DOI: 10.5281/zenodo.15659364
Link: https://zenodo.org/records/15659364

SIKLIK GRUPPALARNING O‘RNI VA AHAMIYATI

Nizomiy nomidagi O‘zbekiston milliy pedagogika universiteti
Matematika va informatika yo‘nalishi,
4-bosqich talabasi Akmalova Nargiza Abbos qizi
Telefon raqami:+ 998999183270
Elektron pochta manzili: akmalovanargiza42@gmail.com

Annotatsiya: *Ushbu maqolada siklik gruppalar nazariyasining nafaqat zamonaviy matematikaning eng muhim bo‘limlaridan biri hisoblangan algebra fanida, balki informatsion texnologiyalar, kriptografik algoritmlar, raqamli xavfsizlik, kodlash tizimlari, kompyuter grafikasi va kvant hisoblash kabi fanlarda ham tutgan o‘rni va ahamiyati , shuningdek gruppalar nazariyasi hamda siklik gruppalar nazariyasining kelib chiqish tarixi haqida so‘z boradi.Shu bilan bir qatorda bu maqolada siklik gruppalarga oid umumiy ma’lumotlar, jumladan siklik gruppaning ta’rifi, unga doir misollar, siklik gruppalarda izomorfizm hamda gomomorfizmlar keltirib o‘tilgan.*

Kalit so‘zlar: *gruppa, siklik gruppa, izomorfizm, gomomorfizm.*

Zamonaviy matematikaning eng muhim bo‘limlaridan biri hisoblangan algebra fani ichida gruppalar nazariyasi alohida o‘rin egallaydi. Algebraik strukturalar ichida gruppalar matematik obyektlar ustida bajariladigan operatsiyalarni tartibga soluvchi eng asosiy va universal model sifatida maydonga chiqadi. Har qanday strukturaviy o‘zgarish yoki simmetriya gruppa ko‘rinishida ifodalansa, gruppaning alohida ko‘rinishlari — masalan, siklik gruppalar — ushbu tizimlarning oddiy, ammo chuqur xususiyatlarini o‘rganish uchun qulay vosita bo‘lib xizmat qiladi.

Gruppalar nazariyasi XIX asrda Evarist Galois (Fransuz matematigi) tomonidan rivojlantirilgan bo‘lib, dastlab algebraik tenglamalarning ildizlarini o‘rganish bilan bog‘liq bo‘lgan. Galois nazariyasi orqali tenglamalarning ildizlari ustida harakat qiluvchi gruppa tushunchasi paydo bo‘ldi. Bir qarashda gruppalar nazariyasi ahamiyatsiz bo‘lib ko‘rinsada, ushbu nazariya nafaqat matematikani, balki butun fan dunyosini tubdan o‘zgartirdi. Keyinchalik bu nazariya umumlashtirilib, barcha turdagi harakatlar, simmetriyalar, tuzilmalar va ularning kombinatsiyalarini ifodalovchi umumiy gruppa tushunchasi shakllantirilgan.

Siklik gruppalar esa gruppalarning eng sodda, eng intuitiv tushunarli va ayni paytda eng ko‘p uchraydigan turlaridan biridir.

Siklik gruppalar tushunchasi qadimgi matematik tushunchalarga borib taqaladi. Antik davr matematiklari, ayniqsa yunonlar, sonlar ustida aylana bo‘ylab aylanish, geometrik transformatsiyalar kabi amallarni o‘rganishgan. Bu jarayonlar tabiiy ravishda siklik strukturalarni keltirib chiqargan. Keyinchalik XVIII-XIX asrlarda Leonhard Eyler, Karl Fridrix Gauss, va Evarist Galoislarning ishlari orqali sonlar nazariyasida qoldiqlar arifmetikasida siklik gruppalar tabiiy tarzda yuzaga keldi. XX asrga kelib, matematikada strukturaviy yondashuv keng tarqalib, gruppalar, halqalar, maydonlar kabi algebraik obyektlar fundamental tushunchalar sifatida shakllandi. Bunda har qanday nihoyalangan abel gruppa (ya’ni, kommutativ gruppa) siklik gruppalarning to‘g‘ri ko‘paytmasi sifatida ifodalanishi mumkinligi isbotladi. Bu esa siklik gruppalarning algebraik strukturalar qurilishidagi asosiy rolini yana bir bor isbotlab bergan.

Siklik gruppa — bu bitta element orqali hosil qilinadigan, ya’ni har bir elementi shu bitta elementning darajalari orqali ifodalanadigan gruppadir. Boshqacha aytganda, siklik gruppaning barcha elementlari bitta “generator” elementning kuchlari orqali aniqlanadi. Bu soddalik ularni o‘rganishni qulaylashtiradi, shuningdek, boshqa murakkab gruppalarni tahlil qilishda tayanch vazifa bajaradi.

