бар једну линеарно независну генератрису (посматрана као $\mathbb{Z}$-модул, наравно).

Пример 0.34. Ако је n било који природан број, група $\mathbb{Z}^n = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} = \mathbb{Z} \times \cdots \times \mathbb{Z}$ је слободна. Њену канонску базу чине вектори $e_1, e_2, \ldots, e_n$, где је e_i n-торка у којој су све компоненте 0, осим што је i-та 1.
Према коментару који је претходио дефиницији, свака комутативна група G која има бар једну базу са n елемената је изоморфна са $\mathbb{Z}^n$.

Сада се питамо да ли може да се деси да комутативна група коначног типа има једну базу кардиналности n, а другу кардиналности m, за $m \neq n$. Подсетимо се да је код векторских простора најпре важило да сваки има базу (коначну или бесконачну), а затим и да се код векторских простора са коначном генератрисом из те генератрисе може издвојити база. На крају смо показали да су онда све базе исте кардиналности, и тај број звали димензија векторског простора. Код група је ситуација мало другачија: да бисмо могли да дефинишемо аналогон димензије, треба нам услов да група има бар једну базу.

Теорема 0.21. *Ако слободна комутативна група има бар једну коначну генератрису, онда су све њене базе коначне и имају исти број елемената.*

Доказ. Нека је G слободна комутативна група са коначном генератрисом. Ако је e једна њена база и g коначна генератриса, тада је сваки елемент из g линеарна комбинација коначно много елемената из e (по дефиницији линеарне комбинације) са коефицијентима из $\mathbb{Z}$. Имамо дакле коначно линеарних комбинација са коначно вектора у свакој, па се у њима укупно појављује коначно вектора базе e, нека су то $\hat{e} = [e_1, e_2, \ldots, e_n]$. Сада из $g \subset \mathcal{L}(\hat{e})$ и $G = \mathcal{L}(g)$ (g је генератриса групе G, то јест $\mathbb{Z}$-модула G), следи $G = \mathcal{L}(g) \subset \mathcal{L}(\mathcal{L}(\hat{e})) = \mathcal{L}(\hat{e})$. Закључујемо да је $\hat{e}$ генератриса целе групе G. То сада даје да је почетна база e коначна и једнака $\hat{e}$! Зашто? -Пошто је $\hat{e}$ генератриса групе G, онда су и преостали вектори (ако их има) из $e \setminus \hat{e}$ комбинације вектора из $\hat{e}$. Међутим, систем e је линеарно независан, па ово није могуће! Дакле, свака база групе G је коначна!

Нека су сада e и f било које базе (коначне) дате групе G, $e = [e_1, e_2, \ldots, e_n]$, $f = [f_1, f_2, \ldots, f_m]$. Пошто је e база, сваки f_j је линеарна комбинација вектора из e и обрнуто, сваки e_i је линеарна комбинација вектора из f, па постоје матрице $P \in M_{nm}(\mathbb{Z})$ и $Q = M_{mn}(\mathbb{Z})$ за које је $f = eP$ и $e = fQ$ (сетите се матрице преласка са базе на базу од прошле године). Одавде даље имамо $e = ePQ$ и $f = fQP$, а како је $PQ \in M_n(\mathbb{Z})$ и $QP \in M_m(\mathbb{Z})$, добијамо следеће једнакости

$$eE_n = ePQ \quad \text{и} \quad fE_m = fQP.$$

Пошто су системи e и f линеарно независни над $\mathbb{Z}$, можемо да "скратимо" претходне једнакости ($eA = eB \Rightarrow A = B$ ако је e линеарно независан, јер $eA = eB$ значи да су линеарне комбинације e-ова чији су коефицијенти редом колоне матрица A и B једнаке, па искористимо линеарну независност да добијемо да је свака колона матрице A једнака одговарајућој колини матрице B). Добијамо $E_n = PQ$ и $E_m = QP$. Тврдимо да одавде следи да је $m = n$.
-Посматраћемо трагове ових матрица:

$$n = Tr(E_n) = Tr(PQ) = Tr(QP) = Tr(E_m) = m.$$

Остаје да објаснимо средњу једнакост ако је не знамо од раније:

$$Tr(PQ) = \sum_i (PQ)_{ii} = \sum_i \sum_j P_{ij}Q_{ji} = \sum_{i,j} P_{ij}Q_{ji},$$

$$Tr(QP) = \sum_j (QP)_{jj} = \sum_j \sum_i Q_{ji}P_{ij} = \sum_{i,j} P_{ij}Q_{ji}.$$

□

Дакле, ако комутативна група G има бар једну коначну базу, онда све њене базе имају исти број елемената. Тај број се зове *ранг* групе G и означава се са $\rho(G)$ (то је значи димензија $\mathbb{Z}$-модула G). Видели смо већ да је свака комутативна група G која има базу са n елемената изоморфна са $\mathbb{Z}^n$, па је

$$\rho(G) = n \quad \Leftrightarrow \quad G \cong \mathbb{Z}^n.$$

Подгрупе слободне комутативне групе

Дефинисали смо аналогон димензије векторског потпростора, и сада желимо да видимо шта овде важи за "потпросторе" (подмодуле), односно подгрупе. Опет наилазимо на разлику у односу на векторске просторе. Подсетимо се да је тамо важило да ако је U потпростор простора V који је исте димензије као сам V, онда мора да буде $U = V$. Овде то својство губимо. На пример, група $\mathbb{Z}^2$ је ранга 2, као и њена подгрупа генерисана (линеарно независним) елементима $(2, 0)$ и $(0, 5)$, али очигледно нису једнаке! Међутим, одређена правилност ипак важи:

Теорема 0.22. *Ако је G слободна комутативна група ранга n, онда је свака њена подгрупа такође слободна и ранга не већег од n.*

Доказ. -индукцијом по $n = \rho(G)$

За $n = 1$ имамо да је $G \cong \mathbb{Z}$, а пошто знамо да опишемо подгрупе групе целих бројева, следиће да је свака подгрупа H од G или $\{0\}$ или изоморфна са $k\mathbb{Z}$ што је даље изоморфно са $\mathbb{Z}$. Дакле, H је ранга 0 или 1.

