O‘ZBEKISTON RESPUBLIKASI OLIY VA
O‘RTA MAXSUS TA’LIM VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI
O‘ZBEKISTON MILLIY UNIVERSITETI

Sh.A.Ayupov, B.A.Omirov, A.X.Xudoyberdiyev

ABSTRAKT ALGEBRA

(o‘quv qo‘llanma)

Toshkent – 2021

Ushbu o'quv qo'llanma "Matematika" bakalavr ta'lim yo'nalishi va magistratura mutaxassisligi talabalari uchun mo'ljallangan bo'lib, "Algebra va sonlar nazariyasi" fanining gruppalar va halqalar nazariyasiga doir boshlang'ich ma'lumotlar bilan bir qatorda "Abstrakt algebra" fanining barcha bo'limlariga doir mavzularni o'z ichiga oladi. Qo'llanmada har bir mavzudan keyin misollar ishlab ko'rsatilib, mustaqil ishlash uchun misol va masalalar berilgan. O'quv qo'llanma gruppalar, halqalar va maydonlar nazariyasini chuqur o'rganishni rejalashtirgan magistrant va tayanch doktorantlar uchun ham foydali hisoblanadi.

Mualliflar:

Ayupov Shavkat Abdullayevich
fizika-matematika fanlari doktori, professor, akademik

Omirov Baxrom Abdazovich
fizika-matematika fanlari doktori, professor

Xudoyberdiyev Abror Xakimovich
fizika-matematika fanlari doktori

Taqrizchilar:
fizika-matematika fanlari doktori, professor
Roziqov O'tkir Abdullayevich

fizika-matematika fanlari doktori, professor
Kudaybergenov Karimbergen Kadirbergenovich

MUNDARIJA

SO‘Z BOSHI

Ma‘lumki, algebra atamasi yurtdoshimiz, buyuk mutafakkir olim, matematik va astronom Muhammad ibn Muso al-Xorazmiy (783–850) tomonidan yozilgan “Al-jabr va al-muqobala” asari nomi bilan befosita bog‘liqdir. Muso al-Xorazmiyning asarlarida sonlar ustidagi arifmetik amallar keltirilgan bo‘lib, birinchi va ikkinchi darajali algebraik tenglamalarga keltiriladigan masalalarni yechishning umumiy usullari berilgan.

Keyinchalik nafaqat sonlar ustida, balki, ixtiyoriy to‘plam elementlari, obyektlar ustida amallar kiritilishi natijasida algebraning abstrakt tushunchasi hisoblangan algebraik sistema paydo bolgan. Algebraik sistemalarning dastlabkisi bu grruppalar hisoblanib, gruppalar nazariyasi abstrakt algebraning asosiy bo‘limlaridan biridir. Gruppalar berilgan to‘plamda bitta algebraik amal kiritish orqali aniqlanib, kommutativ bo‘lmagan gruppalar chekli to‘plamlar ustida o‘rin almashtirishlarni o‘rganish orqali vujudga kelgan. O‘rin almashtirishlar gruppasini, umuman gruppalar nazariyasini paydo bo‘lishida algebraik tenglamalarni yechish masalalarini o‘rganish alohida ahamiyat kasb etadi. Yuqorida ta’kidlaganimizdek, birinchi va ikkinchi darajali algebraik tenglamalarni yechishning umumiy usullari Muso al-Xorazmiyning asarlarida keltirilgan bo‘lsa, uchunchi va to‘rtinchi darajali algebraik tenglamalarni yechish usullari esa, XVI asrda yashab ijod qilgan italiyalik matematiklar J.Kardano (1501-1576) va L.Ferrarilar (1522-1565) tomonodan e‘lon qilingan ishlarda keltirilgan. Beshinchi va undan yuqori darajali tenglamalarning umumiy yechimini topish usullarini aniqlash masalasi juda ko‘p olimlarning qiziqishiga sabab bo‘lib, bu masalalar XIX asrga kelibgina o‘z yechimini topgan.

O‘rin almashtirishlar gruppasini algebraik tenglamalarni radikallarda yechish masalasini hal qilish uchun qo‘llagan fransiyalik matematik Lagranj XVIII asr oxirlarida gruppalar nazariyasida muhim ro‘l o‘ynaydigan qator natijalarni olgan bo‘lsa, XIX asr boshlarida norvegiyalik matematik Abel (1802–1829) tomonidan darajasi besh va undan yuqori bo‘lgan algebraik tenglamalarni umuman olganda radikallarda yechish mumkin emasligi isbotlangan. Evarist Galua (1811–1832) tomonidan aynan qanday tenglamalarni yechish mumkin va qandaylarini yechish mumkin emas degan masalaning o‘rganilishi esa nafaqat gruppalar, balki maydonlar nazariyasini rivojlantiruvchi yangi bir nazariyaning paydo bo‘lishiga olib keldi. Hozirgi kunda ushbu nazariya Galua nazariyasi deb yuritiladi.

Keyinchalik o‘rin almashtirishlar gruppasining Keli, Veber, Jordan va Silovlar tomonidan davom ettirilishi, gruppalarning abstrak ta’rifi kiritilib, ularning umumiy xossalarini o‘rganishga turtki bo‘lgan. Yuqorida aytilganidek, gruppalar va ularning xossalari, XVIII asr oxirlari va XIX asr boshlarida ko‘p o‘rganilgan bo‘lsada, gruppalarning abstrakt ta’rifi XX asr boshlariga kelibgina kiritilgan. Shundan so‘ng bu nazariyaning qator olimlar tomonidan jadal suratda o‘rganilishi halqalar va maydonlar nazariyasining ham rivojlanishiga olib keldi.

Halqalar bu gruppalardan farqli o‘laroq ikkita binar amal orqali aniqlanadigan obyekt hisoblanib, gruppalar nazariyasidagi ko‘plab tushuncha va tasdiqlar halqalar uchun ham davom ettiriladi. Halqa tushunchasi dastlab, D.Gilberdning (1862–1943) ishlarida keltirilgan bo‘lib, keyinchalik E.Artin, E.Nyotr, A. Frenkel kabi matematiklar tomonidan uning abstrakt ta’rifi kiritilgan. Maydonlarning kengaytmasi va gruppalarni bog‘lovchi Galua nazariyasining zamonaviy talqinda bayon qilinishida ham E.Artinning xizmatlari muhim rol o‘ynaydi.

Hozirgi kunga kelib, gruppalar, halqalar va maydonlar nazariyalari algebraning asosiy obyektlari hisoblanib, matematikaning geometriya, topologiya, funksiyalar nazariyasi kabi qator sohalarida qo‘llanilishi bilan birga fizik va mexanik masalalarni yechishda ham ishlatiladi. Zamonaviy algebrada esa, gruppa, halqa va maydon tushunchalaridan ham umumiyroq bo‘lgan algebraik sistemalar o‘rganilmoqda. Jumladan, yurtimiz matematiklari tomonidan assosiativ bo‘lmagan algebralarning bir qator muhum sinflari, ularning xossalarini o‘rganishga doir qator muammolar hal qilingan.

Ushbu o‘quv qo‘llanma “Matematika” ta’lim yo‘nalishi dastlabki kurslarida o‘qitiladigan asosiy fanlardan biri hisoblangan Algebra va sonlar nazariyasi kursining Algebra bo‘limida o‘tiladigan barcha mavzularni va magistrantlar uchun mo‘ljallangan “Abstrakt algebra” fanini to‘liq qamrab olgan. Qo‘llanmada ingliz va rus tillarida yozilgan qator zamonaviy adabiyotlardan foydalanilgan bo‘lib, ko‘plab mavzularning yoritilishida D.S.Malik, John N.Monderson, M.K.Sen “Fundamentals of Abstract algebra”, P.A. Grillet “Abstract Algebra”, T.W. Hungerford “Algebra” kitoblaridan hamda Moskva Davlat universiteti “Oliy algebra (Высшая алгебра)” kafedrasi materiallaridan keng foydalanilgan. Galua nazariyasiga doir mavzular esa M.M.Postnikovning rus tilida yozilgan “Galua nazariyasi (Теория Галуа)” kitobi asosida yozilgan. O‘quv qo‘llanma yuqori kurs talabalari, magistrantlar hamda gruppalar, halqalar va maydonlar nazariyasini chuqur o‘rganishni rejalashtirgan tayanch doktorantlar uchun ham foydali hisoblanadi.

BOB 1

Gruppalar nazariyasiga kirish

Sonlar to‘plami va ularda aniqlangan qo‘shish va ko‘paytirish amallari algebraik sistemalarga eng dastlabki misollar bo‘la oladi. Masalan, natural, butun, ratsional, haqiqiy va kompleks sonlar to‘plami qo‘shish va ko‘paytirish amallari bilan birgalikda algebraik sistema tashkil qiladi. Lekin barcha sonlar to‘plami ham ushbu amallarga nisbatan algebraik sistema bo‘lavermaydi, masalan manfiy sonlar to‘plami ko‘paytirish amaliga nisbatan algebraik sistema emas, chunki ikkita manfiy sonning ko‘paytmasi musbat son bo‘ladi. Shuningdek, irratsional sonlar to‘plami qo‘shish amaliga nisbatan algebraik sistema bo‘lmaydi, chunki ikkita irratsional sonning yig‘indisi ratsional son bo‘lib qolishi mumkin. Sonlar ustidagi qo‘shish va ko‘paytirish amallari binar amallar hisoblanib, gruppa tushunchasi ham biror to‘plamda aniqlangan binar amal yordamida kiritiladi. Umiman olganda algebraik amal deganda nafaqat binar amal, balki n-ar amallar ham tushuniladi.

1.1 Binar amal, yarimgruppa, monoid va gruppalar

Bizga bo‘sh bo‘lmagan A to‘plam berilgan bo‘lib, $A \times A$ uning dekart ko‘paytmasi bo‘lsin. $A \times A$ dekart ko‘paytmani A to‘plamga akslantiruvchi $* : A \times A \to A$ asklantirish **binar amal** deyilib, A to‘plamda binar amal aniqlangan deyiladi. $(A, *)$ juftlikka esa **algebraik sistema** yoki **gruppoid** deb ataladi. Odatda (a, b) elementning bu akslantirishdagi qiymati $a * b$, $a \cdot b$ yoki ab kabi belgilanadi.

1.1.1-misol.

- *Bizga biror A to‘plam berilgan bo‘lib, ushbu to‘plamdan olingan ixtiyoriy x va y elementlar uchun $x * y = x$ ko‘rinishda aniqlangan $*$ amali binar amal bo‘ladi.*

- $\mathbb{N}$ *natural sonlar to‘plamida quyidagi amallar binar amal bo‘ladi:*

$$+,\ \cdot,\ \max,\ \min,\ EKUB,\ EKUK,$$

ya'ni qo'shish, ko'paytirish, sonlarning maximumi, minimumi, eng katta umumiy bo'luvchisi va eng kichik umumiy karralisi.

- $\mathbb{Z}$ *butun sonlar to'plamida qo'shish* $(+)$ *va ko'paytirish* $(\cdot)$ *amallari binar amal bo'ladi.*

- $[a, b]$ *kesmada uzluksiz bo'lgan barcha funksiyalar fazosi* $C[a, b]$ *da ixtiyoriy* $f, g \in C[a, b]$ *funksiyalar uchun* $(f \circ g)(x) = f(g(x))$ *kabi aniqlangan amal binar amal bo'ladi.*

1.1.1-ta'rif. *Agar* $(S, *)$ *algebraik sistemada ixtiyoriy* $a, b, c \in S$ *elementlarlar uchun assosiativlik xossasi ya'ni*

$$(a * b) * c = a * (b * c)$$

tenglik o'rinli bo'lsa, u holda $(S, *)$ *algebraik sistemaga* ***yarim gruppa*** *deyiladi.*

1.1.2-misol.

- $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$ *algebraik sistemalar yarim gruppa bo'ladi.*

- A *to'plamda olingan ixtiyoriy* x, y *elementlar uchun* $*$ *amali* $x * y = x$ *ko'rinishda aniqlangan bo'lsa,* $(A, *)$ *algebraik sistema yarim gruppa bo'ladi.*

1.1.2-ta'rif. *Agar* $(M, *)$ *yarim gruppada shunday* $e \in M$ *element mavjud bo'lib, ixtiyoriy* $a \in M$ *element uchun*

$$e * a = a * e = a$$

tenglik bajarilsa, u holda $(M, *)$ *yarim gruppaga* ***monoid*** *deyiladi. Ushbu* e *elementga esa* ***birlik element*** *deb ataladi.*

1.1.3-misol.

- $(\mathbb{Z}, \cdot)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$ *algebraik sistemalar monoid tashkil qiladi.*

- $(M_n(\mathbb{R}), +)$ – *elementlari haqiqiy sonlardan iborat bo'lgan* n*-tartibli kvadrat matrisalar to'plami, matritsalarni qo'shish amaliga nisbatan monoid tashkil qiladi.*

- $(M_n(\mathbb{R}), \cdot)$ – *elementlari haqiqiy sonlardan iborat bo'lgan* n*-tartibli kvadrat matrisalar to'plami, matritsalarni ko'paytirish amaliga nisbatan monoid tashkil qiladi.*

Endi asosiy tushuncha hisoblangan gruppaning ta'rifini keltiramiz.

1.1.3-ta'rif. *Agar $(G, *)$ monoid berilgan bo'lib, ixtiyoriy $a \in G$ element uchun*

$$a^{-1} * a = a * a^{-1} = e$$

*tenglikni qanoatlantiruvchi $a^{-1} \in G$ element mavjud bo'lsa, u holda $(G, *)$ algebraik sistemaga **gruppa** deyiladi. a^{-1} element esa a elementning **teskari elementi** deyiladi.*

Demak, gruppa bu biror to'plamda aniqlangan algebraik amalga nisbatan assosiativlik xossasi o'rinli bo'ladigan, birlik elementi mavjud bo'lib, ixtiyoriy elementi teskarilanuvchi bo'ladigan algebraik sistema ekan.

Agar $(G, *)$ gruppaning ixtiyoriy $a, b \in G$ elementlari uchun

$$a * b = b * a$$

tenglik o'rinli bo'lsa, u holda $(G, *)$ gruppa **kommutativ gruppa** yoki **Abel gruppasi** deyiladi. Kommutativ bo'lmagan gruppaga **nokommutativ gruppa** deyiladi.

1.1.4-misol.

- $(\mathbb{Z}, +), (\mathbb{Q}, +),\ (\mathbb{R}, +), (\mathbb{C}, +)$ *algebraik sistemalar kommutativ gruppa bo'ladi.*
- $(\mathbb{Q} \setminus \{0\}, \cdot),\ (\mathbb{R} \setminus \{0\}, \cdot),\ (\mathbb{C} \setminus \{0\}, \cdot)$ *algebraik sistemalar kommutativ gruppa bo'ladi.*
- $(M_n(\mathbb{R}), +)$ *– elementlari haqiqiy sonlardan iborat bo'lgan n-tartibli kvadrat matrisalar to'plami, matritsalarni qo'shish amaliga nisbatan kommutativ gruppa tashkil qiladi.*
- $(GL_n(\mathbb{R}), \cdot)$ *– elementlari haqiqiy sonlardan iborat bo'lgan n-tartibli xosmas matrisalar to'plami, matritsalarni ko'paytirish amaliga nisbatan nokommutativ gruppa tashkil qiladi.*
- $(SL_n(\mathbb{R}), \cdot)$ *– elementlari haqiqiy sonlardan iborat bo'lgan determinanti 1 ga teng n-tartibli matrisalar to'plami, matritsalarni ko'paytirish amaliga nisbatan nokommutativ gruppa tashkil qiladi.*

Qiyudagi misolda X to'plamning barcha qism to'plamlaridan tuzilgan $P(X)$ sistemani qarab, bu sistemadagi birlashma, kesishma va simmetrik ayirma kabi amallar qanday algebraik sistema bo'lishini aniqlaymiz.

1.1.5-misol. *Bo'sh bo'lmagan X to'plamning barcha qism to'plamlaridan tuzilgan $P(X)$ sistema uchun quyidagilar o'rinli bo'ladi:*

- $P(X)$ *to'plam birlashma* $\cup$ *amaliga nisbatan monoid tashkil qiladi, lekin* $(P(X), \cup)$ *gruppa emas. Haqiqatdan ham, birlashma amali binar amal bo'lib, assosiativlik o'rinli bo'ladi. Birlik element vazifasini* $e = \emptyset$ *bajarsa, bo'sh to'plamdan farqli bo'lgan ixtiyoriy to'plam teskarilanuvchi emas. Shuning uchun* $(P(X), \cup)$ *monoid bo'lib, gruppa tashkil qilmaydi.*

- $P(X)$ *to'plam kesishma* $\cap$ *amaliga nisbatan monoid tashkil qiladi, lekin* $(P(X), \cap)$ *gruppa emas. Bu yerda ham aniqlangan amal binar amal bo'lishi va assosiativlikning bajarilishi ravshan. Birlik element vazifasini* $e = X$ *bajarsa,* X *dan farqli bo'lgan ixtiyoriy to'plam teskarilanuvchi emas.*

- $P(X)$ *to'plam simmetrik ayirma* $\triangle$ *amaliga nisbatan kommutativ gruppa tashkil qiladi. Chunki, simmetrik ayirmaga nisbatan birlik element* $e = \emptyset$ *bo'lib, ixtiyoriy* $A \in P(X)$ *elementning teskarisi o'ziga teng bo'ladi, ya'ni* $A^{-1} = A$.

Bizga sonlar nazariyasidan ma'lumki, ixtiyoriy n natural son uchun $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ chegirmalar sinfini hosil qilish mumkin, hamda bu chegirmalar sinfida qo'shish va ko'paytirish amallari aniqlanadi.

1.1.6-misol. $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ *chegirmalar sinfi uchun quyidagilar o'rinli:*

- $(\mathbb{Z}_n, +_n)$ *kommutativ gruppa tashkil qiladi.*

- $(\mathbb{Z}_n, \cdot_n)$ *modoid tashkil qiladi, lekin gruppa bo'lmaydi.*

1.1.7-misol. $(\mathbb{Z}_n, \cdot_n)$ *monoidning barcha teskarilanuvchi elementlari to'plami* $\mathbb{U}_n = \{\overline{a} \in \mathbb{Z}_n \setminus \{\overline{0}\} \mid (a, n) = 1\}$ *ko'rinishida bo'lib, bu to'plam ko'paytirish amaliga nisbatan gruppa tashkil qiladi. Ya'ni* $(\mathbb{U}_n, \cdot_n)$ *kommutativ gruppa.*

Endi gruppaning ba'zi sodda xossalarini o'z ichiga olgan qiyudagi tasdiqni keltiramiz.

1.1.1-tasdiq. *Ixtiyoriy* $(G, *)$ *gruppa uchun quyidagilar o'rinli:*

1) Gruppaning birlik elementi yagona.

2) Ixtiyoriy $a \in G$ *element uchun yagona teskari element mavjud.*

3) Ixtiyoriy $a \in G$ *element uchun* $(a^{-1})^{-1} = a$.

4) Ixtiyoriy $a, b \in G$ *elementlar uchun* $(a * b)^{-1} = b^{-1} * a^{-1}$.

Isbot. 1). Faraz qilaylik $(G, *)$ gruppada ikkita e_1 va e_2 birlik elementlar mavjud bo'lsin. U holda $e_1 * e_2$ ko'paytmani qarasak, e_1 element birlik element bo'lganligi uchun $e_1 * e_2 = e_2$. Ikkinchi tomondan esa, e_2 element birlik element bo'lganligi uchun $e_1 * e_2 = e_1$. Demak, $e_1 = e_2$.

2) Faraz qilaylik $a \in G$ element uchun ikkita teskari element mavjud bo‘lsin, ya’ni shunday $b, c \in G$ elementlar mavjud bo‘lib,

$$a * b = b * a = e, \quad a * c = c * a = e$$

bo‘lsin. Quyidagi tengliklardan b va c elementlarning tengligini hosil qilamiz:

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

Demak, a elementga teskari element yagona.

3) $a \in G$ elementning teskarisi a^{-1} bo‘lganligi uchun $a * a^{-1} = a^{-1} * a = e$. Faraz qilaylik $b \in G$ element a^{-1} ga teskari element bo‘lsin. U holda $b * a^{-1} = a^{-1} * b = e$. Bu tenkliklardan biz a va b elementlar a^{-1} ga teskari element ekanligini hosil qilamiz. 2)-xossaga ko‘ra ixtiyoriy elementning teskari elementi yagona bo‘lganligi uchun $b = a$ ekanligi kelib chiqadi. b element a^{-1} ning teskarisi ekanligidan $(a^{-1})^{-1} = a$ bo‘ladi.

4) Bizga $a, b \in G$ elementlarlar berilgan bo‘lib, a^{-1} va b^{-1} elementlar ularning teskari elementlari bo‘lsin, ya’ni

$$a * a^{-1} = a^{-1} * a = e, \quad b * b^{-1} = b^{-1} * b = e.$$

Quyidagi tengliklarni qaraymiz

$$(a * b) * (b^{-1} * a^{-1}) = (a * (b * b^{-1})) * a^{-1} = (a * e) * a^{-1} = a * a^{-1} = e.$$
$$(b^{-1} * a^{-1}) * (a * b) = (b^{-1} * (a^{-1} * a)) * b = (b^{-1} * e) * b = b^{-1} * b = e.$$

Ushbu tengliklardan $a * b$ elementning teskarisi $b^{-1} * a^{-1}$ ekanligi kelib chiqadi, ya’ni

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

□

Endi gruppaning tartibi va gruppa elementi tartibi tushunchalarini kiritamiz.

1.1.4-ta’rif. *Agar G gruppaning elementlari soni cheklita bo‘lsa, u holda G gruppa chekli gruppa deyiladi. Chekli gruppaning elementlari soni uning tartibi deyiladi va $|G|$ kabi belgilanadi. Elementlari cheksiz ko‘p bo‘lgan gruppalar cheksiz gruppalar deyiladi.*

Bizga $(G, *)$ gruppa va uning $a \in G$ elementi berilgan bo‘lsin. Ushbu elementning darajalarini quyidagicha aniqlaymiz:

$$a^0 = e,$$
$$a^n = a^{n-1} * a, \quad n > 1,$$
$$a^n = (a^{-1})^{-n}, \quad n < 0.$$

Ta’kidlash joizki, ixtiyoriy k, s butun sonlar uchun $a^k * a^s = a^{k+s}$ tenglik o‘rinli bo‘ladi. Agar qandaydir $k, s (k > s)$ butun sonlar uchun $a^k = a^s$, tenglik o‘rinli bo‘lsa, u holda $a^{k-s} = e$ munosabatga ega bo‘lamiz.

1.1.5-ta'rif. *G gruppaning $a \in G$ elementi uchun $a^n = e$ shartni qanoatlantiruvchi natural sonlarning eng kichigiga berilgan elementning tartibi deb ataladi. Agar $a^n = e$ shartni qanoatlantiruvchi natural son mavjud bo'lmasa, u holda bu elementning tartibi cheksizga teng deb ataladi. Berilgan $a \in G$ elementning tartibi $ord(a)$ kabi belgilanadi.*

1.1.8-misol. *$(\mathbb{Z}_6, +_6)$ gruppani qarasak, bu gruppaning tartibi 6 ga teng, ya'ni $|Z_6| = 6$, hamda*

$$ord(\overline{0}) = 1,\ ord(\overline{1}) = 6,\ ord(\overline{2}) = 3,\ ord(\overline{3}) = 2,\ ord(\overline{4}) = 3,\ ord(\overline{5}) = 6.$$

1.1.9-misol. *$M = \{1, i, -1, -i\}$ to'plam ko'paytitish amaliga nisbatan gruppa tashkil qilib,*

$$ord(1) = 1,\ ord(i) = 4,\ ord(-1) = 2,\ ord(-i) = 4.$$

Gruppada assosiativlik xossasi o'rinli bo'lganligi uchun, $a_1, a_2, \dots, a_n$ elementlarni ko'paytirishda qavslarning qo'yilishi ahamiyatli emas, shuning uchun odatda chapdan qo'yilgan qavslar ishlatilib, ko'paytma $(\dots((a_1 * a_2) * a_3 \dots) * a_n)$ kabi yoziladi.

Bundan tashqari gruppalar uchun qiyidagi xossalar xam o'rinli bo'lib, biz ularni isbotsiz keltirib o'tamiz.

1.1.2-tasdiq. *$(G, *)$ gruppadagi ixtiyoriy $a, b, c \in G$ elementlar uchun quyidagilar o'rinli:*

1) *$a * x = b$ tenglama yagona yechimga ega bo'lib, $x = a^{-1} * b$ bo'ladi.*

2) *$x * a = b$ tenglama yagona yechimga ega bo'lib, $x = b * a^{-1}$ bo'ladi.*

3) *$a * b = a * c$ yoki $b * a = c * a$ tenglikdan $b = c$ kelib chiqadi.*

4) *agar $a^2 = a$ bo'lsa, u holda $a = e$ bo'ladi.*

Ushbu teoremada gruppaning elementi tartibi bilan bo'g'liq bo'lgan asosiy xossalarni keltiramiz.

1.1.1-teorema. *Aytaylik G gruppaning $a \in G$ elementi uchun $ord(a) = n$ bo'lsin, u holda quyidagilar o'rinli:*

1) *Agar qandaydir m natural son uchun $a^m = e$ bo'lsa, u holda m soni n ga bo'linadi.*

2) *Ixtiyoriy t natural son uchun $ord(a^t) = \frac{n}{EKUB(t,n)}$.*

Isbot. 1) Aytaylik, $m = qn + r$ bo'lsin, bu yerda $0 \leq r < n$. U holda

$$a^r = a^{m-qn} = a^m * a^{-qn} = a^m * (a^n)^{-q} = e.$$

Berilgan elementning tartibi n ga teng bo'lganligi uchun n soni $a^n = e$ shartni qanoatlantiruvchi eng kichik natural son. $a^r = 0$ va $0 \leq r < n$ ekanligidan esa, $r = 0$ kelib chiqadi, ya'ni m soni n ga qoldiqsiz bo'linadi.

2) Aytaylik, $ord(a^t) = k$ bo'lsin, u holda $a^{tk} = (a^t)^k = e$. Demak, tk soni n ga bo'linadi, ya'ni $tk = nr$. Aytaylik $EKUB(t, n) = d$ bo'lsin, u holda $t = du, n = dv$, $EKUB(u, v) = 1$ bo'ladi. $tk = nr$ ekanligidan $duk = dvr$ tenglikka, bundan esa $uk = vr$ munosabatga ega bo'lamiz. Bu esa, uk soni v soniga bo'linishini anglatadi. Bundan esa, $EKUB(u, v) = 1$ ekanligini hisobga olsak, k soni $v = \frac{n}{d}$ soniga bo'linishi kelib chiqadi.

Endi $(a^t)^{\frac{n}{d}}$ elementni qaraymiz:

$$(a^t)^{\frac{n}{d}} = a^{\frac{nt}{d}} = a^{\frac{ndu}{d}} = a^{nu} = e.$$

Bu tenglikdan, $ord(a^t) = k$ ekanligini hisobga olgan holda, $\frac{n}{d}$ soni k ga bo'linishini keltirib chiqaramiz. Demak, $k = \frac{n}{d}$, ya'ni $ord(a^t) = \frac{n}{EKUB(t,n)}$. □

Yuqoridagi teoremaning isbotidan osongina ko'rish mumkinki, agar a elementning tartibi n ga teng bo'lsa, u holda

$$e, a, a^2, \dots a^{n-1}$$

elementlar turli bo'lib, ixtiyoriy m butun son uchun a^m element ulardan biriga teng bo'ladi.

1.1.10-misol. *$G = (-1; 1)$ intervaldan iborat bo'lgan to'plamning $a * b = \frac{a+b}{1+ab}$ amalga nisbatan gruppa tashkil qilishini isbotlang.*

Yechish. Dastlab ushbu amal haqiqatdan ham binar amal bo'lishini tekshiramiz, ya'ni $a, b \in G$ ekanligidan $a * b \in G$ kelib chiqishini ko'rsatamiz. Buning uchun $a^2 < 1$, $b^2 < 1$ ekanligidan foydalanib, quyidagiga ega bo'lamiz:

$$(1 - a^2)(1 - b^2) > 0,$$

$$1 - a^2 - b^2 + a^2b^2 > 0,$$

$$a^2 + b^2 < 1 + a^2b^2,$$

$$a^2 + 2ab + b^2 < 1 + 2ab + a^2b^2,$$

$$(a + b)^2 < (1 + ab)^2,$$

$$\left|\frac{a + b}{1 + ab}\right| < 1.$$

Demak, haqiqatdan ham $a*b \in G$ bo‘ladi. Endu ushbu amalning assosiativligini ko‘rsatamiz. Tekshirish qiyin emaski,

$$(a*b)*c = \frac{a+b}{1+ab}*c = \frac{\frac{a+b}{1+ab}+c}{1+\frac{a+b}{1+ab}c} = \frac{a+b+c+abc}{1+ab+ac+bc},$$

hamda

$$a*(b*c) = a*\frac{b+c}{1+bc} = \frac{a+\frac{b+c}{1+bc}}{1+a\frac{b+c}{1+bc}} = \frac{a+b+c+abc}{1+ab+ac+bc}.$$

Ya’ni assosiativlik xossasi o‘rinli. Ushbu algebraik sistemada birlik element vasifasini $e=0$ bajarib, ixtiyoriy $a \in G$ elementning teskarisi esa $-a$ bo‘ladi. Demak, $(G,*)$ gruppa bo‘ladi. □

1.1.11-misol. *Tartibi juft songa teng bo‘lgan gruppada $a^2 = e$ shartni qanoatlantiruvchi $a \neq e$ element mavjud ekanligini ko‘rsating.*

Yechish. Bizga G gruppa beringan bo‘lib, $|G| = 2n$ bo‘lsin. Ma’lumki, agar qandaydir $a \in G$ element uchun $a^{-1} = a$ bo‘lsa, u holda $a^2 = e$ bo‘ladi.

$A = \{g \in G \mid g^{-1} \neq g\}$ to‘plamni qaraymiz. Ma’lumki, $e \notin A$ bo‘lib, A to‘plamda yotuvchi biror elementning teskarisi ham shu to‘plamda yotadi. Demak, A to‘plamning elementlari soni juft son bo‘lib, $A \neq G$. Bundan esa, A to‘plamda yotmaydigan birlik elementdan farqli, $a \in G$ element mavjudligi kelib chiqadi, ya’ni $a \neq e, a^{-1} = a$. Demak, $a^2 = e$. □

1.1.1 Mustaqil ishlash uchun misol va masalalar

1. Quyidagi to‘plamlar keltirilgan amallarga nisbatan gruppa bo‘ladimi?

   - $(n\mathbb{Z},+)$ – natural n soniga karrali butun sonlar to‘plami qo‘shish amaliga nisbatan;
   - $(\{2n+1 \mid n \in \mathbb{Z}\},+)$ – barcha toq butun sonlar to‘plami qo‘shish amaliga nisbatan;
   - $(\mathbb{R}_+,\cdot)$ – musbat haqiqiy sonlar to‘plami ko‘paytirish amaliga nisbatan;
   - $(\{z \in \mathbb{C} \mid z^n = 1\},\cdot)$ – birning n-darajali barcha kompleks ildizlari to‘plami ko‘paytirish amaliga nisbatan;
   - $(\mathbb{R},*)$ – haqiqiy sonlar to‘plami, $a*b = a$ kabi aniqlangan amalga nisbatan;
   - $(\mathbb{R},*)$ – haqiqiy sonlar to‘plami, $a*b = \frac{a+b}{2}$ kabi aniqlangan amalga nisbatan;
   - $(\mathbb{R},*)$ – haqiqiy sonlar to‘plami, $a*b = a^b$ kabi aniqlangan amalga nisbatan;

- $(M \times M, *)$ to'plam, $(x, y) * (z, t) = (x, t)$ kabi aniqlangan amalga nisbatan, bu yerda M qandaydir to'plam va $M \times M$ – dekart ko'paytma;

2. $G = \mathbb{R} \setminus \{1\}$ to'plamni $a * b = a + b - ab$ amalga nisbatan gruppa tashkil qilishini isbotlang.

3. $G = \mathbb{R} \setminus \{-1\}$ to'plamni $a * b = a + b + ab$ amalga nisbatan gruppa tashkil qilishini isbotlang.

4. $G = \{(a, b) |\ a, b \in R, b \neq 0\}$ to'plamdan olingan ixtiyoriy $(a, b), (c, d) \in G$ elementlar o'rtasida $*$ binar amal $(a, b) * (c, d) = (a + bc, bd)$ ko'rinishida aniqlansa, u holda $(G, *)$ nokommutativ gruppa bo'lishini isbotlang.

5. Quyidagi matritsalar to'plaminining qaysilari matritsalarni qo'shish amaliga nisbatan gruppa bo'lishini aniqlang.

   - $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$
   - $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in 2\mathbb{Z} \right\}$
   - $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$
   - $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$

6. Quyidagi matritsalar to'plaminining qaysilari matritsalarni ko'paytirish amaliga nisbatan gruppa bo'lishini aniqlang.

   - $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2 + b^2 \neq 0,\ a, b \in \mathbb{R} \right\}$
   - $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1,\ a, b, c, d \in \mathbb{R} \right\}$
   - $G = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$
   - $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$

7. Quyidagi matritsalar to‘plami ko‘rsatilgan amallarga nisbatan gruppa bo‘ladimi?
    - Simmetrik matritsalar to‘plami qo‘shish amaliga nisbatan.
    - Simmetrik matritsalar to‘plami ko‘paytirish amaliga nisbatan.
    - Xosmas matritsalar to‘plami qo‘shish amaliga nisbatan.
    - Xosmas matritsalar to‘plami ko‘paytirish amaliga nisbatan.
    - Dioganal ko‘rinishidagi matritsalar to‘plami qo‘shish amaliga nisbatan.
    - Dioganal ko‘rinishidagi matritsalar to‘plami ko‘paytirish amaliga nisbatan.
    - Yuqori uchburchak ko‘rinishidagi matritsalar to‘plami qo‘shish amaliga nisbatan.
    - Yuqori uchburchak ko‘rinishidagi matritsalar to‘plami ko‘paytirish amaliga nisbatan.
    - Yuqori uchburchak ko‘rinishidagi xosmas matritsalar to‘plami ko‘paytirish amaliga nisbatan.
    - Barcha ortogonal ($A^TA = AA^T = E$ shartni qanoatlantiruvchi) matritsalar to‘plami ko‘paytirish amaliga nisbatan.
8. Biror X to‘plamni o‘zini o‘ziga o‘tkazuvchi barcha akslantirishlar to‘plami, superpozitsiya amaliga nisbatan yarim gruppa tashkil qilib, gruppa bo‘lmasligini isbotlang.
9. $y = \frac{ax+b}{cx+d}$, $a, b, c, d \in \mathbb{R}$, $ad - bc \neq 0$ ko‘rinishidagi funksiyalar to‘plami superpozitsiya amaliga gruppa tashkil qilishini isbotlang.
10. $\mathbb{U}_6, \mathbb{U}_7, \mathbb{U}_9, \mathbb{U}_{12}, \mathbb{U}_{24}$ gruppalarning elementlarini ko‘rsating.
11. $(\mathbb{Z}_{12}, +)$ gruppa elementlarining tartiblarini aniqlang.
12. $(\mathbb{U}_9, \cdot)$ gruppa elementlarining tartiblarini aniqlang.
13. $(GL_2(\mathbb{R}), \cdot)$ gruppaning tartibi 2 ga teng bo‘lgan barcha elementlarini toping.
14. Agar $(G, *)$ gruppaning ixtiyoriy $a \in G$ elementi uchun $a^2 = e$ tenglik o‘rinli bo‘lsa, u holda $(G, *)$ gruppa kommutativ ekanligini isbotlang.
15. Agar $(G, *)$ gruppaning ixtiyoriy $a, b \in G$ elementlari uchun $(a * b)^2 = a^2 * b^2$ tenglik o‘rinli bo‘lsa, u holda $(G, *)$ gruppa kommutativ ekanligini isbotlang.
16. $(G, *)$ gruppa kommutativ bo‘lishi uchun, ixtiyoriy $a, b \in G$ elementlar uchun $(a*b)^{-1} = a^{-1}*b^{-1}$ tenglik o‘rinli bo‘lishi zarur va yetarli ekanligini isbotlang.

17. Agar $(G,*)$ gruppaning $a,b\in G$ elementlari uchun $a^4=e$ va $a^2*b=b*a$ bo‘lsa, u holda $a=e$ ekanligini ko‘rsating.

18. Agar $(G,*)$ gruppaning $a,b\in G$ elementlari uchun $a*b=b*a^{-1}$ va $b*a=a*b^{-1}$ bo‘lsa, u holda $a^4=b^4=e$ ekanligini isbotlang.

19. Agar $(G,*)$ gruppaning $a,b\in G$ elementlari uchun $a^2=e$ va $a*b^4*a=b^7$ bo‘lsa, u holda $b^{33}=e$ ekanligini ko‘rsating.

20. Agar $(G,*)$ gruppaning $a,b\in G$ elementlari uchun $a^{-1}*b^2*a=b^3$ va $b^{-1}*a^2*b=a^3$ bo‘lsa, u holda $a=b=e$ ekanligini ko‘rsating.

21. $(G,*)$ gruppaning ixtiyoriy $a,b\in G$ elementlari uchun quyidagilarni isbotlang:

    - $ord(a)=ord(a^{-1})$;
    - $ord(a)=ord(b*a*b^{-1})$;
    - $ord(a*b)=ord(b*a)$.

22. Agar $(G,*)$ gruppaning $a,b\in G$ elementlari uchun $a*b=b^5*a^3$ munosabat o‘rinli bo‘lsa, u holda $ord(b*a^{-1})=ord(b^5*a)=ord(b^3*a^3)$ ekanligini isbotlang.

23. Agar $(G,*)$ gruppaning $a,b\in G$ elementlari uchun $ord(a)=n$, $ord(b)=m$, $(n,m)=1$ va $a*b=b*a$ munosabatlar o‘rinli bo‘lsa, u holda $ord(a*b)=nm$ ekanligini isbotlang.

1.2 O‘rin almashtirishlar gruppasi

Endi chekli nokommutativ gruppa bo‘lgan o‘rin almashtirishlar gruppasini aniqlaymiz. O‘rin almashtirishlar gruppasi bu bo‘sh bo‘lmagan chekli to‘plamni o‘zini o‘ziga o‘tkazuvchi barcha biyektiv akslantirishlar to‘plamining superpozitsiya amaliga nisbatan gruppa hisoblanadi. Ushbu gruppa muhim gruppalardan bo‘lib, to‘plamning quvvati 2 dan katta bo‘lganda u nokommutativ gruppa bo‘ladi.

Demak, X bo‘sh bo‘lmagan to‘plamda aniqlangan $\pi : X\to X$ biyektiv akslantirishga X to‘plamning **o‘rin almashtirishi** deb ataladi. X to‘plamning barcha o‘rin almashtirishlaridan iborat bo‘lgan to‘plamni $S(X)$ kabi belgilaymiz. Yuqorida ta’kidlaganimizdek, $S(X)$ to‘plam superpozitsiyasi (kompizitsiya) amaliga nisbatan gruppa tashkil qiladi, ya’ni $f,g\in S(X)$ o‘rin almashtirishlarning ko‘paytmasi sifatida ularning $f\circ g$ superpozitsiyasi qaraymiz.

Ushbu amal uchun assosiativlik o‘rinli bo‘lib, birlik element vazifasini ayniy akslantirish, teskari element vazifasini esa teskari akslantirish bajaradi. Ushbu $(S(X),\circ)$ gruppaga **o‘rin almashtirishlar** gruppasi deb ataladi.

Agar X to'plam chekli to'plam bo'lib, uning elementlari soni n ta, ya'ni $|X| = n$ bo'lsa, u holda $(S(X), \circ)$ gruppani S_n kabi belgilanadi. S_n o'rin almashtirishlar gruppasining elementlarini qulayroq ko'rinishda yozish uchun quyidagi belgilashlarni kiritib olamiz. $|X| = n$ bo'lganligi uchun X to'plam o'rniga $I_n = \{1, 2, \ldots, n\}$ to'plamni qarab $\pi : I_n \to I_n$ biyektiv akslantirishni

$$\pi = \{(1, \pi(1)), (2, \pi(2)), \ldots, (n, \pi(n))\}$$

yoki

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix} \tag{1.1}$$

ko'rinishda yozib olsih mumkin. Demak, S_n gruppaning elementlarini (1.1) ko'rinishda yozish mumkin.

Masalan, I_4 da aniqlangan $\pi \in S_4$ biyektiv akslantirishni $\pi(1) = 2, \pi(2) = 4, \pi(3) = 3$ va $\pi(4) = 1$ ko'rinishda aniqlasak, bu elementni quyidagicha yozish mumkin:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

S_n gruppadagi $\pi, \varphi \in S_n$ o'rin almashtirishlar o'rtasidagi ko'paytma ularning superpozitsiyasi kabi aniqlanganligi uchun

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix} \quad \text{va} \quad \varphi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \varphi(1) & \varphi(2) & \varphi(3) & \ldots & \varphi(n) \end{pmatrix}$$

o'rin almashtirishlarning ko'paytmasi

$$\pi \circ \varphi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(\varphi(1)) & \pi(\varphi(2)) & \pi(\varphi(3)) & \ldots & \pi(\varphi(n)) \end{pmatrix}$$

kabi bo'ladi.

Masalan, $\pi_1, \pi_2 \in S_4$ o'rin almashtirishlar uchun,

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

bo'lsa, u holda

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

bo'ladi.

Takidlash joizki, S_n gruppa birlik elementining ko'rinishi

$$e = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

kabi bo'lsa,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

elementning teskarisi esa

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi^{-1}(1) & \pi^{-1}(2) & \pi^{-1}(3) & \dots & \pi^{-1}(n) \end{pmatrix}$$

koʻrinishida boʻladi.

Masalan, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ oʻrin almashtirish uchun $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ boʻladi.

1.2.1-tasdiq. *S_n ($n \geq 3$) gruppa nokommutativ (kommutativ emas) va $|S_n| = n!$.*

Isbot. Dastlab, ushbu gruppaning nokommutativ ekanligini koʻrsatamiz. Buning uchun quyidagi $\pi_1, \pi_2 \in S_n$ elementlarni qaraymiz

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix}.$$

U holda

$$\pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}$$

va

$$\pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 1 & 2 & 4 & \dots & n \end{pmatrix}.$$

Demak, $\pi_1 \circ \pi_2 \neq \pi_2 \circ \pi_1$, ya'ni S_n gruppa kommutativ emas.

Endi $|S_n| = n!$ ekanligini ko'rsatamiz. Bu gruppaning elementlari umumiy koʻrinishi

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

boʻlib, $\pi(1) \in \{1, 2, \dots, n\}$, ya'ni $\pi(1)$ ning qiymati n ta sondan birini qabul qilishi mumkin. $\pi(2) \in \{1, 2, \dots, n\} \setminus \{\pi(1)\}$ bo'lganligi uchun $\pi(2)$ ning qiymati $n-1$ ta sondan birini va hokazo $\pi(n) \in \{1, 2, \dots, n\} \setminus \{\pi(1), \pi(2), \dots, \pi(n-1)\}$ ekanligidan $\pi(n)$ ning qiymati faqat bitta sonni tanlab olishi mumkinligi kelib chiqadi. Natijada, π oʻrin almashtirishni hosil qilish mumkin boʻlgan barcha imkoniyatlari $1 \cdot 2 \cdot 3 \cdot \dots \cdot n = n!$ soniga teng, ya'ni $|S_n| = n!$. □

Endi sikl koʻrinishidagi va transpozitsiya deb nomlanuvchi oʻrin almashtirishlarni keltiramiz.

1.2.1-ta'rif. *$\pi \in S_n$ oʻrin almashtirish*

$$\pi = \begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k \\ i_2 & i_3 & \dots & i_k & i_1 \end{pmatrix}$$

ko‘rinishda aniqlangan bo‘lsa, ya’ni $\pi(i_1) = i_2, \pi(i_2) = i_3, \ldots, \pi(i_{k-1}) = i_k, \pi(i_k) = i_1$ *bo‘lib,* $a \in I_n \setminus \{i_1, i_2, \ldots, i_k\}$ *elementlar uchun* $\pi(a) = a$ *bo‘lsa, u holda bu o‘rin almashtirishga* ***uzunligi*** k ***ga teng bo‘lgan sikl*** *yoki* k***-sikl*** *deb ataladi va* $(i_1, i_2, \ldots, i_k)$ *ko‘rinishida yoziladi. Uzunligi 2 ga teng bo‘lgan sikl esa* ***traspozitsiya*** *deyiladi.*

Ta’kidlash joizki, uzunligi k ga teng bo‘lgan $\pi = (i_1, i_2, \ldots, i_{k-1}, i_k)$ siklni k xil usulda yozish mumkin, ya’ni quyidagi tengliklar o‘rinli

$$\pi = (i_1, i_2, \ldots, i_{k-1}, i_k) = (i_2, i_3, \ldots, i_k, i_1) = \cdots = (i_k, i_1, \ldots, i_{k-2}, i_{k-1}).$$

Sikl ko‘rinishidagi o‘rin almashtirishlarni sonlarning orasiga vergul qo‘ymasdan $(i_1 i_2 \ldots i_k)$ kabi yozish ham qabul qilingan. Masalan, $(S_3, \circ)$ gruppaning barcha elementlari

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

bo‘lib, ular sikl ko‘rinishida mos ravishda quyidagicha yoziladi

$$e,\ (12),\ (13),\ (23),\ (123),\ (132).$$

1.2.2-ta’rif. *Bizga* $\pi_1, \pi_2 \in S_n$ *o‘rin almashtirishlar berilgan bo‘lsin. Agar* $\pi_1(k) \neq k$ *shartni qanoatlantiruvchi barcha* k *lar uchun* $\pi_2(k) = k$ *bo‘lib, va aksincha* $\pi_2(i) \neq i$ *lar uchun* $\pi_1(i) = i$ *bo‘lsa, u holda* π_1 *va* π_2 *o‘rin almashtirishlar* ***kesishmaydigan*** *o‘rin almashtirishlar deyiladi.*

Masalan,

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \quad \text{va} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

o‘rin almashtirishlar kesishmaydigan o‘rin almashtirishlar bo‘lib, ularning sikl ko‘rinishidagi ifodalari esa $\pi_1 = (123)$ va $\pi_2 = (45)$ bo‘ladi.

Tekshirish qiyin emaski, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ o‘rin almashtirish uchun $\pi = \pi_1 \circ \pi_2 = \pi_2 \circ \pi_1$ tenglik o‘rinli bo‘ladi. Bu esa, π o‘rin almashtirishni kesishmaydigan π_1 va π_2 sikllarning ko‘paytmasi shaklida ifodalanishini bildiradi. Bundan tashqari, o‘zaro kesishmaydigan o‘rin almashtirishlar uchun kommutativlik xossasi o‘rinli bo‘lib, bir nechta o‘zaro kesishmaydigan o‘rin almashtirishlarni ko‘paytirganda ham ularning joylashish tartibi ahamiyatga ega emas.

Quyidagi teoremada birlik elementdan farqli bo‘lgan ixtiyoriy o‘rin almashtirishni kesishmaydigan sikllar ko‘paytmasi ko‘rinishida yozish mumkinligi ko‘rsatiladi.

1.2.1-teorema. *Birlik elementdan farqli ixtiyoriy $\pi \in S_n$ $(n \geq 2)$ o‘rin almashtirish uzunligi kamida 2 ga teng bo‘lgan, o‘zaro kesishmaydigan sikllar ko‘paytmasi ko‘rinishida (sikllarning joylashish tartibini hisobga olmagan holda) yagona tarzda ifodalanadi.*

Isbot. Teoremani isbotlash uchun induksiya usulidan foydalanamiz. Agar $n = 2$ bo‘lsa, u holda $S_2 = \{e, (12)\}$ bo‘lib, $\pi \neq e$ uchun $\pi = (12)$ ekanligidan teorema o‘rinli bo‘lishi kelib chiqadi. Teoremani barcha S_k, $2 \leq k < n$ gruppalar uchun o‘rinli bo‘lsin deb faraz qilib, uni S_n uchun isbotlaymiz. Ixtiyoriy $\pi \in S_n$, $\pi \neq e$ element uchun $\{\pi(1), \pi^2(1), \pi^3(1), \ldots, \pi^s(1), \ldots\} \subseteq I_n$ to‘plamni qaraymiz. I_n to‘plam chekli bo‘lganligi uchun, $\pi^l(1) = \pi^m(1)$ tenglikni qanoatlantiradigan l va m natural sonlari mavjud. U holda $p = |l - m|$ uchun $\pi^p(1) = 1$. Demak, $\pi^p(1) = 1$ tenglikni qanoatlantiruvchi p natural soni mavjud. Bunday sonlarning eng kichigini i deb belgilaymiz, ya’ni $i = \min\limits_p\{p \in \mathbb{N} | \ \pi^p(1) = 1\}$. U holda quyidagi

$$A = \{1, \pi(1), \pi^2(1), \ldots, \pi^{i-1}(1)\}.$$

to‘plamning barcha elementlari turli bo‘lib, quyidagi $\tau \in S_n$ o‘rin almashtirishni aniqlash mumkin

$$\tau = (1, \pi(1), \pi^2(1), \ldots, \pi^{i-1}(1)).$$

Ya’ni biz uzunligi i ga teng bo‘lgan siklni aniqladik.

Endi $B = I_n \setminus A$ to‘plamni qaraymiz. Agar $B = \emptyset$ bo‘lsa, u holda $i = n$ bo‘lib, $\pi = \tau$, ya’ni π o‘rin almashtirish sikldan iborat bo‘ladi. Agar $B \neq \emptyset$ bo‘lsa, u holda $\sigma = \pi|_B$ o‘rin almashtirishni, ya’ni σ sifatida π o‘rin almashtirishni B to‘plamda aniqlangan qismini qaraymiz.

Agar $\sigma = \pi|_B$ o‘rin almashtirish $S(B)$ da birlik element bo‘lsa, u holda $\pi = \tau$, ya’ni

$$\pi = (1, \pi(1), \pi^2(1), \ldots \ \pi^{i-1}(1))$$

bo‘lib, π o‘rin almashtirish uzunligi i ga teng bo‘lgan sikldan iborat bo‘ladi. Agar σ o‘rin almashtirish $S(B)$ da birlik element bo‘lmasa, $|B| < n$ ekanligidan induksiya faraziga ko‘ra, σ o‘rin almashtirishni B to‘plamda o‘zaro kesishmaydigan sikllarning ko‘paytmasi ko‘rinishida yozish mumkin, ya’ni $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r$.

Endi, $1 \leq i \leq r$ soni uchun, π_i o‘rin almashtirishni quyidagicha aniqlaymiz:

$$\pi_i(a) = \begin{cases} \sigma_i(a), & \text{agar } a \in B, \\ a, & \text{agar } a \notin B. \end{cases}$$

U holda, $\pi_1, \pi_2, \ldots, \pi_r$ va τ o‘rin almashtirishlar S_n to‘plamda o‘zaro kesishmaydigan sikllar bo‘lib, $\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_r \circ \tau$ tenglik o‘rinli bo‘ladi, ya’ni π o‘rin almashtirish o‘zaro kesishmaydigan sikllar ko‘paytmasi ko‘rinishida ifodalanadi.

Demak, ixtiyoriy o'rin almashtirishni o'zaro kesishmaydigan sikllar ko'paytmasi ko'rinishida ifodalash mumkinligi ko'rsatildi. Endi, bunday yoyilma sikllarning joylashish tartibini hisobga olmagan holda yagona ekanligini ko'rsatamiz. Teskarisini faraz qilaylik, ya'ni π o'rin almashtirish r va s ta o'zaro kesishmaydigan sikllarning ko'paytmasi ko'rinishida ifodalansin. U holda

$$\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_r = \mu_1 \circ \mu_2 \circ \cdots \circ \mu_s.$$

Ixtiyoriy $\pi_i, 1 \leq i \leq r$ siklni qaraylik. Aytaylik, $\pi_i = (i_1\ i_2\ \dots\ i_l)$ bo'lsin, u holda $\pi(i_1) \neq i_1$ bo'lganligi uchun, i_1 soni qaysidir μ_j siklda ham qatnashadi. Sikllar o'zaro kesishmasligini hisobga olsak, bunday μ_j siklning yagona ekanligiga ega bo'lamiz. Ushbu μ_j siklni esa $\mu_j = (i_1\ c_2\ \dots\ c_m)$ ko'rinishida yozib olish mumkin. U holda

$$\begin{gathered}
i_2 = \pi_i(i_1) = \pi(i_1) = \mu_j(i_1) = c_2, \\
i_3 = \pi_i(i_2) = \pi(i_2) = \pi(c_2) = \mu_j(c_2) = c_3, \\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
i_l = \pi_i(i_{l-1}) = \pi(i_{l-1}) = \pi(c_{l-1}) = \mu_j(c_{l-1}) = c_l
\end{gathered}$$

tengliklardan $l = m$, hamda $\pi_i = \mu_j$ ekanligini hosil qilamiz. Demak, ixtiyoriy π_i sikl uchun shunday μ_j sikl topilib, $\pi_i = \mu_j$ tenglik bajarilar ekan.

Ushbu mulohazani ixtiyoriy μ_k sikl uchun yuritib, unga mos $\mu_k = \pi_t$ shartni qanoatlantiruvchi π_t siklning mavjudligini keltirib chiqazish mumkin. Demak, ixtiyoriy π_i sikl uchun $\pi_i = \mu_j$ shartni qanoatlantiruvchi yagona μ_j sikl topiladi. □

Yuqoridagi teoremadan qiyidagi natijaga ega bo'lamiz.

1.2.1-natija. $(S_n, \circ)$, $n \geq 2$ *gruppadagi ixtiyoriy* π *o'rin almashtirishni transpositsiyalar ko'paytmasi ko'rinishida ifodalash mumkin.*

Isbot. 1.2.1-teoremaga ko'ra ixtiyoriy o'rin almashtirish sikllar ko'paytmasi ko'rinishisa yoziladi. Demak, natijani isbotlash uchun uzunligi k ga teng bo'lgan ixtiyoriy siklni transpositsiyalar ko'paytmasi ko'rinishida yozish mumkinligini isbotlash yetarli. $k = 1$ bo'lsa, u holda $(i) = e$ bo'lib, $e = (1) = (1\ 2) \circ (1\ 2)$ bo'ladi. Agar $k \geq 2$ bo'lsa, u holda

$$(i_1\ i_2\ \dots\ i_k) = (i_1\ i_k) \circ (i_1\ i_{k-1}) \circ \cdots \circ (i_1, i_2),$$

tenglikdan ixtiyoriy siklni transpositsiyalar ko'paytmasi ko'rinishida yozish mumkinligi kelib chiqadi. □

1.2.1-natijada biz ixtiyoriy o'rin almashtirishni transpositsiyalar ko'paytmasi ko'rinishida ifodalash mumkin ekanligini isbotladik. Ammo, o'rin almashtirishning bunday ifodasi yagona emas. Masalan, $(1\ 2\ 3)$ siklni $(1\ 2\ 3) = (1\ 3) \circ (1\ 2) =$

(2 1) $\circ$ (2 3) ifodalaridan tashqari (1 2 3) = (1 2) $\circ$ (1 3) $\circ$ (2 3) $\circ$ (1 2) kabi bir nechta usullar orqali ifodalash mumkin. Ya’ni bu yoyilmalarda transpositsiyalar farq qilishi bilan birga ularning soni ham turli bo‘lishi mumkin.

Quyida biz biror o‘rin almashtirishni turli xil ko‘rinishda transpositsiyalar ko‘paytmalari shaklida ifodalangan bo‘lsa, bunda barcha ifodalardagi transpositsiyalar soni yoki juft yoki toq bo‘lishini ko‘rsatamiz.

Buning uchun dastlab qiyidagi belgilash va tushunchalarni kiritib olamiz. Bizga $a_1, a_2, \ldots, a_n$ sonlari berilgan bo‘lsin. χ orqali quyidagi ko‘paytmani belgilaymiz

$$\chi = \prod_{1\leq i<j\leq n} (a_i - a_j).$$

Ixtiyoriy π o‘rin almashtirish uchun

$$\pi(\chi) = \prod_{1\leq i<j\leq n} (a_{\pi(i)} - a_{\pi(j)})$$

bo‘lsin.

1.2.3-ta’rif. *Agar $\pi \in S_n$ o‘rin almashtirish uchun $\pi(\chi) = \chi$ bo‘lsa, u holda π o‘rin almashtirishga **juft o‘rin almashtirish**, agar $\pi(\chi) = -\chi$ bo‘lsa **toq o‘rin almashtirish** deyiladi.*

Quyidagi lemmada ixtiyoriy transpozitsiyaning toq o‘rin almashtirish ekanligini ko‘rsatamiz.

1.2.1-lemma. *Ixtiyoriy $\sigma \in S_n$ $(n \geq 2)$ transpozitsiya uchun $\sigma(\chi) = -\chi$ bo‘ladi.*

Isbot. Aytaylik, $\sigma = (i\ j), i < j$ bo‘lsin. U holda χ ifodada ishtirok etuvchi $a_i - a_j$ ko‘paytuvchi $\sigma(\chi)$ ifodada $a_{\sigma(i)} - a_{\sigma(j)} = a_j - a_i = -(a_i - a_j)$ kabi qatnashadi.

Endi $a_k - a_l (k < l)$ ifodani qaraymiz. Bunda k va l lardan ko‘pi bilan bittasi i yoki j ga teng bo‘lishi mumkin. Quyidagi hollarni qaraymiz:

1. $k, l \notin \{i, j\}$ bo‘lsin, ya’ni k va l larning har ikkalasi i va j dan farq qilsin, u holda $a_{\sigma(k)} - a_{\sigma(l)} = a_k - a_l$ bo‘lib, ushbu $a_k - a_l$ ko‘paytuvchi χ va $\sigma(\chi)$ larning ifodasida o‘z ishorasini o‘zgartirmaydi.

2. $l = i$ bo‘lsin, u holda $k < i$ bo‘lib, χ ko‘paytmada $a_k - a_i$ va $a_k - a_j$ ko‘paytuvchilar ishtirok etadi. Ushbu ko‘paytuvchilar $\sigma(\chi)$ ifodada esa

$$(a_{\sigma(k)} - a_{\sigma(i)})(a_{\sigma(k)} - a_{\sigma(j)}) = (a_k - a_j)(a_k - a_i)$$

kabi bo‘lib, $(a_k - a_i)(a_k - a_j)$ ko‘paytmaning ishorasi o‘zgarmaydi.

3. $l = j$ bo‘lsin. Agar $k < i$ bo‘lsa, biz yana $(a_k - a_i)(a_k - a_j)$ ko‘rinishidagi ko‘paytmaga ega bo‘lib, yuqorida qaralgan holni hosil qilamiz.

   Agar $i < k < j$ bo‘lsa, u holda χ ifodada $(a_i - a_k)(a_k - a_j)$ ko‘rinishidagi ko‘paytma qatnashib, $\sigma(\chi)$ da esa

$$(a_{\sigma(i)} - a_{\sigma(k)})(a_{\sigma(k)} - a_{\sigma(j)}) = (a_j - a_k)(a_k - a_i) = (a_i - a_k)(a_k - a_j)$$

   bo‘ladi. Demak, bu holda ham $(a_i - a_k)(a_k - a_j)$ ko‘paytma o‘z ishorasini o‘zgartirmaydi.

4. $k = j$ bo‘lsin, u holda $l > j$ bo‘lib, χ ifodada $(a_j - a_l)(a_i - a_l)$ ko‘rinishidagi ko‘paytma qatnashadi. Ushbu ko‘paytmaning $\sigma(\chi)$ dagi ifodasi esa, quyidagicha bo’ladi

$$(a_{\sigma(j)} - a_{\sigma(l)})(a_{\sigma(i)} - a_{\sigma(l)}) = (a_i - a_l)(a_j - a_l).$$

   Ya’ni ushbu holda ham $(a_j - a_l)(a_i - a_l)$ ko‘paytmaning ishorasi o‘zgarmaydi.

5. $k = i$ bo‘lgan hol esa, $i < l < j$ bo‘lganda 3-holga, $j < l$ bo‘lganda esa 4-holga keltiriladi.

Demak, $a_i - a_j$ ko‘paytuvchidan boshqa barcha ko‘paytuvchilar yoki o‘z ishorasini o‘zgartirmaydi yoki ishorasini saqlovchi juftiga ega. Bundan $\sigma(\chi) = -\chi$ ekanligi kelib chiqadi. $\square$

Yuqoridagi lemmadan π o‘rin almashtirish turli usulda transpozitsiyalar ko‘paytmasi ko‘rinishda yozilgan bo‘lsa, ya’ni

$$\pi = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_s,$$

u holda $|r - s|$ soni doim juft son bo‘lishi kelib chiqadi. Ya’ni r va s sonlari bir vaqtda yoki juft yoki toq bo‘ladi. Haqiqatdan ham, σ_i va τ_j transpozitsiyalar uchun $\sigma_i(\chi) = -\chi$ va $\tau_j(\chi) = -\chi$ ekanligini hisobga olsak,

$$\pi(\chi) = (\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r)(\chi) = \sigma_1(\sigma_2(\ldots \sigma_r(\chi))) = (-1)^r \chi,$$

$$\pi(\chi) = (\tau_1 \circ \tau_2 \circ \cdots \circ \tau_s)(\chi) = \tau_1(\tau_2(\ldots \tau_s(\chi))) = (-1)^s \chi$$

tengliklarga ega bo‘lamiz. Bundan esa r va s sonlari bir vaqtda yoki juft yoki toq bo‘lishi kelib chiqadi.

Demak, $\pi \in S_n$ o‘rin almashtirish juft o‘rin almashtirish bo‘lishi uchun uning juft sondagi transpozitsiyalarning ko‘paytmasi ko‘rinishda yozilishi zarur va yetarli ekan.

Uzunligi k ga teng bo‘lgan $\pi = (1\ 2\ \ldots\ k)$ siklni $\pi = (1\ k) \circ (1\ k-1) \circ \cdots \circ (1\ 2)$ ko‘rinishda yozish mumkin ekanligidan, quyidagicha xulosa qilishimiz mumkin:

uzunligi k ga teng sikl juft o‘rin almashtirish bo‘lishi uchun k toq bo‘lishi zarur va yetarli.

S_n simmetrik gruppaning barcha juft o‘rin almashtirishlari to‘plami A_n kabi belgilanadi. Quyida juft o‘rin almashtirishlar to‘plamini gruppa bo‘lishini ko‘rsatamiz:

$e = (1\ 2) \circ (1\ 2)$ tenglik o‘rinli ekanligidan $e \in A_n$, ya’ni $A_n \neq \emptyset$. Ma’lumki, $\pi_1 \circ \pi_2$ juft o‘rin almashtirish bo‘lishi uchun, π_1 va π_2 o‘rin almashtirishlar bir vaqtda juft yoki toq bo‘lishi zarur va yetarli. Bundan esa $\circ$ amali A_n to‘plamda yopiq ekanligi kelib chiqadi. Agar $\pi \in A_n$ bo‘lsa, u holda $\pi \circ \pi^{-1} = e$ juft ekanligidan, $\pi^{-1} \in A_n$. Demak, $(A_n, \circ)$ gruppa bo‘ladi. Ushbu gruppaga **ishora almashishlar** gruppasi deb ataladi.

Quyidagi teoremada ishora almashishlar gruppasining ixtiyoriy elementini uzunligi 3 ga teng bo‘lgan sikllar ko‘paytmasi shaklida ifodalash mumkinligini ko‘rsatamiz.

1.2.2-teorema. $A_n (n \geq 3)$ *gruppaning ixtiyoriy elementini uzunligi 3 ga teng bo‘lgan sikllar ko‘paytmasi ko‘rinishida yozish mumkin.*

Isbot. Aytaylik, $\pi \in A_n$ o‘rin almashtirish berilgan bo‘lib, uning transpozitsiyalar ko‘paymasi ko‘rinishidagi ifodasi quyidagicha bo‘lsin

$$\pi = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{2r}.$$

Shuningdek, ixtiyoriy (a, b) transpozitsiyani $(a\ \ b) = (1\ \ a) \circ (1\ \ b) \circ (1\ \ a)$ ko‘rinishida yozish mumkin bo‘lganligi uchun o‘rin almashtirish

$$\pi = (1\ i_1) \circ (1\ i_2) \circ \cdots \circ (1\ i_{2m})$$

shaklga keladi.

Nixoyat, $(1\ i_1) \circ (1\ i_2) = (1\ i_2\ i_1)$ tenglikdan foydalanib, π o‘rin almashtirishni uzunligi 3 ga teng bo‘lgan sikllar ko‘paytmasi ko‘rinishda yozish mumkinligini hosil qilamiz. $\square$

1.2.1-misol. *Quyidagi $\pi \in S_7$ o‘rin almashtirishni sikllar ko‘paytmasi shaklida ifodalang.*

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

Yechish. Dastlab,

$$\pi(1) = 6, \quad \pi^2(1) = \pi(6) = 7, \quad \pi^3(1) = \pi(7) = 1$$

tengliklardan foydalanib, $\sigma_1 = (1\ \pi(1)\ \pi^2(1)) = (1\ 6\ 7)$ siklga ega bo‘lamiz. Endi, I_7 to‘plamdan σ_1 siklda mavjud bo‘lmagan elementni, masalan 2 sonini olamiz. U holda,

$$\pi(2) = 3, \quad \pi^2(2) = \pi(3) = 5, \quad \pi^3(2) = \pi(5) = 4, \quad \pi^4(2) = \pi(4) = 2,$$

ya'ni $\sigma_2 = (2\ 3\ 5\ 4)$. Demak, $\pi = \sigma_1 \circ \sigma_2$. $\square$

1.2.2-misol. *Quyidagi* $(1\ 3\ 5\ 7) \circ (2\ 3\ 5\ 4) \in S_7$ *elementning tartibini toping.*

Yechish. Dastlab, ushbu elementlarning ko'paytmasini topib olamiz

$$(1\ 3\ 5\ 7) \circ (2\ 3\ 5\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 7 & 6 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 2 & 4 & 6 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 7 & 2 & 4 & 6 & 1 \end{pmatrix} = (1\ 3\ 7) \circ (2\ 5\ 4).$$

Demak, berilgan element uzunligi uchga teng bo'lgan ikkita kesishmaydigan sikllarning ko'paytmasi ko'rinishida ifodalandi. Har bir siklning tartibi uchga teng ekanligidan berilgan elementning ham tartibi 3 ga teng ekanligini hosil qilamiz.

$\square$

1.2.1 Mustaqil ishlash uchun misol va masalalar

1. Quyidagi o'rin almashtirishlarni o'zaro kesishmaydigan sikllar ko'paytmasi ko'rinishida yozing. Shuningdek, berilgan o'rin almashtirishlarni transpozitsiyalar ko'rinishida ham ifodalang.

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

2. Quyidagi α va β o'rin almashtirishlar uchun $\alpha \circ \beta \circ \alpha^{-1}$ ifodani toping:

   - $\alpha = (1\ 2\ 5\ 7), \quad \beta = (2\ 4\ 6) \in S_7$.
   - $\alpha = (1\ 3\ 5\ 7), \quad \beta = (2\ 4\ 8) \circ (1\ 3\ 6) \in S_8$.
   - $\alpha = (1\ 3) \circ (5\ 8), \quad \beta = (2\ 3\ 6\ 7) \in S_8$.
   - $\alpha = (2\ 5\ 9) \circ (1\ 3\ 6), \quad \beta = (1\ 5\ 7) \circ (2\ 4\ 6\ 9) \in S_9$.

3. $(1\ 3\ 5\ 7)$ va $(2\ 3\ 6\ 8) \in S_8$ sikllar uchun $\alpha \circ (1\ 3\ 5\ 7) \circ \alpha^{-1} = (2\ 3\ 6\ 8)$ tenglikni qanoatlantiruvchi α o'rin almashtirishni toping.

4. Quyidagi elementlarning tartiblarini aniqlang.

- $(1\ 2\ 3) \circ (4\ 5) \in S_5$.
- $(1\ 2\ 4\ 3) \circ (5\ 6) \in S_6$.
- $(1\ 7\ 4\ 3) \circ (2\ 6\ 5) \in S_7$.
- $(1\ 2\ 4\ 3) \circ (2\ 6\ 5) \in S_6$.
- $(1\ 2\ 7) \circ (1\ 3\ 5) \in S_7$.

5. Agar $\sigma \in S_n$ o'rin almashtirish o'zaro kesishmaydigan sikllar ko'paymasi ko'rinishida
$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$$
kabi ifodalangan bo'lib, $ord(\sigma_i) = n_i,\ i \in \{1, 2, \ldots, k\}$ bo'lsa, u holda
$$ord(\sigma) = EKUB(n_1, n_2, \ldots, n_k)$$
ekanligini isbotlang.

6. $(1\ 2\ \ldots\ n-1\ n)^{-1} = (n\ n-1\ \ldots\ 2\ 1)$ tenglikni isbotlang.

7. $\alpha = (a_1\ a_2\ \ldots\ a_k) \in S_n$ sikl berilgan bo'lsin. U holda quyidagi tenglikni isbotlang.
$$\alpha^2 = \begin{cases} (a_1\ a_3\ \ldots\ a_{2m-1}) \circ (a_2\ a_4\ \ldots\ a_{2m}), & \text{agar } k = 2m; \\ (a_1\ a_3\ \ldots\ a_{2m+1}\ a_2\ a_4\ \ldots\ a_{2m}), & \text{agar } k = 2m+1. \end{cases}$$

8. S_4 gruppaning tartibi ikkiga teng bo'lgan barcha elementlarini toping.

9. S_4 gruppaning tartibi uchga teng bo'lgan barcha elementlarini toping.

10. A_4 gruppaning barcha elementlarini toping.

11. Ixtiyoriy $\alpha, \beta \in S_n$ o'rin almashtirishlar uchun $\alpha^{-1} \circ \beta^{-1} \circ \alpha \circ \beta \in A_n$ ekanligini isbotlang.

12. $|A_n| = \frac{n!}{2}$ tenglikni isbotlang.

13. S_n simmetrik gruppada uzunligi r ga teng bo'lgan turli xil sikllar soni $\frac{1}{r} \frac{n!}{(n-r)!}$ ga teng bo'lishini isbotlang.

14. $\sigma \in S_n,\ n \geq 2$ siklning uzunligi k ga teng bo'lishi uchun, $ord(\sigma) = k$ bo'lishi zarur va yetarli ekanligini isbotlang.

1.3 Qism gruppalar. Siklik gruppalar

Bizga $(G, *)$ gruppa va uning bo'sh bo'lmagan $H \subset G$ qism to'plami berilgan bo'lsin. Agar $\forall a, b \in H$ elementlar uchun $a * b \in H$ bo'lsa, u holda H to'plam $*$ amaliga nisbatan yopiq deb ataladi. Ta'kidlash joizki, G to'plam gruppa bo'lganligi va $H \subset G$ ekanligidan $\forall a, b, c \in H$ elementlar uchun assosiativlik sharti bajariladi, ya'ni $(a * b) * c = a * (b * c)$ munosabat o'rinli bo'ladi. Demak, agar H to'plam $*$ amaliga nisbatan yopiq bo'lsa, u holda $(H, *)$ yarimgruppa tashkil qiladi.

1.3.1-ta'rif. *Agar H to'plam G gruppada aniqlangan $*$ amaliga nisbatan gruppa tashkil qilsa, u holda H to'plam $(G, *)$ gruppaning qism gruppasi deyiladi va $H \leq G$ kabi belgilanadi.*

Ta'kidlash joizki, ixtiyoriy gruppaning kamida ikkita $H_1 = \{e\}$ va $H_2 = G$ qism gruppalari mavjud. Gruppaning birlik elementdan va o'zidan iborat bo'lgan qism gruppalaridan farq qiluvchi qism gruppalariga xosmas qism gruppalar deyiladi.

Biz avvalgi mavzularda qaragan juda ko'p gruppalarimizning biri ikkinchisiga qism gruppa bo'ladi. Masalan, butun sonlar to'plamining additiv (qo'shish amaliga nisbatan) gruppasi, ratsional sonlar to'plamining additiv gruppasiga qism qruppa, o'z navbatida ratsional sonlar haqiqiy sonlarning, haqiqiy sonlar esa kompleks sonlar to'plamining additiv gruppasiga qism gruppa bo'ladi, ya'ni qiyudagilar o'rinli

$$(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +).$$

Bundan tashqari sonlar to'plamlarining multiplikativ(ko'paytirish amaliga nisbatan) gruppalari uchun ham quyidagilar o'rinli

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

Ma'lumki, n-tartibli xosmas matritsalar to'plami $GL_n(\mathbb{C})$ va determinanti 1 ga teng bo'lgan matritsalar to'plami $SL_n(\mathbb{C})$ ko'paytirish amaliga nisbatan gruppa tashkil qilib, $SL_n(\mathbb{C}) \leq GL_n(\mathbb{C})$ bo'ladi. Bundan tashqari $GL_n(\mathbb{C})$ gruppaning qism gruppalari bo'lgan quyidagi muhim gruppalar mavjud:

$$\mathbf{O}(n) = \{A \in GL_n(\mathbb{R}) \mid AA^T = A^T A = E\},$$

$$\mathbf{SO}(n) = \{A \in \mathbf{O}(n) \mid det(A) = 1\},$$

$$\mathbf{U}(n) = \{A \in GL_n(\mathbb{C}) \mid AA^* = A^* A = E\},$$

$$\mathbf{SU}(n) = \{A \in \mathbf{U}(n) \mid det(A) = 1\},$$

bu yerda $A^* = \overline{A}^T$, ya'ni A matritsaning elementlarini kompleks qo'shmasi bilan almashtirib, so'ngra transponirlashdan hosil bo'lgan matritsa.

Endi qism gruppaning xossalarini batafsilroq o'rganishni boshlaymiz.

1.3.1-tasdiq. *Gruppaning ixtiyoriy qism gruppasining birlik elementi, gruppa birlik elementi bilan ustma-ust tishadi.*

Isbot. Aytaylik, H to'plam G gruppaning qism gruppasi bo'lib, e_H va e_G elementlar mos ravishda $(H, *)$ va $(G, *)$ gruppalarning birlik elementlari bo'lsin. U holda, ixtiyoriy $a \in H$ element uchun

$$a * e_H = e_H * a = a.$$

Ikkinchi tomondan $H \subset G$ ekanligidan

$$a * e_G = e_G * a = a$$

hosil bo'ladi. Bu tengliklardan $e_G * a = e_H * a$ tenglik kelib chiqadi. Gruppada qisqartirish qoidasi o'rinli bo'lganligi uchun $e_G = e_H$ ekanligini hosil qilamiz. $\square$

Ushbu tasdiqdan ko'rinadiki, berilgan $H \subset G$ to'plam $(G, *)$ gruppaning qism gruppasi bo'lishi uchun H to'plam $*$ amaliga nisbatan yopiq bo'lishi, G gruppaning birlik elementi H to'plamda yotishi va $\forall a \in H$ elementning teskarisi a^{-1} yana H to'plamga tegishli bo'lishi zarur va yetarli.

Quyidagi teoremada esa, yuqorida aytilgan shartlani umumiy bitta shart bilan almashtiruvchi tasdiq beriladi.

1.3.1-teorema. $(G, *)$ *gruppaning bo'sh bo'lmagan* $H \subset G$ *qism to'plami qism gruppa bo'lishi uchun ixtiyoriy* $a, b \in H$ *elementlar uchun* $a * b^{-1} \in H$ *munosabatning o'rinli bo'lishi zarur va yetarli.*

Isbot. *Zaruriylik.* Aytaylik, $(H, *)$ qism gruppa bo'lsin, u holda ixtiyoriy $a, b \in H$ elementlar uchun $b^{-1} \in H$ bo'lib, bundan esa $a * b^{-1} \in H$ munosabat o'rinli ekanligi kelib chiqadi.

Yetarlilik. Endi, ixtiyoriy $a, b \in H$ elementlar uchun $a * b^{-1} \in H$ munosabat o'rinli bo'lsin. Agar $b = a$ deb olsak, u holda $a * a^{-1} = e \in H$. Demak, e birlik element H to'plamga tegishli bo'ladi. Endi a element o'rniga e elementni olib, ixtiyoriy $b \in H$ element uchun $e * b^{-1} \in H$, ya'ni $b^{-1} \in H$ munosabatni hosil qilamiz. Demak H da yotuvchi ixtiyoriy elementning teskarisi H da yotadi. Endi $a * b^{-1} \in H$ munosabatda, $b \in H$ element o'rniga $b^{-1} \in H$ elementni qo'yib, $a * (b^{-1})^{-1} = a * b \in H$ ekanligiga ega bo'lamiz. Bundan esa, $(H, *)$ qism gruppa ekanligi kelib chiqadi. $\square$

Berilgan H qism to'plam chekli bo'lgan holda quyidagi natijaga ega bo'lamiz.

1.3.1-natija. $(G, *)$ *gruppa va uning bo'sh bo'lmagan* $H \subset G$ *chekli qism to'plami berilgan bo'lsin. Agar* $\forall a, b \in H$ *elementlar uchun* $a * b \in H$ *munosabat o'rinli bo'lsa, u holda* $(H, *)$ *qism gruppa bo'ladi.*

Isbot. Natijaning shartidan ixtiyoriy $a \in H$ element va ixtiyoriy $n \in \mathbb{N}$ uchun $a^n \in H$ o'rinli ekanligi hosil bo'ladi, ya'ni $a \in H$ elementning ixtiyoriy natural darajasi yana H ga tegishli bo'ladi. H to'plam chekli to'plam bo'lganligi uchun $\{a, a^2, \dots, a^k, \dots\}$ elementlarning ichida o'zaro tenglari mavjud, aks holda H ning elementlari cheksiz ko'p bo'lar edi. Demak, qandaydir m va k $(m > k)$ natural sonlar topilib, $a^m = a^k$ tenglik o'rinli bo'ladi. Bu tenglikdan $e = a^{m-k} \in H$ ekanligini, ya'ni gruppaning birlik elementi H to'plamda yotishini hosil qilamiz.

Endi H dagi barcha elementlarning teskarisi ham H da yotishini ko'rsatamiz. Ixtiyoriy $a \in H$ element uchun $a^{m-k} = e$ ekanligidan $a * a^{m-k-1} = a^{m-k-1} * a = e$ tenglikka ega bo'lamiz, ya'ni a elementning teskarisi $a^{-1} = a^{m-k-1} \in H$. Demak, $(H, *)$ qism gruppa bo'lar ekan. □

1.3.2-ta'rif. $(G, *)$ *gruppaning markazi deb*

$$Z(G) = \{b \in G \mid a * b = b * a, \ \forall a \in G\}$$

to'plamga aytiladi.

1.3.2-teorema. $(G, *)$ *gruppaning markazi uning kommutativ qism gruppasi bo'ladi.*

Isbot. Ixtiyoriy $a \in G$ element uchun $e * a = a * e$ ekanligidan $e \in Z(G)$ kelib chiqadi. Demak, $Z(G)$ bo'sh bo'lmagan to'plam. Aytaylik, $b, c \in Z(G)$ bo'lsin, ya'ni $b*a = a*b$, $c*a = a*c$ tengliklar $\forall a \in G$ uchun o'zinli bo'lsin. Bundan esa, $a*c^{-1} = c^{-1}*a$ tenglik ham $\forall a \in G$ uchun o'rinli ekanligi kelib chiqadi. Quyidagi

$$a*(b*c^{-1}) = (a*b)*c^{-1} = (b*a)*c^{-1} = b*(a*c^{-1}) = b*(c^{-1}*a) = (b*c^{-1})*a$$

tenglikdan esa $b*c^{-1} \in Z(G)$ ekanligini hosil qilamiz. Demak, $Z(G)$ qism gruppa bo'ladi. $Z(G)$ ning kommutativ ekanligi esa ta'rifdan kelib chiqadi. □

Quyidagi teoremada berilgan gruppaning qism gruppalari kesishmasi yana qism gruppa bo'lishi ko'rsatiladi.

1.3.3-teorema. $(G, *)$ *gruppaning ixtiyoriy sondagi qism gruppalari kesishmasi yana qism gruppa bo'ladi.*

Isbot. Bizga G gruppaning $H_\alpha, \alpha \in I$ qism gruppalari berilgan bo'lib, $\bigcap\limits_{\alpha \in I} H_\alpha$ to'plamni qaraylik. Ixtiyoriy H_α qism gruppa uchun $e \in H_\alpha$ bo'lganligi uchun, $e \in \bigcap\limits_{\alpha \in I} H_\alpha$ bo'ladi. Demak, $\bigcap\limits_{\alpha \in I} H_\alpha$ to'plam bo'sh emas.

Endi $\forall a, b \in \bigcap\limits_{\alpha \in I} H_\alpha$ elementlarni olamiz. Bu elementlar har bir qism gruppaga tegishli, ya'ni $a, b \in H_\alpha$ bo'lganligi uchun $a * b^{-1} \in H_\alpha$ bo'ladi. Bundan esa $a * b^{-1} \in \bigcap\limits_{\alpha \in I} H_\alpha$ kelib chiqadi. Demak, $\bigcap\limits_{\alpha \in I} H_\alpha$ qism gruppa. □

1.3.3-ta'rif. *Aytaylik $(G, *)$ gruppa va M uning qism to'plami bo'lsin. G gruppaning M to'plamni o'z ichiga oluvchi barcha qism gruppalari kesishmasi M to'plam orqali hosil qilingan qism gruppa deyiladi va $\langle M\rangle$ kabi belgilanadi.*

1.3.4-teorema. *G gruppaning M qism to'plami orqali hosil qilingan qism gruppasi uchun quyidagi tenglik o'rinli*

$$\langle M\rangle = \{a_1^{\varepsilon_1} * a_2^{\varepsilon_2} * \cdots * a_n^{\varepsilon_n} | a_1, a_2, \ldots, a_n \in M,\ \varepsilon_i = \pm 1,\ n = 1, 2, \ldots\}$$

Isbot. Teoremadagi tenglikning o'ng tominini H orqali belgilab olaylik. Ma'lumki, $n = 1$ va $\varepsilon_1 = 1$ bo'lgan holda $a_1 \in H$, ya'ni M to'plamning ixtiyoriy elementi H ga tegishli ekanligi kelib chiqadi. Bundan tashqari, $\forall h, g \in H$ uchun $h = a_1^{\varepsilon_1} * a_2^{\varepsilon_2} * \cdots * a_n^{\varepsilon_n}$ va $g = b_1^{\epsilon_1} * b_2^{\epsilon_2} * \cdots * b_k^{\epsilon_k}$ bo'lib,

$$h * g^{-1} = a_1^{\varepsilon_1} * a_2^{\varepsilon_2} * \cdots * a_n^{\varepsilon_n} * b_k^{-\epsilon_k} * \cdots * b_2^{-\epsilon_2} * b_1^{-\epsilon_1} \in H.$$

Demak, H to'plam qism gruppa bo'lib, M ni o'z ichiga oladi. Bu esa $\langle M\rangle \subset H$ ekanligini anglatadi.

Ikkinchi tomondan esa barcha a_i elementlar $\langle M\rangle$ qism gruppada yotganligi uchun, $a_1^{\varepsilon_1} * a_2^{\varepsilon_2} * \cdots * a_n^{\varepsilon_n}$ ko'rinishidagi barcha elementlar $\langle M\rangle$ da yotadi. Bendan esa, $H \subset \langle M\rangle$ kelib chiqadi. Demak, $\langle M\rangle = H$. $\square$

Agar M to'plam bitta elementdan iborat to'plam, ya'ni $M = \{a\}$ bo'lsa, u holda $\langle\{a\}\rangle$ o'rniga $\langle a\rangle$ belgilashdan foydalanish qabul qilingan.

1.3.2-natija. *G gruppaning ixtiyoriy a elementi uchun $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ bo'ladi.*

1.3.4-ta'rif. *Agar G gruppada $G = \langle a\rangle$ tenglikni qanoatlantiruvchi $a \in G$ element mavjud bo'lsa, u holda G gruppa **siklik gruppa** deyiladi.*

Ta'kidlash joizki, har qanday siklik gruppa kommutativ gruppa bo'ladi. Haqiqatan ham, $G = \langle a\rangle$ 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 bo'ladi. 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 gruppa kommutativ ekanligiga ega bo'lamiz.

1.3.1-misol.

- *Qo'shishga nisbatan butun sonlar gruppasi $(\mathbb{Z}, +)$ siklik gruppa bo'ladi, ya'ni $\mathbb{Z} = \langle 1\rangle$.*
- *Qo'shishga nisbatan chegirmalar gruppasi $(\mathbb{Z}_n, +)$ ham siklik gruppa bo'ladi, ya'ni $\mathbb{Z}_n = \langle\overline{1}\rangle$.*

Quyidagi teorema chekli siklik gruppalarni aniq tasnifini ifodalaydi.

1.3.5-teorema. *Agar G tartibi n ga teng bo‘lgan siklik gruppa bo‘lsa, u holda* $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

Isbot. G siklik gruppa bo‘lganligi uchun $G = \langle a \rangle$ bo‘lib, 1.3.2-natijaga ko‘ra $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$ kelib chiqadi. Suningdek, $\langle a \rangle$ chekli bo‘lganligi uchun shunday i, j $(j > i)$ butun sonlar topilib, $a^i = a^j$ bo‘ladi. Natijada $a^{j-i} = e, \ j - i > 0$ tenglikka ega bo‘lamiz. Endi $T := \{k \in \mathbb{N} \mid a^k = e\}$ to‘plamning eng kichik elementini m bilan belgilaymiz. U holda $S := \{e, a, a^2, \ldots, a^{m-1}\}$ to‘plamning barcha elementlari turli xil bo‘ladi. Darhaqiqat, agar $a^s = a^t, \ 0 \leq s < t < m$, bo‘lsa, u holda $a^{t-s} = e, \ 0 < t - s < m$ bo‘lib, m soni T to‘plamning eng kichik elementi ekanligiga zidddiyat kelib chiqadi.

Shuningdek $S \subseteq \langle a \rangle$ ekanligi ma’lum. Endi $\langle a \rangle \subseteq S$ munosabat o‘rinli ekanligini ko‘rsatamiz. Buning uchun a ning ixtiyoriy darajasi S to‘plamga tegishli ekanini ko‘rsatish kifoya. Ixtiyoriy $a^k \in \langle a \rangle, \ k \in \mathbb{Z}$ uchun, qoldiqli bo‘lish qoidasiga ko‘ra k sonini $k = qm + r, \ 0 \leq r < m$ ko‘rinishda yozib olsak:

$$a^k = a^{qm+r} = (a^m)^q * a^r = e * a^r = a^r \in S.$$

Bundan esa, $\langle a \rangle \subseteq S$ kelib chiqadi. Shunday qilib, $S = \langle a \rangle$ va S ning elementlari turli xil, hamda $\langle a \rangle$ gruppaning tartibi n ga teng ekanligidan $m = n$ kelib chiqadi. $\square$

Yuqoridagi teoremadan quyidagi natijaga ega bo‘lamiz.

1.3.3-natija. *G gruppa siklik bo‘lishi uchun shunday $a \in G$ element topilib, $ord(a) = |G|$ bo‘lishi zarur va yetarli*

Quyidagi teoremada siklik gruppaning ixtiyoriy qism gruppasi yana siklik gruppa bo‘lishini ko‘rsatamiz.

1.3.6-teorema. *Siklik gruppaning ixtiyoriy qism gruppasi yana siklik gruppa bo‘ladi.*

Isbot. Aytaylik, $G = \langle a \rangle$ siklik gruppa berilgan bo‘lib, H uning qism gruppasi bo‘lsin. Agar $H = \{e\}$ bo‘lsa, u holda uning siklik ekanligi ravshan. Aytaylik, $H \neq \{e\}$ bo‘lib, $b \in H, b \neq e$ bo‘lsin. U holda $b = a^m$ bo‘lib, H qism gruppa bo‘lganligi uchun $b^{-1} = a^{-m} \in H$ bo‘ladi. Bundan esa, H qism gruppa $a^k, k > 0$ elementni o‘z ichiga olishi kelib chiqadi.

Aytaylik, n soni $a^n \in H$ munosabat o‘rinli bo‘ladigan eng kichik natural son bo‘lsin. U holda biz $H = \langle a^n \rangle$ ekanligini ko‘rsatamiz. Buning uchun ixtiyoriy $h \in H$ elementni a^n ning darajasi ko‘rinishida yozilishini ko‘rsatish kifoya. $h \in G$ bo‘lganligi uchun shunday $k \in \mathbb{Z}$ topilib, $h = a^k$ bo‘ladi. k sonini n ga qoldiqli bo‘lsak, $k = nq + r$, $0 \leq r < n$ bo‘ladi. U holda, $r = k - nq$ ekanligidan

$$a^r = a^{k-nq} = a^k (a^n)^{-q} \in H$$

kelib chiqadi. n soni a elementning darajasi H ga tegishli bo‘ladigan eng kichik natural son bo‘lganligi uchun $r = 0$ ekanligiga ega bo‘lamiz. Demak, $k = nq$, ya’ni $h = (a^n)^q$ kelib chiqadi. Bu esa, $H = \langle a^n \rangle$ ekanligini anglatadi. $\square$

Ma’lumki $\mathbb{Z}_4$ to‘rtinchi tartibli siklik gruppa bo‘lib, uning qism gruppalari quyidagilardan iborat bo‘ladi

$$H_1 = \{\overline{0}\}, \quad H_2 = \{\overline{0}, \overline{2}\}, \quad H_3 = \mathbb{Z}_4.$$

Ko‘rinib turibdiki, $\mathbb{Z}_4$ gruppaning barcha qism gruppalari ham siklik bo‘ladi.

Quyidagi misolda yana bir to‘rtinchi tartibli gruppani keltiramiz.

1.3.2-misol. *Aytaylik bizga $G = \{e, a, b, c\}$ to‘plam berilgan bo‘lib, bu to‘plamda $*$ binar amal quyidagicha aniqlangan bo‘lsin:*

$$e * a = a * e = a, \quad e * b = a * b = b, \quad e * c = a * c = c,$$

$$e * e = a * a = b * b = c * c = e,$$

$$a * b = b * a = c, \quad a * c = c * a = b, \quad b * c = c * b = a.$$

U holda $(G, *)$ kommutativ gruppa bo‘lib, ushbu gruppa uchun

$$\langle e \rangle = \{e\}, \quad \langle a \rangle = \{e, a\}, \quad \langle b \rangle = \{e, b\}, \quad \langle c \rangle = \{e, c\}$$

munosabatlar o‘rinli bo‘ladi. Ko‘rinib turibdiki, bu gruppa siklik emas. Ushbu gruppa 4-tartibli Kleyn gruppasi deb atalib, u $\mathbf{K}_4$ kabi belgilanadi.

1.3.3-misol. *G gruppaning H qism gruppasi uchun $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ to‘plam qism gruppa bo‘lishini va $|gHg^{-1}| = |H|$ ekanligini ko‘rsating.*

Yechish. Dastlab, gHg^{-1} to‘plam G gruppaning qism gruppasi bo‘lishini ko‘rsatamiz. $e = geg^{-1} \in gHg^{-1}$ ekanligidan bu to‘plamning bo‘sh emasligi kelib chiqadi. Ixtiyoriy $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$ elementlar uchun

$$gh_1g^{-1}(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1}.$$

Bundan esa, gHg^{-1} to‘plamning qism gruppa ekanligi kelib chiqadi.

Endi $|gHg^{-1}| = |H|$ tenglikni ko‘rsatamiz. Buning uchun $f : H \to gHg^{-1}$, $f(h) = ghg^{-1}$ akslantirishni aniqlaymiz. Ushbu akslantirish inyektiv bo‘ladi, chunki agar $f(h) = f(h')$ bo‘lsa, u holda $ghg^{-1} = gh'g^{-1}$ bo‘lib, bundan $h = h'$ kelib chiqadi. Bu akslantirishning syurektivligi esa ixtiyoriy $a = ghg^{-1}$ element uchun $f(h) = a$ ekanligidan kelib chiqadi. Demak, f akslantirish o‘zaro bir qiymatli. Bundan esa, $|gHg^{-1}| = |H|$ kelib chiqadi. $\square$

1.3.4-misol. *Tartibi $nm (n > 1, m > 1)$ ga teng bo‘lgan gruppaning xosmas qism gruppasi mavjud ekanligini ko‘rsating.*

Yechish. Aytaylik, G gruppaning tartibi nm soniga teng bo‘lsin. Agar G siklik bo‘lsa, u holda $G = \langle a \rangle$ bo‘lib, $ord(a^m) = n$ bo‘ladi. $H = \langle a^m \rangle$ to‘plam esa, G gruppaning xosmas qism gruppasi bo‘ladi.

Agar G gruppa siklik bo‘lmasa, u holda uning birlik elementdan farqli ixtiyoriy $a \in G$ elementini olib, $H = \langle a \rangle$ to‘plamni qarasak, ushbu to‘plam G gruppaning xosmas qism gruppasi bo‘ladi. $\square$

1.3.1 Mustaqil ishlash uchun misol va masalalar

1. Quyidagi to‘plamlar $(\mathbb{Z}_{12}, +_{12})$ gruppaning qism gruppasi bo‘lishini isbotlang:
   - $H_1 = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$.
   - $H_2 = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$.
   - $H_3 = \{\overline{0}, \overline{4}, \overline{8}\}$.

2. Quyidagi matritsalar to‘plamlarini $(GL_2(\mathbb{R}), \cdot)$ gruppaning qism gruppasi bo‘lishini isbotlang:
   - $S_1 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1 \right\}$.
   - $S_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \neq 0 \right\}$.
   - $S_3 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2 + b^2 \neq 0 \right\}$;
   - $S_4 = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad \neq 0 \right\}$.

3. $H = SL_n(\mathbb{R})$ to‘plam $G = (GL_n(\mathbb{R}, \cdot)$ gruppaning qism gruppasi bo‘lishini isbotlang.

4. $H = \{z \in \mathbb{C} \mid |z| = 1\}$ to‘plam $(\mathbb{C} \setminus \{0\}, \cdot)$ gruppaning qism gruppasi bo‘lishini ko‘rsating.