Siklik gruppalar haqida umumiy bilimlarni ko‘rib chiqamiz.

Gruppa tushunchasi to‘rtta asosiy aksiomani qanoatlantiruvchi to‘plam va unda aniqlangan binar operatsiyadan iborat. Bu aksiomalar quyidagilardan iborat: operatsiyaga nisbatan yopiqlik, operatsiyaning assotsiativligi, birlik elementning mavjudligi va har bir element uchun teskari elementning mavjudligi.

Siklik gruppa esa yanada xosroq tuzilishga ega. Agar G gruppada shunday ‘a’ element mavjud bo‘lsaki, G ning har bir elementi ‘a’ ning darajasi (agar gruppa amali ko‘paytirish bo‘lsa) yoki ‘a’ ning karrali (agar gruppa amali qo‘shish bo‘lsa) ko‘rinishida ifodalansa, u holda G **siklik gruppa** deyiladi. Bunday ‘a’ elementi **siklik gruppaning generatori** deb ataladi. Agar P gruppaning ixtiyoriy ‘a’ elementi olinsa va bu elementning musbat, nol va manfiy darajalaridan tuzilgan to‘plam har bir $a \in P$ uchun qism gruppa bo‘lsa, u holda bu to‘plam **siklik gruppa** deyiladi.

Ta’rif. *Agar G gruppada* $G = (a)$ *tenglikni qanoatlantiruvchi* $a \in G$ *element mavjud bo‘lsa, u holda G gruppa* ***siklik gruppa*** *deyiladi.*

Siklik gruppalarga quyidagilarni misol qilishimiz mumkin:

- *Qo‘shishga nisbatan butun sonlar gruppasi* $(Z, +)$ *siklik gruppa bo‘ladi, ya’ni* $Z = (1)$.
- *Qo‘shishga nisbatan chegirmalar gruppasi* $(Z_n, +)$ *ham siklik gruppa bo‘ladi, ya’ni* $Z_n = (1)$.

Har qanday siklik gruppa kommutativ gruppa bo‘ladi.Buni quyidagicha keltirishimiz mumkin:

$G = (a)$ siklik gruppaning ixtiyoriy b va c elementlari uchun shunday butun n va m sonlar topilib, $b = a^n$ va $c = a^m$ tengliklar o‘rinli. Ushbu $b * c = a^n * a^m = a^{n+m} = a^m * a^n = c * b$ tenglikdan b va c elementlar o‘zaro o‘rin almashinuvchi ekanligi kelib chiqadi. O‘z navbatida b va c elementlarning ixtiyoriy ekanligidan G gruppaning kommutativligi kelib chiqadi.

Gruppalar o‘rtasidagi gomomorfizm $\varphi: G \to H$ deb shunday φ funksiyaga aytiladiki, barcha $a, b \in G$ uchun $\varphi(ab) = \varphi(a)\varphi(b)$ sharti bajariladi, bu yerda chap tomonda G dagi amal, o‘ng tomonda esa H dagi amal tushuniladi. Izomorfizm esa biektiv (o‘zaro bir qiymatli va butun qamrovli) gomomorfizmdir. Izomorf gruppalar bir xil algebraik tuzilishga ega bo‘lib, faqat elementlarining nomlari farq qilishi mumkin.

$G = < a >$ va $H = < b >$ siklik gruppalari o‘rtasida gomomorfizm mavjudligi G ning generatori ‘a’ ning obrazi bilan to‘liq aniqlanadi. Agar G cheksiz bo‘lsa, $\varphi(a)$ H ning istalgan elementi bo‘lishi mumkin. Agar G ning tartibi n bo‘lgan chekli bo‘lsa, u holda $\varphi(a)$ ning H dagi tartibi n ni bo‘lishi kerak.

Siklik gruppalar izomorf bo‘lishi uchun quyidagi shartlar bajarilishi kerak: ikkita cheksiz siklik gruppa har doim izomorfdir. Izomorfizm $\varphi: Z \to Z$ orqali $\varphi(n) = n$

yoki $\varphi(n) = -n$ ko‘rinishida aniqlanishi mumkin. Ikkita chekli siklik gruppa izomorf bo‘lishi uchun ularning tartiblari teng bo‘lishi zarur va kifoya. Agar $|G| = n$ va $|H| = n$ bo’lib, $G = < a >$ va $H = < b >$ bo‘lsa, u holda izomorfizm

$$\varphi: G \to H \; \varphi(a < sup > k < /sup >) = b < sup > k < /sup >$$

orqali aniqlanadi, bu yerda $k = 0, 1, \ldots, n-1$.

