CSOPORTELMÉLET

GULÁCSI TAMÁS

1. Definíciók, tételek

1.1. Csoport fogalma. G halmaz csoport a $\cdot$ műveletre, ha

1. $\forall a,b\in G\ \exists! c\in G : ab = c$.
2. $\forall a,b,c\in G\ a(bc) = (ab)c$ — **asszociatív**
3. $\exists e\in G : \forall g\in G eg = g$ — **egységelem, 1**
4. $\forall a\in G\ \exists a^{-1}\in G : aa^{-1} = 1$ — **inverz**

G **Abel-csoport**, ha *kommutatív*, azaz $\forall a,b\in G\ ab = ba$.

1.1.1. Állítás. *G csoport neutrális eleme és G elemeinek inverzei egyértelműen meghatározottak.*

1.1.2. Tétel. *Ha $a,b\in G$, akkor az $ax = b$, $ya = b$ egyenletek G-ben egyértelműen megoldhatóak, és ez a tulajdonság helyettesítheti a 3. axiómát.*

Véges csoport esetén a fenti axiómarendszerben a 3. és 4. axióma helyettesíthető az egyszerűsítési szabállyal*: ha $a,x,y\in G$, akkor $ax = ay\ \vee\ xa = ya \implies x = y$.*

1.2. Komplexusok. G csoport részhalmazai a **komplexusok**. Legyenek $K_1, K_2\subseteq G$ komplexusok, ekkor szorzatuk: $K_1K_2 = \{ab \mid a\in K_1, b\in K_2\}$. Erre a szorzásra is érvényes az asszociativitás.

1.3. Ciklikus csoportok. G csoport **ciklikus**, ha egy elemmel generálható, azaz $G = \langle a\rangle = \{a^n \mid n\in\mathbb{N}\}$.

Ha a véges rendű, azaz $\exists r\in\mathbb{N} : a^r = 1\ \wedge\ a^1,..,a^{r-1} \neq 1$, akkor G is véges ciklikus csoport.

1.3.1. Tétel. *Végtelen ciklikus csoport izomorf az egészek additív csoportjával ($\implies$ a végtelen ciklikus csoportok izomorfak egymással).*

Véges n-edrendű ciklikus csoport izomorf a $\mod n$ maradékosztályok additív csoportjával.

Ciklikus csoport minden részcsoportja is ciklikus.

1.4. Mellékosztályok. $H\leq G$-re és $a\in G$-re Ha az a jobb-, aH a baloldali mellékosztálya.

1.4.1. Tétel. *Ha aH és bH a G-nek két, H szerinti mellékosztálya, akkor vagy $aH = bH$, vagy aH és bH diszjunktak.*

Megkapjuk G H szerinti indexét is: G tehát felbomlik a H szerinti mellékosztályokra, $G = H + aH + bH + \ldots$ — az itt szereplő mellékosztályok száma $|G : H|$.

G-nek a H részcsoport szerinti bal- és jobboldali mellékosztályainak száma azonos.

Date: 1998. november 19.

1.4.2. Tétel (Lagrange)**.** *Véges csoport részcsoportjának rendje és indexe osztója a csoport rendjének, azaz $|G| = |G : H|\cdot|H|$.*

$\circ$*Köv.* 1.4.2.1. G véges csoportra $\forall a\in G\ o(a) \mid |G|$.

Prímszámrendű csoport ciklikus.

1.4.3. Tétel. *Egy G csoport pontosan akkor prímszámrendű, ha pontosan két részcsoportja van.*

1.5. Normális részcsoportok. $N\leq G$ normálosztó, ha $\forall a\in G$-re $aN = Na$, azaz $a^{-1}Na = N$, jele $N\lhd G$.

$a\in G$ rögzített elemre G önmagára való $x \to a^{-1}xa$ leképezését **konjugálás**nak nevezzük, *bijektív homomorfizmus* — belső automorfizmus.

$a^{-1}Ha \cong H\ \forall a\in G$-re, de csak akkor egyenlő, ha $H \lhd G$:

1.5.1. Tétel. *A G csoport N részcsoportja pontosan akkor egyezik meg minden konjugáltjával, ha N a G-nek normálosztója ($N \lhd G$).*

Normális részcsoportok metszete is normális.