5. $G = \{(a, b) \mid a, b \in \mathbb{R}, b \neq 0\}$ to‘plamda binar amal $(a, b) * (c, d) = (a + bc, bd)$ kabi kiritilgan bo‘lsa, u holda quyidagilarni isbotlang:
   - $(G, *)$ nokommutativ gruppa.
   - $H_1 = \{(a, b) \in G \mid a \neq 0\}$ to‘plam G gruppaning qism gruppasi.
   - $H_2 = \{(a, b) \in G \mid b > 0\}$ to‘plam G gruppaning qism gruppasi.
   - $H_3 = \{(a, b) \in G \mid b = 1\}$ to‘plam G gruppaning qism gruppasi.

6. $G = \{(a, b) |\ a, b \in \mathbb{R}, b \neq 0\}$, $(a, b) * (c, d) = (a + bc, bd)$ gruppaning tartibi 2 ga teng bo‘lgan elementlarini toping.

7. $(\mathbb{Z}, +)$ gruppaning quyidagi qism gruppalarini aniqlang:

   - $H_1 = \langle 4, 6\rangle$.
   - $H_2 = \langle 4, 7\rangle$.
   - $H_3 = \langle 6, 9\rangle$.

8. $(\mathbb{Z}, +)$ gruppaning barcha qism gruppalarini aniqlang.

9. S_3 gruppaning quyidagi $T = \{x \in S_3 |\ x^2 = e\}$ qism to‘plami qism gruppa bo‘ladimi?

10. S_3 gruppaning barcha qism gruppalarini aniqlang.

11. S_4 gruppaning tartibi 3 ga teng bo‘lgan barcha qism gruppalarini aniqlang.

12. Ushbu $H = \{e,\ (1\,2)\circ(3\,4),\ (1\,3)\circ(2\,4),\ (1\,4)\circ(2\,3)\}$ to‘plam S_4 gruppaning qism gruppasi bo‘lishini isbotlang.

13. S_4 gruppaning tartibi 4 ga teng bo‘lgan barcha qism gruppalarini aniqlang.

14. S_4 gruppaning $H = \langle(1\ 2),\ (1\ 2\ 3\ 4)\rangle$ qism gruppasini aniqlang.

15. S_n gruppa uchun quyidagilarni isbotlang:

    - $S_n = \langle(1\ 2),\ (1\ 3), \dots, (1\ n)\rangle$.
    - $S_n = \langle(1\ 2),\ (1\ 2\ 3 \dots,\ n)\rangle$.
    - $S_n = \langle(1\ 2),\ (2\ 3), \dots, (n-1\ n)\rangle$.
    - $A_n = \langle(1\ 2\ 3),\ (1\ 2\ 4), \dots, (1\ 2\ n)\rangle$.

16. G gruppaning a va b elementlari uchun $ord(a) = 6, ord(b) = 2$, va $(ab)^2 = e$ tengliklar o‘rinli bo‘lsa, u holda quyidagilarni isbotlang.

    - $aba = b$.
    - $(a^2b)^2 = e$.
    - $ba^2b = a^4$.
    - $ba^3b = a^3$.

17. Kommutativ gruppaning barcha chekli tartibli elementlaridan tuzilgan to‘plam qism gruppa bo‘lishini isbotlang.

18. Barcha elementlarining tartibi chekli bo‘lgan cheksiz gruppa mavjudmi?

19. G gruppani ikkita xosmas qism gruppalarning birlashmasi ko'rinishida tasvirlab bo'lmasligini isbotlang.

20. Gruppaning ikkita qism gruppasi birlashmasi qism gruppa bo'lishi uchun biri ikkinchisining ichida yotishi zarur va yetarli ekanligini isbotlang.

21. G gruppaning H qism gruppasi uchun $\langle H \rangle = H$ tenglik o'rinli ekanligini isbotlang.

22. Tartibi 30 ga teng bo'lgan $\langle a \rangle$ siklik gruppa berilgan bo'lsin. u holda quyidagi qism gruppalarning elementlarini toping.

    - $\langle a^2 \rangle$.
    - $\langle a^3 \rangle$.
    - $\langle a^4 \rangle$.
    - $\langle a^5 \rangle$.
    - $\langle a^6 \rangle$.

23. Tartibi 20 ga teng bo'lgan siklik gruppaning tartibi 5 ga teng bo'lgan elementlari sonini aniqlang.

24. Quyidagi gruppalardan qaysilari siklik gruppa bo'ladi.

    - $(2\mathbb{Z}, +)$.
    - $(\mathbb{Q}, +)$.
    - $(\mathbb{R}, +)$.
    - $(\{z \in \mathbb{C} \mid z^n = 1\}, \cdot)$ – birning n-darajali barcha kompleks ildizlari to'plamining multiplikativ gruppasi.
    - $(\mathbb{Q} \setminus \{0\}, \cdot)$.
    - $(\mathbb{R} \setminus \{0\}, \cdot)$.

25. $GL_2(\mathbb{C})$ gruppaning quyidagi qism gruppalarini aniqlang.

    - $A = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$.
    - $B = \left\langle \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \right\rangle$.
    - $C = \left\langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \right\rangle$.

26. $GL_2(\mathbb{R})$ gruppaning $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ va $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ elementlarining tartiblarini toping. $\langle AB \rangle$ siklik gruppa $GL_2(\mathbb{R})$ gruppaning cheksiz siklik gruppasi bo‘lishini isbotlang.

27. Elementlari butun sonlardan iborat bo‘lgan n-tartibli ortogonal matritsalar to‘plami $\mathbf{O}(\mathbb{Z})$ gruppa tashkil qilishini ko‘rsating, hamda uning tartibini aniqlang.

28. Tartibi n ga teng bo‘lgan siklik gruppaning yasovchilari soni $\varphi(n)$ ga teng ekanligini isbotlang, bu yerda φ-Eyler funksiyasi.

29. S_3 gruppaning ixtiyoriy xosmas qism gruppasi siklik gruppa bo‘lishini isbotlang.

30. S_4 gruppaning barcha siklik qism gruppalarini toping.

31. Ixtiyoriy nokommutativ gruppa xosmas qism gruppaga ega ekanligini isbotlang.

32. Quyidagi mulohazalardan qaysilari o‘rinli?

    - Ixtiyoriy n natural son uchun, tartibi n ga teng bo‘lgan siklik gruppa mavjud.
    - A_4 gruppaning ixtiyoriy xosmas qism gruppasi siklik bo‘ladi.
    - A_3 – siklik gruppa.
    - A_4 – siklik gruppa.
    - $(\mathbb{R}, +)$ gruppaning ixtiyoriy xosmas qism gruppasi siklik gruppa bo‘ladi.

1.4 Qo‘shni sinflar. Lagranj teoremasi

Biz ushbu mavzuda chekli gruppalar uchun asosiy teoremalardan hisoblangan Lagranj teoremasi haqida gaplashamiz. Lagranj teoremasi chekli gruppa qism gruppalari tartibi haqida ma‘lumot beruvchi teorema hisoblanadi. Dastlab, qism gruppaning chap va o‘ng qo‘shni sinflari tushunchalarini kiritamiz.

1.4.1-ta’rif. *Bizga G gruppa va uning H qism gruppasi berilgan bo‘lsin. Ixtiyoriy $a \in G$ element uchun quyidagi $aH = \{a * h \mid h \in H\}$ va $Ha = \{h * a \mid h \in H\}$ to‘plamlar mos ravishda H qism gruppaning G gruppadagi chap va o‘ng qo‘shni sinflari deyiladi.*

Ta'kidlash joizki, $eH = He$ tenglik har doim o'rinli bo'ladi. Bundan tashqari, a element har doim aH va Ha qo'shni sinflarga tegishli bo'ladi. Agar G kommutativ gruppa bo'lsa, u holda $aH = Ha$ tenglik ixtiyoriy $a \in G$ uchun o'rinli bo'ladi.

1.4.1-misol. *S_3 gruppaning A_3 qism gruppasi barcha chap qo'shni sinflarini tuzamiz, bu yerda*

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}.$$

Buning uchun $S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ gruppaning barcha elemtntlari bo'yicha aA_3 chap qo'shni sinflarni yozib chiqamiz:

$$\begin{aligned} eA_3 &= \{e, (1\ 2\ 3), (1\ 3\ 2)\}, \\ (1\ 2)A_3 &= \{(1\ 2), (1\ 3), (2\ 3)\}, \\ (1\ 3)A_3 &= \{(1\ 2), (1\ 3), (2\ 3)\}, \\ (2\ 3)A_3 &= \{(1\ 2), (1\ 3), (2\ 3)\}, \\ (1\ 2\ 3)A_3 &= \{e, (1\ 2\ 3), (1\ 3\ 2)\}, \\ (1\ 3\ 2)A_3 &= \{e, (1\ 2\ 3), (1\ 3\ 2)\}. \end{aligned}$$

Demak, $eA_3 = (1\,2\,3)A_3 = (1\,3\,2)A_3$ va $(1\,2)A_3 = (1\,3)A_3 = (2\,3)A_3$ tengliklar o'rinli bo'lar ekan.

Yuqoridagi misoldan ko'rinib turibdiki, turli xil $a, b \in G$ elementlar uchun ham aH va bH qo'shni sinflar teng bo'lishi mumkin. Quyidagi teoremada turli xil elementlarga mos keluvchi chap (o'ng) qo'shni sinflarning teng bo'lishining zaruriy va yetarlilik kriteriyasini keltiramiz.

1.4.1-teorema. *G gruppa va uning H qism gruppasi berilgan bo'lsin. Ixtiyoriy $a, b \in G$ elementlar uchun quyidagi munosabatlar o'rinli:*

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

2. $Ha = Hb \Leftrightarrow a * b^{-1} \in H.$

Isbot. Faraz qilaylik $aH = bH$ tenglik o'rinli bo'lsin. U holda $a \in aH$ va $aH = bH$ ekanligidan, $a = b * h'$ tenglikni qanoatlantiruvchi $h' \in H$ element mavjudligi kelib chiqadi. Bundan $b^{-1} * a = h' \in H$ munosabatga ega bo'lamiz.

Endi, aksincha $b^{-1} * a \in H$ munosabat o'rinli bo'lsin, u holda $b^{-1} * a = h' \in H$ deb belgilasak, $a = b * h'$ kelib chiqadi. Ixtiyoriy $a * h \in aH$ elementni qaraylik, u holda $a * h = b * h' * h \in bH$ ekanligidan $aH \subseteq bH$ munosabatga ega bo'lamiz. Endi, $bH \subseteq aH$ munosabat o'rinli ekanligini ko'rsatamiz. $b^{-1} * a = h'$ tenglikni $a * (h')^{-1} = b$ ko'rinishida yozib olaylik. Ixtiyoriy $b * h \in bH$ elementni olsak, u holda $b * h = a * (h')^{-1} * h \in aH$ ekanligidan $bH \subseteq aH$ munosabatga ega bo'lamiz. Demak, $aH = bH$.

Teoremaning 2-qismining isboti ham 1-qismining isbotiga o'xshash ko'rsatiladi. □

Endi turli qo'shni sinflarning kesishmasligini isbotlaymiz.

1.4.2-teorema. *Bizga G gruppa va uning H qism gruppasi berilgan bo'lsin. Ixtiyoriy $a, b \in G$ elementlar uchun $aH = bH$ yoki $aH \cap bH = \emptyset$ munosabatlardan biri o'rinli, ya'ni qo'shni sinflar yoki ustma-ust tushadi, yoki kesishmaydi.*

Isbot. Faraz qilaylik ixtiyoriy $a, b \in G$ elementlar uchun $aH \cap bH \neq \emptyset$ o'rinli bo'lsin. U holda $c \in aH \cap bH$ element mavjud, ya'ni $c \in aH$ va $c \in bH$. Bundan esa, c elementni quyidagicha ifodalash mumkinligi kelib chiqadi $c = a * h_1$ va $c = b * h_2$, bu yerda $h_1, h_2 \in H$. Natijada, $a * h_1 = b * h_2$ tenglikka ega bo'lamiz. Bu tenglikdan esa, $b^{-1} * a = h_2 * h_1^{-1}$ munosabatga ega bo'lamiz, ya'ni $b^{-1} * a \in H$. U holda 1.4.1-teoremadan $aH = bH$ tenglik kelib chiqadi. Demak, agar $aH \cap bH \neq \emptyset$ bo'lsa, u holda $aH = bH$ bo'lar ekan. □

1.4.1-natija. *G gruppa va H uning qism gruppasi bo'lsin. U holda $\{aH \mid a \in G\}$ to'plamlar sistemasi G gruppaning o'zaro kesishmaydigan bo'laklaridan iborat bo'ladi.*

Berilgan G gruppaning H qism gruppasini barcha chap qo'shni sinflaridan tashkil topgan sistemani $\mathcal{L} := \{aH \mid a \in G\}$ kabi, barcha o'ng qo'shni sinflaridan tashkil topgan sistemani esa $\mathcal{R} := \{Ha \mid a \in G\}$ kabi belgilaymiz.

1.4.3-teorema. *H, aH va Ha to'plamlar orasida o'zaro bir qiymatli moslik ornatish mumkin.*

Isbot. Ixtiyoriy $a \in G$ element uchun aH chap qo'shni sinf berilgan bo'lsin. $f : H \to aH$, $f(h) = ah$ akslantirishni qarab, bu akslantirishni o'zaro bir qiymatli, ya'ni biyektiv ekanligini ko'rsatamiz. Dastlab, f akslantirish inyektiv ekanligini ko'rsatamiz. Ushbu

$$f(h_1) = f(h_2) \ \Rightarrow \ a * h_1 = a * h_2 \ \Rightarrow \ h_1 = h_2$$

tengliklardan f akslantirishning inyektiv ekanligi kelib chiqadi.

O'z navbatida ixtiyoriy $a * h \in aH$ element uchun $f(h) = a * h$ tenglikni qanoatlantiradigan $h \in H$ element doim topilganligi uchun f akslantirish syurektiv bo'ladi. Demak, biz qurgan f akslantirish biyektiv ekan, ya'ni H va aH to'plamlar orasida o'zaro bir qiymatli moslik mavjud.

H va Ha to'plamlar orasidagi o'zaro bir qiymatli moslik ham yuqoridagi kabi o'rnatiladi. □

1.4.2-natija. *G gruppaning ixtiyoriy H qism gruppasi va ixtiyoriy $a \in G$ elementi uchun $|H| = |aH| = |Ha|$ tengliklar o'rinli.*

Demak, chekli H qism gruppaning barcha chap va oʻng qoʻshni sinflari elemetnlari soni bir xil boʻlgan toʻplamlardan iborat boʻlar ekan. Quyidagi teoremada esa, barcha chap sinflar soni barcha oʻng qoʻshni sinflar soniga teng boʻlishini koʻrsatamiz.

1.4.4-teorema. *G gruppaning H qism gruppasini barcha chap va oʻng qoʻshni sinflaridan tashkil topgan sistemalar oʻrtasida oʻzaro bir qiymatli moslik mavjud, ya'ni $|\mathcal{L}| = |\mathcal{R}|$.*

Isbot. Ma'lumki, teoremani isbotlash uchun $f : \mathcal{L} \to \mathcal{R}$ biyektiv akslantirish qurish kifoya. f akslantirishni quyidagicha aniqlaymiz: $f(aH) = Ha^{-1}$, $aH \in \mathcal{L}$.

Dastlab, bu akslantirishning toʻgʻri aniqlangan ekanligini koʻrsatamiz. Agar $aH = bH$ boʻlsa, u holda 1.4.1-teoremaning 1-bandiga koʻra, $b^{-1} * a \in H$ munosabat oʻrinli boʻladi. Natijada, $b^{-1} * (a^{-1})^{-1} \in H$ va 1.4.1-teoremaning 2-bandiga koʻra, $Hb^{-1} = Ha^{-1}$ tenglikka ega boʻlamiz. Ya'ni $f(aH) = f(bH)$ tenglik oʻrinli. Demak, f toʻgʻri aniqlangan akslantirish ekan.

Endi f akslantirishning inyektiv ekanligini koʻrsatamiz. Darhaqiqat, agar $f(aH) = f(bH)$ oʻrinli boʻlsa, u holda $Ha^{-1} = Hb^{-1}$ boʻlib, 1.4.1-teoremaning 2-bandiga koʻra $a^{-1} * (b^{-1})^{-1} \in H$ munosabat kelib chiqadi, ya'ni $a^{-1} * b \in H$. Oʻz navbatida, $b^{-1} * a = (a^{-1} * b)^{-1} \in H$ munosabatdan $aH = bH$ tenglik kelib chiqadi, ya'ni f inyektiv akslantirish boʻladi.

f akslantirishning syurektiv ekanligi esa, ixtiyoriy $Ha \in \mathcal{R}$ element uchun $Ha = H(a^{-1})^{-1} = f(a^{-1}H)$ munosabat oʻrinli ekanligidan kelib chiqadi. Demak, $f : \mathcal{L} \to \mathcal{R}$ biyektiv akslantirish ekanligi kelib chiqdi. □

Shunday qilib biz G gruppaning H qism gruppasi boʻyicha olingan chap yoki oʻng qoʻshni sinflari soni bir xil ekanligini koʻrsatdik. Ularning soniga H qism gruppaning G gruppadagi **indeksi** deb ataladi va $[G : H]$ kabi belgilanadi. Ma'lumki, agar G chekli gruppa boʻlsa, u holda $[G : H]$ indeks ham chekli boʻladi.

Endi ushbu mavzuning asosiy teoremasi hisoblangan Lagranj teoremasini keltiramiz.

1.4.5-teorema (Lagranj teoremasi). *G chekli gruppa va H uning qism gruppasi boʻlsin. U holda G gruppaning tartibi H qism gruppaning tartibiga qoʻldiqsiz boʻlinadi va $|G| = [G : H]|H|$ tenglik oʻrinli boʻladi.*

Isbot. Bizga G gruppa va uning H qism gruppasi berilgan boʻlsin. Gruppa chekli boʻlganligi uchun, H qism gruppaning chap qoʻshni sinflari cheklita boʻladi. Aytaylik, H ning barcha chap qoʻshni sinflari soni r ta boʻlib, ular $\{a_1H, a_2H, \dots, a_rH\}$ boʻlsin, ya'ni $[G : H] = r$. U holda 1.4.1-natijaga koʻra $G = \bigcup\limits_{i=1}^{r} a_iH$ boʻladi, bu yerda $a_iH \cap a_jH = \emptyset$, $i \neq j$, $1 \leq i, j \leq r$. Ushbu qoʻshni sinflar kesishmaydigan bo'lganligi uchun

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH|$$

tenglik o'rinli.

1.4.2-natijaga ko'ra $|H| = |a_iH|, \ 1 \leq i \leq r$ bo'lganligi uchun

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH| = \underbrace{|H| + |H| + \cdots + |H|}_{r \text{ marta}} = r|H| = [G : H]|H|.$$

Demak, G gruppaning tartibi H qism gruppaning tartibiga qo'ldiqsiz bo'linar ekan. □

1.4.3-natija. *Agar G gruppaning tartibi n ga teng bo'lsa, u holda ixtiyoriy $a \in G$ elementning tartibi n ning bo'luvchisi bo'lib, $a^n = e$ bo'ladi.*

Isbot. Aytaylik $ord(a) = k$ bo'lsin, u holda $H = \langle a \rangle$ siklik qism gruppa k ta elementdan iborat, ya'ni $|H| = |\langle a \rangle| = ord(a) = k$. 1.4.5-teoremaga ko'ra esa, n soni k ga bo'linadi, ya'ni $n = kq$. Demak, $a^n = a^{kq} = (a^k)^q = e^q = e$. □

1.4.4-natija. *Agar G tartibi tub son bo'lgan gruppa bo'lsa, u holda G siklik gruppa bo'ladi. Bundan tashqari, tartibi tub songa teng bo'lgan siklik gruppalar xosmas qism gruppaga ega emas.*

Isbot. G gruppaning birlik elementdan farqli $a \in G$ elementi uchun $H = \langle a \rangle$ siklik qism gruppani qarasak, u holda $|H|$ soni $|G|$ ning bo'luvchilaridan biri bo'ladi. $|G|$ tub son bo'lganligi va $|H| \geq 2$ ekanligi uchun $|G| = |H|$ tenglik kelib chiqadi, ya'ni $G = H$. □

Endi qism gruppalarning ko'paytmasi tushunchasini kiritamiz.

1.4.2-ta'rif. *G gruppaning H va K bo'sh bo'lmagan qism to'plamlari ko'paytmasi deb quyidagi to'plamga aytiladi*

$$HK = \{h * k \mid h \in H, k \in K\}.$$

Tabiiyki, ushbu ta'rif yordamida G gruppaning bir nechta $H_1, H_2, \ldots, H_n$ bo'sh bo'lmagan qism to'plamlari ko'paytmasini quyidagicha aniqlanishi kelib chiqadi

$$H_1H_2 \ldots H_n = \{h_1 * h_2 * \cdots * h_n \mid h_i \in H_i\}.$$

Agar G gruppaning H va K bo'sh bo'lmagan qism to'plamlari qism gruppalar bo'lsa, ularning ko'paytmasi HK to'plam ham G gruppaning qism gruppasi bo'ladimi degan tabiiy savol tug'iladi. Ushbu savolga quyidagi teoremada javob beriladi.

1.4.6-teorema. *G gruppaning H va K qism gruppalarining ko'paytmasi HK to'plam G gruppaning qism gruppasi bo'lishi uchun $HK = KH$ bo'lishi zarur va yetarli.*

Isbot. *Zaruriyligi.* Aytaylik HK to'plam G gruppaning qism gruppasi bo'lsin. Ixtiyoriy $y \in KH$ elementni olsak, bu element $y = k*h, k \in K, h \in H$ ko'rinishida yoziladi. O'z navbatida $k = e*k$ va $h = h*e$ ekanligidan, xamda e birlik element H va K qism gruppalarning har ikkalasida yotganligidan foydalanib, $k, h \in HK$ ekanligini hosil qilamiz. HK qism gruppa bo'lganligi uchun $k*h \in HK$ bo'ladi. Demak, ixtiyoriy $y \in KH$ uchun $y \in HK$ kelib chiqdi, ya'ni $KH \subseteq HK$.

Endi bu minosabatning ikkinchi tomonini ko'rsatamiz. Ixtiyoriy $z \in HK$ element uchun HK to'plam qism gruppa bo'lganligidan $z^{-1} \in HK$, ya'ni $z^{-1} = h_1 * k_1$ kelib chiqadi. Demak, $z = (z^{-1})^{-1} = (h_1 * k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$, ya'ni $HK \subseteq KH$. Bulardan esa, $HK = KH$ ekanligini hosil qilamiz.

Yetarliligi. Aytaylik, $HK = KH$ bo'lsin. Ixtiyoriy $x, y \in HK$ elementlarni olamiz. U holda $x = h_1 * k_1$ va $y = h_2 * k_2$, bu yerda $h_1, h_2 \in H$, $k_1, k_2 \in K$. $HK = KH$ tenglikdan foydalangan holda, quyidagi munosabatga ega bo'lamiz:

$$x * y^{-1} = h_1 * k_1 * (h_2 * k_2)^{-1} = (h_1 * k_1) * (k_2^{-1} * h_2^{-1}) = (h_1 * k_1) * (h_3 * k_3) =$$

$$h_1 * (k_1 * h_3) * k_3 = h_1 * (h_4 * k_4) * k_3 = (h_1 * h_4) * (k_4 * k_3) \in HK.$$

Bundan esa, HK to'plamning qism gruppa ekanligi kelib chiqadi. □

Endi qism gruppalarning ko'paytmasi HK qism gruppa bo'lishi uchun yana bir zaruriy va yetarlilik shartni keltiramiz. Bu shart berilgan qism gruppalarning birlashmasi orqali beriladi.

1.4.7-teorema. *G gruppaning H va K qism gruppalari ko'paytmasi ham qism gruppa bo'lishi uchun $HK = \langle H \cup K \rangle$ bo'lishi zarur va yetarli.*

Isbot. Aytaylik, HK ko'paytma G gruppaning qism gruppasi bo'lsin. U holda $H \subseteq HK$ va $K \subseteq HK$ bo'lib, $H \cup K \subseteq HK$ bo'ladi. $\langle H \cup K \rangle$ qism gruppa $H \cup K$ to'plamni o'z ichiga oluvchi eng kichik qism gruppa bo'lganligi uchun $\langle H \cup K \rangle \subseteq HK$ kelib chiqadi. Bu munosabatning teskarisi $H, K \subseteq \langle H \cup K \rangle$ ekanligidan va $\langle H \cup K \rangle$ ning qism gruppaligidan kelib chiqadi, ya'ni ixtiyoriy $h \in H$ va $k \in K$ elementlar uchun $h, k \in \langle H \cup K \rangle$ bo'lib, $h * k \in \langle H \cup K \rangle$ bo'ladi. Demak, $HK \subseteq \langle H \cup K \rangle$, bundan esa, $HK = \langle H \cup K \rangle$ kelib chiqadi.

Teorema ikkinchi tomonining isboti esa, $\langle H \cup K \rangle$ ning qism gruppaligidan bevosita kelib chiqadi. □

Quyidagi teoremada chekli H va K qism gruppalarning ko'paytmasi elementlari soni uchun o'rinli bo'lgan formulani keltiramiz.

1.4.8-teorema. *G gruppa uning H va K chekli qism gruppalari berilgan bo'lsin. U holda*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Isbot. Ma'lumki, H va K qism gruppalarning kesishmasi $A = H \cap K$ ham G gruppaning qism gruppasi bo'ladi. Bundan tashqari, A to'plam H ning ham qism gruppasi bo'ladi. Demak, Lagranj teoremasiga ko'ra $|H|$ soni $|A|$ soniga bo'linadi, ya'ni $|H| = |A| \cdot n$ deb olish mumkin. U holda $[H : A] = n$, ya'ni H qism gruppada A ning n ta turli chap qo'shni sinflari mavjud. Ushbu chap qo'shni sinflar oilasini $\{x_1A, x_2A, \ldots, x_nA\}$ ko'rinishda yozib olamiz. U holda $H = \bigcup\limits_{i=1}^{n} x_iA$ bo'lib, A to'plam K gruppaning ham qism gruppasi ekanligidan foydalansak,

$$HK = \Big(\bigcup_{i=1}^{n} x_iA\Big)K = \bigcup_{i=1}^{n} x_iK$$

tenglikka ega bo'lamiz. Endi x_iK va $x_jK = (i \neq j)$ chap qo'shni sinflarning turli xil ekanligini ko'rsatamiz. Faraz qilaylik, $x_iK = x_jK$ bo'lsin, u holda $x_i^{-1} * x_j \in K$. Ikkinchi tomondan esa, $x_i^{-1} * x_j \in H$ bo'lganligi uchun $x_i^{-1} * x_j \in A$ munosabatga ega bo'lamiz. Natijada $x_jA = x_iA$ tenglik kelib chiqadi, bu esa A ning H dagi turli chap qo'shni sinflari sifatida tanlab olinganiga zid. Demak, $x_1K, x_2K, \ldots, x_nK$ to'plamlar turli qo'shni sinflar bo'ladi. U holda

$$|HK| = |x_1K| + |x_2K| + \cdots + |x_nK|$$

bo'lib, $|K| = |x_iK|$, $i = \overline{1, n}$ ekanligidan (1.4.2-natijaga qarang)

$$|HK| = \underbrace{|K| + \cdots + |K|}_{n \text{ marta}} = n|K| = \frac{|H||K|}{|A|} = \frac{|H||K|}{|H \cap K|}$$

tenglikka ega bo'lamiz. □

Quyidagi natija yuqoridagi teoremadan to'g'ridan-to'g'ri kelib chiqadi.

1.4.5-natija. *Agar G gruppaning H va K qism gruppalari berilgan bo'lib, $H \cap K = \{e\}$ bo'lsa, $|HK| = |H||K|$ bo'ladi.*

1.4.2-misol. *Agar G gruppaning tartibi p^n ga teng bo'lsa (p – tub son), u holda uning tartibi p ga teng elementi mavjud ekanligini ko'rsating.*

Yechish. Gruppaning ixtiyoriy $a \neq e$ elementi uchun $H = \langle a \rangle$ siklik qism gruppani qarasak, ushbu siklik qism gruppaning tartibi p^n ning bo'luvchisi bo'ladi. Demak, $|H| = p^m$, bu yerda $0 < m \leq n$. Bundan ixtiyoriy $d \mid p^m$ soni uchun H siklik gruppaning tartibi d ga teng qism gruppasi mavjudligi kelib chiqadi. Ya'ni tartibi p ga teng bo'lgan qism gruppasi ham mavjud. Bu esa, tartibi p ga teng elementi mavjudligini anglatadi. □

1.4.3-misol. *Agar G kommutativ gruppaning tartibi 2 ga teng bo'lgan ikkita turli elementi mavjud bo'lsa, u holda gruppa tartibini 4 ga bo'linishini ko'rsating. Bu natija nokommutativ holda o'rinli emasligiga misol keltiring.*

Yechish. Aytaylik, G kommutativ gruppaning a va b elementlari tartiblari 2 ga teng bo'lsin. U holda $K = \{e, a\}$ va $H = \{e, b\}$ qism gruppalarning ko'paytmasi HK ni qarasak, G kommutativ bo'lganligi uchun $HK = \{e, a, b, ab\}$ ham qism gruppa bo'ladi. Demak, G gruppaning tartibi 4 ga bo'linadi.

Nokommutativ bo'lgan holga misol sifatida S_3 gruppani va uning $a = (1\,2)$, $b = (1\ 3)$ elementlarini keltirish mumkin. Ushbu elementlar turli hil bo'lib, ularning tartiblari 2 ga teng, lekin gruppaning tartibi 4 ga bo'linmaydi. □

1.4.1 Mustaqil ishlash uchun misol va masalalar

1. Quyidagi G gruppalarning H qism gruppalari bo'yicha o'ng qo'shni sinflarini aniqlang.
   - $G = S_3$ va $H = \{e, (2\ 3)\}$.
   - $G = S_3$ va $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$.
   - $G = (\mathbb{Z}, +)$ va $H = n\mathbb{Z}$.
   - $G = (\mathbb{C}, +)$ va $H = \mathbb{R}$.
   - $G = (\mathbb{R}, +)$ va $H = \mathbb{Z}$.
   - $G = (\mathbb{R} \setminus \{0\}, \cdot)$ va $H = \mathbb{R}_+$.
   - $G = (\mathbb{C} \setminus \{0\}, \cdot)$ va $H = \mathbb{R} \setminus \{0\}$.
   - $G = (\mathbb{C} \setminus \{0\}, \cdot)$ va $H = \{z \in \mathbb{C} \mid |z| = 1\}$.
2. $G = GL_n(\mathbb{R})$ va $H = SL_n(\mathbb{R})$ berilgan bo'lsa, ixtiyoriy $g \in GL_n(\mathbb{R})$ matritsa uchun gH qo'shni sinfning elementlari determinanti g matritsaning determinantiga teng matritsalar bo'lishini isbotlang.
3. S_4 gruppaning $H = \{e, (1\,2) \circ (3\,4),\ (1\,4) \circ (3\,2), (1\,3) \circ (2\,4)\}$ qism gruppasi barcha o'ng (chap) qo'shni sinflarini toping.
4. G gruppaning bo'sh bo'lmagan H qism to'plami qism gruppa bo'lishi uchun $HH = H$ bo'lishi zarur va yetarli ekanligini isbotlang.
5. G-gruppa va uning H, K qism gruppalari berilgan bo'lsin. Ixtiyoriy $x \in G$ element uchun $(H \cap K)x = Hx \cap Kx$ tenglik o'rinli ekanligini isbotlang.
6. G-gruppa va uning H, K qism gruppalari berilgan bo'lsin. Ixtiyoriy $a, b \in G$ elementlar uchun $Ha \cap Kb = \emptyset$ bo'lishini yoki $\exists\ c \in G$ uchun $Ha \cap Kb = (H \cap K)c$ tenglik o'rinli bo'lishini isbotlang.

7. Agar G gruppaning H va K qism gruppalari indekslari chekli bo'lsa, u holda $H \cap K$ ham chekli indeksli qism gruppa bo'lishini isbotlang.

8. Tartibi $pq, (p, q) = 1$ ga teng bo'lgan gruppaning ixtiyoriy xosmas qism gruppasi siklik bo'lishini isbotlang.

9. Agar G chekli gruppaning H va K qism gruppalari uchun $|H| > \sqrt{|G|}$ va $|K| > \sqrt{|G|}$ bo'lsa, u holda $|H \cap K| > 1$ ekanligini isbotlang.

10. G chekli gruppaning A va B qism gruppalari uchun, bu yerda $A \subseteq B$, quyidagi tenglik o'rinli bo'lishini isbotlang:
$$[G : A] = [G : B][B : A].$$

11. G chekli gruppaning A va B qism gruppalari uchun quyidagilarni isbotlang:
$$[A : A \cap B] \leq [G : B], \quad [G : A \cap B] \leq [G : A] \cdot [G : B].$$

12. Tartibi 200 dan kichik bo'lgan G gruppa berilgan bo'lsin. Agar G gruppaning tartibi 25 va 35 ga teng bo'lgan qism gruppalari mavjud bo'lsa, u holda G gruppaning tartibini toping.

13. Tartibi 35 ga teng bo'lgan G gruppa berilgan bo'lib, A va B uning mos ravishda tartibi 5 va 7 ga teng bo'lgan qism gruppalar bo'lsa, u holda $G = AB$ ekanligini isbotlang.

1.5 Normal qism gruppalar va faktor gruppalar

Biz avvalgi paragrafda G gruppaning H qism gruppasi chap va o'ng qo'shni sinflari tushunchasini kiritdik. Ma'lumki, agar G kommutativ gruppa bo'lsa u holda chap va o'ng qo'shni sinflar ustma-ust tushadi. Gruppa kommutativ bo'lmagan holda esa ular turli xil bo'lishi ham mumkin. Qism gruppalar ichida chap va o'ng qo'shni sinflari ustma-ust tushadiganlari muhim ahamiyatga ega bo'lib, bunday qism gruppalar normal qism gruppalar deb ataladi. Ushbu paragrafda normal qism gruppalar tushunchasini kiritib, ularning xossalarini o'rganamiz.

1.5.1-ta'rif. *Bizga G gruppa va uning H qism gruppasi berilgan bo'lsin. Agar ixtiyoriy $a \in G$ element uchun $aH = Ha$ tenglik o'rinli bo'lsa, u holda H qism gruppa G gruppaning* ***normal qism gruppasi*** *yoki* ***normal bo'luvchisi*** *deb ataladi va $H \lhd G$ kabi belgilanadi.*

Ta'kidlash joizki, ixtiyoriy G gruppaning kamida ikkita G va $\{e\}$ normal qism gruppalari mavjud bo'lib, gruppaning G va $\{e\}$ dan farq qiluvchi normal qism gruppalariga xosmas yoki notrivial normal qism gruppalari deyiladi.

1.5.2-ta'rif. *Agar G gruppaning xosmas normal qism gruppalari mavjud bo'lmasa, ya'ni normal qism gruppalari faqat $\{e\}$ va G lardan iborat bo'lsa, u holda G gruppa **sodda gruppa** deyiladi.*

Ta'kidlash joizki, kommutativ gruppaning ixtiyoriy qism gruppasi normal qism gruppa bo'ladi. Demak, agar kommutativ gruppa siklik bo'lmasa, u holda uning siklik qism gruppasi mavjud bo'lib, siklik bo'lmagan kommutativ gruppalar sodda bo'lmaydi. Agar chekli siklik gruppaning tartibi murakkab son bo'lsa, u holda uning xosmas qism gruppasi mavjud bo'lib, tartibi tub son bo'lgan siklik gruppalar xosmas qism gruppaga ega emas. Demak, kommutativ bo'lgan holda faqat tartibi tub songa teng bo'lgan siklik gruppalargini sodda gruppalar bo'ladi. Biz quyiroqda kommutativ bo'lmagan A_n juft o'rin almashtirishlar gruppasini sodda ekanligini ko'rsatamiz.

Ushbu teoremada berilgan qism gruppaning normal qism gruppa bo'lishi zaruriy va yetarlilik shartini keltiramiz.

1.5.1-teorema. *G gruppaning H qism gruppasi normal qism gruppa bo'lishi uchun ixtiyoriy $a \in G$ uchun $aHa^{-1} \subseteq H$ bo'lishi zarur va yetarli.*

Isbot. *Zaruriyligi.* Aytaylik, $H \lhd G$ bo'lsin. Ixtiyoriy $x \in aHa^{-1}$ element olsak, bu element $x = a * h * a^{-1}$ kabi yoziladi. $a * h \in aH = Ha$ bo'lganligi uchun, shunday $h_1 \in H$ element mavjudki, $a * h = h_1 * a$ tenglik o'rinli bo'ladi. Bundan esa, $a * h * a^{-1} = h_1 \in H$, ya'ni $aHa^{-1} \subseteq H$ kelib chiqadi.

Yetarliligi. Aytaylik, ixtiyoriy $a \in G$ uchun $aHa^{-1} \subseteq H$ munosabat o'rinli bo'lsin. Ixtiyoriy $x = a*h \in aH$ element uchun $x*a^{-1} = a*h*a^{-1} \in aHa^{-1} \subset H$ bo'lganligi uchun $x * a^{-1} \in H$ kelib chiqadi. Ya'ni, $x * a^{-1} = h_1 \in H$, u holda $x = h_1 * a \in Ha$. Bu esa, $aH \subseteq Ha$ ekanligini anglatadi. Xuddi shunga o'xhab, a element o'rniga a^{-1} elementni qo'yish orqali $Ha \subseteq aH$ munosabatga ega bo'lish mumkin. Demak, $aH = Ha$, ya'ni $H \lhd G$. □

Quyidagi teorema orqali normal qism gruppalarni muhim xossalari keltiramiz.

1.5.2-teorema. *G gruppaning H va K normal qism gruppalari uchun quyidagilar o'rinli:*

1. *$H \cap K$ ham G gruppaning normal qism gruppasi bo'ladi;*
2. *$HK = KH$ bo'lib, HK ham G gruppaning normal qism gruppasi bo'ladi,*
3. *$\langle H \cup K \rangle = HK$.*

Isbot. 1. Gruppaning ixtiyoriy ikkita qism gruppasining keshishmasi yana qism gruppa bo'lishidan $H \cap K$ ham G gruppaning qism gruppasi bo'lishi kelib chiqadi. Endi uning normal qism gruppa ekanligini ko'rsatamiz. Buning uchun ixtiyoriy $g \in G$ element uchun $g(H \cap K)g^{-1} \subseteq H \cap K$ bo‘lishini ko‘rsatish kifoya. Ma’lumki, $g(H \cap K)g^{-1}$ to‘plamning ixtiyoriy elementi $g * a * g^{-1}$, $a \in H \cap K$ ko‘rinishida bo‘ladi. $a \in H \cap K$ ekanligidan $g * a * g^{-1} \in H$ va $g * a * g^{-1} \in K$ munosabatlarga ega bo‘lamiz. Demak, $g * a * g^{-1} \in H \cap K$ ya’ni $g(H \cap K)g^{-1} \subseteq H \cap K$.

2. Dastlab, $HK = KH$ tenglikni isbotlaymiz. Ixtiyoriy $h * k \in HK$ elementni tanlab olaylik, bu yerda $h \in H$ va $k \in K$. U holda $K \lhd G$ ekanligidan $hK = Kh$, demak $\exists\ k_1 \in K$ element mavjudki, $h * k = k_1 * h \in KH$, o‘rinli bo‘ladi, ya’ni $HK \subseteq KH$. Shu usul bilan $KH \subseteq HK$ munosabat ham o‘rinli bo‘lishini ko‘rsatish qiyin emas. Demak, $HK = KH$, u holda 1.4.6-teoremadan HK to‘plam G gruppaning qism gruppasi ekanligi kelib chiqadi. Endi $HK \lhd G$ ekanligini ko‘rsatamiz. H va K normal qism gruppalar bo‘lganligi uchun ixtiyoriy $g \in G$ element uchun $gHg^{-1} \subseteq H$ va $gKg^{-1} \subseteq K$ munosabat o‘rinli. Natijada,

$$g(HK)g^{-1} = g(Hg^{-1}gK)g^{-1} = (gHg^{-1})(gKg^{-1}) \subseteq HK.$$

Demak, 1.5.1-teoremaga ko‘ra $HK \lhd G$.

3. Ushbu teoremaning 2-qismidan ma’lumki $HK \leq G$. U holda 1.4.7-teoremadan $HK = \langle H \cup K \rangle$ tenglikka ega bo‘lamiz. $\square$

Biz avvalgi paragrafda G gruppaning biror H qism gruppasining barcha chap qo‘shni sinflari oilasini $\mathcal{L}$, barcha o‘ng qo‘shni sinflari oilasini esa $\mathcal{R}$ kabi belgilagan edik. Agar H normal qism gruppa bo‘lsa u holda chap va o‘ng go‘shni sinflar ustma ust tushadi. Biz ushbu (chap yoki o‘ng) qo‘shni sinflar oilasini G/H kabi belgilaymiz. Endi ushbu G/H to‘plamda ixtiyoriy $aH, bH \in G/H$ elementlar uchun $aH * bH = (a * b)H$ ko‘rinishida binar amal aniqlaymiz.

1.5.3-teorema. *G gruppaning H normal qism gruppasi berilgan bo‘lsin. U holda $(G/H, *)$ gruppa tashkil qiladi.*

Isbot. Dastlab, G/H to‘plamda aniqlangan $*$ amalini to‘g‘ri aniqlangan ekanligini ko‘rsatamiz. Ya’ni $aH = a_1H$ va $bH = b_1H$ ekanligidan $aH*bH = a_1H*b_1H$ yoki $(a * b)H = (a_1 * b_1)H$ bo‘lishini ko‘rsatamiz. $aH = a_1H$ va $bH = b_1H$ tengliklardan $a = a_1 * h_1$ va $b = b_1 * h_2$ tengliklarni qanoatlantiradigan $h_1, h_2 \in H$ elementlar mavjud ekanligi kelib chiqadi. U holda

$$(a_1 * b_1)^{-1} * (a * b) = b_1^{-1} * a_1^{-1} * a * b = b_1^{-1} * a_1^{-1} * a_1 * h_1 * b_1 * h_2 = b_1^{-1} * h_1 * b_1 * h_2.$$

H normal qism gruppa va $h_1 \in H$ ekanligidan $b_1^{-1}*h_1*b_1*h_2 = (b_1^{-1}*h_1*b_1)*h_2 \in H$, ya’ni $(a_1 * b_1)^{-1} * (a * b) \in H$ munosabatlarga ega bo‘lamiz. Demak, 1.4.1-teoremaning birinchi qismidan $(a*b)H = (a_1*b_1)H$ tenglik kelib chiqadi. Shunday qilib, G/H to‘plamdagi $*$ amal to‘g‘ri aniqlangan bo‘lib, $(G/H, *)$ algebraik sistema bo‘ldi.

Endi biz $*$ amalning assosiativ ekanligini isbotlaymiz. Ixtiyoriy $aH, bH, cH \in G/H$ elementlar uchun

$$(aH) * [(bH) * (cH)] = (aH) * [(b * c)H] = [a * (b * c)]H$$

$$= [(a * b) * c]H = [(a * b)H] * (cH) = [(aH) * (bH)] * (cH).$$

Demak, $*$ assosiativ amal ekan.

Ravshanki, $(G/H, *)$ algebraik sistemada eH element birlik element vazifasini bajaradi. Haqiqatdan ham ixtiyoriy $aH \in G/H$ element uchun

$$(aH) * (eH) = (eH) * (aH) = aH.$$

Ixtiyoriy $aH \in G/H$ elementning teskari esa, $a^{-1}H$ element bo'ladi. Haqiqatan

$$(aH) * (a^{-1}H) = (a^{-1}H) * (aH) = (a * a^{-1})H = eH.$$

Demak, $(G/H, *)$ gruppa tashkil qilar ekan. $\square$

1.5.3-ta'rif. *G gruppaning H normal qism gruppasi yordamida hosil qilingan $(G/H, *)$ gruppaga **faktor gruppa** deb ataladi.*

1.5.1-misol. *$G = (\mathbb{Z}, +)$ gruppani $H = 5\mathbb{Z}$ qism gruppasi normal qism gruppa bo'lib, G/H faktor gruppaning elementlari esa quyidagicha b'oladi*

$$\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z},\ 1 + 5\mathbb{Z},\ 2 + 5\mathbb{Z},\ 3 + 5\mathbb{Z},\ 4 + 5\mathbb{Z}\}.$$

1.5.2-misol. *$G = S_3$ gruppani $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ qism gruppasi normal qism gruppa bo'lib,*

$$G/H = \{H, (1\ 2)H\}$$

bo'ladi.

1.5.3-misol. *G gruppaning indeksi 2 ga teng bo'lgan ixtiyoriy H qism gruppasi normal qism gruppa bo'ladi. Chunki, H qism gruppaning turli chap va o'ng qo'shni sinflari H va $G \setminus H$ dan iborat bo'lib, $a \in H$ elementlar uchun $aH = H = Ha$, $a \notin H$ elementlar uchun esa $aH = G \setminus H = Ha$ bo'ladi.*

Yuqoridagi misoldan S_n gruppaning A_n qism gruppasi normal ekanligini hosil qilamiz. Demak, S_n gruppa xosmas normal qism gruppaga ega, ya'ni u sodda gruppa emas.

Quyidagi misolda esa, A_4 gruppaning normal qism gruppasini keltiramiz.

1.5.4-misol. *A_4 gruppaning $H = \{e, (1\ 2) \circ (3\ 4),\ (1\ 4) \circ (3\ 2), (1\ 3) \circ (2\ 4)\}$ qism gruppasi normal qism gruppa bo'ladi. Demak, A_4 gruppa sodda gruppa emas.*

Endi biz $n \neq 4$ bo‘lgan holda A_n gruppaning sodda ekanligini ko‘rsatamiz. Ma’lumki, $n = 1$ va $n = 2$ bo‘lgan hollarda A_n to‘plam bitta elementdan iborat bo‘ladi, $n = 3$ bo‘lganda esa A_3 to‘plam 3 ta elementdan iborat siklik gruppa bo‘lib, uning sodda ekanligi ravshan.

1.5.4-teorema. *A_n, $n \geq 5$ gruppa sodda gruppadir.*

Isbot. Faraz qilaylik A_n gruppaning $H \neq \{e\}$ normal qism gruppasi mavjud bo‘lsin. Aytaylik, $\pi \in H$, $\pi \neq e$ element $I_n = \{1, 2, \dots n\}$ to‘plamning eng kam sonini o‘zgartiradigan o‘rin almashtirish bo‘lsin. m orqali ushbu π o‘rin almashtirish o‘zgartiradigan elementlar sonini belgilaymiz, ya’ni $m = |\{u \in I_n \mid \pi(u) \neq u\}|$.

Faraz qilaylik $m > 3$ bo‘lsin. Berilgan π o‘rin almashtirishning kesishmaydigan sikllar ko‘paytmasi ko‘rinishidagi ifodasi

$$\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_k$$

bo‘lsin. Quyidagi hollarni qaraymiz.

- **1-hol.** $\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_k$ ifodadagi barcha sikllar transpozitsiyalardan iborat bo‘lsin, ya’ni barcha sikllarning uzunligi 2 ga teng bo‘lsin. U holda π kamida ikkita transpozitsiyaning ko‘paytmasi ko‘rinishida yoziladi, ya’ni $k \geq 2$. Aytaylik, $p_1 = (a\ b)$ va $p_1 = (c\ d)$ bo‘lsin. Ixtiyoriy $f \in I_n \setminus \{a, b, c, d\}$ son olib, $\sigma = (c\ d\ f)$ o‘rin almashtirishni qaraymiz. Ma’lumki, $\sigma \in A_n$ bo‘lib, H normal qism gruppa bo‘lganligi uchun $\sigma \circ \pi \circ \sigma^{-1} \in H$, ya’ni $\pi' = \pi^{-1} \circ (\sigma \circ \pi \circ \sigma^{-1})$ o‘rin almashtirish ham H ga tegishli bo‘ladi. Ushbu π' o‘rin almashtirish uchun $\pi'(a) = a$ va $\pi'(b) = b$ bo‘lib, $\pi'(f) = c$ bo‘ladi. Bundan tahsqari, $\pi(u) = u$ bo‘ladigan $u \notin \{a, b, c, d, f\}$ sonlari uchun $\pi'(u) = u$ bo‘ladi. Bundan esa $\pi' \in H$ o‘rin almashtirish birlik elementdan farqli bo‘lib, π o‘rin almashtirishdan kamroq sonlarni o‘zgartirishi kelib chiqadi, bu esa π eng kam sonni o‘zgartiradigan o‘rin almashtirish ekanligiga zid.

- **2-hol.** $\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_k$ ifodadagi uzunligi 2 dan katta bo‘lgan sikl mavjud. Umimiylikka ziyon yetkazmagan holda π_1 siklning uzunligi 2 dan katta deb olish mumkin, chunki kesishmaydigan sikllar uchun kommutativlik xossasi o‘rinli. Agar $m = 4$ bo‘lsa, u holda $\pi = \pi_1$ bo‘lib, u toq o‘rin almashtirish bo‘lib qoladi, demak, $m \geq 5$ bo‘lishi kerak, ya’ni π o‘rin almashtirish kamida 5 ta sonni o‘zgartiradi. Aytaylik, $\pi_1 = (a\ b\ c\ \dots)$ bo‘lib, $d, f \in I_n \setminus \{a, b, c\}$ sonlari uchun $\sigma = (c\ d\ f)$ o‘rin almashtirishni qaraylik. Bu yerda ham $\pi' = \pi^{-1} \circ (\sigma \circ \pi \circ \sigma^{-1}) \in H$ bo‘lib, $\pi'(a) = a$, $\pi'(b) = \pi^{-1}(d) \neq b$, bo‘ladi. Bundan tahsqari, $\pi(u) = u$ bo‘ladigan $u \notin \{a, b, c, d, f\}$ sonlari uchun $\pi'(u) = u$. Demak, ushbu holda ham π o‘rin almashtirishdan kamroq sonlarni oʻzgartiradigan $\pi' \in H$ oʻrin almashtirish mavjud boʻlar ekan. Bu esa π eng kam sonni oʻzgartiradigan oʻrin almashtirish ekanligiga zid.

Demak, $m > 3$ deb faraz qilib, tahlil qilingan har ikkala holda ham biz ziddiyatga keldik. Bundan esa, $m = 3$ boʻlishi, yaʼni A_n gruppaning ixtiyoriy $H \neq \{e\}$ normal qism gruppasi $\pi = (a\ b\ c)$ sikl koʻrinishidagi oʻrin almashtirishga ega ekanligi kelib chiqadi. Endi bundan foydalanib, $H = A_n$ ekanligini koʻrsatamiz. Ixtiyoriy $\varphi = (u\ v\ w) \in A_n$ sikl uchun $\sigma(a) = u$, $\sigma(b) = v$, $\sigma(c) = w$ shartni qanoatlantiruvchi $\sigma \in S_n$ oʻrin almashtirishni qaraymiz. Tekshirish qiyin emaski, $\sigma \circ \pi \circ \sigma^{-1} = \varphi$ tenglik oʻrinli. Bundan esa, agar $\sigma \in A_n$ boʻlsa, H ning normal qism gruppa ekanligidan $\varphi \in H$ boʻlishi kelib chiqadi.

Agar $\sigma \notin A_n$ boʻlsa, u holda σ toq oʻrin almashtirish boʻlib, $d, f \in I_n \setminus \{a, b, c\}$ sonlari yordamida tuzilgan $\sigma \circ (d\ f)$ oʻrin almashtirish juft boʻladi, yaʻni $\sigma \circ (d\ f) \in A_n$. Quyidagi tengliklardan

$$\varphi = \sigma \circ \pi \circ \sigma^{-1} = \sigma \circ (a\ b\ c) \circ (d\ f) \circ (d\ f)^{-1} \circ \sigma^{-1}$$

$$= \sigma \circ \circ (d\ f) \circ (a\ b\ c) \circ (d\ f)^{-1} \circ \sigma^{-1} = \big(\sigma \circ (d\ f)\big) \circ \pi \circ \big(\sigma \circ (d\ f)\big)^{-1}$$

yana $\varphi \in H$ ekanligiga ega boʻlamiz.

Shunday qilib, biz A_n gruppaning ixtiyoriy $H \neq \{e\}$ normal qism gruppasi barcha $\varphi = (u\ v\ w)$ sikllarni oʻz ichiga olishini koʻrsatdik. Uzunligi 3 ga teng boʻlgan barcha sikllar A_n gruppani hosil qilganligi uchun $H = A_n$ boʻladi (1.2.2-teoremaga qarang). $\square$

1.5.1 Mustaqil ishlash uchun misol va masalalar

1. $GL_n(\mathbb{R})$ gruppaning $SL_n(\mathbb{R})$ qism gruppasi normal ekanligini isbotlang.

2. $H = \{e, (1\ 2) \circ (3\ 4),\ (1\ 4) \circ (3\ 2), (1\ 3) \circ (2\ 4)\}$ toʻplam S_4 gruppaning normal qism gruppasi ekanligini isbotlang.

3. A_4 gruppa uchun shunday H va K qism gruppalarni topingki, H qism gruppa K da normal boʻlib, A_4 da normal bo'lmasin.

4. G gruppa va H uning qism gruppasi boʻlsin. H normal qism gruppa boʻlishi uchun ixtiyoriy $g \in G$ va $h \in H$ elementlar uchun $ghg^{-1} \in H$ boʻlishi zarur va yetarli ekanligini isbotlang.

5. G gruppa va H uning qism gruppasi boʻlsin. Agar ixtiyoriy $a, b \in G$ elementlar uchun $ab \in H$ munosabat oʻrinli boʻlishidan $ba \in H$ kelib chiqsa, u holda $H \lhd G$ ekanligini isbotlang.

6. G gruppa va H, K uning qism gruppalari boʻlsin. Agar $H \lhd G$ boʻlsa, u holda $(H \cap K) \lhd K$ ekanligini isbotlang.

7. G gruppa va uning H normal qism gruppasi uchun faktor gruppa elementlarini toping.
   - $G = (\mathbb{Z}, +)$ va $H = (2\mathbb{Z}, +)$;
   - $G = (\mathbb{Q}, +)$ va $H = (\mathbb{Z}, +)$;
   - $G = (\mathbb{Z}_{12}, +_{12})$ va $H = \langle \overline{4} \rangle$.
8. $G = (\mathbb{R} \setminus \{0\}, \cdot)$ gruppa va uning $H = \mathbb{Q} \setminus \{0\}$ qism gruppasi uchun G/H faktor gruppaning siklik emasligini isbotlang.
9. Agar G gruppaning H va K normal qism gruppalari uchun $H \cap K = \{e\}$ bo‘lsa, u holda ixtiyoriy $h \in H$ va $k \in K$ elementlar uchun $hk = kh$ tenglik o‘rinli bo‘lishini isbotlang.
10. Gruppaning H qism gruppasi va K normal qism gruppalarining ko‘paytmasi qism gruppa bo‘lishini isbotlang.
11. Agar H to‘plam G gruppuning tartibi n ga teng bo‘lgan yagona qism gruppasi bo‘lsa, u holda $H \lhd G$ ekanligini isbotlang.
12. A_4 gruppaning tartibi 6 ga teng bo‘lgan qism gruppasi mavjud emasligini isbotlang.
13. A_4 gruppaning barcha qism gruppalarini toping.

1.6 Sentralizator, normalizator va kommutant

Biz avvalgi mavzuda G gruppaning markazi $Z(G) = \{b \in G \mid a * b = b * a, \ \forall a \in G\}$ to‘plamni aniqlab, uning kommutativ qism gruppa bo‘lishini isbotlagan edik. Ta’kidlash joizki, gruppa markazi nafaqat qism gruppa balki, normal qism gruppa bo‘ladi. Haqiqatdan ham, $\forall a \in Z(G)$ va $\forall b \in G$ uchun $a * b = a * b$ ekanligidan foydalansak, $b^{-1} * a * b = b^{-1} * b * a = a \in Z(G)$ kelib chiqadi. Demak, $Z(G) \lhd G$.

Endi gruppaning sentralizatori va normalizatori tushunchalarini kiritib, ularning xossalarini keltiramiz. Ixtiyoriy $a \in G$ element uchun

$$C(a) = \{b \in G \mid a * b = b * a\}$$

to‘plamni aniqlaymiz. Bu to‘plam a elementning **sentralizatori** deyiladi.

1.6.1-tasdiq. *$C(a)$ to‘plam uchun quyidagilar o‘rinli.*

1) *Ixtiyoriy $a \in G$ element uchun $C(a)$ to‘plam G gruppaning qism gruppasi bo‘ladi;*

2) $Z(G) = \bigcap_{a \in G} C(a);$

3) $C(a) = G$ *bo'lishi uchun* $a \in Z(G)$ *bo'lishi zarur va yetarli;*

4) Ixtiyoriy $a, b \in G$ *elementlar uchun* $C(b^{-1} * a * b) = b^{-1} * C(a) * b;$

Isbot. 1) Agar $b, c \in C(a)$ bo'lsa, u holda $a * b = b * a$ va $a * c = c * a$ ekanligidan,

$$a * (b * c) = (a * b) * c = (b * a) * c = b * (a * c) = b * (c * a) = (b * c) * a$$

tenglikni hosil qilamiz, ya'ni $b * c \in C(a)$.

Bundan tashqari, $a * b = b * a$ tenglikdan $a * b^{-1} = b^{-1} * a$ ekanligi ham osongina kelib chiqadi. Demak, $C(a)$ qism gruppa.

Ikkinchi va uchinchi xossalarning o'rinli ekanligi ta'rifadan to'g'ridan-to'g'ri kelib chiqadi.

4) Ixtiyoriy $x \in C(b^{-1} * a * b)$ element olaylik, u holda $x * (b^{-1} * a * b) = (b^{-1} * a * b) * x$ tenglikning bajarilishi zarur vayetarli. Ushbu tenglik esa $(b * x * b^{-1}) * a = a * (b * x * b^{-1})$ tenglikka teng kuchli. Bundan esa, $b * x * b^{-1} \in C(a) \Leftrightarrow x \in b^{-1} * C(a) * b$ bo'lishini hosil qilamiz. Demak, tenglikning chap tomoni o'ng tomoniga qism, o'z navbatida o'ng tomoni chap tomoniga qism bo'ladi. □

Endi G gruppaning biror M qism to'plami va H qism gruppasi uchun sentralizator va normalizator tushunchalarini kiritamiz.

1.6.1-ta'rif.

$$C_H(M) = \{a \in H \mid ax = xa, \ \forall x \in M\}$$

to'plam M *ning* H *qism gruppa bo'yicha* ***sentralizatori***

$$N_H(M) = \{a \in H \mid aMa^{-1} = M\}$$

to'plam esa ***normalizatori*** *deb ataladi.*

Odatda M qism to'plami va G gruppa bo'yicha sentralizatori va normalizatori qaralganda $C_H(M)$ va $N_G(M)$ belgilashlar o'rniga $C(M)$ va $N(M)$ belgilashlardan foydalaniladi. Agar M to'plam bitta elementdan iborat bo'lsa, u holda sentralizator va normalizatorlar ustma ust tushub, $H = G$ bo'lganda esa, elementning sentaralizatoriga teng bo'ladi.

1.6.2-tasdiq. *Normalizator uchun quyidagilar o'rinli:*

- $N(M)$ *to'plam* G *gruppaning qism gruppasi bo'ladi;*
- *Agar* H *to'plam* G *gruppaning qism gruppasi bo'lsa,* $N(H) = G$ *bo'lishi uchun* $H \lhd G$ *bo'lishi zarur va yetarli;*

- *Agar H to'plam G gruppaning qism gruppasi bo'lsa, u holda $H \lhd N(H)$;*
- *$N(H)$ gruppa G gruppaning H ni normal qism gruppa sifatida o'z ichiga oluvchi eng katta qism gruppasi bo'ladi.*

Bundan tashqari, sentralizator normalizatorning normal qism gruppasi bo'ladi, ya'ni

$$C_H(M) \lhd N_H(M).$$

Endi kommutator va kommutant tushunchalarini kiritamiz. Berilgan G gruppaning a, b elementlari kommutatori deb $aba^{-1}b^{-1}$ elementga aytiladi va $[a, b]$ kabi belgilanadi. Ma'lumki, $[a, b] = e$ bo'lishi uchun $ab = ba$ bo'lishi zarur va yetarli. Bundan tashqari, kommutator uchun quyidagi elementar xossalar o'rinli.

1. $[a, b]^{-1} = [b, a]$;
2. $[a, b]ba = ab$;
3. $c^{-1}[a, b]c = [c^{-1}ac, c^{-1}bc]$;
4. $[ab, c] = a[b, c]a^{-1}[a, c]$;
5. $[c, ab] = [c, a]a[c, b]c^{-1}$.

1.6.2-ta'rif. *G gruppaning barcha kommutatorlaridan hosil qilingan qism gurppaga **kommutant** deb ataladi va $[G, G]$ kabi belgilanadi. Ya'ni $[G, G] = \langle [a, b] \mid a, b \in G \rangle$.*

1.6.3-tasdiq. *Gruppaning kommutanti normal qism gruppa bo'ladi, ya'ni $[G, G] \lhd G$.*

Isbot. $[a, b]^{-1} = [b, a]$ tenglikdan $[G, G]$ to'plamning ixtiyoriy elementi chekli sondagi kommutantlarning ko'paytmasidan iborat ekanligi kelib chiqadi. U holda $g^{-1}(ab)g = (g^{-1}ag)(g^{-1}bg)$ va $g^{-1}[a, b]g = [g^{-1}ag, g^{-1}bg]$ tengliklardan foydalanib, ixtiyoriy $x = [a_1, b_1][a_2, b_2] \dots [a_k, b_k] \in [G, G]$ element uchun

$$g^{-1}xg = g^{-1}[a_1, b_1][a_2, b_2] \dots [a_k, b_k]g = (g^{-1}[a_1, b_1]g)(g^{-1}[a_2, b_2]g) \dots (g^{-1}[a_k, b_k]g)$$

$$= [g^{-1}a_1g, g^{-1}b_1g][g^{-1}a_2g, g^{-1}b_2g] \dots [g^{-1}a_kg, g^{-1}b_kg]$$

ekanligiga ega bo'lamiz. Demak, $g^{-1}xg \in [G, G]$ ya'ni $[G, G] \lhd G$. □

Shuni ta'kidlash lozimki, G gruppaning A va B qism gruppalari uchun ham kommutantni aniqlash mumkin, ya'ni

$$[A, B] = \langle [a, b] \mid a \in A,\ b \in B \rangle.$$

1.6.1-misol. *Agar $A \lhd G$ va $B \lhd G$ bo'lsa, u holda $[A, B] \lhd G$ va $[A, B] \subseteq A \cap B$ ekanligini isbotlang.*

Yechish. $g^{-1}[a, b]g = [g^{-1}ag, g^{-1}bg]$ xossadan $[A, B] \lhd G$ kelib chiqadi.

$A \lhd G$ ekanligidan $[a, b] = aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in A$ kelib chiqadi. Xuddi shunday $[a, b] = aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in B$ bo'lishini hosil qilamiz. Demak, $[A, B] \subseteq A \cap B$. □

1.6.1 Mustaqil ishlash uchun misol va masalalar

1. S_4 gruppaning quyidagi elementlari uchun $C(a)$ sentralizatorni aniqlang:
   - $a = (1\ 2)$;
   - $a = (1\ 2) \circ (3\ 4)$;
   - $a = (1\ 2\ 3\ 4)$.
2. Quyidagi gruppalarning markazlarini toping:
$$S_3, \quad A_4, \quad S_4, \quad GL_n(\mathbb{R}), \quad SL_n(\mathbb{R}).$$
3. $Z(S_n) = \{e\}$ ekanligini isbotlang.
4. Agar $G/Z(G)$ faktor gruppa siklik bo'lsa, u holda G gruppaning kommutativ ekanligini isbotlang.
5. Agar $H \lhd G$ va $|H| = 2$ bo'lsa, u holda $H \subseteq Z(G)$ bo'lishini isbotlang.
6. Quyidagilarni isbotlang
   - $[S_2, S_2] = \{e\}$;
   - $[A_3, A_3] = \{e\}$;
   - $[A_4, A_4] = \{e, (1\ 2) \circ (3\ 4),\ (1\ 4) \circ (3\ 2), (1\ 3) \circ (2\ 4)\}$;
   - $[S_n, S_n] = A_n$;
   - $[A_n, A_n] = A_n,\ n \geq 5$;
   - $[GL_n(\mathbb{R}), GL_n(\mathbb{R})] = SL_n(\mathbb{R})$;
   - $[SL_n(\mathbb{R}), SL_n(\mathbb{R})] = SL_n(\mathbb{R})$.
7. S_3 gruppaning barcha elementlari uchun $[[x, y], z] = e$ tenglik bajariladimi?
8. Agar gruppada $[[x, y], z] = e$ ayniyat bajarilsa, u holda $[x, yz] = [x, y][x, z]$ va $[xy, z] = [x, z][y, z]$ ayniyatlar o'rinli ekanligini isbotlang.

BOB 2

Gruppaning morfizmlari. Izomorfizm haqidagi teoremalar

2.1 Gruppaning gomomorfizmi va izomorfizmi. Keli teoremasi

Ma'lumki, izomorfizm tushunchasi algebraik sistemalarning, hususan gruppalarning asosiy tushunchalaridan hisoblanadi. Chiziqli algebra kursida chiziqli fazolar uchun izomorfizm tushunchasi aniqlangan bo'lib, bir xil o'lchamli barcha chiziqli fazolarning izomorf ekanligi isbotlangan. Ya'ni bir xil o'lchamli chiziqli fazolar bir xil strukturaga ega bo'ladi. Gruppalar uchun ham izomorfizm tushunchasini kiritilishi, ularni tasniflash imkonini beradi. Biz avvalgi mavzularda o'rgangan bir qancha gruppalar biz xil strukturaga ega hisoblanadi. Masalan 4-tartibli Kleyn gruppasi $\mathbf{K}_4 = \{e, a, b, ab\}$ bilan S_4 gruppaning qism gruppasi $G = \{e, (1\ 2)\circ(3\ 4),\ (1\ 4)\circ(3\ 2), (1\ 3)\circ(2\ 4)\}$ bir xil strukturaga ega. Tartibi bir xil bo'lmagan gruppalarni har xil strukturaga ega ekanligini tushunarli. Lekin bir xil tartibli gruppalar ham turli strukturaga ega bo'lishi mumkin. Masalan, $(\mathbb{Z}_4, +)$ va $\mathbf{K}_4$ gruppalari bir xil tartibli bo'lishiga qaramasdan ular turli strukturalarga ega. Chunki, $\mathbb{Z}_4$ gruppa siklik bo'lib, $\mathbf{K}_4$ gruppa siklik emas. Demak, gruppalarni farqlash uchun qandaydir umumiy tushuncha kiritish talab qilinadi. Izomorfizm tushunchasi aynan shunday tushuncha hisoblanib, u orqali gruppalarning tasniflari keltiriladi va hususiyatlari o'rganiladi. Biz dastlab gomomorfizm tushunchasini kiritamiz.

2.1.1-ta'rif. *Bizga $(G, *)$ va $(G_1, *_1)$ gruppalar berilgan bo'lsin. Ixtiyoriy $a, b \in G$ elementlar uchun $f(a * b) = f(a) *_1 f(b)$ shartni qanoatlantiruvchi $f : G \to G_1$ akslantirishga G gruppani G_1 gruppaga o'tkazuvchi* ***gomomorfizm*** *deb ataladi.*

Biz G va G_1 gruppalarning birlik elementlarini mos ravishda e va e_1 kabi belgilaymiz.

2.1.1-misol. *Ixtiyoriy $a \in G$ uchun $f(a) = e_1$ ko'rinishidagi akslantirish gomo-*

morfizm bo'ladi. Haqiqatdan ham, ixtiyoriy $a, b \in G$ elementlar uchun $f(a * b) = e_1 = e_1 *_1 e_1 = f(a) *_1 f(b)$ tenglik o'rinli bo'ladi.

Yuqoridagi misolda keltirilgan gomomorfizmga **trivial gomomorfizm** deb ataladi. Ushbu misoldan ko'rinadiki, ixtiyoriy G gruppani G_1 gruppaga o'tkazuvchi gomomorfizm har doim mavjud. Bundan tashqari, G gruppani o'ziga akslantiruvchi ayniy akslantirish ham gomomorfizmga misol bo'ladi.

Endi gomomorfizmning muhim xossalarini keltirib o'tamiz.

2.1.1-teorema. *G gruppani G_1 gruppaga o'tkazuvchi f gomomorfizm berilgan bo'lsin. U holda qiyidagilar o'rinli:*

1. *$f(e) = e_1$, bu yerda e va e_1 elementlar mos ravishda G va G_1 gruppalarning birlik elementlari;*
2. *ixtiyoriy $a \in G$ uchun $f(a^{-1}) = f(a)^{-1}$ tenglik o'rinli;*
3. *agar $H \leq G$ bo'lsa, u holda $f(H) := \{f(h) |\ h \in H\} \leq G_1$;*
4. *agar $H_1 \leq G_1$ bo'lsa, u holda $f^{-1}(H_1) := \{g \in G |\ f(g) \in H_1\} \leq G$;*
5. *agar $H_1 \lhd G_1$ bo'lsa, u holda $f^{-1}(H_1) \lhd G$;*
6. *agar G kommutativ bo'lsa, u holda $f(G)$ ham kommutativ;*
7. *agar $a \in G$ elementning tartibi n ga teng bo'lsa, u holda $ord(f(a))$ soni n ning bo'luvchisi bo'ladi.*

Isbot. 1. f gomomorfizm ekanligidan, $f(e) *_1 f(e) = f(e * e) = f(e) = f(e) *_1 e_1$ tenglikka ega bo'lamiz. Qisqartirish qoidasiga ko'ra $f(e) = e_1$ tenglik o'rinli.

2. Ixtiyoriy $a \in G$ element uchun $f(a) *_1 f(a^{-1}) = f(a * a^{-1}) = f(e) = e_1$. Shuningdek, $f(a^{-1}) *_1 f(a) = e_1$ tenglikni ham ko'rsatish mumkin. Gruppadagi ixtiyoriy elementning teskari elementi yagona ekanligidan $f(a^{-1}) = f(a)^{-1}$ tenglik kelib chiqadi.

3. $H \leq G$ bo'lsin, u holda $e \in H$ bo'lib, teoremaning birinchi qismida berilgan, $f(e) = e_1$ xossaga ko'ra $e_1 = f(e) \in f(H)$ munosabat o'rinli. Demak, $f(H) \neq \emptyset$. Ixtiyoriy $f(a), f(b) \in f(H)$ elementlarni qaraymiz, bu yerda $a, b \in H$. U holda

$$f(a) *_1 f(b)^{-1} = f(a) *_1 f(b^{-1}) = f(a * b^{-1})$$

kelib chiqadi. $H \leq G$ bo'lganligi uchun $a * b^{-1} \in H$, bundan esa $f(a) *_1 f(b)^{-1} \in f(H)$ kelib chiqadi. Demak, 1.3.1-teoremaga ko'ra $f(H) \leq G_1$.

4. Teoremaning birinchi qismiga ko'ra, $e \in f^{-1}(H_1)$, demak $f^{-1}(H_1) \neq \emptyset$. Ixtiyoriy $f(a), f(b) \in H_1$ elementlar uchun $f(a * b^{-1}) = f(a) *_1 f(b^{-1}) = f(a) *_1 f(b)^{-1} \in H_1$. Demak, $a * b^{-1} \in f^{-1}(H_1)$ va 1.3.1-teoremaga ko'ra $f^{-1}(H) \leq G$.

5. $H_1 \lhd G_1$ ekanligidan ixtiyoriy $f(g) \in G_1$ element uchun $f(g)H_1f(g)^{-1} \subseteq H_1$ bo‘ladi. Biz ixtiyoriy $g \in G$ uchun $gf^{-1}(H_1)g^{-1} \subseteq f^{-1}(H_1)$ munosabat o‘rinli bo‘lishini ko‘rsatish kifoya. $gf^{-1}(H_1)g^{-1}$ to‘plamdan ixtiyoriy a element olsak, bu elementni $a = g * b * g^{-1}$ ko‘rinishda yozish mumkin, bu yerda $b \in f^{-1}(H_1)$. U holda

$$f(a) = f(g * b * g^{-1}) = f(g) *_1 f(b) *_1 f(g^{-1}) = f(g) *_1 f(b) *_1 f(g)^{-1} \in H_1.$$

Demak, $a \in f^{-1}(H_1)$, bundan esa $g * f^{-1}(H_1) * g^{-1} \subseteq f^{-1}(H_1)$ kelib chiqadi. Shunday qilib, $f^{-1}(H_1) \lhd G$.

6. G kommutativ gruppa bo‘lsin. Ixtiyoriy $f(a), f(b) \in f(G)$ elementlar uchun $f(a) *_1 f(b) = f(a * b) = f(b * a) = f(b) *_1 f(a)$ tenglikdan $f(G)$ ham kommutativ ekanligi kelib chiqadi.

7. $(f(a))^n = f(a^n) = f(e) = e_1$ tenglikdan, 1.1.1-teoremaga ko‘ra $ord(f(a))$ soni n ning bo‘luvchisi ekanligi kelib chiqadi. $\square$

2.1.2-ta’rif. *Bizga G va G_1 gruppalar, hamda $f : G \to G_1$ gomomorfizm berilgan bo‘lsin.*

- *Agar f syurektiv bo‘lsa, u holda f akslantirish* ***epimorfizm*** *deyiladi;*
- *Agar f inyektiv bo‘lsa, u holda f akslantirish* ***monomorfizm*** *deyiladi;*
- *Agar f biyektiv bo‘lsa, u holda f akslantirish* ***izomorfizm*** *deyiladi;*
- *G gruppani G_1 gruppaga akslantiruchi epimorfizm mavjud bo‘lsa, u holda G_1 gruppa G ning* ***gomomorf obrazi*** *deyiladi;*

Demak, gruppalarning izomorfizmi bu birinchi gruppani ikkinchi gruppaga o‘tkazuvchi biyektiv (o‘zaro bir qiymatli) gomomorfizm ekan. Agar G gruppani G_1 gruppaga akslantiruvchi izomorfizm mavjud bo‘lsa, u holda G va G_1 gruppalar o‘zaro **izomorf** deyiladi va $G \simeq G_1$ kabi belgilanadi.

Gruppani o‘zini o‘ziga akslantiruvchi izomorfizm esa **avtomorfizm** deb ataladi. Berilgan G gruppaning barcha avtomorfizmlar to‘plamini $Aut(G)$ kabi belgilanadi.

2.1.3-ta’rif. *G va G_1 gruppalar, hamda $f : G \to G_1$ gomomorfizm berilgan bo‘lsin. U holda $\{a \in G \mid f(a) = e_1\}$ to‘plam f gomomorfizmning* ***yadrosi*** *deyiladi va $Kerf$ kabi belgilanadi.*

2.1.1-teoremadan ma’lumki, $e \in \mathrm{Ker} f$ bo‘ladi. Demak, ixtiyoriy gomomorfizmning yadrosi bo‘sh bo‘lmagan to‘plamdan iborat bo‘lar ekan.

2.1.2-teorema. *G gruppani G_1 gruppaga akslantiruvchi f gomomorfizm berilgan bo‘lsin. U holda f monomorfizm bo‘lishi uchun $Kerf = \{e\}$ tenglik o‘rinli bo‘lishi zarur va yetarli.*

Isbot. Faraz qilaylik f monomorfizm bo'lsin, u holda ixtiyoriy $a \in \mathrm{Ker} f$ element uchun $f(a) = e_1 = f(e)$ tenglikka ega bo'lamiz. f inyektiv bo'lganligi uchun $a = e$ kelib chiqadi, ya'ni $\mathrm{Ker} f = \{e\}$.

Endi $\mathrm{Ker} f = \{e\}$ tenglik o'rinli bo'lsin. a va b elementlar uchun $f(a) = f(b)$ tenglikdan

$$f(a * b^{-1}) = f(a) *_1 f(b^{-1}) = f(a) *_1 f(b)^{-1} = e_1$$

kelib chiqadi. Natijada, $a * b^{-1} \in \mathrm{Ker} f = \{e\}$ munosabatga ega bo'lamiz, bu munosabat esa o'z navbatida $a * b^{-1} = e$ tenglikka ekvivalent, ya'ni $a = b$. Demak, f monomorfizm ekan. $\square$

Quyidagi teoremada birinchi gruppani ikkinchi gruppaga o'tkazuvchi ixtiyoriy gomomorfizmning yadrosi birinchi gruppaning normal qism gruppasi bo'lishini ko'rsatamiz.

2.1.3-teorema. *G gruppani G_1 gruppaga akslantiruvchi f gomomorfizm berilgan bo'lsin, u holda $Kerf \lhd G$.*

Isbot. Ma'lumki, ixtiyoriy gomomorfizmning yadrosi bo'sh to'plam emas. Ixtiyoriy $a, b \in \mathrm{Ker} f$ elementlar uchun

$$f(a) *_1 f(b^{-1}) = f(a) *_1 f(b)^{-1} = e_1 * (e_1)^{-1} = e_1 * e_1 = e_1$$

tenglik o'rinli ekanligidan, $a * b^{-1} \in \mathrm{Ker} f$ munosabat kelib chiqadi. Demak, 1.3.1-teoremaga ko'ra $\mathrm{Ker} f$ to'plam G gruppaning qism gruppasi bo'ladi.

Endi $\mathrm{Ker} f$ ning normal qism gruppa ekanligini ko'rsatamiz. Ixtiyoriy $a \in G$ va $h \in \mathrm{Ker} f$ elementlar uchun quyidagi munosabat o'rinli bo'ladi

$$f(a * h * a^{-1}) = f(a) *_1 f(h) *_1 f(a^{-1}) = f(a) *_1 e_1 *_1 f(a)^{-1} = e_1.$$

Bundan esa, $a * h * a^{-1} \in \mathrm{Ker} f$ kelib chiqadi, ya'ni $a \mathrm{Ker} f a^{-1} \subseteq \mathrm{Ker} f$, demak $\mathrm{Ker} f \lhd G$. $\square$

Biz 2.1.1-teoremada H qism gruppaning f gomomorfizmdagi obrazi $f(H)$ yana qism gruppa bo'lishini ko'rsatdik, lekin normal qism gruppa uchun bu munosabat har doim ham o'rinli emas. Quyidagi tasdiqda normal qism gruppaning epimorfizmdagi obrazi yana normal qism gruppa bo'lishini ko'rsatamiz.

2.1.1-tasdiq. *Agar $f : G \to G_1$ epimorfizm berilgan bo'lib, $H \lhd G$ bo'lsa, u holda $f(H) \lhd G_1$ bo'ladi.*

Isbot. H qism gruppa G da normal bo'lganligi uchun, $\forall h \in H$ va $\forall g \in G$ elementlar uchun $g * h * g^{-1} \in H$. Ixtiyoriy $h_1 \in H_1$ va $g_1 \in G_1$ elementlarni olamiz. f gomomorfizm syurektiv bo'lganligi uchun shunday $h \in H$ va $g \in G$ elementlar topilib, $f(h) = h_1$ va $f(g) = g_1$ bo'ladi. Bundan esa,

$$g_1 *_1 h_1 *_1 g_1^{-1} = f(g) *_1 f(h) *_1 f(g)^{-1} = f(g * h * g^{-1}) \in f(H)$$

ekanligini hosil qilamiz. Demak, $f(H)$ to'plam G_1 gruppaning normal qism gruppasi. $\square$

Biz o'tgan paragrafda G gruppa va uning H normal qism gruppasi bo'yicha G/H faktor gruppa tushunchasini kiritgan edik. Berilgan G gruppani G/H faktor gruppaga akslantiruvchi $g : G \to G/H$ akslantirishni quyidagicha aniqlaymiz:

$$g(a) = aH, \quad \forall a \in G.$$

Ta'kidlash joizki, ushbu g akslantirish epimorfizm bo'ladi. Haqiqatdan ham $g : G \to G/H$ akslantirish aniqlanishiga ko'ra syurektiv bo'lib, ixtiyoriy $a, b \in G$ elementlar uchun

$$g(a * b) = (a * b)H = (a * H) * (b * H) = g(a) * g(b).$$

Bundan tashqari $\mathrm{Ker} g = H$, chunki $a \in \mathrm{Ker} g$ ekanligi $g(a) = eH$ tenglikka, bu esa $aH = eH$ tenglikka ekvivalent. Oxirgi tenglik esa $a \in H$ munosabatga teng kuchli ekanligidan $\mathrm{Ker} g = H$ kelib chiqadi.

2.1.4-ta'rif. *Berilgan G gruppani G/H faktor gruppaga akslantiruvchi $g(a) = aH$, $\forall a \in G$ ko'rinishda aniqlangan gomomorfizmga* ***tabiiy gomomorfizm*** *deb ataladi.*

Ushbu teoremada gruppalarda aniqlangan izomorfizmning xossalarini keltiramiz.

2.1.4-teorema. *G gruppani G_1 gruppaga akslantiruvchi f izomorfizm berilgan bo'lsin, u holda quyidagilar o'rinli:*

1. *$f^{-1} : G_1 \to G$ ham izomorfizm;*

2. *G kommutativ bo'lishi uchun G_1 ham kommutativ bo'lishi zarur va yetarli;*

3. *Ixtiyoriy $a \in G$ element uchun $ord(a) = ord(f(a))$ tenglik o'rinli;*

4. *G siklik gruppa bo'lishi uchun G_1 ham siklik bo'lishi zarur va yetarli.*

Isbot. 1. f akslantirish biyektiv ekanligidan, f^{-1} ham biyektiv ekanligi kelib chiqadi. Endi, f^{-1} akslantirishning gomomorfizm ekanligini ko'rsatamiz. Ixtiyoriy $u, v \in G_1$ elementlar uchun $f(a) = u$ va $f(b) = v$ tengliklarni qanoatlantiruvchi $a, b \in G$ elementlar topiladi. Bundan esa, $a = f^{-1}(u)$, $b = f^{-1}(v)$ kelib chiqib, $u *_1 v = f(a) *_1 f(b) = f(a * b)$ ekanligidan, $f^{-1}(u *_1 v) = a * b = f^{-1}(u) * f^{-1}(v)$ tenglikka ega bo'lamiz, ya'ni f^{-1} akslantirish gomomorfizm bo'ladi. Demak, f^{-1} izomorfizm ekan.

2. Aytaylik, G gruppa kommutativ bo'lsin. f akslantirishning syurektiv ekanligidan, ixtiyoriy $u, v \in G_1$ elementlar uchun shunday $a, b \in G$ elementlar topilib, $f(a) = u,\ f(b) = v$ bo'ladi. U holda

$$u *_1 v = f(a) *_1 f(b) = f(a * b) = f(b * a) = f(b) *_1 f(a) = v *_1 u.$$

Demak, G_1 ham kommutativ gruppa.

Va aksincha, agar G_1 kommutativ gruppa bo'lsa, ixtiyoriy $a, b \in G$ elementlar uchun

$$f(a * b) = f(a) *_1 f(b) = f(b) *_1 f(a) = f(b * a).$$

f akslantirish o'zaro bir qiymatli bo'lganligi uchun $a * b = b * a$ kelib chiqadi. Demak, G ham kommutativ gruppa.

3. f akslantirishning gomomorfizmligidan ixtiyoriy $a \in G$ element va $n \in \mathbb{N}$ uchun $f(a^n) = (f(a))^n$ tenglik o'rinli ekanligi kelib chiqadi. Agar $f(b) = e_1$ bo'lsa, u holda f inyektiv ekanligidan $b = e$ tenglik kelib chiqadi. Demak, $a^n = e$ tenglik o'rinli bo'lishi uchun $(f(a))^n = e_1$ tenglik o'rinli bo'lishi zarur va yetarli. Agar a elementni tartibi chekli bo'lsa, u holda $f(a)$ elementning tartibi ham chekli bo'ladi. Faraz qilaylik, $ord(a) = m$ va $ord(f(a)) = n$ bo'lsin, u holda $a^m = e$ ekanligidan $(f(a))^m = e_1$ ekanligi kelib chiqadi. 1.1.1-teoremaga ko'ra n soni m ga karrali va shuningdek, $(f(a))^n = e_1$ ekanligidan m soni n ga karrali ekanligi kelib chiqadi. Demak, $m = n$.

4. Faraz qilaylik, G siklik gruppa bo'lsin, ya'ni $G = \langle a \rangle$. U holda $f(a) \in G_1$ ekanligidan $\langle f(a) \rangle \subseteq G_1$ kelib chiqadi. G_1 gruppadan b element tanlab olsak, u holda f syurektiv akslantirish bo'lgani uchun $f(c) = b$ tenglikni qanoatlantiradigan $c \in G$ element mavjud. G siklik gruppa ekanligini hisobga olsak, $c = a^n$ tenglikni qanoatlantiruvchi n butun son mavjud. Natijada,

$$b = f(c) = f(a^n) = (f(a))^n \in \langle f(a) \rangle.$$

Demak, $G_1 = \langle f(a) \rangle$, ya'ni siklik gruppa. f^{-1} akslantirishning ham izomorfizm ekanligidan G_1 siklik gruppaligidan G gruppaning ham siklik gruppa bo'lishi kelib chiqadi. $\square$

Quyidagi teoremada siklik gruppalarning to'liq tasnifini keltiramiz.

2.1.5-teorema. *Tartibi n ga teng bo'lgan ixtiyoriy siklik gruppa $(\mathbb{Z}_n, +_n)$ gruppaga, ixtiyoriy cheksiz siklik gruppa esa $(\mathbb{Z}, +)$ gruppaga izomorf bo'ladi.*

Isbot. Aytaylik $(G, *)$ tartibi n ga teng bo'lgan siklik gruppa bo'lsin, ya'ni $G = \langle a \rangle$. Quyidagi $f : G \to \mathbb{Z}_n,\ f(a^i) = \bar{i},\ \forall\ i = 0, 1, \ldots, n-1$ akslantirishni qaraymiz. Ma'lumki, bu akslantirish syurektiv bo'ladi. Bundan tashqari, uning inyektiv ekanligi quyidagi munosabatlardan kelib chiqadi:

$$f(a^i) = f(a^j)\ \Rightarrow\ \bar{i} = \bar{j}\ \Rightarrow\ n \mid (j - i)\ \Rightarrow\ a^{i-j} = e\ \Rightarrow\ a^i = a^j.$$

Demak, f o‘zaro bir qiymatli akslantirish ekan. Endi bu akslantirishning izomorfizm ekanligini ko‘rsatamiz:

$$f(a^i * a^j) = f(a^{i+j}) = \overline{i+j} = \overline{i} +_n \overline{j} = f(a^i) +_n f(a^j).$$

Demak, $G \simeq \mathbb{Z}_n$.

Agar $G = \langle a \rangle$ cheksiz gruppa bo‘lsa, u holda $f : G \to \mathbb{Z}$ akslantirishni $f(a^i) = i, \ \forall\, i \in \mathbb{Z}$ ko‘rinishda aniqlaymiz. Bu akslantirish ham o‘zaro bir qiymatli bo‘lib,

$$f(a^i * a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j)$$

ekanligidan uning izomorfizmligi kelib chiqadi, ya’ni $G \simeq \mathbb{Z}$. $\square$

Yuqoridagi teoremadan ushbu natijaga ega bo‘lamiz.

2.1.1-natija. *Bir xil tartibli ikkita siklik gruppa o‘zaro izomorf bo‘ladi.*

Biz endi ixtiyoriy chekli gruppa S_n o‘rin almashtirishlar gruppasining biror qism gruppasiga izomorf bo‘lishi haqidagi Keli teoremasini keltiramiz.

Berilgan G gruppaning ixtiyoriy $a \in G$ elementi uchun quyidagi

$$f_a : G \to G, \quad f_a(b) = a * b, \ \forall\, b \in G$$

akslantirishni aniqlaymiz. Ma’lumki, ushbu akslantirish biyektiv akslantirish bo‘ladi. Haqiqatdan ham, $f_a(b) = f_a(c)$ tenglikdan $a * b = a * c$, bundan esa $b = c$ tenglikning kelib chiqishi bu akslantirishning inyektiv ekanligini, ixtiyoriy $b \in G$ element uchun $f_a(x) = b$ tenglikni qanoatlantiradigan $x = a^{-1} * b$ elementning mavjudligi esa f_a akslantirishning syurektiv ekanligini anglatadi.

Demak, f_a akslantirishni G to‘plamdagi o‘rin almashtirish deb qarash mumkin. Ma’lumki, ixtiyoriy G to‘plamdagi barcha o‘rin almashtirishlar to‘plami $S(G)$ superpozitsiya amaliga nisbatan gruppa tashkil qiladi. Ushbu $(S(G), \circ)$ gruppaning $F(G) = \{f_a |\ a \in G\}$ qism to‘plamini qaraymiz. Quyidagi teoremada $F(G)$ to‘plamning qism gruppa bo‘lishini va uning G gruppaga izomorf bo‘lishini ko‘rsatamiz.

2.1.6-teorema (**Keli teoremasi**). *Ixtiyoriy G gruppa uchun $(F(G), \circ)$ to‘plam gruppa bo‘lib, $F(G) \simeq G$ bo‘ladi.*

Isbot. Dastlab, $(f_a)^{-1} = f_{a^{-1}}$ ekanligini ko‘rsatamiz. Darhaqiqat, ixtiyoriy $b \in G$ element uchun $f_{a^{-1}}(b) = a^{-1} * b$ tenglik o‘rinli. Ikkinchi tomondan esa, $f_a(a^{-1} * b) = b$ ekanligidan $(f_a)^{-1}(b) = a^{-1} * b$ tenglikni hosil qilamiz. Demak, $(f_a)^{-1} = f_{a^{-1}}$.

Endi, $(F(G), \circ)$ to‘plamning gruppa ekanligini, ya’ni bu to‘plam $(S(G), \circ)$ gruppaning qism gruppasi ekanligini ko‘rsatamiz. Ixtiyoriy $f_a, f_b \in F(G)$ va $c \in G$ elementlar uchun

$$(f_a \circ f_b^{-1})(c) = (f_a \circ f_{b^{-1}})(c) = f_a(f_{b^{-1}}(c)) = f_a(b^{-1} * c)$$

$$= a * (b^{-1} * c) = (a * b^{-1}) * c = f_{a*b^{-1}}(c).$$

Demak, $f_a \circ f_b^{-1} = f_{ab^{-1}} \in F(G)$, ya'ni 1.3.1-teoremaga ko'ra $F(G)$ to'plam $S(G)$ gruppaning qism gruppasi ekanligi kelib chiqadi.

Endi $F(G) \simeq G$ ekanligini ko'rsatamiz. Buning uchun $g : G \to F(G)$ akslantirishni quyidagicha aniqlaymiz: $g(a) = f_a$, $\forall\, a \in G$. Bu akslantirish aniqlanishiga ko'ra syurektiv bo'lib, uning inyektiv ekanligi quyidagi tengliklardan kelib chiqadi

$$f_a = f_b \;\Rightarrow\; f_a(c) = f_b(c), \forall c \in G \;\Rightarrow\; a * c = b * c \;\Rightarrow\; a = b.$$

Endi, g akslantirishning gomomorfizm bo'lishini ko'rsatamiz. Ixtiyoriy $c \in G$ element uchun

$$f_{a*b}(c) = (a * b) * c = a * (b * c) = f_a(b * c) = f_a(f_b(c)) = (f_a \circ f_b)(c)$$

tenglik o'rinli, ya'ni $f_{a*b} = f_a \circ f_b$. Shuningdek, $g(a*b) = f_{a*b}$ va $g(a) \circ g(b) = f_a \circ f_b$ ekanligidan $g(a * b) = g(a) \circ g(b)$ tenglikka ega bo'lamiz. Demak, g biyektiv gomomorfizm ekan, ya'ni g izomorfizm. $\square$

Demak, Keli teoremasidan tartibi n ga teng bo'lgan ixtiyoriy gruppa S_n o'rin almashtirishlar gruppasining biror qism gruppasiga izomorf bo'lishi kelib chiqadi.

2.1.1 Mustaqil ishlash uchun misol va masalalar

1. Quyidagi berilgan f akslantirishlar G gruppani G_1 gruppaga o'tkazuvchi gomomorfizm bo'ladimi? Agar gomomorfizm bo'lsa, u holda uning yadrosini toping.

   - $G = (\mathbb{Z}, +)$, $G_1 = (\mathbb{Z}, +)$, $f(a) = 2a$.
   - $G = (\mathbb{Z}, +)$, $G_1 = (\mathbb{Z}, +)$, $f(a) = a + 1$.
   - $G = (\mathbb{R}^+, \cdot)$, $G_1 = (\mathbb{R}^+, \cdot)$, $f(a) = a^2$.
   - $G = (\mathbb{R}, +)$, $G_1 = (\mathbb{R}^+, \cdot)$, $f(a) = 2^a$.
   - $G = (\mathbb{R} \setminus \{0\}, \cdot)$, $G_1 = (\mathbb{R}^+, \cdot)$, $f(a) = |a|$.
   - $G = (\mathbb{C} \setminus \{0\}, \cdot)$, $G_1 = (\mathbb{R}^+, \cdot)$, $f(z) = |z|$.
   - $G = (\mathbb{C} \setminus \{0\}, \cdot)$, $G_1 = (\mathbb{R}^+, \cdot)$, $f(z) = \frac{1}{|z|}$.

2. G gruppani G_1 gruppaga o'tkazuvchi barcha gomomorfizmlarni toping .

   - $G = (\mathbb{Z}, +)$, $G_1 = (\mathbb{Z}, +)$.
   - $G = (\mathbb{Z}, +)$, $G_1 = (\mathbb{Z}_6, +_6)$.
   - $G = (\mathbb{Z}_6, +_6)$, $G_1 = (\mathbb{Z}_4, +_4)$.
   - $G = (\mathbb{Z}_8, +_8)$, $G_1 = (\mathbb{Z}_{12}, +_{12})$.

- $G = (\mathbb{Z}_{20}, +_{20})$, $G_1 = (\mathbb{Z}_{10}, +_{10})$.

3. Quyidagi gruppalarning o'zaro izomorf emasligini ko'rsating.
   - $G = (\mathbb{Q}, +)$ va $G_1 = (\mathbb{R}, +)$.
   - $G = (\mathbb{Z}, +)$ va $G_1 = (\mathbb{R}, +)$.
   - $G = (\mathbb{Q}, +)$ va $G_1 = \mathbb{Q}/\mathbb{Z}$.
   - $G = (\mathbb{Q} \setminus \{0\}, \cdot)$ va $G_1 = (\mathbb{R} \setminus \{0\}, \cdot)$.
   - $G = (\mathbb{R} \setminus \{0\}, \cdot)$ va $G_1 = (\mathbb{C} \setminus \{0\}, \cdot)$.