Siklik gruppalarning fundamental teoremasi ushbu gruppalarning tuzilishini to‘liq tavsiflaydi:

1. Har bir siklik gruppaning kichik gruppa siklikdir.
2. n tartibli chekli siklik gruppa uchun n ning har bir musbat bo‘luvchisi d uchun tartibi d bo‘lgan yagona kichik gruppa mavjud. Bu kichik gruppa G ning ‘a’ generatori uchun $a^{(\frac{n}{d})}$ elementi tomonidan hosil qilinadi.

Teoremaning birinchi qismi har qanday siklik gruppaning (cheksiz yoki chekli) har qanday qism gruppa ham o‘zi kabi bir element tomonidan hosil qilinishini ta’kidlaydi. Bu siklik gruppalarning qism gruppalari ham xuddi o‘ziga o‘xshash oddiy tuzilishga ega ekanligini ko‘rsatadi.

Teoremaning ikkinchi qismi n tartibli chekli siklik gruppalarning kichik gruppalari tuzilishini yanada aniqroq tasvirlaydi. U gruppa tartibining har bir bo‘luvchisi uchun tartibi shu bo‘luvchiga teng bo‘lgan yagona kichik gruppa mavjudligini aytadi. Bundan tashqari, bu kichik gruppani gruppa generatorining mos darajasini olish orqali qanday hosil qilish mumkinligini ko‘rsatadi. Bu teorema chekli siklik gruppalarning kichik gruppalari tuzilishini to‘liq klassifikatsiya qiladi va ularni topish masalasini gruppa tartibining bo‘luvchilarini topishga olib keladi.

Fundamental teorema siklik gruppalarning juda oddiy va yaxshi aniqlangan tuzilishga ega ekanligini ko‘rsatadi. Ularning kichik gruppalari tuzilishi gruppaning tartibi bilan to‘liq belgilanadi. Bu soddalik siklik gruppalarni gruppalar nazariyasida fundamental rol o‘ynashining asosiy sabablaridan biridir.

Siklik gruppalar — nafaqat nazariy matematikaning bir qismi, balki amaliyotda ham keng qo‘llaniladigan modellar toifasiga kiradi. Zamonaviy informatsion texnologiyalar, kriptografik algoritmlar, raqamli xavfsizlik, kodlash tizimlari, kompyuter grafikasi va kvant hisoblash kabi fanlarda siklik gruppalar fundamental asos sifatida qo‘llaniladi. Masalan, Diffie-Hellman kalit almashinuvi algoritmi, RSA shifrlash tizimi yoki El-Gamal kabi algoritmlarning matematik asosida aynan siklik gruppalarning xossalari yotadi. Shuningdek, kompyuter fanlarida ma’lumotlarni aylantirish, kodlash, shifrlash va verifikatsiya qilish kabi jarayonlarda siklik strukturalardan foydalaniladi. Bularning barchasi siklik gruppalarning tuzilishi, generatorlari, tartibi, elementlar soni va izomorfizmlarini chuqur o‘rganishni talab qiladi. Bundan tashqari, ta’lim tizimida siklik gruppalar mavzusi maktab va universitet darajasida algebra kurslarida o‘qitiladi. Bu mavzuni chuqur o‘rganish talabalar tafakkurini rivojlantiradi, mantiqiy fikrlash, isbotlash, tushunchalar orasidagi bog‘liqlikni ko‘rish qobiliyatini kuchaytiradi. Ayniqsa, siklik gruppalar orqali har qanday nihoyalangan gruppaning tuzilmasini tahlil qilish, unga izomorfik modell topish, hosil qiluvchi elementlarni aniqlash orqali mukammal bilim hosil qilish mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Ayupov Sh.A., Omirov B.A. Xudoyberdiyev A.X., Haydarov F.H. Algebra va sonlar nazaryasi. \Tafakkur bo`stoni", 2019 y. 296 b.
2. Fraleigh J.B., Brand N. A First Course in Abstract Algebra. 8th Edition. “Pearson Education”, 2020, p. 443.
3. Malik D.S., Mordeson J.N., Sen M.K. Fundamentals of abstract algebra.“WCB McGrew-Hill”, 1997, p.636.
4. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. “Наука”,1982, 288 с.
5. Курош А.Г. Лекции по общей алгебре. “Физматлит”, 1973, 400с.
6. Курош А.Г. Теория групп. “Наука”, 1967, 648 с.
7. yangiasr.uz,https://yangiasr.uz/files/books/2024-02-27-07-47-20_8cad2b26320355d7cd3fe86eb1de5fb6 .pdf 2 . Matematika.Абдуллаева-Б.pdf - Jizzax davlat pedagogika universiteti
8. Sh.A.Ayupov, B.A.Omirov, A.X.Xudoyberdiyev. ABSTRAKT ALGEBRA (o‘quv qo‘llanma). Toshkent 2021