Ha $N \lhd G$ és $H \leq G$, akkor $G \geq \{N, H\} = NH = HN$.

2 indexű részcsoport mindig normálosztó.

A normális részcsoportok szerinti mellékosztályok a csoportnak kompatibilis osztályozását adják, és minden kompatibilis osztályozás valamely normáalosztó mellékosztályai.

Triviális normálosztó: 1 és G. Ha G-ben csak triviális normálosztó van, akkor ***G* egyszerű**. A kommutatív csoportok között az egyszerűek a prímszámrendűek.

1.6. Faktorcsoport.

1.6.1. Tétel. *Egy G csoportnak valamely N normálosztója szerinti mellékosztályai a komplexusszorzásra nézve csoportot alkotnak, ez G-nek N szerinti **faktorcsoport**ja, jele G/N.*

G tetszőleges homomorfizmusának magja G-nek normálosztója, G tetszőleges normálosztólya G alkalmas homomorfizmusának magja.

1.6.2. Tétel (Homomorfizmus-tétel)**.** *Ha ϕ a G csoportnak egy G' csoportra való homomorfizmusa, és N e homomorfizmus magja, akkor $G' \cong G/N$, azaz $\phi(G) \cong G/\mathrm{Ker}\,\phi$.*

Epimorfizmus akkor és csak akkor izomorfizmus, ha magja 1.

1.7. Izomorfizmus-tételek.

1.7.1. Tétel. *Legyen $N \lhd G$. Kölcsönösen egyértelmű megfeleltetés áll fenn G-nek N-et tartalmazó részcsoportjai és a $\overline{G} = G/N$ faktorcsoportnak részcsoportjai közt. A megfeleltetést a természetes homomorfizmus, ill. annak inverze adja meg. Normális részcsoportok egymásnak felelnek meg.*

1.7.2. Tétel. ***I. izomorfizmus-tétel*** *Ha* $H \le G$ *és* $N \lhd G$, *akkor* $H \cap N \lhd H$, *és* $\{H,N\}/N \cong H/H\cap N$.

II. izomorfizmus-tétel *Ha* $N, M \lhd G$ *és* $N \subset M$, *akkor* $(M/N) \lhd (G/N)$ *és*

$$(G/N)/(M/N) \cong G/M \tag{I.1}$$

1.8. Normálláncok.

A G részcsoportjainak olyan véges sorozatát, amelyik G-vel kezdődik és 1-el végződik, és mindegyik közbülső részcsoport normálosztója az előzőnek, G normálláncának nevezzük.

(I.2) G **normállánca:** $G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = 1$

a lánc faktorai: $G_0/G_1, G_1/G_2, .., G_{r-1} \rhd G_r = 1$

Ha a G_i-k mind különbözők, akkor a normálláncot ismétlődés nélkülinek mondjuk. A lánc faktorainak száma r, a lánc hossza.

G két normállánca izomorf, ha a faktorcsoportok izomorfak. Izomorf láncok hossza megegyezik, láncok izomorfizmusa tranzitív.

Minden normállánc a $G \rhd 1$ normállánc **finomítása**. Ha egy normállánc ismétlődés nélküli és csak triviálisan (ismétlődéssel) finomítható, akkor **kompozíciólánc**nak hívjuk.

1.8.1. Tétel. *Egy normállánc pontosan akkor kompozíciólánc, ha faktorai egyszerű csoportok.*

Jordan-Hölder tétel: *Ha a G csoportnak van kompozíciólánca, akkor G-nek tetszőleges két kompozíciólánca izomorf.*

Schreier-finomítás: *tetszőleges csoport bármely két normállánca finomítható úgy, hogy a keletkező új normálláncok izomorfak.*

G csoport **feloldható**, ha van olyan normállánca, melyben minden faktorcsoport Abel-csoport. Ha tehát van kompozíciólánca is, akkor van olyan kompozíciólánca, melynek faktorai kommutatívak, így

1.8.2. Tétel. *Véges csoport pontosan akkor feloldható, ha kompozícióláncának faktorai prímrendűek.*

1.9. Permutációcsoportok.

Permutáció: egy n elemű halmaz önmagára való bijektív leképezése; az $(1\,2\,3\ldots n)$ elemnek a $(i_1\, i_2\, i_3 \ldots i_n)$ elemet felelteti meg; A szorzás asszociatív, de nem feltétlenül kommutatív; az egységelem az identikus leképezés.