Нека је сада $n > 1$ и претпоставимо да тврђење важи за све групе ранга мањег од n. Ако је $e = [e_1, e_2, \ldots, e_n]$ једна база групе G, тада се сваки елемент $g \in G$ може представити у облику $g = k_1e_1 + k_2e_2 + \cdots + k_ne_n$, где су k_i неки цели бројеви. Посебно, то важи и за елементе било које њене подгрупе H. Да бисмо искористили индуктивну претпоставку треба да "избацимо" један базни елемент и зато ћемо посматрати пресликавање које елементу додељује његову прву координату у бази e, односно пројекцију $\pi : H \to \mathbb{Z}$ дефинисану са $\pi(k_1e_1 + k_2e_2 + \cdots + k_ne_n) = k_1$. Ово је очигледно хомоморфизам (прва координата збира једнака је збиру првих координата) и његова слика је нека подгрупа групе $\mathbb{Z}$, $Im\pi = k\mathbb{Z}$.

Ако је $k = 0$, следи да сви елементи из H имају прву координату 0. То значи да је H садржана у $\mathbb{Z}$-модулу генерисаном елементима $e_2, \ldots, e_n$, односно да је подгрупа слободне групе $\mathbb{Z}[e_2, \ldots, e_n]$ која је ранга $n-1$, па је онда, по индуктивној претпоставци, и H слободна и ранга највише $n-1$.

Нека је $k \neq 0$. Пошто је $Im\pi = k\mathbb{Z}$, постоји бар један елемент $g \in G$ који се слика баш у k. Доказаћемо да је онда $H = Ker\pi \oplus g\mathbb{Z}$, при чему је $g\mathbb{Z}$ подгрупа од H генерисана елементом g. Нека је $h \in H$ произвољно. Из $Im\pi = k\mathbb{Z}$ следи да је $\pi(h) = mk$ за неко $m \in \mathbb{Z}$. Сада из $k = \pi(g)$ имамо $\pi(h) - m\pi(g) = 0$, односно $\pi(h - mg) = 0$. То значи да је $h - mg \in Ker\pi$, а тиме и $h \in Ker\pi + g\mathbb{Z}$, па је $H = Ker\pi + g\mathbb{Z}$.

Зашто је ова сума директна? Нека $h \in Ker\pi \cap g\mathbb{Z}$. То значи да да је h облика $h = mg$ и $\pi(h) = 0$, па имамо $\pi(mg) = m\pi(g) = mk = 0$. Претпоставили смо да је $k \neq 0$, што даје да $m = 0$, а онда је и h из пресека једнако 0. Дакле, $Ker\pi \cap g\mathbb{Z} = \{0\}$ и сума је директна.

Шта смо добили овим разлагањем подгрупе H на директну суму? - $Ker\pi$ је подгрупа слободне групе $\mathbb{Z}[e_2, \ldots, e_n]$ ранга $n-1$, па је по индуктивној претпоставци и $Ker\pi$ слободна и ранга не већег од $n-1$. То значи да је H директна сума слободне подгрупе ранга $\leq n-1$ и слободне подгрупе $g\mathbb{Z}$ ранга 1, па је и H слободна и $\rho(H) \leq n-1+1 = n$, што је и требало доказати. □

Према томе, ако слободна комутативна група G има базу дужине n, тада и свака њена подгрупа H има базу дужине $m \leq n$. Видели смо такође да и за $H \neq G$ рангови m и n могу да буду једнаки. Осим те, још једна разлика у односу на векторске просторе је што произвољна база подгрупе H не мора да буде део неке базе саме групе G. Ипак, и овде важи извесна правилност.

Теорема 0.23. *За сваку праву подгрупу слободне комутативне групе G ранга n постоји систем целих бројева $[n_1, n_2, \ldots, n_k]$ међу којима сваки дели онај наредни и за које група G има бар једну базу $e = [e_1, e_2, \ldots, e_n]$ такву да је*

$$f = [n_1e_1, n_2e_2, \ldots, n_ke_k]$$

једна база подгрупе H. При том су бројеви $n_1, n_2, \ldots, n_k$ одређени једнозначно до на знак.

Доказ. Управо смо доказали да је и подгрупа H слободна, па ћемо посматрати произвољне базе g од G и h од H. Пошто је g база целе групе G, то се и h-ови могу изразити преко g-ова: $h = gA$ за јединствено одређену матрицу $A \in M_{kn}(\mathbb{Z})$, где је k ранг подгрупе H.