4. Bo'sh bo'lmagan X to'plamning barcha qism to'plamlaridan tuzilgan $P(X)$ sistema uchun aniqlangan $(P(X), \cup)$ va $(P(X), \cap)$ yarim gruppalar izomorf ekanligini isbotlang.

5. G gruppada aniqlangan $f : G \to G$, $f(a) = a^{-1}$ akslantirish gomomorfizm bo'lishi uchun G kommutativ bo'lishi zarur va yetarli ekanligini isbotlang.

6. $G = \{(-1, 1), *\}$, $a * b = \frac{a+b}{1+ab}$ gruppa $(\mathbb{R}, +)$ gruppaga izomorf ekanligini ko'rsating.

7. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ matritsani $y = \frac{ax+b}{cx+d}$ funksiyaga o'tkazuvchi aklsantirish $GL_2(\mathbb{R})$ gruppani $G = (\{\frac{ax+b}{cx+d}, ad - bc \neq 0\}, \circ)$ gruppaga o'tkazuvchi gomomorfizm bo'ladimi?

8. $(\mathbb{Z}_4, +)$ gruppani va $(\mathbb{U}_5, \cdot)$ gruppaga o'tkazuvchi barcha izomorfizmlarni toping.

9. Agar G, H va K gruppalar berilgan bo'lib, $f : G \to H$ va $g : H \to K$ gomomorfizmlar bo'lsa, u holda $g \circ f$ akslantirish G gruppani K gruppaga o'tkazuvchi gomomorfizm ekanligini ko'rsating.

10. Tartibi 20 ga teng bo'lgan gruppadan, tartibi 70 ga teng bo'lgan gruppaga gomomorfizm mavjudmi?

11. Tartibi 70 ga teng bo'lgan gruppadan, tartibi 20 ga teng bo'lgan gruppaga epimorfizm mavjudmi?

2.2 Diedr va kvaternion gruppalari

Ma'lumki, tartibi tub songa teng bo'lgan ixtiyoriy gruppa siklik bo'lib, bunday gruppalar $\mathbb{Z}_p$ gruppaga izomorf bo'ladi. Hususan, izomorfizm aniqligida tartibi $1, 2, 3, 5$ va 7 ga teng bo'lgan yagona gruppalar mavjud. Biz tartibi 4 va 6 ga teng bo‘lgan gruppalarning tasnifini va tartibi 8 ga teng bo‘lgan nokommutativ gruppalarni keltiramiz. Kichik tartibli gruppalarning to‘liqroq tasnifini esa keyinroq keltiramiz.

Dastlab to‘rtinchi tartibli gruppalarni keltiramiz. Bizga shu paytgacha ikkita to‘rtinchi tartibli gruppa $\mathbb{Z}_4$ va $\mathbf{K}_4$ gruppalar ma‘lum bo‘lib, ularning biri siklik, ikkinchisi siklik emas, demak, ular izomorf emas. Quyidagi teoremada izomorfizm aniqligida $\mathbb{Z}_4$ va $\mathbf{K}_4$ gruppalardan boshqa to‘rtinchi tartibli gruppa mavjud emasligini ko‘rsatamiz.

2.2.1-teorema. *Ixtiyoriy to‘rtinchi tartibli gruppa $\mathbb{Z}_4$ va $\mathbf{K}_4$ gruppalardan biriga izomorf bo‘ladi.*

Isbot. Aytaylik, $G = \{e, a, b, c\}$ to‘rtinchi tartibli gruppa bo‘lib, u siklik gruppa bo‘lsin, u holda $G \simeq \mathbb{Z}_4$ bo‘ladi. Demak, G siklik bo‘lmagan holni qarash kifoya, ya’ni siklik bo‘lmagan to‘rtinchi tartibli gruppani $\mathbf{K}_4$ ga izomorf ekanligini ko‘rsatamiz. G gruppa sisklik bo‘lmaganligi uchun uning to‘rtinchi tarlibli elementi mavjud emas. Ixtiyoriy elementning tartibi gruppaning tartibi bo‘luvchisi bo‘lganligi uchun a, b, c elementlarning tartiblari 2 ga teng bo‘ladi, ya’ni $a^2 = b^2 = c^2 = e$. Endi $a \cdot b$ elementning c ga tengligini ko‘rsatamiz. Faraz qilaylik $a \cdot b = e$ bo‘lsin, u holda $a = a \cdot e = a \cdot (a \cdot b) = a^2 \cdot b = b$ tenglikdan $a = b$ ekanligini hosil qilamiz, bu esa ziddiyat, demak $a \cdot b \neq e$. Agar $a \cdot b = a$ bo‘lsa ham $e = a \cdot a = a \cdot (a \cdot b) = a^2 \cdot b = b$ tenglikdan $e = b$ ekanligi hosil qilib, yana ziddiyatga kelamiz, ya’ni $a \cdot b \neq a$. Xuddi shunga o‘xshab $a \cdot b \neq b$ ham kelib chiqadi, demak, $a \cdot b = c$. Yuqoridagi kabi $b \cdot a = c$ tenglikni ham ko‘rsatish mumkin. Bundan tashqari

$$a \cdot c = c \cdot a = b, \quad b \cdot c = c \cdot b = a$$

tengliklar ham shu usul bilan ko‘rsatilasi. Bu esa, to‘rtinchi tartibli ixtiyoriy siklik bo‘lmagan gruppa $\mathbf{K}_4$ ga izomorf ekanligini bildiradi. □

Endi oltinchi tartibli gruppalarni o‘rganamiz. Ma’lumki, $\mathbb{Z}_6$ siklik gruppa va o‘rin almashtirishlar gruppasi S_3 oltinchi tartibli gruppalar bo‘ladi. Ta’kidlash joizki, S_3 siklik bo‘lmagan nokommutativ gruppadir, shuning uchun $\mathbb{Z}_6$ va S_3 gruppalar izomorf emas. Bundan tashqari S_3 eng kichik tartibli nokommutativ gruppadir. Quyidagi teoremada izomorfizm aniqligida faqat 2 ta oltinchi tartibli gruppa mavjud ekanligini ko‘rsatamiz.

2.2.2-teorema. *Ixtiyoriy oltinchi tartibli gruppa $\mathbb{Z}_6$ va S_3 gruppalardan biriga izomorf bo‘ladi.*

Isbot. Aytaylik G oltinchi tartibli siklik bo‘lmagan gruppa bo‘lsin. G ning tartibi juft son bo‘lganligi uchun unda tartibi 2 ga teng bo‘lgan $a \in G$ element mavjud, ya'ni $a^2 = e$. Agar G gruppaning barcha elementlari ikkinchi tartibli bo'lsa, u holda G kommutativ gruppa bo'lib, uning turli xil a, b elementlari orqali hosil qilingan qism gruppa $\{e, a, b, ab\}$ to'plamdan iborat bo'ladi. Bu esa ziddiyat chunki, 6-tartibli gruppa 4-tartibli qism gruppaga ega emas. Demak, G gruppaning tartibi 2 dan farqli elementi mavjud. G siklik emasligini va barcha elementining tartibi 6 ning bo'luvchisi ekanligini hisobga olsak, tartibi 3 ga teng bo'lgan $b \in G$ element mavjudligini hosil qilamiz. Demak, $ord(a) = 2$ va $ord(b) = 3$. Ma'lumki, $H = \{e, b, b^2\}$ to'plam G gruppaning indeksi 2 ga teng bo'lgan qism gruppasi bo'lib, ixtiyoriy gruppaning indeksi 2 ga teng qism gruppasi normal bo'lganligi uchun $H \lhd G$ bo'ladi. $a \notin H$ ekanligidan $G = H \cup aH$ kelib chiqadi, ya'ni $G = \{e, b, b^2, a, a \cdot b, a \cdot b^2\}$. Endi $b \cdot a$ va $b^2 \cdot a$ elementlarni qaraymiz. Buning uchun H ning normal ekanligidan foydalansak, $a^{-1} \cdot b \cdot a \in H$ kelib chiqadi. Demak, $a^{-1} \cdot b \cdot a$ element e, b va b^2 elementlardan biriga teng bo'lishi kerak.

Agar $a^{-1} \cdot b \cdot a = e$ bo'lsa, u holda $b = a \cdot e \cdot a^{-1} = e$ bo'ladi. Bu esa ziddiyat. Agar $a^{-1} \cdot b \cdot a = b$ bo'lsa, u holda $b \cdot a = a \cdot b$ bo'lib, $ord(a \cdot b) = ord(a)ord(b) = 6$ kelib chiqadi. Bu ham G ning siklik emasligiga zid. Demak $a^{-1} \cdot b \cdot a = b^2$, ya'ni $b \cdot a = a \cdot b^2$ ekanligi kelib chiqadi. Xuddi shunga o'xshab, $b^2 \cdot a = a \cdot b$ tenglikka ega bo'lamiz. Ya'ni G gruppa $\{e, b, b^2, a, a \cdot b, a \cdot b^2\}$ elementlardan iborat bo'lib,

$$a^2 = b^3 = e, \quad b \cdot a = a \cdot b^2, \quad b^2 \cdot a = a \cdot b$$

bo'ladi.

Shunday qilib, biz ixtiyoriy oltinchi tartibli siklik bo'lmagan gruppa yagona gruppaga izomorf bo'lishini, hususan S_3 ga izomorf bo'lishini ko'rsatdik. $\square$

Quyidagi misolda ikkita hosil qiluvchi elementga ega bo'lgan n-darajali diedr gruppasini keltiramiz.

2.2.1-misol. *Ikkita a, b hosil qiluvchi elementlarga ega bo'lib $ord(a) = 2, ord(b) = n, b \cdot a = a \cdot b^{-1}$ bo'lgan $D_n = \langle a, b\rangle$ gruppa n-darajali diedr gruppasi deyiladi, bu yerda $n \geq 3$. Ta'kidlash joiski, D_n gruppa tartibi $2n$ ga teng bo'lgan nokommutativ gruppa bo'lib, uning elementlari quyidagilardan iborat bo'ladi*

$$D_n = \{e, b, b^2, \dots, b^{n-1}, a, a \cdot b, a \cdot b^2, \dots, a \cdot b^{n-1}\}.$$

Ma'lumki, D_3 oltinchi tartibli gruppa bo'lib, $D_3 \simeq S_3$ bo'ladi. D_4 esa sakkisinchi tartibli nokommutativ gruppa bo'ladi. Ya'ni D_4 gruppaning elementlari

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

bo'lib, $a^2 = b^4 = e$, $ba = ab^3$, $b^2a = ab^2$, $b^3a = ab$ bo'ladi.

Demak, $ord(a) = ord(b^2) = ord(ab) = ord(ab^2) = ord(ab^3) = 2$ va $ord(b) = ord(b^3) = 4$.

Quyidagi misolda $GL_2(\mathbb{R})$ ikkinchi tartibli xosmas kvadrat matrisalar gruppasining D_4 gruppaga izomorf boʻlgan qism gruppasi mavjudligini koʻrsatamiz.

2.2.2-misol. *Aytaylik $G \subseteq GL_2(\mathbb{R})$ quyidagi matrisalardan hosil qilunivchi gruppa boʻlsin*

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

U holda $ord(A) = 2$ va $ord(B) = 4$. Bundan tashqari

$$BA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

va

$$AB^3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Demak, $BA = AB^3$, bundan esa, G gruppa 4-tartibli diedr gruppasi boʻlishi kelib chiqadi.

Endi S_4 oʻrin almashtirishlar gruppasining 4-tartibli diedr qism gruppasini koʻrsatamiz.

2.2.3-misol. *S_4 gruppaning $a = (24)$ va $b = (1234)$ elementlarini qaraylik, Ma'lumki,*

$$a^2 = e, \; b^2 = (13) \circ (24), \; b^3 = (1432), \; b^4 = e, \; b \circ a = a \circ b^3.$$

Bundan esa, $G = \langle a, b \rangle$ gruppa 4-tartibli diedr gruppasi ekanligi kelib chiqadi.

Endi D_4 diedr gruppasining barcha qism gruppalarini aniqlaymiz. Lagranj teoremasiga koʻra, D_4 ning xosmas qism gruppalarining tartibi faqat 2 va 4 ga teng boʻlishi mumkin. Tekshirish qiyin emaski,

$$H_1 = \{e, a\}, \; H_2 = \{e, b^2\}, \; H_3 = \{e, a \cdot b\}, \; H_4 = \{e, a \cdot b^2\}, \; H_5 = \{e, a \cdot b^3\}$$

gruppalar D_4 ning tartibi 2 ga teng qism gruppalari boʻladi. Uning tartibi 4 ga teng qism boʻlgan qism gruppalari esa quyidagilardan iborat

$$T_1 = \{e, b, b^2, b^3\},$$

$$T_2 = \{e, a, b^2, a \cdot b^2\},$$

$$T_3 = \{e, a \cdot b, b^2, a \cdot b^3\}.$$

Endi yana bir tartibi 8 ga teng boʻlgan gruppa Q_8 kvaternion gruppasini qaraymiz.

2.2.1-ta'rif. *Hosil qiluvchi elementlari a, b bo'lib,*

$$ord(a) = 4, \ a^2 = b^2 \ va \ b \cdot a = a^3 \cdot b$$

*bo'lgan G gruppaga **kvaternion** gruppasi deyiladi.*

Boshqacha aytganda, kvaternion gruppasi $\{1, i, j, k, -1, -i, -j, -k\}$ elementlardan tashkil topib, $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$ shartlarni qanoatlantiruvchi gruppadir.

Quyidagi misolda matrisalar gruppasining Q_8 gruppaga izomorf bo'lgan qism gruppasini ko'rsatamiz.

2.2.4-misol. *Aytaylik $G \subseteq GL_2(\mathbb{C})$ quyidagi matrisalardan hosil qilunivchi gruppa bo'lsin*

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \ va \ B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

U holda $ord(A) = 4$ va

$$A^2 = B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Bundan tashqari,

$$BA = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

va

$$A^3B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Ya'ni, $BA = A^3B$, demak $G = \langle A, B \rangle$ kvaternion gruppasi bo'ladi.

Kvaternion gruppasining elementlari umimiy ko'rinishi qiyidagicha bo'lib,

$$Q_8 = \{e, a, a^2, a^3, b, a \cdot b, a^2 \cdot b, a^3 \cdot b\},$$

$ord(a^2) = 2$ va $ord(a) = ord(a^3) = ord(b) = ord(a \cdot b) = ord(a^2 \cdot b) = ord(a^3 \cdot b) = 4$ bo'ladi.

Endi Q_8 gruppaning barcha qism gruppalarini aniqlaymiz. Takidlash joizki, uning xosmas qism gruppalari quyidagilardan iborat bo'ladi

$$H_1 = \{e, a^2\}, \quad H_2 = \{e, a, a^2, a^3\},$$

$$H_3 = \{e, a \cdot b, a^2, a^3 \cdot b\}, \quad H_4 = \{e, b, a^2, a^2 \cdot b\}.$$

$[Q_8 : H_2] = [Q_8 : H_3] = [Q_8 : H_4] = 2$ bo'lganligi uchun H_2, H_3 va H_4 qism gruppalar Q_8 ning normal bo'luvchilari bo'ladi.

Bundan tashqari, H_1 ning ham normal qism gruppa bo'lishini tekshirish qiyin emas. Demak, Q_8 kvaternion gruppaning ixtiyoriy qism gruppasi normal bo'lar ekan.

Ushbu teoremada izomorfizm aniqligida D_4 va Q_8 dan boshqa tartibi 8 ga teng bo'lgan nokommutativ grupppa mavjud emasligini isbotlaymiz.

2.2.3-teorema. *Izomorfizm aniqligida tartibi* 8 *ga teng bo'lgan 2 ta nokommutativ gruppa mavjud.*

Isbot. Biz yuqorida D_4 va Q_8 gruppalarning tartibi 8 ga teng bo'lgan nokommutativ grupppalar ekanligini aytib o'tdik. Bundan tashqari Q_8 gruppada tartibi 4 ga teng bo'lgan elementlar 6 ta bo'lsa, D_4 gruppada esa bunday elementlar 2 tani tashkil qiladi. Demak, D_4 va Q_8 gruppalar izomorf emas.

Endi tartibi 8 ga teng bo'lgan ixtiyoriy G nokommutativ gruppani olaylik. $|G|$ juft son bo'lganligi uchun, G da tartibi 2 ga teng bo'lgan $u \in G$ element mavjud, ya'ni $u^2 = e$. Ma'lumki, G gruppaning qolgan elementlari tartibi $2, 4$ va 8 ga teng bo'lishi mumkin. Agar gruppaning ixtiyoriy elementining kvadrati e ga teng bo'lsa, u holda G kommutativ gruppa bo'ladi. Bundan tashqari, gruppada tartibi 8 ga teng element mavjud bo'lsa, u holda G siklik bo'ladi. Demak, G gruppada tartibi 4 ga teng bo'lgan $a \in G$ element mavjud.

Aytaylik, $H = \{e, a, a^2, a^3\}$ bo'lsin, u holda $[G : H] = 2$ bo'lganligi uchuun $H \lhd G$ bo'ladi. Demak, $b \notin H$ element uchun $G = H \cup Hb$ bo'lib $H \cap Hb = \emptyset$ bo'ladi. Ya'ni,

$$G = \{e, a, a^2, a^3, b, a \cdot b, a^2 \cdot b, a^3 \cdot b\} = \langle a, b \rangle.$$

$H \lhd G$ bo'lganligi uchun $b \cdot a \cdot b^{-1} \in H$ bo'ladi. Bundan esa, $b \cdot a \cdot b^{-1}$ element e, a, a^2 va a^3 elementlardan biriga teng bo'lishi kelib chiqadi. Qiyida bu element e, a, a^2 elementlarga teng bo'lmasligini ko'rsatamiz. Chunki, agar

- $b \cdot a \cdot b^{-1} = e$ bo'lsa, u holda $a = e$,
- $b \cdot a \cdot b^{-1} = a$ bo'lsa, u holda $a \cdot b = b \cdot a$, ya'ni G kommutativ,
- $b \cdot a \cdot b^{-1} = a^2$ bo'lsa, u holda $a^2 = e$.

Ya'ni har uchala holda ham ziddiyatga keldik. Demak, $b \cdot a \cdot b^{-1} = a^3$ bo'ladi, ya'ni $b \cdot a = a^3 \cdot b$.

Bundan tashqari, $|G/H| = 2$ bo'lganligi uchun $ord(Hb) = 2$ bo'lib $b^2 \in H$ ekanligi kelib chiqadi. Yuqoridagi kabi b^2 ham H ning 4 ta elementidan biriga teng bo'lishi mumkin. Agar $b^2 = a$ yoki $b^2 = a^3$ bo'lsa, u holda $ord(b) = 8$ bo'lib, G gruppa kommutativ bo'lib qoladi. Bu esa, ziddiyat. Demak, $b^2 = e$ yoki $b^2 = a^2$ bo'lishi kerak. Ushbu ikkala holda ham $G = \langle a, b \rangle$ gruppa nokommutativ gruppa bo'lib, mos ravishda D_4 va Q_8 gruppalarga izomorf bo'ladi. $\square$

2.2.5-misol. *D_4 gruppaning markazini toping.*

Yechish: Ma'lumki, ixtiyoriy gruppaning markazi uning qism gruppasi bo'ladi. D_4 gruppa oltita D_4, $\{e\}$, $H_2 = \{e, b^2\}$, $T_1 = \{e, b, b^2, b^3\}$, $T_2 = \{e, a, b^2, a \cdot b^2\}$, va $T_3 = \{e, a \cdot b, b^2, a \cdot b^3\}$ normal qism gruppalarga ega bo'lganligi uchun $Z(D_4)$ shu oltita qism gruppalardan biriga teng bo'ladi. $a \cdot b \neq b \cdot a$, ekanligidan $a, b \notin Z(D_4)$ kelib chiqadi. Demak $Z(D_4)$ markaz D_4, T_1 va T_2 qism gruppalarga teng emas. Agar $a \cdot b \in Z(D_4)$ bo'lsa, u holda $b = a \cdot (a \cdot b) = (a \cdot b) \cdot a = (b^3 \cdot a) \cdot = b^3$ bo'lib, $b^2 = e$, hosil bo'ladi. Bu esa, ziddiyat, demak $Z(D_4) \neq T_3$. Ushbu

$$b^2 \cdot a = b \cdot (b \cdot a) = b \cdot (a \cdot b^3) = a \cdot b^6 = a \cdot b^2$$

tenglikdan b^2 elementning a bilan o'rin almashishi kelib chiqadi. Bundan esa, $b^2 \in Z(D_4)$ ekanligini ko'rish qiyin emas, demak, $Z(D_4) = \{e, b^2\}$. $\square$

2.2.1 Mustaqil ishlash uchun misol va masalalar

1. D_3 diedr gruppasini S_3 gruppaga o'tkazuvchi barcha izomorfizmlarni toping.

2. Q_8 gruppaning markazini toping.

3. $GL_4(\mathbb{R})$ – to'rtinchi tartibli xosmas matritsalar gruppasining Q_8 gruppaga izomorf qism gruppasini toping.

4. G gruppani G_1 gruppaga o'tkazuvchi barcha gomomorfizmlarni toping

   - $G = \mathbb{Z}_4$, $G_1 = \mathbf{K}_4$;
   - $G = \mathbf{K}_4$, $G_1 = \mathbb{Z}_4$;
   - $G = S_3$, $G_1 = \mathbb{Z}_6$;
   - $G = \mathbb{Z}_6$, $G_1 = S_3$;
   - $G = \mathbb{Z}_8$, $G_1 = D_4$;
   - $G = \mathbb{Z}_8$, $G_1 = Q_8$;
   - $G = Q_8$, $G_1 = D_4$;
   - $G = D_4$, $G_1 = Q_8$.

5. G gruppani G_1 gruppaga o'tkazuvchi barcha epimorfizmlarni toping

   - $G = D_4$, $G_1 = \mathbf{K}_4$;
   - $G = Q_8$, $G_1 = \mathbb{Z}_4$;
   - $G = Q_8$, $G_1 = \mathbb{Z}_2$;
   - $G = D_4$, $G_1 = \mathbb{Z}_2$.

2.3 Izomorfizm haqidagi teoremalar

Ushbu mavzuda gruppalarning izomorfizmlari bilan bo‘g‘liq bo‘lgan, izomorfizm va moslik teoremalari deb nomlanuvchi natijalarni keltiramiz. Ushbu teoremalar gruppaning gomomorfizmlari va faktor gruppalar orasidagi bo‘glanishlarni ifodalovchi teoremalar hisoblanadi.

2.3.1-teorema. *Bizga G gruppani G_1 gruppaga o‘tkazuvchi $f : G \to G_1$ epimorfizm berilgan bo‘lsin. Agar G gruppaning H normal qism gruppasi uchun $H \subseteq \mathrm{Ker} f$ munosabat o‘rinli bo‘lsa, u holda $g : G \to G/H$ syurektiv tabiiy gomomorfizm uchun $f = h \circ g$ shartni qanoatlantiruvchi yagona $h : G/H \to G_1$ epimorfizm mavjud. Shuningdek, h inyektiv bo‘lishi uchun $H = \mathrm{Ker} f$ tenglik o‘rinli bo‘lishi zarur va yetarli.*

CHIZMA CHIZILADI

Isbot. $h : G/H \to G_1$ akslantirishni ixtiyoriy $aH \in G/H$ uchun $h(aH) = f(a)$ ko‘rinishida aniqlaymiz. Dastlab, bu akslantirishning to‘g‘ri aniqlangan ekanligini ko‘rsatamiz. Ya’ni, $aH = bH$ bo‘lsa, u holda $b^{-1} * a \in H$ bo‘ladi. O‘z navbatida $H \subseteq \mathrm{Ker} f$ ekanligidan,

$$f(b^{-1} * a) = e_1 \;\Rightarrow\; f(a) = f(b) \;\Rightarrow\; h(aH) = h(bH)$$

kelib chiqadi. Demak, h akslantirish to‘g‘ri aniqlangan.

Ixtiyoriy a element uchun, $(h \circ g)(a) = h(g(a)) = h(aH) = f(a)$ tenglik o‘rinli ekanligidan, $h \circ g = f$ tenglik kelib chiqadi.

Endi, $h : G/H \to G_1$ akslantirishning epimorfizm bo‘lishini ko‘rsatamiz. $f : G \to G_1$ akslantirish syurektiv bo‘lganligi uchun $h : G/H \to G_1$ ham syurektiv bo‘ladi. Shuningdek,

$$h((aH) * (bH)) = h((a * b)H) = f(a * b) = f(a) *_1 f(b) = h(aH) *_1 h(bH).$$

Demak, h akslantirish epimorfizm ekan.

Endi bu shartlarni qanoatlartiruvchi epimorfizm yagona ekanligini ko‘rsatamiz. Faraz qilaylik, boshqa $h_1 : G/H \to G_1$ epimorfizm mavjud bo‘lib, $f = h_1 \circ g$ bo‘lsin. U holda, ixtiyoriy $aH \in G/H$ element uchun $h(aH) = f(a) = (h_1 \circ g)(a) = h_1(g(a)) = h_1(aH)$ tenglik o‘rinli. Demak, $h = h_1$.

Endi teoremaning ikkinchi qismini, ya’ni h inyektiv akslantirish bo‘lishi uchun $H = \mathrm{Ker} f$ bo‘lishi zarur va yetarli ekanligini isbotlaymiz.

Faraz qilaylik, h inyektiv akslantirish bo‘lsin. U holda $\mathrm{Ker} f \subseteq H$ ekanligi quyidagi munosabatlardan kelib chiqadi

$$\forall a \in \mathrm{Ker} f \;\Rightarrow\; f(a) = e_1 \;\Rightarrow\; h(aH) = e_1 = h(eH) \;\Rightarrow\; aH = eH \;\Rightarrow\; a \in H.$$

Shuningdek, teorema shartiga ko‘ra $H \subseteq \mathrm{Ker} f$ bo‘lganligi uchun $H = \mathrm{Ker} f$ tenglikni hosil qilamiz.

Endi $H = \mathrm{Ker} f$ tenglik o‘rinli bo‘lsa, h akslantirishning inyektiv bo‘lishini ko‘rsatamiz. Agar $h(aH) = h(bH)$ bo‘lsa, u holda

$$f(a) = f(b) \;\Rightarrow\; f(b^{-1} * a) = e_1 \;\Rightarrow\; b^{-1} * a \in \mathrm{Ker} f = H \;\Rightarrow\; aH = bH.$$

Demak, h inyektiv akslantirish. □

Demak, 2.3.1-teoremada $H = \mathrm{Ker} f$ bo‘lsa, u holda h izomorfizm bo‘lar ekan, ya’ni $G/\mathrm{Ker} f \simeq G_1$ munosabat o‘rinli bo‘ladi. Ushbu natija gruppalar nazariyasida muhim o‘rin egallab, uni gruppalar uchun **gomomorfizmlarning asosiy teoremasi** yoki gruppalar uchun **izomorfizm haqidagi birinchi teorema** deb nomlanadi.

2.3.2-teorema (**izomorfizm haqidagi birinchi teorema**). *Agar f akslantirish G gruppani G_1 gruppaga o‘tkazuvchi gomomorfizm bo‘lsa, u holda $G/\mathrm{Ker} f \simeq f(G)$ bo‘ladi.*

2.3.1-teoremadan G gruppaning har bir G_1 gomomorf obraziga yagona N normal qism gruppa mos kelib, $G/N \simeq G_1$ bo‘lishi kelib chiqadi. Masalan, S_3 gruppaning uchta gomomorf obrazi, shuningdek uchta normal qism gruppasi mavjud. Uning gomomorf obrazlari S_3, $\mathbb{Z}_2$ va $\mathbb{Z}_1$ bo‘lsa, normal qism gruppalari esa, $\{e\}$, A_3 va S_3 lardan iborat bo‘lib,

$$S_3 \simeq S_3/\{e\}, \quad \mathbb{Z}_2 \simeq S_3/A_3, \quad \mathbb{Z}_1 \simeq S_3/S_3.$$

2.3.3-teorema. *Aytaylik G_1 gruppa G gruppaning gomomorf obrazi bo‘lsin, u holda quyidagilar o‘rinli.*

1. *Agar G siklik gruppa bo‘lsa, u holda G_1 ham siklik gruppa bo‘ladi.*

2. *Agar G kommutativ gruppa bo‘lsa, u holda G_1 ham kommutativ gruppa bo‘ladi.*

3. *Agar G_1 gruppada tartibi n bo‘lgan element mavjud bo‘lib, G chekli gruppa bo‘lsa, u holda G gruppada tartibi n ga teng bo‘lgan element topiladi.*

Isbot. Teorema 1 va 2-qismlarining isboti 2.1.1-teoremaning 6-qismidan kelib chiqadi. Shuning uchun, biz faqat teoremaning 3-qismini isbotlaymiz.

Aytaylik, $a_1 \in G_1$ elementning tartibi n ga teng bo‘lsin. Agar $n = 1$ bo‘lsa, u holda $e \in G$ biz qidirayotgan element bo‘ladi. Endi, $n > 1$ bo‘lgan holni qaraylik. $f : G \to G_1$ akslantirish syurektiv bo‘lganligi sababli, $f(a) = a_1$ shartni qanoatlantiruvchi $a \in G$ element topiladi. G gruppaning tartibi chekli bo‘lganligi sababli, $ord(a)$ ham chekli bo‘ladi, hamda 2.1.1-teoremaning 7-qismidan $ord(a_1)$

soni $ord(a)$ ning bo‘luvchisi ekanligi kelib chiqadi, ya’ni $n \mid ord(a)$. U holda $ord(a) = nt,\ t \in \mathbb{N} \ \Rightarrow\ t < ord(a) \ \Rightarrow\ a^t \neq e$. Agar $b = a^t$ deb olsak, u holda $b^n = e$ bo‘lib, 1.1.1-teoremaga ko‘ra

$$ord(b) = ord(a^t) = \frac{ord(a)}{\text{EKUB}(t, ord(a))} = \frac{nt}{t} = n.$$

□

2.3.4-teorema (izomorfizm haqidagi ikkinchi teorema). *Bizga G gruppa va uning $H,\ K$ qism gruppalari berilgan bo‘lsin. Agar $K \lhd G$ bo‘lsa, u holda*

$$H/(H \cap K) \simeq (HK)/K.$$

Isbot. Ixtiyoriy $h \in H$ element uchun $f : H \to (HK)/K$ akslantirishni $f(h) = hK$ ko‘rinishida aniqlaymiz. Ushbu f akslantirish gomomorfizm bo‘ladi, chunki ixtiyoriy $h_1, h_2 \in H$ elementlar uchun

$$f(h_1 * h_2) = (h_1 * h_2)K = (h_1K) * (h_2K) = f(h_1) * f(h_2).$$

Ixtiyoriy $xK \in (HK)/K$ element uchun $x = h * k$ tenglikni qanoatlantiruvchi $h \in H$ va $k \in K$ elementlar topiladi. Shuningdek,

$$xK = (h * k)K = (hK) * (kK) = hK = f(h)$$

tenglik o‘rinli ekanligidan f akslantirishning syurektivligidan kelib chiqadi, ya’ni $f(H) = (HK)/K$. U holda gomomorfizmning birinchi teoremasiga ko‘ra,

$$H/\text{Ker}f \simeq (HK)/K$$

munosabat o‘rinli bo‘ladi.

Endi, $\text{Ker}f = H \cap K$ ekanligini ko‘rsatamiz. Aniqlanishiga ko‘ra

$$\text{Ker}f = \{h \in H \mid f(h) \text{ element } (HK)/K \text{ ning birlik elementi}\}.$$

Bundan esa,

$$\text{Ker}f = \{h \in H \mid hK = K\} = \{h \in H \mid h \in K\} = H \cap K$$

kelib chiqadi. Demak, $H/(H \cap K) \simeq (HK)/K$. □

2.3.5-teorema. *G gruppani G_1 gruppaga akslantiruvchi f epimorfizm berilgan bo‘lib, $H \lhd G$ uchun* $\text{Ker}f \subseteq H$ *bo‘lsin. Agar $g : G \to G/H$ va $g_1 : G_1 \to G_1/f(H)$ tabiiy gomomorfizmlar bo‘lsa, u holda $g_1 \circ f = h \circ g$ shartni qanoatlantiruvchi yagona $h : G/H \to G_1/f(H)$ izomorfizm mavjud.*

CHIZMA CHIZILADI

Isbot. Teoremani isbotlash uchun $\mathrm{Ker}(g_1 \circ f) = H$ tenglik o‘rinli ekanligi ko‘rsatish kifoya. Chinki, bu tenglikdan 2.3.1-teoremaga ko‘ra, yagona $h : G/H \to G_1/f(H)$ izomorfizm mavjud ekanligi kelib chiqadi.

Ixtiyoriy $a \in H$ element uchun $f(a) \in f(H) = \mathrm{Ker}\ g_1$ ekanligidan $(g_1 \circ f)(a) = g_1(f(a))$ element $G_1/f(H)$ faktor gruppaning birlik elementiga tengligi kelib chiqadi. Ya’ni, $a \in \mathrm{Ker}(g_1 \circ f)$, bundan esa $H \subseteq \mathrm{Ker}(g_1 \circ f)$ kelib chiqadi.

Agar $a \in \mathrm{Ker}(g_1 \circ f)$ bo‘lsa, u holda $g_1(f(a))$ element $G_1/f(H)$ gruppaning birlik elementi bo‘ladi, bundan esa $f(a) \in \mathrm{Ker}\ g_1 = f(H)$ kelib chiqadi. Natijada, $f(a) = f(b)$ tenglikni qanoatlantiradigan $b \in H$ element topiladi, u holda

$$f(a) = f(b) \ \Rightarrow\ f(a * b^{-1}) = e_1 \ \Rightarrow\ a * b^{-1} \in \mathrm{Ker}\ f \subseteq H,$$

ya’ni

$$a = (a * b^{-1}) * b \in H \ \Rightarrow\ \mathrm{Ker}(g_1 \circ f) \subseteq H.$$

Demak, $\mathrm{Ker}(g_1 \circ f) = H$. □

2.3.6-teorema (izomorfizm haqidagi uchinchi teorema). *G gruppa va uning H_1, H_2 $(H_1 \subseteq H_2)$ normal qism gruppalari berilgan bo‘lsin. U holda*

$$(G/H_1)/(H_2/H_1) \simeq G/H_2.$$

Isbot. 2.3.5-teorema shartidagi G_1, H va $G_1/f(H)$ gruppalar o‘rniga mos ravishda G/H_1, H_2 va $(G/H_1)/(H_2/H_1)$ gruppalarni qo‘yib, f sifatida $f : G \to G/H_1$ tabiiy gomomorfizmni qarasak, $f(H_2) = H_2/H_1$ tenglik o‘rinli bo‘lib, teoremaning isboti kelib chiqadi, ya’ni

CHIZMA CHIZILADI

□

Aytaylik, G gruppani G_1 guppaga akslantiruvchi f epimorfizm berilgan bo‘lsin. G gruppaning ushbu gomomorfizm yadrosini o‘z ichiga oluvchi barcha qism gruppalari oilasini $\Omega(G, \mathrm{Ker} f)$ kabi, G_1 gruppaning barcha qism gruppalari oilasini esa $\Omega(G_1)$ kabi belgilaymiz.

2.3.7-teorema (Moslik teoremasi). *Agar G gruppani G_1 guppaga akslantiruvchi f epimorphizm berilgan bo‘lsa, u holda ushbu epimorfizm yordamida o‘zaro bir qiymatli $f^* : \Omega(G, \mathrm{Ker} f) \to \Omega(G_1)$ moslik o‘rnatish mumkin. Bundan tashqari, agar $f^*(H) = K$ bo‘lsa, u holda $H \lhd G$ bo‘lishi uchun $K \lhd G_1$ bo‘lishi zarur va yetarli.*

Isbot. $f^* : \Omega(G, \mathrm{Ker}f) \to \Omega(G_1)$ akslantirishni quyidagicha aniqlaymiz:

$$\forall H \in \Omega(G, \mathrm{Ker}f) \text{ uchun } f^*(H) = \{f(h) \mid h \in H\}.$$

Dastlab, ushbu akslantirishning syurektiv ekanligini ko‘rsatamiz. Aytaylik, $K \in \Omega(G_1)$ bo‘lsin. Ushbu K qism gruppaning proobrazi $f^{-1}(K)$ ni H orqali belgilaylik. Ma’lumki, H to‘plam G gruppaning qism gruppasi bo‘lib, u $\mathrm{Ker}f$ ni o‘z ichiga oladi, ya’ni $H \in \Omega(G, \mathrm{Ker}f)$. Bundan tashqari, $f^*(H) = K$ ekanligidan, f^* akslantirishning syurektiv ekanligi kelib chiqadi. Endi ushbu akslantirishning inyektiv ekanligini ko‘rsatamiz. Aytaylik $H_1, H_2 \in \Omega(G, \mathrm{Ker}f)$ bo‘lib $f^*(H_1) = f^*(H_2)$ bo‘lsin. U holda ixtiyoriy $h \in H_1$ uchun shunday $h_2 \in H_2$ element topilib, $f(h_1) = f(h_2)$ bo‘ladi. Bundan esa, $f(h_1 \cdot h_2^{-1}) = e_1$ ekanligi, ya’ni $h_1 \cdot h_2^{-1} \in \mathrm{Ker}f \subseteq H_2$ kelib chiqadi. $h_1 = (h_1 \cdot h_2^{-1}) \cdot h_2 \in H_2$ ekanligidan esa $H_1 \subseteq H_2$ munosabatga ega bo‘lamiz. Xuddi shunday, $H_2 \subseteq H_1$ munosabatni ham hosil qilish mumkin. Demak, $H_1 = H_2$, ya’ni f^* o‘zaro bir qiymatli akslantirish.

Endi teoremaning ikkinchi qismini isbotlaymiz. Aytaylik, $f^*(H) = K$ bo‘lib, $H \lhd G$ bo‘lsin. U holda $a \in G$ va $h \in K$ elementlar uchun $a \cdot h \cdot a^{-1} \in H$ bo‘ladi. Ixtiyoriy $f(a) \in G_1$ va $f(h) \in K$ elementlar uchun $f(a) \cdot f(h) \cdot f(a)^{-1} = f(a \cdot h \cdot a^{-1}) \in K$ bo‘ladi. Demak, K to‘plam G_1 gruppaning normal qism gruppasi. Va aksincha, agar $K \in \Omega(G_1)$ bo‘lsa, u ixtiyoriy $a \in G$ va $h \in K$ elementlar uchun $f(a \cdot h \cdot a^{-1}) = f(a) \cdot f(h) \cdot f(a)^{-1} \in K$, ya’ni $a \cdot h \cdot a^{-1} \in H$. Demak, $H \lhd G$. □

Yuqoridagi teoremada agar G_1 gruppa o‘rniga G gruppaning biror normal qism gruppasi N bo‘yicha G/N faktor gruppasini olib, $g : G \to G/N$ tabiiy gomomorfizmni qarasak, quyidagi natijaga ega bo‘lamiz.

2.3.1-natija. *G/N faktor gruppaning barcha qism gruppalari K/N ko‘rinishida bo‘ladi, bu yerda $N \subseteq K$ va $K \leq G$. Bundan tashqari, $K/N \lhd G/N$ bo‘lishi uchun $K \lhd G$ bo‘lishi zarur va yetarli.*

Isbot. Aytaylik, $g : G \to G/N$ tabiiy gomomorfizm bo‘lsin, ya’ni $a \in G$ uchun $g(a) = aN$. U holda $\mathrm{Ker}g = N$ bo‘lib, 2.3.7-teoremaga ko‘ra G gruppaning N ni o‘z ichiga oluvchi qism qruppalari oilasi bilan G/N to‘plamning qism qruppalari oliasi o‘rtasida o‘zaro bir qiymatli g^* moslik mavjud. Ya’ni ixtiyoriy $K \subseteq G/N$ qism gruppa uchun $H \subseteq G$, qism gruppa topilib,

$$K = g^*(H) = \{g(a) \mid a \in K\} = K/N.$$

Teoremaning ikkinchi qismi esa 2.3.7-teoremadan to‘g‘ridan to‘g‘ri kelib chiqadi. □

Quyidagi misolda moslik teoremasining izohini keltiramiz.

2.3.1-misol. *Aytaylik, $(\mathbb{Z}, +)$ va $(\mathbb{Z}_{12}, +_{12})$ gruppalar berilgan bo‘lib, $f : \mathbb{Z} \to \mathbb{Z}_{12}$ epimorfizm $f(n) = [n]$ kabi aniqlangan bo‘lsin. U holda $Kerf = \langle 12 \rangle$ bo‘lib,*

$$\Omega(\mathbb{Z}, Kerf) = \{\langle 12 \rangle, \langle 6 \rangle, \langle 4 \rangle, \langle 3 \rangle, \langle 2 \rangle, \mathbb{Z}\},$$

va

$$\Omega(\mathbb{Z}_{12}) = \{\langle\overline{0}\rangle, \langle\overline{6}\rangle, \langle\overline{4}\rangle, \langle\overline{3}\rangle, \langle\overline{2}\rangle, \mathbb{Z}\}$$

bo'ladi. $f^* : \Omega(\mathbb{Z}, Kerf) \to \Omega(\mathbb{Z}_{12})$ *akslantirish esa, quyidagicha aniqlanadi*

$$f^*(\langle 12\rangle) = \langle[0]\rangle, \quad f^*(\langle 3\rangle) = \langle[3]\rangle,$$

$$f^*(\langle 2\rangle) = \langle[2]\rangle, \quad f^*(\langle 6\rangle) = \langle[6]\rangle,$$

$$f^*(\langle 4\rangle) = \langle[4]\rangle, \quad f^*(\mathbb{Z}) = \mathbb{Z}_{12}.$$

Endi biz G gruppani o'zini o'ziga o'tkazuvchi izomorfizmlarni, ya'ni avtomorfizmlarni qaraymiz. Ma'lumki, avtomorfizmlar to'plami $Aut(G)$ kabi belgilanib, unda superpozitsiya amali binar amal bo'ladi. Bundan tashqari, $\forall f, g, h \in Aut(G)$ uchun

$$(f \circ g) \circ h = f \circ (g \circ h)$$

tenglik o'rinli, ya'ni superpozitsiya amali uchun assosiativlik bajariladi. Ayniy akslantirish $i_G \in Aut(G)$ esa birlik element vazifasini bajarsa, $\forall f \in Aut(G)$ uchun f^{-1} avtomorfizm teskari element bo'ladi. Demak, $(Aut(G), \circ)$ gruppa bo'lar ekan.

Endi ushbu avtomorfizmlar gruppasining qism gruppasi bo'ladigan ichki avtomorfizmlar tushunchasini kiritamiz. Ixtiyoriy $a \in G$ element uchun $\theta_a : G \to G$ akslantirishni

$$\theta_a(b) = a \cdot b \cdot a^{-1}, \ \forall b \in G$$

kabi aniqlaymiz. Ta'kidlash joizki, ushbu θ_a akslantirish avtomorfizm bo'ladi.

Haqiqatdan ham, $\theta_a(c\cdot d) = a\cdot(c\cdot d)\cdot a^{-1} = (a\cdot c\cdot a^{-1})\cdot(a\cdot d\cdot a^{-1}) = \theta_a(c)\circ\theta_a(d)$ tenglikdan uning gomomorfizm ekanligi kelib chiqadi. Ixtiyoriy $c \in G$ uchun $c = \theta_a(a^{-1} \cdot c \cdot a)$ tenglikdan θ_a akslantirishning syurektiv ekanligi,

$$\theta_a(c) = \theta_a(d) \Rightarrow a \cdot c \cdot a^{-1} = a \cdot d \cdot a^{-1} \Rightarrow c = d$$

munosabatdan esa, inyektivligi kelib chiqadi. Demak, $\theta_a \in Aut(G)$.

2.3.1-ta'rif. θ_a *ko'rinishidagi avtomorfizmga ichki avtomorfizm defiladi.* G *gruppaning barcha ichki aftomorfizmlar to'plami* $Inn(G)$ *kabi belgilanadi.*

2.3.1-tasdiq. *Ichki avtomorfizmlar quyidagi xossalarga ega:*

1) $\theta_a \circ \theta_b = \theta_{a\cdot b}$;

2) $(\theta_a)^{-1} = \theta_{a^{-1}}$;

3) ixtiyoriy $\varphi \in Aut(G)$ *uchun* $\varphi \circ \theta_a \circ \varphi^{-1} = \theta_{\varphi(a)}$.

Isbot. 1) Ixtiyoriy $a, b \in G$ elementlar uchun

$$(\theta_a \circ \theta_b)(c) = \theta_a(\theta_b(c)) = \theta_a(b \cdot c \cdot b^{-1})$$
$$= a \cdot (b \cdot c \cdot b^{-1}) \cdot a^{-1} = (a \cdot b) \cdot c \cdot (a \cdot b)^{-1} = \theta_{a \cdot b}(c).$$

Demak, $\theta_a \circ \theta_b = \theta_{ab}$.

2) $\theta_a \circ \theta_{a^{-1}} = \theta_{a \cdot a^{-1}} = \theta_e = i_G$ va $\theta_{a^{-1}} \circ \theta_a = \theta_{a^{-1} \cdot a} = \theta_e = i_G$ ekanligidan $(\theta_a)^{-1} = \theta_{a^{-1}}$ kelib chiqadi.

3) Ixtiyoriy $\varphi \in Aut(G)$ uchun

$$(\varphi \circ \theta_a \circ \varphi^{-1})(b) = \varphi(\theta_a(\varphi^{-1}(b))) = \varphi(a \cdot \varphi^{-1}(b) \cdot a^{-1})$$
$$= \varphi(a) \cdot \varphi(\varphi^{-1}(b)) \cdot \varphi(a^{-1}) = \varphi(a) \cdot b \cdot (\varphi(a))^{-1} = \theta_{\varphi(a)}(b).$$

Demak, $\varphi \circ \theta_a \circ \varphi^{-1} = \theta_{\varphi(a)}$. □

2.3.8-teorema. *G gruppaning barcha ichki aftomorfizmlari $Inn(G)$ aftomorfizmlar gruppasi $Aut(G)$ ning normal qism gruppasi bo'ladi, ya'ni $Inn(G) \lhd Aut(G)$.*

Isbot. Ayniy akslantirish uchun $i_G = \theta_e$ ekanligidan $i_G \in Inn(G)$ kelib chiqadi. Ixtiyoriy $\theta_a, \theta_b \in Inn(G)$ uchun $\theta_a \circ \theta_b^{-1} = \theta_a \circ \theta_{b^{-1}} = \theta_{a \cdot b^{-1}} \in Inn(G)$ bo'lganligi uchun $Inn(G)$ qism gruppa bo'ladi. Va nihoyat, $\forall \varphi \in Aut(G)$ uchun $\varphi \circ \theta_a \circ \varphi^{-1} = \theta_{\varphi(a)} \in Inn(G)$ ekanligidan $Inn(G) \lhd Aut(G)$ kelib chiqadi. □

Ta'kidlash joizki, G gruppaning markazi $Z(G) = \{b \in G \mid a * b = b * a, \ \forall a \in G\}$ normal qism gruppa bo'lib, $G/Z(G)$ faktor gruppa esa G gruppaning ichki avtomorfizmlar gruppasiga izomorf bo'ladi. Ya'ni quyidagi teorema o'rinli.

2.3.9-teorema. *G gruppa berilgan bo'lib, $Z(G)$ uning markazi bo'lsin. U holda $G/Z(G) \simeq Inn(G)$.*

Isbot. G gruppadan $Inn(G)$ gruppaga $f : G \to Inn(G)$ akslantirishni quyidagi aniqlaymiz

$$f(a) = \theta_a, \quad \forall a \in G.$$

Ma'lumki, ushbu akslantirish syurektiv bo'lib, u gomomorfizm bo'ladi. Haqiqatdan ham, ixtiyoriy $a_1, a_2 \in G$ uchun

$$f(a_1 \cdot a_2) = \theta_{a_1 \cdot a_2} = \theta_{a_1} \circ \theta_{a_2} = f(a_1) \circ f(a_2).$$

Endi ushbu gomomorfizmning yadrosini topamiz:

$$\begin{aligned}
\mathrm{Ker} f &= \{a \in G \mid f(a) = i_G\} \\
&= \{a \in G \mid \theta_a = i_G\} \\
&= \{a \in G \mid \theta_a(b) = i_G(b), \ \forall b \in G\} \\
&= \{a \in G \mid a \cdot b \cdot a^{-1} = b, \ \forall b \in G\} \\
&= \{a \in G \mid a \cdot b = b \cdot a, \ \forall b \in G\} \\
&= Z(G).
\end{aligned}$$

Demak, $\mathrm{Ker}f = Z(G)$ bo'lar ekan. U holda izomorfizm haqidagi birinchi teoremaga ko'ra $G/Z(G) \simeq Inn(G)$ kelib chiqadi. $\square$

2.3.2-misol. $(\mathbb{Z}, +)$ *gruppaning barcha gomomorf obrazlarini toping.*

Yechish. Aytaylik H gruppa $(\mathbb{Z}, +)$ gruppaning gomomorf obrazi bo'lsin, ya'ni $f : \mathbb{Z} \to H$ epimorfizm mavjud. U holda izomorfizmning birinchi teoremasiga ko'ra $\mathbb{Z}/\mathrm{Ker}f \simeq H$ bo'ladi. $\mathrm{Ker}f$ yadro $\mathbb{Z}$ gruppaning normal qism gruppasi bo'lganligi uchun, $\mathrm{Ker}f = n\mathbb{Z}$ bo'ladi, bu yerda $n \geq 0$. Demak, $H \simeq \mathbb{Z}/n\mathbb{Z}$. Ma'lumki, $\mathbb{Z}/n\mathbb{Z}$ gruppa $n = 0$ da $\mathbb{Z}$ ga $n > 0$ da esa $\mathbb{Z}_n$ ga izomorf bo'ladi. Shunday qilib, $\mathbb{Z}$ gruppaning gomomorf obrazlari $\mathbb{Z}$ va $\mathbb{Z}_n$ ekanligiga ega bo'lamiz.

2.3.3-misol. *Agar chekli G gruppadan $\mathbb{Z}_8$ gruppaga epimorfizm mavjud bo'lsa, u holda G indeksi 4 va 2 ga teng bo'lgan qism gruppalarga ega ekanligini isbotlang.*

Yechish: Aytaylik $f : G \to \mathbb{Z}_8$ epimorfizm bo'lsin, u holda izomorfizmning birinchi teoremasiga ko'ra $G/\mathrm{Ker}f \simeq \mathbb{Z}_8$. Demak, $G/\mathrm{Ker}f$ tartibi 8 ga teng bo'lgan siklik gruppa bo'ladi. Bundan esa, $G/\mathrm{Ker}f$ tartibi 4 va 2 ga teng bo'lgan H_1 va H_2 normal qism gruppalarga ega ekanligi kelib chiqadi. Moslik teoremasiga ko'ra esa G gruppaning N_1 va N_2 nornal qism gruppalari mavjud bo'lib,

$$\mathrm{Ker}f \subseteq N_1,\ N_1/\mathrm{Ker}f = H_1 \quad \text{va} \quad \mathrm{Ker}f \subseteq N_2,\ N_2/\mathrm{Ker}f = H_2$$

bo'ladi. Bundan esa,

$$[G : N_1] = \frac{[G : \mathrm{Ker}f]}{[N_1 : \mathrm{Ker}f]} = \frac{8}{4} = 2,$$

$$[G : N_2] = \frac{[G : \mathrm{Ker}f]}{[N_2 : \mathrm{Ker}f]} = \frac{8}{2} = 4$$

kelib chiqadi.

2.3.4-misol. *D_4 gruppaning ichki avtomorfizmlar gruppasi $Inn(D_4)$ ni toping.*

Yechish: 2.3.9-teoremaga ko'ra $Inn(D_4) \cong D_4/Z(D_4)$ bo'lib, o'z navbatida $|Z(D_4)| = 2$ ekanligidan $D_4/Z(D_4)$ faktor gruppaning tartibi 4 ga tengligi kelib chiqadi, ya'ni

$$D_4/Z(D_4) = \{e \cdot Z(D_4), a \cdot Z(D_4), b \cdot Z(D_4), (a \cdot b) \cdot Z(D_4)\}.$$

Bundan esa, $b^2 \in Z(D_4)$, $a^2 = e$ va $(a \cdot b)^2 = e$ ekanligidan $D_4/Z(D_4)$ faktor gruppaning birlik elementdan farqli barcha elementlarining tartibi 2 ga teng bo'lishi kelib chiqadi. Demak, $D_4/Z(D_4) \simeq \mathbf{K}_4$ ekanligini hosil qilamiz.

2.3.1 Mustaqil ishlash uchun misol va masalalar

1. Aytaylik, $G = (\mathbb{R}^*, \cdot)$ noldan farqli haqiqiy sonlar to'plamining multiplikativ gruppasi va uning $T = \{1, -1\}$ normal bo'luvchisi berilgan bo'lsin. $G/T \simeq (\mathbb{R}^+, \cdot)$ ekanligini isbotlang, bu yerda $(\mathbb{R}^+, \cdot)$ barcha musbat haqiqiy sonlar to'plamining multiplikativ gruppasi.

2. Ixtiyoriy n natural son uchun $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ ekanligini isbotlang.

3. Isbotlang: $4\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}_3$.

4. Isbotlang: $8\mathbb{Z}/56\mathbb{Z} \simeq \mathbb{Z}_7$.

5. Ixtiyoriy o'zaro tub m va n natural sonlari uchun $m\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}_n$ ekanligini isbotlang.

6. Shunday G gruppa va uning A va B normal qism gruppalariga misol keltiringki, $A \simeq B$, va $G/A \not\simeq G/B$ bo'lsin.

7. $\mathbb{Z}_8$ gruppa $\mathbb{Z}_{15}$ gruppaning gomomorf obrazi emasligini ko'rsating.

8. Agar $\mathbb{Z}_{15}$ gruppa G gruppaning gomomorf obrazi bo'lsa, u holda G gruppa indeksi 5 va 3 ga teng bo'lgan normal qism gruppalarga ega ekanligini isbotlang.

9. Isbotlang:

   - $Aut(\mathbb{Z}_5) \simeq \mathbb{Z}_4$.
   - $Aut(\mathbb{Z}_8) \simeq \mathbf{K}_4$, bu yerda $\mathbf{K}_4$ – 4-tartibli Kleyn gruppasi.
   - $Aut(\mathbb{Z}_n) \simeq \mathbb{U}_n$.

10. $Inn(S_3) \simeq Aut(S_3) \simeq S_3$ ekanligini isbotlang.

11. $Aut(S_4)$ ni toping.

12. $Aut(\mathbf{K}_4)$ ni toping.

13. $Aut(D_4)$ ni toping.

14. $Aut(Q_8)$ ni toping.

15. $(\mathbb{Q}, +)$ gruppaning barcha avtomorfizmlarini toping.

16. Agar G gruppaning markazi faqat birlik elementdan iborat bo'lsa, u holda $Aut(G)$ gruppaning markazi ham birlik avtomorfizmdan iborat ekanligini isbotlang.

17. D_4 gruppaning shunday H va K qism gruppalarini topingki, $K \lhd H$ va $H \lhd D_4$ bo‘lib, lekin K qism gruppa D_4 da normal bo‘lmasin.

18. Q_8 gruppaning indeksi 2 ga teng bo‘lgan 3 ta qism gruppalar birlashmasi ko‘rinishida tasvirlang .

19. D_4 gruppaning barcha gomomorf akslarini toping.

20. Q_8 gruppaning barcha gomomorf akslarini toping.

21. Ixtiyoriy qism gruppasi normal bo‘lgan, kommutativ bo‘lmagan gruppaga misol keltiring.

2.4 Gruppalarning to‘gri va yarim to‘g‘ri ko‘paytmasi

Ushbu paragrafda gruppalarning to‘g‘ri ko‘paytmasi tushunchasini kiritamiz. Gruppalarning to‘g‘ri ko‘paytmasi yuqori tartibli gruppalarni kichik tartibli gruppalar orqali o‘rganish imkonini beradi. Bu orgali gruppalarning ba’zi umumiy xossalarini ham o‘rganish mumkin. Dastlab, quyidagi misolni qarab chiqamiz.

2.4.1-misol. *Bizga $(G_1, *_1)$ va $(G_2, *_2)$ gruppalar berilgan bo‘lsin. Ushbu to‘plamlarning $G_1 \times G_2$ dekart ko‘paytmasida quyidagicha binar amal aniqlaymiz.*

$$(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2).$$

Tekshirish qiyin emaski, $G_1 \times G_2$ dekart ko‘paytma ushbu amalga nisbatan gruppa tashkil qiladi. Haqiqatdan ham, ushbu amal binar amal ekanligi va assosiativlik shartining bajarilishini osingina ko‘rish mumkin. $G_1 \times G_2$ to‘plamda (e_1, e_2) element birlik element vazifasini bajaradi, bu yerda e_1 va e_2 mos ravishda G_1 va G_2 gruppalarning birlik elementlari. Ixtiyoriy (a_1, a_2) elementning teskarisi esa, (a_1^{-1}, a_2^{-1}) bo‘ladi, bu yerda a_1^{-1} va a_2^{-1} elementlar mos ravishda G_1 va G_2 gruppalardagi a_1 va a_2 elementlarning teskarisi.

Endi yuqoridagi misolni umumlashtirgan holda ixtiyoriy sondagi $G_1, G_2, \ldots, G_n$ gruppalarning tashqi to‘g‘ri ko‘paytmasi tushunchasini kiritamiz. Buning uchun

$$G = G_1 \times G_2 \times \cdots \times G_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in G_i\}$$

to‘plamda $*$ binar amalni

$$(a_1, a_2, \ldots, a_n) * (b_1, b_2, \ldots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n)$$

kabi aniqlaymiz, bu yerda shartli ravishda G_i gruppalarning barchasidagi binar amallar bir xil $\cdot$ kabi belgilangan. G to‘plam ushbu amalga nisbatan gruppa tashkil qilib, u $G_1, G_2, \ldots, G_n$ gruppalarning **tashqi to‘g‘ri ko‘paytmasi** deb ataladi.

Ta’kidlash joizki, gruppalarning tashqi to‘g‘ri ko‘paytmasining birlik elementi $(e_1, e_2, \ldots, e_n)$ bo‘lib, $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_n^{-1}, \ldots, a_n^{-1})$ bo‘ladi. Quyidagi teoremada gruppalarning tashqi to‘g‘ri ko‘paytmasining ba’zi muhim xossalarini keltiramiz.

2.4.1-teorema. *Aytaylik, $G_1, G_2, \ldots, G_n$ gruppalar berilgan bo‘lib, G ularning tashqi to‘g‘ri ko‘paytmasi bo‘lsin. $H_i = \{(e_1, e_2, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) \mid a_i \in G_i\}$ to‘plamlar uchun quyidagilar o‘rinli*

1) *Ixtiyoriy $i (1 \leq i \leq n)$ uchun H_i to‘plam G gruppaning normal qism gruppasi bo‘ladi.*

2) *Ixtiyoriy $a \in G$ elementni yagona ravishda $a = h_1 * h_2 * \cdots * h_n$ kabi yozish mumkin, bu yerda $h_i \in H_i$.*

3) *$G = H_1 * H_2 * \cdots * H_n$.*

4) *$H_i \cap (H_1 * \cdots * H_{i-1} * H_{i+1} * \cdots * H_n) = \{e\}$.*

Isbot. 1) Aytaylik, $a = (e_1, \ldots, a_i, \ldots, e_n), b = (e_1, \ldots, b_i, \ldots, e_n) \in H_i$ bo‘lsin, u holda

$$\begin{aligned} a * b^{-1} &= (e_1, \ldots, a_i, \ldots, e_n) * (e_1, \ldots, b_i, \ldots, e_n)^{-1} \\ &= (e_1, \ldots, a_i, \ldots, e_n) * (e_1, \ldots, b_i^{-1}, \ldots, e_n) \\ &= (e_1, \ldots, a_i \cdot b_i^{-1}, \ldots, e_n) \in H_i. \end{aligned}$$

Bundan esa, H_i to‘plam G gruppaning qism gruppasi ekanligi kelib chiqadi. Endi uning normal qism gruppa bo‘lishini ko‘rsatamiz. Ixtiyoriy $g = (g_1, g_2, \ldots, g_n) \in G$ element uchun

$$\begin{aligned} g * a * g^{-1} &= (g_1, g_2, \ldots, g_n) * (e_1, \ldots, a_i, \ldots, e_n) * (g_1, g_2, \ldots, g_n)^{-1} \\ &= (g_1, \ldots, g_i \cdot a_i, \ldots, g_n) * (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}) \\ &= (e_1, \ldots, g_i \cdot a_i \cdot g_i^{-1}, \ldots, e_n) \in H_i. \end{aligned}$$

Demak, H_i normal qism gruppa.

2) Ixtiyoriy $a = (a_1, a_2 \ldots, a_n) \in G$ element uchun $h_i = (e_1, \ldots, a_i, \ldots, e_n) \in H_i$, $1 \leq i \leq n$ elementlarni olsak $a = h_1 * h_2 * \cdots * h_n$ bo‘ladi. Endi a elementning bunday ifodasini yagona ekanligini ko‘rsatamiz. Faraz qilaylik, qandaydir $k_i \in H_i$ elementlar uchun $a = k_1 * k_2 * \cdots * k_n$ bo‘lsin, u holda $k_i = (e_1, \ldots, b_i, \ldots, e_n)$ bo‘lib,

$$a = (a_1, a_2 \ldots, a_n) = k_1 * k_2 * \cdots * k_n = (b_1, b_2, \ldots, b_n)$$

bo‘ladi. Bundan esa, $a_i = b_i$, ya’ni $h_i = k_i$ ekanligi kelib chiqadi.

3) $G = H_1 * H_2 * \cdots * H_n$ ekanligi (ii) dan to‘g‘ridan-to‘g‘ri kelib chiqadi.
4) Aytaylik $a \in H_i \cap (H_1 * \cdots * H_{i-1} * H_{i+1} * \cdots * H_n)$ bo‘lsin, u holda

$$a \in H_i \quad \text{va} \quad a \in H_1 * \cdots * H_{i-1} * H_{i+1} * \cdots * H_n.$$

Demak, birinchi tomondan $a = (e_1, \ldots, a_i, \ldots, e_n)$, ikkinchi tomondan esa u

$$h_1, \ldots, h_i, h_{i+1}, \ldots, h_n$$

elementlarning ko‘paytmasi ko‘rinishida ifodalanadi, bu yerda $a_i \in G_i$ va $h_j \in H_j$, ya’ni $h_j = (e_1, \ldots, b_j, \ldots, e_n)$. Demak,

$$a = (e_1, \ldots, a_i, \ldots, e_n) = h_i * \ldots h_{i-1} * h_{i+1} * \cdots * h_n = (b_1, \ldots, b_{i-1}, e_i, b_{i+1}, \ldots, b_n).$$

Dundan esa, $a_i = e_i$ va $b_j = e_j$ ekanligi kelib chiqadi, ya’ni

$$H_i \cap (H_1 * \cdots * H_{i-1} * H_{i+1} * \cdots * H_n) = \{e\}.$$

□

Endi gruppada nornal qism gruppalarning ichki to‘g‘ri ko‘paytmasi tushunchasini kiritamiz. Ichki to‘g‘ri ko‘paytma tushunchasini kiritishga yuqoridagi teoremada G gruppaning kesishmalari birlik elementlardan iborat bo‘lgan H_i normal qism gruppalarning ko‘paytmasi ko‘rininshda ifodalanishi asosiy turtki bo‘lgan deyish mumkin.

2.4.1-ta’rif. *Agar G gruppada H va K normal qism gruppalar berilgan bo‘lib, $G = H \cdot K$ va $H \cap K = \{e\}$ bo‘lsa u holda G gruppa ushbu normal qism gruppalarning **ichki to‘g‘ri ko‘paytmasi** shaklida ifodalanadi deyiladi.*

Ta’kidlash joizki agar gruppaning ixtiyoriy H va K normal qism gruppalari uchun $H \cap K = \{e\}$ shart o‘rinli bo‘lsa, u holda $\forall h \in H$ va $\forall k \in K$ uchun $h \cdot k = k \cdot h$ bo‘ladi. Haqiqatdan ham, H va K larning normalligidan foydalansak, $(k^{-1} \cdot h \cdot k) \cdot h^{-1} = k^{-1} \cdot (h \cdot k \cdot h^{-1})$ element $H \cap K$ da yotishi hosil qilamiz. Demak, $(k^{-1} \cdot h \cdot k) \cdot h^{-1} = e$, bundan esa $h \cdot k = k \cdot h$ kelib chiqadi.

Bundan tashqari, G gruppa H va K normal qism gruppalarning ichki to‘g‘ri ko‘paytmasi shaklida ifodalansa, ixtiyoriy $g \in G$ elementni yagona ravishda $g = h \cdot k$, $h \in H$, $k \in K$ ko‘rinishida ifodalash mumkin. Ushbu ifodaning mavjudligi ta’rifdan bevosita kelib chiqsa, uning yagonaligi esa quyidagi mulohazalardan kelib chiqadi. Faraz qilaylik $g = h \cdot k = h_1 \cdot k_1$, $h, h_1 \in H$, $k, k_1 \in K$ bo‘lsin, u holda $h_1^{-1} \cdot h, k_1^{-1} \cdot k \in H \cap K = \{e\}$ ekanligidan $h_1 = h$ va $k_1 = k$ kelib chiqadi.

Ushbu mulohazalardan foydalanib, G gruppa o‘zning bir nechta $H_1, H_2, \ldots H_n$ normal qism gruppalarining ichki to‘g‘ri ko‘paytmasi shaklidagi yoyilmasi ta’rifini quyidagicha kiritamiz.

2.4.2-ta'rif. *Agar G gruppaning ixtiyoriy $g \in G$ elementini $h_i \in H_i (H_i \lhd G)$ elementlarning ko'paytmasi ko'rinishida $g = h_1 \cdot h_2 \dots h_n$ yagona ravishda ifodalash mumkin bo'lsa, u holda G gruppa $H_1, H_2, \dots H_n$ normal qism gruppalarining ichki to'g'ri ko'paytmasi shaklida ifodalanadi deyiladi.*

Ta'kidlash joizki, G gruppa $H_1, H_2, \dots H_n$ normal qism gruppalarining ichki to'g'ri ko'paytmasi shaklida ifodalanishi uchun $G = N_1 \cdot N_2 \dots N_n$ va $N_i \bigcap (N_1 \dots N_{i-1} N_{i+1} \dots N_n) = \{e\}$ bo'lishi zarur va yetarli.

Endi tashqi va ichki to'g'ri ko'paytmalar orasidagi bog'lanishni keltiramiz. Agar G gruppa $H_1, H_2, \dots H_n$ normal qism gruppalarning ichki to'g'ri ko'paytmasi shaklida ifodalansa, u holda G gruppani ushbu normal qism gruppalarning tashqi to'g'ri ko'paytmasi sifatida qarash mumkin. Ya'ni quyidagi teorema o'rinli.

2.4.2-teorema. *Agar G gruppa $H_1, H_2, \dots H_n$ normal qism gruppalarining ichki to'g'ri ko'paytmasi shaklida ifodalansa u holda*

$$G \simeq H_1 \times H_2 \times \dots \times H_n$$

bo'ladi, ya'ni G gruppa ushbu normal qism gruppalarining tashqi to'g'ri ko'paytmasiga izomorf bo'ladi.

Isbot. Ixtiyoriy $g \in G$ element yagona ravishda $g = h_1 h_2 \dots h_n$, $h_i \in H_i$ ko'rinishida ifodalanishidan foydalanib, $f : G \to H_1 \times H_2 \times \dots \times H_n$ akslantirishni

$$f(g) = (h_1, h_2, \dots, h_n)$$

kabi aniqlaymiz.

Ushbu akslantirishning to'g'ri aniqlangani va o'zaro bir qiymatli moslik ekanligi bevosita kelib chiqadi. Endi ushbu akslantirishning gomomorfizm ekanligini ko'rsatamiz.

Ixtiyoriy $a = a_1 a_2 \dots a_n$ va $b = b_1 b_2 \dots b_n$ elementlarni olamiz, bu yerda $a, b \in G$ va $a_i, b_i \in N_i$. $N_i \bigcap N_j = \{e\}$ bo'lganligi uchun $a_i \cdot b_j = b_j \cdot a_j$. U holda

$$f(a \cdot b) = f\big((a_1 a_2 \dots a_n) \cdot (b_1 b_2 \dots b_n)\big) = f(a_1 b_1 a_2 b_2 \dots a_n b_n) =$$

$$= (a_1 b_1, a_2 b_2, \dots a_n b_n) = f(a) \cdot f(b),$$

ya'ni f gomomorfizm bo'ladi. Demak, $G \simeq H_1 \times H_2 \times \dots \times H_n$. $\square$

Yuqoridagi teoremadan gruppalarning tashqi va ichki to'g'ri ko'paytmalari bir xil hususiyatga ega ekanligi kelib chiqadi. Shuning uchun keyinchalik ularni farqlamasdan gruppalarning, shunchaki to'g'ri ko'paytma deb ishlatiladi.

Quyida gruppalarning to'g'ri ko'paytmasiga doir ba'zi tasdiqlarni keltiramiz.

2.4.1-tasdiq. *Aytaylik G va G_1 gruppalar va $f : G \to G_1$ gomomorfizm berilgan bo'lsin. Agar $H \lhd G$ uchun f akslantirish H ni G_1 ga o'tkazuvchi izomorfizm bo'lsa, u holda $G = H \times Kerf$.*

Isbot. $f(H) = G_1$ ekanligidan ixtiyoriy $a \in G$ element uchun shunday $h \in H$ element topilib $f(a) = f(h)$ bo‘lishi, ya’ni $f(h^{-1} \cdot a) = e_1$ ekanligi kelib chiqadi. Bu esa, $h^{-1} \cdot a \in \mathrm{Ker} f$ ekanligini anglatadi. Bundan foydalanib, qandaydir $b \in \mathrm{Ker} f$ element uchun $b = h^{-1} \cdot a$, ya’ni $a = b \cdot h$ deb yozish mumkin. Demak, $G = H \cdot \mathrm{Ker} f$ ekanligini hosil qildik. Endi $H \cap \mathrm{Ker} f = \{e\}$ bo‘lishini ko‘rsatamiz. Aytaylik $a \in H \cap \mathrm{Ker} f$ bo‘lsin, u holda $a \in \mathrm{Ker} f$ ekanligidan $f(a) = e_1 = f(e)$ tenglik kelib chiqadi. $a, e \in H$ va $f|_H : H \to G_1$ akslantirishning o‘zaro bir qiymatliligidan $a = e$ ekanligiga ega bo‘lamiz, ya’ni $H \cap \mathrm{Ker} f = \{e\}$. Demak, $G = H \times \mathrm{Ker} f$. $\square$

2.4.2-tasdiq. *Aytaylik $G_1, G_2, \ldots G_n$ siklik gruppalar berilgan bo‘lib, $|G_i| = m_i$ bo‘lsin. $G = G_1 \times G_2 \times \cdots \times G_n$ gruppa siklik bo‘lishi uchun $m_1, m_2, \ldots, m_n$ sonlari o‘zaro tub bo‘lishi zarur va yetarli.*

Isbot. Aytaylik, $G_i = \langle a_i \rangle$ bo‘lib, ixtiyoriy i, j uchun $(m_i, m_j) = 1$ bo‘lsin. $(a_1, a_2, \ldots, a_n)^k = (e_1, e_2, \ldots, e_n)$ ekanligidan $a_i^k = e_i, 1 \leq i \leq n$ bo‘lishi, ya’ni $k = m_i q_i$ kelib chiqadi. $(m_i, m_j) = 1$ bo‘lganligi uchun k soni ya’ni $(a_1, a_2, \ldots, a_n)$ elementning tartibi $m_1 m_2 \ldots m_n$ soniga bo‘linishi kelib chiqadi. $|G| = m_1 m_2 \ldots m_n$ bo‘lganligi uchun $ord\big((a_1, a_2, \ldots, a_n)\big) = m_1 m_2 \ldots m_n$, ya’ni $G = \langle (a_1, a_2, \ldots, a_n) \rangle$.

Agar qandaydir i, j uchun $(m_i, m_j) = d > 1$ bo‘lsa u holda $p = EKUK(m_1, m_2, \ldots, m_n) < m_1 m_2 \ldots m_n$ bo‘lib, $\forall g_i \in G_i$ uchun

$$(g_1, g_2, \ldots, g_n)^p = (g_1^p, g_2^p, \ldots, g_n^p) = (e_1, e_2, \ldots, e_n)$$

bo‘ladi. Ya’ni G gruppaning ixtiyoriy elementining tartibi $m_1 m_2 \ldots m_n = |G|$ sonidan kichik bo‘ladi. Bundan esa, G gruppaning siklik emasligi kelib chiqadi. $\square$

Endi gruppaning uning ikkita qism gruppalari yarim to‘g‘ri ko‘paytmasiga yoyilishi ta’rifini keltiramiz. Yarim to‘g‘ri ko‘paytmaning to‘g‘ri ko‘paytmadan farqli tomoni shundaki, bunda qism gruppalardan biri normal bo‘lishi shart emas.

2.4.3-ta’rif. *Agar G gruppada H va K qism gruppalari berilgan bo‘lib, quyidagi shartlar bejarilsa:*

1. *H normal qism gruppa,*

2. *$H \cap K = \{e\}$,*

3. *$G = HK$,*

u holda G gruppa H va K qism gruppalarning yarim to‘g‘ri ko‘paytmasi shaklida ifodalanadi deyiladi va $G = H \leftthreetimes K$ kabi belgilanadi.

Ta'kidlash joizki, ushbu ta'rifdagi 2) va 3) sahrtlarni G gruppaning ixtiyoriy elementi yagona ravishda $h \cdot k$, $h \in H, k \in K$ ko'rinishida ifodalaninsh sharti bilan almashtirish mumkin. Bundan tashqari, chekli gruppalar uchun $|G| = |H||K|$ tenglik o'rinli bo'ladi.

2.4.2-misol. *Ushbu misolda ba'zi qism gruppalarning yarim to'g'ri ko'paytmalarini keltiramiz:*

- $S_n = A_n \leftthreetimes \langle(1,2)\rangle$, *ya'ni o'rin almashtirishlar gruppasi, juft o'rin almashtirishlar gruppasi va ikkinchi tartibli* $\langle(1,2)\rangle$ *siklik gruppalarning yarim to'g'ri ko'paytmasi shaklida ifodalanadi*
- $S_4 = \mathbf{K}_4 \leftthreetimes S_3$, *bu yerda* $\mathbf{K}_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ *to'rtinchi tartibli Kleyn gruppasi,* S_3 *esa,* S_4 *ning* 4 *ni o'z joyida qoldiruvchi elementlaridan tashkil topgan qism gruppasi.*
- $GL_n(\mathbb{R}) = SL_n(\mathbb{R}) \leftthreetimes \{diag(\lambda, 1, \dots, 1), \lambda \neq 0\}$,

Agar $G = H \leftthreetimes K$ bo'lsa u holda $G/H \simeq K$ ekanligini ko'rish qiyin emas. Lekin teskarisi har doim ham o'rinli bo'lavermaydi, ya'ni G gruppaning ixtiyoriy H normal qism gruppasi uchun G/H faktor gruppaga izomorf bo'lgan K gruppa har doim ham mavjud bo'lavermaydi. Masalan, $G = \mathbb{Z}$ va $H = 2\mathbb{Z}$ deb olsak, u holda $Z/2\mathbb{Z}$ gruppaga izomorf bo'ladigan qism gruppa mavjud emas.

2.4.1 Mustaqil ishlash uchun misol va masalalar

1. Quyidagi gruppalarning qaysilari siklik bo'lishini aniqlang
   - $\mathbb{Z}_2 \times \mathbb{Z}_9$,
   - $\mathbb{Z}_6 \times \mathbb{Z}_9$,
   - $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8$,
   - $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{12}$,
   - $\mathbb{Z}_7 \times \mathbb{Z}_{15} \times \mathbb{Z}_{16}$.
2. Quyidagi gruppalarning siklik ekanligini ko'rsating va barcha hosil qiluvchi elementlarini toping
   - $\mathbb{Z}_2 \times \mathbb{Z}_3$,
   - $\mathbb{Z}_5 \times \mathbb{Z}_6$,
   - $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$,
   - $\mathbb{Z}_2 \times A_3$.

3. $G = A \times B$ kommutativ bo‘lishi uchun A va B gruppalar kommutativ bo‘lishi zarur va yetarli ekanligini isbotlang.

4. Agar A, B, C va D gruppalar uchun $A \simeq C$ va $B \simeq D$ bo‘lsa, u holda $A \times B \simeq C \times D$ ekanligini isbotlang.

5. $\mathbb{Z}_2 \times \mathbb{Z}_{15} \simeq \mathbb{Z}_5 \times \mathbb{Z}_6$ ekanligini isbotlang.

6. $\mathbf{K}_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ ekanligini isbotlang.

7. Ixtiyoriy $G_1, G_2, \ldots, G_n$ gruppalar uchun
$$Z(G_1 \times G_2 \times \cdots \times G_n) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n).$$
ekanligini isbotlang.

8. G gruppa H va K uning qism gruppalari bo‘lib, $G = H \times K$ bo‘lsa, u holda $G/K \simeq H$ va $G/H \simeq K$ ekanligini isbotlang.

9. Aytaylik G gruppa H va K uning normal qism gruppalari bo‘lsin. Agar $G = HK$ va $H \cap K = N$ bo‘lsa, u holda $G/N \simeq H/N \times K/N$ ekanligini isbotlang.

10. Quyidagi gruppalarning qiysilarini ikkita qism gruppasining to‘g‘ri yig‘indisi shaklida ifodalash mimkin:
$$\begin{array}{llll} \mathbb{Z}_8, & \mathbb{Z}_{12}, & \mathbb{Z}_{15}, & \mathbb{Z}_{20}, \\ S_3, & D_3, & (\mathbb{Z}, +), & (\mathbb{Q}, +) \end{array}$$

11. Quyidagi gruppalarning mumkin bo‘lgan barcha to‘g‘ri yoyilmalarini toping
$$\mathbb{Z}_{12}, \quad \mathbb{Z}_{18}, \quad \mathbb{Z}_{30}, \quad \mathbb{Z}_{60}.$$

12. Quyidagi gruppalarning qaysilari o‘zaro izomorf bo‘ladi
$$\mathbb{Z}_2 \times S_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_6, \quad \mathbb{Z}_{12}.$$

13. $\mathbb{Z}_9$ va $\mathbb{Z}_3 \times \mathbb{Z}_3$ gruppalar izomorf emasligini ko‘rsating.

14. Quyidagi gruppalarning o‘zaro izomorf emasligini ko‘rsating $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ va $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

15. $\mathbb{Z}_{12}$ va $\mathbb{Z}_2 \times \mathbb{Z}_6$ gruppalarning izomorf emasligini ko‘rsating.

16. $\mathbb{Z}_2 \times S_3$ va A_4 gruppalarning izomorf emasligini ko‘rsating.

17. $\mathbb{Z}_2 \times S_3$ va D_6 gruppalarning izomorfligini ko‘rsating va barcha izomorfizmlarni toping.

18. Isbotlang: $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_3$.

19. $Aut(\mathbb{Z}_2 \times \mathbb{Z}_3)$ ni toping.

20. $Aut(\mathbb{Z}_2 \times \mathbb{Z}_4)$ ni toping.

21. $Aut(\mathbb{Z}_3 \times \mathbb{Z}_4)$ ni toping.

22. $Aut(\mathbb{Z}_3 \times \mathbb{Z}_3)$ ni toping.

23. $Aut(\mathbb{Z}_2 \times \mathbb{Z}_5)$ ni toping.

BOB 3

Abel gruppalari

3.1 Chekli abel gruppalari

Biz uchbu mavzuda abel ya'ni kommutativ gruppalar haqida batafsil to'xtalib o'tamiz. Chekli abel gruppalarni tasniflash masalasi XIX asrda o'rganilgan muhim muammolaridan biri hisoblanib, algebra, sonlar nazariyasi, topologiya va kombinatorika kabi bir qator fanlarda o'z tadbig'iga ega. Ma'lumki, siklik gruppalar abel gruppasi bo'lib, ixtiyoriy chekli siklik gruppa $\mathbb{Z}_n$ gruppaga, cheksiz siklik gruppa esa $\mathbb{Z}$ gruppaga izomorf bo'ladi. Biz ushbu mavzuda chekli abel gruppalarining to'liq tasnifini keltirib, ixtiyoriy chekli abel gruppasi siklik gruppalarning to'g'ri yig'indisi shaklida ifodalanishini isbotlaymiz. Bundan tashqari, ushbu natija hosil qiluvchi elementi cheklita bo'lgan cheksiz abel gruppalari uchun ham o'rinli ekanligini ko'rsatamiz.

Bizga G abel gruppasi berilgan bo'lsin. Odatda abel gruppasida binar amalni $+$ orqali, birlik elementni 0 orqali va a elementga teskari elementni $-a$ orqali belgilash qabul qilingan. Shuning uchun biz ham ushbu mavzuda aynan shunday belgilashlardan foydalanamiz. U holda a^n o'rniga na ifoda ishlatilsa, $ord(a) = n$ deganda esa $na = 0$ ekanligi tushuniladi. Bundan tashqari, A va B abel gruppalarining to'g'ri ko'paytmasi $A \times B$ ham $A \oplus B$ kabi belgilanib, to'g'ri ko'paytma o'rnigi to'g'ri yig'indi atamasi ishlatiladi.

Ixtiyoriy G gruppa uchun qiyidagi to'plamni aniqlaymiz

$$T(G) = \{g \in G \mid ord(g) < \infty\},$$

ya'ni G gruppaning tartibi chekli bo'lgan elementlaridan tuzilgan to'plamni $T(G)$ kabi belgilaymiz. Ushbu $T(G)$ to'plam G gruppaning **davriy qismi** bed ataladi. Agar $T(G) = \{e\}$ bo'lsa, ya'ni gruppaning birlik elementdan farqli barcha elementlari tartibi cheksizga teng bo'lsa, u holda G gruppaga **buralishga ega bo'lmagan** gruppa deb ataladi.

Ta'kidlash joizki, nokommutativ gruppalarning davriy qismi har doim ham qism gruppa bo‘lavermaydi. Masalan, $GL_2(\mathbb{R})$ gruppaning $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ va $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ elementlarining tartiblarlari chekli, ya’ni $ord(A) = 4$, $ord(B) = 3$, bo‘lib, $AB = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$ elementning tartibi cheksizga teng. Demak, $T(GL_2(\mathbb{R}))$ to‘plam $GL_2(\mathbb{R})$ gruppaning qism gruppasi bo‘lmaydi. Quyidagi teoremada esa, abel gruppalarining davriy qismi qism gruppa bo‘lishini ko‘rsatamiz.

3.1.1-teorema. *G abel gruppasi uchun quyidagilar o‘rinli*

1) $T(G)$ qism gruppa.

2) $T(G/T(G)) = 0$, ya’ni $G/T(G)$ gruppa buralishga ega bo‘lmagan gruppa bo‘ladi.

Isbot. 1) Aytaylik, $a, b \in T(G)$ bo‘lsin, u holda $ord(a) = r$ va $ord(b) = s$, ya’ni $ra = 0$, $sb = 0$ bo‘lib,

$$rs(a + b) = s(ra) + r(sb) = 0,$$

$$r(-a) = -ra = 0$$

tengliklardan $a + b \in T(G)$ va $-a \in T(G)$ ekanligi kelib chiqadi. Demak, $T(G)$ qism gruppa.

2) Ixtiyoriy $a+T(G) \in T(G/T(G))$ element osak, bu elementning tartibi chekli bo‘lganligi uchun

$$s(a + T(G)) = sa + T(G) = T(G)$$

bo‘lib, bundan $sa \in T(G)$ ekanligi kelib chiqadi. U holda $ord(sa) = r$ bo‘lib, $(rs)a = r(sa) = 0$ ekanligidan $a \in T(G)$. Bu esa $a + T(G) = T(G)$, ya’ni $T(G/T(G)) = 0$ ekanligini anglatadi. $\square$

Endi tartibi p tub sonining biror darajasidan iborat bo‘lgan elementlar to‘plamini, ya’ni

$$G(p) = \{g \in G \mid ord(g) = p^k, \ k \geq 1\}$$

to‘plamni qaraymiz. Ko‘rsatish qiyin emaski, $G(p)$ to’plam ham G gruppaning qism gruppasi bo‘ladi. Chunki, agar $a, b \in G(p)$ bo‘lsa, u holda $ord(a) = p^s$, $ord(b) = p^m$, ya’ni $p^s a = 0$, $p^m b = 0$. Agar $t = \max\{s, m\}$ deb olsak, u holda

$$p^t(a + b) = p^t a + p^t b = 0, \quad p^s(-a) = -p^s a = 0,$$

tengliklardan $a + b, -a \in G(p)$ ekanligi kelib chiqadi. Ushbu $G(p)$ qism gruppalarga **primar komponentalar** deb ataladi.

Agar gruppa o‘zining davriy qismi bilan ustma-ust tushsa, ya’ni $T(G) = G$ bo‘lsa, u holda u **davriy gruppa** deyiladi. Boshqacha aytganda, davriy gruppa ixtiyoriy elementining tartibi chekli bo‘lgan gruppadir.

3.1.2-teorema. *Ixtiyoriy davriy gruppa primar komponentalarning to‘g‘ri yig‘indisi shaklida ifodalanadi, ya’ni*

$$G = \bigoplus_p G(p).$$

Isbot. Ixtiyoriy $a \in G$ element olsak, u holda $ord(a) < \infty$. Aytaylik, $ord(a) = n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ bo‘lsin. Quyidagi belgilashni kiritamiz $n_i = \frac{n}{p_i^{k_i}}$, $1 \leq i \leq r$. Ta’kidlash joizki, $n_i a \in G(p_i)$, chunki, $p_i^{k_i}(n_i a) = na = 0$. Bundan tashqari, ushbu n_i sonlari o‘zaro tub bo‘lganligi uchun $t_1, t_2, \dots t_r$ butun sonlari topilib,

$$t_1 n_1 + t_2 n_2 + \cdots + t_r n_r = 1.$$

U holda a elementni quyidagicha yozish mumkin

$$a = 1 \cdot a = \Big(\sum_{i=1}^{r} t_i n_i\Big) \cdot a = \sum_{i=1}^{r} t_i (n_i a),$$

bu yerda $n_i a \in G(p_i)$. Demak, G gruppaning ixtiyoriy elementi $G(p_i)$ qism gruppalar elementlarining yig’indisi ko‘rinishida ifodalanadi.

Endi $q \notin \{p_1, p_2, \dots, p_k\}$ uchun $G(q) \cap (G(p_1) + G(p_2) + \cdots + G(p_k)) = 0$ ekanligini ko‘rsatamiz. Ixtiyoriy $b \in G(p_1) + G(p_2) + \cdots + G(p_k)$ element olsak, u holda $ord(b) = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$, $s_i \geq 0$ bo‘ladi. $G(q)$ gruppa esa, tartibi q sonining darajaliran iborat elementlardan tashkil topgan, hamda $q \notin \{p_1, p_2, \dots, p_k\}$ bo‘lganligi uchun $G(q) \cap (G(p_1) + G(p_2) + \cdots + G(p_k)) = 0$ kelib chiqadi. Demak, $G = \bigoplus_p G(p)$. $\square$

Biz endi chekli abel gruppalarini batafsilroq o‘rganamiz. Ta’kidlash joizki, ixtiyoriy chekli gruppa davriy gruppa bo‘ladi, ya’ni chekli gruppalar uchun $T(G) = G$ shart o‘rinli. Demak, 3.1.2-teoremaga ko‘ra ixtiyoriy chekli abel gruppasi ham primar komponentalarning to‘g‘ri yig‘indisi shaklida ifodalanishi kelib chiqadi. Ya’ni G chekli abel gruppasi uchun $|G| = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ bo‘lsa, u holda

$$G = G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_r)$$

yoyilma o‘rinli, bu yerda $|G(p_i)| = p^{r_i}$. Bundan tashqari, ushbu yoyilma qo‘shiluvchilarning o‘rnini almashtirish aniqligida yagona bo‘ladi. Ya’ni agar $G = B_1 \oplus B_2 \oplus \cdots \oplus B_r$ bo‘lib, $|B_i| = p_i^{s_i}$ bo‘lsa, u holda $s_i = r_i$ va $B_i = G(p_i)$ bo‘ladi. Bu esa, chekli abel gruppalarini o‘rganish masalasi primar komponentalarni o‘rganish masalasiga keltirilishini bildiradi. Demak, biz tartibi p^k (p-tub son) soniga teng bo‘lgan gruppalarni o‘rganamiz, ya’ni barcha elementining tartibi p sonining darajalaridan iborat bo‘lgan abel gruppalarini o‘rganamiz.

Aytaylik, G gruppa uchun $|G| = p^k$ bo‘lib, $a \in G$ element tartibi eng katta bo‘lgan element bo‘lsin. Ya’ni $\forall b \in G$ uchun $ord(a) \geq ord(b)$. U holda $ord(a) = p^s, s \leq k$, bo’lib, $s = k$ bo‘lgan holda G gruppa siklik bo‘ladi.

3.1.1-lemma. *Aytaylik, G gruppa uchun $|G| = p^k$ bo'lib, $a \in G$ element tartibi eng katta bo'lgan element bo'lsin. U holda shunday $B \subset G$ qism gruppa mavjud bo'lib, $G = \langle a \rangle \oplus B$ yoyilma o'rinli bo'ladi.*

Isbot. Aytaylik, $ord(a) = p^r$ bo'lib, H qism gruppa $H \cap \langle a \rangle = 0$ shartni qanoatlantiruvchi maksimal qism gruppa bo'lsin. Ushbu $\langle a \rangle$ va H qism gruppalarning to'g'ri yig'indisini $G_0 = H \oplus \langle a \rangle$ kabi belgilaymiz. Agar $G_0 = G$ bo'lsa, u holda $B = H$ bo'lib, lemmaning isboti kelib chiqadi.

Faraz qilaylik, $G_0 \neq G$ bo'lsin, u holda $b \in G \setminus G_0$ element mavjud bo'lib, $ord(b) = p^s, 1 \leq s \leq r$. Endi $G \setminus G_0$ to'plamdan tartibi minimal bo'lgan x elementni tanlab olamiz, ya'ni $x \in G \setminus G_0$ bo'lib, $\forall b \in G \setminus G_0$ uchun $ord(x) \leq ord(b)$. Agar px elementni qarasak, u holda $ord(px) = \frac{ord(x)}{p}$ ekanligidan va $ord(x)$ ning minimalligidan $px \in G_0$ ekanligi kelib chiqadi. U holda shunday $l \in \mathbb{Z}$ va $y \in H$ elementlar topilib, $px = la + y$ bo'ladi. p^r soni gruppaning elementlari tartiblarining eng kattasi bo'lganligi uchun gruppaning ixtiyoriy $c \in G$ elementi uchun $p^r c = 0$. Xususan, $p^r x = 0$, u holda biz quyidagi teglikka ega bo'lamiz

$$0 = p^r x = p^{r-1}(px) = p^{r-1}(la + y) = p^{r-1}la + p^{r-1}y.$$

Bundan esa, $p^{r-1}la = -p^{r-1}y \in \langle a \rangle \oplus H$ ekanligi, ya'ni $p^{r-1}la = 0$ kelib chiqadi. Demak, $p^{r-1}l$ soni p^r ga bo'linadi, bu esa l soni p ga bo'linishini anglatadi, ya'ni $l = pt$. Shunday qilib, biz $px = la + y = pta + y$ ekanligini, ya'ni $p(x - ta) = y$ bo'lishini hosil qildik. Ushbu $x - ta$ element H qism gruppada yotmaydi, chunki agar $x - ta \in H$ bo'lsa, u holda $x \in ta + H$ bo'lib, $x \in G_0$ ekanligi kelib chiqadi. Demak, $\langle x - ta \rangle \oplus H$ qism gruppa H gruppadan kattaroq qism gruppa bo'ladi. H gruppa $H \cap \langle a \rangle = 0$ shartni qanoatlantiruvchi maksimal qism gruppa bo'lganligi uchun

$$\big(\langle x - ta \rangle \oplus H\big) \cap \langle a \rangle \neq 0.$$

Demak, shunday $k, m \in \mathbb{Z}$ sonlari va $z \in H$ element topilib, $m(x - ta) + z = ka \neq 0$ bo'ladi. Bundan esa,

$$mx = (mt + k)a - z \in \langle a \rangle \oplus H = G_0$$

ekanligi kelib chiqadi.

Agar m soni p ga bo'linsa, u holda $p(x - ta) \in H$ ekanligidan $m(x - ta) \in H$ bo'lishi kelib chiqadi. Bu esa ziddiyat, chinki $ka = m(x - ta) + z \notin H$.

Agar m soni p ga bo'linmasa, u holda shunday u, v butun sonlari topilib, $up + vm = 1$ bo'ladi. Endi $px, mx \in G_0$ ekanligini hisobga olib,

$$x = 1 \cdot x = (up + vm)x = u(px) + v(mx) \in G_0$$

bo'lishini hosil qilamiz. Bu esa $G_0 \neq G$ ekanligiga zid, demak, $G = \langle a \rangle \oplus H$. $\square$

Qiyidagi misolda tartibi p^2 ga teng bo'lgan siklik bo'lmagan abel gruppalarining tashnifini keltiramiz.

3.1.1-misol. *Tartibi p^2 ga teng bo'lgan siklik bo'lmagan abel gruppasi $\mathbb{Z}_p \oplus \mathbb{Z}_p$ ga izomorf bo'ladi. Haqiqatdan ham, agar G siklik bo'lmagan abel gruppasi uchun $|G| = p^2$ bo'lsa, u holda G gruppaning 0 dan farqli barcha elementlarining tartibi p ga teng bo'ladi. Ixtiyoriy noldan farqli $a \in G$ element uchun 3.1.1-lemmaga ko'ra, shunday B qism gruppa toplib, $G = \langle a \rangle \oplus B$. Endi $|B| = \frac{|G|}{|\langle a \rangle|} = p$ ekanligidan B qsim gruppaning ham siklikligi kelib chiqadi. Demak, $G \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$.*

Quyidagi teoramada tartibi p^k ga teng bo'lgan ixtiyoriy abel gruppasini yagona ravishda siklik gruppalarning to'g'ri yig'indisi shaklida yozish mumkinligini isbotlaymiz.