A permutációk ciklikus írásmódja: a $\tau = (i_1\, i_2 \ldots i_n)$ **ciklus** az a permutáció, mely az i_1-et i_2-be, az i_3-at i_4-be … viszi; A nem szereplő elemek fixen maradnak. „Ciklus rendje" = „ciklus hossza".

A kételemű (ik) ciklus a **transzpozíció** — az i és k elemet felcseréli, a többit változatlanul hagyja.

1.9.1. Tétel. *n elemű halmaz önmagára való leképezései csoportot alkotnak, ez az n-edfokú szimmetrikus csoport, melynek jele S_n, rendje $n!$.*

Részcsoportjai az n-edfokú permutációcsoportok. Az $x_1, .., x_n$ elemekkel generált $A = \prod_{1\le k<i\le n}(x_i - x_k)$ *Vandermonde-determinánst fixen hagyó* $\left(\prod_{1\le \pi(k)<\pi(i)\le n}(x_{\pi(i)} - x_{\pi(k)}) = \prod_{1\le k<i\le n}(x_i - x_k)\right)$ *pi permutációk S_n-nek részcsoportját alkotják, ez az **n-edfokú alternáló csoport**, jele A_n, rendje $\frac{n!}{2}$, és normálosztó, mert $|S_n : A_n| = 2$.*

Diszjunkt ciklusok szorzata kommutatív, és minden permutáció egyértelműen felírható idegen ciklusok szorzataként.

*$n \ge 5$ esetén az A_n alternáló csoport egyszerű, így ekkor **S_n kompozíciólánca:** $S_n \rhd A_n \rhd 1$. Ebből következik, hogy S_n nem feloldható, hiszen így faktorai nem prímrendűek* $\left(|S_n/A_n| = \frac{n!}{\frac{n!}{2}} = 2,\ |A_n/1| = \frac{n!}{2}\right)$.

Cayley-tétel: *Tetszőleges n-edrendű csoport izomorf egy n-edfokú permutációcsoporttal.*

1.10. Direkt szorzat.

a G csoport az $A, B \le G$ részcsoportok direkt szorzata, ha

I_1 $\{A, B\} = G$
I_2 $A \cap B = 1$
I_3 $A \lhd G$ és $B \lhd G$.

és

$\mathrm{II}_{1,2}$ $\forall g\in G\ \exists! a\in A, \exists! b\in B : g = ab$
II_3 $ab = ba\ \forall a\in A,\ b\in B$.

ezen két definíció ekvivalens. Jelölés: $G = A \times B$ (additív esetben $G = A+B$)Hasonlóan értelmezhető a direktszorzat kettőnél több tagra.

Tetszőleges két A, B csoportra is értelmezhető a direktszorzat: $G := \{(a,b) \mid a\in A, b\in B\}$, $(a,b) = (a',b') \iff a=a' \wedge b=b'$, $(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2, b_1b_2)$. Erre a műveletre G csoport.

1.10.1. Tétel. *Ha n kanonikus felbontása $n = p_1^{k_1} \ldots p_r^{k_r}$, akkor az n-edrendű $\{a\}$ ciklikus csoport felbontható $p_1^{k_1}, .., p_r^{k_r}$ rendű ciklikus csoportok direkt szorzatára:*

$$C_n = C_{p_1^{k_1}} \times \ldots \times C_{p_r^{k_r}} \tag{I.3}$$

1.11. Véges Abel-csoportok.

***p*-csoport**nak nevezünk olyan csoportot, amelyben minden elem rendje a (rögzített) p prímnek valamilyen hatványa $(o(1)=1=p^0)$.

1.11.1. Tétel. *Minden G véges Abel-csoport (sőt elég feltenni, hogy minden elem rendje véges) különböző prímekhez tartozó p-csoportok direkt szorzata. Ezek a G_p csoportok G által egyértelműen meg vannak határozva. A G_p részcsoportokat a G **p-komponensei**nek nevezzük.*

Véges Abel-féle p-csoport felbontható p-hatványrendű ciklikus csoportok direk szorzatára.