С друге стране, за базе које желимо да нађемо важи $f = eA^0$, где је

$$A^0 = \begin{bmatrix} n_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & n_2 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & n_k & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix} \quad (n_i \mid n_{i+1}).$$

Ако би, као за матрице над пољем, важило да постоје инверзибилне матрице P и Q које A "своде" на A^0, то јест такве да је $PAQ = A^0$, могли бисмо да нађемо везу између g и e, односно између h и f:
једнакост $h = gA$ помножимо здесна са Q и добијемо $hQ = gAQ$; сада уметнемо $P^{-1}P$ између g и A да бисмо имали заједно PAQ:
$hQ = gP^{-1}PAQ$, односно $hQ = gP^{-1}A^0$. Сада је, за $f = hQ$ и $e = gP^{-1}$, $f = eA^0$.

Дакле, ако докажемо да за произвољну матрицу над $\mathbb{Z}$ постоје инверзибилне матрице P и Q одговарајућих формата такве да је PAQ траженог облика, могли бисмо од почетних (произвољних) база g и h да добијемо e и f за које важи дата веза.
Зато ћемо посебно формулисати то тврђење о матрицама, уз подсећање да смо имали аналогно у Линеарној алгебри, и да донекле можемо применити исту технику у доказивању (не у потпуности јер смо тамо радили са матрицама над пољем, где имамо дељење - немогућност да од произвољног ненула броја добијемо јединицу у $\mathbb{Z}$ превазилазимо еуклидским дељењем!)

Лема 0.3. *За сваку матрицу $A \in M_{mn}(\mathbb{Z})$, постоје инверзибилне матрице $P \in M_m(\mathbb{Z})$ и $Q \in M_n(\mathbb{Z})$ за које је матрица $PAQ = A^0$, где је A^0 матрица чије су скоро све компоненте нула, осим k њих на почетном делу дијагонале и за њих важи да свака дели наредну. Ти бројеви су, за дату матрицу, одређени једнозначно до на знак.*

Доказ. Довољно је да докажемо да се матрица A може применом коначно много елементарних операција на врстама или колонама трансформисати у матрицу траженог облика, јер смо прошле године имали да се свака елементарна операција на врстама може заменити множењем слева *елементарном матрицом* која настаје применом те исте операције на врстама јединичне матрице: $\psi(A) = \psi(E)A$, где је ψ једна од следећих операција:
1) $V_i \leftrightarrow V_j$;
2) $V_i \mapsto \alpha V_i \quad (\alpha \in \mathbb{Z}^* = \{-1, 1\})$;
3) $V_i \mapsto V_i + \alpha V_j \quad (\alpha \in \mathbb{Z},\ i \neq j)$.

Исто важи и за операције на колонама, само што ту A множимо елементарном матрицом здесна: $\phi(A) = A\phi(E)$.
Оно што је овде круцијално је да су елементарне матрице инверзибилне (њихови инверзи су поново елементарне матрице настале применом инверзне елементарне операције на E). То нам даје објашњење зашто се елементарне операције могу заменити множењем инверзибилним матрицама слева и здесна:

$$\psi_r \cdots \psi_2\psi_1 A\phi_1\phi_2 \cdots \phi_s = \psi_r(E) \cdots \psi_2(E)\psi_1(E)A\phi_1(E)\phi_2(E) \cdots \phi_s(E) = \ = P_r \cdots P_2P_1AQ_1Q_2 \cdots Q_s = PAQ,$$

а матрице P и Q су инверзибилне као производи елементарних!

Дакле, нека је дата матрица

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix} \in M_{mn}(\mathbb{Z}).$$

Доказаћемо прво да се матрица A може елементарним трансформацијама свести на матрицу облика

$$B = \begin{bmatrix} d & 0 & 0 & \cdots & 0 \\ 0 & b_{22} & b_{23} & \cdots & b_{2n} \\ 0 & b_{32} & b_{33} & \cdots & b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m2} & b_{m3} & \cdots & b_{mn} \end{bmatrix} \quad (d \mid b_{ij}),$$

у којој је d највећи заједнички делилац свих компонената a_{ij} матрице A. Можемо да претпоставимо да A није нула матрица (јер код нас остварује везу између две базе, а и да јесте, може се рећи да је траженог облика). Уочимо елемент a_{ij} који је најмањи по апсолутној вредности међу свим не-нула компонентама. Без умањења општости претпоставимо да је то a_{11}, јер га операцијама типа $V_1 \leftrightarrow V_j$ и $K_1 \leftrightarrow K_j$ свакако можемо довести у горњи леви угао. Ако је $|a_{11}| = 1$, понашаћемо се исто као и код матрица над пољем, односно тим елементом ћемо "очистити" остатак прве врсте и прве колоне (у зависности од тога да ли је $a_{11} = 1$ или $a_{11} = -1$, вршимо операције $V_i \mapsto V_i - a_{i1}V_1$ и $K_j \mapsto K_j - a_{1j}K_1$, односно $V_i \mapsto V_i + a_{i1}V_1$ и $K_j \mapsto K_j + a_{1j}K_1$). Тиме смо добили матрицу B јер јединица дели свако b_{ij}.