3.1.3-teorema. *Aytaylik, G chekli abel gruppasi bo'lib, $|G| = p^k$ bo'lsin, u holda quyidagilar o'rinli.*

1) G gruppa siklik gruppalarning to'g'ri yig'indisi shaklida

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$$

kabi ifodalanadi, bu yerda $|G_1||G_2| \dots |G_r| = p^k$.

2) Agar G gruppaning $G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$ va $G = H_1 \oplus H_2 \oplus \cdots \oplus H_s$ yoyilmalari mavjud bo'lib, $|G_1| \leq |G_2| \leq \cdots \leq |G_r|$ va $|H_1| \leq |H_2| \leq \cdots \leq |H_s|$ bo'lsa, u holda $s = r$ va $|H_i| = |G_i|$, $1 \leq i \leq r$ bo'ladi.

Isbot. 1) Chekli abel gruppasi uchun $|G| = p^k$ ekanligidan 3.1.1-lemmaga ko'ra tartibi maksimal bo'lgan $a \in G$ element uchun $G = \langle a \rangle \oplus B$ munosabat o'rinli. O'z navbatida B gruppa uchun ham $|B| = p^l, l < k$ bo'lganligi uchun $B = \langle b \rangle \oplus C$ yoyilma mavjud. G gruppa chekli bo'lganligi uchun, induktiv tarzda uni cheklita $\langle a \rangle, \langle b \rangle, \dots, \langle c \rangle$ siklik gruppalarning to'g'ri yig'indisi shaklida ifodalanishi kelib chiqadi.

2) Dastlab $s = r$ ekanligini ko'rsatamiz. Buning uchun

$$G[p] = \{a \in G \mid pa = 0\}$$

to'plamni qaraymiz. Ushbu to'plam ham G gruppaning qism gruppasi bo'ladi. Tartibi p^{c_i} ga teng bo'lgan G_i siklik qism gruppalari uchun $|G_i[p]| = p$ tenglik o'rinli, chunki $G_i[p]$ to'plam noldan farqli ixtiyoriy elementining tartibi p ga teng bo'lgan siklik qism gruppadir, ya'ni $G_i[p] \simeq \mathbb{Z}_p$. Demak biz

$$|G[p]| = |(G_1 \oplus G_2 \oplus \cdots \oplus G_r)[p]| = |G_1[p] \oplus G_2[p] \oplus \cdots \oplus G_r[p]|$$

$$= |G_1[p]| + |G_2[p]| + \cdots + |G_r[p]| = rp$$

tenglikka ega bo'lamiz. Ikkinchi tomondan esa,

$$|G[p]| = |(H_1 \oplus H_2 \oplus \cdots \oplus H_s)[p]| = |H_1[p]| + |H_2[p]| + \cdots + |H_s[p]| = sp.$$

Bundan $s = r$ ekanligi kelib chiqadi.

Endi $|G_1| \leq |G_2| \leq \cdots \leq |G_r|$ va $|H_1| \leq |H_2| \leq \cdots \leq |H_s|$ bo‘lsa, $|H_i| = |G_i|$ ekanligini ko‘rsatamiz. Aytaylik, $|G_i| = p^{c_i}$ va $|H_i| = p^{d_i}$ bo‘lib,

$$c_1 = d_1,\ c_2 = d_2,\ \ldots,\ c_{j-1} = d_{j-1},\ c_j \neq d_j$$

bo‘lsin. Umumiylikka ziyon yetkazmagan holda $c_j < d_j$ deb olish mumkin. U holda $c_1 \leq c_2 \leq \cdots \leq c_j \leq \cdots \leq c_r$ ekanligini hisobga olsak, $p^{c_j} G_i = 0$, $1 \leq i \leq j$. Demak,

$$p^{c_j} G = p^{c_j}(G_1 \oplus G_2 \oplus \cdots \oplus G_r) = G_{j+1} \oplus G_{j+2} \oplus \cdots \oplus G_r.$$

Ikkinchi tomondan esa, $p^{c_j} H_i = 0$, $1 \leq i \leq j-1$ ekanligidan

$$p^{c_j} G = p^{c_j}(H_1 \oplus H_2 \oplus \cdots \oplus H_r) = H_j \oplus H_{j+1} \oplus H_{j+2} \oplus \cdots \oplus H_r.$$

Ya’ni, $p^{c_j} G$ gruppa bir tomondan $r - j - 1$ ta, ikkinchi tomondan esa $r - j$ ta siklik gruppalarning to‘g‘ri yig‘indisi shaklida ifodalandi. Bu esa, teoremaning birinchi qismida isbotlangan $s = r$ ekanligiga zid. Demak, $|H_i| = |G_i|$. □

Quyidagi misolda tartibi 8 ga teng bo‘lgan abel gruppalarining tasnifini keltiramiz.

3.1.2-misol. *Tartibi 8 ga teng bo‘lgan ixtiyoriy abel gruppasi $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ va $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ gruppalardan biriga izomorf bo‘ladi.*

Haqiqatdan ham agar G gruppada $ord(a) = 8$ bo‘lgan element mavjud bo‘lsa, u holda $G \simeq \mathbb{Z}_8$ bo‘ladi. Agar G gruppaning barcha elementlari uchun $ord(a) < 8$ bo‘lsa, u holda uning noldan farqli elementlari tartibi 4 yoki 2 ga teng bo‘ladi. Gruppaning tartibi 4 ga teng elementi mavjud bo‘lsa, u holda ushbu $a \in G$ alement tartibi eng katta bo‘lgan element bo‘lib, $G = \langle a \rangle \oplus B$ bo‘ladi, ya’ni $G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2$. Agar G gruppaning noldan farqli barcha elementlari uchun $ord(a) = 2$ bo‘lsa, u holda ixtiyoriy $a \in G$, $a \neq 0$ element uchun $G = \langle a \rangle \oplus B$ bo‘lib, $|B| = 4$ bo‘lganligi uchun o‘z navbatida B qism gruppa ham $B = C \oplus D$ yoyilmaga ega bo‘ladi. Demak, $G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Shunday qilib, tartibi p^n ga teng bo‘lgan abel gruppasi $G = G_1 \oplus G_2 \oplus \cdots \oplus G_k$ kabi tartibi p^{n_i} ga teng bo‘lgan siklik gruppalarning to‘g‘ri yig‘indisi shaklida ifodalanar ekan. Agar $|G_i| = n_i$, sonlari uchun $n_1 \leq n_2 \leq \cdots \leq n_k$ bo‘lsa, u holda $n_1, n_2, \ldots, n_k$ sonlari G gruppaning invariantlari deb ataladi. Yig‘indisi n ga teng bo‘lgan turli $n_1, n_2, \ldots, n_k$ invarianlarga turli abel gruppalari mos keladi. Demak, tartibi p^n ga teng bo‘lgan abel gruppalarining soni, turli invariantlarning soniga teng. Boshqacha qilib aytganda tartibi p^n ga teng bo‘lgan abel gruppalarining soni n sonini $n_1 \leq n_2 \leq \cdots \leq n_k$ sonlarining yig‘indisi ko‘rinishida $n = n_1 + n_2 + \cdots + n_k$ kabi ifodalashlar soniga teng.

Yuqoridagi teorema va lemmalardan foydalanib, chekli abel gruppalarining tuzilishi va tasnifi haqida to‘liq ma’lumot beruvchi chekli abel gruppalar uchun fundamental teoremani keltirishimiz mumkin.

3.1.4-teorema. *Ixtiyoriy chekli abel gruppasi siklik gruppalarning to‘g‘ri yig‘indisi shaklida ifodalanadi. Agar G chekli abel gruppasi uchun $|G| = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ bo‘lsa, u holda*

$$\begin{array}{c}1 \le c_{1,1} \le c_{1,2} \le \dots \le c_{1,t_1},\ c_{1,1} + c_{1,2} + \dots + c_{1,t_1} = k_1,\\ 1 \le c_{2,1} \le c_{2,2} \le \dots \le c_{2,t_2},\ c_{2,1} + c_{2,2} + \dots + c_{2,t_2} = k_2,\\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\ 1 \le c_{r,1} \le c_{r,2} \le \dots \le c_{r,t_r},\ c_{r,1} + c_{r,2} + \dots + c_{r,t_r} = k_r\end{array}$$

shartni qanoatlantiruvchi

$$G = \bigoplus_{i=1}^{r}\Big(\bigoplus_{j=1}^{t_i} G_{i,j}\Big), \quad \textit{bu yerda} \quad G_{i,j} = \langle a_{i,j}\rangle, \quad ord(a_{i,j}) = p_i^{c_{i,j}}$$

yoyilma bir qiymatli aniqlanadi.

Isbot. Ixtiyoriy chekli gruppa primar komponentalarning yig‘indisi shaklida ifodalanganligi uchun $|G| = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$ gruppani

$$G = \bigoplus_{i=1}^{r} G_i, \quad |G_i| = p_i^{k_i}$$

kabi ifodalash mumkin. 3.1.3-teoremaga ko‘ra esa, G_i gruppalar siklik gruppalarning to‘g‘ri yig‘indisi shaklida ifodalanadi. Demak, $G_{i,j}$ siklik gruppalar topilib, $G_i = \bigoplus\limits_{j=1}^{t_i} G_{i,j}$ bo‘ladi, bu yerda

$$p^{k_i} = \prod_{j=1}^{t_i} |G_{i,j}|, \quad 1 \le i \le r.$$

Demak, $ord(a_{i,j}) = |G_{i,j}| = p_i^{c_{i,j}}$ elementlar topilib, $G_{i,j} = \langle a_{i,j}\rangle$ bo‘ladi, ya’ni $G = \bigoplus\limits_{i=1}^{r}\Big(\bigoplus\limits_{j=1}^{t_i} G_{i,j}\Big)$.

Endi ushbu yoyilmaning teoremada berilgan shartlar asosida yagona ekanligini ko‘rsatamiz. Faraz qilaylik, $G = \bigoplus\limits_{i=1}^{r'}\Big(\bigoplus\limits_{j=1}^{t'_i} H_{i,j}\Big)$ yoyilma mavjud bo‘lib, $|H_{i,j}| = p^{d_{i,j}}$ va

$$\begin{array}{c}1 \le d_{1,1} \le d_{1,2} \le \dots \le d_{1,t'_1},\ d_{1,1} + d_{1,2} + \dots + d_{1,t'_1} = k_1,\\ 1 \le d_{2,1} \le d_{2,2} \le \dots \le d_{2,t'_2},\ d_{2,1} + d_{2,2} + \dots + d_{2,t'_2} = k_2,\\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\ 1 \le d_{r',1} \le d_{r',2} \le \dots \le d_{r',t'_{r'}},\ d_{r',1} + d_{r',2} + \dots + d_{r',t'_{r'}} = k_{r'}\end{array}$$

bo‘lsin. U holda har bir p_i tub soni uchun primar komponentalarni alohida hisoblasak, r ta $G(p_i)$ komponentalar hosil bo‘lib, $r' = r$ ekanligi kelib chiqadi. Bundan tashqari,

$$G(p_i) = \bigoplus_{j=1}^{t_i} G_{i,j} = \bigoplus_{j=1}^{t'_i} H_{i,j}$$

ekanligidan

$$1 \leq c_{i,1} \leq c_{i,2} \leq \cdots \leq c_{i,t_j},$$

$$1 \leq d_{i,1} \leq d_{i,2} \leq \cdots \leq d_{i,t'_j},$$

munosabatlarni hisobga olsak, 3.1.3-teoremaga ko‘ra $t'_j = t_j$ va $d_{i,j} = c_{i,j}$ bo‘ladi. $\square$

Demak, 3.1.4-teoremaga ko‘ra ixtiyoriy chekli abel gruppasi siklik gruppalarning to‘g‘ri yig‘indisi shaklida ifodalanib, $G \simeq \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$ bo‘ladi, bu yerda p_i tub sonlar bo‘lib, ularning orasida o‘zaro tenglari ham bo‘lishi mumkin. Ushbu $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ sonlari G gruppaning **elementar bo‘luvchilari** deb ataladi. Endi elementar bo‘luvchilarni quyidagi tartibda joylashtirib chiqamiz

$$\begin{array}{ll}
p_1^{n_{1,1}}, p_1^{n_{1,2}}, p_1^{n_{1,3}}, \ldots & n_{1,1} \geq n_{1,2} \geq n_{1,3} \geq \ldots \\
p_2^{n_{2,1}}, p_2^{n_{2,2}}, p_2^{n_{2,3}}, \ldots & n_{2,1} \geq n_{2,2} \geq n_{2,3} \geq \ldots \\
\dots\dots\dots\dots\dots\dots & \dots\dots\dots\dots\dots\dots\dots \\
p_k^{n_{k,1}}, p_k^{n_{k,2}}, p_k^{n_{k,3}}, \ldots & n_{k,1} \geq n_{k,2} \geq n_{k,3} \geq \ldots
\end{array}$$

Agar ushbu qatorlarning uzunliklari maksimumi s ga teng bo‘lsa, qolganlarini birlar bilan to‘ldirgan holda, barchasining uzunligi bir xil deb, ya’ni s ga teng deb olish mumkin. U holda

$$m_j = p_1^{n_{1,j}} p_2^{n_{1,j}} \ldots p_k^{n_{k,j}}, \quad 1 \leq j \leq s$$

sonlari uchun $m_{j+1} \mid m_j$ munosabat o‘rinli bo‘lib, $|G| = m_1 m_2 \ldots m_s$ bo‘ladi. Ushbu $(m_1, m_2, \ldots, m_s)$ sonlari esa G gruppaning **invariant faktorlari** deb ataladi.

Agar $G_j = \langle a_{1,j} \rangle \oplus \langle a_{2,j} \rangle \oplus \cdots \oplus \langle a_{k,j} \rangle$ deb olsak, bu yerda $ord(a_{i,j}) = p_i^{n_{i,j}}$. U holda $p_1, p_2, \ldots, p_k$ sonlari tub sonlar bo‘lganligi uchun, G_j gruppa ham siklik bo‘lib, $|G_j| = m_j$ bo‘ladi. Shunday qilib biz G gruppani tartibi invariant faktorlarga teng bo‘lgan abel gruppalarning to‘gri yig‘indisi shaklida ifodalash mumkinligini hosil qildik.

3.1.3-misol. *Taritibi* 32 *ga teng bo‘lgan barcha abel gruppalarini toping.*

Yechish. $32 = 2^5$ bo‘lganligi uchun 5 sonini barcha mumkin bo‘lgan yoyilmalarini qaraymiz.

$$\begin{aligned} 5 &= 4+1 \\ &= 3+2 \\ &= 3+1+1 \\ &= 2+2+1 \\ &= 2+1+1+1 \\ &= 1+1+1+1+1 \end{aligned}$$

bo‘lganligi uchun taritibi 32 ga teng bo‘lgan ixtiyoriy abel gruppasi quyidagi gruppalardan biriga izomorf bo‘ladi

$$\begin{aligned} &\mathbb{Z}_5, \\ &\mathbb{Z}_{16} \oplus \mathbb{Z}_2, \\ &\mathbb{Z}_8 \oplus \mathbb{Z}_4, \\ &\mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \\ &\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2, \\ &\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \\ &\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2. \end{aligned}$$

□

3.1.4-misol. *Taritibi* 20 *ga teng bo‘lgan barcha abel gruppalarini toping.*

Yechish. $20 = 2^2 \cdot 5$ ekanligidan, tartibi 20 ga teng bo‘lgan ixtiyoriy gruppa $G(5)$ va $G(2)$ primar komponentalarning to‘g‘ri yig‘indisi shaklida ifodalanib, $|G(5)| = 5$ va $|G(2)| = 4$ bo‘ladi. O‘z navbatida $G(5) \simeq \mathbb{Z}_5$ bo‘lsa $G(2)$ esa $\mathbb{Z}_4$ va $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ gruppalrdan biriga izomorf bo‘ladi. Demak, taritibi 20 ga teng bo‘lgan ixtiyoriy abel gruppasi $\mathbb{Z}_5 \oplus \mathbb{Z}_4$ va $\mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ gruppalardan biriga izomorf bo‘ladi.

□

3.1.5-misol. $G = \mathbb{Z}_{50} \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_8$ *gruppaning elementar bo‘luvchilarini toping.*

Yechish. $50 = 5^2 \cdot 2$, $20 = 2^2 \cdot 5$ va $8 = 2^3$ bo‘lganligi uchun $\mathbb{Z}_{50} \simeq \mathbb{Z}_{25} \oplus \mathbb{Z}_2$ va $\mathbb{Z}_{20} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_5$ bo‘ladi. U holda

$$G \simeq \mathbb{Z}_{5^2} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2$$

bo‘ladi. Demak, G gruppaning elementar bo‘luvchilari $5^2, 5, 2^3, 2^2, 2$ lardan iborat.

□

3.1.6-misol. $G = \mathbb{Z}_{24} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{10}$ *gruppaning invariant faktorlarini toping.*

Yechish. $24 = 2^3 \cdot 3$, $36 = 2^2 \cdot 3^2$ va $10 = 2 \cdot 5$ bo‘lganligi uchun gruppaning elementar bo‘luvchilari $2^3, 2^2, 2, 3^2, 3, 5$ sonlaridan iborat. U holda

$$\begin{array}{lll} 2^3, & 2^2, & 2 \\ 3^2, & 3, & 1 \\ 5, & 1, & 1 \end{array}$$

deb olsak, $m_1 = 2^3 \cdot 3^2 \cdot 5 = 360$, $m_2 = 2^2 \cdot 3 = 12$ va $m_3 = 2$ bo‘ladi. Ya’ni invariant faktorlari $360, 12, 2$. Demak, G gruppa $\mathbb{Z}_{360} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_2$ gruppaga izomorf. $\square$

3.1.1 Mustaqil ishlash uchun misol va masalalar

1. Taritibi $9, 16$ va 27 sonlariga teng bo‘lgan barcha abel gruppalarini toping.

2. Taritibi $15, 21, 22, 26, 33$ va 35 sonlariga teng bo‘lgan barcha abel gruppalarini toping.

3. Taritibi $12, 18, 28, 36, 45$ va 60 sonlariga teng bo‘lgan barcha abel gruppalarini toping.

4. Taritibi $63, 80, 180, 240$ va 360 sonlariga teng bo‘lgan barcha abel gruppalarini toping.

5. Taritibi pq (p va q turli tub sonlar) ga teng bo‘lgan ixtiyoriy abel gruppasi $\mathbb{Z}_p \oplus \mathbb{Z}_q$ gruppaga izomorf ekanligini isbotlang.

6. $G = \mathbb{Z}_{144} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_8$ gruppaning elementar bo‘luvchilarini toping.

7. $G = \mathbb{Z}_{120} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_8$ gruppaning elementar bo‘luvchilarini toping.

8. $G = \mathbb{Z}_{180} \oplus \mathbb{Z}_{40} \oplus \mathbb{Z}_9$ gruppaning elementar bo‘luvchilarini toping.

9. $G = \mathbb{Z}_{40} \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{36}$ gruppaning invariant faktorlarini toping.

10. $G = \mathbb{Z}_{22} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{18}$ gruppaning invariant faktorlarini toping.

11. $G = \mathbb{Z}_{44} \oplus \mathbb{Z}_{66} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{72}$ gruppaning invariant faktorlarini toping.

12. Tartibi 540 ga teng bo‘lgan barcha abel gruppalarini toping.

13. Tartibi 504 ga teng bo‘lgan barcha abel gruppalarini toping.

14. Tartibi p^3 ga teng bo‘lgan barcha abel gruppalarini toping.

15. Tartibi p^4 ga teng bo‘lgan barcha abel gruppalarini toping.

16. Tartibi p^3q^2 ga teng bo‘lgan barcha abel gruppalarini toping.

17. Tartibi 120 ga teng boʻlgan gruppaning tartibi uchga teng boʻlgan nechta elementi mavjud.

18. Tartibi $2^4 \cdot 3^2 \cdot 5^3$ ga teng boʻlgan nechta abel gruppasi mavjud.

19. Tartibi $2^3 \cdot 3^2 \cdot 5 \cdot 7^2$ ga teng boʻlgan nechta abel gruppasi mavjud.

3.2 Hosil qiluvchi elementlari cheklita boʻlgan abel gruppalari

Biz ushbu mavzuda cheksiz abel gruppalarini oʻrganamiz. Avvalgi mavzuda biz ixtiyoriy chekli abel gruppasi siklik gruppalarning toʻgʻri yigʻindisi shaklida ifodalanishini koʻrsatgan edik. Biz hosil qiluvchi elementlari cheklita boʻlgan cheksiz abel gruppalini oʻrganib, ularni ham ziklik gruppalarning toʻgʻri yigʻindisi shaklida ifodalanishini koʻrsatamiz. Ma'lumki, $\mathbb{Z}$ gruppa bitta hosil qiluvchiga ega boʻlgan cheksiz siklik gruppa boʻlsa, $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}$ gruppa siklik boʻlmagan gruppa boʻladi. Ushbu $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}$ gruppaning hosil qiluvchi elementlari 3 ta boʻlib, ular qiyudagilardan iborat

$$(\overline{1}_2, 0, 0),\ (0, \overline{1}_6, 0),\ (0, 0, 1).$$

Bizga G abel gruppasi va uning $\{a_1, a_2, \ldots, a_k\}$ elementlar toʻplami berilgan boʻlsin. $n_1a_1 + n_2a_2 + \cdots + n_ka_k$, $n_i \in \mathbb{Z}$ ifodaga bu elementlarning chiziqli kombinatsiyasi deb ataladi.

3.2.1-ta'rif. *Agar G gruppaning $a_1, a_2, \ldots, a_k$ elementlarining chiziqli kombinatsiyasi nolga tengligidan, ya'ni $n_1a_1 + n_2a_2 + \cdots + n_ka_k = 0$ ekanligidan $n_1 = n_2 = \cdots = n_k = 0$ boʻlishi kelib chiqsa, u holda ushbu elementlar toʻplami* ***chiziqli erkli*** *deb ataladi. Agar $a_1, a_2, \ldots, a_k$ elementlar toʻplami chiziqli erkli boʻlib, G gruppaning ixtiyoriy $a \in G$ elementini ushbu elementlarning chiziqli kombinatsiyasi orqali $a = n_1a_1 + n_2a_2 + \cdots + n_ka_k$ kabi ifodalash mumkin boʻlsa, u holda $X = \{a_1, a_2, \ldots, a_k\}$ toʻplam G gruppaning* ***bazisi*** *deb ataladi.*

Agar G gruppada bazis mavjud boʻlsa, u holda u **erkin abel gruppasi** deb ataladi. Butun sonlar gruppasining chekli sondagi toʻgʻri yigʻindisi $\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ erkin abel gruppasi boʻladi. Chiuni, ushbu gruppada cheklita

$$(1, 0, 0 \ldots, 0), (0, 1, 0 \ldots, 0), \ldots, (0, 0, 0, \ldots, 1)$$

bazis mavjud. Lekin biz yuqorida koʻrgan $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}$ gruppa erkin abel gruppasi emas, cunki $(\overline{1}_2, 0, 0)$, $(0, \overline{1}_6, 0)$, $(0, 0, 1)$ elementlar toʻplami chiziqli erkli emas. Ya'ni, hosil qiluvchi elementlari cheklita boʻlgan gruppalar har doim ham erkin abel gruppasi boʻlavermaydi.

Quyidagi teoremada ixtiyoriy erkin abel gruppasi chekli sondagi siklik gruppalarning toʻgʻri yigʻindisi shaklida ifodalanishini koʻrsatamiz

3.2.1-teorema. *Ixtiyoriy erkin abel gruppasi cheksiz siklik gruppalarning to‘g‘ri yig‘indisi shaklida ifodalanadi, ya’ni* $G \simeq \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$.

Isbot. Aytaylik, $X = \{a_1, a_2, \dots, a_k\}$ to’plam G gruppaning bazisi bo‘lsin. U holda $a_1, a_2, \dots, a_k$ elementlarning chiziqli erkli ekanligidan $n_i a_i = 0a_1 + \cdots + n_i a_i + \cdots + 0a_k = 0$ tenglikdan $n_i = 0$ kelib chiqadi. Bu esa, a_i elementning tartibi cheksizga teng ekanligini bildiradi. Gemak, G gruppa $\langle a_i \rangle$, $1 \leq i \leq k$ siklik gruppalarning to‘g‘ri yig‘indisi shaklida ifodalanadi, ya’ni $G = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \cdots \oplus \langle a_k \rangle$. Cheksiz siklik gruppalar $\mathbb{Z}$ ga izomorf bo‘lganligi uchun $G \simeq \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ ekanligini hosil qilamiz. $\square$

Ta’kidlash joizki, erkin abel gruppalarida turli xil bazislar mavjud bo‘lishi mimkin. Mazalan, $\mathbb{Z} \oplus \mathbb{Z}$ gruppada $\{(1,0),(0,1)\}$ bazisdan tashqari $\{(1,0),(0,-1)\}$, $\{(-1,0),(0,1)\}$ va $\{(-1,0),(0,-1)\}$ bazislar ham mavjud. Quyidagi teoremada erkin abel gruppasining turli bazislaridagi elementlari soni bir xil bo‘lishini ko‘rsatamiz.

3.2.2-teorema. *Agar G erkin abel gruppasining $\{a_1, a_2, \dots, a_k\}$ va $\{b_1, b_2, \dots, b_s\}$ bazislari berilgan bo‘lsa, u holda $k = s$ bo‘ladi.*

Isbot. Dastlab, $\{a_1, a_2, \dots, a_k\}$ elementlar to‘plami bazis ekanligidan foydalansak, $G \simeq \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{k\ ta}$ kelib chiqadi. U holda $2G \simeq \underbrace{2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}}_{k\ ta}$ bo‘lib,

$$G/(2G) \simeq \underbrace{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}}_{k\ ta} \simeq \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2}_{k\ ta}.$$

Demak, $|G/2G| = 2^k$. Ikkinchi tomondan esa, $\{b_1, b_2, \dots, b_s\}$ ham bazis bo‘lganligi uchun $|G/2G| = 2^s$ ekanligini hosil qilamiz. Bundan esa, $k = s$ kelib chiqadi. $\square$

Erkin abel gruppasining bazisidagi elementlar soniga gruppaning **rangi** deb ataladi va $rk(G)$ kabi belgilanadi. Rangi k ga teng bo‘lgan erkin abel gruppasini esa F_k kabi belgilaymiz. Quyida ba’zi zaruriy lemmalarni keltirib o‘tamiz.

3.2.1-lemma. *Bizga F_k abel gruppasi va uning $\{a_1, a_2, \dots, a_k\}$ bazisi berilgan bo‘lsin. Agar F_k gruppadan qandaydir G abel gruppasiga $f : F_k \to G$ va $g : F_k \to G$ gomomorfizmlar berilgan bo‘lib, $f(a_i) = g(a_i)$, $1 \leq i \leq k$ bo‘lsa u holda $f = g$ bo‘ladi.*

Isbot. Ixtiyoriy $x \in F_k$ element uchun $x = n_1 a_1 + n_2 a_2 + \cdots + n_k a_k$ bo‘lganligi uchun

$$\begin{aligned} f(x) = f(n_1 a_1 + n_2 a_2 + \cdots + n_k a_k) &= n_1 f(a_1) + n_2 f(a_2) + \cdots + n_k f(a_k) \\ &= n_1 g(a_1) + n_2 g(a_2) + \cdots + n_k g(a_k) = g(x) \end{aligned}$$

tenglikdan $f = g$ kelib chiqadi. $\square$

3.2.2-lemma. $F_k \oplus F_s \simeq F_{k+s}$

Isbot. Bizga F_k va F_s abel gruppalari berilgan bo'lib, ularning bazislari mos ravishda $\{a_1, a_2, \ldots, a_k\}$ va $\{b_1, b_2, \ldots, b_s\}$ bo'lsin. U holda $\{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_s\}$ elementlar to'plami $F_k \oplus F_s$ gruppaning bazisi bo'ladi. Haqiqatdan ham, ixtiyoriy $x \in F_k \oplus F_s$ uchun $x = y + z$, $y \in F_k$, $z \in F_s$ bo'lganligi va

$$y = n_1a_1 + n_2a_2 + \cdots + n_ka_k, \quad z = m_1b_1 + m_2b_2 + \cdots + m_sb_s,$$

ekanligidan

$$x = y + z = n_1a_1 + n_2a_2 + \cdots + n_ka_k + m_1b_1 + m_2b_2 + \cdots + m_sb_s$$

kelib chiqadi. Ya'ni $F_k \oplus F_s$ gruppaning ixtiyoriy elementi

$$a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_s$$

elementlarning chiziqli kombinatsiyasi orqali ifodalanadi.

Endi bu elementlar to'plamining chiziqli erkli ekanligini ko'rsatamiz. Aytaylik,

$$n_1a_1 + n_2a_2 + \cdots + n_ka_k + m_1b_1 + m_2b_2 + \cdots + m_sb_s = 0$$

bo'lsin. U holda

$$n_1a_1 + n_2a_2 + \cdots + n_ka_k = -(m_1b_1 + m_2b_2 + \cdots + m_sb_s) \in F_k \cap F_s$$

bo'lib, ularning nolga teng ekanligi kelib chiqadi. Ya'ni

$$n_1a_1 + n_2a_2 + \cdots + n_ka_k = 0, \quad m_1b_1 + m_2b_2 + \cdots + m_sb_s = 0.$$

Bundan esa, $n_1 = n_2 = \cdots = n_k = 0$ va $m_1 = m_2 = \cdots = m_s = 0$ kelib chiqadi. Demak, $rk(F_k \oplus F_s) = k + s$. Bundan esa, $F_k \oplus F_s \simeq F_{k+s}$ kelib chiqadi. $\square$

3.2.3-lemma. *Agar G va G' abel gruppalari berilgan bo'lib, $f : G \to G'$ va $g : G' \to G$ gomomorfizmlar uchun $f \circ g = 1_{G'}$ bo'lsa, ya'ni $f \circ g$ akslantirish G' da ayniy bo'lsa, u holda quyidagilar o'rinli.*

1) $Kerg = 0$.

2) $Imf = G'$.

3) $Kerf \oplus Img = G$.

Isbot. 1) Agar $y \in \mathrm{Ker}g$ bo'lsa, u holda $g(y) = 0$ bo'lib,

$$y = (f \circ g)(y) = f(g(y)) = f(0) = 0.$$

Demak $y = 0$, ya'ni $\mathrm{Ker}g = 0$.

2) Agar $y \in G'$ bo'lsa, u holda

$$y = (f \circ g)(y) = f(g(y)) \in \mathrm{Im}g$$

ekanligidan $\mathrm{Im}f = G'$ kelib chiqadi.

3) Ixtiyoriy $x \in G$ elementni $x = x - g(f(x)) + g(f(x))$ deb yozib olsak,

$$f(x - g(f(x))) = f(x) - (f \circ g)(f(x)) = f(x) - f(x) = 0.$$

Demak, $x - g(f(x)) \in \mathrm{Ker}f$. Ikkinchi tomondan esa, $g(f(x)) \in \mathrm{Im}g$. Bu esa, ixtiyoriy $x \in G$ element $x = y + z$ kabi ifodalanishini bildiradi, bu yerda

$$y = x - g(f(x)) \in \mathrm{Ker}f, \quad z = g(f(x)) \in \mathrm{Im}g.$$

Endi $\mathrm{Ker}f \cap \mathrm{Im}g = 0$ ekanligini ko'rsatamiz. Aytaylik, $a \in \mathrm{Ker}f \cap \mathrm{Im}g$ bo'lsin. U holda $f(a) = 0$ va qandaydir $y \in G'$ uchun $a = g(y)$. Bundan esa,

$$a = g(y) = g((f \circ g)(y)) = g(f(g(y))) = g(f(z)) = g(0) = 0$$

kelib chiqadi. Demak, $\mathrm{Ker}f \cap \mathrm{Im}g = 0$, ya'ni $G = \mathrm{Ker}f \oplus \mathrm{Im}g$. □

Biz yuqorida hosil qiluvchi elementlari cheklita bo'lgan gruppalar har doim ham erkin abel gruppasi bo'lavermasligini ta'kidlagan edik. Quyidagi teoremada ularning erkin abel gruppasi bo'lishining zaruriy va yetarlilik shartini keltiramiz.

3.2.3-teorema. *Hosil qiluvchilari cheklita bo'lgan abel gruppasi erkin abel gruppasi bo'lishi uchun uning buralishga ega bo'lmasligi, ya'ni $T(G) = 0$ bo'lishi zarur va yetarli.*

Isbot. ***Zaruriyligi.*** Aytaylik, G erkin abel gruppasi bo'lib, $\{a_1, a_2, \ldots, a_k\}$ uning bazisi bo'lsin. Ixtiyoriy $x \in T(G)$ element uchun $ord(x) = r$, ya'ni $rx = 0$ va $x = n_1a_1 + n_2a_2 + \cdots + n_ka_k$. U holda

$$0 = rx = r(n_1a_1 + n_2a_2 + \cdots + n_ka_k) = (rn_1)a_1 + (rn_2)a_2 + \cdots + (rn_k)a_k$$

bo'lib, bundan $rn_i = 0, 1 \leq i \leq k$ kelib chiqadi. $r > 0$ ekanligidan $n_i = 0$ tenglikni olamiz. Bu esa $x = 0$ ekanligini, ya'ni $T(G) = 0$ bo'lishini bildiradi.

Yetarliligi. Aytaylik $G = \langle a_1, a_2, \ldots, a_k \rangle$, ya'ni hosil qiluvchilari cheklita bo'lgan abel gruppasi bo'lib, $T(G) = 0$ bo'lsin. U holda bunday gruppalarning erkin abel gruppasi bo'lishini k ga nisbatan induksiya metodi orqali ko'rsatamiz. $k = 1$ bo'lgan holda $G = \langle a_1 \rangle \simeq \mathbb{Z}$ bo'lib, u erkin abel gruppasi bo'ladi. Endi hosil qiluvchi elementlar soni k tadan kam bo'lgan gruppalar uchun teorema sharti o'rinli deb faraz qilib, k uchun to'g'ri bo'lishini ko'rsatamiz. Agar $\{a_1, a_2, \ldots, a_k\}$ elementlar to'plami chiziqli erkli bo'lsa, u holda u bazis bo'lib, G erkin abel gruppasi bo'ladi, ya'ni $G \simeq F_k$.

Faraz qilaylik, $\{a_1, a_2, \ldots, a_k\}$ elementlar to’plami chiziqli bog‘liq bo‘lsin, ya’ni hech bo‘lmaganda bittasi noldan farqli bo’lgan $n_1, n_2, \ldots, n_k$ butun sonlari topilib,

$$n_1a_1 + n_2a_2 + \cdots + n_ka_k = 0$$

bo‘lsin. Ushbu sonlarning eng katta umumiy bo‘luvchisi $d = EKUB(n_1, n_2, \ldots, n_k)$ uchun $m_i = \frac{n_i}{d}$ deb olsak, u holda

$$d(m_1a_1 + m_2a_2 + \cdots + m_ka_k) = 0.$$

$T(G) = 0$ va $d \neq 0$ ekanligidan

$$m_1a_1 + m_2a_2 + \cdots + m_ka_k = 0 \tag{3.1}$$

tenglikni olamiz, bu yerda $EKUB(m_1, m_2, \ldots, m_k) = 1$. Agar $m_1 = \pm 1$ bo‘lsa, u holda $a_1 = \pm(m_2a_2 + \cdots + m_ka_k)$ bo‘lib, G gruppa $k-1$ ta hosil qiluvchi elementga ega ekanligini bildiradi. U holda induksiya faraziga ko‘ra $G = \langle a_2, a_3, \ldots, a_k\rangle$ gruppa erkin bo‘ladi. Agar $m_1 \neq 0$ va $m_2 = \cdots = m_k = 0$ bo‘lsa, u holda $m_1a_1 = 0$ bo‘lib, gruppa buralishga ega bo‘lmaganligi uchun $a_1 = 0$ bo‘ladi. Ushbu holda ham biz $G = \langle a_2, a_3, \ldots, a_k\rangle$ ekanligini, ya’ni induksiya faraziga ko‘ra uning erkin gruppa bo‘lishini hosil qilamiz. Demak, kamida ikkita m_i, m_j noldan farqli sonlari mavjud. Umumiylikka ziyon yetkazmagan holda $|m_1| \geq |m_2| > 0$ deb olish mumkin. U holda a_2 hosil qiluvchi element o‘rniga $a_2' + ma_1$ element olish hisobiga biz yangi $\{a_1, a_2', \ldots, a_k\}$ hosil qiluvchilarga ega bo‘lamiz. Ushbu hosil qiluvch elementlarga nisbatan (3.1) tenglik quyidagi shaklga keladi.

$$(m_1 - mm_2)a_1 + m_2a_2' + \cdots + m_ka_k = 0.$$

Ushbu tenglikda m sonini $|m_1 - mm_2| < m_2$ tengsizlik o‘rinli bo‘ladigan qilib tanlash mumkin. Demak, a_1 elementning oldidagi koeffitsientni kamaytirish mumkin. Ushbu jarayonni davom ettirib, biz yuqoridagi qaragan holga, ya’ni $m_1 = \pm 1$ ga keltirishimiz mumkin. Demak, hosil qiluvchi elementlar chiziqli erkli bo‘ladi, ya’ni G gruppa erkin gruppa bo‘ladi. $\square$

Endi biz rangi k ga teng bo‘lgan F_k erkin gruppasidan ixtiroriy G abel gruppasiga bo‘lgan gomomorfizmlar haqida to’xtalib o‘tamiz. Bizga rangi k ga teng bo‘lgan F_k erkin gruppa berilgan bo‘lib, $\{a_1, a_2, \ldots, a_k\}$ uning bazisi bo‘lsin. Ushbu $a_1, a_2, \ldots, a_k$ elementlarni G gruppaning $b_1, b_2, \ldots, b_k$ elementlariga o‘tkazuvchi φ akslantirishni qaraymiz, ya’ni $\varphi(a_i) \in G$.

3.2.4-teorema. *Agar F_k erkin gruppaning $\{a_1, a_2, \ldots, a_k\}$ bazisini G gruppa elementlarigi o‘tkauvchi φ akslantirish berilgan bo‘lsa, u holda $f(a_i) = \varphi(a_i)$, $1 \leq i \leq k$ shartni qanoatlantiruvchi $f : F_k \to G$ gomomorfizm mavjud va yagona.*

Isbot. Aytaylik, $\varphi(a_i) = b_i$, $1 \le i \le k$ bo'lsin. Ixtiyoriy $x \in F_k$ element uchun

$$x = n_1a_1 + n_2a_2 + \cdots + n_ka_k$$

bo'lganligi uchun $f : F_k \to G$ akslantirishni $f(x) = n_1b_1 + n_2b_2 + \cdots + n_kb_k$ kabi aniqlaymiz. U holda, $f(a_i) = \varphi(a_i)$, $1 \le i \le k$ bo'lib, ushbu akslantirish gomomorfizm bo'ladi. Haqiqatdan ham, ixtiyoriy $x, y \in F_k$ uchun

$$x = n_1a_1 + n_2a_2 + \cdots + n_ka_k, \quad y = m_1a_1 + m_2a_2 + \cdots + m_ka_k$$

bo'lsa, u holda $x + y = (n_1 + m_1)a_1 + (n_2 + m_2)a_2 + \cdots + (n_k + m_k)a_k$ bo'lib,

$$f(x + y) = (n_1 + m_1)b_1 + (n_2 + m_2)b_2 + \cdots + (n_k + m_k)b_k =$$

$$= n_1a_1 + n_2a_2 + \cdots + n_ka_k + m_1a_1 + m_2a_2 + \cdots + m_ka_k = f(x) + f(y).$$

Ixtiyoriy $g : F_k \to G$ gomomorfizm $g(a_1), g(a_2), \ldots, g(a_k)$ elementlar orqali bir qiymatli aniqlanganligi uchun $f(a_i) = \varphi(a_i)$, $1 \le i \le k$ shartni qanoatlantiruvchi gomomorfizmning yagona ekanligi kelib chiqadi. □

Yuqoridagi teoremadan ko'rinadiki, ixtiyoriy F_k erkin gruppaning bazisini G abel gruppasiga o'tkazuvchi akslantirishni gomomorfizmgacha davom ettirish mumkin va bunday gomomorfizm yagona ravishda aniqlanadi. Quyidagi teoremada esa, hosil qiluvchilari chekli bo'lgan ixtiyoriy abel gruppasi erkin abel gruppasining gomomorf obrazi bo'lishini ko'rsatamiz.

3.2.5-teorema. *Hosil qiluvchilari $\{b_1, b_2, \ldots, b_k\}$ bo'lgan ixtiyoriy G abel gruppasiga F_k gruppadan $f : F_k \to G$ syurektiv gomomorfizm mavjud va $G \simeq F_k/Kerf$ bo'ladi.*

Isbot. Ayatylik, F_k erkin gruppaning bazisi $\{a_1, a_2, \ldots, a_k\}$ bo'lsin. U holda 3.2.4-teoremaga ko'ra F_k gruppadan G gruppaga $f(a_i) = b_i$ shartni qanoatlantiruvchi gomomorfizm mavjud. $b_1, b_2, \ldots, b_k$ elementlar G gruppaning hosil qiluvchi elementlari bo'lganligi uchun ushbu f gomomorfizm syurektiv bo'ladi. Gomomorfizm haqidagi birinchi teoremaga ko'ra esa, $G \simeq F_k/\mathrm{Ker} f$. □

Endi hosil qiluvchilari cheklita bo'lgan abel gruppalarining tuzilishi haqida to'liq ma'lumot beruvchi teoremani keltiramiz.

3.2.6-teorema. *Hosil qiluvchilari cheklita bo'lgan ixtiyoriy abel gruppasi chekli abel gruppasi va rangi chekli bo'lgan erkin abel gruppasining to'g'ri yig'indisi shaklida ifodalanadi. Ya'ni $G = T(G) \oplus H$, bu yerda $T(G)$ chekli abel gruppasi va $H \simeq F_k$.*

Bundan tashqari, bunday yoyilma yagonadir, ya'ni agar $G = A \oplus H = B \oplus M$ bo'lib, A, B chekli abel gruppalari va $H \simeq F_k$, $M \simeq F_s$ bo'lsa, u holda $A = B$ va $H \simeq M$ (ya'ni $s = k$) bo'ladi.

Isbot. Ayatylik, G hosil qiluvchilari cheklita bo'lgan gruppa bo'lib, $\{b_1, b_2, \dots, b_n\}$ uning hosil qiluvchilari bo'lsin. U holda $G/T(G)$ ham hosil qiluvchilari cheklita bo'lgan gruppa bo'lib, $T(G/T(G)) = 0$ bo'ladi. U holda 3.2.3-teoremaga ko'ra $G/T(G)$ gruppa erkin abel gruppasi bo'ladi. Demak, $G/T(G) \simeq F_k$, bu yerda $k = rk(G/T(G))$. Ixtiyoriy gruppadan uning biror normal qism gruppasi bo'yicha faktor gruppasiga tabiiy gomomorfizm mavjud va u syurektiv bo'lganligi uchun $f : G \to F_k$ syurektiv gomomorfizm mavjud. U holda F_k gruppaning $\{a_1, a_2, \dots, a_k\}$ bazis elementlariga o'tuvchi $c_1, c_2, \dots, c_k \in G$ elementlar topilib, $f(c_i) = a_i$ bo'ladi. Endi $\varphi(a_i) = c_i$, $\varphi : F_k \to G$ akslantirishni qarasak, 3.2.4-teoremaga ko'ra ushbu akslantirishni $g : F_k \to G$ gomomorfizmgacha davom ettirish mumkin, ya'ni $g(a_i) = c_i$. Demak, $f : G \to F_k$ va $g : F_k \to G$ gomomorfizmlar mavjud bo'lib, ular uchun

$$(f \circ g)(a_i) = f(g(a_i)) = f(c_i) = a_i$$

munosabat o'rinli. Bu esa, $f \circ g = 1_{F_k}$ ekanligini anglatadi. U holda 3.2.3-lemmaga ko'ra $G = \mathrm{Ker} f \oplus \mathrm{Im} g$. Agar $\mathrm{Ker} f = T(G)$ ekanligini hisobga olib $H = \mathrm{Im} g$ deb belgilasak, $G = T(G) \oplus H$ kelib chiqadi. Endi $H \simeq F_k$ ekanligini ko'rsatamiz. Buning uchun $f_H : G \to F_k$ akslantirishni qarasak, $f(H) = f(G) = F_k$ ekanligidan f_H ning syurektiv ekanligi,

$$\mathrm{Ker} f_H = \mathrm{Ker} f \cap H = \mathrm{Ker} f \cap \mathrm{Im} g = 0$$

tenglikdan esa, uning inyektivligi kelib chiqadi. Demak, $H \simeq F_k$.

Endi $T(G)$ gruppaning chekli ekanligini ko'rsatamiz. $T(G) \simeq G/H$ ekanligidan uning ham hosil qiluvchilari chekli ekanligi kelib chiqadi. Demak, $T(G)$ gruppaning $x_1, x_2, \dots, x_s$ hosil qiluvchi elementlari mavjud bo'lib, barchasi chekti tartibga ega, ya'ni $ord(x_i) = r_i$ U holda G gruppaning elementlari

$$n_1 x_1 + n_2 x_2 + \cdots + n_s x_s, \quad 0 \le n_i \le r_i$$

ko'rinishida bo'lib, $|T(G)| \le r_1 r_2 \dots r_s$ bo'ladi. Ya'ni $T(G)$ chekli gruppa.

Endi teoremaning ikkinchi qismini isbotlaymiz. Aytaylik, $G = A \oplus H = B \oplus M$ bo'lib, A, B chekli abel gruppalari va $H \simeq F_k$, $M \simeq F_s$ bo'lsin, u holda

$$T(A) = A, \quad T(B) = B, \quad T(H) = 0, \quad T(M) = 0.$$

Bundan esa

$$A = T(A) = T(A) \oplus T(H) = T(A \oplus H) = T(G) =$$

$$= T(B \oplus M) = T(B) \oplus T(M) = T(B) = B$$

ekanligi, ya'ni $A = B$ kelib chiqadi. Bundan tashqari,

$$F_k \simeq H \simeq G/A = G/B \simeq M \simeq F_s$$

ekanligidan $k = s$ hosil bo‘ladi. □

Shunday qilib, biz yuqoridagi teoremada hosil qiluvchilari cheklita bo‘lgan ixtiyoriy abel gruppasi chekli abel gruppasi va rangi chekli bo‘lgan erkin abel gruppasining to‘g‘ri yig‘indisi shaklida $G = T(G) \oplus F_k$ kabi ifodalanishini ko‘rsatdik. O’z navbatida $T(G)$ chekli abel gruppasi siklik gruppalarning to‘g‘ri yig‘indisidan iborat bo‘lganligi uchun $T(G) \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s}$. Rangi k ga teng bo‘lgan F_k erkin abel gruppasi esa cheksiz siklik gruppalarning to‘g‘ri yig‘indisi shaklida ifodalanadi, ya’ni $F_k \simeq \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{k \text{ ta}}$. Demak, hosil qiluvchilari cheklita bo‘lgan ixtiyoriy abel gruppasi uchun quyidagi yoyilma o‘rinli bo‘ladi

$$G \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_s} \oplus \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{k \text{ ta}}.$$

Ushbu yoyilmada $m_1, m_2, \ldots, m_s$ sonlarini invariant faktorlar deb ya’ni $m_{j+1} \,| m_j$ shartni qanoatlantiradigan qilib tanlashimiz mumkin.

3.2.1 Mustaqil ishlash uchun misol va masalalar

1. $(\mathbb{Q}, +)$ gruppaning hosil qiluvchilari chekli bo‘lgan gruppa emasligini isbotlang.
2. $\mathbb{Z} \oplus \mathbb{Z}_6$ gruppa hosil qiluvchilari chekli bo‘lgan gruppa bo‘lib, erkin gruppa emasligini ko‘rsating.
3. $G = \mathbb{Z}_4 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}$ gruppa uchun $T(G)$ qism gruppani aniqlang.
4. $\mathbb{Z}_{20} \oplus \mathbb{Z}_{75} \oplus \mathbb{Z}_{90}$ va $\mathbb{Z}_{120} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{45}$ gruppalar izomorf bo‘ladimi?
5. $\mathbb{Z}_{200} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{36}$ va $\mathbb{Z}_{120} \oplus \mathbb{Z}_{18} \oplus \mathbb{Z}_{100}$ gruppalar izomorf bo‘ladimi?
6. $\mathbb{Z}_{15} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z} \oplus \mathbb{Z}$ va $\mathbb{Z}_{108} \oplus \mathbb{Z}_{50} \oplus \mathbb{Z} \oplus \mathbb{Z}$ gruppalar izomorf bo‘ladimi?
7. Hosil qiluvchilari chekli bo‘lgan abel gruppasining gomomorf obrazi yana hosil qiluvchilari chekli gruppa ekanligini isbotlang.
8. Isbotlang $Aut(\mathbb{Z}_{30}) \simeq Aut(\mathbb{Z}_{15})$.
9. Isbotlang $Aut(\mathbb{Z} \oplus \mathbb{Z}_2) \simeq Aut(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$.

BOB 4

Gruppalarga oid qo‘shimcha tushuncha va teoremalar

4.1 Gruppaning to‘plamga ta’siri

Ma’lumki, gruppalar nazariyasi vujudga kelishida o‘rin almashtirishlar gruppasining aniqlanishi asosiy omil hisoblanadi. Chunki, dastlabki o‘rganilgan kommutativ bo‘lmagan gruppalar aynan o‘rin almashtirishlar gruppasidir. Keyinchalik gruppaning abstrakt ta’rifi va undagi tushunchalar kiritilishi xam aynan o‘rin almashtirishlar gruppasining xususiyatlarini o‘rganish uchun xizmat qilgan.

Ma’lumki, o‘rin almashtirishlar gruppasi bu biror X to‘plamdagi barcha o‘zaro bir qiymatli akslantirishlar to‘plamidan iborat bo‘lib, u $S(X)$ kabi belgilanadi. Agar $\forall f \in S(X)$ va $\forall a \in X$ elementlar uchun, $(f, a) \to f(a)$ elementni moslikni qarasak, biz $S(X) \times X$ to‘plamni X to‘plamga akslantiruchchi amal aniqlagan bo‘lamiz.

Ushbu aniqlangan amal kabi ixtiyoriy bo‘sh bo‘lmagan X to‘plam va ixtiyoriy G gruppa uchun gruppaning to‘plamga ta’siri tushunchasi kiritiladi.

Bizga G gruppa va bo‘sh bo‘lmagan X to‘plam berilgan bo‘lib, $G \times X$ to‘plamni X to‘plamga akslantiruvchi $\star : G \times X \to X$ amal aniqlangan bo‘lsin. Ixtiyoriy $g \in G$ va $x \in S$ elementlarning ushbu amal yordamida aniqlangan $g \star x$ qiymati o‘qniga (g, x) yoki gx belgilashlardan ham foydalaniladi.

4.1.1-ta’rif. *Agar $\star : G \times X \to X$ amal aniqlangan bo‘lib, quyidagi shartlar bajarilsa,*

- $(g_1 \cdot g_2) \star x = g_1 \star (g_2 \star x)$, *bu yerda* $x \in X, g_1, g_2 \in G$,
- $e \star x = x$, *bu yerda* $e \in G$ *gruppaning birlik elementi,*

u holda G gruppaning X to‘plamga ***(chap) ta’siri*** *aniqlangan deyiladi.*

Agar G gruppaning X to‘plamga (chap) ta’siri aniqlangan bo‘lsa, u holda G gruppa X to‘plamga ta’sir qiladi deyiladi, X to‘plam esa G-to‘plam deb ataladi.

Ushbu misolda yuqorida ta'kidlab o'tilgan $S(X)$ o'rin almashtirishlar gruppasining X to'plamga ta'siri aniqlanishini ko'rsatamiz.

4.1.1-misol. *Bizga X to'plam va $G = S(X)$ o'rin almashtirishlar gruppasi berilgan bo'lsin. G gruppaning X to'plamga ta'sirini quyidagicha aniqlaymiz*

$$f \star x = f(x), \quad \forall f \in G, \ x \in X.$$

U holda $e \in G$ birlik element uchun $e \star x = e(x) = x$ va ixtiyoriy $f, g \in G$ uchun

$$(f \circ g) \star x = (f \circ g)(x) = f(g(x)) = f \star (g(x)) = f \star (g \star x)$$

tengliklar bajariladi. Ya'ni G gruppaning X to'plamga ta'siri aniqlangan.

Quyidagi misolda X to'plam sifatida G gruppaning biror H normal qism gruppasini olib, uning G-to'plam bo'lishini ko'rsatamiz.

4.1.2-misol. *Aytaylik, G gruppa va uning H normal qism gruppasi berilgan bo'lsin. G gruppaning H to'plamga ta'sirini quyidagicha aniqlaymiz:*

$$g \star h = g \cdot h \cdot g^{-1}, \quad \forall g \in G, \ \forall h \in H.$$

H normal qism gruppa bo'lganligi uchun $g \star h \in H$ bo'lib, $e \star h = e \cdot h \cdot e^{-1} = h$ va $\forall g_1, g_2 \in G$ uchun

$$(g_1 \cdot g_2) \star h = (g_1 \cdot g_2) \cdot h \cdot (g_1 \cdot g_2)^{-1} = (g_1 \cdot g_2) \cdot h \cdot (g_2^{-1} \cdot g_1^{-1})$$

$$= g_1 \cdot (g_2 \cdot h \cdot g_2^{-1}) \cdot g_1^{-1} = g_1 \cdot (g_2 \star h) \cdot g_1^{-1} = g_1 \star (g_2 \star h)$$

tengliklar o'rinli bo'ladi. Demak, H qism gruppa G-to'plam bo'ladi.

4.1.3-misol. *Aytaylik G gruppaning biror H qism gruppasi berilgan bo'lsin, $X = \{aH \mid a \in G\}$ deb olsak, u holda G gruppaning X to'plamga ta'sirini quyidagicha aniqlaymiz:*

$$g \star (aH) = (g \cdot a)H, \quad \forall g \in G, \ \forall aH \in X.$$

U holda, $e \star (aH) = (e \cdot a)H = aH$ va $(g_1 \cdot g_2) \star (aH) = ((g_1 \cdot g_2) \cdot a)H = (g_1(\cdot g_2 \cdot a))H = g_1 \star (g_2 \star (aH))$ ekanligidan X ning G-to'plam ekanligi kelib chiqadi.

Endi G gruppaning X to'plamga ta'siri aniqlangan bo'lsa, bu orgali X to'plamda ekvivalentlik munosabatini kiritish mumkinligini ko'rsatamiz. Buning uchun X to'plamning a, b elementlari orasidagi $a \sim b$ munosabatni quyidagicha aniqlaymiz:

$$\text{agar } g \in G \text{ mavjud bo'lib, } g \star a = b \text{ bo'lsa, u holda } a \sim b.$$

Quyidagi teoremada, ushbu $\sim$ munosabatning ekvivalentlik munosabati ekanligini isbotlaymiz

4.1.1-teorema. *Aytaylik G gruppa berilgan bo‘lib, bo‘sh bo‘lmagan X to‘plam esa G-to‘plam bo‘lsin. X to‘plamda aniqlangan $\sim$ munosabat ekvivalentlik munosabati bo‘ladi, bu yerda*

$$a \sim b \;\Leftrightarrow\; \exists g \in G,\; g \star a = b.$$

Isbot. Ixtiyoriy $a \in X$, uchun $e \star a = a$ ekanligidan $a \sim a$, ya'ni $\sim$ munosabatning refleksiv ekanligi kelib chiqadi.

Endi ushbu munosabatning simmetrik ekanligini ko‘rsatamiz. Agar $a, b \in X$ uchun $a \sim b$ bo‘lsa, u holda $g \in G$, element topilib $g \star a = b$ bo‘ladi. Bundan esa,

$$g^{-1} \star b = g^{-1} \star (g \star a) = (g^{-1} \cdot g)a = e \star a = a$$

ekanligi, ya'ni $b \sim a$ kelib chiqadi. Demak, $\sim$ munosabat simmetrik ekan.

Endi munosabatning tranzitivligini ko‘rsatamiz. Agar $a \sim b$ va $b \sim c$ bo‘lsa, u holda $g_1, g_2 \in G$ elementlar topilib, $g_1 \star a = b$ va $g_2 \star b = c$ bo‘ladi. $(g_2 \cdot g_1) \star a = g_2 \star (g_1 \star a) = g_2 \star b = c$ ekanligidan esa, $a \sim c$ ekanligi, ya'ni $\sim$ munosabatning tranzitivligi kelib chiqadi. Demak, $\sim$ munosabat ekvivalentlik munosabati bo‘ladi. $\square$

Har qanday ekvivalentlik munosabati berilgan to‘plamni o‘zaro kesishmaydigan sinflarga ajratgani uchun, yuqorida aniqlangan ekvivalentlik munosabati ham X to‘plamni sinflarga ajratadi. Ushbu sinflar G ruppaning X to‘plamdagi **orbitalari** deb ataladi. Demak, $a \in X$ elementning orbitasi $[a] = \{b \in X \mid b \sim a\}$ to‘plamdan iborat bo‘ladi va $orb(a)$ kabi belgilanadi.

Endi $a \in X$ element uchun G to‘plamning quyidagi qism to‘plamini aniqlaymiz:

$$St(a) = \{g \in G \mid g \star a = a\}$$

Ta'kidlash joizki, ushbu $St(a)$ to‘plam G gruppaning qism gruppasi bo‘ladi. Haqiqatdan ham, $e \star a = a$ ekanligidan $e \in St(a)$ kelib chiqiadi. Ixtiyoriy $g, h \in St(a)$ elementlar uchun, $g \star a = a$ va $h \star a = a$ ekanligidan quyidagi tengliklarga ega bo‘lamiz.

$$(g \cdot h) \star a = g \star (h \star a) = g \star a = \star a,$$

$$h^{-1} \star a = h^{-1} \star (h \star a) = (h^{-1} \cdot h) \star a = e \star a = a.$$

Demak, $g \cdot h \in St(a)$ va $h^{-1} \in St(a)$, ya'ni $St(a)$ to‘plam G gruppaning qism gruppasi bo‘ladi. Ushbu $St(a)$ qism gruppalar **statsionar qism gruppalar** yoki **stabilizatorlar** deyiladi. Quyidagi lemmada $a \in X$ elementning orbitasi va stabilizatori orasidagi munosabatni keltiramiz.

4.1.1-lemma. *Aytaylik, G gruppaning X to‘plamga ta’siri aniqlangan bo‘lsin. Ixtiyoriy $a \in X$ element uchun $[G : St(a)] = |orb(a)|$ tenglik o‘rinli. Ya’ni, a elementning orbitasi elementlari soni $St(a)$ qism gruppaning indeksiga teng.*

Isbot. $\mathcal{L}$ orqali $St(a)$ qism gruppaning barcha chap qo‘shni sinflaridan tashkil topgan sistemani bilgilaymiz, ya’ni $\mathcal{L} = \{gSt(a) \mid g \in G\}$. Biz ushbu $\mathcal{L}$ to‘plam va $orb(a)$ orasida o‘zaro bir qiymatli moslik o‘rnatamiz. Buning uchun $f : \mathcal{L} \to orb(a)$ akslantirishni quyidagicha aniqlaymiz:

$$f(gSt(a)) = g \star a, \quad \forall gSt(a) \in \mathcal{L}.$$

Bu akslantirishning to‘g‘ri aniqlanganligi va inyektivligi quyidagi munosabatlardan kelib chiqadi:

$$g_1St(a) = g_2St(a) \;\Leftrightarrow\; g_2^{-1} \cdot g_1 \in St(a)$$

$$\Leftrightarrow\; g_2^{-1} \star (g_1 \star a) = (g_2^{-1} \cdot g_1) \star a = a \;\Leftrightarrow\; g_1 \star a = g_2 \star a.$$

Uning syurektiv bo‘lishi ham osongina kelib chiqadi, chunki $\forall b \in orb(a)$ uchun $g \in G$ topilib, $g \star a = b$, ya’ni, $f(gSt(a)) = g \star a = b$.

Demak, $f : \mathcal{L} \to orb(a)$ biyektiv, ya’ni $[G : St(a)] = |\mathcal{L}| = |orb(a)|$. □

Agar gruppaning $a, b \in G$ elementlari uchun $\exists g \in G$ element topilib, $b = g^{-1} \cdot a \cdot g$ tenglik o‘rinli bo‘lsa, u holda a va b elementlar o‘zaro **qo‘shma** elementlar deyiladi.

4.1.2-misolda H sifatida G gruppani o‘zini olsak, gruppaning o‘zidan o‘ziga bo‘lgan ta’sirini hosil qilamiz. $a \in G$ elementning ushbu ta’sirdagi orbitasi, unga qo‘shma bo‘lgan elementlar to‘plamidan iborat bo‘ladi, ya’ni

$$orb(a) = \{b \in G \mid b = g^{-1} \cdot a \cdot g\}.$$

Ushbu to‘plamga a elementning qo‘shma sinfi deb ataladi. Ravshanki, G gruppa o‘zaro kesishmaydigan qo‘shma sinflarning birlashmasidan iborat bo’ladi.

Endi qism gruppalar uchun qo‘shmalik ta’rifini keltiramiz. Agar G gruppaning H va K qism gruppalari uchun $\exists g \in G$ element topilib, $H = g^{-1} \cdot K \cdot g$, tenglik o‘rinli bo‘lsa, u holda bu **qism gruppalar qo‘shma** deyiladi.

Yuqoridagi lemmadan G chekli gruppa bo‘lsa, u holda ixtiyoriy elementning orbitasining quvvati (elementlar soni) gruppaning tartibi bo‘luvchisi ekanligi kelib chiqadi. Bundan tashqari ekvivalent sinflarning aniqlanishi undagi elementning tanlanishiga bog‘liq bo‘lmaganligini hisobga olsak, $a \sim b$ ekanligidan $[G : St(a)] = [G : St(b)]$ tenglik kelib chiqadi. Yuqoridagi mulohazalardan va 4.1.1-lemmadan foydalanib, quyidagi teoremani isbotlash mumkin.

4.1.2-teorema. *Aytaylik G gruppaning X to‘plamga ta’siri aniqlangan bo‘lsin.*

1) *Agar $a, b \in X$ elementlar uchun $a \sim b$ bo'lsa, u holda $St(a)$ va $St(b)$ gruppalar o'zaro qo'shma bo'ladi.*

2) *Agar G chekli gruppa bo'lib, X chekli to'plamning ekvivalentlik munosabati orqali kesishmaydigan sinflarga yoyilmasi $X = orb(a_1) \cup orb(a_2) \cup \cdots \cup orb(a_r)$ ko'rinishida bo'lsa, u holda*

$$|X| = \sum_{i=1}^{r} [G : St(a_i)].$$

Isbot. 1) Aytaylik, $a, b \in X$ elementlar uchun $a \sim b$ bo'lsin. U holda, shunday $g \in G$ element topilib, $b = g \star a$ bo'ladi, bundan esa, $a = g^{-1} \star b$ kelib chiqadi. Ixtiyoriy $g \cdot h \cdot g^{-1} \in gSt(a)g^{-1}$ elementni qaraymiz, bu yerda $h \in St(a)$, ya'ni $h \star a = a$. U holda

$$(g \cdot h \cdot g^{-1}) \star b = g \star (h \star (g^{-1} \star b)) = g \star (h \star a) = g \star a = b.$$

Demak, $g \cdot h \cdot g^{-1} \in St(b)$, bundan esa, $gSt(a)g^{-1} \subseteq St(b)$ hosil bo'ladi. Xuddi shunga o'xshab $g^{-1}St(b)g \subseteq St(a)$ ekanligini ham ko'rsatish mumkin. Natijada biz $gSt(a)g^{-1} = St(b)$ tenglikka ega bo'lamiz, ya'ni $St(a)$ va $St(b)$ qism gruppalar o'zaro qo'shma bo'ladi.

2) 4.1.1-teoremaga ko'ra X to'plam kesishmaydigan sinflarning birlashmasi ko'rinishida ifodalanadi. X to'plam chekli bo'lganligi uchun, uni r ta sinfning birlashmasi ko'rinishida yozish mumkin. 4.1.1-lemmaga ko'ra $|X| = \sum\limits_{i=1}^{r} [G : St(a_i)]$ ekanligini hosil qilamiz. $\square$

Endi G gruppaning X to'plamga ta'siri yordamida G gruppadan $S(X)$ o'rin almashtirishlar gruppasiga gomomorfizm qurish mumkinligini ko'rsatamiz. Dastlab, ixtiyoriy $g \in G$ element uchun $\tau_g : X \to X$ akslantirishni $\tau_g(a) = g \star a$ kabi aniqlaymiz. Ushbu τ_g akslantirish o'zaro bir qiymatli akslantirish bo'ladi. Chunki,

$$\tau_g(a) = \tau_g(b) \;\Rightarrow\; g \star a = g \star b \;\Rightarrow\; a = b$$

munosabatdan uning inyektiv ekanligi kelib chiqsa, $g \star (g^{-1} \star b) = b$ tenglikdan $\forall b \in X$ uchun $a = g^{-1} \star b$ element topilishi, ya'ni akslantirishning syurektiv ekanligi kelib chiqadi.

Demak, $\tau_g \in S(X)$. Bundan tashqari, $g_1, g_2 \in G$ elementlar va $\forall a \in X$ uchun

$$\tau_{g_1 \cdot g_2}(a) = (g_1 \cdot g_2) \star a = g_1 \star (g_2 \star a) = \tau_{g_1}(g_2 \star a) = \tau_{g_1}(\tau_{g_2}(a)) = (\tau_{g_1} \circ \tau_{g_2})(a)$$

tengliklardan $\tau_{g_1 \cdot g_2} = \tau_{g_1} \circ \tau_{g_2}$ kelib chiqadi.

Endi G gruppadan $S(X)$ o'rin almashtirishlar gruppasiga $\psi : G \to S(X)$ akslantirishni quyidagicha aniqlaymiz

$$\psi(g) = \tau_g, \quad \forall g \in G.$$

U holda ψ akslantirsih uchun

$$\psi(g_1 \cdot g_2) = \tau_{g_1 \cdot g_2} = \tau_{g_1} \circ \tau_{g_2} = \psi(g_1) \circ \psi(g_2)$$

tenglik bajarilishi, ya'ni uning gomomorfizm ekanligi kelib chiqadi.

Agar X to'plam sifatida G gruppaning biror H qism gruppasi barcha chap qo'shni sinflari to'plamini olsak, ya'ni $X = \{aH | a \in G\}$ deb olsak, u holda 4.1.3-misolga ko'ra ushbu to'plamga G gruppaning ta'sirini $g(aH) = (g \cdot a)H$ kabi aniqlash mumkin. Demak, yuqoridagi mulohazalar yordamida $\psi : G \to S(X)$ gomomorfizm aniqlanadi. Ushbu tasdiq Kelining umumlashgan teoremasi deb nomlanadi.

4.1.1-tasdiq. *Aytaylik G gruppa va uning H biror qism gruppasi burilgan bo'lib, $X = \{aH | a \in G\}$ bo'lsin. U holda $\psi : G \to S(X)$ gomomorfizm mavjud bo'lib, $Ker\psi \subseteq H$ bo'ladi.*

Isbot. Tasdiqni isbotlash uchun $\mathrm{Ker}\psi \subseteq H$ ekanligini ko'rsatish kifoya. Ixtiyoriy $g \in \mathrm{Ker}\psi$ olsak, u holda $\psi(g) = \tau_g$ akslantirish X to'plamdagi birlik akslantirish bo'ladi, ya'ni $\forall aH \in X$ uchun $\tau_g(aH) = aH$. Bundan esa, $g(aH) = aH$, $\forall aH \in X$ ekanligi, xususan $gH = H$, ya'ni $g \in H$ kelib chiqadi. Demak, $\mathrm{Ker}\psi \subseteq H$. □

Quyidagi natijada G gruppaning H qism gruppasi bo'yicha indeksi orqali normal qism gruppasi mavjudligini aniqlash kriteriyasini keltiramiz.

4.1.1-natija. *Aytaylik G gruppa va ining indeksi n ga teng bo'lgan H xosmas qism gruppasi berilgan bo'lsin, Agar G gruppaning tartibi $n!$ ning bo'luvchisi bo'lmasa, u holda G gruppa notrivial normal bo'luvchiga ega.*

Isbot. 4.1.1-tasdiqqa ko'ra, $\psi : G \to S(X)$ gomomorfizm mavjud bo'lib, $\mathrm{Ker}\psi \subseteq H$ bo'ladi. Bundan esa, $G/\mathrm{Ker}\psi \simeq \psi(G) \subset S(X)$ kelib chiqadi. H qism gruppaning indeksi n ga teng bo'lganligi uchun $|S(X)| = n!$, demak $\psi(G)$ gruppaning tartibi $n!$ ning bo'luvchisi bo'ladi. Ya'ni $|G/\mathrm{Ker}\psi|$ soni ham $n!$ ning bo'luvchisi. Lekin G gruppaning tartibi $n!$ ning bo'luvchisi bo'lmaganligi uchun $|\mathrm{Ker}\psi| \neq 1$ kelib chiqadi. Ixtiyoriy gomomorfizmning yadrosi normal bo'luvchi bo'lganligi, hamda $\mathrm{Ker}\psi \neq e$ va $\mathrm{Ker}\psi \subseteq H$ ekanligidan uning notrivial normal bo'luvchi ekanligi kelib chiqadi. □

Endi qo'zg'almas nuqta ta'rifini kiritamiz.

4.1.2-ta'rif. *Aytaylik G gruppaning X to'plamga ta'siri aniqlangan bo'lsin. Agar $g \star a = a$ tenglik bajarilsa, u holda $a \in X$ element $g \in G$ elementga nisbatan* ***qo'zg'almas nuqta*** *deyiladi. Agar $a \in X$ element G gruppaning barcha elementlariga nisbatan qo'zg'almas bo'lsa, u holda u G gruppaga nisbatan qo'zg'almas nuqta deyiladi.*

X^g orqali X to‘plamning g elementga nisbatan qo‘zg‘almas nuqtalar to‘plamini belgilaymiz, ya’ni

$$X^g = \{a \in X \mid g \star a = a\}.$$

X to‘plamning berilgan ta’sirdagi orbitalar sonini $|X/G|$ kabi belgilaymiz. Ushbu teoremada orbitalar sonini qo‘zg‘almas nuqtalar soni orqali beruvchi ifodasi keltiriladi.

4.1.3-teorema (**Bernsayd lemmasi**). *Aytaylik, G chekli gruppaning X chekli to‘plamga ta’siri aniqlangan bo‘lsin. U holda*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|.$$

Isbot. Quyidagi to‘plamni qaraymiz

$$T = \{(g,a) \in G \times X \mid g \star a = a\}$$

Agar T to‘plamning elementlari sonini $g \in G$ elementni fiksirlab, unga mos keladigan qo‘zg‘almas nuqtalar to‘plami X^g bo‘yicha sanab chiqsa, u holda $|T| = \sum\limits_{g\in G}|X^g|$ tenglik o‘rinli bo‘ladi.

Ikkinchi tomondan esa, agar $a \in X$ elementni fiksirlab, bu elementga mos keluvchi $St(a)$ qism gruppalarning elementi bo‘yicha sanab chiqsak, $|T| = \sum\limits_{a\in X}|St(a)|$ bo‘ladi.

Aytaylik, $|X/G| = r$ bo‘lsin, ya’ni $X = orb(a_1) \cup orb(a_2) \cup \cdots \cup orb(a_r)$, u holda

$$\sum_{g\in G}|X^g| = \sum_{a\in orb(a_1)}|St(a)| + \sum_{a\in orb(a_2)}|St(a)| + \cdots + \sum_{a\in orb(a_k)}|St(a)|.$$

Agar a va b elementlar bitta orbitaga tegishli bo‘lsa, ya’ni $orb(a) = orb(b)$ bo‘lsa, u holda $[G : St(a)] = [G : St(b)]$ bo‘lib, $|St(a)| = |St(b)|$ kelib chiqadi. Bundan esa,

$$\begin{aligned}\sum_{g\in G}|X^g| &= |orb(a_1)||St(a_1)| + |orb(a_2)||St(a_2)| + \cdots + |orb(a_r)||St(a_r)| \\ &= \frac{|G|}{|St(a_1)|}|St(a_1)| + \frac{|G|}{|St(a_2)|}|St(a_2)| + \cdots + \frac{|G|}{|St(a_r)|}|St(a_r)| \\ &= r|G|,\end{aligned}$$

kelib chiqadi, ya’ni orbitalar soni r uchun quyidagi tenglikka ega bo‘lamiz $r = \frac{1}{|G|}\sum\limits_{g\in G}|X^g|$. □

4.1.4-misol. *Aytaylik G tartibi p^n (p tub son) bo‘lgan gruppa bo‘lib, X chekli G-to‘plam bo‘lsin. Agar $X_0 = \{a \in X \mid g \star a = a, \ \forall g \in G\}$, bo‘lsa $|X| - |X_0|$ sonining p ga bo‘linishini isbotlang.*

Yechish: Agar $X = orb(a_1) \cup orb(a_2) \cup \cdots \cup orb(a_r)$ bo‘lsa, u holda 4.1.2-teoremaga ko‘ra

$$|X| = \sum_{i=1}^{r} [G : St(a_i)].$$

$A = \{a_1, a_2, \dots a_r\}$ kabi belgilab olamiz, bu yerda a_i elementlar turli orbitalarga ega bo‘lgan elementlardir. Ma’lumki, $a \in X_0$ ekanligi $g \star a = a$, $\forall g \in G$ ekanligiga, bu esa $orb(a) = \{a\}$, ya’ni $St(a) = G$ ekanligiga teng kuchli. Bundan esa,

$$|X| = |X_0| + \sum_{a \in A \setminus X_0} \frac{|G|}{|St(a)|}$$

tenglikka ega bo‘lamiz. $a \in A \setminus X_0$ elementlar uchun $St(a) \neq G$ ekanligidan, ushbu elementlar uchun $\frac{|G|}{|St(a)|} \neq 1$ kelib chiqadi. $|G| = p^n$ bo‘lganligi uchun, ushbu $\frac{|G|}{|St(a)|}$ sonlari ham p ninq qandaydir darajasi ko‘rinishida ifodalanadi, ya’ni ular p ga bo‘linadi. Bundan esa, $|X| - |X_0|$ sonining p ga bo‘linishi kelib chiqadi. □

4.1.5-misol. *Agar $|G| = p^n$ (p tub son) bo‘lib, X chekli G-to‘plam uchun $p \nmid |X|$ bo‘lsa, u holda G gruppaga nisbatan qo‘zg‘almas nuqta mavjudligini isbotlang.*

Yechish: Aytaylik $X_0 = \{a \in X \mid g \star a = a, \ \forall g \in G\}$ bo‘lsin. 4.1.4-Misolga ko‘ra $|X| - |X_0|$ soni p ga bo‘linadi. $|X|$ soni p ga bo‘linmaganligi uchun $|X_0|$ ham p ga bo‘linmasligi kelib chiqadi. Demak, $X_0 \neq \emptyset$, ya’ni $a \in X_0$ qo‘zg‘almas nuqta mavjud. □

4.1.6-misol. *Aytaylik G gruppa va uning H qism gruppasi berilgan bo‘lib, $|H| = p^k$, (p tub son) bo‘lsin. U holda quyidagilarni isbotlang:*

(i) $[G : H] \equiv_p [N(H) : H]$, bu yerda $N(H) = \{g \in G \mid gHg^{-1} = H\}$.

(ii) Agar $p | [G : H]$ bo‘lsa, u holda $N(H) \neq H$.

Yechish: (i) Ushbu misolni yechish uchun H gruppaning $X = \{aH \mid a \in G\}$ to‘plamga $h(xH) = (hx)H$ kabi aniqlangan ta’sirini qaraymiz. Ushbu ta’sir bo‘yicha qo‘zg‘almas nuqtalar to‘plami

$$X_0 = \{aH \in X \mid h(aH) = aH, \ \forall h \in H\}$$

ko‘rinishida bo‘ladi.

4.1.4-misolga ko‘ra $|X| \equiv_p |X_0|$. Bundan tashqari, X to‘plmaning aniqlanishiga ko‘ra $|X| = [G : H]$. Demak, qo‘yilgan masala $|X_0| = [N(H) : H]$ tenglikni ko‘rsatish masalasiga keltirildi.

Aytaylik, $aH \in X_0$ bo'lsin, u holda $h(aH) = aH, \forall h \in H$, ya'ni $a^{-1}ha \in H, \forall h \in H$. Bundan esa, $a^{-1}Ha \subseteq H$ kelib chiqadi. H chekli gruppa bo'lganligi uchun $|a^{-1}Ha| = |H|$, demak $a^{-1}Ha = H$, ya'ni $a \in N(H)$. Demak, agar $aH \in X_0$ bo'lsa, u holda $a \in N(H)$ ekanligi hosil bo'ldi. Bu munosabatning aksi ham yuqoridagi mulohazalarni teskari tomonga yuritish oqrali kelib chiqadi. Shunday qilib biz $X_0 = \{aH \mid a \in N(H)\}$ ekanligini ko'rsatdik. Bundan esa, $|X_0| = [N(H) : H]$ kelib chiqadi, ya'ni $[G : H] \equiv_p [N(H) : H]$.

(ii) Misolning (i)-qismiga ko'ra $[G : H] \equiv_p [N(H) : H]$. Agar $[G : H]$ soni p ga bo'linsa, u holda $[N(H) : H]$ ham p ga bo'linadi. Demak, $[N(H) : H] > 1$, bundan esa $N(H) \neq H$ kelib chiqadi.

4.1.7-misol. *G chekli gruppa H uning qism gruppasi bo'lsin. Agar $[G : H] = p$ bo'lib, p soni $|G|$ ning eng kichik tub bo'luvchisi bo'lsa, u holda H to'plam G gruppaning normal qism gruppasi ekanligini isbotlang.*

Yechish: $X = \{aH \mid a \in G\}$ deb olsak, $[G : H] = p$ bo'lganligi uchun $|X| = p$. Demak, $|S(X)| = p!$. Ushbu X to'plamda $g \star (aH) = (ga)H$ kabi aniqlangan ta'sirni qaraymiz. Ma'lumki, ushbu ta'sir yordamida $\psi : G \to S(X)$ gomomorfizm $\psi(g) = \tau_g$ kabi aniqlanadi, bu yerda $\tau_g(aH) = (ga)H$.

Endi ushbu gomomorfizmning yadrosi H ga tengligini ko'rsatamiz. Aytaylik, $g \in \mathrm{Ker}\psi$ bo'lsin, u holda $(ga)H = eH$, $\forall aH \in X$, hususan $gH = H$. Bundan esa, $g \in H$ kelib chiqadi, ya'ni $\mathrm{Ker}\psi \subseteq H$.

Aytaylik $|G/\mathrm{Ker}\psi| = n$ bo'lib $n = p_1p_2 \dots p_k$ bo'lsin. Barcha p_i tub sonlari $|G|$ ning bo'luvchilari bo'lib, p soni $|G|$ ning eng kichik tub bo'luvchisi bo'lganligi uchun $p_i \geq p$. Ikkinchi tomondan esa, $|G/\mathrm{Ker}\psi|$ soni $|S(X)|$ ning bo'luvchisi ekanligini hisobga olsak, $p!$ soni n ga bo'linishini, ya'ni barcha p_i sonlariga bo'linishini hosil qilamiz. Bu esa, faqatgina $i = 1$ va $p_1 = p$ bo'lgan holdagini o'rinli bo'ladi. Shunday qilib biz $[G : \mathrm{Ker}\psi] = p$ ekanligini hosil qilsik. Bundan esa, $H = \mathrm{Ker}\psi$ kelib chiqadi, ya'ni H normal qism gruppa bo'ladi. □

4.1.8-misol. *Aytaylik G gruppa va H uning qism gruppasi bo'lsin. Agar $|G| = pn$, bu yerda p – tub son, $p \geq n$ va $|H| = p$ bo'lsa, u holda H normal qism gruppa ekanligini isbotlang.*

Yechish: Ma'lumki, $X = \{aH \mid a \in G\}$ uchun $|X| = [G : H] = \frac{|G|}{|H|} = \frac{pn}{p} = n$ bo'ladi. 4.1.7-misolga ko'ra $\psi : G \to S(X)$ gomomorfizm uchun $\mathrm{Ker}\psi \subseteq H$ o'rinli. $|H| = p$ tub son bo'lganligi uchun $\mathrm{Ker}\psi = \{e\}$ yoki $\mathrm{Ker}\psi = H$. Agar $\mathrm{Ker}\psi = \{e\}$ bo'lsa, u holda G gruppa $S(X)$ gruppaga izomorf akslantiriladi. Bundan esa $|S(X)|$ ning $|G|$ ga bo'linishi, ya'ni $pn \mid n! \Rightarrow p \mid (n-1)!$ ekanligi kelib chiqadi. Lekin $p \geq n$ bo'lganligi uchun bunday bo'lishi mumkin emas, ya'ni bu ziddiyat. Shunday qilib, biz $\mathrm{Ker}\psi = H$ ekanligini ko'rsatdik, demak H normal qism gruppa.

□

4.1.9-misol. *Tartibi $2m$ (m toq son) ga teng gruppa tartibi m ga teng normal qism gruppaga ega ekanligini ko‘rsating.*

Yechish: Keli teoremasiga ko‘ra G gruppa $S(G)$ gruppaning biror H qism gruppasiga izomorf bo‘lib, $\psi : G \to H \subseteq A(G)$ izomorfizm esa quyidagicha aniqlanadi

$$\psi(g) = \tau_g \text{ bu yerda } \tau_g(a) = g \cdot a.$$

G gruppaning tartibi juft bo‘lganligi uchun $g \in G$ element topilib, $ord(g) = 2$ bo‘ladi. U holda $\tau_g(\tau_g(a)) = g^2 a = a$ ekanligidan τ_g o‘rin almashtirish $(a,\ ga)$ ko‘rinishidagi transpositsiyalarning ko‘paytmasi ko‘rinishida ekanligi kelib chiqadi. $|G| = 2m$ bo‘lganligi uchun τ_g o‘rin almashtirish orqali hosil bo‘ladigan $(a,\ ga)$ transpositsiyalarning soni m ta bo‘ladi, ya’ni τ_g toq o‘rin almashtirish bo‘ladi. Bundan esa, H qism gruppadada toq o‘rin almashtirishlar ham mavjudligi kelib chiqadi (chunki $\tau_g \in H$).

Endi H gruppadan $\{-1, -1\}$ gruppaga $f : H \to \{-1, -1\}$ akslantirishni aniqlaymiz

$$f(\sigma) = \begin{cases} 1 & \text{agar } \sigma \text{ juft o‘rin almashtirish bo‘lsa} \\ -1 & \text{agar } \sigma \text{ toq o‘rin almashtirish bo‘lsa} \end{cases}$$

Ushbu akslantirish epimorfizm bo‘lib, $H/\mathrm{Ker} f \simeq \{-1, 1\}$ bo‘ladi. Bundan esa,

$$|\mathrm{Ker} f| = \frac{|H|}{|\{-1, 1\}|} = \frac{2m}{2} = m$$

kelib chiqadi. Demak, H gruppa tartibi m ga teng bo‘lgan normal qism gruppaga ega. H gruppa G ga izomorf bo‘lganligi uchun G ham tartibi m ga teng bo‘lgan normal qism gruppaga ega bo‘ladi. □

4.1.1 Mustaqil ishlash uchun misol va masalalar

1. S_4 o‘rin almashtirishlar gruppasining $I_3 = \{1, 2, 3, 4\}$ to‘plamga quyidagi ko‘rinishda aniqlangan $\pi \star a = \pi(a)$ ta’sirining barcha orbitalari va statsionar qism gruppalarni toping.

2. n-o‘lchamli V chiziqli fazodagi barcha xosmas chiziqli almashtirishlar gruppasining V to‘plamga ta‘siri orbitasini toping.

3. n-o‘lchamli V chiziqli fazodagi barcha ortogonal chiziqli almashtirishlar gruppasining V to‘plamga ta‘siri orbitasini toping.

4. Uch o‘lchamli V chiziqli fazodagi barcha ortogonal chiziqli almashtirishlar gruppasining $St(x)$ statsionar qism gruppalari va $orb(x)$ orbitalarini aniqlang.

5. $I_{10} = \{1, 2, \ldots, 10\}$ to‘plamga S_{10} gruppaning qiyidagi siklik qism gruppalari ta’siri barcha statsionar qism gruppalari va orbitalarini toping:
   - $G = \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 3 & 9 & 4 & 10 & 6 & 2 & 1 & 7 \end{pmatrix} \right\rangle;$
   - $G = \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 4 & 6 & 1 & 8 & 3 & 2 & 9 & 5 & 10 \end{pmatrix} \right\rangle;$
   - $G = \langle (1\ 6\ 9)(2\ 10)(3\ 4\ 5\ 7\ 8\ ) \rangle$.

6. Agar G gruppaning H qism gruppasi berilgan bo‘lib, $|H| = 11$ va $[G : H] = 4$ bo‘lsa u holda $H \lhd G$ ekanligini isbotlang.

7. Agar G gruppaning H qism gruppasi berilgan bo‘lib, $[G : H] = n$ va H qism gruppa G ning notrivial normal qism gruppasini o‘z ichiga olmasa, $\psi : H \to S_n$ monomorfizm mavjudligini isbotlang.

8. $G = GL_2(\mathbb{R})$ gruppa va $S = \mathbb{R}^2$ to‘plam berilgan bo‘lsin. U holda S ning G-to‘plam ekanligini ko‘rsating, bu yerda
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (x, y) = (ax + by, cx + dy),$$

9. Agar G gruppadan X to‘plamga ta’sir aniqlangan bo‘lib, $|G| = 77$ va $|X| = 20$ bo‘lsa u holda qo‘zg‘almas nuqta mavjudligini ko‘rsating.

10. Agar G tartibi 80 ga teng bo‘lgan gruppa H esa, unung tartibi 16 ga teng qism gruppasi bo‘lsa. G ning sodda emasligini ko‘rsating.

11. Agar G tartibi 70 ga teng bo‘lgan gruppa H esa, unung tartibi 14 ga teng qism gruppasi bo‘lsa. G ning sodda emasligini ko‘rsating.

12. Tartibi 6, 10, 14, 22, 26, 34 va 58 ga teng bo‘lgan gruppalar sodda emasligini isbotlang.

13. Tartibi 8 ga teng bo‘lgan gruppa sodda emasligini ko‘rsating

14. Tartibi 63 ga teng bo‘lgan sodda gruppaning tartibi 21 bo‘lgan qism gruppasi mavjud emasligini isbotlang.

15. Isbotlang: $N(aHa^{-1}) = aN(H)a^{-1}$;

16. G gruppaning H va K qism gruppalari berilgan bo‘lsin. $H \lhd K$ bo‘lishi uchun $H \subseteq K \subseteq N(K)$ bo‘lishi zarur va yetarli ekanligini isbotlang.

17. Agar G gruppaning H va K qism gruppalari qo‘shma bo‘lsa, u holda $N(H)$ va $N(K)$ qism gruppalar ham qo‘shma ekanligini isbotlang.

4.2 Silov teoremalari

Langranj teoremasidan ma'lumki, chekli gruppaning ixtiyoriy qism gruppasining tartibi, gruppaning bo'luvchisi bo'ladi. Lekin ushbu teoremaning teskarisi o'rinli emas, ya'ni tartibi gruppa tartibining bo'luvchisiga teng bo'lgan qism gruppa har doim ham mavjud bo'lavermaydi. Masalan, tartibi 12 ga teng bo'lgan A_4 gruppaning tartibi 6 ga teng bo'lgan qism gruppasi mavjud emas. Haqiqatdan ham, agar A_4 gruppaning tartibi 6 ga teng qism gruppasi mavjud bo'lganida, u $\mathbb{Z}_6$ va S_3 gruppalardan biriga izomorf bo'lar edi. A_4 gruppada tartibi 6 ga teng element element mavjud bo'lmaganligi uchun, uning $\mathbb{Z}_6$ gruppaga izomorf qism gruppasi mavjud emas. S_3 gruppada tartibi 2 ga teng bo'lib, o'zaro o'rin almashmaydigan (12) va (13) elementlar mavjud. Lekin A_4 gruppada bunday elementlar mavjud emas, yani uning tartibi 2 ga teng bo'lgan (12)(34), (13)(24), (14)(23) elementlarining barchasi o'zaro o'rin almashinuvchi bo'ladi. Demak A_4 gruppaning S_3 ga izomorf bo'lgan qism gruppasi ham mavjud emas.

Ushbu paragrafda biz tartibi p^k(p – tub) soniga bo'lingan har qanday gruppa tartibi p^k ga teng bo'lgan qism gruppaga ega ekanligi va bunday qism gruppalarning o'zaro qo'shmaligi, hamda ularning soni haqida malumot beruvchi teoremalarni o'rganamiz. Ushbu teoremalar norvegiyalik matematik L.Silov tomonidan 1872 yilda isbotlangan bo'lib, uning sharafiga Silov teoremalari deb nomlanadi.

Quyidagi lemmada kommutativ gruppalar uchun Langranj teoremasining teskarisi p tub son uchun o'rinli ekanligini ko'rsatamiz.

4.2.1-lemma. *Agar kommutativ gruppaning tartibi p tub soniga bo'linsa, u holda bu gruppaning tartibi p ga teng bo'lgan elementi mavjud.*

Isbot. Aytaylik, G kommutativ gruppa bo'lib, $n = |G|$ va $p \mid n$ bo'lsin. Teorema isbotini gruppa tartibiga nisbatan induksiya metodini qo'llab amalga oshiramiz. Agar $n = 2$ bo'lsa u holda teorema o'rinli bo'lishi ravshan. Teoremani tartibi n dan kichik kommutativ gruppalar uchun o'rinli deb faraz qilib, uni G gruppa uchun isbotlaymiz. Aytaylik, $a \in G, a \neq e$ element uchun $ord(a) = m$ bo'lsin. Agar $p \mid m$ bo'lsa, u holda $m = pk$ bo'lib, $(a^k)^p = a^m = e$ ekanligidan $g = a^k$ elementning tartibi p ga teng bo'ladi.

Agar $p \nmid m$ bo'lsa, u holda $H = \langle a \rangle$ qism gruppani qaraymiz. G gruppa kommutativ bo'lganligi uchun H qism gruppa G da normal bo'lib, G/H faktor gruppaning elementlari soni n dan kam bo'ladi. Bundan tashqari, $|G/H| = \frac{|G|}{m}$ va $p \nmid m$ ekanligidan, $p \mid |G/H|$ kelib chiqadi. Induksiya faraziga ko'ra, G/H gruppada tartibi p ga teng bo'lgan bH element mavjud, ya'ni $(bH)^p = b^p H = H$. Bundan esa, $b^p \in H$ kelib chiqadi. Agar $g = b^m$ deb belgilasak, $|H| = m$ bo'lganligi uchun $g^p = (b^m)^p = (b^p)^m = e$, demak $g^p = e$ bo'ladi. Ma'lumki,

$g \neq e$, aks holda $(bH)^m = H$ bo'lib, $p \mid m$ bo'lar edi, bu esa ziddiyat. Demak, $ord(g) = p$, ya'ni G gruppada tartibi p ga teng bo'lgan element mavjud. □

Yuqoridagi lemmada tartibi p tub soniga bo'linuvchi kommutativ gruppa $a \in G$, $ord(a) = p$ elementga ega ekanligini ko'rsatdik. p tub son bo'lganligi uchun ushbu a element orqali hosil bo'lgan $\langle a \rangle$ siklik gruppaning ham tartibi p ga teng, ya'ni G gruppa tartibi p ga teng bo'lgan qism gruppaga ega. Bundan esa, kommutativ gruppalar tartibi gruppa tartibining tub bo'luvchisiga teng bo'lgan qism gruppalarga ega ekanligi kelib chiqadi.

Quyidagi teoremada esa, kommutativ gruppalar tartibi gruppa tartibining ixtiyoriy bo'luvchisiga teng bo'lgan qism gruppaga ega ekanligini, ya'ni Lagranj teoremasining teskarisi kommutativ gruppalar uchun o'rinli bo'lishini ko'rsatamiz.

4.2.1-teorema. *Aytaylik, G gruppan tartibi n ga teng bo'lgan kommutativ gruppa bo'lib, m soni n ning bo'luvchisi bo'lsin. U holda G gruppaning tartibi m ga teng bo'lgan qism gruppasi mavjud.*

Isbot. $n = 1$ va $n = 2$ uchun teorema o'rinli ekanligi ravshan. Faraz qilaylik, tartibi n dan kichik kommutativ gruppalar uchun teorema o'rinli bo'lsin. Aytaylik, p tub soni uchun $p \mid m$ bo'lsin, u holda $m = pm_1$ bo'lib, 4.2.1-lemmaga ko'ra G gruppada tartini p ga teng bo'lgan H qism gruppa mavjud. G gruppa kommutativ bo'lganligi uchun H normal qism gruppa bo'lib, G/H faktor gruppa uchun

$$|G/H| = \frac{|G|}{|H|} = \frac{n}{p}$$

bo'ladi.

$|G/H| < n$ va $m_1 \mid |G/H|$ bo'lganligi uchun induksiya faraziga ko'ra G/H faktor gruppada tartibi m_1 ga teng bo'lgan K/H qism gruppa mavjud. Bu yerdagi K to'plam G gruppaning qism gruppasi bo'lib, $|K| = |K/H| \cdot |H| = m_1 p = m$ ekanligidan uning tartibi m ga teng ekanligi kelib chiqadi. □

Quyidagi teorema Koshi teoremasi nomi bilan atalib, unda tartibi p tub soniga bo'linuvchi kommutativ bo'lmagan gruppalar ham tartibi p ga teng bo'lgan elementga ega eganligi ko'rsatiladi. Ushbu teorema Silovning birinchi teoremasining xususiy xoli bo'lganligi uchun biz uni isbotsiz keltiramiz.