$\circ$*Köv.* 1.11.1.1. Az A véges Abel-féle p-csoport p-hatványrendű ciklikus csoportok direkt szorzata, így A rendje is p-hatvány. Ha tehát véges Abel-csoport rendje n, és p-nek az n-ben foglalt legnagyobb hatványa p^k, akkor G-nek G_p p-komponense pontosan p^k rendű kell, hogy legyen.

1.11.2. Tétel (Véges Abel-csoportok alaptétele)**.** *Véges Abel-csoport felbontható véges sok prímhatványrendű ciklikus csoport direkt szorzatára. A felbontásban szereplő ciklikus csoportok rendjei a (sorrendtől eltekintve) egyértelműen meg vannak határozva.*

Könnyen látható, hogy ha két véges Abel-csoporthoz ugyanaz a prímhatvány-halmaz tartozik, akkor a két csoport izomorf, és hogy tetszőleges véges prímhatvány-halmazhoz tartozik véges Abel-csoport, a véges Abel-csoportok tehát izomorfizmus erejéig tökéletesen jellemezhetők prímhatványok véges halmazaival.

1.12. Centrum, centralizátor, normalizátor. Nem-kommutatív csoport minden más elemmel felcserélhető elemei: $Z := \{c \in G \mid cx = xc\ \forall x \in G\}$ a G csoport **centruma**, elemei a centrumelemek.

1.12.1. Tétel. *Csoport centruma a csoportnak normálosztója.*

Egy G csoport centruma G-nek pontosan azon elemeiből áll, amelyek G-nek minden belső automorfizmusánál fixen maradnak, azaz $Z = \mathrm{Ker}(\mathrm{Inn}\, G)$, így $G/Z = \mathrm{Inn}\, G$.

A G-nek az $a \in G$-vel felcserélhető elemei G egy nemüres részhalmazát adják — ez részcsoport, de nem feltétlenül normálosztó. Ez **az a elem centralizátora**: $C(a)$. Nyilván $C(a)=G \iff a \in Z$.

$A \subseteq G$ centralizátora G-ben: $C(A) = \{g \in G \mid ga=ag\ \forall g \in A \subseteq G\}$. **$A$ normalizátora**: $N(A) = \{h \in G \mid hA = Ah\}$ (G-nek az a maximális részcsoportja, amelyben az adott A normálosztó — $A \triangleleft N(A)$).

Nyilván $\forall a \in G$-re $C(a)=N(a)$, és $C(A) \subseteq N(A)$ ($A \subseteq G$).

1.12.2. Tétel. *Az $a \in G$ elemnek G-ben annyi különböző konjugáltja van, mint a centralizátorának indexe, azaz $|\{x^{-1}ax \mid x \in G\}| = |G : C(a)|$.*

A G csoport A részcsoportjának pontosan annyi különböző konjugáltja van, mint A normalizátorának indexe G-ben, azaz $|\{x^{-1}Ax \mid x \in G\}| = |G : N(A)|$.

Ha tehát G véges csoport, akkor tetszőleges elem különböző konjugáltjainak száma G renjének osztója (részcsoport indexe a rend osztója).

Ha $|G| = p^n$ $(n \geq 1)$, akkor $Z \neq 1$.

Prímhatványrendű csoport feloldható.

1.13. Sylow tételei. Egy $P \leq G$ rcs. **p-Sylow-részcsoport**, ha $p \mid n=|G|$, prím, melyre $|P| = p^k$, k a legmagasabb hatv'y, mellyel n még osztható. G csoport p-Sylow részcsoportjait jelölje $\mathrm{Syl}_p(G)$.