Нека је сада $|a_{11}| = n > 1$ и претпоставимо да тврђење важи за сваку матрицу чија је најмања не-нула апсолутна вредност мања од n. Напоменули смо већ да у $\mathbb{Z}$ немамо дељење и разломке, али имамо еуклидско дељење. Зато ћемо узети редом компоненте прве колоне и сваку еуклидски поделити са a_{11}:
$a_{21} = a_{11}q + r, \quad r < a_{11}$
$a_{31} = a_{11}q' + r', \quad r' < a_{11}$
и тако даље. Затим извршимо операције $V_2 \mapsto V_2 - qV_1$, $V_3 \mapsto V_3 - q'V_1$ и исто са преосталим врстама. То исто урадимо и са компонентама прве врсте, то јест сваку еуклидски поделимо са a_{11}, а онда вршимо операције на колонама да у остатку прве врсте добијемо компоненте мање од a_{11}. Шта добијамо после те две серије елементарних операција? Једна могућност је да је бар једна компонента осим a_{11} у првој врсти или првој колони различита од нуле. То ће онда бити најмања апсолутна вредност мања од n и по индуктивној претпоставци добијена матрица се даље може свести на матрицу облика B. Друга могућност је да су остатку прве врсте као и у остатку прве колоне, све компоненте осим a_{11} једнаке нула. То свакако личи на матрицу B, али шта ако ту a_{11} не дели неко b_{ij}? - У том случају, додамо j-ту колону првој (ту у којој је елемент који није дељив са a_{11}) и онда опет изведемо описане операције по врстама које ће бар на месту $(i, 1)$ дати не-нула вредност мању од n и онда можемо применити индуктивну хипотезу.

Дакле, индукцијом по најмањој апсолутној вредности различитој од нуле, следи да се добијена матрица у сваком случају своди на матрицу облика B, а самим тим

и почетна матрица A. Тврдимо да је онда не само $d = NZD(A)$ (у смислу највећи заједнички делилац свих компонената матрице A), већ и $d = NZD(B)$. То оправдавамо на исти начин као у коментару код Еуклидовог алгоритма: $NZD(bq + r, b) = NZD(b, r)$, а ми смо компоненте у матрици A мењали искључиво на овај начин - бројеве смо замењивали њиховим остацима при дељењу са $a_{11} = d$. Сада настављамо на описани начин да трансформишемо подматрицу матрице B коју чине компоненте $[b_{ij}]$. Пошто d дели свако b_{ij}, делиће и њихов NZD. Означићемо d са n_1, $NZD[b_{ij}]$ са n_2 и тако даље. На крају ћемо добити матрицу облика A^0. □

Бројеви $n_1, n_2, \ldots, n_k$ из претходне леме се зову *инваријантни делиоци* матрице A, док се у контексту претходне теореме зову *инваријантни делиоци* подгрупе H.

Комутативне групе коначног типа

Подсетимо се да за комутативну групу G кажемо да је коначног типа ако има бар једну коначну генератрису. Ако је G коначно генерисана комутативна група, она не мора да буде слободна (за све $\mathbb{Z}_n$ важи да им је једночлана генератриса линеарно зависна, $n1 = 0$). Ипак, као и код ранијих одступања од правилности које важе у векторским просторима, и овде постоји веза између комутативних група коначног типа и слободних комутативних група (комутативних група са базом).

Теорема 0.24. *За сваку базу $[e_1, e_2, \ldots, e_n]$ слободне комутативне групе F ранга n и произвољне елементе $g_1, g_2, \ldots, g_n$ комутативне групе G, постоји јединствен хомоморфизам $f : F \to G$ такав да је $f(e_i) = g_i$ за свако $i \in \{1, 2, \ldots, n\}$.*

Одавде следи да је свака коначно генерисана комутативна група изоморфна количничкој групи неке слободне групе по некој њеној подгрупи.

Доказ. Ако тражени хомоморфизам постоји, онда за произвољне целе бројеве k_i мора да важи

$$f(k_1e_1 + k_2e_2 + \cdots + k_ne_n) = k_1f(e_1) + k_2f(e_2) + \cdots + k_nf(e_n) = k_1g_1 + k_2g_2 + \cdots + k_ng_n.$$

Такође, пошто за сваки елемент из F постоје његови јединствени коефицијенти у бази e, са

$$f(k_1e_1 + k_2e_2 + \cdots + k_ne_n) = k_1g_1 + k_2g_2 + \cdots + k_ng_n$$

је добро дефинисано једно пресликавање $f : F \to G$. Оно је очигледно хомоморфизам:

$$f(\sum k_ie_i + \sum k'_ie_i) = f(\sum (k_i + k'_i)e_i) = \sum (k_i + k'_i)g_i =$$
$$= \sum k_ig_i + \sum k'_ig_i = f(\sum k_ie_i) + f(\sum k'_ie_i).$$

Јасно је и да важи $f(e_i) = g_i$. (Сетите се од прошле године: линеарно пресликавање је јединствено одређено ако је задато на бази).

Нека је сада G произвољна коначно генерисана комутативна група са генератрисом $[g_1, g_2, \ldots, g_n]$. Узећемо слободну комутативну групу ранга n (на пример $\mathbb{Z}^n$) и као горе, пресликати $e_i \mapsto g_i$, где је e_i i-ти канонски вектор. Јасно је да ће онда слика бити цела група G, $Imf = G$, па из $F/Kerf \cong Imf$ следи $G \cong F/H$ за подгрупу $H = Kerf$. □

Ова теорема нас уводи у следеће битно тврђење које већ даје опис комутативних група коначног типа.