4.2.2-teorema (**Koshi teoremasi**). *Agar G gruppaning tartibi n ga teng bo'lib, n soni p tub soniga bo'linsa, u holda G gruppada tartibi p ga teng bo'lgan element mavjud. Xususan, tartibi p ga teng bo'lgan siklik qism gruppaga ega.*

Endi bevosita Silov teoremasi uchun kerak bo'ladigan tushuncha va xossalarni keltirib o'tamiz. Bizga biror G gruppa berilgan bo'lsin. Malumki, $g * a = g \cdot a \cdot g^{-1}$ amal orqali G gruppaning o'zidan o'ziga ta'sir aniqlash mumkin. U holda ushbu ta'sirda $a \in G$ elementning stabilizatori $C(a) = \{g \in G \mid a \cdot g = g \cdot a\}$ to'plamdan, orbitasi esa a bilan qo‘shma bo‘ladigan elementlardan iborat bo‘ladi, yani $St(a) = C(a)$, $orb(a) = \{b \in G \mid b = g \cdot a \cdot g^{-1}\}$. Bizga gruppaning to‘plamga ta’siri mavzusidan ma’lum bo‘lgan $|orb(a)| = [G : St(a)]$ tenglikdan esa $|orb(a)| = \frac{|G|}{|C(a)|}$ ekanligiga ega bo‘lamiz.

4.1.2-teoremaga ko‘ra esa

$$|G| = \sum_{a} [G : C(a)] \tag{4.1}$$

tenglikka ega bo‘lamiz, bu yerda yig‘indi turli orbitalardan bittadan olingan elementlar bo‘yicha olinadi.

Malumki, agar $a \in Z(G)$ bo‘lsa, u holda $C(a) = G$ bo‘lib, $orb(a) = \{a\}$ bo‘ladi. Demak (4.1) tenglikni

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)] \tag{4.2}$$

kabi yozish mumkin.

4.2.1-misol. *Agar S_3 o‘rin almashtirishlar gruppasi uchun yuqoridagi kabi ta’sir aniqlasak, u holda*

$$Z(e) = G, \quad Z\big((12)\big) = \{e, (12)\}, \quad Z\big((13)\big) = \{e, (13)\}, \quad Z\big((23)\big) = \{e, (23)\},$$
$$Z\big((123)\big) = Z\big((132)\big) = \{e, (123), (132)\}$$

bo‘lib,

$$orb(e) = \{e\}, \quad orb\big((12)\big) = \{(12), (13), (23)\}, \quad orb\big((132)\big) = \{(123), (132)\}$$

bo‘ladi. Demak, S_3 gruppa uchta kesishmaydigan orbitalarga ajraladi.

Endi ushbu mavzudagi asosiy tushuncha hisoblangan p-gruppa va p-qism gruppa tushunchalarini kiritamiz.

4.2.1-ta’rif. *Agar gruppaning ixtiyoriy elementi tartibi p tub sonning darajasi ko‘rinishida bo‘lsa, u holda bunday gruppaga p-gruppa deyiladi.*

4.2.2-misol.

- $\mathbf{K}_4$ – *To‘rtinchi tartibli Kleyn gruppasi p-gruppa bo‘ladi (bu yerda $p = 2$).*
- *Ixtiyoriy $n = p^k$ uchun $\mathbb{Z}_n$ gruppa p-gruppa bo‘ladi.*

Agar G gruppaning H qism gruppasi p-gruppa bo‘lsa, u holda H ga G gruppaning p-qism gruppasi deyiladi. Masalan, $\mathbb{Z}_{12}$ gruppa uchun $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ gruppa p-qism gruppa ($p = 2$) bo‘ladi.

Quyidagi teoremada ixtiyoriy p-gruppaning markazi trivial emasligi ko‘rsatamiz.

4.2.3-teorema. *Ixtiyoriy notrivial p-gruppaning markazi bittadan ko‘p elementga ega, ya’ni agar $|G| = p^k,\ k > 1$ bo‘lsa, u holda $|Z(G)| > 1$ bo‘ladi.*

Isbot. Agar $Z(G) = G$ bo‘lsa, u holda teorema isboti to‘g‘ridan to‘g‘ri kelib chiqadi. Aytaylik, $Z(G) \neq G$ bo‘lsin, u holda $a \notin Z(G)$ elementlar uchun $C(a) \neq G$ bo‘lganligidan va $C(a) \subset G$ ekanligidan $[G : C(a)]$ sonlari p ga bo‘linishi kelib chiqadi. Demak, (4.2) tenglikdagi $\sum\limits_{a \notin Z(G)} [G : C(a)]$ soni p ga bo‘linadi. Nihoyat, $|G| = p^k$ ekanligidan $|Z(G)|$ ham p ga bo‘linishi kelib chiqadi. $\square$

Yuqoridagi teoremadan quyidagi natijaga ega bo‘lamiz.

4.2.1-natija. *Tartibi p^2 (p – tub son) ga teng bo‘lgan ixtiyoriy gruppa kommutativ bo‘ladi.*

Isbot. Aytaylik $|G| = p^2$ bo‘lsin, u holda yuqoridagi teoremaga ko‘ra $|Z(G)| > 1$ bo‘lib, Lagranj teoremasidan $|Z(G)| = p$ yoki p^2 ekanligi kelib chiqadi. Faraz qilaylik $|Z(G)| = p$ bo‘lsin, u holda $a \in G \setminus Z(G)$ element mavjud bo‘lib, $C(a)$ gruppa uchun $Z(G) \subset C(a)$ va $a \in C(a)$ ekanligidan $|C(a)| = p^2$ kelib chiqadi. Bundan esa $C(a) = G$, yani $a \in Z(G)$ munosabatga ega bo‘lamiz. Bu esa ziddiyat, demak $Z(G) = G$, ya’ni G – komutativ. $\square$

Endi bevosita Silov teoremalarini keltirishga o‘tamiz.

4.2.4-teorema (Silovning birinchi teoremasi). *Agar $|G| = p^k{\cdot}m$ bo‘lsa ($p-$tub son, $(p, m) = 1$), u holda G gruppaning tartibi $p^r (0 \leq r \leq k)$ ga teng bo‘lgan qism gruppasi mavjud.*

Isbot. Aytaylik $n = |G| = p^k \cdot m$ bo‘lsin. Teorema isbotini n ga nisbatan induksiya metodi orqali amalga oshiramiz. Agar $n = 1$ bo‘lsa, u holda $k = 0$ bo‘lib, $G = \{e\}$ gruppaning izlanayotgan qism gruppasi o‘zidan iborat bo‘ladi. Demak, $n = 1$ uchun teorema o‘rinli. Endi n dan kichik tartibli gruppalar uchun teorema o‘rinli deb faraz qilib n uchun ko‘rsatamiz, bunda $k \geq 1$ deb olish mumkin.

1-hol. G gruppa markazining tartibi p ga bo‘linsin, yani $p \mid |Z(G)|$, u holda $Z(G)$ komutativ gruppaning tartibi p ga teng elementi mavjud bo‘ladi (4.2.1-Lemma qarang), demak shunday $a \in Z(G)$ element topilib, $ord(a) = p$. Ushbu element orqali hosil qilingan $H = \langle a \rangle$ gruppa esa G gruppaning normal qism gruppasi bo‘lib, G/H faktor gruppaning tartibi p^{k-1} bo‘ladi. Induksiya faraziga ko‘ra G/H gruppa tartibi $p^i (1 \leq i \leq k-1)$ bo‘lgan K_i/H qism gruppalarga ega. Ushbu $\{e\}, H, K_1, \dots K_{k-1}$ gruppalar esa G gruppaning tartiblari mos ravishda $1, p, p^2, \dots, p^k$ sonlariga teng bo‘lgan qism gruppalari bo‘ladi.

2-hol. $|Z(G)|$ soni p ga bo‘linmasin. U holda $|G| = |Z(G)| + \sum\limits_{a \notin Z(G)} [G : C(a)]$ ekanligidan ushbu tenglikning o‘ng tomonidagi ikkinchi qo‘shiluvchi ham p ga bo‘linmasligi kelib chiqadi.

Demak, shunday $a \notin Z(G)$ element topilib, $[G : C(a)]$ soni p ga bo‘linmaydi. $[G : C(a)] = \frac{|G|}{C(a)} = \frac{p^k \cdot m}{C(a)}$ ekanligidan $|C(a)|$ soni p^k ga bo‘linishi, hamda $a \in C(a), a \notin Z(G)$ ekanligidan $C(a) \neq G$ kelib chiqadi. Demak, $C(a)$ to‘plam G gruppaning tartibi n dan kichik va p^k ga bo‘linuvchi qism gruppasi. Induksiya faraziga ko‘ra $C(a)$ gruppaning tartibi $p^r (0 \leq r \leq k)$ bo‘lgan qism gruppalari mavjud bo‘lib, ular G gruppaning ham qism gruppalari bo‘ladi. □

Endi Silov p-qism gruppasining ta’rifini keltiramiz.

4.2.2-ta’rif. *Tartibi $p^k \cdot m$ ga teng bo‘lgan (p – tub son, $(p, m) = 1$) gruppaning tartibi p^k ga teng bo‘lgan qism gruppasiga **Silov p-qism gruppasi deyiladi**, ya’ni Silov p-qism gruppa G gruppaning maksimal p-qism gruppasidir.*

Ta’kidlash joizki, Silovning birinchi teoremasidan tartibi p soniga bo‘linuvchi ixtiyoriy chekli tartibli gruppa Silov p-qism gruppasiga ega ekanligi kelib chiqadi.

Biz endi Silovning ikkinchi teoremasini keltiramiz. Silovning ikkinchi teoremasida G gruppaning ixtiyoriy p-qism gruppasi qandaydir Silov p-qism gruppasida yotishi va gruppaning barcha Silov p-qism gruppalari o‘zaro qo‘shma bo‘lishi ko‘rsatiladi.

4.2.5-teorema (Silovning ikkinchi teoremasi). *Aytaylik G chekli gruppa bo‘lib, $|G| = p^k \cdot m$ bo‘lsin, bu yerda $k \geq 1$ va $(m, p) = 1$. U holda G gruppaning ixtiyoriy p-qism gruppasi qandaydir Silov p-qism gruppasida yotadi. Barcha Silov p-qism gruppalari o‘zaro qo‘shma bo‘ladi.*

Isbot. $|G| = p^k \cdot m$ bo‘lganligi uchun uning $S-$ Silov p-qism gruppasi mavjud bo‘ladi, ya’ni $|S| = p^k$. Quyidagi o‘ng qo‘shni sinflar oilasini qaraymiz

$$\mathcal{L}_S = \{xS \mid x \in G\}.$$

Aytaylik H to‘plam G gruppaning p-qism gruppasi bo‘lsin. H gruppadan $\mathcal{L}_S$ to‘plamga chap ta’sirni quyidagicha aniqlaymiz. $\forall h \in H$ va $xS \in \mathcal{L}_S$ uchun $h * xS = (h \cdot x)S$. Takidlash joizki bu ta’sir to‘g‘ri aniqlangan, chunki $xS = x'S$ ekanligidan $x' = x \cdot s, s \in S$, bundan esa $h \cdot x' = (h \cdot x) \cdot s$, ya’ni $h * x'S = (h \cdot x)S$ kelib chiqadi.

Ma’lumki, $|\mathcal{L}_S| = \frac{|G|}{|S|} = \frac{p^k \cdot m}{p^k} = m$, ya’ni o‘ng qo‘shni sinflar oilasi elementlari soni p ga bo‘linmaydi. H gruppaning $\mathcal{L}_S$ to‘plamga ta’siri esa ushbu to‘plamni kesishmaydigan orbitalarga ajratib, bu orbitalarning elementlari soni

$$|orb(y)| = \frac{|H|}{|St(y)|}$$

bo‘ladi, bu yerda $y \in \mathcal{L}_S$ va $St(y)$ statsional qism gruppa. Demak,

$$|\mathcal{L}_S| = \sum_y \frac{|H|}{|St(y)|} = \sum_y |orb(y)|,$$

bu yerda yig‘indi har bir orbitadan bittadan tanlangan y element bo‘yicha olinadi.

Ma’lumki, xar bir orbitalardagi elementlar soni p ning qandaydir darajasi ko‘rinishida bo‘lib, bittadan ko‘p elementga ega bo‘lgan orbitalar elementlari soni p ga bo‘linadi.

Tenglikning chap tomonida turgan $|\mathcal{L}_S|$ soni p ga bo‘linmaganligi uchun bitta elementli orbitalar mavjudligi kelib chiqadi. Demak, $xS \in \mathcal{L}_S$ element mavjud bo‘lib, $orb(xS) = \{xS\}$, ya’ni $\forall h \in H$ uchun $(h \cdot x)S = xS$. Bundan esa, $Hx \subset xS$, ya’ni $H \subset xSx^{-1}$ kelib chiqadi. $|xSx^{-1}| = |S| = p^k$ ekanligidan xSx^{-1} xam Silov p-qism gruppasi bo‘lib, u H qism gruppani o‘z ichiga olishi kelib chiqadi.

Agar H qism gruppa Silov p-qism gruppasi bo‘lsa, u holda $|H| = p^k$ ekanligidan $H = xSx^{-1}$ bo‘ladi, ya’ni H gruppa berilgan S Silov p-qism gruppasiga qo‘shma bo‘ladi. Bundan esa, G gruppaning barcha Silov p-qism gruppalari o‘zaro qo‘shma ekanligi kelib chiqadi. $\square$

Agar G gruppaning yagona Silov p-qism gruppasi mavjud bo‘lsa, u holda Silovning ikkinchi teoremasidan uning normal qism gruppa ekanligi kelib chiqadi. Chunki, agar H yagona Silov p-qism gruppasi bo‘lsa, u holda unga qo‘shma bo‘lgan barcha qism gruppalar H bilan ustma-ust tushadi, ya’ni $\forall g \in G$ uchun $gHg^{-1} = H$ bo‘ladi. Bu esa H qism gruppaning normal ekanligini anglatadi.

Endi Silovning uchinchi teoremasini, ya’ni chekli gruppaning Silov p-qism gruppalari soni bilan bog‘liq bo‘lgan teoremani keltiramiz.

4.2.6-teorema (**Silovning uchinchi teoremasi**). *Chekli gruppaning Silov p-qism gruppalari soni gruppa tartibini bo‘lib, p modul bo‘yicha 1 bilan taqqoslanuvchi bo‘ladi.*

Isbot. Aytaylik G gruppa uchun $n = |G| = p^k \cdot m, \ k \geq 1, \ (p, m) = 1$ bo‘lsin. G gruppaning barcha qism gruppalari to‘plamini $S(G) = \{H \mid H \leq G\}$ kabi barcha Silov p-qism gruppalari sonini esa n_p kabi belgilaymiz. Berilgan G gruppadan $S(G) = \{H \mid H \leq G\}$ to‘plamga ta’sirini quyidagicha aniqlaymiz:

$$g * H = g \cdot H \cdot g^{-1}, \ \forall g \in G, \ \forall H \in S(G),$$

ya’ni, ta’sir orqali H qism gruppa o‘ziga qo‘shma bo‘lgan qism gruppaga o‘tadi.

Silovning ikkinchi teoremasiga ko‘ra, ushbu ta’sir orqali barcha Silov p-qism gruppalari bitta orbitada yotishi kelib chiqadi. Demak, qandaydir S Silov p-qism gruppasi uchun $n_p = |orb(S)|$ bo‘ladi. $|G| = |orb(S)| \cdot |St(S)|$ tenglikdan Silov p-qism gruppalari soni n ning bo‘luvchisi ekanligi kelib chiqadi, ya’ni $n_p \mid n$.

Endi $n_p = 1 + p \cdot q$ ekanligini, ya’ni Silov p-qism gruppalari soni p modul bo‘yicha 1 bilan taqqoslanuvchi bo‘lishini ko‘rsatamiz. Buning uchun barcha Silov p-qism gruppalari to‘plamini $\sum_S = \{S_1, S_2, \ldots, S_{|n_p|}\}$ kabi belgilab, S_1 gruppaning $\sum_S$ to‘plamiga ta’sirini $a * S_i = a \cdot S_i \cdot a^{-1}$ kabi aniqlaymiz, bu yerda $a \in S_i$ va $S_i \in$

$\sum_S$ (umuman olganda ixtiyoriy S_{i_0} uchun ta'sir aniqlash mumkin, umumiylikka ziyon yetkazmagan holda $i_0 = 1$ deb olib, S_1 gruppa uchun aniqlangan ta'sirni qaraymiz).

Malumki, $\forall a \in S_1$ uchun $a \cdot S_1 \cdot a^{-1} = S_1$, ya'ni S_1 nuqta qo'zg'almas nuqta bo'ladi. Demak, ushbu ta'sirga nisbatan $|orb(S_1)| = 1$. Endi ushbu S_1 nuqta yagona qo'zg'almas nuqta ekanligini ko'rsatamiz. Teskarisini faraz qilaylik, ya'ni qandaydir $i \neq 1$ uchun S_i nuqta qo'zg'almas nuqta bo'lsin, u holda $a \cdot S_i \cdot a^{-1} = S_i$, $\forall a \in S_1$. Bundan esa, $S_1 \cdot S_i = S_i \cdot S_1$ tenglik kelib chiqadi. U holda 1.4.6-teoremaga ko'ra bu qism gruppalarning ko'paytmasi $H = S_i \cdot S_1$ ham G gruppaning qism gruppasi bo'ladi.

S_1 va S_i Silov p-qism gruppalari H qism gruppada yotganligi uchun, ular H gruppaning Silov p-qism gruppalari. Bundan esa, Silovning ikkinchi teoremasiga ko'ra, ular H gruppada ham o'zaro qo'shma bo'ladi, ya'ni $\exists h \in H$ topilib, $S_1 = h \cdot S_i \cdot h^{-1}$. Bundan esa, $h = a \cdot b,\ a \in S_1,\ b \in S_i$ ekanligini hisobga olib,

$$S_1 = a \cdot b \cdot S_i \cdot (a \cdot b)^{-1} = a \cdot (b \cdot S_i \cdot b^{-1}) \cdot a^{-1} = a \cdot S_i \cdot a^{-1} = S_i$$

tenglikka ega bo'lamiz. Demak $i = 1$.

Shunday qilib, biz $S_1 * \sum_S \to \sum_S$ ta'sir S_1 nuqtadan boshqa qo'zg'almas nuqtaga ega emasligini ko'rsatdik. $\sum_S$ to'plamning elementlari soni orbitalardagi elementlar soni yig'indilariga teng va faqatgina bitta orbita bitta elementli qolgan orbitalar elementlari soni $|orb(S_i)| = \frac{p^k}{|St(S_i)|}$ bo'lib, ular p ga bo'linganligi uchun $n_p = 1 + p \cdot q$ tenglik kelib chiqadi. $\square$

Demak, Silovning uchinchi teoremasidan G gruppaning tartibi $p^k \cdot m$ ga teng bo'lsa, u holda uning Silov p-qism gruppalari soni $n_p = 1 + pq$ bo'lib, $n_p \mid m$ ekanligi kelib chiqadi.

4.2.3-misol. *Agar G nokommutativ gruppa uchun $|G| = p^3$ bo'lsa, u holda $|Z(G)| = p$ ekanligini ko'rsating, bu yerda p – tub son.*

Yechish: $|G| = p^3$ ekanligidan 4.2.3-teoremaga ko'ra $|Z(G)| > 1$ kelib chiqadi. G gruppa nokommutativ bo'lganligi uchun $|Z(G)| \neq p^3$. Demak, $|Z(G)| = p$ yoki $|Z(G)| = p^2$. Agar $|Z(G)| = p^2$ bo'lsa, u holda $|G/Z(G)| = p$ bo'lib, G/Z faktor gruppaning siklik ekanligi, bundan esa, G gruppaning kommutativligi kelib chiqadi. Demak, $|Z(G)| = p$. $\square$

4.2.4-misol. *Tartibi 45 ga teng bo'lgan ixtiyoriy gruppa tartibi 9 ga teng normal qism gruppaga ega ekanligini ko'rsating.*

Yechish: Gruppaning tartibi $45 = 3^2 \cdot 5$ bo'lganligi uuchun, uning Silov 3-qism gruppasi mavjud. U holda Silovning uchinchi teoremasiga ko'ra, Silov 3-qism gruppalarning soni uchun $n_3 = 3k + 1$ va $n_3 \mid 45$ bo'ladi. Bu tenglik esa

$k = 0$, ya'ni $n_3 = 1$ bo'lgandagina bajariladi. Demak, gruppaning yagona Silov 3-qism gruppasi mavjud bo'lib, uning tartibi 9 ga teng. Silov 3-qism gruppasining yagonaligidan esa, uning normal bo'lishi kelib chiqadi. $\square$

4.2.5-misol. *Tartibi* 96 *ga teng bo'lgan gruppaning tartibi* 16 *yoki* 32 *ga teng bo'lgan normal qism gruppasi mavjudligini ko'rsating.*

Yechish: Tartibi $96 = 2^5 \cdot 3$ bo'lgan G gruppaning Silov 2-qism gruppalari soni n_2 bo'lsin. Silovning uchinchi teoremasiga ko'ra $n_2 = 2k + 1$ va $n_2 \mid 96$ bo'ladi. Bundan esa, $n_2 = 1$ yoki $n_2 = 3$ ekanligi kelib chiqadi.

Agar $n_2 = 1$ bo'lsa, u holda gruppaning yagona Silov 2-qism gruppasi mavjud. Uning tartibi 32 ga teng bo'lib, u normal qism gruppa bo'ladi.

Agar $n_2 = 3$, ya'ni G gruppaning 3 ta Silov 2-qism gruppasi mavjud bo'lsa, u holda ushbu Silov 2-qism gruppalarni A, B, va C kabi belgilab, $A \cap B$ kesishmani qaraymiz. $|A| = |B| = |C| = 32$ ekanligidan $A \cap B$ qism gruppaning tartibi ham 32 ning bo'luvchisi ekanligi kelib chiqadi. $A \neq B$ bo'lganligi uchun $|A \cap B| < 32$, xamda $|AB| \leq 96$ ekanligidan va $|A \cap B| = |AB| = \frac{|A||B|}{|AB|} = \frac{32 \cdot 32}{|AB|} = \frac{32 \cdot 32}{|AB|}$ tenglikdan $|A \cap B| > 8$ bo'lishini hosil qilamiz. Demak, $|A \cap B| = 16$. Bundan esa, $[A : A \cap B] = 2$ va $[B : A \cap B] = 2$ kelib chiqib, $A \cap B \lhd A$ va $A \cap B \lhd B$ ekanligi hosil bo'ladi. Bu esa, $A, B \subseteq N(A \cap B)$, ya'ni $AB \subseteq N(A \cap B)$ ekanligini bildiradi. $|N(A \cap B)| \geq |AB| = \frac{|A||B|}{|A \cap B|} = \frac{32 \cdot 32}{16} = 64$ munosabatdan esa, $|N(A \cap B)| = 96$, ya'ni $N(A \cap B) = G$ kelib chiqadi. Bu esa $A \cap B$ qism gruppa G gruppaning tatribi 16 ga teng normal qism gruppasi ekanligini anglatadi. $\square$

4.2.6-misol. *Agar tartibi* 52 *ga teng bo'lgan gruppa tartibi* 4 *ga teng normal qism gruppaga ega bo'lsa, u holda gruppaning kommutativ ekanligini isbotlang.*

Yechish: Aytaylik, G gruppaning H normal qism gruppasi mavjud bo'lib, $|H| = 4$ bo'lsin. U holda H kommutativ bo'ladi. Ikkinchi tomondan esa, $|G| = 13 \cdot 4$ bo'lgani uchun gruppaning Silov 13-qism gruppalari mavjud, hamda ularning soni $13k + 1$ bo'lib, u 52 sonining bo'luvchisi. Bundan esa, G gruppa yagona Silov 13-qism gruppaga ega ekanligi kelib chiqadi. Agar ushbu Silov 13-qism gruppani A orqali belgilasak, $A \lhd G$ bo'lib, $A \cap H = \{e\}$ bo'ladi. Ushbu A va H qism gruppalarning normal ekanligidan va $|AH| = \frac{|A||H|}{|A \cap H|} = 52$ bo'lishidan esa, $G = A \times H$ kelib chiqadi. Har ikkala A va H normal qism gruppalar kommutativ bo'lganligi uchun G ham kommutativ bo'ladi. $\square$

4.2.1 Mustaqil ishlash uchun misol va masalalar

1. Tartibi 14 ga teng bo'lgan gruppaning tartibi 7 ga teng yagona normal qism gruppasi mavjudligini isbotlang.

2. Tartibi 24 ga teng bo‘lgan gruppaning tartibi 7 ga teng bo‘lgan elementlari nechta bo‘lishini aniqlang.

3. Tartibi 36 ga teng bo‘lgan kommutativ gruppaning tartibi 6 ga teng bo‘lgan elementga ega ekanligini ko‘rsating.

4. Tartibi 15 ga teng bo‘lgan gruppaning kommutativ ekanligini isbotlang.

5. $(\mathbb{Z}_{12}, +_{12})$ gruppaning barcha 2-qism gruppalarini toping.

6. $(\mathbb{Z}_{12}, +_{12})$ gruppaning barcha 3-qism gruppalarini toping.

7. A_4 gruppaning barcha 2-qism gruppalarini toping.

8. Tartibi pq ga teng bo‘lgan kommutativ gruppaning siklik ekanligini isbotlang. Bu yerda, p, q-tub sonlar va $p \neq q$.

9. Tartibi p^2 ga teng bo‘lgan gruppaning yoki siklik bo‘lishi yoki siklik gruppalarning to‘g‘ri yig‘indisi shaklida ifodalanishini isbotlang.

10. Agar tartibi 28 ga teng bo‘lgan gruppa tartibi 4 ga teng yagona qism gruppaga ega bo‘lsa, u holda bu gruppaning kommutativ ekanligini isbotlang.

11. S_4 gruppaning barcha Silov 3-qism gruppalarini toping.

12. Gruppa yagona xosmas qism gruppaga ega bo‘lishi uchun uning tartibi p^2 ga teng bo‘lgan siklik gruppa bo‘lishi zarur va yetarli ekanligini isbotlang.

13. Qandaydir G gruppa uchun $|G/Z(G)| = 91$ bo‘lishi mumkinmi?

14. Agar G gruppaning P Silov p-qism gruppasi va H qism grupalari berilgan bo‘lib, $N_G(P) \subseteq H$ bo‘lsa, u holda $N_G(H) = H$ ekanligini isbotlang.

15. Agar G gruppaning P Silov p-qism gruppasi va H qism grupalari berilgan bo‘lib, $P \lhd H$ va $H \lhd G$ bo‘lsa, u holda $P \lhd G$ ekanligini isbotlang.

16. Agar $|G| = 143$ bo‘lsa, uning Silov 11-qism gruppasi yagona ekanligini ko‘rsating.

17. G gruppa va uning H normal qism gruppasi berilgan bo‘lsin. H gruppaning ixtiyoriy P Silov p-qism gruppasi uchun $G = H \cdot N_G(P)$ bo‘lishini isbotlang.

18. Ixtiyoriy chekli kommutativ gruppa o‘zining Silov p-qism gruppalari ichki to‘g‘ri ko‘paytmalari shaklida ifodalanishini isbotlang.

19. Agar $|G| = p^m$ bo‘lib, H to‘plam G gruppaning xosmas qism gruppasi bo‘lsa, u holda $aHa^{-1} = H$ shartni qanoatlantiruvchi $a \in G,\ a \notin H$ element mavjud ekanligini isbotlang.

4.3 Silov teoremalarining ba'zi tadbiqlari

Ushbu mavzuda Silov teoremalarining chekli gruppalarni o'rganish va kichik tartibli gruppalarni tasniflashdagi ba'zi tadbiqlarini ko'rib chiqamiz. Dastlab, chekli tartibli sodda gruppalarning ba'zi xossalarini keltiramiz. Ma'lumki, kommutativ gruppalar sodda bo'lishi uchun ularning tartibi tub songa teng bo'lishi zarur va yetarli. Chunki, tartibi murakkab songa teng bo'lgan, ya'ni biror m soniga bo'lingan kommutativ gruppaning tartibi m ga teng bo'lgan qism gruppasi mavjud bo'lib, u xosmas normal qism gruppa bo'ladi. Demak, chekli tartibli sodda kommutativ gruppalar haqida to'liq ma'lumot mavjud. Nokommutativ sodda gruppalarni o'rganish masalasi esa, bir muncha murakkab hisoblanadi. Biz Silov teoremalarini qo'llagan holda ba'zi gruppalarning sodda emasligini ko'rsatamiz.

4.3.1 Chekli sodda gruppalar

4.3.1-teorema. *Tartibi p^n ga teng bo'lgan ixtiyoriy gruppa sodda emas, bu yerda p – tub son, $n > 1$.*

Isbot. Aytaylik, $|G| = p^n$ bo'lib, $Z(G)$ uning markazi bo'lsin. 4.2.3-teoremaga ko'ra $|Z(G)| > 1$. Agar $G = Z(G)$ bo'lsa, u holda G gruppa kommutativ bo'lib, uning sodda emasligi kelib chiqadi. Agar $Z(G) \neq G$ bo'lsa, u holda aynan $Z(G)$ markaz G gruppaning normal qism gruppasi bo'ladi. Demak, G sodda emas. □

4.3.1-misol. *Tartibi 9 ga teng bo'lgan ixtiyoriy gruppa $\mathbb{Z}_9$ va $\mathbb{Z}_3 \times \mathbb{Z}_3$ gruppalardan biriga izomorf bo'lishini ko'rsating.*

Yechish. Yuqoridagi teoremaga ko'ra tartibi 9 ga teng bo'lgan G gruppaning sodda emasligi kelib chiqadi. Bundan tashqari, $|G| = 9 = 3^2$ ekanligidan 4.2.1-natijaga ko'ra tartibi 9 ga teng bo'lgan gruppaning kommutativ bo'lishini hosil qilamiz. Agar G gruppada tartibi 9 ga teng $a \in G$ element mavjud bo'lsa, u holda $G = \langle a \rangle$ bo'lib, $G \simeq \mathbb{Z}_9$ bo'ladi. Agar gruppada tartibi 9 ga teng bo'lgan element mavjud bo'lmasa, u holda uning birlik elementdan boshqa barcha elementlari tartibi 3 ga teng bo'ladi. Ixtiyoriy $a \in G$, $a \neq e$ element uchun $H = \{e, a, a^2\}$ qism gruppani qarab, ixtiyoriy $b \in G$, $b \notin H$ element uchun $K = \{e, b, b^2\}$ qism gruppani hosil qilamiz. Demak, G gruppaning H va K normal qism gruppalari mavjud bo'lib, $H \cap K = \{e\}$ va $G = HK$. Bu esa $G = H \times K \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ ekanligini anglatadi. Demak, tartibi 9 ga teng bo'lgan ixtiyoriy gruppa $\mathbb{Z}_9$ va $\mathbb{Z}_3 \times \mathbb{Z}_3$ gruppalardan biriga izomorf bo'ladi. □

Endi tartibi pq ga teng bo'lgan gruppalarning sodda emasligini ko'rsatamiz.

4.3.2-teorema. *Tartibi pq ga teng bo'lgan ixtiyoriy gruppa sodda emas, bu yerda p va q – tub sonlar.*

Isbot. Aytaylik G gruppaning tartibi pq ga teng bo'lib, $p > q$ bo'lsin. Gruppaning barcha Silov p-qism gruppalari sonini n orqali belgilasak, Silovning uchinchi teoremasiga ko'ra $n = pk+1$ va $n \mid pq$. Bundan esa, $n = 1$ ekanligini, ya'ni G gruppaning yagona Silov p-qism gruppasi mavjud ekanligini hosil qilamiz. Ushbu Silov p-qism gruppasining taribi p ga teng bo'lib, u normal qism gruppa bo'ladi. Demak, G sodda emas. □

4.3.2-misol. *Tartibi* 15 *ga teng bo'lgan ixtiyoriy gruppa* $\mathbb{Z}_{15}$ *ga izomorf ekanligini ko'rsating.*

Yechish. Silovning birinchi teoremasiga ko'ra tartibi 15 ga teng bo'lgan G gruppaning Silov 5-qism gruppasi va Silov 3-qism gruppalari mavjud. Bundan tashqari, bunday qism gruppalarning yagona ekanligini aniqlash ham qiyin emas. Chunki, Silov 5-qism gruppaning yagonaligi yuqoridagi teorema (4.3.2-teorema) isbotidagi kabi kelib chiqsa, Silov 3-qism gruppalarning soni ham $3k + 1$ bo'lib, 15 ning bo'luvchisi bo'lishi kerak. Bu esa, faqat $k = 0$ da o'rinli.

Ushbu qism gruppalarni A va B orqali belgilasak, ular G gruppaning normal qism gruppalari bo'lib, $A \cap B = \{e\}$ bo'ladi. Bundan esa, $G = A \times B \simeq \mathbb{Z}_5 \times \mathbb{Z}_3$ ekanligi kelib chiqadi. 3 va 5 sonlari o'zaro tubligidan 2.4.2-tasdiqqa ko'ra $\mathbb{Z}_5 \times \mathbb{Z}_3$ gruppaning siklik ekanligini hosil qilamiz. Demak, $G \simeq \mathbb{Z}_{15}$. □

Ta'kidlash joizki, tartibi pq ga teng bo'lgan barcha gruppalar ham siklik bo'lavermaydi. Masalan, tartibi 10 ga teng bo'lgan gruppa uchun yuqoridagi misolning yechimini aynan qo'llab bo'lmaydi. Chunki, $10 = 2 \cdot 5$ ekanligidan, Silov 2-qism gruppalarining soni $2k + 1$ va $(2k + 1) \mid 10$ ekanligidan, $k = 0$ yoki $k = 2$ bo'lishi mumkinligi kelib chiqadi. Bu esa, tartibi 10 ga teng bo'lgan gruppaning 5 ta Silov 2-qism gruppasi mavjud bo'lishi mumkinligini anglatadi. Masalan, $D_5 = \langle a, b\rangle$ diedr gruppasi tartibi 10 ga teng bo'lgan siklik bo'lmagan gruppa bo'lib, uning 5 ta Silov 2-qism gruppasi mavjud.

Quyidagi teoremada tartibi $2p$ ga teng bo'lgan ixtiyoriy gruppaning siklik yoki D_p diedr gruppasiga izomorf bo'lishini ko'rsatamiz.

4.3.3-teorema. *Tartibi* $2p$ *ga teng bo'lgan ixtiyoriy* G *gruppa* $\mathbb{Z}_{2p}$ *yoki* D_p *diedr gruppalaridan biriga izomorf bo'ladi.*

Isbot. Koshi teoremasiga ko'ra tartibi $2p$ ga teng bo'lgan ixtiyoriy gruppaning tartibi p va 2 ga teng bo'lgan elementlari mavjud. Aytaylik, $ord(a) = p$ va $ord(b) = 2$ bo'lsin. Agar $H = \langle a\rangle$ qism gruppani qarasak, $[G : H] = 2$ bo'lganligi uchun H normal qism gruppa bo'ladi. U holda $bab = bab^{-1} \in H$ bo'lib, qandaydir $a^i \in H$ uchun $bab = a^i$ bo'ladi. Bundan esa, $a = ba^ib$ tenglik kelib chiqadi. Ikkinchi tomondan esa $a^{i^2} = (a^i)^i = (bab)^i = (bab^{-1})^i = ba^ib$. Demak, $a = a^{i^2}$ bo'lib, $a^{i^2-1} = e$ kelib chiqadi. $ord(a) = p$ bo'lganligi uchun $p \mid (i^2 - 1)$, ya'ni $p \mid (i - 1)$ yoki $p \mid (i + 1)$. Agar $p \mid (i - 1)$ bo'lsa, u holda $i = 1$ bo'lib, $ba = ab$

tenglikka ega bo'lamiz. Bundan esa $ord(ab) = 2p$ ekanligini, ya'ni G gruppa tartibi $2p$ ga teng bo'lgan elementga egaligini hosil qilamiz. Demak, $G \simeq \mathbb{Z}_{2p}$.

Agar $p \mid (i+1)$ bo'lsa, u holda $i = -1$ bo'lib, $bab = a^{-1}$ ekanligi kelib chiqadi. Bu esa, G gruppa $ord(a) = p$, $ord(b) = 2$ va $ba = a^{-1}b$ shartni qanoatlanturuvchi a, b elementlardan hosil bo'lishini anglatadi. Demak, $G \simeq D_p$. □

Quyidagi teoremada tartibi pq ga teng bo'lgan gruppalarning tasnifini keltiramiz.

4.3.4-teorema. *Tartibi pq (p va q tub sonlar va $p < q$) ga teng bo'lgan ixtiyoriy G gruppa yoki siklik gruppaga yoki $a^p = e$, $b^q = e$ va $a^{-1}ba = b^r$ shartni qanoatlantiruvchi a, b elementlardan hosil bo'livchi gruppaga izomorf , bu yerda q soni $r-1$ ning bo'luvchisi emas, lekin $q \mid (r^p - 1)$. Ikkinchi holat faqat $p \mid (q-1)$ bo'lgandagina o'rinli bo'ladi.*

Isbot. Koshi teoremasiga ko'ra G gruppaning tartibi p va q ga teng bo'lgan a, b elementlari mavjud, ya'ni $ord(a) = p$ va $ord(b) = q$. Ushbu elementlardan hosil qilingan siklik gruppalarni mos ravishda $A = \langle a \rangle$ va $B = \langle b \rangle$ kabi belgilasak, ular G gruppaning Silov qism gruppalari bo'ladi. Silov q-qism gruppalarining soni $1+mq$ bo'lib, $(1+mq) \mid pq$. Bundan esa $(1+mq) \mid p$ kelib chiqib, $p < q$ bo'lganligi uchun $m = 0$ ekanligini hosil qilamiz. Demak, B qism gruppa G gruppaning normal qism gruppasi bo'ladi. Ikkinchi tomondan Silov p-qism gruppalarning soni $1 + kp$ bo'lib, $(1 + kp) \mid pq$, ya'ni $(1 + kp) \mid q$ kelib chiqib, bundan esa $k = 0$ yoki $p \mid (q-1)$ ekanligini hosil qilamiz.

Agar $k = 0$ bo'lsa, u holda A ham G gruppaning normal qism gruppasi bo'lib, $G = A \times B$ ekanligini, ya'ni $G \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$ bo'lishini hosil qilamiz.

Agar $k \neq 0$, ya'ni $p \mid (q-1)$ bo'lsa, u holda A qism gruppa normal emas. Bu esa G gruppaning kommutativ emasligini bildiradi. Lekin B qism gruppa normal bo'lganligi uchun $a^{-1}ba \in B$, ya'ni $a^{-1}ba = b^r$. Bu yerdan $r-1$ soni q ga bo'linmasligini hosil qilamiz, aks holda $ba = ab$ bo'lib, G gruppaning kommutativligi kelib chiqadi. Bundan tashqari, induktiv ravishda $a^{-j}ba^j = b^{r^j}$ tenglikni hosil qilish mumkin. Masalan, $j = 2$ bo'lgan holda ushbu tenglikning to'g'ri ekanligi qiyudagicha ko'rsatiladi

$$a^{-2}ba^2 = a^{-1}(a^{-1}ba)a = a^{-1}b^r a = (a^{-1}ba)(a^{-1}ba)\dots(a^{-1}ba) = b^{r^2}.$$

Demak, $a^{-j}ba^j = b^{r^j}$ tenglik o'rinli. Xususan, $j = p$ bo'lganda $b = b^{r^p}$ tenglikni, ya'ni $q \mid (r^p - 1)$ munosabatni hosil qilamiz. □

4.3.1-natija. *Agar p va q ($p < q$) tub sonlari berilgan bo'lib, $q-1$ soni p ga bo'linmasa, u holda tartibi pq ga teng bo'lgan gruppa siklik bo'ladi.*

Endi yuqoridagi natijalardan foydalanib, tartibi 60 dan kichik bo'lgan nokommutativ sodda gruppa mavjud emasligini ko'rsatamiz. 4.3.1-teoremaga ko'ra tartibi

$$8, \quad 9, \quad 16, \quad 25, \quad 27, \quad 32, \quad 49$$

ga teng bo'lgan gruppalar sodda emas. 4.3.2-teoremadan esa tartibi quyidagi sonlarga teng bo'lgan gruppalarning sodda emasligi kelib chiqadi

$$\begin{array}{llllll} 6 = 3 \cdot 2, & 10 = 5 \cdot 2, & 14 = 7 \cdot 2, & 15 = 5 \cdot 3, & 21 = 7 \cdot 3, & 22 = 11 \cdot 2, \\ 26 = 13 \cdot 2, & 33 = 11 \cdot 3, & 34 = 17 \cdot 2, & 35 = 7 \cdot 5, & 38 = 19 \cdot 2, & 39 = 13 \cdot 3, \\ 46 = 23 \cdot 2, & 51 = 17 \cdot 3, & 55 = 11 \cdot 5, & 57 = 19 \cdot 3, & 58 = 29 \cdot 2. & \end{array}$$

Biz 4.1.8-misolda G gruppa H qism gruppaga ega bo'lib, $|G| = pn$, $|H| = p$, (p – tub son, $n \leq p$) bo'lsa, u holda H normal qism gruppa ekanligini isbotlagan edik. Bunga ko'ra, tartibi $20 = 5 \cdot 4$, $28 = 7 \cdot 4$, $42 = 7 \cdot 6$, $44 = 11 \cdot 4$ va $52 = 13 \cdot 4$ sonlariga teng bo'lgan gruppalarning tartiblari mos ravishda $5, 7, 11$ va 13 ga teng bo'lgan qism gruppalari normal bo'ladi. Demak, tartibi

$$20, \quad 28, \quad 42, \quad 44, \quad 52$$

sonlariga teng bo'lgan gruppalar ham sodda emas.

Bundan tashqari, 4.1.9-misolga ko'ra tartibi $2m$ (m toq son) ga teng gruppalar ham sodda emas. Demak, tartibi $18, 30, 50$ va 54 ga teng bo'lgan gruppalarning ham sodda emasligini hosil qilamiz.

4.1.1-natijaga ko'ra esa G gruppaning indeksi n ga teng bo'lgan H xosmas qism gruppasi mavjud bo'lib, $n!$ soni gruppaning tartibiga bo'linmasa, u holda G gruppa notrivial normal bo'luvchiga ega. Tartibi 12 ga teng bo'lgan gruppaning tartibi 4 ga teng bo'lgan Silov qism gruppasi mavjud bo'lib, uning indeksi 3 ga teng. $3! = 6$ soni 12 ga bo'linmaganligi uchun tartibi 12 ga teng bo'lgan gruppaning ham sodda emasligi kelib chiqadi. Xuddi shu mulohaza bilan tartibi 24, 36, 45 va 48 ga teng bo'lgan gruppalarning ham sodda emasligini hosil qilamiz. Chunki

- $|G| = 24 = 3 \cdot 2^3$ bolsa, $|H| = 8$ bo'lgan Silov qism gruppasi mavjud bo'lib, $[G : H] = 3$ va $3!$ soni 24 ga bo'linmaydi;
- Agar $|G| = 36 = 4 \cdot 3^2$ bolsa, $|H| = 9$ bo'lgan Silov qism gruppasi mavjud bo'lib, $[G : H] = 4$ va $4!$ soni 36 ga bo'linmaydi;
- Agar $|G| = 45 = 5 \cdot 3^2$ bolsa, $|H| = 9$ bo'lgan Silov qism gruppasi mavjud bo'lib, $[G : H] = 5$ va $5!$ soni 45 ga bo'linmaydi;
- Agar $|G| = 48 = 3 \cdot 2^4$ bolsa, $|H| = 16$ bo'lgan Silov qism gruppasi mavjud bo'lib, $[G : H] = 3$ va $3!$ soni 48 ga bo'linmaydi.

Quyidagi misollarda tartibi 40 va 56 ga teng bo'lgan gruppalarning sodda emasligini ko'rsatamiz.

4.3.3-misol. *Tartibi* 40 *ga teng bo'lgan gruppaning sodda emasligini ko'rsating.*

Yechish. Gruppaning tartibi $40 = 5 \cdot 2^3$ bo'lganligi uchun uning Silov 5-qism gruppalari mavjud. Ma'lumki, Silov 5-qism gruppalarining soni $5k+1$ bo'lib, $5k+1 \mid 40$ bo'ladi. Bundan esa $k = 0$, ya'ni Silov 5-qism gruppasining yagona ekanligini hosil qilamiz. Bu esa, Silov 5-qism gruppaning normal ekanligini bildiradi, ya'ni tartibi 40 ga teng bo'lgan gruppa sodda emas. □

4.3.4-misol. *Tartibi* 56 *ga teng bo'lgan gruppaning sodda emasligini ko'rsating.*

Yechish. Gruppaning tartibi $56 = 7 \cdot 2^3$. Ayatylik, n_7 va n_2 mos ravishda gruppaning Silov 7 va 2-qism gruppalari soni bo'lsin. U holda $n_7 = 7m + 1$ va $n_2 = 2k+1$ bo'lib, $n_7 \mid 56$ va $n_2 \mid 56$ bo'ladi. Bundan esa, $n_7 = 1$ yoki 8 ekanligini, $n_2 = 1$ yoki 7 bo'lishini hosil qilamiz. Agar $n_7 = 1$ bo'lsa gruppaning yagona Silov 7-qism gruppasi mavjud bo'lib u normal bo'ladi, va o'z navdatida $n_2 = 1$ bo'lsa gruppaning yagona Silov 2-qism gruppasi normal bo'ladi. Demak, $n_7 = 1$ yoki $n_2 = 1$ bo'lgan hollarda gruppa sodda emas.

Aytaylik, $n_7 = 8$ va $n_2 = 7$ bo'lsin, u holda gruppaning 8 ta $A_1, A_2, \dots, A_8$ Silov 7-qism gruppalari va 7 ta $B_1, B_2, \dots, B_7$ Silov 2-qism gruppalari mavjud. Ushbu Silov 7-qism gruppalari uchun $|A_i| = 7$ va $A_i \cap A_j = \{e\}$ tengliklar o'rinli bo'ladi. Ixtiyoriy $a \in A_i$, $a \neq e$ elementning tartibi 7 ga teng bo'lganligidan G gruppada tartibi 7 ga teng bo'lgan ning 48 ta element mavjudligini hosil qilamiz. Ikkinchi tomindan barcha B_i Silov 2-qism gruppalar 8 ta elementli bo'lib, $|B_1 \cap B_2| \leq 4$ bo'ladi. Bundan esa, $B_1 \cup B_2$ to'plam kamida 12 ta elementdan iborat ekanligi, hamda bu elementlarning barchasining tartibi 7 dan farqli ekanligi kelib chiqadi. Shunday qilib, biz gruppada tartibi 7 ga teng bo'lgan 48 ta, tartibi 7 dan farqli 12 ta element mavjudligini ko'rsatdik. Bu esa, gruppaning elementlari soni 56 ta ekanligiga zid. Demak, $n_7 = 8$ va $n_2 = 7$ bo'lishi mumkin emas. □

Shunday qilib biz yuqoridagi mulohazalar va misollar orqali quyidagi teoremani hosil qilamiz.

4.3.5-teorema. *Tartibi* 60 *dan kichik bo'lgan nokommutativ sodda gruppa mavjud emas.*

Endi tartibi 60 ga teng bo'lgan sodda gruppalarni o'rganamiz. Ma'lumki, tartibi 60 ga teng bo'lgan kommutativ gruppalar sodda emas, chinki 60 soni murakkab son. Biz 1.5.4-Teoremada A_5 gruppaning sodda ekanligini isbotlagan edik. Ushbu gruppaning tartibi 60 ga teng bo'lib, u nokommutativ gruppadir. Demak, tartibi 60 ga teng bo'lgan sodda gruppa mavjud. Tabbiy ravishda, A_5 gruppadan boshqa tartibi 60 ga teng bo'lgan sodda gruppa mavjudmu degan savol tug'iladi. Ushbu savolga javob berish uchun dastlab quyidagi lemmani isbotlaymiz.

4.3.1-lemma. *Tartibi* 60 *ga teng bo'lgan sodda gruppada tartibi* 12 *ga teng bo'lgan qism gruppa mavjud.*

Isbot. Aytaylik, gruppaning Silov 5-qism gruppalari soni n_5, Silov 2-qism gruppalari soni esa n_2 bo'lsin. U holda $n_5 = 5m+1$, $n_5 \mid 60$ va $n_2 = 2k+1$, $n_2 \mid 60$ bo'ladi. Bundan esa, $n_5 = 1$ yoki 6 ekanligini hosil qilamiz. Berilgan gruppa sodda bo'lganligi uchun $n_5 = 6$, ya'ni grupaning 6 ta Silov 5-qism gruppalari mavjud. Ushbu Silov 5-qism gruppalarni $A_1, A_2, \ldots, A_6$ kabi belgilasak, $|A_i| = 5$ bo'lib, $A_i \cap A_j = \{e\}$, $i \neq j$ bo'ladi. Bundan tashqari, $a \in A_i, a \neq e$ element uchun $ord(a) = 5$ ekanligidan gruppada tartibi 5 ga teng bo'lgan 24 ta element mavjud ekanligini hosil qilamiz.

Ikkinchi tomindan esa, $n_2 = 2k+1$, $n_2 \mid 60$ munosabatdan va gruppaning soddaligidan $n_2 = 3, 5, 15$ bo'lishi kelib chiqadi. Faraz qilaylik $n_2 = 15$, ya'ni Silov 2-qism gruppalar soni 15 ta bo'lsin. Ushbu Silov 2-qism gruppalarni $B_1, B_2, \ldots, B_{15}$ kabi belgilasak, $|B_i \cap B_j| \leq 2$ bo'ladi. Agar barcha $i \neq j$ uchun $B_i \cap B_j = \{e\}$ bo'lsa, u holda $\bigcup\limits_i B_i$ to'plam 46 ta elementni o'z ichiga olib, uning barcha elementlari tartibi 5 dan farqli bo'ladi. Biz yuqorida gruppaning tartibi 5 ga teng bo'lgan 24 ta elementi mavjud ekanligini ko'rsatgan edik, bu esa gruppa elementlari son 60 ta ekanligiga zid. Demak, $B_i \cap B_j \neq \{e\}$ bo'ladigan Silov 2-qism gruppalari mavjud. U holda $|B_i \cap B_j| = 2$ bo'lib, $B_i \cap B_j$ to'plam B_i va B_j gruppalarning normal qism gruppasi bo'ladi. Bundan esa, $B_i, B_j \subseteq N(B_i \cap B_j)$, ya'ni $B_iB_j \subseteq N(B_i \cap B_j)$ kelib chiqadi. $N(B_i \cap B_j)$ to'plam G gruppaning qism gruppasi ekanligi $|N(B_i \cap B_j)| \geq |B_iB_j| = 8$ munosabatdan foydalansak, $|N(B_i \cap B_j)| = 12, 20, 30$, yoki 60 bo'lishini hosil qilamiz.

- Agar $|N(B_i \cap B_j)| = 60$ bo'lsa, u holda $B_i \cap B_j$ qism gruppa G da normal bo'ladi, bu esa G ning sodda ekanligiga zid.

- Agar $|N(B_i \cap B_j)| = 30$ bo'lsa, u holda $N(B_i \cap B_j)$ qism gruppa G da normal bo'ladi, bu ham G ning sodda ekanligiga zid.

- Agar $|N(B_i \cap B_j)| = 20$ bo'lsa, u holda $[G : N(B_i \cap B_j)] = 3$ bo'lib, $3!$ soni 60 ga bo'linmaganligi uchun 4.1.1-natijaga ko'ra G gruppaning normal qism gruppasi mavjud.

Demak, $|N(B_i \cap B_j)| = 12$, ya'ni G gruppaning tartibi 12 ga teng bo'lgan qism gruppasi mavjud.

Agar $n_2 = 3$ bo'lsa, u holda ixtiyoriy B_i Silov 2-qism gruppa uchun $n_2 = 3 = [G : N(B_i)]$ bo'lib, $|N(B_i)| = 20$ ekanligini hosil qilamiz. Bu holda ham yuqoridagi kabi, 4.1.1-natijaga ko'ra G gruppaning normal qism gruppasi mavjud ekanligi kelib chiqadi.

Agar $n_2 = 5$ bo'lsa, u holda $n_2 = 5 = [G : N(B_i)]$ bo'lib, $|N(B_i)| = 12$, ya'ni G gruppaning tartibi 12 ga teng bo'lgan qism gruppasi mavjud bo'ladi. $\square$

4.3.6-teorema. *Tartibi* 60 *ga teng bo'lgan ixtiyoriy sodda gruppa* A_5 *gruppaga izomorf bo'ladi.*

Isbot. Aytaylik, G tartibi 60 ga teng bo'lgan sodda gruppa bo'lsin. 4.3.1-lemmaga ko'ra G gruppada tartibi 12 ga teng bo'lgan H qism gruppa mavjud. U holda $[G : H] = 5$ b'olib, 4.1.1-tasdiqqa ko'ra G gruppani S_5 gruppaga o'tkazib, $\mathrm{Ker} f \subseteq H$ shartni qanoatlantiruvchi $f : G \to S_5$ gomomorfizm mavjud ekanligi kelib chiqadi. G gruppa sodda bo'lganligi uchun $\mathrm{Ker} f = \{e\}$ bo'lib, f akslantirish inyektiv bo'ladi. Demak, G gruppa S_5 gruppaning qandaydir T qism gruppasiga izomorf. Endi $T = A_5$ ekanligini ko'rsatamiz, buning uchun T to'plamda toq o'rin almashtirish mavjud emasligini ko'rsatish kifoya. Agar T to'plamda qandaydir toq o'rin almashtirish yotsa, u holda T da yotuvchi barcha juft o'rin almashtirishlar to'plami T ning notrivial normal qism gruppasi bo'ladi. Bu esa ziddiyat, chunki, T gruppa sodda G gruppaga izomorf. Bundan esa, $T = A_5$ ekanligini hosil qilamiz, ya'ni $G \simeq A_5$. $\square$

4.3.2 Kichik tartibli gruppalarning tasnifi

Endi tartibi 15 dan katta bo'lmagan gruppalarning to'liq tasnifini keltiramiz. Aytaylik, G gruppaning tartibi n bo'lsin. Agar $n = 1$ bo'lsa, u holda $G = \{e\}$. Agar $n = 2, 3, 5, 7, 11$ yoki 13 bo'lsa, u holda G siklik bo'lib, u $\mathbb{Z}_n$ ga izomorf bo'ladi. Agar $n = 4$ bo'lsa, u holda G gruppa $\mathbb{Z}_4$ va $\mathbf{K}_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ gruppalardan biriga izomorf bo'lishi ma'lum (2.2.1-teoremaga qarang). Agar $n = 6$ bo'lsa, u holda G gruppa $\mathbb{Z}_6$ va $S_3 \simeq D_3$ gruppalardan biriga izomorf bo'ladi (2.2.2-teoremaga qarang).

Agar $n = 8$ bo'lib, G nokommutativ bo'lsa, u holda G gruppa D_4 va Q_8 gruppalardan biriga izomorf ekanligi 2.2.3-teoremada ko'rsatilgan edi. Tartibi 8 ga teng bo'lgan kommutativ gruppalar esa, $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ va $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ gruppalardan iborat bo'ladi.

Biz 4.3.1-misolda tartibi 9 ga teng bo'lgan gruppa $\mathbb{Z}_9$ va $\mathbb{Z}_3 \times \mathbb{Z}_3$ gruppalardan biriga izomorf bo'lishini ko'rsatgan bo'lsak, 4.3.2-misoldan esa, tartibi 15 ga teng bo'lgan gruppa $\mathbb{Z}_{15}$ ga izomorf ekanligini kelib chiqadi.

Bundan tashqari, 4.3.3-teoremadan tartibi 10 ga teng bo'lgan gruppa $\mathbb{Z}_{10}$ yoki D_5 gruppaga, tartibi 14 ga teng bo'lgan gruppa esa $\mathbb{Z}_{14}$ yoki D_7 gruppalardan biriga izomorf bo'lishi kelib chiqadi.

Shunday qilib, tartibi 15 gacha bo'lgan gruppalarning to'liq tasnifini olish uchun faqatgina tartibi 12 ga teng bo'lgan gruppalarning tasnifini keltirish kifoya.

Tartibi 12 ga teng bo‘lgan 5 ta gruppa mavjud bo‘lib, 2 tasi kommutativ va 3 tasi nokommutativ gruppalardir. Kommutativ gruppalar $\mathbb{Z}_{12}$ va $\mathbb{Z}_6 \times \mathbb{Z}_2$ gruppalardan biriga izomorf bo‘lsa, quyidagi teoremada tartibi 12 ga teng bo‘lgan nokommutativ gruppalarning tasnifini keltiramiz.

4.3.7-teorema. *Tartibi* 12 *ga teng bo‘lgan nokommutativ gruppalar quyidagi o‘zaro izomorf bo‘lmagan gruppalarning biriga izomorf.*

1. A_4 – *to‘rtinchi tartibli juft o‘rin almashtirishlar gruppasi.*
2. D_6 – *oltinchi darajali Diedr gruppasi.*
3. $\widehat{S}_3 = \langle a, b\rangle$ – *ikkita hosil qiluvchiga ega bo‘lib,* $a^6 = e$, $ba = a^{-1}b$ *va* $b^2 = a^3$ *shartni qanoatlantiruvchu gruppa.*

Isbot. Aytyaylik, G tartibi 12 ga teng bo‘lgan nokommutativ gruppa bo‘lsin. U holda uning Silov 2-qism gruppalari va Silov 3-qism gruppalari mavjud bo‘lib, ularning sonini mos ravishda n_2 va n_3 orqali belgilaymiz. Ma‘lumki, $n_2 = 2k + 1$ bo‘lib, $n_2 \mid 12$, hamda o‘z navbatida $n_3 = 3k + 1$ bo‘lib, $n_3 \mid 12$. U holda $n_2 = 1$ yoki 3, o‘z navbatida $n_3 = 1$ yoki 4 ekanligi kelib chiqadi. Agar $n_2 = 1$ va $n_3 = 1$ bo‘lsa, gruppaning Silov qism gruppalari har ikkalasi ham normal bo‘luvchi bo‘ladi. Bundan esa, G gruppa ushbu gruppalarning to‘g‘ri ko‘paytmasi shaklida yozilishi, ya’ni kommutativ ekanligi kelib chiqadi.

Agar $n_2 = 3$ va $n_3 = 4$ bo‘lsa, u holda har biri 3 ta elementdan iborat bo‘lgan turli B_1, B_2, B_3, B_4 Silov 3-qism gruppalari uchun $B_i \cap B_j = \{e\}$ bo‘lib, $\bigcup\limits_i B_i$ to‘plam 9 ta elementdan iborat bo‘ladi. Ikkinchi tomondan esa 4 ta elementdan iborat turli A_1, A_2, A_3 Silov 2-qism gruppalarining birlashmasida kamida 6 ta element mavjud. Bu esa, $|G| = 12$ ekanligiga zid. Demak, $n_2 = 3$ va $n_3 = 4$ bo‘lishi mumkin emas. Shunday qilib, biz $n_2 = 1$, $n_3 = 4$ va $n_2 = 3$, $n_3 = 1$ bo‘lgan hollarni qarashimiz yetarli ekan.

Aytaylik, $n_2 = 1$ va $n_3 = 4$ bo‘lsin, ya’ni G gruppaning bitta Silov 2-qism gruppasi va 3 ta Silov 3-qism gruppalari mavjud. U holda Silov 2-qism gruppa normal qism gruppa bo‘lib, uni K orqali belgilaymiz, H esa biror Silov 3-qism gruppa bo‘lsin, u holda $K = \{e, k_1, k_2, k_3\}$ va $H = \{e, h_1, h_2\}$. Ushbu H gruppaning K normal qism gruppaga $h \star k = hkh^{-1}$, $\forall h \in H$, $\forall k \in K$ kabi aniqlangan $\star : H \times K \to K$ ta‘sirini qaraymiz. Agar ushbu ta‘sirning barcha orbitalari bitta elementli bo‘lsa, u holda $k = hkh^{-1}$, ya’ni $kh = hk$ bo‘lib, G gruppaning kommutativ ekanligi kelib chiqadi. Demak, orbitalar ichida bitta elementdan farqli bo‘lgani mavjud. $|H| = 3$ ekanligi uchun ushbu orbita ham 3 ta elementdan iborat bo‘ladi. Demak, k_1, k_2, k_3 elementlar bitta orbitada yotadi. Bundan esa, ularning tartiblari bir hil ekanligi, ya’ni 2 ga teng bo‘lishi kelib chiqadi. Demak,

$K = \{e, k_1, k_2, k_3\}$ gruppa $\mathbf{K}_4$ – to‘rtinchi tartibli Kleyn gruppasiga izomorf bo‘lar ekan.

Bundan tashqari k_1, k_2, k_3 elementlar bitta orbitada yotganligi uchun qandaydir $h \in H$ element uchun

$$hk_1h^{-1} = k_2, \quad hk_2h^{-1} = k_3, \quad hk_3h^{-1} = k_1$$

bo‘ladi. Bundan esa, G gruppaning barcha elementlari quyidagi ko‘rinishda bo‘lishi kelib chiqadi

$$G = \{e,\ k_1,\ k_2,\ k_3,\ h,\ hk_1,\ hk_2,\ hk_3,\ h^2,\ h^2k_1,\ h^2k_2,\ h^2k_3\}.$$

Shunday qilib biz $n_2 = 1$ va $n_3 = 4$ bo‘lgan holda G gruppada ko‘paytmalar yagona ravishda aniqlanishini hosil qildik. Ushbu gruppaning A_4 ga izomorf ekanligini tekshirish esa qiyin emas.

Endi $n_2 = 3$ va $n_3 = 1$ bo‘lgan holni qaraymiz. Ushbu holda $H = \{e, h_1, h_2\}$ Silov 3-qism gruppasi yagona bo‘lib, u normal bo‘ladi. Shuning uchun endi $K = \{e, k_1, k_2, k_3\}$ Silov 2-qism gruppaning H normal qism gruppaga $k \star h = khk^{-1}$ ta’sirini qaraymiz. Yuqoridagi kabi, ushbu ta’sirda elementlari soni bittadan ko‘p orbita mavjud bo‘ladi, aks holda G kommutativ bo‘lib qoladi. Bundan esa, ikkita elementdan iborat orbita mavjud bo‘lib, u $\{h_1, h_2\}$ to‘plamdan iborat ekanligi kelib chiqadi. $|St(h_1)| = \frac{|K|}{|orb(h_1)|} = 2$ ekanligidan K to‘plamda birlik elementdan boshqa $k_{i_0}h_1 = h_1k_{i_0}$ shartni qanoatlantiruvchi k_{i_0} element mavjud ekanligi kelib chiqadi. Bundan esa ushbu k_{i_0} element H ning barcha elementlari bilan o‘rin almashinuvchi ekanligi kelib chiqib, uning tartibi 2 ga teng ekanligini hosil qilamiz. Aks holda, agar tartibi 4 ga teng bo‘lsa, u holda G kommutativ bo‘lib qoladi. Demak, $A = H \cup k_0H$ to‘plam 6 ta elementdan iborat bo‘lib, u kommutativ qism gruppa bo‘ladi, ya’ni $A \simeq \mathbb{Z}_6$.

Endi A qism gruppaning $a \in A$ hosil qiluvchi elementi va $k \in K \setminus \{e, k_{i_0}\}$ element olib, kak^{-1} elementni qaraymiz. Ushbu element uchun $kak^{-1} \in A$ bo‘lib, u a dan farqli bo‘ladi, aks holda G kommutativ bo‘lib qoladi. Bundan tashqari, $ord(kak^{-1}) = ard(a) = 6$ ekanligidan, $kak^{-1} = a^{-1}$ bo‘lishi kelib chiqadi. Demak, $G = A \cup kA$ bo‘lib, a va b elementlar gruppaning hosil qiluvchi elementlari bo‘ladi, bu yerda $ord(a) = 6$ bo‘lib, $ord(k)$ esa 2 yoki 4. Agar $ord(k) = 2$ bo‘lsa, u holda $G \simeq D_6$ bo‘ladi. Agar $ord(k) = 4$ bo‘lsa, u holda $K \simeq \mathbb{Z}_4$ bo‘lib, biz $\widehat{S}_3$ gruppani hosil qilamiz. $\square$

Ta’kidlash joizki, biz yuqoridagi teoremada ikkita a, b hosil qiluvchiga ega bo‘lib, $a^6 = e$, $ba = a^{-1}b$ va $b^2 = a^3$ shartni qanoatlantiruvchi $\widehat{S}_3 = \langle a, b\rangle$ gruppa haqida aytib ketdik. Bu shartlarni qanoatlantiruvchi gruppaning yagona ekanligini ko‘rsatish qiyin emas, quyidagi misolda esa, bunday gruppaning mavjudligini ko‘rsatamiz.

4.3.5-misol. *$GL_2(\mathbb{C})$ gruppaning quyidagi ikkita elementini olamiz:*

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} i & 0 \\ i & -i \end{pmatrix}$$

Tekshirish qiyin emaski, $ord(A) = 6$, $ord(B) = 4$ va $A^3 = B^2$ va $H = \langle A, B\rangle$ gruppa 12 ta elementdan iborat bo'ladi, ya'ni $\widehat{S}_3$ gruppaga izomorf bo'ladi. Ushbu $\widehat{S}_3$ gruppaning markazi $Z(\widehat{S}_3) = \{e, a^3\}$ bo'lib, $\widehat{S}_3/Z(\widehat{S}_3)$ faktor gruppa S_3 ga izomorf bo'ladi. Shuning uchun odatda ushbu gruppa S_3 gruppaning markaziy kengaytmasi deb ataladi.

Shunday qilib, ushbu mavzuda biz kichik tartibli gruppalarning qiyudagi ko'rinishdagi tasnifini hosil qildik.

Gruppaning tartibi	Gruppalar soni	Kommutativ gruppalar	Nokommutativ gruppalar
1	1	$\{e\}$	–
2	1	$\mathbb{Z}_2$	–
3	1	$\mathbb{Z}_3$	–
4	2	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$	–
5	1	$\mathbb{Z}_5$	–
6	2	$\mathbb{Z}_6$	S_3
7	1	$\mathbb{Z}_7$	–
8	5	$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$	$D_4,\ Q_8$
9	2	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$	–
10	2	$\mathbb{Z}_{10}$	D_5
11	1	$\mathbb{Z}_{11}$	–
12	5	$\mathbb{Z}_{12},\ \mathbb{Z}_6 \times \mathbb{Z}_2$	$A_4,\ D_6,\ \widehat{S}_3$
13	1	$\mathbb{Z}_{13}$	–
14	2	$\mathbb{Z}_{14}$	D_7
15	1	$\mathbb{Z}_{15}$	–

4.3.6-misol. *Agar G gruppaning tartibi 231 ga teng bo'lsa, u holda:*

1) *Gruppaning Silov 11-qism gruppasi normal ekanligini isbotlang.*

2) *Gruppaning Silov 7-qism gruppasi normal ekanligini isbotlang.*

3) *Gruppaning tartibi 77 ga teng bo'lgan siklik qism qism gruppasi mavjud ekanligi isbotlang.*

4) *Gruppaning H, G va L qism gruppalari mos ravishda uning Silov 11, 7 va 3-qism gruppalari bo'lsa, $G = HKL$ ekanligini isbotlang.*

5) $H \subseteq Z(G)$ ekanligini ko'rsating.

Yechish: 1) $231 = 11 \cdot 7 \cdot 3$ ekanligidan, uning Silov 11, 7 va 3-qism gruppalari mavjud ekanligi kelib chiqadi. Silov 11-qism gruppalari soni $n_{11} = 1 + 11k$ bo'lib, $(1+11k)|3 \cdot 7$ ekanligidan $n_{11} = 1$ kelib chiqadi. Demak, gruppaning yagona Silov 11-qism gruppasi mavjud bo'lib, u normal bo'ladi.

2) Silov 7-qism gruppalari soni esa $n_7 = 1 + 7k$ bo'lib, $(1+11k)|3 \cdot 11$. Bundan $n_7 = 1$ kelib chiqadi, ya'ni Silov 7-qism gruppasi ham normal bo'ladi.

3) Gruppaning H Silov 11-qism gruppasa va K Silov 7-qism gruppalari normal bo'lganligi uchun HK ham normal qism gruppa bo'lib, $H \cap K = \{e\}$ bo'ladi, demak $HK = 77$. Bundan tashqari H va K lar siklik gruppalar bo'lib, $(7, 11) = 1$ ekanligidan HK ning siklik qism gruppa ekanligi kelib chiqadi.

4) Gruppaning L Silov 3-qism gruppasi uchun $L \cap (HK) = \{e\}$ bo'ladi, chunki HK qism gruppada tartibi 3 ga teng element mavjud emas. Bundan tashqari,

$$|HKL| = \frac{|HK| \cdot |L|}{|L \cap (HK)|} = \frac{77 \cdot 3}{1} = 231 = |G|$$

ekanligidan $G = HKL$ kelib chiqadi.

5) HK siklik gruppa ekanligi uchun ixtiyoriy $h \in H$ va $k \in K$ uchun $hk = kh$ tenglik o'rinli bo'ladi. Endi G/K faktor gruppani qarasak, $|G/K| = 33$ ekanligidan, uning Silov 11 va 3-qism gruppalarining yagona ekanligini hosil qilamiz. Demak, G/K faktor gruppa siklik bo'ladi. Birlik elementdan farqli $a \in L$ va $h \in H$ elementlarni olsak, $a, h \notin K$ bo'lib, G/K faktor gruppaning kommutativligidan $(aK)(hK) = (hK)(aK)$, ya'ni $(ah)K = (ha)K$ tenglikka ega bo'lamiz. Bundan esa, $(ah)^{-1}(ha) \in K$ kelib chiqadi. H normal qism gruppa bo'lganligi uchun $a^{-1}ha \in H$ munosabatni, o'z navbatida $(ah)^{-1}(ha) \in H$ ekanligini hosil qilamiz. Demak, $(ah)^{-1}(ha) \in H \cap K = \{e\}$, ya'ni $h^{-1}a^{-1}ha = e$, bundan esa $ha = ah$ kelib chiqadi. Shunday qilib, biz $\forall h \in H$, $\forall k \in K$, $\forall a \in L$ elementlar uchun $hk = kh$ va $ha = ah$, ekanligini hosil qildik. Bundan esa $H \subseteq Z(G)$ munosabat osongina kelib chiqadi. □

4.3.7-misol. *Tartibi 255 ga teng bo'lgan gruppaning siklik ekanligini isbotlang.*

Yechish: $255 = 3 \cdot 5 \cdot 17$ bo'lganligi uchun, uning Silov 17, 5 va 3-qism gruppalari mavjud. Ularning sonini mos ravishda n_{17}, n_5 va n_3 kabi belgilasak, $n_{17} = 1 + 17m$ va $n_{17} \mid 15$ ekanligidan $n_{17} = 1$ bo'lishi kelib chiqadi. Demak, gruppaning Silov 17-qism gruppasi normal bo'ladi. Gruppaning Silov 5-qism gruppalari soni uchun $n_5 = 1 + 5k$ va $n_5 \mid 51$ bo'lib, bundan $n_5 = 1$ yoki $n_5 = 51$ ekanligi kelib chiqadi. O'z navbatida $n_3 = 1 + 3l$ va $n_3 \mid 85$ ekanligidan $n_3 = 1$ yoki $n_3 = 85$ hosil bo'ladi.

Agar $n_5 = 51$ va $n_3 = 85$ bo'lsa u holda 51 ta Silov 5-qism gruppalarning birlashmasida tartibi 5 ga teng bo'lgan jami 204 ta element yotadi. Xuddi shunday, 85 ta Silov 3-qism gruppalarning birlashmasida esa tartibi 3 ga teng bo‘lgan 170 ta element mavjudligi kelib chiqadi. Bu esa gruppaning elementlari 255 ta ekanligiga zid. Demak, $n_5 = 1$ yoki $n_3 = 1$ tengliklardan hech bo‘lmaganda bittasi o‘rinli bo‘lishi shart.

Aytaylik, $n_5 = 1$ bo‘lsin, u holda K Silov 5-qism gruppasi ham normal bo‘lib, $H \cap K = \{e\}$ bo‘ladi. Bundan esa, $\forall h \in H$ va $\forall k \in K$ uchun $hk = kh$ ekanligi kelib chiqadi. Avvalgi misolning 5) bandiga (4.3.6-misol) o‘xshab G/K faktor gruppani qaragan holda $H \subseteq Z(G)$ ekanligini hosil qilish mumkin. Bundan esa, $|Z(G)| = 17, 51, 85$ yoki 255 ekanligi, o‘z navbatida $|G/Z(G)| = 15, 5, 3$ yoki 1 bo‘lishi kelib chiqadi. Tartibi $15, 5, 3$ va 1 bo‘lgan gruppalar siklik bo‘lganligi uchun $G/Z(G)$ faktor gruppa siklik, ya’ni G kommutativ bo‘ladi. Bu esa, gruppaning Silov 3-qism gruppasi ham yagona ekanligini anglatadi, ya’ni $n_3 = 1$. Demak, tartibi 255 ga teng bo‘lgan gruppa tartiblari 17, 5 va 3 bo‘lgan siklik qism gruppalarning to‘g‘ri ko‘paytmasidan iborat bo‘ladi. 17, 5 va 3 sonlarining o‘zaro tub ekanligidan esa, gruppaning siklik ekanligi kelib chiqadi.

Agar $n_3 = 1$ deb faraz qilinsa ham, xuddi yuqoridagi mulohazalar kabi $n_5 = 1$ ekanligini hosil qilish mumkin. $\square$

4.3.8-misol. *Tartibi 455 ga teng bo‘lgan gruppaning siklik ekanligini isbotlang.*

Yechish: $|G| = 455 = 5 \cdot 7 \cdot 13$ bo‘lganligi uchun gruppaning Silov 13-qism gruppasi mavjud, va ularning soni $n_{13} = 1 + 13k$, $n_{13} \mid 35$. Bundan esa, $n_{13} = 1$ ekanligi kelib chiadi. Demak, G gruppaning H Silov 13-qism gruppasi normal bo‘ladi. Bundan esa, $N(H) = G$ kelib chiqadi. Endi $Aut(H)$ ni qarasak, H ning tartibi 13 ga teng bo‘lganligidan $|Aut(H)| = 12$ ekanligini hosil qilamiz. Bundan tashqari, $N(H)/C(H)$ faktor gruppadan $Aut(H)$ gruppaga monomorfizm mavjud. Demak, $|N(H)/C(H)|$ soni 12 ning bo‘luvchisi bo‘ladi. Ikkinhi tomondan esa $|N(H)/C(H)|$ soni 455 ning bo‘luvchisi. $(455, 12) = 1$ ekanligidan $|N(H)/C(H)| = 1$ kelib chiqadi, demak, $C(H) = N(H) = G$. Bundan esa, $H \subseteq Z(G)$ ekanligiga ega bo‘lamiz. $|Z(G)|$ soni 455 ning bo‘luvchisi bo‘lganligi uchun $|Z(G)| = 13, 65, 91,$ yoki 455 ekanligi, bundan esa, $|G/Z(G)| = 35, 7, 5,$ yoki 1 bo‘lishi kelib chiqadi. Ushbu hollarning barchasida $G/Z(G)$ gruppaning sisklik ekanligini, ya’ni kommutativligini hosil qilamiz. Bu esa, G gruppaning yagona K Silov 5-qism gruppaga va yagona L Silov 7-qism gruppaga ega ekanligini anglatadi. Bundan $G = H \times K \times L$ ekanligi, ya’ni uning siklik bo‘lishi kelib chiqadi. $\square$

4.3.3 Mustaqil ishlash uchun misol va masalalar

1. Tartibi 125 ga teng bo‘lgan ixtiyoriy gruppaning sodda emasligini ko‘rsating.

2. Tartibi 65 ga teng bo‘lgan ixtiyoriy gruppaning sodda emasligini ko‘rsating.

3. Tartibi 130 ga teng bo‘lgan ixtiyoriy gruppaning sodda emasligini ko‘rsating.
4. Tartibi 75 ga teng bo‘lgan ixtiyoriy gruppaning sodda emasligini ko‘rsating.
5. Tartibi 96 ga teng bo‘lgan ixtiyoriy gruppaning sodda emasligini ko‘rsating.
6. Tartibi 150 ga teng bo‘lgan ixtiyoriy gruppaning sodda emasligini ko‘rsating.
7. Tartibi 200 ga teng bo‘lgan ixtiyoriy gruppaning sodda emasligini ko‘rsating.
8. Tartibi 133 ga teng bo‘lgan gruppaning siklik ekanligini ko‘rsating.
9. Tartibi 665 ga teng bo‘lgan gruppaning siklik ekanligini ko‘rsating.
10. Yagona Silov 2-qism gruppaga ega bo‘lib, tartibi 100 bo‘lgan gruppaning kommutativ ekanligini isbotlang.
11. Tartibi 70 ga teng bo‘lgan gruppaning tartibi 35 ga teng bo‘lgan siklik qism gruppasi mavjud ekanligini isbotlang.
12. Tartibi 385 ga teng bo‘lgan gruppaning Silov 7-qism gruppasi gruppa markaziga qism ekanligini isbotlang.
13. Tartibi 1045 ga teng bo‘lgan gruppaning Silov 11-qism gruppasining normal bo‘lishini va Silov 19-qism gruppasi gruppa markaziga qism ekanligini isbotlang.
14. Tartibi 627 ga teng bo‘lgan gruppaning Silov 19-qism gruppasining normal bo‘lishini va Silov 11-qism gruppasi gruppa markaziga qism ekanligini isbotlang.
15. Tartibi 168 ga teng bo‘lgan sodda gruppaning sakkizta Silov 7-qism gruppasi mavjudligini va tartibi 14 ga teng qism gruppasi mavjud emasligini ko‘rsating.
16. Izomorfizm aniqligida tartibi 70 ga teng bo‘lgan barcha gruppalarni toping.
17. D_n diedr gruppasining markazini toping.
18. D_{2n} va D_{2n+1} gruppalarning qo‘shma sinflarini toping.
19. Agar G gruppaning tartibi p^2q^2 ga teng bo‘lsa, (p, q – tub sonlar va $p > q$) u holda uning Silov p-qism gruppalari sonini aniqlang.
20. Tartibi p^2q^2 ga teng bo‘lgan ixtiyoriy gruppaning sodda emasligini ko‘rsating.

4.4 Yechiluvchan va nilpotent gruppalar

Biz avvalgi mavzularda kommutativ va chekli gruppalar bilan yaqindan tanishib, ularning xossalari va tasniflarini keltirdik. Lekin hayotda kommutativ bo‘lmagan gruppalar ham, cheksiz gruppalar ham juda ko‘p uchraydi. Bunday gruppalarni sanoqli sondagi kamayuvchi normal qatorlar yordamida, chekli gruppalar bilan bog‘lash orqali o‘rganish mumkin. Kommutativ gruppalarning muhim umumlashmalari bu yechiluvchan va nilpotent gruppalar hisoblanadi. Yechiluvchan gruppalarni kommutativ gruppaning bir necha marta kengaytmasini olish orqali hosil qilingan gruppa deb aytish mumkin. Nilpotent gruppalar sinfi esa, kommutativ gruppalar bilan yechiluvchan gruppalarning orasida yotuvchi sinf hisoblanadi. Yechiluvchan gruppalarning asosiy jihati shundan iboratki, ular algebraik tenglamalarni radikallarda yechish masalasi bilan uzviy bog‘liq. Bizga ma’lumki, darajasi 5 gacha bo‘lgan algebraik tenglamalarnigina radikallarda yechish mumkin bo‘lib, undan yuqori darajali algebraik tenglamalarni esa radikallarda yechish mumkin emas. Ushbu masala S_n o‘rin almashtirishlar gruppasining yechiluvchan bo‘lishi bilan ekvivalent bo‘lib, $n < 5$ bo‘lganda S_n gruppa yechiluvchan, $n \geq 5$ bo‘lganda esa yechiluvcham bo‘lmaydi.

4.4.1 Yechiluvchan gruppalar

Biz dastlab, yechiluvchan va nilpotent gruppalarni ta’rifini keltirish uchun zaruriy bo‘lgan tushunchalarni kiritib olamiz. Bizga G gruppa va uning quyidagi shartni qanoatlantiruvchi H_i qism gruppalari berilgan bo‘lsin

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n = \{e\}. \tag{4.3}$$

Agar ushbu H_i qism gruppalar turli xil bo‘lsa, ya’ni $H_i \neq H_{i+1}$, $0 \leq i \leq n$ bo‘lsa, u holda n soni ushbu qatorning **uzunligi** deyiladi. Ya’ni qatorning uzunligi, turli xosmas qism gruppalarning sonidir.

4.4.1-ta’rif.

- *Agar* (4.3) *qatorda H_i qism gruppa H_{i+1} ning normal qism gruppasi bo‘lsa, u holda ushbu qatorga* ***subnormal*** *qator deyiladi.*

- *Agar* (4.3) *qatorda H_i qism gruppa G gruppaning normal qism gruppasi bo‘lsa, u holda ushbu qatorga* ***normal*** *qator deyiladi.*

Ta’kidlash joizki, ixtiyoriy normal qator subnormal qator bo’ladi. Chunki, H_i gruppa G da normal bo‘lishidan H_{i+1} da ham normal bo‘lishi kelib chiqadi. Ushbu H_i/H_{i+1} faktor gruppalarga **faktorlar** deb ataladi. Agar $H_i = H_{i+1}$ bo’lsa, u holda H_i/H_{i+1} faktorga trivial faktor deb ataladi. Demak, subnormal(normal) qatorning uzunligi, bu trivial bo‘lmagan faktorlarning soniga teng bo‘ladi.

Agar G gruppada $H_0 = G$ va $H_1 = \{e\}$ deb olsak, u holda ixtiyoriy gruppaning normal qatorga ega ekanligi hosil qilamiz, ya’ni

$$G = H_0 \supseteq H_1 = \{e\}.$$

Ushbu normal qatorni trivial normal qator deb ataladi.

Quyidagi misolda subnormal bo‘lib, normal bo‘lmaydigan qatorga misol keltiramiz

4.4.1-misol. *S_4 o‘rin almashtirishlar gruppasida*

$$H_1 = \{e, (1\ 2) \circ (3\ 4), (1\ 3) \circ (2\ 4), (1\ 4) \circ (2\ 3)\}$$

va

$$H_2 = \{e, (1\ 2) \circ (3\ 4)\}$$

deb olsak, $S_4 = H_0 \supset H_1 \supset H_2 \supset H_3 = \{e\}$ qator subnormal qator bo‘lib, normal qator bo’lmaydi. Chunki, H_2 qism gruppa H_1 qism gruppada normal, lekin S_4 gruppaning normal qism gruppasi emas.

Kommutativ gruppalar uchun ixtiyoriy subnormal qator, normal qator bo’ladi, chunki kommutativ gruppalarning ixtiyoriy qism gruppasi normal qism gruppa bo‘ladi. Masalan, $(\mathbb{Z}_{12}, +_{12})$ gruppaning quyidagi normal qatorlari mavjud

$$\begin{aligned}
&\mathbb{Z}_{12} \supset \langle\overline{6}\rangle \supset \{\overline{0}\},\\
&\mathbb{Z}_{12} \supset \langle\overline{3}\rangle \supset \langle\overline{6}\rangle \supset \{\overline{0}\},\\
&\mathbb{Z}_{12} \supset \langle\overline{2}\rangle \supset \langle\overline{4}\rangle \supset \{\overline{0}\},\\
&\mathbb{Z}_{12} \supset \langle\overline{2}\rangle \supset \langle\overline{6}\rangle \supset \{\overline{0}\}.
\end{aligned}$$

Endi subnormal qatorlarning ekvivalentligi tushunchasini kiritamiz.

4.4.2-ta’rif. *Bizga G gruppaning ikkita subnormal qatorlar berilgan bo‘lsin*

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}, \tag{4.4}$$

$$G = K_0 \supseteq K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{m-1} \supseteq K_m = \{e\}. \tag{4.5}$$

Agar ushbu subnormal qatorlarning faktorlari o‘rtasida o‘zaro bir bir qiymatli moslik o‘rnatish mumkin bo’lib, mos faktorlar o‘zaro izomorf bo‘lsa, u holda ushbu qatorlar ekvivalent deyiladi.

Ta’rifdan ko‘rinadiki, ekvivalent subnormal qotorlarning uzunliklari teng bo‘ladi. Quyidagi misolda butun sonlar gruppasininng ikkita ekvivalent subnormal qatorlariga misol keltiramiz.

4.4.2-misol. *$\mathbb{Z}$ gruppaning quyidagi subnormal qatorlarini qaraymiz*

$$\mathbb{Z} \supset 4\mathbb{Z} \supset 12\mathbb{Z} \supset 24\mathbb{Z} \supset 120\mathbb{Z} \supset \{0\} \tag{4.6}$$

$$\mathbb{Z} \supset 2\mathbb{Z} \supset 8\mathbb{Z} \supset 24\mathbb{Z} \supset 120\mathbb{Z} \supset \{0\}. \tag{4.7}$$

Birinchi qatorning faktorlari

$$\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}_4, \quad 4\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}_3, \quad 12\mathbb{Z}/24\mathbb{Z} \simeq \mathbb{Z}_2, \ 24\mathbb{Z}/120\mathbb{Z} \simeq \mathbb{Z}_5, \ 120\mathbb{Z}/\{0\} \simeq \mathbb{Z}$$

bo'lsa, ikkinchi qatorning faktorlari esa,

$$\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}_2, \quad 2\mathbb{Z}/8\mathbb{Z} \simeq \mathbb{Z}_4, \quad 8\mathbb{Z}/24\mathbb{Z} \simeq \mathbb{Z}_3, \ 24\mathbb{Z}/120\mathbb{Z} \simeq \mathbb{Z}_5, \ 120\mathbb{Z}/\{0\} \simeq \mathbb{Z}.$$

bo'ladi.

Ko'rinib turibdiki, ushbu fatroklar orasida o'zaro bir qiymatli moslik mavjud bo'lib, ular izomorf bo'ladi. Demak, ushbu ukkita subnormal qator ekvivalent bo'lar ekan.

Endi yechiluvchan algebralar ta'rifini kiritamiz.

4.4.3-ta'rif. *Agar G gruppada*

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}$$

subnormal qator mavjud bo'lib, H_i/H_{i+1} faktor gruppalar kommutativ bo'lsa, u holda G gruppaga ***yechiluvchan*** *gruppa deb ataladi. Berilgan qatorga esa G gruppaning* ***yechiluvchan qatori*** *deyiladi.*

Ma'lumki, ixtiyoriy kommutativ gruppa yechiluvchandir, chunki kommutativ gruppaning trivial normal qatori ham yechiluvchan qator bo'ladi. Shuning uchun S_1 va S_2 gruppalar yechiluvchan gruppalar bo'ladi. Quyidagi misollarda S_3 va S_4 gruppalarning yechiluvchan ekanligini ko'rsatamiz.

4.4.3-misol. *S_3 o'rin almashtirishlar gruppasida $H_1 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ qism gruppani qarasak,*

$$S_3 \supset H_1 \supset \{e\}$$

qator yechiluvchan qator bo'ladi. Demak, S_3 yechiluvchan gruppa.

4.4.4-misol. *S_4 o'rin almashtirishlar gruppasida $H_1 = A_4$ va $H_2 = \{e, (1\ 2) \circ (3\ 4), (1\ 3) \circ (2\ 4), (1\ 4) \circ (2\ 3)\}$ qism gruppalarni qarasak,*

$$S_4 \supset H_1 \supset H_2 \supset \{e\}$$

qator yechiluvchan qator bo'ladi. Demak, S_4 yechiluvchan gruppa.

Demak, S_n o'rin almashtirishlar gruppasi $n \leq 4$ bo'lganda yechiluvchan gruppa bo'lar ekan. Biz keyinroq S_n, $n \geq 5$ gruppalarning yechiluvchan gruppalar bo'lmasligini isbotlaymiz. Quyidagi teoremada esa ixtiyoriy yechiluvchan gruppaning qism gruppasi ham gomomorf obrazi ham yana yechiluvchan bo'lishini ko'rsatamiz.

4.4.1-teorema. *Agar G gruppa yechiluvchan bo'lsa, u holda uning ixtiyoriy qism gruppasi ham gomomorf obrazi ham yana yechiluvchan bo'ladi.*

Isbot. Aytaylik, bizga

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}$$

yechiluvchan qator berilgan bo'lib, K esa G gruppaning qism gruppasi bo'lsin. Qiyidagi $K_i = K \cap H_i$ qism gruppalar uchun

$$K = K_0 \supseteq K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{n-1} \supseteq K_n = \{e\}$$

qatorni yechiluvchan qator bo'lishini ko'rsatamiz. $H_{i+1} \lhd H_i$ bo'lganligi uchun $K_{i+1} \lhd K_i$ ekanligi osongina kelib chiqadi. Bundan tashqari $K_{i+1} = K_i \cap H_{i+1}$ va $K_i/K_{i+1} = K_i/(K_i \cap H_{i+1})$ ekanligidan izomorfizm haqidagi ikkinchi teoremaga ko'ra

$$K_i/K_{i+1} \simeq (K_iH_{i+1})/H_{i+1}$$

bo'lishi kelib chiqadi. H_i/H_{i+1} faktor gruppaning kommutativligi va $(K_iH_{i+1})/H_{i+1} \leq H_i/H_{i+1}$ ekanligidan K_i/K_{i+1} gruppaning ham kommutativligi kelib chiqadi. Bundan esa, K qism gruppaning yechiluvchan ekanligi kelib chiqadi.

Endi G gruppaning gomomorf obrazi yechiluvchan bo'lishini ko'rsatamiz. Aytaylik, $f : G \to G'$ epimorfizm berilgan bo'lsin. $H_i' = f(H_i)$ to'plamlarni qarasak, f epimorfizm bo'lganligi uchun $f(H_{i+1}) \lhd f(H_i)$ bo'ladi. Demak,

$$G' = H_0' \supseteq H_1' \supseteq H_2' \supseteq \cdots \supseteq H_{n-1}' \supseteq H_n' = \{e\} \tag{4.8}$$

qator subnormal qator bo'ladi. Biz endi H_i'/H_{i+1}' faktorlarning kommutativ ekanligini ko'rsatamiz. Buning uchun $g(h_i) = f(h_i)H_{i+1}'$ kabi aniqlangan $g : H_i \to H_i'/H_{i+1}'$ akslantirishni qaraymiz. Ushbu g akslantirish epimorfizm bo'lib, ixtiyoriy $h_{i+1} \in H_{i+1}$ uchun

$$g(h_{i+1}) = f(h_{i+1})H_{i+1}' = f(h_{i+1})f(H_{i+1}) = f(H_{i+1}) = H_{i+1}'$$

bo'ladi. Bundan esa $H_{i+1} \subseteq \mathrm{Ker} g$ ekanligi kelib chiqadi. Demak, g epimorfizm orqali H_i/H_{i+1} gruppadan H_i'/H_{i+1}' gruppaga epimorfizm aniqlash mumkin. Bundan esa, H_i'/H_{i+1}' fakrorlarning kommutativ ekanligi, ya'ni G' gruppaning yechiluvchanligi kelib chiqadi. □

4.4.1-teoremadan quyidagi natijani hosil qilamiz.

4.4.1-natija. *Agar G yechiluchan gruppa bo'lib, H uning normal qism gruppasi bo'lsa, u holda H va G/H gruppalar ham yechiluvchan bo'ladi.*

Quyidagi teoremada esa, yuqoridagi natijaning teskarisi ham o'rinli ekanligini ko'rsatamiz.

4.4.2-teorema. *Agar G gruppaning H normal qism gruppasi berilgan bo'lib, H va G/H gruppalar yechiluvchan bo'lsa, u holda G gruppa ham yechiluvchan bo'ladi.*

Isbot. Aytaylik, G/H yechiluvchan gruppa uchun

$$G/H = \overline{K}_0 \supseteq \overline{K}_1 \supseteq \overline{K}_2 \supseteq \cdots \supseteq \overline{K}_{m-1} \supseteq \overline{K}_m = \{eH\} = \{H\}$$

yechiluvchan qator berilgan bo'lsin. U holda, G gruppaning $\overline{K}_i = K_i/H$ va $K_{i+1} \lhd K_i$ shartlarni qanoatlantiruvchi K_i, $0 \leq i \leq m$ qism gruppalari mavjud. Izomorfizm haqidagi uchinchi teoremaga ko'ra $K_i/K_{i+1} \simeq \overline{K}_i/\overline{K}_{i+1}$ bo'lib, K_i/K_{i+1} gruppalarning ham kommutativ ekanligi kelib chiqadi.

Ikkinchi tomondan esa, H yechiluvchan bo'lganligi uchun

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}$$

yechiluvchan qator mavjud. U holda

$$G = K_0 \supseteq K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{m-1} \supseteq H \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}$$

qator ham yechiluvchan bo'ladi. Demak, G gruppa ham yechiluvchan. $\square$

Endi gruppaning yechiluvchan bo'lishini uning kommutanti orqali ifodalovchi natijani keltiramiz. Ma'lumki, G gruppaning kommutanti $[G,G] = \langle [a,b] = aba^{-1}b^{-1} \mid a,b \in G\rangle$ to'plamdan iborat bo'lib, u normal qism gruppa bo'ladi (1.6.3-tasdiqqa qarang). Bundan tashqari, $G/[G,G]$ faktor gruppa kommutativ bo'ladi.

4.4.3-teorema. *Bizga G gruppa va uning H qism gruppasi berilgan bo'lsin. $[G,G] \subseteq H$ bo'lishi uchun $H \lhd G$ va G/H faktor gruppaning kommutativ bo'lishi zarur va yetarli.*

Isbot. Aytaylik, $[G,G] \subseteq H$ bo'lsin, u holda ixtiyoriy $h \in H$ va $a \in G$ uchun $aha^{-1}h^{-1} \in [G,G] \subseteq H$ bo'lib, $aha^{-1} = (aha^{-1}h^{-1})h \in H$ ekanligi kelib chiqadi. Demak, H normal qism gruppa bo'ladi. Endi G/H gruppaning kommutativligini ko'rsatamiz. Buning uchun ixtiyoriy $aH, bH \in G/H$ elementlarni olsak,

$$(aH)(bH)(aH)^{-1}(bH)^{-1} = aHbHa^{-1}Hb^{-1}H = aba^{-1}b^{-1}H$$

bo'ladi. $aba^{-1}b^{-1} \in [G,G] \subseteq H$ ekanligidan $(aH)(bH)(aH)^{-1}(bH)^{-1} = H$ bo'lishi, ya'ni $aHbH = bHaH$ ekanligi kelib chiqadi.