1.13.1. Tétel. ***I. Sylow-tétel:*** *G véges csoport minden p prímszámra tartalmaz p-Sylow-részcsoportot ($\mathrm{Syl}_{p\nmid n}(G) := \{1\}$), sőt véges csoport minden p-részcsoportja benne van egy p-Sylow részcsoportban.*

Cauchy tétele: *Ha G véges csoport rendje osztható p prímmel, akkor G tartalmaz p-edrendű elemeket.*

<u>*Köv:*</u> *Véges p-csoport rendje p-hatvány.*

II. Sylow-tétel: *A G véges csoport p-Sylow részcsoportjainak száma kongrunens 1-el modulo p, azaz $|\mathrm{Syl}_p(G)| \equiv 1 \mod p$.*

III. Sylow-tétel: *A G véges csoport p-Sylow részcsoportjai egymás konjugáltjai.*

Ha G feloldható, és m olyan osztója $n=|G|$ rendnek, hogy $(m, \frac{n}{m}) = 1$, akkor G tartalmaz m-edrendű részcsoportokat, és ezek mind egymás konjugáltjai.

1.14. Szabad csoportok. Szimbóllumok (betűk), gyártása — az egyetlen megkötés, hogy betű és inverze ne kerüljön egymás mellé. Szavak szorzása: egymás mellé írás, tiltott kapcsolat elhagyása.

1.14.1. Tétel. *Az $x_1, .., x_n$ szimbólumokkal készített szavak a fenti szorzásra nézve csoportot alkotnak, ezt* ***szabad csoport****nak nevezzük; $x_1, .., x_n$ a csoport szabad generátorai. „Csoport rangja" = „szabad generátorok száma".*

Legyen F szabad csoport az $x_1, .., x_n$ szabad generátorokkal, és G tetszőleges csoport. Feleltessünk meg minden x_i-nek tetszőlegesen egy $g_i \in G$ elemet. Ekkor van F-nek egy oly egyértelműen meghatározott homomorfizmusa G-be, melynél minden x_i a neki megfeleltetett g_i-be megy át.

Minden G csoport előállítható egy F szabad csoport faktorcsoportjaként. Ha G n elemmel generálható, akkor F választható F_n-nek (F_n: n szabad generátor generálta szabad csoport).

1.15. Csoport megadása definiáló relációkkal. Legyenek $g_1, .., g_n, \ldots$ tetszőleges szimbólumok, és $g_{i_1}^{k_1} \cdots g_{i_r}^{k_r} = e$, $\ g_{i_{r+1}}^{k_{r+1}} \cdots g_{i_{r+s}}^{k_{r+s}} = 1, \ldots$ tetszőleges egyenlőségek, melyek bal oldalán a g_n-ekből készített szavak, jobb oldalán pedig az 1 szimbólum áll. Ekkor

$$F/N \cong G = \{g_1, .., g_n, \ldots \mid g_{i_1}^{k_1} \cdots g_{i_r}^{k_r} = 1, \ldots\}$$

ahol F szabad csoport, melynek szabad generátorai a g_n szimbólumoknak bijektíven megfeleltetett x_n szimbólumok; N az F-nek az a normális részcsoportja, amelyet az adott egyenletek baloldalainak megfelelő $x_{i_1}^{k_1} \cdots x_{i_r}^{k_r}, \ldots$ F-beli elemek generálnak. Ez a **G megadása generátorokkal és definiáló relációkkal**.

1.15.1. Tétel (Dyck). *Ha a G és G' ugyanazon generátorokkal vannak értelmezve úgy, hogy G-nek minden definiáló relációja szerepel G definiáló relációi közt, akkor G' a G-nek egy faktorcsoportjával izomorf — a II. izomorfia-tétel alapján $G' \cong F/N' \cong (F/N)/(N'/N)$.*

1.16. Fontos csoportok.

1.16.1. Def. G véges csoport megadható **Cayley-táblázattal:** G elemeit felsoroljuk, a táblázatba a szorzatok kerülnek.

Egyszerű példák: $\langle Z, +\rangle$, ennek egy részcsoportja az m-el osztható egészek; $\langle K, +\rangle$, $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$; $\langle K, \cdot\rangle$, $K \in \{\mathbb{Q}_+, \mathbb{R}\}$, itt a pozotívak részcsoportot alkotnak;

<u>Csoportot alkotnak:</u> A nem zérus komplex számok (multiplikatív) — az 1 absz. értékűek részcsoport (egységgyökök csoportja); Az $n \times n$-es mátrixok a mátrixszorzásra, mátrixösszeadásra; A maradékosztályok mod m (additív); A nem zérus maradékosztályok tetsz. modulusnál (multiplikatív).