Теорема 0.25. *За сваку комутативну групу G коначног типа постоје цео број $s \geq 0$ и систем подгрупа $n_1\mathbb{Z} \supseteq n_2\mathbb{Z} \supseteq \cdots \supseteq n_k\mathbb{Z}$ групе $\mathbb{Z}$, тако да је*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^s.$$

Доказ. Према претходној теореми, G је изоморфна количнику неке слободне групе F. Узећемо да је $F = \mathbb{Z}^n$ (ако G има n-точлану генератрису, то је то n). Дакле, $G \cong \mathbb{Z}^n/H$ за неку подгрупу H групе $\mathbb{Z}^n$. Сада, према теореми о подгрупама слободне комутативне групе, постоје $n_1, n_2, \ldots, n_k \in \mathbb{Z} \setminus \{0\}$ такви да сваки дели следећи, и нека база $e = [e_1, e_2, \ldots, e_n]$ групе $\mathbb{Z}^n$ за које је

$$f = [n_1e_1, n_2e_2, \ldots, n_ke_k]$$

једна база подгрупе H. Из услова $n_i \mid n_{i+1}$ одмах следи $n_1\mathbb{Z} \supseteq n_2\mathbb{Z} \supseteq \cdots \supseteq n_k\mathbb{Z}$. Нама треба изоморфизам из G, то јест $\mathbb{Z}^n/H$ у групу $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^s$. Шта ћемо узети за s? - Пошто је $k \leq n$, биће $n - k \geq 0$, па ћемо ставити $s = n - k$.
Произвољан елемент из $\mathbb{Z}^n$ се може изразити у бази e: $a = a_1e_1 + a_2e_2 + \cdots + a_ne_n$. Дефинисаћемо пресликавање

$$f : \mathbb{Z}^n \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^s$$

са

$$f(a_1e_1 + a_2e_2 + \cdots + a_ne_n) = (a_1 + n_1\mathbb{Z}, \ldots, a_k + n_k\mathbb{Z}, a_{k+1}, \ldots, a_n).$$

Јасно је да је f хомоморфизам, јер су операције у количнику и Декартовом производу тако дефинисане:

$$f(\sum a_ie_i + \sum b_ie_i) = f(\sum (a_i+b_i)e_i) = (a_1+b_1+n_1\mathbb{Z}, \ldots, a_k+b_k+n_k\mathbb{Z}, a_{k+1}+b_{k+1}, \ldots, a_n+b_n) =$$

$$= (a_1+n_1\mathbb{Z}, \ldots, a_k+n_k\mathbb{Z}, a_{k+1}, \ldots, a_n)+(b_1+n_1\mathbb{Z}, \ldots, b_k+n_k\mathbb{Z}, b_{k+1}, \ldots, b_n) = f(\sum a_ie_i)+f(\sum b_ie_i).$$

Јасно је и да је f 'на', па је $Imf = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^s$. Шта је језгро?

$$a = a_1e_1 + \cdots + a_ne_n \in Kerf \Leftrightarrow (a_1 + n_1\mathbb{Z}, \ldots, a_k + n_k\mathbb{Z}, a_{k+1}, \ldots, a_n) = (n_1\mathbb{Z}, \ldots, n_k\mathbb{Z}, 0, \ldots, 0)$$

$$\Leftrightarrow a_i \in n_i\mathbb{Z},\ i \in \{1, \ldots, k\} \wedge a_{k+1} = \cdots = a_n = 0 \Leftrightarrow a_ie_i \in n_ie_i\mathbb{Z},\ i \in \{1, \ldots, k\} \wedge a_{k+1} = \cdots = a_n = 0$$

$$\Leftrightarrow a \in \mathcal{L}(f_1, \ldots, f_k) = \mathcal{L}(f) \Leftrightarrow a \in H.$$

Сада из $\mathbb{Z}^n/Kerf \cong Imf$ имамо $\mathbb{Z}^n/H \cong Imf$, односно

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}^s.$$

□

Бројеви $n_1, n_2, \ldots, n_k$ у претходној теореми су из скупа $\mathbb{Z}\backslash\{0\}$, али пошто за $n \in \mathbb{N}$, n и $(-n)$ генеришу исту подгрупу $n\mathbb{Z}$, можемо да претпоставимо да су природни. Штавише, узећемо да су сви већи од 1, јер ако је неколико почетних једнако 1, можемо да их изоставимо због $\mathbb{Z}/\mathbb{Z} \cong \{0\}$. То значи да су $\mathbb{Z}/n_i\mathbb{Z} \cong \mathbb{Z}_{n_i}$ коначне цикличне групе редова већих од 1 и то такве да ред сваке дели ред наредне.

Дакле, свака коначно генерисана комутативна група је Декартов производ (директна сума) неких коначних цикличних група редова већих од 1 таквих да ред сваке дели ред следеће и неке слободне групе ранга $s \geq 0$:

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^s, \quad n_i > 1,\ n_i \mid n_{i+1},\ s \geq 0.$$

Претходну релацију зовемо *нормална форма* групе G, а бројеве $n_1, n_2, \ldots, n_k$ *инваријантни делиоци* групе G. Они, као и $s \geq 0$ су једнозначно одређени за дату групу G.

Ако наставимо даље, имајући у виду да је свака циклична група реда $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, где су p_i различити прости бројеви, изоморфна групи $\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$,сваку $\mathbb{Z}_{n_i}$ можемо раставити на директан производ цикличних група $\mathbb{Z}_{p^r}$ чији су редови степени неких простих бројева. При том, из $n_i \mid n_{i+1}$ следи да су степени истих простих бројева који се ту јављају неопадајући, па имамо:

За сваку коначно генерисану комутативну групу G постоје једнозначно одређени прости бројеви $p < \cdots < q$ и систем природних бројева $[k_1 \leq \cdots \leq k_i; \ldots; l_1 \leq \cdots \leq l_j]$ за које је

$$G \cong \mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_i}} \times \cdots \times \mathbb{Z}_{q^{l_1}} \times \cdots \times \mathbb{Z}_{q^{l_j}} \times \mathbb{Z}^s,\ s \geq 0.$$

Претходну релацију зовемо *елементарна форма* групе G, а систем $[p^{k_1}, \ldots, p^{k_i}; \ldots; q^{l_1}, \ldots, q^{l_j}]$

систем елементарних делилаца групе G. Овим системом и бројем $s \geq 0$ комутативна група је једнозначно одређена.