Va aksincha, agar $H \lhd G$ bo‘lib, G/H kommutativ bo‘lsa, u holda $a, b \in G$ elementlar uchun $(aH)(bH) = (bH)(aH)$ tenglikdan $aba^{-1}b^{-1} \in H$ munosabat kelib chiqadi. Bu esa, $[G, G] \subseteq H$ ekanligini anglatadi. $\square$

Quyidagi belgilashlarni kiritamiz

$$G^{(1)} = [G, G], \quad G^{(k+1)} = [G^{(k)}, G^{(k)}], \ k \geq 1.$$

U holda biz kommutantlardan iborat quyidagi qatorga ega bo‘lamiz

$$G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq G^{(3)} \supseteq \dots.$$

Ushbu qator G gruppaning **hosilaviy qatori** deb ataladi. Quyidagi teoremada berilgan gruppaning yechiluvchan bo‘lishini hosilaviy qator orqali beriluvchi zaruriy va yetarlilik kriteriyasini keltiramiz.

4.4.4-teorema. *G gruppa yechiluvchan bo‘lishi uchun shunday $m \in \mathbb{N}$ soni topilib, $G^{(m)} = \{e\}$ bo‘lishi zarur va yetarli.*

Isbot. Aytaylik, $G^{(m)} = \{e\}$ bo‘lsin, u holda

$$G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(m-1)} \supseteq G^{(m)} = \{e\}$$

qator yechiluvchan qator bo‘lib, G gruppaning yechiluvchanligini hosil qilamiz.

Endi G gruppaning yechiluvchanligidan $G^{(m)} = \{e\}$ bo‘ladigan m soni mavjud ekanligini ko‘rsatamiz. G gruppa yechiluvchan bo‘lganligi uchun

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_{n-1} \supseteq H_n = \{e\}$$

yechiluvchan qator mavjud. $H_{i+1} \lhd H_i$ va H_i/H_{i+1} faktorning kommutativ ekanligidan 4.4.3-teoremaga ko‘ra $[H_i, H_i] \subseteq H_{i+1}$ ekanligi kelib chiqadi. Bundan esa,

$$H_1 \supseteq [H_0, H_0] = G^{(1)}, \ H_2 \supseteq [H_1, H_1] = G^{(2)}, \dots, \{e\} = H_n \supseteq [H_{n-1}, H_{n-1}] = G^{(n)}$$

ekanligini hosil qilamiz. Demak, $G^{(n)} = \{e\}$. $\square$

Endi S_n o‘rin almashtirishlar gruppasining $n \geq 5$ bo‘lganda yechiluvchan emasligini ko‘rsatamiz.

4.4.5-teorema. $S_n (n \geq 5)$ *o‘rin almashtirishlar gruppasi yechiluvchan emas.*

Isbot. Ayatylik, S_n gruppaning H qism gruppasi berilgan bo‘lib, u uzunligi 3 ga teng bo‘lgan barcha sikllarni o‘z ichiga olsin. Ixtiyoriy $\pi = (a \ b \ c) \in H$ sikl uchun a, b, c sonlaridan farqli d, f sonlarni olib ($n \geq 5$ bo‘lgani uchun bunday sonlar mavjud), $\alpha = (a \ b \ d)$ va $\beta = (a \ c \ f)$ sikllarni qaraymiz. U holda $\pi, \alpha, \beta \in H$ bo‘lib,

$$(a \ b \ c) = (a \ b \ d) \circ (a \ c \ f) \circ (a \ d \ b) \circ (a \ f \ c) = \alpha\beta\alpha^{-1}\beta^{-1} \in [H, H]$$

bo‘ladi. Bu esa, uzunligi 3 ga teng bo‘lgan ixtiyoriy $\pi = (a\ b\ c)$ siklning $[H, H]$ kommutantda yotishini bildiradi. Bundan esa, $S_n^{(1)} = [S_n, S_n]$ ham uzunligi 3 ga teng bo‘lgan barcha sikllarni o‘z ichiga olishi kelib chiqadi. Induktiv ravishda, ixtiyoriy $k \geq 1$ uchun $S_n^{(k)}$ qism gruppa uzunligi 3 ga teng bo‘lgan barcha sikllarni o‘z ichiga olishiga ega bo‘lamiz. Demak, $S_n^{(m)} = \{e\}$ tenglik o‘rinli bo‘ladigan m soni mavjud emas. Ya’ni S_n $(n \geq 5)$ gruppa yechiluvchan emas. $\square$

4.4.2 Nilpotent gruppalar

Endi nilpotent gruppalar ta’rifini kiritib ularning xossalarini keltiramiz.

4.4.4-ta’rif. *Agar G gruppada $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$ shartni qanoatlantiruvchi*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n = \{e\}$$

*normal qator mavjud bo‘lsa, u holda G gruppaga **nilpotent** gruppa deb ataladi. Berilgan qatorga esa G gruppaning **markaziy qatori** deyiladi.*

Takidlash joizki, ixtiyoriy normal qator subnormal bo‘lganligi va $Z(G/G_i)$ gruppaning kommutativ ekanligidan, ixtiyoriy nilpotent gruppaning yechiluvchan ekanligi kelib chiqadi. Bundan tashqari, ixtiyoriy kommutativ gruppa ham nilpotent bo‘ladi. Quyidagi misolda esa, yechiluvchan S_3 gruppaning nilpotent emasligini ko‘rsatamiz.

4.4.5-misol. *S_3 o’rin almashtirishlar gruppasi uchun ikkita normal qator mavjud bo‘lib, ular quyidagilardan iboratdir*

$$S_3 \supseteq \{e\}$$

va

$$S_3 \supseteq \{e, (1\ 2\ 3), (1\ 3\ 2)\} \supseteq \{e\}.$$

Birinchi qator uchun $S_3/\{e\} \nsubseteq Z(S_3/\{e\})$ ekanligi ravshan.

Ikkinchi qator uchun esa $H_1/\{e\} \nsubseteq Z(S_3/\{e\})$ bo‘ladi, bu yerda $H_1 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$. Demak, S_3 gruppa nilpotent emas.

Quyidagi teoremada ixtiyoriy chekli p-gruppasining nilpotent ekanligini ko‘rsatamiz.

4.4.6-teorema. *Chekli p-gruppasi nilpotent bo‘ladi.*

Isbot. Aytaylik, G gruppa chekli p-gruppasi bo‘lsin. Agar $|G| = 1$ bo’lsa, u holda uning nilpotent ekanligi ma’lum. Aytaylik, $|G| > 1$ bo‘lsin, u holda p-gruppaning markazi uchun $|Z(G)| > 1$ ekanligidan $Z_1 = Z(G) \neq \{e\}$ bo‘ladi (4.2.3-teoremaga ko‘ra). Agar $G \neq Z(G)$ bo‘lsa, u holda $|G/Z(G)| > 1$ bo‘lib,

$G/Z(G)$ ham p-gruppa bo‘lganligi uchun $|Z(G/Z_1)| > 1$. U holda G gruppaning shunday Z_2 normal qism gruppasi topilib, $Z_1 \subset Z_2$ va $Z_2/Z_1 = Z(G/Z_1)$ bo‘ladi. Natijada biz $\{e\} \subset Z_1 \subset Z_2$ qatorni hosil qilamiz. Agar $G \neq Z_2$ bo‘lsa, u holda ushbu jarayonni yana davom ettirgan holda,

$$\{e\} \subset Z_1 \subset Z_2 \subset \cdots \subset Z_n$$

normal qatorni hosil qilamiz. G gruppa chekli bo‘lganligi uchun bu jarayon chekli qadamdan keyin to‘xtaydi, ya’ni $Z_n = G$ bo‘ladi. Ushbu normal qator uchun $Z_{i+1}/Z_i = Z(G/Z_i)$ ekanligidan G gruppaning nilpotentligi kelib chiqadi. □

Endi berilgan G gruppa uchun quyi markaziy qator tushunchasini kiritamiz. Gruppaning $G^{[i]}$ qism gruppalarini quyidagicha aniqlaymiz

$$G^{[1]} = G,\ G^{[2]} = [G^{[1]}, G], \dots, G^{[i]} = [G^{[i-1]}, G],\ i \geq 1.$$

U holda ushbu qator

$$G = G^{[1]} \supseteq G^{[2]} \supseteq G^{[3]} \supseteq \dots$$

markaziy qator bo’lib, uni G gruppaning **quyi markaziy qatori** deb ataladi.

4.4.7-teorema. *G gruppa nilpotent bo‘lishi uchun $G^{[n]} = \{e\}$ shartni qanoatlantiruvchi n natural son topilishi zarur va yetarli.*

Isbot. Aytaylik, qandaydir natural n soni uchun $G^{[n]} = \{e\}$ bo‘lsin. U holda

$$\{e\} = G^{[n]} \subseteq G^{[n-1]} \subseteq \cdots \subseteq G^{[2]} \subseteq G^{[1]} = G$$

qator markaziy qator bo‘lib, G gruppaning nilpotent ekanligi kelib chiqadi.

Endi buning aksini, ya’ni agar G gruppa nilpotent bo‘lsa, u holda $G^{[m]} = \{e\}$ shartni qanoatlantiruvchi m natural soni mavjudligini ko‘rsatamiz. Gruppa nilpotent bo‘lganligi uchun

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

markaziy qator mavjud. U holda $G_{i+1}/G_i \subseteq Z(G/G_i)$ bo‘lib, $\forall g_{i+1} \in G_{i+1}$ va $g \in G$ uchun $g_{i+1}G_i \cdot gG_i = gG_i \cdot g_{i+1}G_i$ bo‘ladi. Bundan esa, $g_{i+1}gG_i = gg_{i+1}G_i$ ekanligi, ya’ni $g_{i+1}^{-1}g^{-1}g_{i+1}gG_i = G_i$ bo‘lishi kelib chiqadi. Bu esa, $g_{i+1}^{-1}g^{-1}g_{i+1}g \in G_i$ ekanligini, ya’ni $[G_{i+1}, G] \subseteq G_i$ bo‘lishini anglatadi.

Biz endi $G^{[i]} \subseteq G_{n-i+1},\ \ 1 \leq i \leq n+1$ ekanligini ko‘rsatamiz. Buning uchun i ga nisbatan induksiya metodidan foydalanamiz. $G^{[1]} = G = G_n$ ekanligidan ushbu munosabatning $i = 1$ da o‘rinli ekanligi kelib chiqadi. Faraz qilaylik, $G^{[j]} \subseteq G_{n-j+1}$ munosabat o‘rinli bo‘lsin. U holda

$$G^{[j+1]} = [G^{[j]}, G] \subseteq [G_{n-j+1}, G] \subseteq G_{n-j}.$$

Demak, $G^{[i]} \subseteq G_{n-i+1}$ munosabat $i = 1, 2, \dots, n+1$ lar uchun o'rinli. Demak, $G^{[n+1]} \subseteq G_0 = \{e\}$ bo'ladi. □

Yuqoridagi teoremadan foydalanib, nilpotent gruppaning ixtiyoriy qism gruppasi yana nilpotent bo'lishini ko'rsatish qiyin emas. Chunki, agar G nilpotent gruppa bo'lsa, u holda qandaydir n soni uchun $G^{[n]} = \{e\}$ bo'ladi. Gruppaning ixtiyoriy H qism gruppasi uchun $H^{[i]} \subseteq G^{[i]}$ ekanligidan $H^{[n]} = \{e\}$ bo'lishi, ya'ni qism gruppaning ham nilpotentligi kelib chiqadi.

Endi gruppa uchun yuqori markaziy qator tushunchasini kiritamiz. Berilgan G gruppa uchun $Z_0(G) = \{e\}$ va $Z_1(G) = Z(G)$ kabi belgilashlarni kiritamiz. $Z_1(G)$ qism gruppa G da normal bo'lganligi uchun $G/Z_1(G)$ faktor gruppani qarash mumkin, hamda $Z(G/Z_1(G))$ ham o'z navbatida faktor gruppaning normal qism gruppasi bo'ladi. U holda G gruppaning $Z_1(G) \subseteq Z_2(G)$ va $Z_2(G)/Z_1(G) = Z(G/Z_1(G))$ shartlarni qanoatlantiruvchi yagona $Z_2(G)$ normal qism gruppasi mavjud.

Ushbu jarayonni davom ettirgan holda, $Z_i(G) \subseteq Z_{i+1}(G)$ va $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ shartlarni qanoatlantiruvchi

$$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \dots \subseteq Z_n(G) \subseteq \dots$$

qatorni hosil qilamiz. Ushbu $Z_i(G)$ qism gruppalar G da normal bo'lganligi uchun, biz hosil qilgan qator normal qator bo'ladi. Ushbu qatorga G gruppaning **yuqori markaziy qatori** deb ataladi.

Ta'kidlash joizki, agar G gruppada qandaydir n natural son uchun $Z_n(G) = G$ tenglik o'rinli bo'lsa, biz hosil qilgan

$$\{e\} = Z_0(G) \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \dots \subseteq Z_n(G) = G$$

qator markaziy qator bo'ladi, chunki $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. Demak, agar $Z_n(G) = G$ bo'lsa, u holda G nilpotent bo'ladi.

Quyidagi teoremada esa, ushbu munosabatning teskarisi ham o'rinli ekanligini isbotlaymiz.

4.4.8-teorema. *Agar G gruppa nilpotent bo'lsa, u holda n natural soni mavjud bo'lib, $G = Z_n(G)$ bo'ladi.*

Isbot. Gruppa nilpotent ekanligidan

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \dots \subseteq G_n = G$$

markaziy qator mavjud ekanligi kelib chiqadi. Ya'ni $G_i/G_{i-1} \subseteq Z(G/G_{i-1})$. Teoremani isbotlash uchun induktiv tarzda $G_i \subseteq Z_i(G)$ ekanligini ko'rsatamiz. $i = 0$ uchun $G_0 = \{e\} = Z_0(G)$ bo'lib, induksiya bazasi o'rinli ekanligi kelib chiqadi.

Aytaylik, $G_j \subseteq Z_j(G)$ bo‘lsin, u holda $[G_{j+1}, G] \subseteq G_j \subseteq Z_j(G)$ ekanligidan foydalansak, $\forall g_{j+1} \in G_{j+1}$ va $\forall g \in G$ uchun $g_{j+1}^{-1} g^{-1} g_{j+1} g \subseteq Z_j(G)$ kelib chiqadi. Bundan $g_{j+1}Z_j(G) \cdot gZ_j(G) = gZ_j(G) \cdot g_{j+1}Z_j(G)$ tenglikka ega bo‘lamiz. Bu esa $g_{j+1}Z_j(G) \in Z(G/Z_j(G)) = Z_{j+1}(G)/Z_j(G)$ ekanligini, ya’ni $g_{j+1} \in Z_{j+1}(G)$ bo‘lishini anglatadi. Demak, $G_{j+1} \subseteq Z_{j+1}(G)$. U holda $G_n = G$ ekanligidan $Z_n(G) = G$ bo‘lishi kelib chiqadi. □

Quyidagi lemmada yuqori markaziy qator uchun o‘rinli bo‘ladigan xossalardan birini keltiramiz.

4.4.1-lemma. *Agar G gruppa H va K gruppalarning to‘g‘ri ko‘paytmasidan iborat bo‘lsa, ya’ni $G = H \times K$ bo‘lsa, u holda $Z_i(G) = Z_i(H) \times Z_i(K)$ bo‘ladi.*

Isbot. Lemmani i ga nisbatan induksiya usulidan foydalanib isbotlaymiz. Agar $i = 1$ bo‘lsa, u holda

$$Z_1(G) = Z(G) = Z(H \times K) = Z(H) \times Z(K) = Z_1(H) \times Z_1(K)$$

ekanligidan lemmaning o‘rinli bo‘lishi kelib chiqadi.

Faraz qilaylik, lemmadagi tenglik $i = k$ uchun o‘rinli bo‘lsin, ya’ni $Z_k(G) = Z_k(H) \times Z_k(K)$. Biz uni $i = k + 1$ uchun o‘rinli ekanligini ko‘rsatamiz. Ma’lumki, $Z_{k+1}(G)$ qism gruppa G gruppaning $Z_k(G) \subseteq Z_{k+1}(G)$ va $Z_{k+1}(G)/Z_k(G) = Z(G/Z_k(G))$ shatlarni qanoatlantiruvchi yagona normal qism gruppasi. Tabiiy ravishda aniqlanuvchi quyidagi $\psi : H/Z_i(H) \times K/Z_i(K) \to (H \times K)/Z_i(H \times K)$ izomorfizmni qaraymiz. U holda

$$\begin{aligned}
Z(G/Z_k(G)) &= Z\big((H \times K)/Z_k(H \times K)\big) \\
&= Z\big((H \times K)/Z_k(H) \times Z_k(K)\big) \\
&= Z\big(\psi((H/Z_k(H)) \times (K/Z_k(K)))\big) \\
&= \psi\big(Z(H/Z_k(H) \times K/Z_k(K))\big) \\
&= \psi\big(Z(H/Z_k(H)) \times Z(K/Z_k(K))\big) \\
&= \psi\big(Z_{k+1}(H)/Z_i(H) \times Z_{k+1}(K)/Z_k(K)\big) \\
&= \big(Z_{k+1}(H) \times Z_{k+1}(K)\big)/\big(Z_k(H) \times Z_k(K)\big) \\
&= \big(Z_{k+1}(H) \times Z_{k+1}(K)\big)/Z_k(H \times K) \\
&= \big(Z_{k+1}(H) \times Z_{k+1}(K)\big)/Z_k(G).
\end{aligned}$$

Demak, $Z_{k+1}(G) = Z_{k+1}(H) \times Z_{k+1}(K)$. □

Yuqoridagi lemmadan nilpotent gruppalarning to‘g‘ri ko‘paytmasi yana nilpotent bo‘lishi kelib chiqadi. Chunki, agar H va K gruppalar nilpotent bo‘lsa, u holda $Z_n(H) = H$ va $Z_n(K) = K$ bo‘lib, $Z_n(H \times K) = Z_n(H) \times Z_n(K) = H \times K$ ekanligidan ularning to‘g‘ri ko‘paytmasi ham nilpotent bo‘lishini hosil qilamiz. Ushbu mulohazani umumlashtirgan holda quyidagi teoremaga ega bo‘lamiz

4.4.9-teorema. *Agar $G_1, G_2, \dots, G_n$ gruppalar nilpotent bo‘lsa, u holda $G_1 \times G_2 \times \dots \times G_n$ gruppa ham nilpotent bo‘ladi.*

Quyidagi teoremada biz gruppaning nilpotent bo‘lishiga ekvivalent bo‘lgan bir qancha shartlarni keltiramiz. Hususan, ushbu teorema nilpotent gruppalarni p-gruppalar orqali to‘liq tasniflash imkonini beradi.

4.4.10-teorema. *Bizga G chekli gruppa berilgan bo‘lsin. U holda quyidagilar ekvivalent.*

1) G nilpotent gruppa.

2) G gruppaning ixtiyoriy maksimal qism gruppasi normal.

3) G gruppaning ixtiyoriy Silov qism gruppasi normal.

4) G gruppa p-gruppalarning to‘g‘ri ko‘paytmasi shaklida ifodalanadi.

Isbot. 1)$\Rightarrow$2) G gruppa nilpotent bo‘lganligi uchun

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \dots \subseteq G_n = G$$

markaziy qator mavjud. Aytaylik, H maksimal qism gruppa bo‘lsin, u holda $G_0 \subseteq H \subset G_n$ va $H \neq G$ bo‘lgani uchun $G_m \subseteq H$ va $G_{m+1} \nsubseteq H$ shartlarni qanoatlantiruvchi $m \geq 0$ soni topiladi. Demak, $a \in G_{m+1}$, $a \notin H$ element mavjud. Endi $aG_m \in Z(G/G_m)$ ekanligidan ixtiyoriy $h \in H$ uchun $(aG_m)(hG_m) = (hG_m)(aG_m)$ ekanligiga, ya’ni $h^{-1}a^{-1}ha = (ah)^{-1}ha \in G_m \subseteq H$ munosabatga ega bo‘lamiz. Bu esa, $a^{-1}ha \in H$, ya’ni $a^{-1}Ha \subseteq H$ ekanligini anglatadi. Xuddi shunga o‘xshab, $aHa^{-1} \subseteq H$ munosabatni ham hosil qilish mumkin. Demak, $a^{-1}Ha = H$, bu esa, $a \in N(H)$ ekanligini bildiradi. Natijada biz $H \neq N(H)$ ekanligiga ega bo‘ldik. H ning maksimalligidan esa, $N(H) = G$ hosil bo‘ladi. Ya’ni H normal qism gruppa.

2)$\Rightarrow$ 3) Faraz qilaylik G gruppaning biror P Silov p-qism gruppasi berilgan bo‘lib, u normal qism gruppa bo‘lmasin. G gruppa chekli bo‘lganligi uchun $N(P)$ qism gruppani o‘z ichiga oluvchi H maksimal qism gruppa mavjud, ya’ni $N(P) \subseteq H$. U holda H normal qism gruppa bo‘lib, ixtiyoriy $a \in G$ uchun

$$aPa^{-1} \subseteq aN(P)a^{-1} \subseteq aHa^{-1} = H$$

bo‘ladi. Bu esa, P va aPa^{-1} Silov p-qism gruppalarining H ga ham qism bo‘lishini bildiradi. Demak, $h \in H$ element topilib, $h(aPa^{-1})h^{-1} = P$ bo‘ladi. Bundan esa, $ha \in N(P) \subseteq H$ ekanligi, hamda $a = h^{-1}(ha) \in H$ kelib chiqadi. Ya’ni $H = G$ bu esa H ning maksimal ekanligiga zid. Demak, P normal qism gruppa.

3)$\Rightarrow$ 4) Ko‘rsatish qiyin emaski, agar G gruppaning ixtiyoriy Silov qism gruppasi normal bo‘lsa, u holda G gruppa Silov qism gruppalarning to‘g‘ri ko‘paytmasi shaklida yoziladi. Silov qism gruppalari p-gruppalar bo‘lganligi uchun berilgan gruppa p-gruppalarning to‘g‘ri ko‘paytmasi shaklida ifodalanadi.

4)$\Rightarrow$1) Ushbu natifa 4.4.6-teorema va 4.4.9-teoremalardan bevosita kelib chiqadi. $\square$

Biz Silov teoremalari mavzusida kommutativ gruppalar uchun Lagranj teoremasining teskarisi o‘rinli ekanligini ko‘rsatgan edik. Ya’ni kommutativ gruppaning tartibi m ga teng bo‘lib, n soni m ning bo‘luvchisi bo‘lsa, u holda gruppada tartibi n ga teng bo‘lgan qism gruppa mavjud bo‘ladi. Quyidagi teoremada nilpotent gruppalar uchun ham Lagranj teoremasining teskarisi o‘rinli bo‘lishini ko‘rsatamiz.

4.4.11-teorema. *Aytaylik, G nilpotent gruppa bo‘lib, $|G| = m$ bo‘lsin. Agar $n \mid m$ bo‘lsa, ya’ni n soni m ning bo‘luvchisi bo‘lsa, u holda gruppa tartibi n ga teng bo‘lgan qism gruppaga ega.*

Isbot. Aytaylik, $m = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ bo‘lib, $H_i, 1 \leq i \leq k$ qism gruppalar G gruppaning Silov p-qism gruppalari bo‘lsin. U holda $G = H_1 \times H_2 \times H \dots \times H_k$ bo‘lib, ixtiyoriy $n \mid m$ soni $n = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$ ko‘rinishida bo‘ladi. $|H_i| = p_i^{r_i}$ bo‘lganligi uchun bu qism gruppalarning tartibi $p_i^{t_i}$ ga teng bo‘lgan A_i qism gruppalari mavjud. U holda $B = A_1 \times A_2 \times \dots A_k$ qism gruppaning tartibi n ga teng bo‘ladi. $\square$

4.4.6-misol. *Yechiluvchan gruppaning $H \neq \{e\}$ qism gruppasi uchun $H^{(1)} \neq H$ ekanligini isbotlang.*

Yechish. Faraz qilaylik, $H^{(1)} = H$ bo‘lsin, u holda, $H^{(2)} = [H^{(1)}, H^{(1)}] = [H, H] = H^{(1)} = H \neq \{e\}$ ekanligidan, induktiv tarzda $H^{(n)} = H \neq \{e\}$ bo‘lishini hosil qilamiz. Ikkinchi tomondan esa, H yechiluvchan gruppaning qism gruppasi bo‘lganligi uchun, u ham yechiluvchan bo‘ladi. Bu esa, qandaydir k uchun $H^{(k)} = \{e\}$ bo‘lishini anglatadi. Natijada biz ziddiyatga ega bo‘lamiz, demak, $H^{(1)} \neq H$. $\square$

4.4.7-misol. $GL_n(\mathbb{R})$, $n \geq 3$ *gruppaning yechiluvchan emasligini ko‘rsating.*

Yechish. Aytaylik, $G = GL_n(\mathbb{R})$ bo‘lsin. E_{ij} orqali $a_{i,j} = 1$ va qolgan elementlari nolga teng bo‘lgan n-tartibli matritsani belgilaymiz. U holda

$$E_{ij}E_{rs} = \begin{cases} E_{is}, & \text{agar} \quad j = r, \\ 0, & \text{agar} \quad j \neq r. \end{cases}$$

Bundan tashqari, I birlik matritsa uchun $i \neq j$ da $I + E_{ij} \in G$ bo‘lib, $(I + E_{ij})^{-1} = I - E_{ij}$ bo‘ladi. Aytaylik, $T = \langle I + E_{ij}, \mid i \neq j \rangle$ bo‘lsin, ya’ni T orqali $\{I + E_{ij} \mid i \neq j\}$ elementlardan hosil bo‘lgan qism gruppani belgilaylik. U holda

$n \geq 3$ bo‘lganligi uchun shunday k, $1 \leq i \neq k \neq j \leq n$ soni topilib,

$$\begin{aligned}(I+E_{ik})(I+E_{kj})(I+E_{ik})^{-1}(I+E_{kj})^{-1} &= (I+E_{ik})(I+E_{kj})(I-E_{ik})(I-E_{kj}) \\ &= (I+E_{kj}+E_{ik}+E_{ij})(I+E_{kj}+E_{ik}+E_{ij}) = (I+E_{ij})\end{aligned}$$

bo‘ladi. Bu esa $(I+E_{ij}) \in T^{(1)}$ ekanligini anglatadi, ya’ni $T = T^{(1)}$. Demak, T yechiluvchan emas, bundan esa, G gruppaning ham yechiluvchan emasligi kelib chiqadi. □

4.4.8-misol. *D_4 gruppa uchun markaziy qator toping.*

Yechish. Ma’lumki, $D_4 = \langle a, b\rangle$ bo‘lib, $ord(a) = 4, ord(b) = 2$ va $ba = a^3b$. Ushbu gruppa uchun quyidagi qatorni qaraymiz

$$\{e\} \subseteq \{e, a^2\} \subseteq \{e, a, a^2, a^3\} \subseteq D_4,$$

ya’ni $G_0 = \{e\}$, $G_1 = \{e, a^2\}$, $G_2 = \{e, a, a^2, a^3\}$ va $G_3 = D_4$. Ma’lumki, ushbu qator normal qator bo‘lib, $|D_4/G_1| = 4$ va $|D_4/G_2| = 2$ ekanligidan D_4/G_1 va D_4/G_2 gruppalarning kommutativ ekanligi kelib chiqadi. Demak, $G_2/G_1 \subseteq D_4/G_1 = Z(D_4/G_1)$ va $D_4/G_2 \subseteq Z(D_4/G_2) = D_4/G_2$. Bundan tashqari, $Z(D_4) = \{e, a^2\} = G_1$ ekanligidan $G_1/G_0 \subseteq Z(D_4/G_0)$ munosabatni hosil qilamiz. Demak, keltirilgan $G_0 \subseteq G_1 \subseteq G_2 \subseteq G_2$ qator markaziy qator bo‘ladi. □

4.4.3 Mustaqil ishlash uchun misol va masalalar

1. $\mathbb{Z}_{20}$ gruppa uchun mumkin bo‘lgan barcha normal qatorlarni tuzing.

2. Quyidagi gruppalar uchun mumkin bo‘lgan barcha normal qatorlarni tuzing.

$$\mathbf{K}_4, \quad S_3, \quad D_4, \quad Q_8, \quad \mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_{15}, \quad A_4, \quad S_4.$$

3. Quyidagi gruppalar uchun mumkin bo‘lgan barcha subnormal qatorlarni tuzing.

$$S_3, \quad D_4, \quad Q_8, \quad A_4, \quad S_4.$$

4. Tartibi quyidagi sonlarga teng bo‘lgan gruppalarning yechiluvchan ekanligini isbotlang.

$$12, \quad 15, \quad 20, \quad 21, \quad 28, \quad 35, \quad 36, \quad 42, \quad 45, \quad 100.$$

5. Tartibi quyidagi sonlarga teng bo‘lgan gruppalarning nilpotent ekanligini isbotlang.

$$16, \quad 27, \quad 33, \quad 35, \quad 45, \quad 51, \quad 65.$$

6. D_5 gruppaning nilpotent emasligini ko‘rsating.

7. D_n gruppaning yechiluvchan ekanligini isbotlang.

8. D_n gruppa nilpotent bo‘lishi uchun $n = 2^m$ bo‘lishi zarur va yetarli ekanligini isbotlang.

9. Agar G gruppaning N normal qism gruppasi uchun $N \cap G^{(1)} = \{e\}$ bo‘lsa, u holda $N \subseteq Z(G)$ va $Z(G/N) = Z(G)/N$ ekanligini isbotlang.

10. Tartibi pq (p, q – tub sonlar) bo‘lgan ixtiyoriy gruppa yechiluvchan ekanligini isbotlang.

11. Tartibi p^2q (p, q – tub sonlar) bo‘lgan ixtiyoriy gruppa yechiluvchan ekanligini isbotlang.

12. Tartibi pqr (p, q, r – tub sonlar) bo‘lgan ixtiyoriy gruppa yechiluvchan ekanligini isbotlang.

13. Tartibi p^2q^2 (p, q – tub sonlar) bo‘lgan ixtiyoriy gruppa yechiluvchan ekanligini isbotlang.

14. Quyidagi qruppalarning hosilaviy qatorlarini aniqlang

$$D_4, \quad Q_8, \quad A_4, \quad S_4, \quad S_3 \times \mathbb{Z}_2, \quad S_3 \times \mathbb{Z}_3, \quad S_3 \times S_3.$$

15. Quyidagi qruppalarning quyi markaziy qatorlarini aniqlang

$$D_4, \quad Q_8, \quad A_4, \quad S_4, \quad S_3 \times \mathbb{Z}_2, \quad S_3 \times \mathbb{Z}_3, \quad S_3 \times S_3.$$

16. Isbotlang $[S_n, S_n] = A_n$.

17. Isbotlang $[A_n, A_n] = A_n,\ n \geq 5$.

18. Quyidagilarni aniqlang
    - $[SL_2(\mathbb{Z}_2), SL_2(\mathbb{Z}_2)]$,
    - $[GL_2(\mathbb{Z}_2), GL_2(\mathbb{Z}_2)]$,
    - $[SL_2(\mathbb{Z}_3), SL_2(\mathbb{Z}_3)]$,
    - $[GL_2(\mathbb{Z}_3), GL_2(\mathbb{Z}_3)]$.

19. Isbotlang $[GL_n(\mathbb{R}), GL_n(\mathbb{R})] = SL_n(\mathbb{R})$.

20. Isbotlang $[SL_n(\mathbb{R}), SL_n(\mathbb{R})] = SL_n(\mathbb{R})$.

21. Yuqori uchburchak ko‘rinishidagi xosmas matritsalar gruppasi (ko‘paytirish amaliga nisbatan) yechiluvchan ekanligini isbotlang.

22. Yechiluvchan gruppalarning to‘g‘ri ko‘paytmasi yechiluvchan bo‘lishini isbotlang.

23. $S_3 \times \mathbb{Z}$ gruppa cheksiz yechiluvchan gruppa ekanligini isbotlang.

24. G gruppa yechiluvchan bo‘lishi uchun $G/Z(G)$ faktor gruppaning yechiluvchan bo‘lishi zarur va yetarli ekanligini isbotlang.

25. G gruppaning A qism gruppasi va B normal qism gruppasi berilgan bo‘lsin. Agar A va B qism gruppalar yechiluvchan bo‘lsa, u holda AB ham yechiluvchan ekanligini isbotlang.

26. Nilpotent gruppaning gomomorf obazi yana nilpotent bo‘lishini isbotlang.

27. O‘zi nilpotent bo‘lmagan, lekin qandaydir normal qism gruppasi bo‘yicha faktor gruppasi nilpotent bo‘lgan gruppaga misol keltiring.

BOB 5

Halqalar va ideallar

5.1 Halqalar va ularning turlari

Biz avvalgi boblarda bitta binar amalga ega bo‘lgan algebraik sistema bo‘lgan gruppa tushunchasini batafsil o‘rgandik. Ushbu bobda esa ikkita binar amal bilan aniqlanuvchi algebraik sistema bo‘lgan halqa tushunchasini kiritamiz.

Bizga bo‘sh bo‘lmagan R to‘plam berilgan bo‘lib, unda ikkita binar amal aniqlangan bo‘lsin. Ushbu binar amallarni $+$ va $\cdot$ kabi belgilab, ularni shartli ravishda qo‘shish va ko‘paytirish amallari deb ataymiz.

5.1.1-ta’rif. *Bo‘sh bo‘lmagan R to‘plamda aniqlangan $+$ va $\cdot$ binar amallari quyidagi shartlarni qanoatlantirsa:*

1. *$(R, +)$ kommutativ gruppa;*

2. *$(R, \cdot)$ yarim gruppa;*

3. *Barcha $a, b, c \in R$ elementlar uchun*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

u holda $(R, +, \cdot)$ uchlikka ***halqa*** *deyiladi.*

Boshqacha qilib aytganda, bo‘sh bo‘lmagan R to‘plamdagi $+$ va $\cdot$ binar amallari uchun quyidagi aksiomalar bajarilsa, u holda $(R, +, \cdot)$ halqa deb ataladi:
($\mathbf{R}_1$) Ixtiyoriy $a, b, c \in R$ elementlar uchun $(a + b) + c = a + (b + c)$.
($\mathbf{R}_2$) Ixtiyoriy $a, b \in R$ elementlar uchun $a + b = b + a$.
($\mathbf{R}_3$) Shunday $0 \in R$ element mavjudki, ixtiyoriy $a \in R$ uchun $a + 0 = a$.
($\mathbf{R}_4$) Ixtiyoriy $a \in R$ uchun shunday $-a \in R$ element mavjudki, bunda $a + (-a) = 0$.
($\mathbf{R}_5$) Ixtiyoriy $a, b, c \in R$ elementlar uchun $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
($\mathbf{R}_6$) Ixtiyoriy $a, b, c \in R$ elementlar uchun $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ va

$(b+c)\cdot a = (b\cdot a) + (c\cdot a)$.

Halqadagi 0 elementni **halqaning nol elementi** deyiladi. Odatda halqalar uchun $a\cdot b$ o'rniga ab belgilashdan $a+(-b)$ o'rniga esa $a-b$ belgilashdan foydalish qabul qilingan.

5.1.1-misol. *$\mathbb{Z}$ butun sonlar to'plami odatdagi qo'shish va ko'paytirish amallariga nisbatan halqa bo'ladi. Bundan tashqari, ratsional sonlar to'plami $\mathbb{Q}$, haqiqiy sonlar to'plami $\mathbb{R}$ va kompleks sonlar to'plami $\mathbb{C}$ ham qo'shish va ko'paytirish amallariga nisbatan halqa tashkil qiladi.*

5.1.2-ta'rif. *R halqaning barcha $a, b \in R$ elementlari uchun $ab = ba$ tenglik o'rinli bo'lsa, u holda R halqa* ***kommutativ halqa*** *deyiladi. Komutativ bo'lmagan halqalarga esa nokommutativ halqa deb ataladi.*

Endi halqaning markazi va birlik elementi tushunchalarini kiritamiz. Bizga qandaydir R halqa berilgan bo'lsin, ushbu

$$C(R) = \{a \in R \mid ab = ba, \ \forall\, b \in R\}$$

to'plamga R halqaning **markazi** deb ataladi. Ravshanki, R kommutativ halqa bo'lishi uchun $R = C(R)$ bo'lishi zarur va yetarli.

Agar R halqada ko'paytirish amaliga nisbatan birlik element mavjud bo'lsa, ya'ni shunday $e \in R$ element topilib, ixtiyoriy $a \in R$ uchun $ea = a = ae$ tenglik o'rinli bo'lsa, u holda ushbu e elementga halqaning **birlik** elementi deyiladi. Gruppalar nazariyasidan ma'lumki, ixtiyoriy algebraik sistemaning birlik elementi yagona bo'ladi. Demak, halqaning birlik elementi ham yagona bo'lib, biz uni 1 orqali belgilaymiz. Birlik elementga ega bo'lgan halqa **biri bor halqa** deb ataladi.

5.1.2-misol. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ *va* $(\mathbb{C}, +, \cdot)$ *halqalar biri bor kommutativ halqalarga misol bo'ladi.*

5.1.3-misol. $(2\mathbb{Z}, +, \cdot)$ *juft sonlar to'plami birlik elementga ega bo'lmagan halqa bo'ladi.*

5.1.4-misol. *Agar R kommutativ halqa bo'lsa, u holda R ustida aniqlangan bir o'zgaruvchili ko'phadlar to'plami $R[x]$, ko'phadlarni qo'shish va ko'paytirish amallari bilan birgalikda kommutativ halqa bo'ladi. Xususan,* $(\mathbb{Z}[x], +, \cdot)$, $(\mathbb{Q}[x], +, \cdot)$, $(\mathbb{R}[x], +, \cdot)$ *va* $(\mathbb{C}[x], +, \cdot)$ *halqalar kommutativ bo'ladi.*

5.1.5-misol. *Chegirmalar sinfi $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n}\}$ to'plam unda aniqlangan qo'shish va ko'paytirish ammalari bilan birgalikda halqa tashkil qiladi.* $(\mathbb{Z}_n, +_n, \cdot_n)$ *halqa chegirmalar halqasi deb ataladi.*

Yuqorida biz faqat kommutativ halqalarga misollar keltirdik. Quyidagi misolda esa nokommutativ halqaga misol keltiramiz.

5.1.6-misol. *Elementlari biror R halqadan olingan n-tartibli kvadrat matritsalar to'plami $M_n(R)$ matrisalarni qo'shish va ko'paytirish amallariga nisbatan halqa tashkil qiladi. Matrisalarni ko'paytirish amali uchun kommutativlik o'rinli bo'lmaganligi sababli $(M_n(R), +, \cdot)$ nokommutativ halqa bo'ladi.*

Yuqoridagi misoldan ko'rinadiki, $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ va $M_n(\mathbb{C})$ halqalar, ya'ni elementlari mos ravishda butun, ratsional, haqiqiy va kompleks sonlardan iborat bo'lgan n-tartibli kvadrat matritsalar to'plami nokommutativ halqa bo'ladi. Ushbu matritsalar to'plamlarida birlik matritsa yotganligini hisobga olsak, ular birlik elementga ega bo'lgan halqalar bo'ladi. $M_n(2\mathbb{Z})$ to'plam, ya'ni elementlari juft sonlardan iborat matritsalar to'plami esa birlik elementga ega bo'lmagan nokommutativ halqa bo'ladi.

Endi halqaning ayrim elementar xossalarini keltiramiz.

5.1.1-teorema. *R halqa va ixtiyoriy $a, b, \in R$ elementlar uchun quyidagi tengliklar o'rinli:*

1) $a0 = 0a = 0$.

2) $a(-b) = (-a)b = -(ab)$.

Isbot. 1) $aa + a0 = a(a + 0) = aa$ tenglikdan $a0$ elementning qo'shishga nisbatan neytral element ekanligi kelib chiqadi, demak, $a0 = 0$. Xuddi shunga o'xshab $0a = 0$ tenglikni hosil qilish mumkin.

2) $0 = a(b - b) = ab + a(-b)$ tenglikdan $a(-b) = -(ab)$ ekanligi kelib chiqadi. Xuddi shunga o'xshab $(-a)b = -(ab)$ tenglik ham osongina ko'rsatiladi. $\square$

Ta'kidlash joizki, agar R biri bor halqa bo'lib, $R \neq \{0\}$ bo'lsa u holda uning 0 va 1 elementlari har xil bo'ladi. Haqiqatdan ham, agar $1 = 0$ bo'lsa, u holda ixtiyoriy $a \in R$ element uchun $a = a1 = a0 = 0$. Bu esa $R \neq \{0\}$ ekanligiga zid.

Aytaylik, R biri bor halqa bo'lsin. Agar $u \in R$ element uchun shunday $v \in R$ element topilib, $uv = vu = 1$ shart bajarilsa, u holda u element **teskarilanuvchi** deyiladi, v element esa u elementning teskarisi deb ataladi va u^{-1} kabi belgilanadi.

5.1.2-teorema. *R biri bor halqaning barcha teskarilanuvchi elementlaridan tuzilgan T to'plam uchun quyidagilar o'rinli:*

1) $T \neq \emptyset$.

2) $0 \notin T$.

3) $\forall a, b \in T$ *uchun* $ab \in T$.

Isbot. 1) $1 \cdot 1 = 1 = 1 \cdot 1$ bo‘lganligi uchun $1 \in T$, demak $T \neq \emptyset$.

2) Ixtiyoriy $v \in R$ element uchun $0v = 0$ ekanligi va $0 \neq 1$ bo‘lganligi uchun $0 \notin T$ bo‘ladi.

3) Aytaylik, $a, b \in T$ bo‘lsin, u holda $c, d \in R$ elementlar topilib, $ac = ca = 1$ va $bd = db = 1$. Ushbu

$$(ab)(dc) = a(bd)c = ac = 1,$$

$$(dc)(ab) = d(ca)b = db = 1$$

tengliklardan esa ab elementning teskarilanuvchi ekanligi kelib chiqadi, ya’ni $ab \in T$. □

Yuqoridagi teoremadan kelib chiqadiki, biri bor halqaning barcha teskarilanuvchi elementlaridan tashkil topgan to‘plam ko‘paytirish amaliga nisbatan gruppa tashkil qiladi.

5.1.3-ta’rif. *Agar biri bor halqaning ixtiyoriy noldan farqli elementi teskarilanuvchi bo‘lsa, u holda u **jism** deyiladi. Kommutativ jismga **maydon** deb ataladi.*

Ta’kidlash joizki, $(R, +, \cdot)$ halqa jism bo‘lishi uchun $(R \setminus \{0\}, \cdot)$ algebraik sistemaning gruppa bo‘lishi zarur va yetarli. O‘z navbatida R halqa maydon bo‘lishi uchun esa $(R \setminus \{0\}, \cdot)$ algebraik sistemaning kommutativ gruppa bo‘lishi zarur va yetarli.

5.1.7-misol. *1) Butun sonlar halqasi $(\mathbb{Z}, +, \cdot)$ maydon tashkil qilmaydi, chunki uning 1 va -1 dan boshqa elementlari teskarilanuvchi emas.*

2) Ratsional, haqiqiy va kompleks sonlar to‘plami $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ maydon bo‘ladi.

Endi halqalarda yana bir muhim tushuncha bo‘lgan nolning bo‘luvchisi tushunchasini kiritamiz.

5.1.4-ta’rif. *Halqaning noldan farqli $a \in R$ elementi uchun, shunday noldan farqi $b \in R$ element topilib, $ab = 0$ yoki $ba = 0$ bo‘lsa, u holda a element **nolning bo‘luvchisi** deb ataladi.*

Ta’kidlash joizki, jismda hususan maydonda, nolning bo‘luvchisi mavjud emas. Chunki, $ab = 0$ bo‘lsa, u holda $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$ tenglikdan $b = 0$ ekanligi kelib chiqadi.

5.1.5-ta’rif. *Nolning bo‘luvchisiga ega bo‘lmagan kommutativ biri bor halqaga **butunlik sohasi** deyiladi.*

5.1.8-misol. *Butun sonlar halqasi $(\mathbb{Z}, +, \cdot)$ butunlik sohasi bo‘ladi. Juft sonlar to‘plami $(2\mathbb{Z}, +, \cdot)$ esa birlik elementga ega bo‘lmagan kommutativ halqa bo‘lib, nolning bo‘luvchilari mavjud emas.*

5.1.9-misol. *Matritsalar halqasi* $(M_2(\mathbb{R}), +, \cdot)$ *nokommutativ halqa bo'lish bilan birgalikda, nolning bo'luvchilari ega. Husussan,* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ *va* $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *matritsalar nolning bo'luvchilari bo'ladi, chunki*

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Quyidagi teoremada nolning bo'luvchilari bilan halqadagi qisqartirish qoidasi orasidagi bog'lanishni keltiramiz.

5.1.3-teorema. *Nolning bo'luvchisiga ega bo'lmagan halqada qisqartirish qoidasi o'rinli, ya'ni,* $a, b, c \in R$, $a \neq 0$ *elementlar uchun* $ab = ac$ *ekanligidan* $b = c$ *kelib chiqadi (*$ba = ca$ *ekanligidan* $b = c$ *kelib chiqadi). Bu qisqartirish qoidalari mos ravishda chap va o'ng qisqartirish qoidalari deb ataladi. Va aksincha, agar qisqartirish qoidalaridan (chap yoki o'ng) biri o'rinli bo'lsa, u holda* R *nolning bo'luvchisiga ega emas.*

Isbot. Faraz qilaylik R nolning bo'luvchisiga ega bo'lmasin. Aytaylik, $a, b, c \in R$ elementlar uchun $ab = ac$ bo'lib, $a \neq 0$ bo'lsin. U holda $ab - ac = 0$ ekanligidan $a(b - c) = 0$ kelib chiqabi. R nolning bo'luvchisiga ega bo'lmaganligi va $a \neq 0$ ekanligidan $b - c = 0$, ya'ni $b = c$ kelib chiqadi. Xuddi shunda o'xshab, $ba - ca = 0$ ekanligidan ham $b = c$ tenglikni keltirib chiqazish mumkin.

Va aksincha, R halqada qisqartirish qoidalaridan biri aytaylik, chap qisqartirish qoidasi o'rinli bo'lsin. Teskarisini faraz qilaylik, ya'ni R halqa nolning bo'luvchisiga ega bo'lsin. Aytaylik, $a \in R$ element nolning bo'luvchisi bo'lsin, ya'ni $b \neq 0$ element topilib $ab = 0$. U holda $ab = a0$ ekanligidan va chap qisqartirish qoidasi o'rinliligidan $b = 0$ kelib chiqadi. Bu esa, a nolning bo'luvchisi ekanligiga zid. Demak, R nolning bo'luvchisiga ega emas. □

5.1.6-ta'rif. *Elementlari soni cheklita bo'lgan halqa* ***chekli halqa****, aks holda* ***cheksiz halqa*** *deyiladi.*

Chegirmalar halqasi $(\mathbb{Z}_n, +_n, \cdot_n)$ chekli halqa bo'lsa, $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)(\mathbb{R}, +, \cdot)$ va $(M_n(\mathbb{R}), +, \cdot)$ halqalar cheksiz halqalar bo'ladi. Bundan tashqari, $(\mathbb{Z}_n, +_n, \cdot_n)$ halqa n murakkab son bo'lgan holda nolning bo'luvchisiga ega bo'lgan halqa bo'ladi. Masalan, $(\mathbb{Z}_6, +_6, \cdot_6)$ halqada $\overline{2} \cdot \overline{3} = \overline{0}$, ya'ni $\overline{2}$ va $\overline{3}$ nolning bo'luvchilari.

Quyidagi teoremada nolning bo'luvchisiga ega bo'lmagan chekli kommutativ halqa maydon bo'lishini ko'rsatamiz.

5.1.4-teorema. *Elementlari soni kamida ikkita bo'lgan, nolning bo'luvchisiga ega bo'lmagan chekli kommutativ halqa maydon bo'ladi.*

Isbot. Aytaylik, R nolning bo'luvchisiga ega bo'lmagan kommutativ halqa bo'lib, elementlari soni n ta bo'lsin, u holda $R = \{a_1, a_2, \ldots, a_n\}$. Biz ushbu halqaning maydon bo'lishini ko'rsatishimiz uchun, uning birlik elementga ega ekanligini va ixtiyoriy noldan farqli elementi teskarilanuvchiligini ko'rsatishimiz kerak. Ixtiyoriy $a \in R$ element uchun

$$aa_1, aa_2, \ldots, aa_n$$

elementlarni qaraymiz. Ma'lumki, ushbu elementlar turli xil bo'ladi, chunki agar $aa_i = aa_j$ bo'lsa, u holda 5.1.3-teoremaga ko'ra ushbu halqada qisqartirish qoidasi o'rinli bo'lib, bundan $a_i = a_j$ ekanligi kelib chiqadi. Demak, $R = \{aa_1, aa_2, \ldots, aa_n\}$. U holda bu elementlar ichida a ga teng bo'lgani mavjud, ya'ni qandaydir k uchun $aa_k = a$. R halqaning kommutativligini hisobga olsak $a_k a = aa_k = a$ kelib chiqadi. Endi ushbu a_k elementning birlik element ekanligini ko'rsatamiz. Ixtiyoriy $b \in R$ element olsak, bu elementni $b = aa_j$ ko'rinishida yozish mumkin. U holda

$$ba_k = a_k b = a_k(aa_j) = (a_k a)a_j = aa_j = b$$

ekanligidan a_k elementning birlik elementligi kelib chiqadi.

Endi ixtiyoriy a elementning teskarilanuvchi ekanligini ko'rsatamiz. Ushbu a_k birlik element ham R da yotganligi uchun $a_k \in \{aa_1, aa_2, \ldots, aa_n\}$. Bu esa qandaydir s uchun $aa_s = a_k$ ekanligini bildiradi. R halqa kommutativ bo'lganligi uchun $a_s a = aa_s = a_k$. Demak, a element teskarilanuvchi. Bundan esa, R halqaning barcha elementlari teskarilanuvchi ekenligi kelib chiqadi. Shunday qilib biz R halqaning maydon ekanligini ko'rsatdik. $\square$

Yuqoridagi teoremadan ushbu natijalarni olishimiz mumkin.

5.1.1-natija. *Ixtiyoriy chekli butunlik sohasi maydon bo'ladi.*

5.1.2-natija. $\mathbb{Z}_n$ *halqa maydon bo'lishi uchun* n *tub son bo'lishi zarur va yetarli.*

5.1.1 Nilpotent va idempotent elementlar

R halqaning ixtiyoriy $a \in R$ elementi va n butun son uchun na elementni quyidagicha aniqlaymiz:

$$0a = 0, \quad na = \underbrace{a + a + \cdots + a}_{n\ ta}, \ n > 0, \quad na = (-n)(-a), \ n < 0.$$

Halqaning ixtiyoriy $a, b \in R$ elementlari va ixtiyoriy m, n butun sonlar uchun quyidagi xossalar o'rinli ekanligi osongina kelib chiqadi:

$$(m + n)a = ma + na, \quad m(a + b) = ma + mb,$$

$$(mn)a = m(na), \quad m(ab) = (ma)b = a(mb), \quad (ma)(nb) = mn(ab).$$

5.1.7-ta'rif. *Agar shunday n natural soni mavjud bo'lib, ixtiyoriy a element uchun $na = 0$ tenglik o'rinli bo'lsa, u holda bu shartni qanoatlantiruvchi eng kichik natural songa, halqaning **harakteristikasi** deb ataladi. Agar bunday natural son mavjud bo'lmasa, u holda halqaning harakteristikasi nolga teng deyiladi.*

Masalan, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ halqalar harakteristikasi nolga teng bo'lgan halqalar bo'lsa, $\mathbb{Z}_n$ halqa esa, harakteristikasi n ga teng bo'lgan halqadir. Quyidagi misolda harakteristikasi 2 ga teng bo'lgan halqaga misol keltiramiz.

5.1.10-misol. *Ixtiyoriy bo'sh bo'lmagan X to'plamning qism to'plamlaridan tuzilgan $P(X)$ to'plamlar oilasini qaraymiz. Ma'lumki, $P(X)$ to'plam simmetrik ayirma amaliga nisbatan kommutativ gruppa tashkil qiladi. Agar $(P(X), \triangle, \cap)$ uchlikni qarasak, u holda bu uchlik halqa tashkil qiladi, ya'ni $P(X)$ to'plam simmetrik ayirma va kesishma amallariga nisbatan halqa tashkil qiladi. Bu halqa kommutativ, birlik elementga ega halqa bo'lib, birlik element vazifasini bo'sh to'plam bajaradi, ya'ni $e = \emptyset$. Ushbu halqaning harakteristikasi 2 ga teng, chunki*

$$2A = A \triangle A = (A \setminus A) \cup (A \setminus A) = \emptyset.$$

Quyidagi teoremada butunlik sohasining harakteristikasi qanday songa teng bo'lishi mumkinligi haqida ma'lumot beramiz.

5.1.5-teorema. *Butunlik sohasining harakteristikasi faqat nolga yoki tub songa teng bo'ladi.*

Isbot. Faraz qilaylik R butunlik sohasi chekli harakteristikaga ega bo'lib, u murakkab n soniga teng bo'lsin. U holda $n = n_1 n_2, 1 < n_1, n_2 < n$, hamda ixtiyoriy $a \in R$ uchun $na = 0$, hususan $n1 = 0$. U holda $0 = n1 = (n_1 n_2)1 = (n_1 1)(n_2 1)$ bo'ladi. R nolning bo'luvchisiga ega bo'lmaganligi uchun $n_1 1 = 0$ yoki $n_2 1 = 0$. Agar $n_1 1 = 0$ bo'lsa, u holda ixtiyoriy $a \in R$ uchun $n_1 a = n_1(1a) = (n_1 1)a = 0$. Bu esa, halqaning harakteristikasi n ekanligiga, ya'ni n ning minimalligiga zid. Xuddi shunday, $n_2 1 = 0$ ekanligidan ham ziddiyat kelib chiqadi. Demak, n tub son. $\square$

Endi halqaning nilpotent va idempotent elementlari tushunchalarini kiritamiz.

5.1.8-ta'rif. *Agar halqaning $a \in R$ elementi uchun $a^2 = a$ shart bajarilsa, u holda bu element **idempotent** element deb ataladi. Agar qandaydir n natural son uchun $a^n = 0$ bo'lsa, u holda bu element **nilpotent** element deb ataladi.*

Halqaning nilpotent va idempotent elementlari uchun quyidagi sodda xossalar o'rinli.

1. Agar $a \in R$ element idempotent bo'lsa, u holda u nilpotent emas.

2. Agar $a \in R$ element nilpotent bo'lsa, u holda u teskarilanuvchi emas.

3. Agar $a \in R$ element nilpotent bo'lsa, u holda u nolning bo'luvchisi bo'ladi.

4. Agar R kommutativ halqa bo'lib, a va b elementlar nilpotent bo'lsa, u holda $a+b$ ham nilpotent bo'ladi.

5. Agar R birlik elementli, nolning bo'luvchilariga ega bo'lmagan halqa bo'lsa, u holda halqaning 0 va 1 dan boshqa idempotent elementlari mavjud emas.

5.1.11-misol. *$\mathbb{Z}_{12}$ halqaning idempotent elementlari $\overline{0}, \overline{1}, \overline{4}$ va $\overline{9}$, nilpotent elementlari esa $\overline{0}$ va $\overline{6}$ lardan iborat bo'ladi.*

5.1.2 Bul va regulyar halqalari

Biz endi ba'zi muhim halqalarni, ya'ni Bul va regulyar halqalarni keltirib o'tamiz.

5.1.9-ta'rif. *Barcha elementlari idempotent bo'lgan biri bor halqa **Bul halqasi** deyiladi.*

Bul halqasiga eng sodda misol $(\mathbb{Z}_2, +_2, \cdot_2)$ halqa bo'lsa, yana bir Bul halqasiga misol sifatida $(P(X), \triangle, \cap)$ halqani keltirishimiz mumkin.

Bul halqalari uchun quyidagi teorema o'rinli.

5.1.6-teorema. *Ixtiyoriy Bul halqasi kommutativ bo'lib, uning harakteristikasi 2 ga teng.*

Isbot. Aytaylik, R Bul halqasi bo'lsin. Dastlab uning harakteristikasi 2 ga teng ekanligini ko'rsatamiz. Ixtiyoriy $x \in R$ uchun $x^2 = x$, hususan, $x+x$ element uchun ham $(x+x)^2 = x+x$. Bu tenglikdan $x^2+x^2+x^2+x^2 = 2x$, bundan esa, $4x = 2x$, ya'ni $2x = 0$ kelib chiqadi. Demak, halqaning harakteristikasi 2 ga teng.

Endi R halqaning kommutativligini ko'rsatamiz. Buning uchun $(x+y)^2 = x+y$ tenglikni chap tomonini ochib chiqsak, $x+xy+yx+y = x+y$, ya'ni $xy+yx = 0$ kelib chiqadi. Bu tenglikning ikkala tomoniga xy ni qo'shib, halqaning harakteristikasi 2 ga teng ekanligidan foydalansak,

$$xy = 2xy + yx = yx.$$

Demak R kommutativ halqa.

□

5.1.10-ta'rif. *Agar $x \in R$ element uchun $x = xyx$ tenglikni qanoatlantiradigan $y \in R$ element mavjud bo'lsa, u holda x element **regulyar** element deyiladi. Barcha elementlari regulyar bo'lgan halqa **regulyar** halqa deyiladi.*

5.1.12-misol. *1) $\mathbb{Z}$ halqaning regulyar elementlari 0, 1, -1 lardan iborat bo'ladi.*
2) Ixtiyoriy Bul halqasi regulyar halqa bo'ladi.
3) Haqiqiy sonlar halqasi $\mathbb{R}$ regulyar halqa, lekin Bul halqasi emas.

Regulyar halqalar uchun quyidagi teorema o‘rinli.

5.1.7-teorema. *Aytaylik, R regulyar halqa bo‘lib, ixtiyoriy $x \neq 0$ element uchun $x = xyx$ tenglikni qanoatlantiruvchi $y \in R$ element yagona bo‘lsin. U holda*

1) R halqa nolning bo‘luvchisiga ega emas.

2) $x \neq 0$ element uchun $x = xyx$ ekanligidan $y = yxy$ bo‘lishi kelib chiqadi.

3) R halqa jism bo‘ladi.

Isbot. 1) Aytaylik, x, z noldan farqli elementlar uchun $xz = 0$ bo‘lsin. Teorema shartiga ko‘ra $x = xyx$ tenglikni qanoatlantiruvchi yagona $y \in R$ element mavjud. U holda

$$x(y - z)x = xyx - xzx = xyx$$

ekanligidan $y - z = y$ tenglikni, ya’ni $z = 0$ ekanligini hosil qilamiz. Demak, R halqa nolning bo‘luvchisiga ega emas.

2) Noldan farqli x element uchun $x = xyx$ ekanligidan biz quyidagi tenglikka ega bo‘lamiz

$$x(y - yxy) = xy - x(yxy) = xy - (xyx)y = xy - xy = 0.$$

R halqa nolning bo‘luvchisiga ega bo‘lmaganligi uchun $y - yxy = 0$, ya’ni $y = yxy$.

3) Dastlab, teorema shartini qanoatlantiruvchi halqa biri bor halqa ekanligini ko‘rsatamiz. Ixtiyoriy $x \neq 0$ element uchun $x = xyx$ tenglikni qanoatlantiruvchi yagona $y \in R$ element mavjud. Biz $e = xy$ elementni birlik element bo‘lishini ko‘rsatamiz. Ushbu element noldan farqli bo‘lib

$$e^2 = (xy)(xy) = (xyx)y = xy = e.$$

R halqa nolning bo‘luvchisiga ega emasligini hisobga olsak, ixtiyoriy $z \in R$ element uchun

$$(ze - z)e = ze^2 - ze = ze - ze = 0$$
$$e(ez - z) = e^2z - ez = ez - ez = 0$$

tengliklardan $ze - z = 0$ va $ez - z = 0$ ekanligini, ya’ni $ze = ez = z$ munosabatni hosil qilamiz. Demak, $e = xy$ element birlik element bo‘ladi.

Endi R halqaning ixtiyoriy noldan farqli elementining teskarilanuvchi ekanligini ko‘rsatamiz. Aytaylik, $x \neq 0$ bo‘lib, $x = xyx$ bo‘lsin. U holda $xyx = xe$ va $xyx = ex$, ya’ni $x(yx - e) = 0$ va $(xy - e)x = 0$. Bu tengliklardan esa, $yx - e = 0$ va $xy - e = 0$ ekanligi kelib chiqadi, chunki R halqa nolning bo‘luvchisiga ega emas. Demak, $xy = yx = e$, ya’ni x element teskarilanuvchi. Bundan esa, R halqaning jism ekanligini kelib chiqadi.

$\square$

5.1.13-misol. *R halqa noldan farqli nilpotent elementga ega bo'lmasligi uchun $a^2 = 0$ ekanligidan $a = 0$ tenglik kelib chiqishi zarur va yetarli ekanligini isbotlang.*

Yechish. Aytaylik, R halqa noldan farqli nilpotent elementga ega bo'lmasin. U holda $a^2 = 0$ ekanligidan $a = 0$ tenglik kelib chiqishi ravshan.

Endi misolning ikkinchi tomonini ya'ni $a^2 = 0$ ekanligidan $a = 0$ tenglik kelib chiqsa, R halqa noldan farqli nilpotent elementga ega bo'lmasligini ko'rsatamiz. Teskarisini faraz qilaylik, R halqaning noldan farqli $b \in R$ nilpotent elementi mavjud bo'lsin, ya'ni $b^n = 0$. Ushbu n natural sonini $b^n = 0$ tenglikni qanoatlantiruvchi eng kichik natural son deb faraz qilish mumkin.

Agar n soni juft bo'lsa, u holda $n = 2m$ bo'lib, $(b^m)^2 = b^{2m} = b^n = 0$. Bundan esa $b^m = 0$ ekanligini hosil qilamiz. Bu esa n sonining eng kichik ekanligiga zid.

Agar n soni toq son, ya'ni $n = 2m + 1$ bo'lsa, u holda $(b^{m+1})^2 = b^{2m+2} = b^{2m+1}b = 0$ bo'lib, bu tenglikdan $b^{m+1} = 0$ ekanligini hosil qilamiz. Bu ham n sonining eng kichik ekanligiga zid, chunki, $n > 1$ bo'lib $m + 1 < n$. Demak, R halqa noldan farqli nilpotent elementga ega emas. $\square$

5.1.14-misol. *Aytaylik, R halqa birlik elementli kommutativ halqa bo'lsin. Agar $a \in R$ element teskarilanuvchi va $b \in R$ element nilpotent bo'lsa, u holda $a + b$ elementning teskarilanuvchi ekanligini ko'rsating.*

Yechish. $a \in R$ element teskarilanuvchi bo'lganligi uchun, shunday $c \in R$ element topilib, $ac = ca = 1$ bo'ladi. Ikkinchi tomondan esa $b \in R$ element nilpotent bo'lganligi uchun qandaydir n natural soni uchun $b^n = 0$. Endi $d = c - c^2b + c^3b^2 + \cdots + (-1)^{n-1}c^nb^{n-1}$ elementni $a+b$ elementning teskarisi ekanligini ko'rsatamiz. Haqiqatdan ham

$$(a + b)d = (a + b)(c - c^2b + c^3b^2 + \cdots + (-1)^{n-1}c^nb^{n-1}) =$$

$$= ac - ac^2b + ac^3b^2 + \cdots + (-1)^{n-1}ac^nb^{n-1} + bc - bc^2b + bc^3b^2 + \cdots + (-1)^{n-1}bc^nb^{n-1} =$$

$$= 1 - cb + c^2b^2 + \cdots + (-1)^{n-1}c^{n-1}b^{n-1} + cb - c^2b^2 + c^3b^3 + \cdots + (-1)^{n-2}c^{n-1}b^{n-1} = 1.$$

Xuddi shunga o'xshab, $d(a+b) = 1$ ekanligini ham ko'rsatish mumkin. Demak, $a + b$ element teskarilanuvchi. $\square$

Yuqoridagi misolda R halqaning kommutativ bo'lishi muhim ahamiyatga ega. Chunki, kommutativ bo'lmagan halqada teskarilanuvchi va nilpotent elementning yig'indisi har doim ham teskarilanuvchi bo'lavermaydi. Masalan, $M_2(\mathbb{R})$ halqada teskarilanuvchi $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ element va nilpotent $B = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$ elementlarning yig'indisi $A + B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ teskarilanuvchi emas.

Quyidagi misolda $M_2(\mathbb{R})$ halqaning regulyar halqa ekanligini isbotlaymiz.

5.1.15-misol. *$M_2(\mathbb{R})$ halqa regulyar halqa ekanligini ko'rsating.*

Yechish. Misolni yechish uchun ixtiyoriy $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ elementning regulyar ekanligini ko'rsatamiz. Quyidagi hollarni qaraymiz.

1. $det(A) \neq 0$ bo'lsin, u holda A matritsa teskarilanuvchi bo'lib, $B = A^{-1}$ element uchun $A = ABA$ bo'ladi.

2. $det(A) = 0$ bo'lsin. Agar $A = 0$, ya'ni $a = b = c = d = 0$ bo'lsa, u holda ixtiyoriy $B \in M_2(\mathbb{R})$ matritsa uchun $A = ABA$ bo'ladi. Agar $A \neq 0$ va $a \neq 0$ bo'lsa, u holda $d = \frac{bc}{a}$ bo'lib, $B = \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{pmatrix}$ matritsa uchun

$$ABA = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

   Demak, A matritsa regulyar element bo'ladi.

   Xuddi shunga o'xshab, $b \neq 0$, $c \neq 0$ va $d \neq 0$ bo'lgan hollarda ham A matritsaning regulyar element ekanligini ko'rsatish mumkin. Ya'ni, $M_2(\mathbb{R})$ regulyar halqa.

□

5.1.3 Mustaqil ishlash uchun misol va masalalar

1. Quyidagi sonlar to'plamining qaysilari qo'shish va ko'paytirish amallariga nisbatan halqa tashkil qilishini aniqlang.

   - $n\mathbb{Z}$, ya'ni natural n soniga karrali bo'lgan butun sonlar to'plami.
   - maxraji fiksirlangan tub sonning darajalaridan iborat bo'lgan ratsional sonlar to'plami.
   - $x + \sqrt{2}y$ ko'rinishidagi haqiqiy sonlar to'plami, bu yerda $x, y \in \mathbb{Q}$.
   - $x + \sqrt[3]{2}y$ ko'rinishidagi haqiqiy sonlar to'plami, bu yerda $x, y \in \mathbb{Q}$.
   - $x+\sqrt[3]{2}y+\sqrt[3]{4}z$ ko'rinishidagi haqiqiy sonlar to'plami, bu yerda $x, y, z \in \mathbb{Q}$.

2. Quyidagi to'plamlarni halqa tashkil qilishini aniqlang, bu yerda $i^2 = -1$.

   - $\mathbb{Z}[\sqrt{n}] = \{x + y\sqrt{n} \mid x, y \in \mathbb{Z}\}$.
   - $\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$.
   - $\mathbb{Q}[i] = \{x + iy \mid x, y \in \mathbb{Q}\}$.
   - $\mathbb{Z}[i\sqrt{n}] = \{x + iy\sqrt{n} \mid x, y \in \mathbb{Z}\}$.

- $\mathbb{Q}[i\sqrt{n}] = \{x + iy\sqrt{n} \mid x, y \in \mathbb{Q}\}$.

3. Quyidagi matritsalar to‘plamining qaysilari matritsalarni qo‘shish va ko‘paytirish amallariga nisbatan halqa tashkil qilishini aniqlang:
   - elementlari haqiqiy sonlardan iborat bo‘lgan simmetrik matritsalar to‘plami;
   - elementlari haqiqiy sonlardan iborat bo‘lgan kososimmetrik matritsalar to‘plami;
   - elementlari haqiqiy sonlardan iborat bo‘lgan yuqori uchburchak ko‘rinishidagi matritsalar to‘plami;
   - $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ ko‘rinishidagi matritsalar to‘plami bu yerda $a, b \in \mathbb{Z}$;
   - $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ ko‘rinishidagi matritsalar to‘plami bu yerda $z, w \in \mathbb{C}$.
4. Bir o‘zgaruvchili ko‘phadlar to‘plami $P(x)$ ko‘phadlarni qo‘shish va ko‘paytirish amallariga nisbatan halqa tashkil qilishini ko‘rsating.
5. Bir o‘zgaruvchili ko‘phadlar to‘plami $P(x)$ ko‘phadlarni qo‘shish va superpozitsiya amallariga nisbatan halqa tashkil qiladimi?
6. Quyidagi halqalarning barcha teskarilanuvchi elementlarini toping:
$$\mathbb{Z}_6, \quad \mathbb{Z}_8, \quad \mathbb{Z}_{12}, \quad \mathbb{Z}_{15}, \quad \mathbb{Z}_{18}, \quad \mathbb{Z}_{24}, \quad \mathbb{Z}_{30}.$$
7. Quyidagi halqalarda nolning bo‘luvchilarini toping:
$$\mathbb{Z}_5, \quad \mathbb{Z}_8, \quad \mathbb{Z}_{12}, \quad \mathbb{Z}_{15}, \quad \mathbb{Z}_{22}, \quad \mathbb{Z}_{24}, \quad \mathbb{Z}_{30}.$$
8. Quyidagi halqalarning barcha nilpotent elementlarini toping:
$$\mathbb{Z}_6, \quad \mathbb{Z}_8, \quad \mathbb{Z}_{12}, \quad \mathbb{Z}_{15}, \quad \mathbb{Z}_{16}, \quad \mathbb{Z}_{24}, \quad \mathbb{Z}_{36}.$$
9. Quyidagi halqalarning barcha idempotent elementlarini toping:
$$\mathbb{Z}_5, \quad \mathbb{Z}_6, \quad \mathbb{Z}_8, \quad \mathbb{Z}_{10}, \quad \mathbb{Z}_{12}, \quad \mathbb{Z}_{14}. \quad \mathbb{Z}_{27}.$$
10. $\mathbb{Z}_n$ halqa noldan farqli nilpotent elementga ega bo‘lmasligi uchun n sonining kanonik yoyilmasi $n = p_1 p_2 \dots p_k (p_i \neq p_j)$ kabi bo‘lishi zarur va yetarli ekanligini isbotlang.
11. $\mathbb{Z}_n$ halqa nol va birdan farqli idempotent elementga ega bo‘lmasligi uchun $n = p^r$ bo‘lishi zarur va yetarli ekanligini isbotlang.

12. Agar $\mathbb{Z}_n$ halqada $n = m \cdot k$ bo‘lib, $(m, k) = 1$ bo‘lsa, u holda $\mathbb{Z}_n$ halqa nol va birdan farqli kamida ikkita idempotent elementga ega ekanligini isbotlang.

13. Quyidagi halqalarning barcha idempotent elementlarini toping:

$$\mathbb{Z}_{15}, \quad \mathbb{Z}_{30}, \quad \mathbb{Z}_{42}, \quad \mathbb{Z}_{60}, \quad \mathbb{Z}_{72}, \quad \mathbb{Z}_{84}. \quad \mathbb{Z}_{90}.$$

14. Quyidagi halqalarning barcha nilpotent elementlarini toping:

$$\mathbb{Z}_{40}, \quad \mathbb{Z}_{44}, \quad \mathbb{Z}_{60}, \quad \mathbb{Z}_{72}, \quad \mathbb{Z}_{180}, \quad \mathbb{Z}_{252}, \quad \mathbb{Z}_{300}.$$

15. $M_2(\mathbb{R})$ halqaning barcha teskarilanuvchi, idempotent va nilpotent elementlarini toping.

16. $\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$ halqaning barcha teskarilanuvchi, idempotent va nilpotent elementlarini toping.

17. R halqa kommutativ bo‘lishi uchun $(a + b)^2 = a^2 + 2ab + b^2$ bo‘lishi zarur va yetarli ekanligini isbotlang.

18. R halqa kommutativ bo‘lishi uchun $a^2 - b^2 = (a - b)(a + b)$ bo‘lishi zarur va yetarli ekanligini isbotlang.

19. R halqaning ixtiyoriy $a \in R$ elementi uchun $a^3 = a$ tenglik o‘rinli bo‘lsa, u holda R halqaning kommutativ ekanligini isbotlang.

20. Biri bor R halqaning $a \in R$ nilpotent elementi uchun $1 - a$ va $1 + a$ elementlarning teskarilanuvchu ekanligini isbotlang.

21. Agar $a \in R$ element halqaning idempotent elementi bo‘lsa, u holda ixtiyoriy $b \in R$ uchun $(1 - a)ba$ elementning nilpotent ekanligini ko‘rsating.

22. Agar biri bor R halqaning $x, y \in R$ elementlari uchun xy va yx ko‘paytmalar teskarilanuvchi bo‘lsa, u holda x va y elementlar ham teskarilanuvchi bo‘lishini ko‘rsating.

23. Agar biri bor, nolning bo‘luvchilariga ega bo‘lmagan R halqaning $x, y \in R$ elementlari uchun xy ko‘paytma teskarilanuvchi bo‘lsa, u holda x va y elementlar ham teskarilanuvchi bo‘lishini ko‘rsating.

24. Biri bor halqa Bul halqasi bo‘lishi uchun ixtiyoriy a, b elementlar uchun $(a + b)ab = 0$ bo‘lishi zarur va yetarli ekanligini isbotlang.

5.2 Qism halqa va ideallar

Ushbu mavzuda gruppalar nazariyasidan ma'lum bolgan qism gruppa va normal bo'luvchi tushunchalarining halqalar nazariyasidagi analogi hisoblangan qism halqalar va ideallar tushunchalari haqida gaplashamiz.

5.2.1-ta'rif. *Bizga* $(R, +, \cdot)$ *halqa va uning* R' *qism to'plami berilgan bo'lsin. Agar* R' *to'plam, R da aniqlangan amallarga nisbatan halqa tashkil qilsa, u holda* $(R', +, \cdot)$ *halqaga* $(R, +, \cdot)$ *halqaning qism halqasi deb ataladi. Boshqacha aytganda, agar* R' *to'plam* $(R, +)$ *gruppaning qism gruppasi bo'lib,* $\forall x, y \in R'$ *uchun* $x \cdot y \in R'$ *shart bajarilsa, u holda* $(R', +, \cdot)$ *qism halqa deyiladi.*

Berilgan maydonning qism maydoni tushunchasi ham, qism halqa ta'rifi kabi aniqlanadi, ya'ni agar $(F, +, \cdot)$ maydonning F' qism to'plami ham F da aniqlangan amallarga nisbatan maydon tashkil qilsa, u holda $(F', +, \cdot)$ qism maydon deyiladi.

Ushbu teorema halqaning berilgan qism to'plamini qism halqa bo'lishining zaruriy va yetarlilik shartini ifodalaydi.

5.2.1-teorema. $(R, +, \cdot)$ *halqaning* R' *qism to'plami qism halqa bo'lishi uchun quyidagi shartlarning bajarilishi zarur va yetarli:*

$$\forall x, y \in R, \ uchun \quad x - y \in R \quad va \quad x \cdot y \in R.$$

Isbot. Agar $(R', +, \cdot)$ qism halqa bo'lsa, u holda $\forall x, y \in R'$ uchun $x - y \in R$ va $x \cdot y \in R$ bo'lishi ravshan. Va aksincha agar, $\forall x, y \in R'$ uchun $x - y \in R$ bo'lsa, u holda 1.3.1-teoremaga ko'ra R' to'plam $(R, +)$ gruppaning qism gruppasi bo'ladi. $\forall x, y \in R'$ uchun $x \cdot y \in R$ ekanligidan esa, $(R', +, \cdot)$ qism halqa bo'lishi kelib chiqadi.

□

5.2.1-misol. *1)* $n\mathbb{Z}$ *to'plam* $(\mathbb{Z}, +, \cdot)$ *halqaning qism halqasi bo'ladi.*
2) $\mathbb{E}_8 = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \}$ *to'plam* $(\mathbb{Z}_8, +_8, \cdot_8)$ *halqaning qism halqasi bo'ladi.*
3) $(\mathbb{Z}, +, \cdot)$ *halqa* $(\mathbb{Q}, +, \cdot)$ *halqaningning qism halqasi bo'ladi.*
4) $(\mathbb{Q}, +, \cdot)$ *maydon* $(\mathbb{R}, +, \cdot)$ *maydonning qism maydoni bo'ladi.*
5) $(\mathbb{R}, +, \cdot)$ *maydon* $(\mathbb{C}, +, \cdot)$ *maydonning qism maydoni bo'ladi.*

Biz 5.2.2-teoremada halqaning biror qism to'plami qism halqa bo'lishi zaruriy va yetarlilik shartini keltirdik. Xuddi shunga o'xshab F maydonning bo'sh bo'lmagan S qism to'plami qism maydon bo'lishi uchun quyidagi shartlarning bajarishi zarur va yetarli:

1) $|S| \geq 2$;

2) $\forall x, y \in S$ elementlar uchun $x - y \in S$ va $x \cdot y \in S$;

3) $\forall x \in S$ uchun $x^{-1} \in S$.

5.2.2-misol. *$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ to'plam $\mathbb{R}$ maydonning qism maydoni bo'ladi. Haqiqatdan ham, bu to'plamning elementlari soni ikkitadan ko'p va $\forall a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ uchun*

$$a + b\sqrt{2} - (c + d\sqrt{2}) = a - c + (b - d)\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Bundan tashqari noldan farqli $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ element uchun

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

Quyidagi teoremada qism halqalarning kesishmasi yana qism halqa bo'lishini ko'rsatamiz.

5.2.2-teorema. *Ixtiyoriy sondagi qism halqalarning (maydonlarning) kesishmasi yana qism halqa (qism maydon) bo'ladi.*

Isbot. Bizga R halqaning R_i qism halqalari berilan bo'lsin. $\bigcap\limits_i R_i$ to'plamning ham qism halqa ekanligini ko'rsatamiz. Nol element ixtiyoriy qism halqaga tegishli bo'lganligi uchun qism halqalarning kesishmasida ham yotadi, demak $\bigcap\limits_i R_i \neq \emptyset$. Aytaylik, $x, y \in \bigcap\limits_i R_i$ bo'lsin, u holda ixtiyoriy i uchun $x, y \in R_i$ bo'lib, R_i to'plamlarning qism halqa ekanligidan, $x - y, x \cdot y \in R_i$ munosabat ixtiyoriy i uchun bajarilishi kelib chiqadi. Bundan esa, $x - y, x \cdot y \in \bigcap\limits_i R_i$ hosil bo'ladi. Demak, $\bigcap\limits_i R_i$ qism halqa. □

Endi ideal tushunchasini kiritamiz. Yuqorida ta'kidlab o'tganimizdek halqaning ideali tushunchasi gruppaning normal bo'luvchisinining analogi hisoblanadi. Bizga R halqa va uning bo'sh bo'lmagan I qism to'plami berilgan bo'lsin. Quyidagi shartlarni qaraymiz:

(1) I to'plam $(R, +)$ gruppaning qism gruppasi, ya'ni $\forall a, b \in I$ uchun $a - b \in I$;

(2) Ixtiyoriy $\forall a \in I$ va $r \in R$ elementlar uchun $r \cdot a \in I$;

(3) Ixtiyoriy $\forall a \in I$ va $r \in R$ elementlar uchun $a \cdot r \in I$.

5.2.2-ta'rif. *Agar R halqaning bo'sh bo'lmagan I qism to'plami uchun (1) va (2) shartlar o'rinli bo'lsa, u holda I to'plam R halqaning* ***chap ideali*** *deb ataladi.*

Agar (1) va (3) shartlar o‘rinli bo‘lsa, u holda I to‘plam R halqaning ***o‘ng ideali*** *deb ataladi.*

Agar (1), (2) va (3) shartlar o‘rinli bo‘lsa, u holda I to‘plam R halqaning ***ikki tomonli ideali*** *deb ataladi.*

Ikki tomonli ideallar qisqacha ideal deb ham nomlanadi. Ta’kidlash joizki, ixtiyoriy R halqada $\{0\}$ va R to‘plamlar ideal bo‘lib, ular R halqaning trivial ideallari deyiladi. Trivial bo‘lmagan ideallarga notrivial ideallar deyiladi.

5.2.3-ta’rif. *Agar R halqaning notrivial ideallari mavjud bo‘lmasa, u holda bunday halqaga* ***sodda*** *halqa deb ataladi.*

Quyida butun sonlar va matritsalar halqalarining ba’zi ideallariga misollar keltiramiz.

5.2.3-misol. *1) $n\mathbb{Z}$ to‘plam $(\mathbb{Z}, +, \cdot)$ halqaning ideali bo‘ladi.*
2) $(M_2(\mathbb{R}), +, \cdot)$ halqaning quyidagi qism to‘plamlarini qaraylik.

$$I_1 = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\},$$

$$I_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\},$$

$$I_3 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}.$$

I_1 to‘plam $M_2(\mathbb{R})$ halqaning chap ideali, I_2 to‘plam esa o‘ng ideali bo‘ladi. I_3 to‘plam $M_2(\mathbb{R})$ halqaning qism halqasi bo‘lib, ideal tashkil qilmaydi.

Endi halqaning markazi tushunchasini kiritamiz. R halqaning **markazi** deb quyidagi to‘plamga aytiladi.

$$C(R) = \{a \in R \mid ax = xa, \ \forall x \in R\}.$$

Ta’kidlash joizki, ixtiyoriy halqaning markazi qism halqa bo‘ladi, chunki $\forall a, b \in C(R)$ elementlar uchun $ax = xa$ va $bx = xb$ bo‘lib, bundan esa

$$(a - b)x = ax - bx = xa - xb = x(a - b),$$

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$$

kelib chiqadi, ya’ni $a - b, ab \in C(R)$. Demak, $C(R)$ qism halqa. Lekin halqaning markazi ideal bo‘lishi shart emas. Masalan, $M_2(\mathbb{R})$ matritsalar halqasining markazi $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ ko‘rinishidagi matritsalardan iborat bo‘lib, ideal tashkil qilmaydi.

Aytaylik, R kommutativ halqa va I uning ideali bo‘lsin. Quyidagi to‘plamni aniqlaymiz

$$AnnI = \{r \in R \mid r \cdot a = 0, \quad \forall a \in I\}.$$

Ushbu to‘plam R halqaning I ideali bo‘yicha annulyatori deb ataladi. Ko‘rsatish qiyin emaski, halqaning biror ideal bo‘yicha annulyatori ideal tashkil qiladi. Haqiqatdan ham, agar $r_1, r_2 \in AnnI$ bo‘lsa, u holda $\forall a \in I$ uchun $r_1 a = r_2 a = 0$. Quyidagi

$$(r_1 - r_2) \cdot a = r_1 \cdot a - r_2 \cdot a = 0,$$

$$(x \cdot r) \cdot a = x \cdot (r \cdot a) = 0$$

tengliklardan $r_1 - r_2 \in AnnI$ va $\forall x \in R$ uchun $x \cdot r \in AnnI$ ekanligi kelib chiqadi.

Biz 5.2.2-teoremada qism halqalarning kesishmasi yana qism halqa ekanligini ko‘rsatgan edik. Xuddi shunga o‘xshab ideallarning ham kesishmasi yana ideal bo‘lishini ko‘rsatish qiyin emas. Ya’ni quyidagi teorema o‘rinli.

5.2.3-teorema. *Ixtiyoriy sondagi bo‘sh bo‘lmagan chap (o‘ng) ideallarning kesishmasi yana chap (o‘ng) ideal bo‘ladi.*

Endi R halqaning X qism to‘plami orqali hosil qilingan ideal tushunchasini kiritamiz. Berilgan X to‘plamni o‘z ichiga oluvchi ideallarning kesishmasiga X to‘plam orqali hosil qilingan ideal deyiladi va $\langle X \rangle$ kabi belgilanadi. Ma’lumki, ushbu $\langle X \rangle$ ideal X to‘plamni o‘z ichiga oluvchi eng kichik ideal bo‘ladi. X to‘plamni o‘z ichiga oluvchi chap va o‘ng ideallarning kesishmalari esa mos ravishda $\langle X \rangle_l$ va $\langle X \rangle_r$ orqali belgilanadi. Agar X to‘plam bitta elementdan iborat, ya’ni $X = \{a\}$ bo‘lsa u holda $\langle \{a\} \rangle$ belgilash o‘rniga $\langle a \rangle$ belgilashdan foydalanilib, ushbu idealga **bosh ideal** deb ataladi.

5.2.4-ta’rif. *Barcha ideallari bosh ideal bo‘ladigan halqaga* ***bosh ideallar halqasi*** *deb ataladi.*

Butun sonlar halqasi bosh ideallar halqasi bo‘ladi. Chunki, butun sonlar halqasining barcha ideallari $n\mathbb{Z}$ ko‘rinishida bo‘lib, $n\mathbb{Z} = \langle n \rangle$. Ya’ni, $\mathbb{Z}$ halqaning barcha ideallari bosh ideal bo‘ladi.

5.2.4-teorema. *Aytaylik R halqa va uning bo‘sh bo‘lmagan X qism to‘plami berilgan bo‘lsin. U holda ushbu to‘plam orqali hosil qilingan chap va o‘ng ideallar uchun quyidagilar o‘rinli.*

$$\langle X \rangle_l = \left\{ \sum_{i=1}^{k} r_i a_i + \sum_{j=1}^{l} n_j b_j \mid r_i \in R,\ n_j \in \mathbb{Z},\ a_i, b_j \in X \right\},$$

$$\langle X \rangle_r = \left\{ \sum_{i=1}^{k} a_i r_i + \sum_{j=1}^{l} n_j b_j \mid r_i \in R,\ n_j \in \mathbb{Z},\ a_i, b_j \in X \right\}.$$

Isbot. Aytaylik $A = \left\{ \sum_{i=1}^{k} r_i a_i + \sum_{j=1}^{l} n_j b_j \mid r_i \in R,\ n_j \in \mathbb{Z},\ a_i, b_j \in X \right\}$ bo‘lsin. Biz $A = \langle X \rangle_l$ ekanligini ko‘rsatamiz. $\langle X \rangle_l$ to‘plam barcha chap ideallarning kesishmasi bo‘lganligi uchun $X \subseteq \langle X \rangle_l$ munosabat o‘rinli. Bundan tashqari, $\langle X \rangle_l$ to‘plam yig‘indiga va halqaning biror elementiga chapdan ko‘paytirishga nisbatan yopiq bo‘lganligi uchun A to‘plamning ixtiyoriy elementi $\langle X \rangle_l$ idealda yotishi kelib chiqadi. Demak, $A \subseteq \langle X \rangle_l$.

Endi ushbu munosabatning teskarisi o‘rinli ekanligini ko‘rsatamiz. Buning uchun A to‘plam X to‘plamni o‘z ichiga oluvchi chap ideal bo‘lishini ko‘rsatish kifoya. Ixtiyoriy $x \in X$ uchun $x = 0 \cdot x + 1x$ ekanligidan $x \in A$ kelib chiqadi, ya’ni $X \subseteq A$. Bundan tashqari A to‘plamning ixtiyoriy $a, b \in A$ elementlari va $r \in R$ element uchun $a - b \in A$ va $ra \in A$ ekanligini ko‘rsatish qiyin emas. Demak, A to‘plam X to‘plamni o‘z ichiga oluvchi chap ideal bo‘ladi. Bu esa $\langle X \rangle_l \subseteq A$ ekanligini bildiradi. Demak, $A = \langle X \rangle_l$.

Teoremadagi ikkinchi tenglik ham birinchisi kabi ko‘rsatiladi.

□

Agar R halqa biri bor halqa bo‘lsa, u holda yuqoridagi teoremadagi tengliklar quyidagi ko‘rinishga keladi.

$$\langle X \rangle_l = \left\{ \sum_{i=1}^{k} r_i a_i \mid r_i \in R,\ a_i \in X \right\},$$

$$\langle X \rangle_r = \left\{ \sum_{i=1}^{k} a_i r_i \mid r_i \in R,\ a_i \in X \right\}.$$

Bosh ideallar uchun esa qiyidagi munosabatlarni olamiz.

5.2.1-tasdiq. *Bizga R halqa va uning $a \in R$ elementi berilgan bo‘lsin. U holda quyidagilar o‘rinli.*

- $\langle a \rangle = \{ra + as + na + \sum_{i=1}^{k} r_i a s_i \mid r, s, r_i, s_i \in R,\ n \in \mathbb{Z}\}$.
- $\langle a \rangle_l = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- $\langle a \rangle_r = \{ar + na \mid r \in R,\ n \in \mathbb{Z}\}$.
- *Agar R biri bor halqa bo‘lsa, u holda* $\langle a \rangle = \{\sum_{i=1}^{k} r_i a s_i \mid r_i, s_i \in R,\ n \in \mathbb{Z}\}$.
- *Agar $a \in C(R)$ bo‘lsa, u holda* $\langle a \rangle = \{ra + na \mid r \in R,\ n \in \mathbb{Z}\}$.

Berilgan R halqaning ixtiyoriy $a \in R$ elementi uchun quyidagi to‘plamlarni qaraymiz.

$$Ra = \{ra \mid r \in R\}, \quad aR = \{ra \mid r \in R\}.$$

Ushbu to’plamlar R halqaning mos ravishda chap va o‘ng ideallari bo‘ladi. Ushbu ideallar a elementni o‘z ichida olmasligi ham mumkin. Agar R biri bor halqa bo‘lsa, u holda $a \in Ra$ va $a \in aR$. Bundan tashqari, agar R biri bor halqa bo‘lib, $a \in C(R)$ bo‘lsa, u holda $Ra = aR = \langle a \rangle$ bo‘ladi. Demak, biri bor kommutativ halqalar uchun har doim $Ra = aR = \langle a \rangle$ tenglik o‘rinli bo‘lar ekan.

Biz yuqorida butun sonlar halqasi bosh ideallar halqasi bo‘lishini ko‘rsatgan edik, Quyidagi teoremada esa biror maydon ustida berilgan ko‘phadlar halqasini bosh ideallar halqasi ekanligini ko‘rsatamiz.

5.2.5-teorema. *Biror maydon ustida berilgan ko‘phadlar halqasi bosh ideallar halqasi bo‘ladi.*

Isbot. Aytaylik, $\mathbb{F}$ maydon berilgan bo‘lib $\mathbb{F}[x]$ ko‘phadlar halqasi bo‘lsin. Ma’lumki, $\mathbb{F}[x]$ halqa biri bor kommutativ halqa bo‘ladi. Ushbu halqaning ixtiyoriy J idealini bosh ideal ekanligini ko‘rsatamiz. Aytaylik, $g(x)$ ko‘phad J idealning darajasi eng kichik bo‘lgan elementi bo‘lsin. U holda ixtiyoriy $f(x) \in J$ ko‘phad uchun $f(x) = g(x) \cdot q(x) + r(x)$, $degr(x) < degg(x)$ munosabat o‘rinli. J ideal bo‘lganligi uchun $r(x) = f(x) - g(x) \cdot q(x) \in J$. Tanlangan $g(x)$ ko‘phad J idealning darajasi eng kichik elementi bo‘lganligi uchun $r(x) = 0$ ekanligiga, ya’ni ixtiyoriy $f(x) \in J$ uchun $f(x) = g(x) \cdot q(x)$ tenglikka ega bo‘lamiz. Bu esa $J = \langle g(x) \rangle$ ekanligini bildiradi. $\square$

Ta’kidlash joizki, 5.2.5-teoremada $\mathbb{F}$ ning maydon bo‘lishi muhim. Chunki, halqalar ustida berilgan ko‘phadlar halqasi har doim ham bosh idellar halqasi bo‘lavermaydi. Masalan, $\mathbb{Z}[x]$ ko‘phadlar halqasini qarasak, ushbu halqa bosh ideallar halqasi emas. Chinki uning ozod hadi juft butun sonlardan iborat bo‘lgan qism halqasi ideal bo‘lib, bosh ideal bo‘lmaydi.

Aytaylik, R halqaning A, B bo‘sh bo‘lmagan qism to‘plamlari berilgan bo‘lsin. Quyidagi belgilashlarni kiritamiz:

$$A+B = \{a+b \mid a \in A, b \in B\}, \quad AB = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_i \in A, b_i \in B\}.$$

Agar bir nechta $A_1, A_2, \ldots, A_n$ qism to‘plamlar berilgan bo‘lsa, induktiv tarzda $A_1 + A_2 + \cdots + A_n$ va $(\ldots(A_1A_2)A_3\ldots)A_n$ to‘plamlarni ham aniqlash mumkin.

5.2.6-teorema. *R halqaning A, B, C va $A_1, A_2, \ldots, A_n$ ideallari uchun quyidagilar o‘rinli.*

1) $A + B = B + A, \quad A + A = A.$

2) $(A + B) + C = A + (B + C).$

3) $A_1 + A_2 + \cdots + A_n$ *ham ideal bo'ladi.*

4) $(AB)C = A(BC)$.

5) AB *ham ideal bo'ladi.*

6) $B(A_1 + A_2 + \cdots + A_n) = BA_1 + BA_2 + \cdots + BA_n$.

7) $(A_1 + A_2 + \cdots + A_n)B = A_1B + A_2B + \cdots + A_nB$.

Isbot. Teoremaning isboti idealning ta'rifidan va induksiya metodini qo'llash orqali to'g'ridan-to'g'ri kelib chiqadi. □

Biz endi faktor gruppalar kabi faktor halqa tushunchasini kiritamiz. Aytaylik, R halqaning I ideali berilgan bo'lsin. Ma'lumki, $(I, +)$ additiv gruppa $(R, +)$ gruppaning normal bo'luvchisi bo'ladi. U holda biz R/I faktor gruppani aniqlashimiz mumkin, ya'ni R/I to'plamning $a + I$ va $b + I$ elementlari uchun

$$(a + I) + (b + I) = (a + b) + I.$$

Endi ushbu elementlarning ko'paytmasini $(a + I) \cdot (b + I) = ab + I$ kabi aniqlaymiz. Demak, R/I to'plamda qo'shish va ko'paytirish amallari aniqlandi.