A tér vektorai additív csoportot alkotnak; A sík kongruens leképezései a leképezésszorzásra (részcsoportok: a sík mozgásai, az eltolások, az egy pont körüli forgatások); A sík hasonlósági transzformációi.

A $[0, 1]$ intervallumon integrálható fvek (additív), ugyanitt a folytonosak (multiplikatívak); A valós számsorozatok az összeadásra (részcsoportot alkotnak a konvergens sorozatok).

Q: kvaterniócsoport $Q = \{\pm 1, \mp i, \pm j, \pm k\}$, $i^2=j^2=k^2 = -1$, $ij= -ji=k$, $jk= -kj=i$, $ki= -ik=j$.

6 negyendrendű, 1 másod- és 1 elsőrendű eleme van, 6 részcsoport van benne.

D_m: diédercsoport A síknak egy szabályos m-oldalú sokszögét önmagába vivő kongruens leképezéseiből áll. Ha f a $\frac{2\pi}{m}$-el való forgatást, t pedig a szimmetriatengelyre való tükrözést jelöli, akkor $D_m = \{1, f, f^2, .., f^{m-1}, t, tf, .., tf^{m-1}\}$, $f^m=1$, $t^2=1$ és $ft=tf^{m-1}$.

K: Klein-féle csoport — diédercsoport m=2-re; $\{1, f, t, ft\}$.

Faktorcsoportok: Ha $G=\{a\}=C_\infty$, és $N=\{a^n\}$, akkor a G/N faktorcsoport izomorf az n-edrendű ciklikus csoporttal.

Ha $G=Q$ a kvaterniócsoport, és $N=\{-1\}$ kételemű rcs, akkor az N szerinti mellékosztályok neutrális eleme a komplexusszorzásra az N, a többi három m.o. közül bármely kettő szorzata a harmadik, így $G/N \cong K$.

Permutációcsoportok: S_2 másodrendű ciklikus csoport, $S_3 = \{(1), (123), (132), (12), (13), (23)\}$, az első 3 alkotja A_3-at — $S_3 \triangleright A_3 \triangleright 1$ a kompizíciólánc, a faktorok C_2 és C_3.

$|S_4|=24$, $S_4 \triangleright A_4 \triangleright K \triangleright B_i \triangleright 1$, ahol K a Klein-csoport, B_i a K 3 nem-triviális, másodrendű normálosztója. S_4 kompozíciólláncának faktorai: C_2, C_3, C_2, C_2.

S_2, S_3, S_4 tehát feloldható csoportok, $n\geq 5$-re azonban már nem.

Direktszorzat: $G=\{a\}=C_n$, $n=rs$, $(r,s)=1$. Ekkor $G=\{a^r\}\times\{a^s\}=C_r\times C_s$.

Az n dimenziós vektoroka additív csoportja izomorf az egyes koordinátatengelyek irányába eső vektorok additív csoportjainak direkt összegével;

$\langle\mathbb{C}\backslash\{0\},\cdot\rangle \cong \mathbb{R}^+ \times \langle\{z\in\mathbb{C} \mid |z|=1\},\cdot\rangle$.

Véges Abel-csoport: Ha $A=\{a\}\times\{b\}$, ahol $|\{a\}|=p^n$, $|\{b\}|=p^k$, és $n\geq k$, akkor A-nak sok egyéb felbontása is van egy p^n és egy p^k rendű ciklikus csoport direkt szorzatára: pl. $A=\{ab\}\times\{b\}=\ldots=\{ab^{p^{k-1}}\}\times\{b\}$.

Centrum: A Q kvaterniócsport centruma a ± 1 elemekből áll. $Z=G \iff G$ kommutatív. Nem-kommutatív egyszerű csoportban $Z=1$.

Definiáló relációkkal megadott csoportok: $C_n=[a \mid a^n=1]$;

$S_3=[a,b \mid a^3=b^2=1, abab=1]$; $Q=[a,b \mid a^4=abab^{-1}=1, a^2=b^2]$;

$D_m=[a,b \mid a^m=b^2=1, abab=1]$.