0.3.15 Унутрашњи аутоморфизми групе

Знамо да су аутоморфизми групе G изоморфизми из G у G, односно бијективни хоморфизми који сликају групу у саму себе. Скуп свих аутоморфизама дате групе G, који означавамо са $Aut(G)$, је и сам група у односу на композицију пресликавања. Видели смо већ да је тешко одредити ову групу у општем случају, али смо то успели, на пример, за цикличне групе, диедарску и Клајнову.

Сада ћемо се бавити само посебном врстом аутоморфизама дате групе, који су дати експлицитно и чине важну подгрупу групе $Aut(G)$. Више пута до сада смо напоменули да је лева (или десна) транслација у групи, то јест пресликавање $x \mapsto ax$ (или $x \mapsto xa$) где је a фиксирани елемент групе, једна бијекција. Јасно је такође да ово није хоморфизам ($axay \neq axy$ осим за $a = e$). Међутим, сетимо се опет да смо већ приметили

да се пресликавање $x \mapsto axa^{-1}$ слаже са множењем. Ово пресликавање ћемо означити са π_a. Проверимо да заиста $\pi_a \in Aut(G)$:

π_a је хомоморфизам: $\pi_a(xy) = a(xy)a^{-1} = axa^{-1}aya^{-1} = \pi_a(x)\pi_a(y)$

π_a је '1-1': $\pi_a(x) = \pi_a(y) \;\Rightarrow\; axa^{-1} = aya^{-1} \Rightarrow\; x = y$

π_a је 'на': $y = \pi_a(x) \;\Rightarrow\; y = axa^{-1} \Rightarrow\; x = a^{-1}ya$

Дакле,

$$\pi_a(x) = axa^{-1}$$

је један аутоморфизам групе G који зовемо *унутрашњи аутоморфизам* који одговара елементу a. Скуп свих унутрашњих аутоморфизама групе G означавамо са $Inn(G)$:

$$Inn(G) = \{\pi_a : \; a \in G\}.$$

Важи: $Inn(G) \lhd Aut(G)$

- производ два унутрашња аутоморфизма је опет унутрашњи аутоморфизам и још важи $\pi_a \circ \pi_b = \pi_{ab}$, јер:
$(\pi_a \circ \pi_b)(x) = \pi_a(\pi_b(x)) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \pi_{ab}(x) \quad \Rightarrow \quad \pi_a \circ \pi_b = \pi_{ab}$
- инверз унутрашњег изоморфизма је унутрашњи изоморфизам и још важи: $\pi_a^{-1} = \pi_{a^{-1}}$ јер
$(\pi_{a^{-1}} \circ \pi_a)(x) = \pi_{a^{-1}}(\pi_a(x)) = a^{-1}(axa^{-1})(a^{-1})^{-1} = a^{-1}axa^{-1}a = x = id(x) \quad \Rightarrow \quad \pi_a^{-1} = \pi_{a^{-1}}$
- идентично пресликавање је унутрашњи аутоморфизам: $id_G = \pi_e$ јер
$\pi_e(x) = exe^{-1} = x \quad \Rightarrow \quad \pi_e = id_G$

$\Rightarrow\; Inn(G) \leq Aut(G)$

Треба показати и нормалност. Нека је $f \in Aut(G)$ произвољан елемент, то јест аутоморфизам групе G, и $\pi_a \in Inn(G)$ произвољан унутрашњи аутоморфизам. Тада је

$$(f^{-1} \circ \pi_a \circ f)(x) = f^{-1}(\pi_a(f(x))) = f^{-1}(af(x)a^{-1}) =$$

$$= f^{-1}(a)f^{-1}(f(x))f^{-1}(a^{-1}) = f^{-1}(a)x(f^{-1}(a))^{-1} = \pi_{f^{-1}(a)}(x).$$

Овде смо користили то да ако је f аутоморфизам, онда је и f^{-1} аутоморфизам, па пролази кроз производ и инверз. Дакле, $f^{-1} \circ \pi_a \circ f = \pi_{f^{-1}(a)} \in Inn(G)$, па је $Inn(G) \lhd Aut(G)$. (Количник $Aut(G)/Inn(G)$ се зове група спољних аутоморфизама групе G, али нас то сада не занима превише). Количник који нас занима је онај изоморфан са $Inn(G)$, а то је G/C_G:

Теорема 0.26. *Ако је C_G центар групе G, онда је*

$$Inn(G) \cong G/C_G.$$

Доказ. Јасно је да је пресликавање које ћемо посматрати оно које елементу групе G додељује његов унутрашњи аутоморфизам,

$$f : G \to Aut(G), \quad f(a) = \pi_a.$$

Ово је хомоморфизам, јер смо већ показали да је $\pi_a \circ \pi_b = \pi_{ab}$, па је $f(ab) = \pi_{ab} = \pi_a \circ \pi_b = f(a) \circ f(b)$. Слика му је $Imf = Inn(G)$, а језгро

$$Kerf = \{a \in G : f(a) = id_G\} = \{a \in G : \pi_a = id_G\} = \{a \in G : \pi_a(x) = x,\ \forall x \in G\} =$$

$$= \{a \in G : axa^{-1} = x,\ \forall x \in G\} = \{a \in G : ax = xa,\ \forall x \in G\} = C_G.$$

Сада применимо Прву теорему о изоморфизму, $G/Kerf \cong Imf$, и добијамо

$$G/C_G \cong Inn(G).$$

□

Пример 0.35. Пошто је центар симетричне групе тривијалан, из претходне теореме добијамо $Inn(\mathbb{S}_3) \cong S_3$, а имали смо већ да је $Aut(\mathbb{S}_3) \cong S_3$, па је $Aut(\mathbb{S}_3) \cong Inn(\mathbb{S}_3)$, односно сви аутоморфизми групе $\mathbb{S}_3$ су унутрашњи.