5.2.7-teorema. $(R/I, +, \cdot)$ *to'plam halqa tashkil qiladi.*

Isbot. Dastlab, R/I to'plamda aniqlangan ko'paytirish amalini to'g'ri aniqlanganligini isbotlaymiz. Ya'ni agar $a + I = a' + I$ va $b + I = b' + I$ bo'lsa, u holda $ab + I = a'b' + I$ ekanligini ko'rsatamiz. $a' \in a' + I = a + I$ bo'lganligi uchun, shunday $x \in I$ element topilib, $a' = a + x$ bo'ladi. O'z navbatida, $b' \in b + I$ bo'lganligi uchun qandaydir $y \in I$ element uchun $b' = b + y$. U holda

$$a'b' = (a + x)(b + y) = ab + ay + xb + xb.$$

Bundan esa $a'b' - ab = ay + xb + xb \in I$ ekanligi kelib chiqadi, ya'ni

$$ab + I = a'b' + I.$$

R/I to'plamda ko'paytirish amaliga nisbatan assosiativlikning o'rinli bo'lishi va destributivlik shartining bajarilishi esa ko'paytmaning aniqlanishidan va 5.2.6-teoremadan bevosita kelib chiqadi. □

Yuqorida aniqlangan $(R/I, +, \cdot)$ halqaga R halqaning I ideali bo'yicha **faktor halqasi** deb ataladi. Masalan, $\mathbb{Z}$ butun sonlar halqasining $I = n\mathbb{Z}$ ideali bo'yicha faktor halqasi

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\}$$

sinflardan iborat bo'ladi.

5.2.4-misol. *Agar R halqaning ixtiyoriy $a \in R$ elementi uchun $a^2 + a \in C(R)$ bo‘lsa, u holda halqaning kommutativ ekanligini isbotlang.*

Yechish. Aytaylik, $a, b \in R$ bo‘lsin, u holda $a^2 + a, b^2 + b \in C(R)$. Ikkinchi tomondan esa, $(a+b)^2 + a + b \in C(R)$, ya’ni $a^2 + ab + ba + b^2 + a + b \in C(R)$. Bu munosabatdan esa, $ab + ba \in C(R)$ ekanligi kelib chiqadi. Demak, $a(ab + ba) = (ab + ba)a$, ya’ni $a^2b = ba^2$. Bu esa $a^2 \in C(R)$ ekanligini bildiradi. $a^2 + a \in C(R)$ ekanligidan esa $a \in C(R)$ kelib chiqadi. Shunday qilib biz R halqaning ixtiyoriy $a \in R$ elementi uning markazida yotishini ko‘rsatdik. Demak, R kommutativ halqa. $\square$

5.2.5-misol. $M_2(\mathbb{R})$ *halqa sodda halqa ekanligini ko‘rsating.*

Yechish. Aytaylik, $M_2(\mathbb{R})$ halqaning qandaydir notrivial $\mathbf{J}$ ideali mavjud bo‘lsin. U holda noldan farqli $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{J}$ element mavjud. $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ va $C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ matritsalarni qarasak,

$$AB = \begin{pmatrix} b & 0 \\ d & 0 \end{pmatrix}, \quad CD = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}, \quad CAB = \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix}.$$

Ma’lumki, J ideal bo‘lganligi uchun $AB, CA, CAB \in \mathbf{J}$. Bundan esa, a, b, c, d sonlarining hech bo‘lmaganda bittasi noldan farqli bo‘lganligi uchun har doim $a \neq 0$ deb olish mumkinligi kelib chiqadi. U holda

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbf{J}$$

bo‘lib, bundan esa

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

elementlarning ham $\mathbf{J}$ idealga tegishli ekanligi kelib chiqadi. Bundan esa

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbf{J}$$

kelib chiqadi. Bu esa $\mathbf{J} = M_2(\mathbb{R})$ ekanligini bildiradi. Demak, $M_2(\mathbb{R})$ halqa sodda emas. $\square$

5.2.1 Mustaqil ishlash uchun misol va masalalar

1. Butun sonlar halqasining quyidagi qism to‘plamlarining qaysilari qism halqa tashkil qilishini aniqlang.

- $4\mathbb{Z}$.
- $4\mathbb{Z}+1$.
- $5\mathbb{Z}+2$.
- $4\mathbb{Z}+2$.

2. Quyidagi halqalarning barcha qism halqalarini aniqlang.

$$\mathbb{Z}_{12}, \quad \mathbb{Z}_{15}, \quad \mathbb{Z}_{16}, \quad \mathbb{Z}_{20}, \quad \mathbb{Z}_{30}, \quad \mathbb{Z}.$$

3. Quyidagi to‘plamlarni $M_2(\mathbb{R})$ matritsalar halqasining qism halqalari ekanligini ko‘rsating .

- $A_1 = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$.
- $A_2 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$.
- $A_3 = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$.
- $A_4 = \left\{ \begin{pmatrix} a & b\sqrt{3} \\ -b\sqrt{3} & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$.
- $A_5 = \left\{ \begin{pmatrix} a+b & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$.

4. Agar R biri bor halqa bo‘lsa, u holda $T = \{n1 \mid n \in \mathbb{Z}\}$ to‘plam qism halqa bo‘lishini isbotlang.

5. R halqaning $T = \{a \in R \mid na = 0\}$ qism to‘plami qism halqa bo‘lishini ko‘rsating.

6. Agar $a \in R$ element halqaning idempotent elementi bo‘lsa, u holda aRa to‘plam qism halqa bo‘lishini isbotlang.

7. $\mathbb{Z}[x]$ ko‘phadlar halqasining ozod hadi juft butun sonlardan iborat bo‘lgan qism halqasi ideal bo‘lib, bosh ideal bo‘lmasligini ko‘rsating.

8. Quyidagi halqalarning qism to‘plamlari ideali bo‘lishini ko‘rsating.

- $R = \mathbb{Z}_{24}$, $I = \{\overline{0}, \overline{8}, \overline{16}\}$.
- $R = \mathbb{Z}_{28}$, $I = \{\overline{0}, \overline{7}, \overline{14}, \overline{21}\}$.

- $R=\mathbb{Z}[\sqrt{7}],\ I=\{a+b\sqrt{7}\mid a,b\in\mathbb{Z},\ a-b \text{ juft son}\}$.
- $R=\left\{\begin{pmatrix} a & b\\ 0 & c\end{pmatrix}\mid a,b,c\in\mathbb{Z}\right\},\ I=\left\{\begin{pmatrix} 0 & b\\ 0 & c\end{pmatrix}\mid a\in\mathbb{Z}\right\}.$
- $R=\left\{\begin{pmatrix} a & b\\ 0 & c\end{pmatrix}\mid a,b,c\in\mathbb{Z}\right\},\ I=\left\{\begin{pmatrix} 0 & a\\ 0 & 0\end{pmatrix}\mid a\in\mathbb{Z}\right\}.$

9. Yuqoridagi misollardagi halqalarning berilgan ideali bo‘yicha faktor halqalarini aniqlang.

10. $R=\left\{\begin{pmatrix} a & b\\ 0 & c\end{pmatrix}\mid a,b,c\in\mathbb{Z}\right\}$ halqaning barcha ideallarini aniqlang.

11. Aytaylik,
$$R=\left\{\begin{pmatrix} a_{11} & a_{12} & a_{13}\\ 0 & a_{22} & a_{23}\\ 0 & 0 & a_{33}\end{pmatrix}\mid a_{ij}\in\mathbb{Z}\right\},$$
$$I=\left\{\begin{pmatrix} 0 & b & c\\ 0 & 0 & 2d\\ 0 & 0 & 0\end{pmatrix}\mid b,c,d\in\mathbb{Z}\right\},\quad J=\left\{\begin{pmatrix} 0 & x & 2y\\ 0 & 0 & 2z\\ 0 & 0 & 0\end{pmatrix}\mid x,y,z\in\mathbb{Z}\right\}$$
bo‘lsin. U holda I to‘plam R da ideal, J to‘plam esa I da ideal bo‘lishini, lekin J to‘plam R da ideal bo‘lmasligini ko‘rsating.

12. Quyidagi
$$A=\left\{\begin{pmatrix} x & -y & z & -t\\ y & x & -t & z\\ z & t & x & -y\\ t & -z & y & x\end{pmatrix}\mid x,y,z,t\in\mathbb{R}\right\},$$
to‘plam $(M_4(\mathbb{R}),+,\cdot)$ halqaning qism halqasi ekanligini isbotlang.

13. $A=\{x+\sqrt[3]{5}y+\sqrt[3]{25}z\mid x,y,z\in\mathbb{Q}\}$ to‘plam haqiqiy sonlar maydonining qism maydoni ekanligini ko‘rsating.

14. Aytaylik, $\alpha\in\mathbb{R}$ soni ratsional koeffitsiyentli $f(x)$ keltirilmas (ratsional sonlar maydoni ustida keltirilmas) ko‘phadning ildizi bo‘lsin. U holda
$$A=\{x_0+x_1\alpha+x_2\alpha^2+\cdots+x_{n-1}\alpha^{n-1}\mid x_i\in\mathbb{Q}\}$$
to‘plam haqiqiy sonlar maydonining qism maydoni ekanligini isbotlang.

15. Agar R halqaning A chap ideali va B o‘ng ideallari berilgan bo‘lsa, u holda AB to‘plam R halqaning ikki tomonli ideali bo‘lishini ko‘rsating.

16. Kommutativ halqaning nilpotent elementlari to‘plami ideal bo‘lishini isbotlang.

17. R halqaning I_1 va I_2 ideallari birlashmasi $I_1 \cup I_2$ ham ideal bo‘lishi uchun $I_1 \subseteq I_2$ yoki $I_2 \subseteq I_1$ bo‘lishi zarur va yetarli ekanligini isbotlang.

18. R halqaning I va J ideallari uchun $I+J$ ham ideal bo‘lishini va $I+J = \langle I \cup J \rangle$ ekanligini ko‘rsating.

19. Quyidagi halqalarning berilgan I ideali bo‘yicha annulyatorlarini toping.
    - $R = \mathbb{Z}_{12}$, $I = \{\overline{0}, \overline{4}, \overline{8}\}$.
    - $R = \mathbb{Z}_{15}$, $I = \{\overline{0}, \overline{5}, \overline{10}\}$.
    - $R = \mathbb{Z}_{20}$, $I = \{\overline{0}, \overline{2}, \overline{4}, \dots, \overline{18}\}$.
    - $R = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$, $I = \{a + bi \mid a, b \in 2\mathbb{Z}\}$.

20. Regulyar halqaning ixtiyoriy ideali regulyar ekanligini ko‘rsating.

21. $\mathbb{Z}[i]/\langle 2 \rangle$ faktor halqani aniqlang va uni maydon emasligini ko‘rsating.

22. $\mathbb{Z}[i]/\langle 3 \rangle$ faktor halqa maydon bo‘lishini isbotlang.

23. $\mathbb{Z}[i]/\langle n \rangle$ faktor halqa maydon bo‘lishi uchun n tub son bo‘lib, uning ikkita butun sonlar kvadratlari yig‘indisi shaklida ifodalanmasligini zarur va yetarli ekanligini isbotlang.

5.3 Halqalarning gomomorfizmi va izomorfizmi

Uahbu mavzuda biz halqalar uchun gomomorfizm va izomorfizmlar tushunchalarini kiritib, izomorfizm va moslik teoremalarini keltiramiz.

5.3.1-ta’rif. *Bizga $(R, +, \cdot)$ va $(R', +', \cdot')$ halqalar va $f : R \to R'$ akslantirish berilgan bo‘lsin. Agar ixtiyoriy $a, b \in R$ elementlar uchun*

$$f(a + b) = f(a) +' f(b),$$

$$f(a \cdot b) = f(a) \cdot' f(b)$$

tengliklar o‘rinli bo‘lsa, u holda f akslantirish R halqani R' halqaga o‘tkazuvchi gomomorfizm deb ataladi.

5.3.2-ta’rif. *Bizga R va R' halqalar, hamda $f : R \to R'$ gomomorfizm berilgan bo‘lsin.*

- *Agar f syurektiv bo‘lsa, u holda f akslantirish **epimorfizm** deyiladi;*

- *Agar f inyektiv bo'lsa, u holda f akslantirish* ***monomorfizm*** *deyiladi;*
- *Agar f biyektiv bo'lsa, u holda f akslantirish* ***izomorfizm*** *deyiladi;*
- *R halqani o'zini o'ziga akslantiruvchi izomorfizm esa* ***avtomorfizm*** *deb ataladi.*

Agar R halqani R' halqaga o'tkazuvchi izomorfizm mavjud bo'lsa, u holda ushbu halqalar izomorf deyiladi va $R \simeq R'$ kabi belgilanadi. R halqani o'zini o'ziga o'tjkazuvchi barcha avtomorfizmlar to'plami esa $Aut(R)$ kabi belgilanadi. Halqalarning gomomorfizmi uchun quidagi xossalar o'rinli bo'lib, ushbu xossalar gruppaning gomomorfizmi xossalar kabi isbotlanadi.

5.3.1-teorema. *Bizga R va R' halqalar, hamda $f : R \to R'$ gomomorfizm berilgan bo'lsin. U holda quyidagilar o'rinli.*

1) $f(0) = 0'$.
2) $f(-a) = -f(a)$.
3) *Agar R halqaning A qism halqasi berilgan bo'lsa, u holda $f(A) = \{f(x) \mid x \in A\}$ to'plam R' halqaning qism halqasi bo'ladi.*
4) *Agar R' halqaning B qism halqasi berilgan bo'lsa, u holda $f^{-1}(B) = \{x \in R \mid f(x) \in B\}$ to'plam R halqaning qism halqasi bo'ladi.*
5) *Agar R kommutativ bo'lsa, u holda $f(R)$ ham kommutativ bo'ladi.*
6) *Agar R biri bor halqa bo'lib, f epimorfizm bo'lsa, u holda R' ham birlik elementga ega va $f(1) = 1'$ bo'ladi.*
7) *Agar R biri bor halqa bo'lib f epimorfizm va $a \in R$ element teskarilanuvchi bo'lsa, u holda $f(a)$ ham teskarilanuvchi, hamda $f(a)^{-1} = f(a^{-1})$.*

R halqani R' halqaga o'tkazuvchi $f : R \to R'$ gomomorfizmning **yadrosi** deb quyidagi to'plamga aytiladi

$$\mathrm{Ker} f = \{a \in G \mid f(a) = 0'\}.$$

Yuqoridagi teoremaga ko'ra ixtiyoriy gomomorfizmining yadrosi bo'sh emas, chunki $0 \in \mathrm{Ker} f$. Bundan tashqari halqa gomomorfizmining yadrosi ikki tomonli ideal bo'ladi. Haqiqatdan ham, agar $a, b \in \mathrm{Ker} f$ va $x \in R$ bo'lsa, u holda $f(a) = f(b) = 0$ ekanligidan $f(a - b) = f(a) - f(b) = 0$, $f(a \cdot x) = f(a) \cdot f(x) = 0$ va $f(x \cdot a) = f(x) \cdot f(a) = 0$ bo'lishini hosil qilamiz. Bu esa $a - b, a \cdot x, x \cdot a \in \mathrm{Ker} f$ ekanligini, ya'ni halqa gomomorfizmi yadrosining ideal bo'lishini anglatadi.

5.3.1-misol.

- *R halqani R' halqaga o'tkazuvchi $f(a) = 0'$ kabi aniqlangan $f : R \to R'$ akslantirish gomomorfizm bo'lib, $Kerf = R$ bo'ladi.*

- *R halqani o'zini o'ziga o'tkazuvchi ayniy akslantirsh gomomorfizm bo'lib, $Kerf = \{0\}$ bo'ladi. Bundan tashqari ushbu ayniy akslantirish avtomorfizm bo'ladi.*

Endi $(\mathbb{Z}, +, \cdot)$ butun sonlar halqasini $(\mathbb{Z}_n, +_n, \cdot_n)$ chegirmalar halqasiga o'tkazuvchi gomomorfizmga misol keltiramiz.

5.3.2-misol. *$\mathbb{Z}$ halqani $\mathbb{Z}_n$ halqaga o'tkazuvchi $f(a) = \overline{a}$ kabi aniqlangan akslantirish gomomorfizm bo'lib, uning yadrosi uchun $Kerf = n\mathbb{Z}$ munosabat o'rinli. Ya'ni ushbu akslantirishning yadrosi n soniga karrali bo'lgan butun sonlar to'plamidan iborat bo'ladi.*

Quyidagi misolda biri bor R va R' halqalar uchun $f : R \to R'$ gomomorfizm syurektiv bo'lmasa, u holda $f(1) = 1'$ tenglik har doim ham o'rinli bo'lavermasligini ko'rsatamiz. Buning uchun $\mathbb{Z} \times \mathbb{Z}$ to'plamda quyidagi amallarni aniqlaymiz

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \cdot (c, d) = (a \cdot c, b \cdot d).$$

U holda $\mathbb{Z} \times \mathbb{Z}$ to'plam ushbu qo'shish va ko'paytirish amallariga nisbatan halqa tashkil qilib, bu halqaning nol elementi $(0, 0)$, birlik elementi esa $(1, 1)$ bo'ladi.

5.3.3-misol. *$\mathbb{Z}$ halqadan $\mathbb{Z} \oplus \mathbb{Z}$ halqaga bo'lgan $f : \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$ akslantirishni quyidagicha aniqlaylik,*

$$f(x) = (x, 0), \quad \forall x \in \mathbb{Z}.$$

Ushbu akslantirish gomomorfizm bo'lib, u inyektiv, lekin syurektiv bo'ladi. Ya'ni bu akslantirish monomorfizm, lekin epimorfizm emas. $\mathbb{Z}$ halqaning birlik elementi uchun $f(1) = (1, 0)$ bo'lib, bu element $\mathbb{Z} \oplus \mathbb{Z}$ halqaning birlik elementi emas. Ya'ni birinchi halqa birlik elementining obrazi ikkinchi halqaning birlik elementi bo'lmaydi.

Biz avvalgi mavzuda $(\mathbb{Z}[\sqrt{3}], +, \cdot)$ va $(\mathbb{Z}[\sqrt{5}], +, \cdot)$ halqalarni qarab o'tgan edik. Bir qarashda ushbu halqalar izomorf halgalarga o'xshab ko'rinadi. Lekin ular izomorf halqalar bo'lmaydi.

5.3.4-misol. $(\mathbb{Z}[\sqrt{3}], +, \cdot)$ *va* $(\mathbb{Z}[\sqrt{5}], +, \cdot)$ *halqalar izomorf emasligini ko'rsating.*

Yechish. Teskarini faraz qilamiz, ya'ni $f : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{5}]$ izomorfizm mavjud bo'lsin. U holda $f(1) = 1$ bo'lib, bundan esa $f(3) = 3$ ekanligi kelib chiqadi. Ikkinchi tomondan esa,

$$f(3) = f(\sqrt{3}^2) = (f(\sqrt{3}))^2$$

munosabatdan $f(\sqrt{3}) = \sqrt{3}$ tenglikka ega bo'lamiz. Demak, $\sqrt{3} \in \mathbb{Z}[\sqrt{5}]$. Bu esa ziddiyat. $\square$

Endi gruppalar nazariyasida bo'lgani kabi tabiiy gomomorfizm tushunchasi va izomorfizm haqidagi teoremalarni keltiramiz. Teoremalarning isbotlari gruppalar uchun berilgan teoremalar isboti kabi bo'lganligi uchun biz ularning isbotlariga batafsil to'xtalib o'tirmaymiz.

Bizga R halqa va uning I ideali berilgan bo'lsin. U holda quyidagi $g : R \to R/I$ akslantirishni qaraymiz

$$g(a) = a + I, \quad \forall a \in R.$$

Ushbu akslantirish gomomorfizm bo'lib, u **tabiiy gomomorfizm** deb ataladi. Tabiiy gomomorfizm syurektiv bo'lib, $\mathrm{Ker} g = I$ munosabat o'rinli.

5.3.2-teorema. *Bizga R halqani R' halqaga o'tkazuvchi $f : R \to R'$ epimorfizm berilgan bo'lsin. Agar R halqaning I idelai uchun $I \subseteq \mathrm{Ker} f$ munosabat o'rinli bo'lsa, u holda $g : R \to R/I$ syurektiv tabiiy gomomorfizm uchun $f = h \circ g$ shartni qanoatlantiruvchi yagona $h : R/I \to R'$ epimorfizm mavjud. Shuningdek, h inyektiv bo'lishi uchun $I = \mathrm{Ker} f$ tenglik o'rinli bo'lishi zarur va yetarli.*

Isbot. Teoremani isbotlash uchun $h : R/I \to R'$ akslantirishni $h(a+I) = f(a)$ kabi aniqlaymiz. Ushbu akslantirish to'g'ri aniqlangan bo'lib, $f = h \circ g$ tenglik o'rinli bo'ladi. Uning gomomorfizm ekanligi esa quyidagi tenglikdan kelib chiqadi

$$h\big((a + I) \cdot (b + I)\big) = h(a \cdot b + I) = f(a \cdot b) = f(a) \cdot f(b) = h(a + I) \cdot h(b + I).$$

$\square$

Endi bevosita izomorfizm haqidagi teoremalarni keltiramiz.

5.3.3-teorema (izomorfizm haqidagi birinchi teorema.). *Agar f akslantirish R halqani R' halqaga o'tkazuvchi gomomorfizm bo'lsa, u holda $R/\mathrm{Ker} f \simeq f(R)$ bo'ladi.*

5.3.4-teorema (izomorfizm haqidagi ikkinchi teorema.). *R halqaning I va J ideallari uchun $I/(I \cap J) \simeq (I + J)/J$ munosabat o'rinli.*

5.3.5-teorema (izomorfizm haqidagi uchinchi teorema.). *R halqaning I va J ideallari uchun $I \subseteq J$ bo'lsa, u holda*

$$(R/I)/(J/I) \simeq R/J.$$

Quyidagi teoremada esa gruppalar nazariyasidagi kabi halqalar uchun moslik teoremasini keltiramiz.

5.3.6-teorema (moslik teoremasi). *Aytaylik, R halqani R' halqaga akslantiruvchi f epimorphizm berilgan bo'lsin. U holda R halqaning $Kerf \subseteq I$ shartni qanoatlantiruvchi ideallari to'plami bilan R' halqaning ideallari to'plami orasida o'zaro bir qiymatli moslik mavjud.*

Endi ixtiyoriy halqani biri bor halqaga kengaytirish mumkinligini, ya'ni ixtiyoriy halqa uchun shunday biri bor halqa topilib, bu halqalar orasida monomorfizm mavjudligini ko'rsatamiz.

Bizga R halqa berilgan bo'lsin. $R' = R \times \mathbb{Z}$ to'plamda

$$(x, a) + (y, b) = (x + y, a + b), \quad (x, a) \cdot (y, b) = (xy + ay + bx, ab)$$

amallarni qarasak, R' to'plam ushbu amallarga nisbatan halqa tashkil qiladi. Ushbu halqa biri bor halqa bo'lib, $(0, 1)$ element uning birlik elementi bo'ladi. Bundan tashqari, $f(x) = (x, 0)$ kabi aniqlangan $f : R \to R \times \mathbb{Z}$ akslantirish monomorfizm bo'ladi.

5.3.1-tasdiq. *Agar R halqadan biri bor S halqaga φ gomomorfizm berilgan bo'lsa, u holda $\varphi = \psi \circ f$ shartni qanoatlantiruvchi $\psi : R \times \mathbb{Z} \to S$ gomomorfizm mavjud, bu yerda $f : R \to R \times \mathbb{Z}$ bo'lib, $f(x) = (x, 0)$.*

Isbot. $\psi : R \times \mathbb{Z} \to S$ akslantirishni $\psi(x, a) = \varphi(x) + a1_S$ kabi aniqlaymiz, bu yerda 1_S element S halqaning birlik elementi. U holda ixtiyoriy $x \in R$ uchun

$$(\psi \circ f)(x) = \psi(f(x)) = \psi(x, 0) = \varphi(x)$$

tenglik o'rinli, ya'ni $\varphi = \psi \circ f$. Bundan tashqari ushbu akslantirish gomomorfizm bo'ladi, chunki

$$\psi\big((x, a) + (y, b)\big) = \psi(x + y, a + b) = \varphi(x + y) + (a + b)1_S =$$
$$= \varphi(x) + \varphi(y) + a1_S + b1_S = \psi(x, a) + \psi(y, b),$$
$$\psi\big((x, a) \cdot (y, b)\big) = \psi(xy + ay + bx, ab) = \varphi(xy + ay + bx) + (ab)1_S =$$
$$\varphi(x)\varphi(y) + a\varphi(y) + b\varphi(x) + ab1_S = (\varphi(x) + a1_S) \cdot (\varphi(y) + b1_S) = \psi(x, a) \cdot \psi(y, b).$$

□

5.3.5-misol. *Xarakteristikasi nolga teng biri bor ixtiyoriy halqaning $\mathbb{Z}$ butun sonlar halqasiga izomorf qism halqasi mavjud ekanligini isbotlang.*

Yechich. Aytaylik, R xarakteristikasi noldan farqli biri bor halqa bo'lsin. $T = \{n1 \mid n \in \mathbb{Z}\}$ to'plamni qarasak, ushbu to'plam R halqaning qism halqasi bo'ladi. Chunki, $a, b \in T$ elementlar uchun $a = n1$ va $b = m1$ bo'lib,

$$a - b = n1 - m1 = (n - m)1, \quad ab = (n1)(m1) = (nm)1.$$

Ya'ni $a - b, ab \in T$. Endi $\mathbb{Z}$ butun sonlar halqasidan T to'plamga $f(n) = n1$ kabi aniqlangan $f : \mathbb{Z} \to T$ akslantirishni qaraymiz. Bu akslantirish gomomorfizm bo'lib, u syurektivdir. Bundan tashqari R halqaning xarakteristikasi nolga teng ekanligini hisobga olsak, $f(n) = f(m) \Rightarrow n1 = m1 \Rightarrow (n - m)1 = 0 \Rightarrow n = m$ munosabatlardan bu gomomorfizmning inyektivligi kelib chiqadi. Demak, f izomorfizm. □

5.3.6-misol. *Ixtiyoriy p tub soni uchun elementlari soni p ta bo'lgan halqalar izomorfizm aniqligida ikkita ekanligini isbotlang.*

Yechish. Aytaylik, $(R, +, \cdot)$ halqa p ta elementdan iborat bo'lsin. Ma'lumki, p ta elementli ixtiyoriy gruppa $(\mathbb{Z}_p, +_p)$ gruppaga izomof. Agar $(\mathbb{Z}_p, +_p)$ gruppada $\odot_1$ va $\odot_2$ ko'paytmalarni quyidagicha aniqlasak,

$$\overline{a} \odot_1 \overline{b} = 0, \quad \overline{a} \odot_2 \overline{b} = \overline{ab}$$

u holda biz o'zaro izomorf bo'lmagan $(\mathbb{Z}_p, +_p, \odot_1)$ va $(\mathbb{Z}_p, +_p, \odot_2)$ halqalarga ega bo'lamiz. Ya'ni birinchi halqa trivial ko'paytmaga ega bo'lgan halqa bo'lsa, ikkinchi halqa esa, chegirmalar halqasidan iborat bo'ladi.

Endi R halqani yuqoridagi ikkita halqadan biriga izomorf ekanligini ko'rsatamiz. $(R, +) \simeq (\mathbb{Z}_p, +_p)$ bo'lganligi uchun, $(R, +)$ gruppa additiv siklik gruppa bo'ladi. Aytaylik, $(R, +, \cdot)$ halqa $(\mathbb{Z}_p, +_p, \odot_1)$ halqaga izomorf bo'lmasin. U holda R halqada aniqlangan ko'paytma trivial emas. Agar $a \in R$ element $(R, +)$ additiv siklik gruppaning hosil qiluvchi elementi bo'lsa, u holda R ning ixtiyoriy elementi ka ko'rinishiga ega bo'ladi. U holda $a^2 = na$ tenglik o'rinli, bu yerda $n \neq 0$. Endi $mn \equiv 1(\mod p)$ shartni qanoatlantiruvchi m soni uchun $b = ma$ elementni qarasak,

$$b^2 = m^2a^2 = m^2na = ma = b$$

munosabatga ega bo'lamiz. Ya'ni R halqada $b^2 = b$ shartni qanoatlantiruvchi noldan farqli element mavjud. U holda $f(\overline{n}) = nb$ kabi aniqlangan $f : \mathbb{Z}_p \to R$ akslantirish $(\mathbb{Z}_p, +_p, \odot_2)$ halqadan $(R, +, \cdot)$ halqaga bo'lgan izomorfizm bo'ladi. Chunki,

$$f(\overline{n} + \overline{m}) = (n + m)b = nb + mb = f(\overline{n}) + f(\overline{m}),$$
$$f(\overline{n} \odot_2 \overline{m}) = f(\overline{nm}) = (nm)b = (nm)b^2 = (nb) \cdot (mb) = f(\overline{m}) \cdot f(\overline{n}).$$

□

5.3.1 Mustaqil ishlash uchun misol va masalalar

1. $\mathbb{Z}$ butun sonlar to'plamida $a \oplus b = a + b - 1$ va $a \odot b = a + b - ab$ kabi amallar aniqlangan bo'lsin. $(\mathbb{Z}, \oplus, \odot)$ halqa ekanligini ko'rsating va uni $(\mathbb{Z}, +, \cdot)$ halqaga izomorf ekanligini isbotlang.

2. R halqani R' halqaga o'tkazuvchi barcha gomomorfizmlarni aniqlang.

   - $R = (\mathbb{Z}_4, +_4, \cdot_4)$ va $R' = (\mathbb{Z}_6, +_6, \cdot_6)$.
   - $R = (\mathbb{Z}_6, +_6, \cdot_6)$ va $R' = (\mathbb{Z}_{10}, +_{10}, \cdot_{10})$.
   - $R = (\mathbb{Z}, +, \cdot)$ va $R' = (\mathbb{Z}, +, \cdot)$.

- $R = (\mathbb{Z}, +, \cdot)$ va $R' = (2\mathbb{Z}, +, \cdot)$.
- $R = (\mathbb{Z}, +, \cdot)$ va $R' = (\mathbb{Z}_6, +_6, \cdot_6)$.
- $R = (\mathbb{R}, +, \cdot)$ va $R' = (\mathbb{R}, +, \cdot)$.

3. Quyidagi halqalarning izomorf emasligini ko‘rsating.

- $(\mathbb{R}, +, \cdot)$ va $(\mathbb{Q}, +, \cdot)$.
- $(\mathbb{R}, +, \cdot)$ va $(\mathbb{C}, +, \cdot)$.
- $(\mathbb{Z}, +, \cdot)$ va $(2\mathbb{Z}, +, \cdot)$.
- $(2\mathbb{Z}, +, \cdot)$ va $(3\mathbb{Z}, +, \cdot)$.
- $(\mathbb{Q}\sqrt{2}, +, \cdot)$ va $(\mathbb{Q}\sqrt{3}, +, \cdot)$.

4. R halqani R' halqaga o‘tkazuvchi emimorfizm mavjudmi?

- $R = (\mathbb{Z}, +, \cdot)$ va $R' = (\mathbb{Z}_5, +_5, \cdot_5)$.
- $R = (\mathbb{Z}_{15}, +_{15}, \cdot_{15})$ va $R' = (\mathbb{Z}_5, +_5, \cdot_5)$.
- $R = (\mathbb{Z}_{24}, +_{24}, \cdot_{24})$ va $R' = (\mathbb{Z}_7, +_7, \cdot_7)$.
- $R = (\mathbb{Z}_{18}, +_{18}, \cdot_{18})$ va $R' = (\mathbb{Z}_8, +_8, \cdot_8)$.

5. R halqani R' halqaga o‘tkazuvchi monomorfizm mavjudmi?

- $R = (\mathbb{Z}_8, +_8, \cdot_8)$ va $R' = (\mathbb{Z}, +, \cdot)$.
- $R = (\mathbb{Z}_5, +_5, \cdot_5)$ va $R' = (\mathbb{Z}_{15}, +_{15}, \cdot_{15})$.
- $R = (\mathbb{Z}_6, +_6, \cdot_6)$ va $R' = (\mathbb{Z}_8, +_8, \cdot_8)$.
- $R = (\mathbb{Z}_{12}, +_{12}, \cdot_{12})$ va $R' = (\mathbb{Z}_{18}, +_{18}, \cdot_{18})$.

6. Let $T_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}$ va $\mathbb{Z}$ halqalar uchun $f(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) = a$ kabi aniqlangan $f : T_2(\mathbb{Z}) \to \mathbb{Z}$ akslantirishning gomomorfizm ekanligini ko‘rsating va uning yadrosini toping.

7. Agar R Bul halqasi $\{0\}$ va R dan boshqa idealga ega bo‘lmasa, u holda $R \simeq \mathbb{Z}_2$ ekanligini isbotlang.

8. Xarakteristikasi $n(n > 0)$ ga teng biri bor ixtiyoriy halqaning $\mathbb{Z}_n$ halqaga izomorf qism halqasi mavjud ekanligini isbotlang.

9. Kompleks sonlar maydonining haqiqiy sonlarni o‘zgarishsiz qoldiruvchi avtomorfizmlarini toping.

10. $A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ halqa va $(\mathbb{C}, +, \cdot)$ kompleks sonlar maydoni berilgan boʻlsin. $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ akslantirish izomofizm ekanligini koʻrsating.

11. $A = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$ halqa $B = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ halqaga izomorf ekanligini koʻrsating.

12. Quyidagi matritsalar halqalari izomorf boʻladimi?

$$A = \left\{ \begin{pmatrix} x & -y & z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix} \mid x, y, z, t \in \mathbb{R} \right\},$$

$$B = \left\{ \begin{pmatrix} u & w \\ -\overline{w} & \overline{u} \end{pmatrix} \mid u, w \in \mathbb{C} \right\}.$$

5.4 Nilpotent, maksimal va birlamchi(prime) ideallar

Ushbu mavzuda ba'zi muhum ideallar haqida toʻxtalib oʻtamiz. Bizga R halqa va uning I ideali berilgan boʻlsin. Quyidagi qatorni qaraymiz

$$I^1 = I, \quad I^{k+1} = I^k \cdot I, \ k \geq 1.$$

5.4.1-ta'rif. *Agar shunday n natural son topilib, $I^n = \{0\}$ boʻlsa, u holda I* ***nilpotent ideal*** *deb ataladi. Ixtiyoriy elementi nilpotent boʻlgan ideal esa* ***nil ideal*** *deb ataladi.*

Ta'rifdan koʻrinadiki, ixtiyoriy nilpotent ideal nil ideal boʻladi. Lekin teskarisi oʻrinli boʻlishi shart emas. $\mathbb{Z}_8$ chegirmalar halqasining $I = \{\overline{0}, \overline{4}\}$ ideali ham nil, ham nilpotent ideal bo'lsa, quyidagi misolda nil boʻlib, nilpotent boʻlmaydigan idealga misol keltiramiz.

5.4.1-misol. *p tub soni uchun cheklita hadi noldan farqli boʻlgan $\{a_n\}, a_n \in Z_{p^n}$ ketma-ketliklarni qaraymiz, ya'ni qandaydir m sonidan katta barcha k lar uchun $a_k = 0$. Endi R orqali bunday ketma-ketliklardan tuzilgan toʻplamni belgilab, bu toʻplamda qoʻshish va koʻpaytirish amallarini quyidagicha aniqlaymiz*

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}, \quad \{a_n\} \cdot \{b_n\} = \{a_n \cdot b_n\}.$$

U holda R to‘plam ushbu amallarga nisbatan halqa tashkil qiladi. Endi bu halqaning $\{pa_i\}$ ko‘rinishidagi ketma-ketliklardan iborat qism to‘plamini I orqali belgilaymiz. Ushbu I to‘plam R halqaning ideali bo‘lib, uning ixtiyoriy elementi nilpotent bo‘ladi, chunki ixtiyoriy $a_n \in I$ element $(pa_1, pa_2, pa_3, \dots, pa_m, 0, 0, \dots)$ ko‘rinishida bo‘lib,

$$\{a_n\}^m = (p^m a_1, p^m a_2, p^m a_3, \dots, p^m a_m, 0, 0, \dots) = \{0\}.$$

Demak, I nil ideal. Endi ushbu idealning nilpotent emasligini ko‘rsatamiz. Teskarisini faqaz qilaylik, ya’ni I nilpotent ideal bo‘lsin, u holda qandaydir $m \in \mathbb{N}$ natural soni uchun $I^m = \{0\}$. Endi $m+1$ ta hadi p ga teng bo‘lgan $\{a_n\}$ ketma-ketlikni qaraymiz, ya’ni $\{a_n\} = (\underbrace{p, p, \dots, p, p}_{m+1 \ ta}, 0, 0, \dots)$. U holda $\{a_n\}^m = (\underbrace{0, 0, \dots, 0}_{m \ ta}, \overline{p^m}, 0, 0, \dots)$ bo‘ladi. $\overline{p^m}$ element $Z_{p^{m+1}}$ da noldan farqli bo‘lganligi uchun $\{a_n\}^m$ ham I idealning noldan farqli elementi bo‘ladi. Bu esa $I^m = \{0\}$ ekanligiga zid. Demak, I nilpotent emas.

Aytaylik, R kommutativ halqa I esa uning nilpotent elementlaridan tashkil topgan qism to‘plami bo‘lsin. Ma’lumki, kommutativ halqada nilpotent elementlarning ayirmasi yana nilpotent element bo‘ladi. Bundan tashqari, ixtiyoriy $a \in I$ va $x \in R$ elementlar uchun $(xa)^n = x^n a^n$ tenglikdan $xa \in I$ ekanligi kelib chiqadi. Ya’ni I nil ideal bo‘ladi.

5.4.1-tasdiq. *Aytaylik, R kommutativ halqa I esa uning nilpotent elementlaridan tashkil topgan qism to‘plami bo‘lsin. U holda I nil ideal bo‘lib, R/I faktor halqa noldan farqli nilpotent elementga ega emas.*

Isbot. Tasdiqning birinchi qismini, ya’ni I nil ideal ekanligini yuqorida keltirib o‘tdik. Shuning uchun tasdiqning ikkinchi qismini isbotlaymiz. Faraz qilaylik $a+I$ element R/I faktor halqaning nilpotent elementi bo‘lsin. U holda qandaydir n natural soni uchun $(a+I)^n = I$ tenglik o‘rinli bo‘ladi. Ikkinchi tomondan esa $(a+I)^n = a^n + I$ bo‘lganligi uchun $a^n + I = I$, ya’ni $a^n \in I$ ekanligini hosil qilamiz. Bu esa, a^n elementning ham nilpotent element ekanligini bildiradi. Demak, shunday m natural soni uchun $(a^n)^m = 0$, ya’ni $a^{nm} = 0$. Bundan biz a elementning nilpotent ekanligini, ya’ni $a \in I$ bo‘lishini hosil qilamiz. Demak, $a + I = I$, bu esa R/I faktor halqaning nol elementi. Shunday qilib, biz R/I faktor halqa noldan farqli nilpotent elementga ega emasligini ko‘rsatdik. □

5.4.1 Tub va keltirilmas elementlar

Ushbu bo‘limda birlik elementga ega bo‘lgan kommutativ halqaning tub va keltirilmas elementlari tushunchalarini kiritib ularning hossalarini keltiramiz.

Aytaylik, R birlik elementga ega bo‘lgan kommutativ halqa bo‘lsin.

5.4.2-ta'rif. *Agar birlik elementga ega bo'lgan kommutativ R halqaning noldan farqli va teskarilanmaydigan $p \in R$ elementi uchun $p \mid ab$ ekanligidan $p \mid a$ yoki $p \mid b$ ekanligi kelib chiqsa, u holda ushbu element tub element deb ataladi.*

5.4.3-ta'rif. *Agar birlik elementga ega bo'lgan kommutativ R halqaning noldan farqli va teskarilanmaydigan $p \in R$ elementi uchun $p = ab$ ekanligidan a yoki b elementlarning teskarilanuvchi ekanligi kelib chiqsa, u holda ushbu element keltirilmas element deb ataladi. Aks holda, ya'ni agar p elementni teskarilanuvchi bo'lmaydigan a va b elementlarning ko'paytmasi shaklida $p = ab$ kabi ifodalash mumkin bo'lsa, u holda p element keltiriluvchi deyiladi.*

Ta'kidlash joizki, $\mathbb{Z}$ butun sonlar halqasi uchun p tub sonni olsak, u holda p va $-p$ elementlar ham tub ham keltirilmas elementlar bo'ladi.

Quyidagi misolda, tub element bo'lib, keltirilmas bo'lmaydigan elementga misol keltiramiz.

5.4.2-misol. *$\mathbb{Z}_6$ halqaning $p = \overline{3}$ elementi tub element bo'lib, keltiriluvchi bo'ladi. Chunki, agar $\overline{a}, \overline{b} \in \mathbb{Z}_6$ elementlar uchun $\overline{3} \mid \overline{a}\overline{b}$ ekanligidan, shunday $\overline{c} \in \mathbb{Z}_6$ element uchun $\overline{3} \cdot \overline{c} = \overline{a} \cdot \overline{b}$ tenglikning bajarilishi, bundan esa $6 \mid (ab - 3c)$ ekanligi kelib chiqadi. Ushbu munosabatdan esa, $3 \mid (ab - 3c)$, ya'ni $3 \mid ab$ ekanligini olish qiyin emas. Bu esa $3 \mid a$ yoki $3 \mid b$ ekanligini, ya'ni $\overline{3} \mid \overline{a}$ yoki $\overline{3} \mid \overline{b}$ bo'lishini bildiradi. Demak, $p = \overline{3}$ element $\mathbb{Z}_6$ halqaning tub elementi.*

Ushbu $p = \overline{3}$ elementning keltiriluvchi ekanligi esa $\overline{3} = \overline{3} \cdot \overline{3}$ tenglikdan kelib chiqadi. Ya'ni $\overline{3}$ elementni teskarilanmaydigan elementlarning ko'paytmasi shaklida ifodalash mumkin.

Endigi misolda esa, keltirilmas bo'lib, lekin tub bo'lmaydigan element mavjudligini ko'rsatamiz.

5.4.3-misol. $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ *halqaning $p = 3$ elementi keltirilmas bo'lib, tub bo'lmaydi.*

Chunki, ushbu elementni teskarilanmaydigan elementlar ko'paytmasi shaklida $(a + bi\sqrt{5})(c + di\sqrt{5}) = 3$ kabi ifodalash mumkin emas. Demak, $p = 3$ element keltirilmas element. Lekin 3 ga bo'linmaydigan $a = 1 + i\sqrt{5}$ va $b = 1 + i\sqrt{5}$ elementlarning ko'paytmasi $ab = 6$ soni 3 ga bo'linishidan, ushbu elementning tub emasligi kelib chiqadi.

Endi qanday halqalardan tub va keltirilmas elementlar ustma-ust tushishi haqidagi natijalarni keltiramiz.

5.4.1-teorema. *Butunlik sohasining ixtiyoriy tub elementi keltirilmas element bo'ladi.*

Isbot. Aytaylik, R butunlik sohasi bo‘lib, $p \in R$ tub element uchun $p = ab$ bo‘lsin. U holda $p\,|ab$ bo‘lib, bundan esa $p\,|a$ yoki $p\,|b$ ekanligi kelib chiqadi. Agar $p\,|a$ bo‘lsa, u holda $a = pq$ bo‘lib, $p = ab = pqb$, ya’ni $p(1 - qb) = 0$ kelib chiqadi. R soha butunlik sohasi va $p \neq 0$ bo‘lganligi uchun $1 - qb = 0$ tenglikni, ya’ni b elementning teskarilanuvchi ekanligini hosil qilamiz. Xuddi shunga o‘xshab, agar $p\,|b$ bo‘lsa, u holda a element teskarilanuvchi bo‘ladi. Demak, p keltirilmas element. □

5.4.1-teoremaning teskarisi o‘rinli emasligi 5.4.2-misoldan ko‘rinadi. Ya’ni butunlik sohasining keltirilmas elementi tub element bo‘lishi shart emas.

Quyidagi teoremada esa, bosh ideallar sohasining keltirilmas va tub elementlari ustma-ust tushushu ko‘rsatiladi.

5.4.2-teorema. *Bosh ideallar sohasining p elementi keltirilmas bo‘lishi uchun uning tub element bo‘lishi zarur va yetarli.*

Isbot. Ushbu teoremaning yetarliligi 5.4.1-teoremadan bevosita kelib chiqqanligi uchun uning zaruriyligini isbotlaymiz. Aytaylik, R bosh ideallar sohasining p keltirilmas elementi uchun $p \mid ab$ bo‘lsin, u holda $ab = rp$. Ikkinchi tomondan esa R bosh ideallar sohasi bo‘lganligi uchun $\langle p, b\rangle$ ideal qandaydir $\langle d\rangle$ ideal bilan ustma-ust tushadi. Bu esa, $d \mid p$, ya’ni qandaydir $q \in R$ element uchun $p = dq$ ekanligini bildiradi. p element keltirilmas ekanligidan d va q elementlardan hech bo‘lmaganda bittasi teskarilanuvchi ekanligi kelib chiqadi.

Agar d teskarilanuvchi bo‘lsa, u holda $\langle p, b\rangle = \langle d\rangle = R$ bo‘lib, bundan esa R halqaning ixtiyoriy elementi p va b lar orqali ifodalanishi kelib chiqadi. Xususan, qandaydir $s, t \in R$ elementlar uchun $1 = sp + tb$. Bundan esa,

$$a = a(sp + tb) = asp + atb = asp + trp = (as + tr)p$$

tenglikka ega bo‘lamiz. Bu esa a element p ga bo‘linishini bildiradi.

Agar q teskarilanuvchi bo‘lsa, u holda $d = pq^{-1}$ bo‘lib, $d \in \langle p\rangle$ ekanligi kelib chiqadi. U holda $\langle p, b\rangle = \langle p\rangle$ bo‘lib, $b \in \langle p\rangle$ ekanligi, ya’ni b element p ga bo‘linishi kelib chiqadi. Shunday qilib biz agar $p \mid ab$ bo‘lsa, u holda $p \mid a$ yoki $p \mid b$ bo‘lishini ko‘rsatdik. Demak, p tub element. □

5.4.2 Maksimal, birlamchi(prime) va primar(primary) ideallar

Endi halqaning bir qancha maxsus ideallari tushunchalarini keltirib, ularning xossalarini o‘rganamiz. Dastlab, birlamchi(prime) ideal tushunchasini kiritamiz. Takidlab o‘tish joizki, birlamchi ideal tushunchasining bir qancha ekvivalent ta’riflari mavjud bo‘lib, biz asisiy ta’rif sifatida quyidagini keltiramiz.

5.4.4-ta'rif. *Aytaylik, R halqaning P ideali berilgan bo'lsin. Agar ixtiyoriy A, B ideallar uchun $AB \subseteq P$ ekanligidan $A \subseteq P$ yoki $B \subseteq P$ kelib chiqsa, u holda P ideal **birlamchi(prime)** ideal deb ataladi.*

Ta'kidlash joizki, agar P birlamchi ideal bo'lib, $a, b \in R$ elementlar uchun $\langle a\rangle\langle b\rangle \subseteq P$ bo'lsa, u holda $\langle a\rangle \subseteq P$ yoki $\langle b\rangle \subseteq P$ kelib chiqadi. Bu esa, $a \in P$ yoki $b \in P$ ekanligini anglatadi. Demak, P birlamchi ideal bo'lib, $\langle a\rangle\langle b\rangle \subseteq P$ bo'lsa, u holda $a \in P$ yoki $b \in P$. Bundan tashqari, qandaydir $k \in \mathbb{N}$ natural soni uchun $\langle a\rangle^k \subseteq P$ bo'lsa, u holda $a \in P$ bo'ladi.

Birlamchi ideal tushunchasi, yuqoridagi ta'rifga ekvivalent bo'lgan quyidagi ta'rif orqali ham aniqlash mumkin. Ushbu ta'rifning yuqoridagi ta'rifdan farqi shundaki, bunda birlamchi ideal tushunchasi halqaning elementlari orqali beriladi.

5.4.5-ta'rif. *Aytaylik, R halqaning P ideali berilgan bo'lsin. Agar ixtiyoriy $a, b \in R$ elemetlar uchun $aRb \subseteq P$ ekanligidan $a \in P$ yoki $b \in P$ kelib chiqsa, u holda P ideal **birlamchi (prime)** ideal deb ataladi.*

Quyidagi teoremada esa, yuqoridagi ta'riflarning ekvivalent ekanligini ko'rsatamiz.

5.4.3-teorema. *R halqaning P ideali birlamchi ideal bo'lishi uchun ixtiyoriy $a, b \in R$ elemetlar uchun $aRb \subseteq P$ ekanligidan $a \subseteq P$ yoki $b \subseteq P$ kelib chiqishi zarur va yetarli.*

Isbot. ***Zaruriyligi.*** Aytaylik, P birlamchi ideal bo'lib, $a, b \in P$ elementlar uchun $aRb \subseteq P$ bo'lsin. Quyidagi belgilashlarni kiritamiz

$$A = RaR, \quad B = RbR.$$

U holda A va B to'plamlar R halqaning ideallari bo'lib,

$$AB = (RaR)(RbR) \subseteq R(aRb)R \subseteq RPR \subseteq P.$$

P ideal birlamchi ideal bo'lganligi uchun $A \subseteq P$ yoki $B \subseteq P$. Agar $A \subseteq P$ bo'lsa, u holda $\langle a\rangle^3 \subseteq RaR = A \subseteq P$ ekanligidan $a \in P$ kelib chiqadi. Xuddi shunga o'xshab, agar $B \subseteq P$ bo'lsa, u holda $b \in P$ ekanligini hosil qilamiz. Demak, $a \subseteq P$ yoki $b \subseteq P$.

Yetarliligi. Aytaylik, ixtiyoriy $a, b \in R$ elemetlar uchun $aRb \subseteq P$ ekanligidan $a \subseteq P$ yoki $b \subseteq P$ kelib chiqsin. Faraz qilaylik, R halqaning A va B ideallari berilgan bo'lib, $AB \subseteq P$ va $A \nsubseteq P$ bo'lsin. U holda shunday $a \in A$ element topilib, $a \notin P$. Ixtiyoriy $b \in B$ element uchun

$$aRb = (aR)b \subseteq AB \subseteq P$$

ekanligidan, $a \in P$ yoki $b \in P$ kelib chiqadi. Lekin, $a \notin P$ bo‘lganligi uchun biz ixtiyoriy $b \in B$ element uchun $b \in P$ ekanligini hosil qilamiz. Demak, $B \subseteq P$, ya’ni P birlamchi ideal. $\square$

Yuqoridagi teoremadan quyidagi natijani hosil qilamiz.

5.4.1-natija. *R halqaning P ideali berilgan bo‘lib, ixtiyoriy $a, b \in R$ elementlar uchun $ab \in P$ ekanligidan $a \in P$ yoki $b \in P$ kelib chiqsa, u holda P birlamchi ideal bo‘ladi.*

Isbot. Faraz qilaylik, A va B ideallar uchun $AB \subseteq P$ va $A \nsubseteq P$ bo‘lsin. U holda $\forall a \in A \setminus P$ va $\forall b \in B$ elementlar uchun $ab \in AB \subseteq P$ bo‘lib, teorema shartiga ko‘ra $a \in P$ yoki $b \in P$ bo‘ladi. Lekin $a \notin P$ bo‘lganligi uchun $b \in P$ kelib chiqadi. Ushbu b elementling ixtiyoriyligidan $B \subseteq P$ munosabatni hosil qilamiz. Demak, P birlamchi ideal. $\square$

Ta’kidlash kerakki, 5.4.1-natijaning teskarisi R halqa kommutativ bo‘lgan holda to‘g‘ri bo‘lib, umumiy holda esa har doim ham o‘rinli emas. Chunki, agar R halqa kommutativ bo‘lib, P uning birlamchi ideali va $ab \in P$ bo‘lsa, u holda $\langle ab \rangle \subseteq P$ bo‘lib, R halqaning kommutativligidan $\langle a \rangle \langle b \rangle \subseteq \langle ab \rangle \subseteq P$ kelib chiqadi. Bundan esa, $\langle a \rangle \subseteq P$ yoki $\langle b \rangle \subseteq P$ ya’ni $a \in P$ yoki $b \in P$ hosil bo‘ladi. Demak, R halqa kommutativ bo‘lsa 5.4.1-natijaning teskarisi o‘rinli. Halqa kommutativ bo‘lmagan holda ushbu natijaning teskarisi o‘rinli bo‘lmasligiga biz guyidagi misolda javob beramiz.

5.4.4-misol. *$M_n(\mathbb{Z})$ matritsalar halqasi uchun $I = \{0\}$ ideal birlamchi ideal bo‘lib, $ab \in I$ ekanligidan $a \in I$ yoki $b \in I$ bo‘lishi har doim ham kelib chiqmaydi. Chunki, $M_n(\mathbb{Z})$ halqa nolning bo‘luvchilariga ega.*

5.4.5-misol. *$\mathbb{Z}$ butun sonlar halqasida $P = \{3k \mid k \in \mathbb{Z}\}$ iedal birlamchi ideal bo‘lib, $P = \{6k \mid k \in \mathbb{Z}\}$ iedal esa birlamchi emas.*

Quyidagi teoremada biri bor kommutativ halqada birlamchi idellarning xossasini keltiramiz

5.4.4-teorema. *Biri bor kommutativ R halqaning $P (P \neq R)$ ideali birlamchi bo‘lishi uchun R/P faktor halqa butunlik sohasi bo‘lishi zarur va yetarli.*

Isbot. ***Zaruriyligi.*** Aytaylik, R biri bor kommutativ halqa va P uning birlamchi ideali bo‘lsin. U holda R/P haktor halqa ham biri bor halqa bo‘lib, $1_R + P$ element uning birlik elementi bo‘ladi. $P \neq R$ va P birlamchi bo‘lganligi uchun $1_R + P \neq P$, chunki, $P = 0 + P$ element faktor halqaning nol elementi bo‘ladi. Endi R/P faktor halqada nolning bo‘luvchisi mavjud emasligini ko‘rsatamiz. Faraz qilaylik, $a + P$ va $b + P$ elementlar uchun $(a + P)(b + P) = 0 + P$ bo‘lsin, u holda $ab + P = P$ bo‘lib, $ab \in P$ ekanligi kelib chiqadi. Bundan esa, R halqaning kommutativligi va P idealning birlamchi ekanligini hisobga olsak, $a \in P$ yoki $b \in P$ kelib chiqadi. Bu esa, $a + P = 0 + P$ yoki $b + P = 0 + P$ ekanligini anglatadi. Ya'ni, R/P faktor halqa nolning bo'luvchisiga ega emas.

Yetarliligi. Aytaylik, R/P faktor halqa butunlik sohasi bo'lsin. Agar $ab \in P$ bo'lsa, u holda

$$0 + P = ab + P = (a + P)(b + P)$$

ekanligidan $a + P = 0 + P$ yoki $b + P = 0 + P$ kelib chiqadi. Bu esa, $a \in P$ yoki $b \in P$ ekanligini anglatadi. Bundan esa, R halqa kommutativ bo'lganligi uchun P idealning birlamchi ekanligi kelib chiqadi. □

Agar R halqa bosh ideallar sohasi bo'lsa, u holda quyidagiga ega bo'lamiz.

5.4.5-teorema. *Aytaylik, R bosh ideallar sohasi va P uning xosmas ideali bo'lsin. P ideal birlamchi ideal bo'lishi uchun uning tub element orqali hosil qilinishi zarur va yetarli.*

Isbot. Aytaylik, R bosh ideallar sohasi va $P = \langle p \rangle$ uning xosmas ideali bo'lsin. U holda $p \neq 0$ va $P \neq R$ bo'lib, p elementning teskarilanuvchi emasligini hosil qilamiz. Agar $ab \in R$ elementlar uchun $p|ab$ bo'lsa, u holda $ab = pc$ bo'lib, $ab \in P$ ekanligiga, bundan esa, $a \in P$ yoki $b \in P$ munosabatga ega bolamiz. Demak, $p|a$ yoki $p|b$, ya'ni p element tub element bo'ladi.

Va aksincha, agar p tub element uchun $P = \langle p \rangle$ idealni qarasak, u holda $ab \in P$ shartni qanoatlantiruvchi $a, b \in R$ elemnetlar uchun $p|ab$ kelib chiqib, bundan $p|a$ yoki $p|b$ hosil bo'ladi. Bu esa, $a \in P$ yoki $b \in P$ ekanligini, ya'ni P idealning birlamchiligini anglatadi.

□

Yuqoridagi teooremadan butun sonlar halqasining barcha birlamchi ideallari $0, \mathbb{Z}$ va $\langle p \rangle = \{pk \mid p \text{ tub son}\}$ ideallardan iborat bo'lishini hosil qilamiz.

Endi maxsimal ideal tushunchasini kiritamiz.

5.4.6-ta'rif. *Aytaylik, R halqa va unung M ideali berilgan bo'lsin. Agar $M \neq R$ bo'lib, R halqaning $M \subset I \subset R$ shrtni qanoatlantiruvchi I ideali mavjud bo'lmasa, u holda M ideal* ***maksimal ideal*** *deb ataladi.*

Maksimal chap va o'ng ideallar tushunchalari ham yuqoridagi ta'rif kabi kiritiladi.

5.4.6-misol. *$\mathbb{Z}$ butun sonlar halqasida $A = \{3k \mid k \in \mathbb{Z}\}$ iedal maksimal ideal bo'lib, $B = \{4k \mid k \in \mathbb{Z}\}$ iedal esa maksimal emas, chunki ushbu B ideal uchun $I = \{2k \mid k \in \mathbb{Z}\}$ ideal mavjud bo'lib, $B \subset I \subset \mathbb{Z}$.*

Takidlash joizki biri bor kommutativ halqaning ixtiyoriy maksimal ideali birlamchi ideal bo'ladi. Haqiqatdan ham, M ideal R halqaning maksimal ideali bo'lib, $a, b \in R$ elementlar uchun $ab \in M$ va $a \notin M$ bo'lsin. U holda

$\langle M, a\rangle = \{u + ra \mid u \in M, r \in R\}$ idealni qarasak, $M \subset \langle M, a\rangle$ bo‘lib, M ning maksimal ekanligidan $\langle M, a\rangle = R$ kelib chiqadi. Demak, $1 \in \langle M, a\rangle$, ya’ni shunday $u \in M, r \in R$ elementlar mavjud bo‘lib, $1 = u + ra$ bo‘ladi. Bundan esa, $b = bu + rab \in M$ ekanligi kelib chiqadi. Ya’ni M birlamchi ideal.

Quyidagi misolda esa, biri bor kommutativ halqada birlamchi ideal bo‘lib, maksimal bo‘lmagan idealga misol keltiramiz.

5.4.7-misol. *$R = \{(a, b) \mid a, b \in \mathbb{Z}\}$ to‘plamda*

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \cdot (c, d) = (ac, bd)$$

amallarni qarasak, $(R, +, \cdot)$ halqada $I = \{(a, 0) \mid a \in \mathbb{Z}\}$ to‘plam birlamchi ideal bo‘lib, maksimal bo‘lmaydi. Chunki, I idealni o‘z ichiga oluvchi $J = \{(a, b) \mid a \in \mathbb{Z}, b \in 2\mathbb{Z}\}$ ideal mavjud. Ya’ni $I \subset J \subset R$.

Ta’kidalsh joizki, agar kommutativ halqa birlik elementga ega bo‘lmasa, uning ixtiyoriy maksimal ideali birlamchi bo‘lishi shart emas.

5.4.8-misol. *$R = 2\mathbb{Z}$ juft sonlardan iborat halqada $I = 4\mathbb{Z}$ to‘plam maksimal ideal bo‘lib, lekin birlamchi ideal emas, chunki, $2 \notin I$ va $2 \cdot 2 = 4 \in I$.*

5.4.6-teorema. *Bosh ideallar sohasining xosmas P ideali birlamchi bo‘lishi uchun uning maksimal bo‘lishi zarur va yetarli.*

Isbot. Aytaylik, P birlamchi ideal bo‘lsin. U holda 5.4.5-teoremaga ko‘ra qandaydir p tub element uchun $P = \langle p\rangle$ bo‘ladi. Faraz qilaylik, qandaydir I ideal uchun $P \subset I, P \neq I$ bo‘lsin. U holda $a \in I \setminus P$ element mavjud. a va p elementlar o‘zaro tub bo‘lganligi uchun shunday $s, t \in R$ elementlar mavjudki $sa + tp = 1$ bo‘ladi. Bundan esa, $1 = sa + tp \in I$ kelib chiqadi. Demak, $I = R$, ya’ni P maksimal ideal. □

Endi 5.4.4-teoremaning maksimal ideallar uchun analogini keltiramiz.

5.4.7-teorema. *Biri bor kommutativ R halqaning M ideali maksimal bo‘lishi uchun R/M faktor halqa maydon bo‘lishi zarur va yetarli.*

Isbot. ***Zaruriyligi.*** Aytaylik, M maksimal ideal bo‘lsin. R/M halqa ham kommutativ biri bor halqa bo‘lib, ixtiyoriy noldan farqli $a + M \in R/M$ element olsak, $a \notin M$ bo‘ladi. Agar $\langle M, a\rangle$ idealni qarasak, ushbu ideal M ni o‘z ichiga oluvchi M dan farqli ideal bo‘lib, M maksimal bo‘lganligi uchun $\langle M, a\rangle = R$ bo‘ladi. Demak, $1 \in \langle M, a\rangle$, ya’ni shunday $m \in M$ va $r \in R$ elementlar topiladiki, $m+ra = 1$ bo‘ladi. Bu esa $m+ra+M = 1+M$, ya’ni $ra+M = 1+M$, ekanligini bildiradi. Bundan esa $(a+M)(r+M) = 1+M$ ekanligini ya’ni $a+M$ elementning teskarilanuvchiligini hosil qilamiz. Demak, R/M halqa kommutativ biri bor halqa bo‘lib uning ixtiyoriy elementi teskarilanuvchi bo‘ldi, ya’ni R/M maydon.

Yetarliligi. Aytaylik, R/M maydon bo‘lsin. U holda $M \neq R$. Agar I ideal uchun $M \subset I$, bo‘lsa, u holda $a \in I \setminus M$ element uchun $a + M$ element R/M maydonning noldan farqli elementi bo‘ladi. maydonning ixtiyoriy noldan farqli elementi teskarilanuvchi bo‘lganligi uchun shunday $r \in R \setminus M$ element mavjudki, $(a + M) \cdot (r + M) = 1 + M$, ya’ni $1 - ar \in M$. Bundan esa, $1 = m + ar \in I$ ekanligini, ya’ni $I = R$ tenglikni hosil qilamiz. Demak, M maksimal ideal.

□

Endi yana bir muhim ideal bo‘lgan primar ideal tushunchasini kiritamiz. Qayt etish joizki, primar ideal tushunchasining kiritilishini butun sonlar halqasidagi $\langle p^k \rangle$ ko‘rinishidagi halqalar bilan izohlash mumkin. Arifmetikaning asosiy teoremasiga ko‘ra ixtiyoriy n butun sonni $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ ko‘rinishida ifodalash mumkin. Bu yerdagi p_i tusb sonlar orqali hosil qilingan $\langle p_i \rangle$ ideallar $\mathbb{Z}$ halqaning birlamchi ideallari bo‘lsa, $\langle p_i^{\alpha_i} \rangle$ ideallar esa primar ideallar bo‘ladi.

5.4.7-ta’rif. *Aytaylik, R kommutativ halqaning Q ideali berilgan bo‘lsin. Agar $ab \in Q$, $a \notin Q$ shartni qanoatlantiruvchi ixtiyoriy $a, b \in R$ elementlar uchun shunday n natural son topilib, $b^n \in Q$ bo‘lsa, u holda Q ideal primar ideal deb ataladi.*

Ta’rifdan ko‘rinadiki, ixtiyoriy birlamchi ideal primar ideal bo‘ladi. Quyidagi misolda esa, yuqorida aytilganidek, $\langle p^k \rangle$ ko‘rinishidagi ideallarning butun sonlar halqasida primar ideal bo‘lishini ko‘rsatamiz.

5.4.9-misol. *Butun sonlar halqasining $\langle p^k \rangle$ ko‘rinishidagi ideali primar ideal bo‘ladi. Ta’kidlash joizki, $k \geq 2$ bo‘lganda $\langle p^k \rangle$ ideal birlamchi ideal bo‘lmaydi. Biz uning primar ekanligini ko‘rsatamiz. Aytaylik, $ab \in \langle p^k \rangle$ bo‘lib, $a \notin \langle p^k \rangle$ bo‘lsin. U holda shunday $r \in \mathbb{Z}$ son topilib, $ab = rp^k$ bo‘ladi. a soni p^k ga bo‘linmaganligi uchun b soni p ga bo‘linishini, ya’ni $b = qp$ ekanligini hosil qilamiz. Bundan esa, $b^k = q^k p^k \in \langle p^k \rangle$ ekanligi kelib chiqadi. Demak, $\langle p^k \rangle$ primar ideal.*

5.4.8-ta’rif. *Aytaylik, R kommutativ halqa va uning I ideali berilgan bo‘lsin. Quyidagi*

$$\{a \in R \mid a^k \in I \text{ qandaydir } k \in \mathbb{N} \text{ uchun}\}$$

to‘plamga I halqaning ***radikali*** *deb ataladi va $\sqrt{I}$ kabi belgilanadi.*

Ta’kidlash joizki, ixtiyoriy I ideal uchun $I \subseteq \sqrt{I}$ bo‘lib, $\sqrt{I}$ ham ideal bo‘ladi. Chunki, agar $a, b \in \sqrt{I}$ bo‘lsa, u holda shunday n va m natural sonlari uchun $a^n, b^m \in I$. Bundan esa, $(a - b)^{n+m} \in I$ ekanligi kelib chiqadi, ya’ni $a - b \in \sqrt{I}$. Agar $r \in R$ va $a \in I$ bo‘lsa, u holda $(ra)^n = r^n a^n \in I$ ekanligidan $ra \in \sqrt{I}$ hosil bo‘ladi. Demak, $\sqrt{I}$ ideal.

5.4.2-tasdiq. *Agar R kommutativ halqaning Q ideali primar bo‘lsa, u holda $\sqrt{Q}$ ham primar bo‘ladi.*

Isbot. Aytaylik, $a, b \in R$ elementlar uchun $ab \in \sqrt{Q}$ va $a \notin \sqrt{Q}$ bo‘lsin. U holda qandaydir n natural son uchun $(ab)^n \in Q$. Bundan esa, $a^n b^n \in Q$, lekin $a^n \notin Q$ kenligi kelib chiqadi. Q ideal primar bo‘lganligi uchun shunday $m \in \mathbb{N}$ son topilib, $(b^n)^m \in Q$. Demak, $b \in \sqrt{Q}$ ya’ni Q primar ideal.

□

Quyidagi teoremada kommutativ R halqaning I primar idealini R/I faktor halqa bilan xarakterlovchi xossani keltiramiz

5.4.8-teorema. *R kommutativ halqaning I ideali primar bo‘lishi uchun R/I faktor halqadagi ixtiyoriy nolning bo‘luvchisi nilpotent element bo‘lishi zarur va yetarli.*

Isbot. ***Zaruriyligi.*** Aytaylik, I primar ideal bo‘lib, $a + I$ element R/I faktor halqada nolning bo‘luvchisi bo‘lsin. U holda shunday $b + I \in R/I$ element uchun $(a + I)(b + I) = I$ bo‘ladi. Bundan esa, $ab \in I$ kelib chiqadi. I halqaning primarligini va $b \notin I$ ekanligini hisobga olsak, qandaydir $n \in \mathbb{N}$ natural son uchun $a^n \in I$ bo‘lishini hosil qilamiz. Demak, $(a+I)^n = a^n+I = I$, ya’ni $a+I$ nilpotent.

Yetarliligi. Aytaylik, R/I faktor halqadagi ixtiyoriy nolning bo‘luvchisi nilpotent bo‘lib, $a, b \in R$ elementlar uchun $ab \in I$ va $a \notin I$ bo‘lsin. U holda $(a + I)(b + I) = ab + I = I$. Agar $b + I$ element nolning bo‘luvchisi bo‘ladi. Bundan esa uning nilpotent ekanligi, ya’ni $(b + I)^n = b^n + I = I$ bo‘lishi kelib chiqadi. U holda $b^n \in I$ bo‘’lib, I idealning primar ekanligini hosil qilamiz.

□

5.4.10-misol. *Ixtiyoriy ideali birlamchi ideal bo‘ladigan butunlik sohasi maydon bo‘lishini isbotlang.*

Yechish. Aytaylik, R butunlik sohasi bo‘lsin. U holda ixtiyoriy noldan farqli $a \in R$ element uchun a^2R idealni qaraymiz. Ushbu udeal birlamchi ideal bo‘lganligi uchun $a^2 \in a^2R$ munosabatdan $a \in a^2R$ kelib chiqadi. Demak, qandaydir, $b \in R$ element topilib, $a = a^2b$. Bundan esa, $a(1 - ab) = 0$ tenglikni hamda $a \neq 0$ bo‘lganligi uchun $ab = 1$ bo‘lishini hosil qilamiz. Demak, R butunlik sohasining ixtiyoriy noldan farqli a elementi teskarilanuvchi ekan, ya’ni R maydon.

□

5.4.11-misol. *$\langle x \rangle$ ideal $\mathbb{Z}[x]$ halqaning birlamchi ideali bo‘lib, maksimal bo‘lmasligini ko‘rsating.*

Yechish. Aytaylik, $\mathbb{Z}[x]$ halqaning

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad g(x) = b_0 + b_1x + \cdots + b_bx^b$$

elementlari uchun $f(x)g(x) \in \langle x \rangle$ bo'lsin. U holda, $a_0b_0 = 0$ bo'lib, $a_0 = 0$ yoki $b_0 = 0$ bo'ladi. Bundan esa, $f(x) \in \langle x \rangle$ yoki $g(x) \in \langle x \rangle$ kelib chiqadi. Demak, $\langle x \rangle$ birlamchi ideal.

Endi ushbu idealning maksimal ekanligini ko'rsatamiz. Agar $\langle x, 2 \rangle$ idealni qarasak, ushbu ideal uchun $\langle x \rangle \subset \langle x, 2 \rangle \subset \mathbb{Z}[x]$ munosabat o'rinli bo'lib, bundan $\langle x \rangle$ idealning maksimal emasligi kelib chiqadi. $\square$

5.4.12-misol. *$\langle x^2 \rangle$ ideal $\mathbb{Z}[x]$ halqaning primar ekanligini ko'rsating.*

Yechish. Aytaylik, $\mathbb{Z}[x]$ halqaning

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad g(x) = b_0 + b_1x + \cdots + b_bx^b$$

elementlari uchun $f(x)g(x) \in \langle x^2 \rangle$ va $f(x) \notin \langle x^2 \rangle$ bo'lsin. U holda, $a_0b_0 = 0$ va $a_0b_1 + a_1b_0 = 0$ bo'lib, $a_0 \neq 0$ yoki $a_1 \neq 0$.

Agar $a_0 \neq 0$ bo'lsa, u holda $b_0 = b_1 = 0$, ya'ni $g(x) \in \langle x^2 \rangle$. Agar $a_0 = 0$ bo'lsa, u holda $a_1 \neq 0$ bo'lib, bundan $b_0 = 0$, ya'ni $(g(x))^2 \in \langle x^2 \rangle$ kelib chiqadi. Demak, $\langle x^2 \rangle$ primar ideal. $\square$

5.4.3 Mustaqil ishlash uchun misol va masalalar

1. $\overline{2} \in \mathbb{Z}_10$ elementning tub bo'lib, keltiriluvchi ekanligini ko'rsating.

2. $2 + i\sqrt{5}$ element $\mathbb{Z}[i\sqrt{5}]$ halqaning keltirilmas, lekin tub bo'lmagan elementi ekanligini ko'rsating.

3. $\mathbb{Z}[i]$ halqaning $2 - i, 1 + i$ va 11 elementlari keltirilmas ekanligini isbotlang.

4. $\mathbb{Z}_9$ halqaning barcha tub va keltirilmas elementlarini aniqlang.

5. Agar $\mathbb{Z}[i]$ halqaning $a+bi$ elementi uchun a^2+b^2 soni tub son bo'lsa, u holda $a + bi \in \mathbb{Z}[i]$ elementning tub ekanligini isbotlang.

6. Agar $\mathbb{Z}[i\sqrt{3}]$ halqaning $a + bi\sqrt{3}$ elementi uchun $a^2 + 3b^2$ soni tub son bo'lsa, u holda $a + bi \in \mathbb{Z}[i]$ elementning keltirilmas ekanligini isbotlang.

7. Quyidagi halqalarning barcha maksimal ideallarini toping:
$$\mathbb{Z}_6, \quad \mathbb{Z}_8, \quad \mathbb{Z}_{10}, \quad \mathbb{Z}_{12}, \quad \mathbb{Z}_{18}, \quad \mathbb{Z}_{25}.$$

8. Quyidagi halqalarning barcha birlamchi ideallarini toping:
$$\mathbb{Z}_6, \quad \mathbb{Z}_8, \quad \mathbb{Z}_{10}, \quad \mathbb{Z}_{12}, \quad \mathbb{Z}_{16}, \quad \mathbb{Z}_{18}.$$

9. $I = \{(5n, m) \mid n, m \in \mathbb{Z}\}$ ideal $\mathbb{Z} \times \mathbb{Z}$ halqaning maksimal ideali ekanligini ko'rsating.

10. $I = \{a_0 + a_1x + \dots a_nx^n \ | a_0 = 3k\}$ ideal $\mathbb{Z}[x]$ halqaning birlamchi ideali ekanligini koʻrsating.

11. Biri bor chekli kommutativ halqaning ixtiyoriy xosmas birlamchi ideali maxsimal ekanligini isbotlang.

12. Bul halqasining ixtiyoriy xosmas birlamchi ideali maxsimal ekanligini isbotlang.

13. Biri bor R halqaning xosmas I ideali maksimal boʻlishi uchun R/I faktor halqaning sodda boʻlishi zarur va yetarli ekanligini isbotlang.

14. Aytaylik R halqaning I ideali berilgan boʻlsin. U holda R/I faktor halqaning ixtiyoriy P birlamchi ideali uchun $I \subseteq J$ va $J/I = P$ shartlarni qanoatlantiruvchi J birlamchi ideal mavjud ekanligini isbotlang.

15. Ixtiyoriy r haqiqiy son uchun $I_r = \{f(x) \in \mathbb{R}[x] \mid f(r) = 0\}$ toʻplam $\mathbb{R}[x]$ halqaning maksimal ideali ekanligini isbotlang.

16. Ixtiyoriy $\mathbb{K}$ maydon uchun $\mathbb{K}[x]$ koʻphadlar halqasi va ixtiyoriy $a \in K$ element uchun $\varphi_a(f(x)) = f(a)$ kabi $\varphi_a : \mathbb{K}[x] \to K$ akslantirish aniqlangan boʻlsin. U holda ushbu φ_a akslantirishning epimorfizm ekanligini koʻrsating va $\mathrm{Ker}\varphi_a$ toʻplam $\mathbb{K}[x]$ halqaning maksimal ideali boʻlishini isbotlang.

17. Biri bor kommutativ halqaning I_1 va I_2 ideallari uchun $\sqrt{I_1 \cap I_2} = \sqrt{I_1} \cap \sqrt{I_2}$ ekanligini isbotlang.

18. $\mathbb{Z}[x]$ halqaning $\langle x, 4\rangle$ ideali primar ideal ekanligini isbotlang.

19. $\mathbb{Z}[x]$ halqaning $\langle x, 6\rangle$ ideali primar ideal emasligini koʻrsating.

20. Bosh ideallar sohasining ixtiyoriy notrivial I idealini $I = P_1P_2 \dots P_n$ koʻrinishida birlamchi ideallarning koʻpaytmasi shaklida ifodalanishini isbotlang.

5.5 Halqalarning toʻgʻri yigʻindisi

Bizga A va B halqalar berilgan boʻlsin. Ushbu toʻplamlarning $A \times B$ dekart koʻpaytmasida quyidagi amallarni aniqlaymiz

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2), \quad (a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2),$$

bu yerda $a_1, a_2 \in A$, $b_1, b_2 \in B$ boʻlib, birinchi va ikkinchi komponentalar boʻyicha yigʻindi va koʻpaytmalar mos ravishda A va B halqalardagi aniqlangan amallardir.

Tekshirish qiyin emaski, $A \times B$ to‘plam yuqorida aniqlangan amallarga nisbatan halqa tashkil qiladi hamda ushbu halqa A va B halqalarning **to‘g‘ri yig‘indisi** deb ataladi va $A \oplus B$ kabi belgilanadi. Ushbu halqada nol element $(0,0)$ ko‘rinishida bo‘lib, agar A va B halqalar birlik elementli halqalar bo‘lsa, u holda $(1,1)$ element birlik element vazifasini bajaradi. A va B halqalarning to‘g‘ri yig‘indisi nolning bo‘luvchilariga ega bo‘lgan halqa hisoblanadi, chunki, $(a,0) \cdot (0,b) = (0,0)$ ekanligidan $(a,0)$ va $(0,b)$ ko‘rinishidagi elementlar nolning bo‘luvchisi ekanligi kelib chiqadi.

Biz yuqorida ikkita halqaning to‘g‘ri yig‘indisini aniqlagan bo‘lsak, induktiv tarzda bir nechta $R_1, R_2, \dots, R_n$ halqalarning to‘g‘ri yig‘indisini ham aniqlash mumkin, ya’ni $R_1 \times R_2 \times \cdots \times R_n$ to‘plamda har bir komponenta bo‘yicha qo‘shish va ko‘paytirish amallarini aniqlash orqali halqa hosil qilish mumkin.

5.5.1-misol. $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ *halqaning elementlari*

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

ko‘rinishida bo‘lib, $(\overline{0},\overline{0})$ *halqaning nol elementi* $(\overline{1},\overline{1})$ *esa halqaning birlik elementi bo‘ladi.*

Ta’kidlash joizki, ushbu halqa $\mathbb{Z}_6$ *halqaga izomorf, chunki, quyidagicha aniqlangan*

$$f\big((\overline{0},\overline{0})\big) = \overline{0}, \quad f\big((\overline{1},\overline{1})\big) = \overline{1}, \quad f\big((\overline{0},\overline{2})\big) = \overline{2}$$
$$f\big((\overline{1},\overline{0})\big) = \overline{3}, \quad f\big((\overline{0},\overline{1})\big) = \overline{4}, \quad f\big((\overline{1},\overline{2})\big) = \overline{5}$$

akslantirish $\mathbb{Z}_2 \times \mathbb{Z}_3$ *halqani* $\mathbb{Z}_6$ *halqaga o‘tkazuvchi izomorfizm bo‘ladi.*

Quyidagi tasdiqda esa, n va m sonlar o‘zaro tub bo‘lgan holda $\mathbb{Z}_n \oplus \mathbb{Z}_m$ halqaning $\mathbb{Z}_{nm}$ halqaga izomorf ekanligini ko‘rsatamiz.

5.5.1-tasdiq. *Agar n va m sonlari o‘zaro tub bo‘lsa, u holda $\mathbb{Z}_n \oplus \mathbb{Z}_m$ va $\mathbb{Z}_{nm}$ halqalar izomorf.*

Isbot. Tasdiqni isbotlash uchun $\mathbb{Z}_n \oplus \mathbb{Z}_m$ halqadan $\mathbb{Z}_{nm}$ halqaga izomorfizm quramiz. Ma’lumki, f izomorfizm nol elementni nol elementga birlik elementni birlik elementga o‘tkazadi. Shuning uchun

$$f\big((\overline{0},\overline{0})\big) = \overline{0}, \quad f\big((\overline{1},\overline{1})\big) = \overline{1}.$$

Endi $\mathbb{Z}_n \oplus \mathbb{Z}_m$ halqaning $a = (\overline{1},\overline{1})$ elementini olib,

$$(\overline{0},\overline{0}), \quad a, \quad a+a, \quad a+a+a, \quad \dots, \quad \underbrace{a+a+\cdots+a}_{n+m-1 \text{ ta}}$$

elementlarni qarab chiqsak, n va m sonlari o‘zaro tub bo‘lganligi uchun ushbu elementlar turli xil bo‘lib, ular $\mathbb{Z}_n \oplus \mathbb{Z}_m$ halqaning barcha elementlarini beradi.

Agar $\mathbb{Z}_{nm}$ halqaning $\overline{k}$ elementini $\underbrace{a+a+\cdots+a}_{k\ \text{ta}}$ elementga mos qo‘yuvchi akslantirishni qarasak, ushbu akslantirish $\mathbb{Z}_{nm}$ halqani $\mathbb{Z}_n \oplus \mathbb{Z}_m$ halqaga o‘tkazuvchi o‘zaro bir qiymatli akslantirish bo‘lib, qo‘shish va ko‘paytirish amallarini saqlaydi. Demak, ushbu akslantirish izomorfizm bo‘ladi. Ya’ni $\mathbb{Z}_n \oplus \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$. $\square$

Yuqoridagi tasdiqdan ko‘rinadiki, $\mathbb{Z}_{nm}$ halqaning $\overline{k}$ elementini $\mathbb{Z}_n \oplus \mathbb{Z}_m$ halqaning $(\overline{k}(mod\, n), \overline{k}(mod\, m))$ elementiga o‘tkazuvchi $f : \mathbb{Z}_{nm} \to \mathbb{Z}_n \oplus \mathbb{Z}_m$ akslantirish izomorfizm bo‘ladi. Ushbu tasdiqni umumlashtirgan holda quyidagi natijaga ega bo‘lamiz.

5.5.1-natija. *Agar juft-jufti bilan o‘zaro tub bo‘lgan $n_1, n_2, \ldots, n_s$ butun sonlari berilgan bo‘lsa, u holda $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s}$ halqa $\mathbb{Z}_{n_1 n_2 \ldots n_s}$ halqaga izomorf bo‘ladi.*

Bizga A va B halqalar va ularning $R = A \oplus B$ to‘g‘ri yig‘indisi berilgan bo‘lsin. U holda

$$I_1 = \{(a,0) \mid a \in A\} \quad \text{va} \quad I_2 = \{(0,b) \mid b \in B\}$$

to‘plamlar $A \times B$ halqaning idealari bo‘lib, $I_1 \cap I_2 = \{(0,0)\}$ bo‘ladi. Bundan tashqari, $R = A \oplus B$ halqaning ixtiyoriy $x \in R$ elementini yagona ravishda

$$x = y + z, \quad y \in I_1,\ z \in I_2$$

kabi ifodalash mumkin.

5.5.2-tasdiq. *Agar R halqaning I_1 va I_2 ideallari berilgan bo‘lib, $I_1 \cap I_2 = \{0\}$ va ixtiyoriy $x \in R$ elementni $x = y + z$, $y \in I_1,\ z \in I_2$ kabi ifodalash mumkin bo‘lsa, u holda $R \simeq I_1 \oplus I_2$ bo‘ladi.*

Isbot. Agar $I_1 \cap I_2 = \{0\}$ ekanligidan foydalansak, ixtiyoriy $x \in R$ elementni $x = y + z$, $y \in I_1,\ z \in I_2$ kabi yagona ravishda ifodalash mumkinligi kelib chiqadi. Chunki, agar $x = y_1 + z_1 = y_2 + z_2$ bo‘lsa, u holda $y_1 - y_2 = z_2 - z_1 \in I_1 \cap I_2 = \{0\}$. Bundan esa, $y_1 = y_2$ va $z_1 = z_2$ kelib chiqadi. Bundan foydalangan holda R halqadan $I_1 \oplus I_2$ halqaga $f(x) = (y,z)$ kabi akslantirish aniqlaymiz, bu yerda $x = y + z$, $y \in I_1,\ z \in I_2$.

Ushbu $f : R \to I_1 \oplus I_2$ akslantirish biyektiv akslantirish bo‘ladi. Endi uning gomomorfizm ekanligini ko‘rsatamiz. Agar $x_1, x_2 \in R$ elementlar berilib, $x_1 = y_1 + z_1$, $x_2 = y_2 + z_2$, bo‘lsa, u holda

$$x_1 + x_2 = y_1 + z_1 + y_2 + z_2 = (y_1 + y_2) + (z_1 + z_2),$$

$$x_1 \cdot x_2 = (y_1 + z_1) \cdot (y_2 + z_2) = y_1 \cdot y_2 + y_1 \cdot z_2 + z_1 \cdot y_2 + z_1 \cdot z_2 = y_1 \cdot y_2 + z_1 \cdot z_2.$$

Bundan esa

$$f(x_1 + x_2) = f\big(y_1 + y_2 + z_1 + z_2\big) = (y_1 + y_2, z_1 + z_2) = (y_1, z_1) + (y_2 + z_2) = f(x_1) + f(x_2),$$

$f(x_1 \cdot x_2) = f\big(y_1 \cdot y_2 + z_1 \cdot z_2\big) = (y_1 \cdot y_2, z_1 \cdot z_2) = (y_1, z_1) \cdot (y_2 + z_2) f(x_1) + f(x_2)$ kelib chiqadi. Demak, f akslantirish biyektiv gomomorfizm, ya’ni izomorfizm bo‘ladi. $\square$

Agar A va B halqalar birlik elementli halqalar bo‘lsa, u holda $(1, 0)$ va $(0, 1)$ elementlar $A \oplus B$ halqaning idempotent elementlari bo‘lib, ularning yig‘indisi $A \oplus B$ halqaning birlik elementi bo‘ladi. Ya’ni, $e = (1, 0)$ deb belgilasak, e va $1 - e$ elementlar $A \oplus B$ halqaning idempotent elementlari bo‘lib,

$$A \simeq eR, \quad B \simeq (1 - e)R.$$

Boshqacha qilib aytganda

$$R \simeq eR \oplus (1 - e)R$$

munosabat o‘rinli. Shunday qilib biz agar R halqa birlik elementli A va B halqalarning to‘g‘ri yig‘indisidan iborat bo‘lsa, u holda R halqadagi $e = (1, 0)$ idempotent element uchun $R \simeq eR \oplus (1 - e)R$ munosabat o‘rinli ekanligini ko‘rsatdik. Quyidagi tasdiqda esa, ushbu munosabatning teskarisi ham o‘rinli ekanligini ko‘rsatamiz.

5.5.3-tasdiq. *Agar birlik elementli kommutativ R halqa e idempotent elementga ega bo‘lsa, u holda R halqa eR va $(1-e)R$ halqalarning to‘g‘ri yig‘indisiga izomorf bo‘ladi.*

Isbot. Bizga R halqaning e idempotent elementi berilgan bo‘lsin, u holda $1-e$ element ham idempotent bo‘ladi, chunki,

$$(1 - e)(1 - e) = 1 - e - e + e^2 = 1 - e - e + e = 1 - e.$$

Endi eR va $(1 - e)R$ to‘plamlarni qarasak, R halqa kommutativ bo‘lganligi uchun ular ideal tashkil qiladi. Bundan tashqari, ixtiyoriy $x \in R$ elementni

$$x = ex + x - ex = ex + (1 - e)x$$

kabi eR va $(1 - e)R$ ideallardan olingan ex va $(1 - e)x$ elementlarning yig‘indisi shaklida ifodalash mumkin.

Endi, $eR \cap (1 - e)R = \{0\}$ ekanligini ko‘rsatamiz. Aytaylik, $a \in eR \cap (1 - e)R$ bo‘lsin, u holda shunday $b, c \in R$ elementlar topilib, $a = eb$ va $(1 - e)c$. Bu tengliklardan esa, $ea = e^2 b = eb = a$ va $ea = e(1 - e)c = (e - e)c = 0$ ekanligini, ya’ni $a = 0$ bo‘lishini hosil qilamiz. Demak, $eR \cap (1 - e)R = \{0\}$ va 5.5.2-tasdiqqa ko‘ra $R \simeq eR \oplus (1 - e)R$ kelib chiqadi. $\square$

Ta’kidlash joizki, 5.5.3-tasdiq R birlik elementli halqa kommutativ bo‘lmasdan, e idempotent R halqaning markaziga tegishli bo‘lgan holda ham o‘rinli bo‘ladi. Chinki, agar $e \in C(R)$ bo‘lsa, u holda R halqa kommutativ bo‘lmasa ham eR va $(1 - e)R$ to‘plamlarning ikki tomonli ideal ekanligi kelib chiqadi.

5.5.1 Mustaqil ishlash uchun misol va masalalar

1. p tub son uchun $\mathbb{Z}_{p^2}$ halqani ikkita halqaning to‘g‘ri yig‘indisi shaklida ifodalash mumkin emasligini ko‘rsating.

2. Haqiqiy sonlar maydoni ustida uzluksiz funksiyalar halqasi ikkita halqaning to‘g‘ri yig‘indisi shaklida ifodalash mumkin emasligini ko‘rsating.

3. $(a, b) \in A \oplus B$ element teskarilanuvchi bo‘lishi uchun a va b elementlarning teskarilanuvchi bo‘lishi zarur va yetarli ekanligini isbotlang.

4. Quyidagi halqalarning qaysilari o‘zaro izomorf ekanligini aniqlang.
   - $\mathbb{Z}_{24}$ va $\mathbb{Z}_{12} \oplus \mathbb{Z}_2$.
   - $\mathbb{Z}_{24}$ va $\mathbb{Z}_6 \oplus \mathbb{Z}_4$.
   - $\mathbb{Z}_6 \oplus \mathbb{Z}_4$ va $\mathbb{Z}_{12} \oplus \mathbb{Z}_2$.
   - $\mathbb{Z}_{24}$ va $\mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
   - $\mathbb{Z}_{24}$ va $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$.
   - $\mathbb{Z}_6 \oplus \mathbb{Z}_4$ va $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$.
   - $\mathbb{Z}_{12} \oplus \mathbb{Z}_2$ va $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$.
   - $\mathbb{Z}_8 \oplus \mathbb{Z}_3$ va $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$.

5.6 Nyotr va Artin halqalari

Ushbu paragrafda biz maxsus halqalar bo‘lgan Nyotr va Artin halqalari haqida gaplashamiz. Ta’kidlash joizki, Nyotr va Artin halqalari mos ravishda o‘suvchi va kamayuvchi zanjirlarning uzilish shartlari orqali beriladi.

Bizga R halqa va uning $A_1, A_1, \dots, A_s, \dots$ ideallari berilgan bo‘lsin.

5.6.1-ta’rif. *Agar R halqadagi ixtiyoriy o‘suvchi ideallar ketma-ketligi*

$$A_1 \subseteq A_2 \subseteq \cdots \subseteq A_s \subseteq \dots$$

uchun shunday n soni topilib, $A_n = A_{n+1} = \dots$ munosabat o‘rinli bo‘lsa, u holda R halqa ***o‘suvchi zanjirlarning uzilish shartini*** *qanoatlantiradi deb ataladi.*

5.6.2-ta’rif. *Agar R halqadagi ixtiyoriy kamayuvchi ideallar ketma-ketligi*

$$A_1 \supseteq A_2 \supseteq \cdots \supseteq A_s \supseteq \dots$$

uchun shunday n soni topilib, $A_n = A_{n+1} = \dots$ munosabat o‘rinli bo‘lsa, u holda R halqa ***kamayuvchi zanjirlarning uzilish shartini*** *qanoatlantiradi deb ataladi.*

Boshqacha qilib aytganda, ixtiyoriy qat'iy o'suvchi (kamayuvchi) zanjiri chekli bo'lgan halqaga o'suvchi zanjirlarning uzilish shartini (kamayuvchi zanjirlarning uzilish shartini) qanoatlantiradi deyiladi.

5.6.1-misol. *Butun sonlar halqasi $\mathbb{Z}$ o'suvchi zanjirlarning uzilish shartini qanoatlantirib, kamayuvchi zanjirlarning uzilish shartini qanoatlantirmaydi. Haqiqatdan ham, agar $\mathbb{Z}$ halqaning*

$$A_1 \subseteq A_2 \subseteq \dots \subseteq A_s \subseteq \dots$$

o'suvchi zanjiri berilgan bo'lsa, u holda qandaydir m_i sonlar uchun $A_i = m_i\mathbb{Z}$ bo'lib, $m_{i+1}|m_i$ munosabat o'rinli bo'ladi. m_1 son chekli bo'lganligi va uning bo'luvchilari cheklita ekanligidan ixtiyoriy qat'iy o'suvchi zanjir chekli ekanligi kelib chiqadi. Demak, $\mathbb{Z}$ halqa o'suvchi zanjirlarning uzilish shartini qanoatlantiradi.

Lekin $\mathbb{Z}$ halqada cheksiz ko'p ideallardan iborat

$$2\mathbb{Z} \supseteq 4\mathbb{Z} \supseteq \dots \supseteq 2^s\mathbb{Z} \supseteq \dots$$

kamayuychi zanjir mavjud. Shuning uchun $\mathbb{Z}$ halqa kamayuvchi zanjirlarning uzilish shartini qanoatlantirmaydi.

5.6.3-ta'rif. *O'suvchi zanjirlarning uzilish shartini qanoatlantiruvchi halqa **Nyotr halqasi** deb ataladi.*

*Kamayuvchi zanjirlarning uzilish shartini qanoatlantiruvchi halqa **Artin halqasi** deb ataladi.*

Yuqoridagi 5.6.1-misoldan ko'rinadiki, butun sonlar halqasi Nyotr halqasi bo'lib, Artin halqasi bo'lmaydi. Bundan tashqari, ixtiyoriy chekli halqalar ham Nyotr, ham Artin halqasiga misol bo'ladi. Quyidagi misolda esa, Nyotr halqasi ham Artin halqasi ham bo'lmaydigan halqaga misol keltiramiz.

5.6.2-misol. $[0, 1]$ *kesmada uzluksiz bo'lgan funksiyalar to'plamida qo'shish va ko'paytirish amallarini*

$$(f + g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x)g(x)$$

kabi aniqlasak, u holda $C[0, 1]$ to'plam ushbu amallarga nisbatan halqa bo'lib, bu halqa Nyotr halqasi ham Artin halqasi ham bo'lmaydi. Chunki, ushbu halqada

$$A_n = \{f \in C[0, 1] \mid f(x) = 0,\ 0 \leq x \leq \frac{1}{n}\},$$

$$B_n = \{f \in C[0, 1] \mid f(x) = 0,\ \frac{1}{n} \leq x \leq 1\},$$

ideallarni qarasak, $A_1 \subset A_2 \subset \dots \subset A_s \subset \dots$ cheksiz o'suvchi zanjir bo'lsa $B_1 \supset B_2 \supset \dots \supset B_s \supset \dots$ esa cheksiz kamayuvchi zanjir bo'ladi.

Ta'kidlash joizki, biz Nyotr va Artin halqalarining ta'riflarini halqaning ikki tomonli ideallaridan iborat zanjirlar orqali kiritdik. Faqat chap (o'ng) ideallardan iborat zanjirlar orqali chap (o'ng) Nyotr va Artin halqalari ta'riflarini yuqoridagi kabi kiritish mumkin.