0.3.16 Извод групе, решиве групе

Видели смо већ да се количници (или хомоморфне слике, из $G/Kerf \cong Imf$ следи да су та два појма еквивалентна) неких група прилично разликују од тих полазних група. Сада желимо да дамо одговор на следеће питање: по каквој подгрупи треба да сечемо дату некомутативну групу G да бисмо као количник добили комутативну. Шта мора да садржи најмања подгрупа H за коју је G/H Абелова?

$$aH \bullet bH = bH \bullet aH \quad \Leftrightarrow \quad abH = baH \quad \Leftrightarrow \quad (ba)^{-1}ab \in H \quad \Leftrightarrow \quad a^{-1}b^{-1}ab \in H.$$

Елемент $a^{-1}b^{-1}ab$ одређен елементима a и b смо већ посматрали. Зваћемо га *комутатор* елемената a и b и означавати са $[a, b]$. Он "мери" да ли елементи a и b комутирају: $ab = ba \ \Leftrightarrow \ [a, b] = e$. Приметимо одмах да је инверз комутатора такође комутатор, $[a, b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b, a]$, али производ два комутатора није комутатор у општем случају, $[a, b][c, d] = a^{-1}b^{-1}abc^{-1}d^{-1}cd$. Зато скуп свих комутатора затварамо за множење и посматрамо подгрупу генерисану њима. Означавамо је са G' (јер је потпуно одређена датом групом G) и зовемо *извод* групе G (или комутаторска подгрупа групе G):

$$G' = \langle [a, b] : a, b \in G \rangle = \langle a^{-1}b^{-1}ab : a, b \in G \rangle.$$

Вратимо се на низ еквиваленција које смо горе имали. Добили смо да је G/H комутативна ако и само ако H садржи све комутаторе. Пошто је H подгрупа, то је еквивалентно томе да садржи подгрупу генерисану комутаторима. Дакле

$$G/H \text{ је комутативна } \Leftrightarrow \ G' \subseteq H.$$

Овако смо окарактерисали извод групе, а сада ћемо показати да је и он једна нормална подгрупа групе G.

$G' \lhd G$:

- пошто смо извод дефинисали као подгрупу генерисану комутаторима, довољно је да проверимо да је конјугат комутатора такође комутатор:

$$g^{-1}[a,b]g = g^{-1}a^{-1}b^{-1}abg = g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg = [g^{-1}ag, g^{-1}bg] \in G'.$$

Дакле, извод групе је њена најмања нормална подгрупа таква да је одговарајућа количничка група комутативна (Абелова). Тај количник се зато зове *комутант* или *абелизација* групе G:

$$Ab(G) = G^{ab} := G/G'.$$

То је значи највећи комутативни количник групе G. Јасно је да је G комутативна ако и само ако је $Ab(G) = G$, односно $G' = \{e\}$.

Пример 0.36. Извод симетричне групе је одговарајућа алтернирајућа, $\mathbb{S}'_n = \mathbb{A}_n$ за $n \geq 3$ ($\mathbb{S}_2 = \mathbb{Z}_2$ је комутативна па јој је извод тривијалан). Дакле, абелизација симетричне групе је циклична група реда 2, $Ab(\mathbb{S}_n) = \mathbb{S}_n/\mathbb{S}'_n = \mathbb{S}_n/\mathbb{A}_n \cong \mathbb{Z}_2$. То ће показати Никола (у Алгебри 2; можете да нађете сада у његовој скрипти из Алгебре 2 ако желите). Такође, показаће и да је $\mathbb{A}'_n = \mathbb{A}_n$ за $n \geq 5$. За $n = 4$ је $\mathbb{A}'_4 = \mathbb{V}_4$, а $\mathbb{A}_3 = \mathbb{Z}_3$, па јој је извод тривијалан.

Пример 0.37. Извод диедарске групе је њена подгрупа генерисана ротацијом ρ^2, $\mathbb{D}'_n = \langle\rho^2\rangle$ (ово се показује тако што се израчунају комутатори произвољних елемената диедарске групе). Знамо да је за непарно n ова подгрупа једнака целој ротацијској подгрупи од $\mathbb{D}_n$, па је индекса 2 и у том случају абелизација је $Ab(\mathbb{D}_n) = \mathbb{D}_n/\mathbb{D}'_n = \mathbb{D}_n/\langle\rho\rangle \cong \mathbb{Z}_2$. Ако је n паран број, подгрупа $\langle\rho^2\rangle$ је индекса 4 и испоставља се да је количник $\mathbb{D}_n/\langle\rho^2\rangle$ изоморфан Клајновој групи (провери се да су сви елементи у том количнику, осим неутрала $\langle\rho^2\rangle$, реда 2 - опет код Николе у скрипти за Алгебру 2). Дакле, за n непарно, $Ab(\mathbb{D}_n) \cong \mathbb{Z}_2$, а за n парно је $Ab(\mathbb{D}_n) \cong \mathbb{V}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Пошто је извод групе нова група, можемо потражити њен извод. Обележавамо га са $G^{(2)} = (G')'$ и зовемо *други извод* групе G. На исти начин дефинишемо трећи и остале изводе. Тако добијамо низ подгрупа групе G у ком је сваки члан извод претходног (самим тим и нормална подгрупа за коју важи да је одговарајући количник Абелова група):

$$G \supseteq G' \supseteq G^{(2)} \supseteq G^{(3)} \supseteq \cdots$$

Јасно је да ако су два узастопна члана овог низа једнака, онда су и сви наредни једнаки њима. С друге стране, овај низ може да се не устали све док не стигнемо до најмање подгрупе групе G, а то је $\{e\}$. За групу G кажемо да је *решива* ако постоји $n \in \mathbb{N}$ за које је $G^{(n)} = \{e\}$. Термин решива потиче од тога што се алгебарским једначинама вишег степена (а то су једначине облика $p(x) = 0$ где је p полином степена већег од један) могу придружити одређене групе које се зову Галуаове групе. Испоставља се да се та једначина може решити помоћу корена или радикала (односно свођењем на једначине облика $x^k = a$) ако и само ако је њена Галуаова група решива.

Теорема 0.27. *Коначна група G је решива ако и само ако постоји бар један опадајући низ подгрупа*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \{e\}$$

у коме је сваки члан нормална подгрупа претходног таква да је група G_i/G_{i+1} Абелова.

Доказ. Ако је група G решива и n број за који је $G^{(n)} = \{e\}$, за чланове траженог низа ћемо узети баш одговарајуће изводе групе G, $G_i = G^{(i)}$. Како је $G^{(i+1)}$ извод од $G^{(i)}$, важи $G^{(i+1)} \lhd G^{(i)}$ и $G^{(i)}/G^{(i+1)}$ је Абелова.

Обрнуто, нека постоји низ у коме је сваки члан нормална подгрупа претходног и одговарајући количник је комутативан. Сада из комутативности G_i/G_{i+1} и карактеризације извода следи да је $(G_i)' \subseteq G_{i+1}$ за свако i. То значи да је $G' \subseteq G_1$, па је онда $(G')' = G^{(2)} \subseteq G_1'$. Сада из $G_1' \subseteq G_2$ даље следи $G^{(2)} \subseteq G_2$. Ако сада узмемо изводе ових подгрупа и искористимо $(G_2)' \subseteq G_3$, добићемо $G^{(3)} \subseteq G_3$ и тако даље, $G^{(i)} \subseteq G_i$. Одавде следи и да је $G^{(n)} \subseteq G_n = \{e\}$, па је група G решива. □

Јасно је да је свака комутативна група решива јер је већ њен извод тривијалан. Даље, ако је H било која подгрупа групе G, сви њени комутатори су такође комутатори неких елемената из G, па је $H' \leq G'$. Одавде је и $H^{(i)} \subseteq G^{(i)}$, па је свака подгрупа решиве групе такође решива. Такође, важи да ако је група G решива и H било која њена нормална подгрупа, онда је количничка група G/H такође решива: ако је $\pi : G \to G/H$ природни епиморфизам, покаже се да је $\pi(G') = (G/H)'$, а онда и да је $\pi(G^{(i)}) = (G/H)^{(i)}$, па ако је $G^{(n)} = \{e\}$ за неко n, онда је и $(G/H)^{(n)} = \pi(G^{(n)}) = \pi(\{e\}) = \{H\}$. (Ово је у ствари последица тога да је хомоморфна слика решиве групе решива, јер је $f(G^{(i)}) = (f(G))^{(i)})$). На крају, наводимо и тврђење "јаче" од претходног, које нећемо доказати: група G је решива ако и само ако има бар једну нормалну подгрупу H такву да су H и G/H решиве. (Последица овог тврђења је још нешто што можете да користите у задацима: група G је решива акко је G/C_G решива).

Пример 0.38. Симетрична група $\mathbb{S}_n$ и алтернирајућа $\mathbb{A}_n$ су решиве ако и само ако је $n \leq 4$. То следи из примера о изводу ових група. За $n \geq 5$ низови извода за ове две групе су

$$\mathbb{S}_n \rhd \mathbb{A}_n \rhd \mathbb{A}_n \rhd \cdots$$

и

$$\mathbb{A}_n \rhd \mathbb{A}_n \rhd \mathbb{A}_n \rhd \cdots .$$

За $n = 4$ имамо

$$\mathbb{S}_4 \rhd \mathbb{A}_4 \rhd \mathbb{V}_4 \rhd \{\varepsilon\}$$

и

$$\mathbb{A}_4 \rhd \mathbb{V}_4 \rhd \{\varepsilon\}.$$

Низ извода за $\mathbb{S}_3$ је

$$\mathbb{S}_3 \rhd \mathbb{A}_3 \rhd \{\varepsilon\},$$

док су $\mathbb{A}_3$, $\mathbb{S}_2$ и $\mathbb{A}_2$ Абелове, па је већ њихов извод тривијалан.

Пример 0.39. Диедарска група $\mathbb{D}_n$ је решива. Опет на основу примера о изводу диедарске групе следи да је низ извода за ову групу

$$\mathbb{D}_n \rhd \langle \rho^2 \rangle \rhd \{\varepsilon\}.$$