Endi Nyotr halqalarining hususiyatini ta'riflovchi quyidagi teoremani keltiramiz.

5.6.1-teorema. *Berilgan R halqa uchun quyidagilar ekvivalent.*

1) R halqa Nyotr halqasi.

2) R halqaning ixtiyoriy ideallar sinfi maksimal elementga ega.

3) R halqaning ixtiyoriy ideali chekli hosil qiluvchili ideal.

Isbot. 1) $\Rightarrow$ 2). Aytaylik, R halqa Nyotr halqasi bo'lib, uning $\mathcal{I}$ ideallar sinfi berilgan bo'lsin. Ixtiyoriy $A_1 \in \mathcal{I}$ elementni, ya'ni R halqaning $\mathcal{I}$ sinfida yotadigan ixtiyoriy idealini olaylik. Agar A_1 ideal $\mathcal{I}$ sinfning maksimal elementi bo'lmasa, uni o'z ichiga oluvchi A_2 ideal mavjud. Xuddi shunday, agar A_2 ideal ham maksimal element bo'lmasa, u holda uni o'z ichiga oluvchi A_3 ideal mavjud. Ushbu jarayonni davom ettirish natijasida $A_1 \subset A_2 \subset A_3 \subset \dots \subset A_k \subset \dots$ o'suvchi zanjir hosil qilamiz. R halqa Nyotr halqasi bo'lganligi uchun shunday n soni topilib, $A_n = A_{n+1} = \dots$ o'rinli bo'ladi. Ushbu A_n ideal esa, $\mathcal{I}$ ideallar sinfining maksimal elementi bo'ladi.

2) $\Rightarrow$ 3). Aytaylik, R halqadagi ixtiyoriy $\mathcal{I}$ ideallar sinfi maksimal elementga ega bo'lib, R halqaning ixtiyoriy A ideali berilgan bo'lsin. U holda $a_1 \in A$ element uchun $\langle a_1 \rangle$ idealni qaraymiz. Agar $\langle a_1 \rangle = A$ bo'lsa, u holda A ideal bitta hosil qiluvchili ideal bo'lib, tasdiq isboti kelib chiqadi. Agar $\langle a_1 \rangle \subset A$ bo'lsa, u holda $a_2 \in A$, $a_2 \notin \langle a_1 \rangle$ elementni olib, $\langle a_1, a_2 \rangle$ idealni qaraymiz. Ushbu jarayonni davom ettirgan holda

$$\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \dots \subset \langle a_1, a_2, \dots, a_n \rangle \subset \dots$$

ideallarni hosil qilamiz. Agar $\mathcal{I} = \{\langle a_1 \rangle, \langle a_1, a_2 \rangle, \dots \langle a_1, a_2, \dots, a_n \rangle, \dots\}$ ideallar sinfini qarasak, ushbu sinf maksimal elementga ega. Ushbu maksimal element $\langle a_1, a_2, \dots, a_s \rangle$ uchun $\langle a_1, a_2, \dots, a_s \rangle = A$ munosabat o'rinli bo'ladi. Demak, A ideal chekli hosil qiluvchili ideal.

3) $\Rightarrow$ 1). Aytaylik, R halqaning ixtiyoriy ideali chekli hosil qiluvchili bo'lib, $A_1 \subset A_2 \subset \dots \subset A_s \subset \dots$ o'suvchi zanjir berilgan bo'lsin. U holda $A = \bigcup\limits_{i=1}^{\infty} A_i$ to'plam ham R halqaning ideali bo'lib, chekli hosil qiluvchili bo'ladi. Aytaylik, $A = \langle a_1, a_2, \dots, a_n \rangle$ bo'lsin. U holda a_j element qandaydir A_{i_j} elementga tegishli ekanligidan $1, 2, \dots, n$ sonlari uchun $i_1, i_2, \dots, i_n$ sonlarini hosil qilamiz. Agar

$k = \max\{i_1, i_2, \ldots, i_n\}$ deb olsak, $A_k = A$ bo'lib, $A_k = A_{k+1} = \ldots$ munosabat bajariladi. Ya'ni, R halqa Nyotr halqasi. $\square$

Ta'kidalsh joizki, Artin halqalari uchun 5.6.1-teoremaning analogi quyidagicha bo'ladi.

5.6.2-teorema. *R halqa Artin halqasi bo'lishi uchun, uning ixtiyoriy ideallar sinfi minimal elementga ega bo'lishi zarur va yetarli.*

Quyida Artin halqasi bo'lib, Nyotr halqasi bo'lmaydigan halqaga misol keltiramiz.

5.6.3-misol. *Ixtiyoriy p tub son uchun*

$$\mathbb{Z}(p^\infty) = \left\{ \frac{a}{p^n} \in \mathbb{Q} \mid 0 \leq a < p^n, \ n \in \mathbb{N} \right\}$$

to'plamni qaraymiz. Ushbu to'plamda $a \oplus b = (a + b)(mod 1)$, $a \odot b = 0$ amallarni qarasak, $(\mathbb{Z}(p^\infty), \oplus, \odot)$ uchlik birlik elementga ega bo'lmagan kommutativ halqa tashkil qiladi. Ushbu halqadagi ko'paytma trivial bo'lganligi uchun ixtiyoriy $(\mathbb{Z}(p^\infty), \oplus)$ qism gruppa ideal bo'ladi.

Aytaylik, $\mathbb{Z}(p^\infty)$ halqaning qandaydir I ideali berilgan bo'lib, k soni qandaydir q element uchun $\frac{q}{p^k} \notin I$ shart bajariluvchi eng kichik son bo'lsin. Ma'lumki, $EKUB(q, p) = 1$ bo'ladi, aks holda $p|q$ bo'lib, $\frac{q}{p^k} = \frac{a}{p^{k-1}} \notin I$ munosabatdan k sonining eng kichik eganligiga ziddiyat hosil qilamiz. Endi I idealning

$$J_{k-1} = \{0, \frac{1}{p^{k-1}}, \frac{2}{p^{k-1}}, \ldots, \frac{p^{k-1} - 1}{p^{k-1}}\}$$

qism to'plamini qarab, $I = J$ ekanligini ko'rsatamiz.

Faraz qilaylik, I idealda $\frac{r}{p^n}$, $n \geq k$ element mavjud bo'lsin, bu yerda $EKUB(r, p) = 1$. U holda shunday x, y butun sonlar topilib, $xr + yp = 1$. Ikkinchi tomondan esa $\frac{xr}{p^k} = \frac{(xp^{n-k})r}{p^n}$ va $\frac{yr}{p^k} = \frac{y}{p^{k-1}}$ elementlar I idealda yotganligi uchun $\frac{1}{p^k} = \frac{xr+yp}{p^k} \in I$. Bundan esa, ixtiyoriy q uchun $\frac{q}{p^k} \in I$ bo'lib, bu k sonining tanlanishiga zid. Demak, I idealning barcha elementlari $\frac{r}{p^n}, n < k$ ko'rinishida bo'ladi. Bundan esa, $J = I$ kelib chiqadi. Shunday qilib biz, $\mathbb{Z}(p^\infty)$ halqaning ixtiyoriy xosmas ideali chekli ekanligini ko'rsatdik. Bundan esa, ixtiyoriy kamayuvchi zanjirning chekli ekanligi kelib chiqadi. Ya'ni, $(\mathbb{Z}(p^\infty)$ halqa Artin halqasi.

Lekin

$$J_1 \subset J_2 \subset \cdots \subset J_k \subset \ldots$$

qat'iy o'suvchi zanjirni qarasak, bu sanjir chekli emas, ya'ni $\mathbb{Z}(p^\infty)$ halqa Nyotr halqasi emas.

Endi Nyotr halqalarining gomomorf obrasi, faktori va ularning to'g'ri yig'indilarini o'rganamiz.

5.6.3-teorema. *Nyotr halqasining gomomorf obrasi yana Nyotr halqa bo'ladi.*

Isbot. Aytaylik, R Nyotr halqasi bo'lib, $f : R \to S$ epimorfizm berilgan bo'lsin. S halqaning

$$J_1 \subset J_2 \subset \dots \subset J_s \subset \dots$$

ideallardan iborat o'suvchi zanjirini qarasak, ushbu ideallar uchun $I_k = f^{-1}(J_k)$ to'plamlar R halqaning ideallari bo'lib,

$$I_1 \subset I_2 \subset \dots \subset I_s \subset \dots$$

munosabat o'rinli. R halqa Nyotr halqasi bo'lganligi uchun shunday n soni topilib, $I_n = I_{n+1} = \dots$. Bundan esa, f akslantirishning epimorfizm ekanligidan foydalansak, $J_n = J_{n+1} = \dots$ kelib chiqadi. Demak, S halqa ham Nyotr halqasi. $\square$

5.6.4-teorema. *R halqaning I ideali berilgan bo'lib, I va R/I halqalar Nyotr halqalari bo'lsa, u holda R ham Nyotr halqasi bo'ladi.*

Isbot. Aytaylik, R halqaning

$$A_1 \subset A_2 \subset \dots \subset A_s \subset \dots$$

ideallardan iborat o'suvchi zanjiri berilgan bo'lsin. U holda $\varphi : R \to R/I$ tabiiy gomomorfizm uchun

$$\varphi(A_1) \subset \varphi(A_2) \subset \dots \subset \varphi(A_s) \subset \dots$$

ideallar R/I halqadagi o'suvchi zanjir bo'ladi. R/I halqa Nyotr halqasi bo'lganligi uchun shunday n soni topilib, $\varphi(A_n) = \varphi(A_{n+1}) = \dots$.

Bundan tashqari, $A_1 \cap I \subset A_2 \cap I \subset \dots \subset A_s \cap I \subset \dots$ ideallar I Nyotr halqasining o'suvchi zanjiri bo'lib, shunday m soni uchun $A_m \cap I = A_{m+1} \cap I = \dots$. U holda $k = \max\{n, m\}$ uchun $\varphi(A_k) = \varphi(A_{k+1}) = \dots$ va $A_k \cap I = A_{k+1} \cap I = \dots$ munosabatlar o'rinli.

Biz endi, $A_k = A_{k+1} = \dots$ ekanligini ko'rsatamiz. Buning uchun $A_k = A_{k+1}$ tenglikni ko'rsatish yetarli. Ixtiyoriy $b \in A_{k+1}$ element olsak, $\varphi(A_k) = \varphi(A_{k+1})$ bo'lgani uchun $c \in A_k$ element topilib, $\varphi(b) = \varphi(c)$. Bundan esa, $b + I = c + I$ ekanligi, ya'ni $b - c \in I$ kelib chiqadi. Ikkinchi tomondan esa, $b - c \in A_{k+1}$ bo'lganligi uchun $b - c \in A_{k+1} \cap I = A_k \cap I$, ya'ni $b - c \in A_k$. Bu esa, $b \in A_k$ ekanligini, ya'ni $A_k = A_{k+1}$ tenglik o'rinliligini anglatadi. Demak, R halqa Nyotr halqasi. $\square$

5.6.1-natija. *R_1 va R_2 Nyotr halqalarining to'g'ri yig'indisi yana Nyotr halqasi bo'ladi.*

Isbot. $R_1 \oplus R_2$ halqa uchun $(R_1 \oplus R_2)/R_1$ faktor halqani qarasak, $(R_1 \oplus R_2)/R_1 \simeq R_2$ bo‘lib, R_1 va R_2 halqalar Nyotr halqalari bo‘lganligi uchun 5.6.4-teoremaga ko‘ra $R_1 \oplus R_2$ ham Nyotr halqasi ekanligi kelib chiqadi. □

Ta’kidlash joizki, 5.6.1-natija chekli sondagi Nyotr halqalari uchun ham o‘rinli. Ya’ni $R_1, R_2, \dots, R_n$ Nyotr halqalarining to‘g‘ri yig‘indisi $R_1 \oplus R_2 \oplus \dots \oplus R_n$ ham Nyotr halqasi bo‘ladi.

5.6.5-teorema. *Agar R halqa kommutativ va birlik elementli Nyotr halqasi bo‘lsa, u holda $R[x]$ ko‘phadlar halqasi ham Nyotr halqasi bo‘ladi.*

Isbot. Teoremani isbotlash uchun $R[x]$ halqadning ixtiyoriy A ideali chekli hosil qiluvchili ekanligini ko‘rsatamiz. A idealning darajasi n ga teng bo‘lgan $f(x)$ ko‘phadining x^n hadi oldidagi ko‘effitsiyentlaridan va noldan iborat to‘plamni I_n orqali belgilaymiz.

Ushbu I_n to‘plam R halqaning ideali bo‘ladi. Haqiqatdan ham $a, b \in I_n$ bo‘lib, $a \neq 0, b \neq 0$ bo‘lsa, u holda shunday $f(x), g(x) \in A$ ko‘phadlar topilib, $deg(f(x)) = deg(g(x)) = n$ va bu ko‘phadlarning x^n hadi oldidagi koeffitsiyentlari mos ravishda a va b ga teng. Agar $a - b = 0$ bo‘lsa, u holda $a - b \in I_n$. Agar $a - b \neq 0$ bo‘lsa, $f(x) - g(x) \in A$ va $deg(f(x) - g(x)) = n$ bo‘lganligi hamda $a - b$ element $f(x) - g(x)$ ko‘phadning x^n hadi oldidagi koeffitsiyenti ekanligidan $a - b \in I_n$ kelib chiqadi. Endi, $a \in I_n$ va $r \in R$ elementlar uchun $ar \neq 0$ bo‘lsa, u holda ushbu element $rf(x)$ ko‘phadning x^n hadi oldidagi koeffitsiyenti bo‘lib, $ar \in I_n$ bo‘ladi.

R halqaning ushbu I_n ideallari uchun $I_n \subset I_{n+1}$ munosabat o‘rinli. Chunki, $a \in I_n$ bo‘lsa, u holda qandaydir $f(x) = ax^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in A$ ko‘phad mavjud bo‘lib, $xf(x) = ax^{n+1} + a_1x^n + \dots + a_{n-1}x^2 + a_nx \in A$ ekanligidan $a \in I_{n+1}$ kelib chiqadi. Shunday qilib biz, R halqaning ideallaridan iborat bo‘lgan

$$I_0 \subset I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$$

o‘suvchi zanjirni hosil qildik. R halqa Nyotr halqasi bo‘lganligi uchun ushbu zanjir qandaydir m ta qadamdan keyin uziladi, ya’ni $I_m = I_{m+1} = \dots$. Bundan tashqari, Nyotr halqasining ixtiyoriy ideali chekli hosil qiluvchili ekanligidan $I_0, I_1, \dots, I_m$ ideallarning ham chekli hosil qiluvchili bo‘lishi kelib chiqadi, ya’ni

$$I_k = \langle a_{k,1}, a_{k,2}, \dots, a_{k,t_k} \rangle, \quad 0 \leq k \leq m,$$

bu yerda $a_{k,j}$ elementlar A idealning qandaydir k-darajali $f_{k,j}(x)$ ko‘phadlarning bosh koeffitsiyentlari. $R[x]$ halqaning ushbu ko‘phadlar orqali hosil qilingan idealini B orqali belgilaymiz, ya’ni

$$B = \langle f_{k,j}(x) \mid 0 \leq k \leq m, \ 1 \leq j \leq t_k \rangle.$$

Ma'lumki, $B \subset A$. Biz endi $A \subset B$ ekanligini, ya'ni ixtiyoriy $f(x) \in A$ ko'phadni B idealga tegishli ekanligini ko'rsatamiz. Buning uchun $f(x)$ ko'phadning darajasi bo'yicha induksiya usulidan foydalanamiz. Agar $deg(f(x)) = 0$ bo'lsa, u holda $f(x) \in I_0 \subset B$ ekanligi ravshan. Endi A idealda yotuvchi darajasi s dan kichik bo'lgan barcha ko'phadlar B idealga ham tegishli bo'lsin deb faraz qilib,

$$f(x) = c_0x^s + c_1x^{s-1} + \cdots + c_{s-1}x + c_s \in A, \quad c_0 \neq 0$$

ko'phadni qaraymiz. Agar $s \leq m$ bo'lsa, u holda $c_0 \in I_s$ bo'lib, $I_s = \langle a_{s,1}, a_{s,2}, \ldots, a_{s,t_s}\rangle$ bo'lganligi uchun ushbu c_0 element $a_{s,1}, a_{s,2}, \ldots, a_{s,t_s}$ elementlar orqali ifodalanadi, ya'ni

$$c_0 = r_1a_{s,1} + r_2a_{s,2} + \cdots + r_sa_{s,t_s}, \quad r_1, r_2, \ldots, r_s \in R.$$

Bundan esa

$$h_s(x) = r_1f_{s,1}(x) + r_2f_{s,2}(x) + \cdots + r_sf_{s,t_s}(x)$$

ko'phadning B idealga tegishli ekanligi kelib chiqadi. Bundan tashqari, ushbu $h_s(x)$ ko'phadning ham darajasi s ga, bosh koeffitsiyenti esa c_0 ga teng. Demak, $f(x) - h_s(x) \in A$ ko'phadning darajasi s dan kichik bo'lib, induksiya faraziga ko'ra, $f(x) - h_s(x) \in B$ kelib chiqadi, ya'ni $f(x) \in B$. Shunday qilib biz $s \leq m$ bo'lganda $A \subset B$ ekanligini ko'rsatdik.

Endi $s > m$ bo'lgan holni qaraymiz. U holda

$$c_0 \in I_s = I_m = \langle a_{m,1}, a_{m,2}, \ldots, a_{m,t_m}\rangle$$

bo'lib, $c_0 = r_1a_{m,1} + r_2a_{m,2} + \cdots + r_ma_{m,t_m}$, bu yerda $r_1, r_2, \ldots, r_m \in R$.

Endi quyidagi

$$g(x) = f(x) - x^{s-m}\big(r_1f_{m,1}(x) + r_2f_{m,2}(x) + \cdots + r_mf_{m,t_m}(x)\big)$$

ko'phadni qarasak, ushbu ko'phadning darajasi s dan kichik bo'lib, induksiya faqaziga ko'ra u B idealga tegishli. Ikkinchi tomondan esa $r_1f_{m,1}(x) + r_2f_{m,2}(x) + \cdots + r_mf_{m,t_m}(x) \in B$ ekanligidan foydalansak, $f(x) \in B$ kelib chiqadi. Shunday qilib biz, ixtiyoriy $f(x) \in A$ uchun $f(x) \in B$ ekanligini, ya'ni $A \subset B$ bo'lishini ko'rsatdik. B idealning hosil qiluvchi elementlari cheklita bo'lganligi uchun A ideal ham chekli hosil qiluvchili ideal. Demak, $R[x]$ halqaning ixtiyoriy ideali chekli hosil qiluvchili ekan, ya'ni $R[x]$ Nyotr halqasi. □

Yuqoridagi teoremadan quyidagi muhim natijani olamiz.

5.6.6-teorema (Gilbertning bazis haqidagi teoremasi). *Agar R halqa kommutativ birlik elementli Nyotr halqasi bo'lsa, u holda $R[x_1, x_2, \ldots, x_n]$ ko'phadlar halqasi ham Nyotr halqasi bo'ladi.*

Endi Artin halqasining muhim xossalaridan birini keltiramiz.

5.6.7-teorema. *Bittadan ko‘p elementga ega va nolning bo‘luvchilariga ega bo‘lmagan kommutativ Artin halqasi maydon bo‘ladi.*

Isbot. Aytaylik, R halqa nolning bo‘luvchilariga ega bo‘lmagan kommutativ Artin halqasi bo‘lsin. Ixtiyoriy $a \in R$ element olib, quyidagi ideallarni qaraymiz.

$$\langle a\rangle \supset \langle a^2\rangle \supset \langle a^3\rangle \dots$$

U holda shunday n soni topilib, $\langle a^n\rangle = \langle a^{n+1}\rangle = \dots$ munosabat o‘rinli, ya’ni $a^n \in \langle a^{n+1}\rangle$. Demak, qandaydir m butun son va $r \in R$ element uchun $a^n = ra^{n+1} + ma^{n+1}$ tenglik o‘rinli bo‘lib, bundan $a^{n-1}(a - ra^2 - ma^2) = 0$ kelib chiqadi. $a^{n-1} \neq 0$ va R halqa nolning bo‘luvchilariga ega bo‘lmaganligi uchun $a = ra^2 + ma^2 = (ra + ma)a$.

Ushbu $e = ra + ma$ element R halqaning birlik elementi bo‘lib, $e = (r + me)a$ ekanligidan esa a elementning teskarilanuvchi ekanligi kelib chiqadi. Demak, R maydon bo‘ladi. $\square$

5.6.4-misol. $R = \left\{\begin{pmatrix} a & b \\ 0 & c\end{pmatrix} \mid a \in \mathbb{Z},\ b, c \in \mathbb{Q}\right\}$ *halqaning o‘ng Nyotr bo‘lib, chap Nyotr halqasi emasligini ko‘rsating.*

Yechish. Ushbu R halqada $I_n = \left\{\begin{pmatrix} 0 & \frac{m}{2^n} \\ 0 & 0\end{pmatrix} \mid m \in \mathbb{Z}\right\}$ to‘plamlarni qarasak, ular halqaning chap ideallari bo‘lib, $I_n \subset I_{n+1}$ bo‘ladi. Ya’ni R halqada

$$I_1 \subset I_2 \subset I_3 \subset \dots \subset I_k \subset \dots$$

qat’iy o‘zuvchi chap ideallar zanjiri mavjud. Demak, R halqa chap Nyotr halqasi emas.

Endi ushbu R halqaning o‘ng Nyotr halqasi ekanligini ko‘rsatamiz. Buning uchun R halqaning ixtiyoriy o‘ng ideali chekli hosil qiluvchili ekanligini ko‘rsatish kifoya.

Agar R halqaning ideali $A_1 = \left\{\begin{pmatrix} 0 & b \\ 0 & 0\end{pmatrix}\right\}$ ko‘rinishda bo‘lsa, u holda

$$\begin{pmatrix} 0 & b \\ 0 & 0\end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{b}\end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0\end{pmatrix}$$

ekanligidan $\begin{pmatrix} 0 & 1 \\ 0 & 0\end{pmatrix} \in A_1$ bo‘lishini, ya’ni $A = \begin{pmatrix} 0 & 1 \\ 0 & 0\end{pmatrix} R = \left\langle \begin{pmatrix} 0 & 1 \\ 0 & 0\end{pmatrix} \right\rangle_r$ tenglikni hosil qilamiz. Bu esa, A_1 ideal bitta hosil qiluvchi elementga ega ekanligini anglatadi.

Xuddi shunga o‘xshab,

$$A_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} \right\} = \left\langle \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle_r, \quad A_3 = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \right\} = \left\langle \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle_r,$$

$$A_4 = \left\{ \begin{pmatrix} m & d \\ 0 & e \end{pmatrix} \right\} = \left\langle \begin{pmatrix} k & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\rangle_r$$

ekanligini ko‘rsatish mumkin. Bu yerda, $b \neq 0, c \neq 0, m \neq 0$ hamda k element A_4 ko‘rinishidagi idealga tegishli matritsalarning birinchi ustun va birinchi satrida turgan sonlar ichidagi eng kichik natural son. □

5.6.1 Mustaqil ishlash uchun misol va masalalar

1. O’zi Artin halqasi bo‘lib, qism halqasi Artin bo‘lmaydigan halqaga misol keltiring.

2. O’zi Nyotr halqasi bo‘lib, qism halqasi Nyotr bo‘lmaydigan halqaga misol keltiring.

3. Artin halqasining gomomorf obrazi yana Artin halqasi bo‘lishini isbotlang.

4. Agar R halqaning I ideali berilgan bo‘lib, I va R/I halqalar Artin halqalari bo‘lsa, u holda R halqaning ham Artin halqasi ekanligini ko‘rsating.

5. Agar birlik elementli o‘ng Artin halqasida qandaydir a, b elementlar uchun $ab = 1$ bo‘lsa, u holda $ba = 1$ ekanligini ko‘rsating.

6. Birlik elementli kommutativ Artin halqasining ixtiyoriy birlamchi(prime) ideali maksimal ekanligini ko‘rsating.

BOB 6

Galua nazariyasi

Biz ushbu bob maydonning kengaytmalari tushunchasini kiritib, u orqali Galua nazariyasini keltiramiz. Ma'lumki, Galua nazariyasi algebraik tenglamalarni radikallarda yechish masalasini o‘rganish natijasida paydo bo‘lgan bo‘lib, algebraik ko‘phadga o‘rin almashtirishlar gruppasining qism gruppasi bo‘lgan Galua gruppasini mos qo'yish orqali amalga oshiriladi. Galua nazariyasining fundamental teoremasi biror maydonning chekli normal va separabel kengaytmasining Galua gruppasi barcha qism gruppalari bilan ushbu kengaytma qism maydonlari orasidagi moslikni o‘rnatuvchi teorema hisoblanadi. Bobning asosiy teoremalaridan biri bu $f(x) = 0$ algebraik tenglama radikallarda yechilishi uchun ushbu ko‘phadga mos keluvchi Galua gruppasining yechiluvhan bo‘lishi zarur va yetarli ekanligi haqidagi teoremadir.

6.1 Maydonning kengaytmalari

Dastlab maydonning kengaytmalari tushunchalarini kiritib olamiz. Bizga $\mathbb{F}$ maydon va uning $\mathbb{K}$ qism maydoni berilgan bo‘lsa, u holda $\mathbb{F}$ maydon $\mathbb{K}$ maydonning **kengaytmasi** deb ataladi. Biz $\mathbb{K}$ maydonning $\mathbb{F}$ kengaytmasi berilgan bo‘lsa, $\mathbb{K} \subset \mathbb{F}$ kabi belgilashdan foydalanamiz. Takidlash joizki, $\mathbb{K} \subset \mathbb{F}$ kengaytmada $\mathbb{F}$ maydonni $\mathbb{K}$ maydon ustidagi vektor fazo sifatida qarash mumkin.

6.1.1-ta'rif. $\mathbb{K} \subset \mathbb{F}$ *kengaytmada* $\mathbb{F}$ *maydonni* $\mathbb{K}$ *maydon ustidagi vektor fazo sifatidagi o‘lchami* $[\mathbb{F} : \mathbb{K}]$ *kabi belgilanadi va* $\mathbb{F}$ *maydonning* $\mathbb{K}$ *maydon bo‘yicha darajasi deb ataladi.*

Agar $[\mathbb{F} : \mathbb{K}]$ soni chekli bo‘lsa, u holda ushbu kengaytma **chekli kengaytma**, aks holda **cheksiz** deb ataladi. Demak, $\mathbb{K} \subset \mathbb{F}$ kengaytma chekli bo‘lib, $[\mathbb{F} : \mathbb{K}] = n$ bo‘lsa, u holda shunday $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}$ elementlar mavjud bo‘lib, ixtiyoriy $\beta \in \mathbb{F}$ element yagona ravishda

$$\beta = k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n$$

kabi ifodalanadi, bu yerda $k_1, k_2, \dots, k_n \in \mathbb{K}$. Ushbu $\alpha_1, \alpha_2, \dots, \alpha_n$ elementlar esa $\mathbb{K} \subset \mathbb{F}$ kengaytmaning bazisi deb ataladi.

Bizga $\mathbb{K} \subset \mathbb{F}$ kengaytma va $X \subset \mathbb{F}$ to‘plam berilgan bo‘lsin. Ma’lumki, biror maydonning qism maydonlari kesishmasi yana qism maydon bo‘ladi. $\mathbb{F}$ maydonning $\mathbb{K} \cup X$ to’plamni o‘z ichiga oluvchi barcha qism maydonlari kesishmasi $\mathbb{K}$ maydon ustida X to‘plam orqali hosil qilingan maydon deyiladi va $\mathbb{K}(X)$ kabi belgilanadi. Ushbu $\mathbb{K}(X)$ maydon X to‘plam, hamda $\mathbb{K}$ maydonni o‘z ichiga oluvchi eng kichik maydon bo‘ladi. X to‘plam chekli bo‘lib, $X = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ bo‘lgan holda biz $\mathbb{K}$ maydonning chekli $\mathbb{K}(\alpha_1, \alpha_2, \dots, \alpha_n)$ kengaytmasini hosil qilamiz.

6.1.2-ta’rif. *Agar $\mathbb{K} \subset \mathbb{F}$ kengaytmada $a \in \mathbb{F}$ element uchun hech bo‘lmaganda bittasi noldan farqli bo‘lgan $k_0, k_1, \dots, k_{n-1}, k_n \in \mathbb{K}$ elementlar topilib, $k_0 a^n + k_1 a^{n-1} + \dots + k_{n-1} a + k_n = 0$ tenglik o‘rinli bo‘lsa, u holda a element $\mathbb{K}$ maydon ustida* ***algebraik*** *element deb ataladi. Aks holda, ushbu elementga* ***transendent*** *element deyiladi.*

Ta’rifdan ko‘rinadiki, agar $a \in \mathbb{F}$ element $\mathbb{K}$ maydon ustida algebraik bo‘lsa, u holda u koeffitsiyentlari $\mathbb{K}$ maydondan olingan biror ko‘phadning ildizi bo‘ladi. Bunday ko‘phadlarning darajasi eng kichik bo‘lganini a algebraik elementning **minimal ko‘phadi** deb ataladi. Ta’kidlash joizki, minimal ko‘phad bir qiymatli aniqlanib, u $\mathbb{K}$ maydon ustida keltirilmas ko‘phad bo‘ladi. Ushbu minimal ko‘phadning darajasi esa a algebraik elementning **darajasi** deb ataladi.

Masalan, $\sqrt{3} \in \mathbb{R}$ soni $\mathbb{Q}$ ratsional sonlar maydoni ustida algebraik bo‘lib, uning darajasi 2 ga teng.

6.1.3-ta’rif. *Agar $\alpha_1, \alpha_2, \dots, \alpha_n$ algebraik elementlar topilib, $\mathbb{K}(\alpha_1, \alpha_2, \dots, \alpha_n) = \mathbb{F}$ bo‘lsa, u holda $\mathbb{K} \subset \mathbb{F}$ kengaytma* ***algebraik hosil qilingan*** *deyiladi.*

Xususan, $n = 1$, ya’ni $\mathbb{F} = \mathbb{K}(\alpha)$ bo‘lganda bunday kengaytmaga **sodda algebraik kengaytma** deb ataladi. Ushbu α elementga esa **primitiv element** deyiladi.

Agar $\mathbb{K} \subset \mathbb{F}$ kengaytma uchun shunday

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \dots \subset \mathbb{K}_s = \mathbb{F}$$

sodda algebraik kengaytmalar ketma-ketligi mavjud bo‘lsa, u holda ushbu kengaytmaga **murakkab algebraik kengaytma** deb ataladi. Ya’ni murakkab algebraik kengaytma, bu $\alpha_1, \alpha_2, \dots, \alpha_s$ elementlar orqali hosil qilingan $\mathbb{K}_i = \mathbb{K}_{i-1}(\alpha_i)$ ko‘rinishidagi bir nechta sodda algebraik kengaytmalar ketma-ketligidan iborat. Murakkab algebraik kengaytmaning ta’rifida umuman olganda α_i elementlar $\mathbb{K}_{i-1}$ maydonlarda algebraik bo‘lib, $\mathbb{K}$ maydonda algebraik bo‘lishini talab qilinmaydi.

6.1.4-ta'rif. *Agar $\mathbb{K} \subset \mathbb{F}$ kengaytmada ixtiyoriy $a \in \mathbb{F}$ element $\mathbb{K}$ maydonga nisbatan algebraik bo'lsa, u holda ushbu kengaytmaga* ***algebraik kengaytma*** *deb ataladi.*

6.1.1-tasdiq. *$\mathbb{K} \subset \mathbb{F}$ kengaytmada $a \in \mathbb{F}$ algebraik element berilgan bo'lib, bu elementning darajasi n ga teng bo'lsa, u holda $[\mathbb{K}(a) : \mathbb{K}] = n$, ya'ni sodda algebraik kengaytmaning darajasi minimal ko'phadning darajasiga teng.*

Isbot. Aytaylik, $a \in \mathbb{F}$ element $\mathbb{K}$ maydon ustida algebraik element bo'lib, $f(x)$ uning minimal ko'phadi bo'lsin, ya'ni $f(a) = 0$, bu yerda $deg(f(x)) = n$. Quyidagi
$$\mathbb{K}[x] = \{k_0x^s + k_1x^{s-1} + \cdots + k_{s-1}x + k_s \mid k_i \in \mathbb{K}\}$$
bir ozgaruvchili k'phadlar halqasini qaraymiz. Ma'lumki, $\mathbb{K}[a] \subset \mathbb{K}(a)$ munosabat o'rinli. Biz $\mathbb{K}(a) \subset \mathbb{K}[a]$ bo'lishini ko'rsatamiz. Buning uchun ixtiyoriy noldan farqli $\beta = g(a)$ element uchun $\beta^{-1} \in \mathbb{K}[a]$ ekanligini ko'rsatish kifoya, bu yerda $g(x)$ koeffitsiyentlari $\mathbb{K}$ maydondan olingan qandaydir ko'phad.

$g(a) \neq 0$ bo'lganligi uchun $g(x)$ ko'phad $f(x)$ ko'phadga bo'linmaydi hamda $f(x)$ ko'phadning keltirilmas ekanligidan $\text{EKUB}(g(x), f(x)) = 1$ bo'lishi kelib chiqadi. U holda shunday $M(x)$ va $N(x)$ ko'phadlar topilib,
$$f(x)M(x) + g(x)N(x) = 1$$
tenglik o'rinli. Ushbu tenglikdan $x = a$ bo'lganda $g(a)N(a) = 1$ ekanligini, ya'ni $\beta^{-1} = N(a) \in \mathbb{K}[a]$ bo'lishini hosil qilamiz. Demak, $\mathbb{K}(a) \subset \mathbb{K}[a]$.

Shunday qilib, biz ixtiyoriy $\beta \in \mathbb{K}(a)$ element uchun shunday $g(x) \in \mathbb{K}[x]$ ko'phad topilib, $\beta = g(a)$ ekanligini ko'rsatdik. Agar $g(x)$ ko'phadni $f(x)$ ko'phadga qoldiqli bo'lsak, $g(x) = f(x)q(x) + r(x)$ tenglikdan $\beta = g(a) = r(a)$ ekanligiga ega bo'lamiz. Bu esa $\mathbb{K}(a)$ maydonning ixtiyoriy elementini darajasi n dan oshmaydigan $r(x)$ ko'phad orqali $\beta = r(a)$ kabi yozish mumkinligini bildiradi. Bundan tashqari, $1, a, a^2, \ldots, a^{n-1}$ elementlar $\mathbb{K}$ maydonda chiziqli erkli bo'lganligi uchun ular $\mathbb{K}(a)$ maydonda bazis bo'ladi. Demak, $[\mathbb{K}(a) : \mathbb{K}] = n$. □

Ta'kidlash joizki, biz yuqoridagi tasdiqning isbotida sodda algebraik kengaytma uchun $\mathbb{K}[a]$ ko'phadlar halqasining maydon ekanligini va $1, a, a^2, \ldots, a^{n-1}$ elementlarning $\mathbb{K}(a)$ maydonda bazis bo'lishini ko'rsatdik, bu yerda n soni a elementning minimal ko'phadi darajasi. Bundan tashqari, quyidagi natijani ham bevosita tasdiqning isbotidan hosil qilamiz.

6.1.1-natija. $\mathbb{K}(a)$ *maydonning ixtiyoriy β elementi $\beta = g(a)$ kabi ifodalanadi.*

Quyudagi tasdiqda esa, ixtiyoriy chekli kengaytma algebraik kengaytma bo'lishini ko'rsatamiz.

6.1.2-tasdiq. *Ixtiyoriy chekli kengaytma algebraik kengaytma bo'ladi.*

Isbot. Aytaylik, $[\mathbb{F} : \mathbb{K}] = n$ bo‘lsin. U holda $\mathbb{F}$ maydonning ixtiyoriy $n+1$ ta elementi $\mathbb{K}$ maydon ustida chiziqli bog‘liq bo‘ladi. Bundan esa, ixtiyoriy $\beta \in \mathbb{F}$ uchun $1, \beta, \ldots, \beta^{n-1}, \beta^n$ elementlar ham chiziqli bog‘liq ekanligi kelib chiqadi, ya’ni hech bo‘lmaganda bittasi noldan farqli bo‘lgan $k_0, k_1, \ldots, k_n \in \mathbb{K}$ elementlar topilib,

$$k_0\beta^n + k_1\beta^{n-1} + \cdots + k_{n-1}\beta + k_n = 0.$$

Demak, $\beta \in \mathbb{F}$ element $k_0x^n + k_1x^{n-1} + \cdots + k_{n-1}x + k_n$ ko‘phadning ildizi, ya’ni u algebraik element. □

6.1.2-natija. *Ixtiyoriy chekli kengaytma algebraik hosil qilingan kengaytma bo‘ladi.*

Isbot. Aytaylik, $\mathbb{K} \subset \mathbb{F}$ kengaytma chekli bo‘lib, $\alpha_1, \alpha_2, \ldots, \alpha_n$ elementlar bazis bo‘lsin. Yuqoridagi tasdiqqa ko‘ra ushbu elementlar algebraik bo‘lib, ular orqali hosil qilingan $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ maydon $\mathbb{K}$ maydonning algebraik hosil qilingan kengaytmasi bo‘ladi. Bundan tashqari, ushbu kengaytma minimal bo‘lganligi uchun $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{F}$ munosabat o‘rinli.

Ikkinchi tomondan esa, $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ bo‘lganligi va ixtiyoriy $\beta \in \mathbb{F}$ element $\beta = k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n$ kabi ifodalanganligi uchun $\mathbb{F} \subset \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Demak, $\mathbb{F} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, ya’ni $\mathbb{F}$ algebraik hosil qilingan kengaytma. □

Endi ixtiyoriy algebraik hosil qilingan kengaytma murakkab algebraik kengaytma ekanligini ko‘rsatamiz. Aytaylik, $\mathbb{K}$ maydonning $\mathbb{F} = \mathbb{K}(\alpha_1)(\alpha_2)\ldots(\alpha_n)$ murakkab algebraik kengaytmasi berilgan bo‘lsin.

6.1.3-tasdiq. *Ixtiyoriy $\beta \in \mathbb{F} = \mathbb{K}(\alpha_1)(\alpha_2)\ldots(\alpha_n)$ element uchun koeffitsiyentlari $\mathbb{K}$ maydondan olingan shunday $g(x_1, x_2, \ldots, x_n)$ ko‘phad topilib, $\beta = g(\alpha_1, \alpha_2, \ldots, \alpha_n)$ tenglik o‘rinli.*

Isbot. Tasdiqning isbotini n uchun induksiya metodini qo‘llab amalga oshiramiz. $n = 1$ bo‘lgan holda tasdiqning o‘rinli ekanligi 6.1.1-natijadan kelib chiqadi. Faraz qilaylik $\mathbb{L} = \mathbb{K}(\alpha_1)(\alpha_2)\ldots(\alpha_{n-1})$ maydon uchun tasdiq o‘rinli bo‘lsin. Ixtiyoriy $\beta \in \mathbb{F}$ elementni qarasak, $\mathbb{F} = \mathbb{L}(\alpha_n)$ bo‘lganligi uchun, $\mathbb{L}$ maydonda shunday $h(x)$ ko‘phad topilib, $\beta = h(\alpha_n)$.

Aytaylik, $h(x) = \gamma_0x^m + \gamma_1x^{m-1} + \cdots + \gamma_m$ bo‘lsin, bu yerda $\gamma_0, \gamma_1, \ldots, \gamma_m \in \mathbb{L}$. Induksiya faraziga ko‘ra har bir γ_i uchun $g_i(x_1, x_2, \ldots, x_{n-1})$ ko‘phad topilib, $\gamma_i = g_i(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$. Bundan esa,

$$g(x_1, x_2, \ldots, x_n) = g_0(x_1, x_2, \ldots, x_{n-1})x_n^m +$$

$$+ g_1(x_1, x_2, \ldots, x_{n-1})x_n^{m-1} + \cdots + g_m(x_1, x_2, \ldots, x_{n-1})$$

ko‘phad uchun $\beta = g(\alpha_1, \alpha_2, \ldots, \alpha_n)$ ekanligi kelib chiqadi. □

6.1.3-natija. *Ixtiyoriy algebraik hosil qilingan kengaytma murakkab algebraik kengaytma bo'ladi, ya'ni* $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{K}(\alpha_1)(\alpha_2)\ldots(\alpha_n)$.

Isbot. Induktiv tarzda aniqlanuvchi quyidagi maydonlarni qaraymiz

$$\mathbb{L}_0 = \mathbb{K},\ \mathbb{L}_1 = \mathbb{L}_0(\alpha_1),\ \mathbb{L}_2 = \mathbb{L}_1(\alpha_2),\ \ldots, \mathbb{L}_n = \mathbb{L}_{n-1}(\alpha_n).$$

Har bir α_i element $\mathbb{K}$ maydonda algebraik bo'lganligi uchun ular $\mathbb{L}_{i-1}$ maydonda ham algebraik bo'ladi. Demak, $\mathbb{L}_i \subset \mathbb{L}_{i+1}$ kengaytmalarning barchasi sodda algebraik kengaytmalar bo'lib, $\mathbb{L}_n = \mathbb{K}(\alpha_1)(\alpha_2)\ldots(\alpha_n)$. 6.1.3-tasdiqqa ko'ra, $\mathbb{L}_n$ maydonning ixtiyoriy β elementi $\alpha_1, \alpha_2, \ldots, \alpha_n$ elementlar orqali qandaydir ko'phad yordamida ifodalanadi. Bundan esa, $\mathbb{L}_n \subset \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ ekanligiga ega bo'lamiz.

Ikkinchi tomondan esa, $\mathbb{L}_n$ barcha $\alpha_1, \alpha_2, \ldots, \alpha_n$ elementlarni o'z ichiga olganligi uchun $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{L}_n$. Demak, $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \mathbb{K}(\alpha_1)(\alpha_2)\ldots(\alpha_n)$. $\square$

Bizga $\mathbb{K} \subset \mathbb{F}$ kengaytma berilgan bo'lib, $\mathbb{L}$ maydon uchun $\mathbb{K} \subset \mathbb{L} \subset \mathbb{F}$ munosabat o'rinli bo'lsa, u holda $\mathbb{L}$ maydon $\mathbb{K}$ va $\mathbb{F}$ maydonlarning orasida joylashgan maydon deyiladi. Ma'lumki, $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$ elementlar uchun

$$\mathbb{K}(\alpha_1) \subset \mathbb{K}(\alpha_1, \alpha_2) \subset \cdots \subset \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

munosabat o'rinli.

6.1.4-tasdiq. *Agar* $\mathbb{K} \subset \mathbb{L}$ *va* $\mathbb{L} \subset \mathbb{F}$ *kengaytmalar chekli bo'lsa, u holda* $\mathbb{K} \subset \mathbb{F}$ *kengaytma ham chekli bo'lib,*

$$[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{L}] \cdot [\mathbb{L} : \mathbb{K}]$$

tenglik o'rinli.

Isbot. Aytaylik, $[\mathbb{F} : \mathbb{L}] = n$ va $[\mathbb{L} : \mathbb{K}] = m$ bo'lsin, u holda $\mathbb{F}$ maydonda $\alpha_1, \alpha_2, \ldots, \alpha_n$ bazis, $\mathbb{L}$ maydonda esa $\beta_1, \beta_2, \ldots, \beta_m$ bazis mavjud. Tasdiqni isbotlash uchun ushbu

$$\alpha_i\beta_j, \quad 1 \leq i \leq n,\ 1 \leq j \leq m$$

elementlarni $\mathbb{F}$ maydonning $\mathbb{K}$ maydon bo'yicha bazisi bo'lishini ko'rsatish kifoya.

Dastlab, ixtiyoriy $\gamma \in \mathbb{F}$ elementni ushbu elementlarning chiziqli kombinatsiyasi shaklida ifodalanishini ko'rsatamiz. Ma'lumki, γ element $\alpha_1, \alpha_2, \ldots, \alpha_n$ larning chiziqli kombinatsiyasi orqali

$$\gamma = c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n$$

kabi ifodalanadi, bu yerda $c_1, c_2, \ldots, c_n \in \mathbb{L}$. O'z navbatida ushbu $c_1, c_2, \ldots, c_n$ elementlar esa $\beta_1, \beta_2, \ldots, \beta_m$ larning chiziqli kombinatsiyasi orqali

$$c_i = d_{i,1}\beta_1 + d_{i,2}\beta_2 + \cdots + d_{i,m}\beta_m$$

kabi ifodalanadi, bu yerda $d_{i,j} \in \mathbb{K}$.

Demak,

$$\gamma = \sum_{i=1}^{n} c_i\alpha_i = \sum_{i=1}^{n}\sum_{j=1}^{m} d_{i,j}\alpha_i\beta_j,$$

ya'ni ixtiyoriy $\gamma \in \mathbb{F}$ elementni $\alpha_i\beta_j$ elementlarning chiziqli kombinatsiyasi shaklida ifodalash mumkin.

Endi $\alpha_i\beta_j$ elementlarning chiziqli erkli ekanligini ko‘rsatamiz. Aytaylik, qandaydir $k_{i,j} \in \mathbb{K}$ elementar uchun $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} k_{i,j}\alpha_i\beta_j = 0$ bo‘lsin. Agar $c_i = \sum\limits_{j=1}^{m} k_{i,j}\beta_j$ kabi belgilasak, yuqoridagi tenglik

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = 0$$

ko‘rinishga keladi. Bu yerda $c_1, c_2, \ldots, c_n \in \mathbb{L}$ va $\alpha_1, \alpha_2, \ldots, \alpha_n$ elementlar $\mathbb{F}$ maydonning $\mathbb{L}$ maydonga nisbatan bazisi bo‘lganligi uchun $c_1 = c_2 = \cdots = c_n = 0$ ekanligi kelib chiqadi. Demak, ixtiyoriy i $(1 \leq i \leq n)$ uchun $\sum\limits_{j=1}^{m} k_{i,j}\beta_j = 0$. O‘z navbatida $\beta_1, \beta_2, \ldots, \beta_m$ elementlar $\mathbb{L}$ maydonning $\mathbb{K}$ maydonga nisbatan bazisi ekanligidan $k_{i,j} = 0$ kelib chiqadi. Ya'ni, $\alpha_i\beta_j$ elementlar chiziqli erkli. $\square$

Yuqoridagi tasdiqni umumlashtirgan holda ushbu natijaga ega bo‘lamiz.

6.1.4-natija. *Agar*

$$\mathbb{K} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \mathbb{L}_2 \subset \cdots \subset \mathbb{L}_n = \mathbb{F}$$

bo‘lib, har bir $\mathbb{L}_i$ maydon $\mathbb{L}_{i-1}$ maydonda chekli bo‘lsa, u holda $\mathbb{K} \subset \mathbb{F}$ kengaytma ham chekli bo‘lib,

$$[\mathbb{F} : \mathbb{K}] = [\mathbb{L}_1 : \mathbb{L}_0][\mathbb{L}_2 : \mathbb{L}_1] \ldots [\mathbb{L}_n : \mathbb{L}_{n-1}]$$

tenglik o‘rinli.

Bundan tashqari 6.1.4-tasdiqdan quyidagi muhim natija ham kelib chiqadi.

6.1.5-natija. *Ixtiyoriy murakkab algebraik kengaytma chekli kengaytma bo‘ladi.*

Isbot. 6.1.1-tasdiqqa ko‘ra har bir sodda algebraik kengaytma chekli bo‘lib, murakkab algebraik kengaytma chekli sondagi sodda algebraik kengaytmalarning ketma-ket qo‘llanilishi orqali hosil bo‘lishini hisobga olsak, 6.1.4-tasdiqqa ko‘ra ixtiyoriy murakkab algebraik kengaytmaning chekli ekanligi kelib chiqadi. $\square$

Yuqorida hosil qilingan 6.1.2, 6.1.3 va 6.1.5-natijalardan quyidagi teoremaga ega bo‘lamiz.

6.1.1-teorema. $\mathbb{K} \subset \mathbb{F}$ *kengaytma uchun quyidagilar teng kuchli:*

- $\mathbb{K} \subset \mathbb{F}$ *kengaytma chekli;*
- $\mathbb{K} \subset \mathbb{F}$ *kengaytma algebraik hosil qilingan;*
- $\mathbb{K} \subset \mathbb{F}$ *kengaytma murakkab algebraik.*

6.1.1-misol. $x^2 - 3$ *ko'phadni* $\mathbb{Q}(\sqrt{2})$ *maydonda keltirilmas ekanligini isbotlang.*

Yechish. Teskarisini faraz qilaylik, ya'ni $x^2 - 3$ ko'phad $\mathbb{Q}(\sqrt{2})$ maydonda ko'paytuvchilarga ajralsin. U holda

$$x^2 - 3 = (x - (a + b\sqrt{2}))(x - (c + d\sqrt{2})), \quad a, b, c, d \in \mathbb{Q}.$$

Bu tengligdan

$$x^2 - 3 = x^2 - (a + c + (b + d)\sqrt{2})x + ac + 2bd + (ad + bc)\sqrt{2}$$

ekanligi, ya'ni

$$a + c = 0, \quad b + d = 0, \quad ac + 2bd = -3, \quad ad + bc = 0$$

kelib chiqadi. Demak, $c = -a, d = -b, a^2 + 2b^2 = 3$ va $ab = 0$. Oxirgi tenglikdan $a = 0$ yoki $b = 0$ kelib chiqib, $a^2 + 2b^2 = 3$ tenglik esa, $a, b \in \mathbb{Q}$ bo'lganda o'rinli emasligi kelib chiqadi. Shunday qilib biz $x^2 - 3$ ko'phadning $\mathbb{Q}(\sqrt{2})$ maydonda keltirilmas ekanligini ko'rsatdik. $\square$

6.1.2-misol. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ *kengaytmaning bazisini toping.*

Yechish. Quyidagi $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ kengaytmalarni qaraymiz. Ma'lumki, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ kengaytmaning bazisi $\{1, \sqrt{2}\}$ bo'ladi, chunki, $x^2 - 2$ ko'phad $\mathbb{Q}$ maydon ustida $\sqrt{2}$ sonining minimal ko'phadi. Yuqoridagi 6.1.1-misolga ko'ra $x^2 - 3$ ko'phad $\mathbb{Q}\sqrt{2}$ maydon ustida $\sqrt{3}$ sonining minimal ko'phadi bo'lib, bundan $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ kengaytmaning bazisi $\{1, \sqrt{3}\}$ ekanligi kelib chiqadi. U holda 6.1.4-tasdiqqa ko'ra $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ bo'lib, uning bazisi $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ bo'ladi. $\square$

6.2 Separabel va normal kengaytmalar

Ushbu bo'limda biz separabel va normal kengaytmalarni o'rganamiz.

6.2.1-ta'rif. *Bizga $\mathbb{K}$ maydon va $f(x)$ ko'phad berilgan bo'lsin. Agar $\mathbb{K}$ maydonning qandaydir $\mathbb{F}$ kengaytmasida $f(x)$ ko'phad chiziqli ko'paytuvchilarga ajralib, kengaytma orasidagi hech qaysi maydonda chiziqli ko'paytuvchilarga ajralmasa, u holda $\mathbb{F}$ maydon $\mathbb{K}$ maydonning $f(x)$ ko'phad orqali* ***yoyilgan maydoni*** *deb ataladi.*

Boshqacha qilib aytganda, $\mathbb{F}$ maydon $f(x)$ ko‘phad chiziqli ko‘paytuvchilarga ajraluvchi eng kichik maydondir. Agar $f(x)$ ko‘phadning barcha $\alpha_1, \alpha_2, \ldots, \alpha_n$ ildizlarini o‘z ichiga oluvchi qandaydir universal maydon mayjud bo‘lsa, u holda $\mathbb{K}$ maydonning $f(x)$ ko‘phad orqali yoyilgan maydoni $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ maydondan iborat bo‘ladi.

Agar $f(x)$ ko‘phad $\mathbb{K}$ maydonda keltirilmas bo‘lib, $\mathbb{K}$ maydonning $f(x)$ ko‘phad orqali yoyilgan maydonida turli ildizlarga ega bo‘lsa, u holda bu ko‘phadga **separabel** ko‘phad deb ataladi.

6.2.2-ta’rif. *Agar $\mathbb{K}$ maydonning α algebraik elementining minimal ko‘phadi separabel bo‘lsa, u holda ushbu elementga $\mathbb{K}$ maydon ustida **separabel element** deb ataladi. $\mathbb{K} \subset \mathbb{F}$ algebraik kengaytmada ixtiyoriy $\alpha \in \mathbb{F}$ element $\mathbb{K}$ maydon ustida separabel bo‘lsa, u holda ushbu kengaytmaga **separabel kengaytma** deyiladi.*

6.2.1-tasdiq. *Xarakteristikasi nolga teng bo‘lgan maydondagi ixtiyoriy keltirilmas ko‘phad separabel bo‘ladi.*

Isbot. Aytaylik, $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ keltirilmas ko‘phad berilgan bo‘lsin. Ushbu ko’phadning formal hosilasi deb atauvchi

$$f'(x) = na_0x^{n-1} + a_1(n-1)x^{n-1} + \cdots + a_{n-1}$$

ko‘phadni qaraymiz. Ma’lumki, ushbu formal hosila uchun

$$\big(f(x) \cdot g(x)\big)' = f'(x)g(x) + f(x)g'(x)$$

tenglik o‘rinli. U holda, agar $f(x) = (x-\alpha)^m g(x)$ bo‘lsa,

$$f'(x) = (x-\alpha)^m g'(x) + m(x-\alpha)^{m-1}g(x)$$

ko‘rinishida bo‘lib, bundan $f(x)$ va $f'(x)$ ko‘phadlar umumiy ildizga ega bo‘lishi uchun $m \geq 2$ bo‘lishi zarur va yetarli ekanligi kelib chiqadi. Boshqacha aytganda, $f(x)$ ko‘phad karrali ildizga ega bo‘lmasligi, ya’ni separabel bo‘lishi uchun $f(x)$ va $f'(x)$ ko‘phadlar o‘zaro tub bo‘lishi zarur va yetarli. Xarakteristikasi nolga teng bo‘lgan maydonda ixtiyoriy $f(x)$ keltirilmas ko‘phad $f'(x)$ ko‘phad bilan o‘zaro tub bo‘lganligi uchun uning separabel ekanligini hosil qilamiz. $\square$

6.2.1-tasdiqdan quyidagi natijaga ega bo‘lamiz.

6.2.1-natija. *Xarakteristikasi nolga teng bo‘lgan maydonning ixtiyoriy algebraik kengaytmasi separabel bo‘ladi.*

Ta’kidlash joizki, ixtiyoriy maydon ustida berilgan keltirilmas $f(x)$ ko‘phad $f'(x)$ ko‘phad bilan o‘zaro tub bo‘lishi uchun $f'(x) \neq 0$ bo‘lishi zarur va yetarli.

Xarakteristikasi p ($p \neq 0$) ga teng bo'lgan maydonda esa, $f'(x) = 0$ bo'lishi uchun $f(x)$ ko'phad $f(x) = g(x^p)$ ko'rinishida ifodalanishi zarur va yetarli.

Xarakteristikasi p ($p \neq 0$) ga teng bo'lgan maydonda keltirilmas bo'lib, separabel bo'lmaydigan ko'phadlar mavjud. Masalan, xarakteristikasi p ga teng bo'lgan $\mathbb{F}$ maydon va ushbu maydondagi biror t transendent son berilgan bo'lsa, u holda $\mathbb{F}(t^p)$ maydonda $f(x) = x^p - t^p$ ko'phad keltirilmas bo'ladi. $f'(x) = px^{p-1} = 0$ ekanligidan esa $f(x)$ ko'phadning separabel emasligi kelib chiqadi. Bundan tashqari $\mathbb{F}(t^p)$ maydonning $x^p - t^p$ ko'phad orqali yoyilgan maydoni $\mathbb{F}(t)$ bo'lib, ushbu maydonda $x^p - t^p$ ko'phad p karrali bitta t ildizga ega.

6.2.1-teorema. $\mathbb{K}$ *cheksiz maydonning ixtiyoriy chekli separabel kengaytmasi sodda algebraik kengaytma bo'ladi, ya'ni agar* $\mathbb{K} \subset \mathbb{F}$ *kengaytma chekli separabel bo'lsa, u holda shunday* $\theta \in \mathbb{F}$ *algebraik element topilib,* $\mathbb{K}(\theta) = \mathbb{F}$.

Isbot. 6.1.1-teoremaga ko'ra ixtiyoriy chekli kengaytma algebraik hosil qilingan kengaytma bo'ladi. Demak, $\mathbb{K} \subset \mathbb{F}$ separabel kengaytma ham chekli bo'lganligi uchun, ushbu kengaytma ham algebraik hosil qilingan. Ya'ni shunday $\alpha_1, \alpha_2, \ldots, \alpha_m$ algebraik elementlar mavjud bo'lib. $\mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_m) = \mathbb{F}$. Biz $m = 2$ bo'lgan holda $\mathbb{K} \subset \mathbb{F}$ kengaytmaning sodda algebraik ekanligini ko'rsatishimiz yetarli. Chinki, umumiy holni $m = 2$ bo'lgan holdan induksiya orqali osongina keltirib chiqazish mumkin.

Demak, $\mathbb{F} = \mathbb{K}(\beta, \gamma)$ bo'lib, ushbu β, γ algebraik elementlarning minimal ko'phadlari $f(x)$ va $g(x)$ bo'lsin. Aytaylik, ushbu $f(x)$ va $g(x)$ ko'phadlarning ildizlari mos ravishda

$$\beta = \beta_1, \beta_2, \ldots, \beta_n \quad \text{va} \quad \gamma = \gamma_1, \gamma_2, \ldots, \gamma_s$$

bo'lsin. $f(x)$ va $g(x)$ ko'phadlar separabel bo'lganligi uchun, ushbu ildizlar turli bo'lib, quyidagi

$$\lambda_{i,j} = \frac{\beta_j - \beta_1}{\gamma_1 - \gamma_j}, \quad 2 \leq i \leq n, \ 2 \leq j \leq s$$

elementlarni qaraymiz. $\mathbb{K}$ maydon cheksiz bo'lganligi uchun bu $\lambda_{i,j}$ elementlarning hech biriga teng bo'lmagan noldan farqli c element mavjud. U holda $\theta = \beta_1 + c\gamma_1$ elementni qarasak, $\theta \neq \beta_i + c\gamma_j$, $1 \leq i \leq n, 2 \leq j \leq s$ munosabat o'rinli.

Ushbu θ element ham $\mathbb{F}$ maydonga tegishli bo'lganligi uchun, u ham algebraik bo'lib, $\mathbb{K}(\theta)$ sodda algebraik kengaytma $\mathbb{F}$ maydonning qism maydoni bo'ladi, ya'ni $\mathbb{K}(\theta) \subset \mathbb{F}$.

Ikkinchi tomondan esa, $h(x) = f(\theta - cx)$ ko'phadni qarasak, ushbu ko'phad $g(x)$ ko'phad bilan yagona umumiy ildizga ega. Chunki,

$$h(\gamma) = f(\theta - c\gamma) = f(\beta) = 0$$

bo‘lib,

$$h(\gamma_j) = f(\theta - c\gamma_j) \neq 0, \quad 2 \leq j \leq s.$$

Ya’ni faqatgina γ element $h(x)$ ko‘phadning ildizi bo‘lib, qolgan γ_i, $2 \leq j \leq s$ elementlar esa ildiz bo‘lmaydi. Bundan esa, $h(x)$ va $g(x)$ ko‘phadlarning eng kichik umumiy bo‘luvchisi $x - \gamma$ ga teng ekanligini hosil qilamiz. Biz $h(x)$ va $g(x)$ ko‘phadlarni $\mathbb{K}(\theta)$ maydon ustidagi ko‘phadlar deb qarasak, ularning umumiy bo‘luvchisi ham shu maydonga tegishli ekanligidan $\gamma \in \mathbb{K}(\theta)$ kelib chiqadi. Bundan tashqari $\beta = \theta - c\gamma$ ekanligidan $\beta \in \mathbb{K}(\theta)$, ya’ni $\mathbb{F} = \mathbb{K}(\beta, \gamma) \subset \mathbb{K}(\theta)$. Shunday qilib biz $\mathbb{F} = \mathbb{K}(\theta)$ ekanligiga ega bo‘ldik. □

6.2.3-ta’rif. *Bizga $\mathbb{K} \subset \mathbb{F}$ chekli kengaytma berilgan bo‘lsin. Agar $\mathbb{K}$ maydonda keltirilmas bo‘lib, $\mathbb{F}$ maydonda kamida bitta ildizga ega bo‘lgan ixtiyoriy $f(x)$ ko‘phad $\mathbb{F}$ maydonda chiziqli ko‘paytuvchilarga ajralsa, u holda $\mathbb{K} \subset \mathbb{F}$ kengaytmaga* ***normal kengaytma*** *deb ataladi.*

6.2.1-misol. *$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ kengaytma normal bo‘lib, $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ kengaytma esa normal emas, chunki $\mathbb{Q}(\sqrt[3]{2})$ maydonda yechimga ega bo‘lgan x^3-2 ko‘phad chiziqli ko‘paytuvchilarga ajralmaydi.*

Agar $\mathbb{K}$ maydonning α va β algebraik elementlari minimal ko‘phadlari ustma-ust tushsa, u holda ushbu algebraik elementlar **qo‘shma elementlar** deb ataladi. Boshqacha qilib aytganda algebraik elementlar bitta keltirilmas ko‘phadning ildizi bo‘lsa, u holda ular qo‘shma deyiladi. Bundan foydalanib, normal kengaytmaning qo‘shma elementlar orqali beriluvchi quyidagi ta’rifini hosil qilamiz.

6.2.4-ta’rif. *Agar $\mathbb{K} \subset \mathbb{F}$ chekli kengaytma berilgan bo‘lib, ixtiyoriy $\alpha \in \mathbb{F}$ elementning qo‘shmasi yana $\mathbb{F}$ maydonga tegishli bo‘lsa, u holda ushbu kengaytma* ***normal kengaytma*** *deyiladi.*

Quyidagi teoremada normal kengaytma bilan ko‘phad orqali yoyilgan maydon orasidagi bog‘liqlikni keltiramiz.

6.2.2-teorema. *$\mathbb{K}$ maydonning ixtiyoriy normal kengaytmasi qandaydir $f(x)$ ko‘phad orqali yoyilgan maydon bilan ustma-ust tushadi. Va aksincha, $\mathbb{K}$ maydonning ixtiyoriy $f(x)$ ko‘phad orqali yoyilgan maydoni normal kengaytma bo‘ladi.*

Isbot. Aytaylik, $\mathbb{F}$ maydon $\mathbb{K}$ maydonning normal kengaytmasi bo‘lsin. U holda $\mathbb{F}$ maydon $\mathbb{K}$ ustida chekli bo‘lib, shunday $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}$ elementlar uchun $\mathbb{F} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ bo‘ladi.

Aytaylik, $f_i(x)$ ko‘phadlar α_i elementlarga mos keluvchi $\mathbb{K}$ maydondagi minimal keltirilmas ko‘phadlar bo‘lsin. U holda $\mathbb{K} \subset \mathbb{F}$ kengaytma normal bo‘lganligi uchun ushbu $f_i(x)$ ko‘phadlar $\mathbb{F}$ maydonda chiziqli ko‘paytuvchilarga yoyiladi.

Bundan esa,

$$f(x) = f_1(x)f_2(x)\dots f_n(x)$$

ko‘phad ham $\mathbb{F}$ maydonda chiziqli ko‘paytuvchilarga yoyilishi kelib chiqadi. Demak, $\mathbb{F}$ maydon $f(x)$ ko‘phad orqali yoyilgan $\mathbb{P}$ maydonni o‘z ichiga oladi, ya’ni $\mathbb{P} \subset \mathbb{F}$.

Ikkinchi tomondan esa, $\alpha_1, \alpha_2, \dots, \alpha_n$ elementlar $f(x)$ ko‘phadning ildizlari bo‘lganligi uchun $f(x)$ ko‘phad orqali yoyilgan $\mathbb{P}$ maydon $\mathbb{K}(\alpha_1, \alpha_2, \dots, \alpha_n)$ maydonni o‘z ichiga oladi, ya’ni $\mathbb{F} \subset \mathbb{P}$. Shunday qilib biz $\mathbb{F} = \mathbb{P}$ tenglikka ega bo‘ldik.

Endi teoremaning ikkinchi qismini ya‘ni tasdiqning teskarisi o‘rinli ekanligini ko‘rsatamiz. Aytaylik, $\mathbb{F}$ maydon $\mathbb{K}$ maydonning biror $f(x)$ ko‘phadi orqali yoyilgan maydoni bo‘lsin. U holda $\mathbb{F}$ maydoning ixtiyoriy elementi $f(x)$ ko‘phadning $\alpha_1, \alpha_2, \dots, \alpha_n$ ildizlari orqali ifodalanadi. Ya’ni ixtiyoriy $\beta \in \mathbb{F}$ element uchun qandaydir $g(x_1, x_2, \dots, x_n)$ ko‘phad topilib, $\beta = g(\alpha_1, \alpha_2, \dots, \alpha_n)$ tenglik o‘rinli. Ushbu $g(x_1, x_2, \dots, x_n)$ ko‘phadning o‘zgaruvchilari o‘rinlarini almashtirish orqali yangi ko‘phadlarni hosil qilamiz. Ma’lumki, $x_1, x_2, \dots, x_n$ elementlarning o‘rin almashtirishlar soni $n!$ ta bo’lganligi uchun $g(x_1, x_2, \dots, x_n)$ ko‘phad yordamida jami $n!$ ta $g_{\varphi_i}(x_1, x_2, \dots, x_n)$ ko‘phadlar hosil qilinadi, bu yerda φ_i element S_n o‘rin almashtirishlar gruppasining elementi. Quyidagi ko’phadni qaraymiz

$$G(x) = \prod_{i=1}^{n!}(x - g_{\varphi_i}(\alpha_1, \alpha_2, \dots, \alpha_n)).$$

Ta’kidlash joizki, $G(x)$ ko‘phadning barcha koeffitsiyentlari o‘zgaruvchilari $\alpha_1, \alpha_2, \dots, \alpha_n$ bo‘lgan simmetrik ko‘phadlardan iborat bo‘ladi. Ixtiyoriy simmetrik ko‘phad, elementar simmetrik ko‘phadlar orqali ifodalanganligi va elementar simmetrik ko‘phadlarning $\alpha_1, \alpha_2, \dots, \alpha_n$ ildizlardagi qiymatlari $\mathbb{K}$ maydonda yotganligi uchun $G(x)$ ko‘phadning barcha koeffitsiyentlari ham $\mathbb{K}$ maydonga tegishli bo‘ladi.

Bundan tashqari, $\beta = g(\alpha_1, \alpha_2, \dots, \alpha_n)$ element $G(x)$ ko‘phadning ildizi bo‘lib, β elementga mos keluvchi $h(x)$ minimal ko‘phad $G(x)$ ko‘phad bilan umumiy ildizga ega. Bundan esa, $G(x)$ ko‘phadning $h(x)$ minimal ko‘phadga bo‘linishi kelib chiqadi. Bu esa, $h(x)$ ko‘phadning ixtiyoriy ildizi $G(x)$ ko‘phadning ham ildizi bo‘lishini, aniqroq qilib aytganda $g_{\varphi_i}(\alpha_1, \alpha_2, \dots, \alpha_n)$ kabi ifodalanishini anglatadi. Yani $h(x)$ ko‘phadning qolgan ildizlari ham $\mathbb{F}$ maydonda yotadi. Shunday qilib, biz $\mathbb{F}$ maydonning ixtiyoriy β elementiga qo‘shma elementlar yana $\mathbb{F}$ maydonga tegishli ekanligini hosil qildik. $\mathbb{K} \subset \mathbb{F}$ kengaytma chekli bo‘lganligi uchun uning normalligi kelib chiqadi. □

Shuni takidlash joizki, normal kengaytma uchun tranzitivlik xossasi umuman olganda o‘rinli emas. Ya’ni, $\mathbb{K} \subset \mathbb{F}$ va $\mathbb{F} \subset \mathbb{P}$ kengaytmalar normal ekanligidan $\mathbb{K} \subset \mathbb{P}$ kengaytmaning normal ekanligi har doim ham kelib chiqavermaydi.

6.2.2-misol. *$\mathbb{K} = \mathbb{Q}$, $\mathbb{F} = \mathbb{Q}(\sqrt{2})$ va $\mathbb{P} = \mathbb{Q}(\sqrt[4]{2})$ bo'lsin. Ma'lumki, $\mathbb{Q}(\sqrt{2})$ maydon $\mathbb{Q}$ ratsional sonlar maydoni ustida $x^2 - 2$ ko'phad orqali yoyilgan maydon bo'lib, o'z navbatida $\mathbb{Q}(\sqrt[4]{2})$ esa $\mathbb{Q}(\sqrt{2})$ maydon ustida $x^2 - \sqrt{2}$ ko'phad orqali yoyilgan maydondir. Ya'ni $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ va $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ kengaytmalar normal kengaytmalar bo'ladi. Lekin $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$ kengaytma normal kengaytma emas, chunki $\mathbb{Q}(\sqrt[4]{2})$ maydon ratsional sonlar maydoni ustida keltirilmas bo'lgan $x^4 - 2$ ko'phadning ildizlaridan biri $\sqrt[4]{2}$ sonini o'z ichiga olib, boshqa bir ildiz $i\sqrt[4]{2}$ esa ushbu maydonda yotmaydi.*

Quyidagi tasdiqda esa tranzitivlik xossasi o'rinli bo'lishining zaruriy va yetarlilik shartini keltiramiz.

6.2.2-tasdiq. *Bizga $\mathbb{K} \subset \mathbb{F}$ va $\mathbb{F} \subset \mathbb{P}$ normal kengaytmalar berilgan bo'lsin. $\mathbb{K} \subset \mathbb{P}$ kengaytmaning normal bo'lishi uchun $\mathbb{K}$ maydonda shunday $f(x)$ ko'phad topilib, $\mathbb{F}$ maydonning $f(x)$ ko'phad orqali yoyilgan maydoni $\mathbb{P}$ maydon bilan ustma-ust tushishi zarur va yetarli.*

Isbot. ***Zaruriyligi.*** Aytaylik, $\mathbb{K} \subset \mathbb{P}$ kengaytma normal bo'lsin. U holda $\mathbb{K}$ maydonda shunday $f(x)$ ko'phad topilib, ushbu ko'phadning barcha ildizlari $\alpha_1, \alpha_2, \ldots, \alpha_n$ uchun $\mathbb{P} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ bo'ladi. Bundan esa $\mathbb{P} \subset \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ kelib chiqadi.

Ikkinchi tomondan $\mathbb{F} \subset \mathbb{P}$ kengaytma normal ekanligidan $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{P}$ munosabatga ega bo'lamiz. Demak, $\mathbb{P} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, ya'ni $\mathbb{P}$ maydon $\mathbb{F}$ maydonning koeffitsiyentlari $\mathbb{K}$ maydondan olingan $f(x)$ ko'phad orqali yoyilgan maydoni bilan ustma-ust tushadi.

Yetarliligi. Aytaylik, koeffitsiyentlari $\mathbb{K}$ maydondan olingan $f(x)$ ko'phad uchun $\mathbb{P} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ bo'lsin, bu yerda $\alpha_1, \alpha_2, \ldots, \alpha_n$ elementlar $f(x)$ ko'phadning barcha ildizlari. $\mathbb{K} \subset \mathbb{F}$ kengaytma normal bo'lganligi uchun $\mathbb{K}$ maydonda shunday $g(x)$ ko'phad mavjudki, uning barcha $\beta_1, \beta_2, \ldots, \beta_s$ ildizlari uchun $\mathbb{F} = \mathbb{K}(\beta_1, \beta_2, \ldots, \beta_s)$. U holda $\mathbb{P} = \mathbb{K}(\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_s)$ bo'lib, ushbu α_i, β_j elementlar $f(x)g(x)$ ko'phadning barcha ildizlarini beradi. Demak, $\mathbb{P}$ maydon $\mathbb{K}$ maydonning $f(x)g(x)$ ko'phad orqali yoyilgan maydoni bo'ladi. Bu esa, $\mathbb{K} \subset \mathbb{P}$ kengaytma normal ekanligini bildiradi. $\square$

6.2.3-misol. *$\mathbb{F} = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ kengaytma uchun $\mathbb{F} = \mathbb{Q}(\theta)$ shartni qanoatlantiradigan $\theta \in \mathbb{R}$ sonini aniqlang.*

Yechish. Biz $\theta = \sqrt{2}\sqrt[3]{5}$ ekanligini ko'rsatamiz. $\sqrt{2}\sqrt[3]{5} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ bo'lganligi uchun $\mathbb{Q}(\sqrt{2}\sqrt[3]{5}) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. Ikkinchi tomondan esa $(\sqrt{2}\sqrt[3]{5})^3 = 10\sqrt{2}$ ekanligidan $\sqrt{2} \in \mathbb{Q}(\sqrt{2}\sqrt[3]{5})$ bo'lishini, bundan esa $\sqrt[3]{5} \in \mathbb{Q}(\sqrt{2}\sqrt[3]{5})$ munosabatni olamiz. Bu esa, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) \subset \mathbb{Q}(\sqrt{2}\sqrt[3]{5})$ ekanligini anglatadi. Demak, $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt{2}\sqrt[3]{5})$. $\square$

6.2.4-misol. *Agar $\mathbb{K} \subset \mathbb{F}$ kengaytmada $[\mathbb{F} : \mathbb{K}] = 2$ bo'lsa, u holda bu kengaytmaning normal ekanligini isbotlang.*

Yechish. Aytaylik, $\alpha \in \mathbb{F}$ va $\alpha \notin \mathbb{K}$ bo'lsin. U holda $\mathbb{K}(\alpha)$ kengaytmani qarasak, $\mathbb{K} \subset \mathbb{K}(\alpha) \subset \mathbb{F}$ bo'lib, $[\mathbb{F} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}(\alpha)] = [\mathbb{K}(\alpha) : \mathbb{K}]$ ekanligidan $[\mathbb{K}(\alpha) : \mathbb{K}] = 2$, ya'ni $\mathbb{F} = \mathbb{K}(\alpha)$ kelib chiqadi. Bundan $\mathbb{K}$ maydondagi ushbu α elementga mos keluvchi minimal ko'phadning darajasi ham 2 ga teng bo'lib, bu ko'phad $\mathbb{F}$ maydonda α ildizga ega ekanligi kelib chiqadi. Demak, $f(x) = (x - \alpha)(cx - d)$, $c, d \in \mathbb{F}$. Bundan esa, $f(x)$ ko'phadning ikkinchi ildizi $c^{-1}d$ ham $\mathbb{F}$ maydonda yotishi kelib chiqadi. Ya'ni $\mathbb{K} \subset \mathbb{F}$ kengaytma normal. $\square$

6.3 Galua gruppasi va uning tartibi

Bizga $\mathbb{K} \subset \mathbb{F}$ kengaytma berilgan bo'lsin. Ma'lumki, $\mathbb{F}$ maydonning barcha avtomorfizmlar to'plami $Aut(\mathbb{F})$ superpozitsiya amaliga nisbatan gruppa tashkil qiladi. $G(\mathbb{F}, \mathbb{K})$ orqali $\mathbb{K}$ maydonning barcha elementlarini o'zgarishsiz qoldiradigan avtomorfizmlar to'plamini belgilaymiz. Ya'ni

$$G(\mathbb{F}, \mathbb{K}) = \{\varphi \in Aut(\mathbb{F}) \mid \varphi(a) = a, \ \forall a \in \mathbb{K}\}.$$

Ta'kidlash joizki, $G(\mathbb{F}, \mathbb{K})$ to'plam $Aut(\mathbb{F})$ gruppaning qism gruppasi bo'ladi. Haqiqatdan ham, birlik avtomorfizm $G(\mathbb{F}, \mathbb{K})$ to'plamda yotib, ixtiyoriy $\varphi_1, \varphi_2 \in G(\mathbb{F}, \mathbb{K})$ avtomorfizmlar va $a \in \mathbb{K}$ element uchun

$$(\varphi_1 \circ \varphi_2^{-1})(a) = \varphi_1(\varphi_2^{-1}(a)) = \varphi_1(a) = a$$

ekanligidan $\varphi_1 \circ \varphi_2^{-1} \in G(\mathbb{F}, \mathbb{K})$ kelib chiqadi. Demak, $G(\mathbb{F}, \mathbb{K})$ qism gruppa.

6.3.1-ta'rif. *Agar $\mathbb{K} \subset \mathbb{F}$ kengaytma separabel va normal kengaytma bo'lsa, u holda $G(\mathbb{F}, \mathbb{K})$ gruppaga $\mathbb{F}$ maydonning $\mathbb{K}$ maydon ustidagi **Galua gruppasi** deb ataladi va $Gal(\mathbb{F}, \mathbb{K})$ kabi belgilanadi.*

Agar $\mathbb{K}$ maydonda berilgan $f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$ ko'phad $\mathbb{F}$ maydonda qandaydir α ildizga ega bo'lsa, u holda ixtiyoriy $\varphi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ uchun $\varphi(f(\alpha)) = 0$ tenglikdan

$$c_0\varphi(\alpha)^n + c_1\varphi(\alpha)^{n-1} + \cdots + c_{n-1}\varphi(\alpha) + c_n = 0$$

kelib chiqadi. Bu esa $\varphi(\alpha)$ ham $f(x)$ ko'phadning ildizi ekanligini bildiradi. Demak, Galua gruppasining ixtiyoriy elementi $f(x)$ ko'phadning ildizini yana ildizga o'tkazar ekan.

Endi bizga $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasi berilgan bo'lsin. U holda $\mathbb{K} \subset \mathbb{F}$ kengaytma separabel va normal bo'lganligi uchun, 6.2.1-teoremaga ko'ra ushbu kengaytma sodda algebraik bo'ladi. Ya'ni shunday $\alpha \in \mathbb{F}$ element topilib, $\mathbb{F} = \mathbb{K}(\alpha)$ tenglik o'rinli.

Ushbu α elementning minimal ko'phadi $f(x)$ uchun $degf(x) = n$ bo'lsa, u holda $[\mathbb{F} : \mathbb{K}] = n$ tenglik o'rinli. Demak, ixtiyoriy $\theta \in \mathbb{F}$ elementni

$$\theta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

kabi ifodalash mumkin, bu yerda $c_0, c_1, \ldots, c_{n-1} \in \mathbb{K}$.

Yuqoridagi mulohazaga asosan Galua gruppasining ixtiyoriy φ elementi ushbu α ildizni $f(x)$ ko'phadning boshqa bir $\varphi(\alpha)$ ildiziga o'tkazadi. Demak, $\forall\varphi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ avtomorfizmga $f(x)$ ko'phadning $\varphi(\alpha)$ ildizini mos qo'yish mumkin.

6.3.1-tasdiq. *α ildiz uchun $\Phi : \varphi \to \varphi(\alpha)$ ko'rinishida aniqlangan akslantirish $Gal(\mathbb{F}, \mathbb{K})$ Galua gruppasi bilan $f(x)$ ko'phadning ildizlari orasida o'zaro bir qiymatli moslik o'rnatadi.*

Isbot. Aytaylik, β element $f(x)$ ko'phadning qandaydir ildizi bo'lsin. U holda $\mathbb{K} \subset \mathbb{F}$ kengaytmaning normalligi va $\alpha \in \mathbb{F}$ ekanligidan $\beta \in \mathbb{F}$ kelib chiqadi.

Endi ixtiyoriy $\theta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$ element uchun

$$\varphi(\theta) = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}$$

kabi aniqlangan $\varphi : \mathbb{F} \to \mathbb{F}$ akslantirishni qaraymiz. Ushbu akslantirishni $g(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ ko'phad uchun

$$\theta = g(\alpha) \quad \text{bo'lsa}, \quad \varphi(\theta) = g(\beta)$$

kabi aniqlash mumkin.

Ta'kidlash joizki, akslantirishning $g(x)$ ko'phad orqali aniqlanishi ko'phadning darajasiga bog'liq emas. Chunki, agar $deg(g(x)) \geq n$ bo'lsa, u holda $g(x)$ ko'phadni $f(x)$ ko'phadga qoldiqli bo'lib,

$$g(x) = f(x)q(x) + r(x)$$

tenglikdan $\theta = g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$ ekanligiga ega bo'lamiz. $r(x)$ ko'phadning darajasi n dan kichik bo'lganligi uchun $\varphi(\theta) = r(\beta)$ bo'lib, ikkinchi tomondan esa $g(\beta) = f(\beta)q(\beta) + r(\beta) = r(\beta)$ ekanligidan $\varphi(\theta) = g(\beta)$ kelib chiqadi, ya'ni ixtiyoriy $g(x)$ ko'phad uchun $\varphi(g(\alpha)) = g(\beta)$.

Endi ushbu aniqlangan φ akslantirishni avtomorfizm ekanligini ko'rsatamiz. Aytaylik, bizga ixtiyoriy $\theta_1, \theta_2 \in \mathbb{F}$ elementlar berilgan bo'lsin. U holda $g_1(x)$ va $g_2(x)$ ko'phadlar topilib, $\theta_1 = g_1(\alpha)$ va $\theta_2 = g_2(\alpha)$. Bundan tashqari,

$$\theta_1 + \theta_2 = g_1(\alpha) + g_2(\alpha), \quad \theta_1\theta_2 = g_1(\alpha)g_2(\alpha)$$

ekanligidan

$$\varphi(\theta_1 + \theta_2) = \varphi(g_1(\alpha) + g_2(\alpha)) = g_1(\beta) + g_2(\beta) = \varphi(\theta_1) + \varphi(\theta_2)$$

$$\varphi(\theta_1\theta_2) = \varphi(g_1(\alpha)g_2(\alpha)) = g_1(\beta)g_2(\beta) = \varphi(\theta_1)\varphi(\theta_2)$$

kelib chiqadi. Demak, φ akslantirish $\mathbb{F}$ maydondagi qo‘shish va ko‘paytirish amallarini saqlaydi. Endi φ akslantirishning biyektiv ekanligini ko‘rsatamiz. Buning uchun $\mathbb{K}(\beta)$ maydonni qarasak, $\beta \in \mathbb{F}$ bo‘lganligi uchun $\mathbb{K}(\beta) \subset \mathbb{F}$. Ikkinchi tomondan esa, $[\mathbb{F} : \mathbb{K}(\beta)] = deg(f(x)) = n$ bo‘lganligi uchun $\mathbb{K}(\beta) = \mathbb{F}$. Bu esa ixtiyoriy $\theta \in \mathbb{F}$ elementni

$$\theta = c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1}$$

kabi ifodalash mumkinligini beradi. Agar yuqoridagi kabi

$$\psi(\theta) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

akslantirishni aniqlasak, u holda $\psi \circ \varphi = \varphi \circ \psi = \mathrm{id}$ bo‘lib, ushbu ψ akslantirish φ akslantirishning teskarisi ekanligi kelib chiqadi. Demak, φ gomomorfizm teskarilanuvchi, ya’ni avtomorfizm.

Ushbu φ avtomorfizm $\mathbb{K}$ maydonning elementlarini o‘zgarishsiz qoldirganligi uchun $\varphi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$. Demak, $f(x)$ ko‘phadning ixtiyoriy β ildizi uchun $\varphi(\alpha) = \beta$ shartni qanoatlantiruvchi $\varphi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ avtomorfizm aniqlandi.

Endi bunday avtomorfizmning yagona ravishda aniqlanishini ko‘rsatamiz. Faraz qilaylik, $\varphi, \psi \in Gal(\mathbb{F}, \mathbb{K})$ avtomorfizmlar uchun $\varphi(\alpha) = \beta$ va $\psi(\alpha) = \beta$ bo‘lsin. U holda $\varphi(\alpha) = \psi(\alpha)$ ekanligidan $(\psi^{-1} \circ \varphi)(\alpha) = \alpha$ kelib chiqadi. Ya’ni $\psi^{-1} \circ \varphi$ avtomorfizm α elementni o‘zgarishsiz qoldiradi. Ixtiyoriy θ element α orqali $\theta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$ kabi ifodalanganligi uchun $(\psi^{-1} \circ \varphi)(\theta) = \theta$. Demak, $\psi^{-1} \circ \varphi = \mathrm{id}$, ya’ni $\varphi = \psi$. $\square$

Yuqorida isbotlangan tasdiqdan quyidagi natijaga ega bo‘lamiz.

6.3.1-natija. *$Gal(\mathbb{F}, \mathbb{K})$ Galua gruppasining tartibi $\mathbb{K}$ maydonning $\mathbb{F}$ maydon bo‘yicha darajasiga teng, ya’ni $|Gal(\mathbb{F}, \mathbb{K})| = [\mathbb{F} : \mathbb{K}]$.*

6.3.1-misol. *Agar $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ kengaytmaning separabel va normal ekanligini isbotlang va ushbu kengaytmaning Galua gruppasi tartibini aniqlang.*

Yechish. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ kengaytmalarni qarasak, $x^2 - 2$ ko‘phad $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ kengaytma uchun minimal hamda x^2-3 ko‘phad $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ kengaytma uchun minimal ko‘phadlar bo‘lganligidan $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ va $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Demak, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

Ushbu kengaytma algebraik ekanligi va ratsional sonlar maydonining xarakteristikasi nolga teng bo‘lganligi uchun bu kengaytma separabel bo‘ladi. Endi uning normal ekanligini ko‘rsatamiz. $f(x) = (x^2 - 2)(x^2 - 3)$ ko‘phad $\mathbb{Q}$ maydon ustida keltirilmas bo‘lib, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ maydonda

$$f(x) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$$

kabi chiziqli ko‘paytuvchilarga ajraladi. Bundan esa, $\mathbb{Q}(\sqrt{2},\sqrt{3})$ maydon $f(x)$ ko‘phad orqali yoyilgan maydon ekanligi kelib chiqadi. U holda 6.2.2-teoremaga ko‘ra $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$ kengaytma normal bo‘lib, 6.3.1-natijaga ko‘ra esa $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}),\mathbb{Q})| = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4.$ □

6.4 Galua nazariyasining fundamental teoremasi

Aytaylik, $\mathbb{K} \subset \mathbb{F}$ separabel va normal kengaytma berilgan bo‘lib, $\mathbb{K}(\theta) = \mathbb{F}$ bo‘lsin. Ushbu θ elementga mos keluvchi $\mathbb{K}$ maydon ustida berilan minimal $f(x)$ ko‘phadni ixtiyoriy $\mathbb{L}$ ($\mathbb{K} \subset \mathbb{L} \subset \mathbb{F}$) oraliq maydon ustida berilgan deb ham qarash mumkin. U holda $f(x)$ ko‘phad $\mathbb{L}$ maydonda ham separabel bo‘lib, $\mathbb{L}$ maydonning ushbu ko‘phad orqali yoyilgan maydoni $\mathbb{L}(\theta)$ bilan ustma-ust tushadi. Bundan tashqari, $\mathbb{L}(\theta)$ maydon $\mathbb{L}$ ning separabel va normal kengaytmasi bo‘lib, $\mathbb{L}(\theta) \subset \mathbb{F}$.

Ikkinchi tomondan esa, $\mathbb{K} \subset \mathbb{L}$ va $\theta \in \mathbb{K}$ ekanligidan $\mathbb{K}(\theta) \subset \mathbb{L}(\theta)$, ya’ni $\mathbb{F} \subset \mathbb{L}(\theta)$ kelib chiqadi. Shunday qilib biz $\mathbb{F} = \mathbb{L}(\theta)$ ekanligini, bundan esa $\mathbb{L} \subset \mathbb{F}$ kengaytma ham separabel va normal bo‘lishini hosil qildik.

Demak, bizga qangaydir $\mathrm{Gal}(\mathbb{F},\mathbb{K})$ Galua gruppasi berilgan bo‘lsa, u holda $\mathbb{K} \subset \mathbb{L} \subset \mathbb{F}$ shartni qanoatlantiruvchi ixtiyoriy $\mathbb{L}$ maydon uchun $\mathrm{Gal}(\mathbb{F},\mathbb{L})$ Galua gruppasini qarash mumkin.

6.4.1-tasdiq. $\mathbb{K} \subset \mathbb{F}$ *maydonlarning orasidagi ixtiyoriy* $\mathbb{L}$ *maydon uchun* *Gal*$(\mathbb{F},\mathbb{L})$ *Galua gruppasi* *Gal*$(\mathbb{F},\mathbb{K})$ *Galua gruppasining qism gruppasi bo‘ladi va uning tartibi* $[\mathbb{F} : \mathbb{L}]$ *ga teng.*

Isbot. $\mathrm{Gal}(\mathbb{F},\mathbb{L})$ Galua gruppasining elementlari $\mathbb{L}$ maydonning barcha elementlarini o‘z joyida qoldiruvchi avtomorfizmlar to‘plamidan iborat bo‘lganligi va $\mathbb{K} \subset \mathbb{L}$ ekanligi uchun ixtiyoriy $\varphi \in \mathrm{Gal}(\mathbb{F},\mathbb{L})$ element $\mathbb{K}$ maydonning barcha elementlarini o‘z joyida qoldiradi. Demak, $\varphi \in \mathrm{Gal}(\mathbb{F},\mathbb{K})$, ya’ni $\mathrm{Gal}(\mathbb{F},\mathbb{L}) \subset \mathrm{Gal}(\mathbb{F},\mathbb{K})$. Ushbu $\mathrm{Gal}(\mathbb{F},\mathbb{L})$ gruppaning tartibi $[\mathbb{F} : \mathbb{L}]$ ga teng ekanligi esa, 6.3.1-natijadan kelib chiqadi. □

Endi $\mathrm{Gal}(\mathbb{F},\mathbb{K})$ Galua gruppasining ixtiyoriy H qism gruppasi uchun quyidagi to‘plamni aniqlaymiz

$$\mathbb{F}_H = \{a \in \mathbb{F} \mid \varphi(a) = a,\ \forall\ \varphi \in H\}.$$

Ya’ni $\mathbb{F}_H$ to‘plam $\mathbb{F}$ maydonning H avtomorfizmlar qism to‘plamining ixtiyoriy avtomorfizmida o‘zgarishsiz qoladigan elementlaridan idorat to‘plam. Ravshanki, ushbu $\mathbb{F}_H$ to‘plam ham maydon bo‘lib, $\mathbb{K} \subset \mathbb{F}_H \subset \mathbb{F}$ munosabat o‘rinli.

6.4.2-tasdiq. *Gal*$(\mathbb{F},\mathbb{F}_H) = H$.

Isbot. Aytaylik, $\mathbb{F} = \mathbb{F}_H(\theta)$ va $|H| = m$ bo‘lib, H gruppaning elementlari

$$\varphi_1 = \mathrm{id},\ \varphi_2,\ \ldots,\ \varphi_m$$

bo‘lsin. Quyidagi ko‘phadni qaraymiz

$$h(x) = \prod_{i=1}^{m}(x - \varphi_i(\theta)).$$

Ma’lumki, ushbu ko‘phadning ildizlari

$$\varphi_1(\theta) = \theta,\ \varphi_2(\theta),\ \ldots,\ \varphi_m(\theta) \tag{6.1}$$

elementlardan iborat bo‘ladi. Ixtiyoriy $\psi \in H$ avtomorfizm uchun

$$\psi(\varphi_1(\theta)) = \psi(\theta),\ \psi(\varphi_2(\theta)),\ \ldots,\ \psi(\varphi_m(\theta)) \tag{6.2}$$

elementlarni qarasak, $\psi\varphi_1, \psi\varphi_2, \ldots, \psi\varphi_m$ avtomorfizmlar H gruppaning barcha elementlarini berganligi uchun ushbu elementlar (6.1) elementlar bilan ustma-ust tushadi. Boshqacha qilib aytganda, ixtiyoriy $\psi \in H$ avtomorfizm uchun $h(x)$ ko‘phadning ildizlari faqat o‘rinlarini almashtiradi. Demak, o‘zgaruvchilari $\varphi_1(\theta), \varphi_2(\theta), \ldots, \varphi_m(\theta)$ bo‘lgan ixtiyoriy simmetrik ko‘phadning qiymati ixtiyoriy ψ avtomorfizmda o‘zgarishsiz qoladi. $h(x)$ ko‘phadning barcha koeffitsiyentlari o‘zgaruvchilari $\varphi_1(\theta), \varphi_2(\theta), \ldots, \varphi_m(\theta)$ bo‘lgan elementar simmetrik ko‘phadlardan iborat bolganligi uchun $h(x)$ ko‘phadning barcha koeffitsiyentlari ixtiyoriy $\psi \in H$ avtomorfizmda o‘zgarishsiz qoladi.

Demak, $h(x)$ ko‘phadning koeffitsiyentlari $\mathbb{F}_H$ maydonga tegishli, ya’ni $h(x)$ ko‘phad $\mathbb{F}_H$ maydondagi ko‘phad bo‘ladi. Ushbu $h(x)$ ko‘phad θ ildizga ega bo‘lganligi uchun θ elementning $f(x)$ minimal ko‘phadi $h(x)$ ko‘phadning bo‘luvchisi bo‘ladi. Bundan esa, $deg(f(x)) \leq deg(h(x)) = m$ kelib chiqib, $[\mathbb{F} : \mathbb{F}_H] \leq deg(f(x)) \leq m$ ekanligini hosil qilamiz.

Endi $\mathbb{F}_H$ maydon uchun $\mathrm{Gal}(\mathbb{F}, \mathbb{F}_H)$ Galua gruppasini qarasak, $|\mathrm{Gal}(\mathbb{F}, \mathbb{F}_H)| = [\mathbb{F} : \mathbb{F}_H]$ bo‘lib, ikkinchi tomondan esa, $\mathrm{Gal}(\mathbb{F}, \mathbb{F}_H)$ Galua gruppasi $\mathbb{F}_H$ maydonning barcha elementlarini o‘z joyida qoldiruvchi avtomorfizmlardan iborat, ya’ni H gruppaning barcha elementlarini o‘z ichiga oladi. Demak, $|\mathrm{Gal}(\mathbb{F}, \mathbb{F}_H)| \geq m$. Shunday qilib biz $\mathrm{Gal}(\mathbb{F}, \mathbb{F}_H) = H$ ekanligiga ega bo‘ldik. □

Endi $\mathbb{K} \subset \mathbb{F}$ maydonlarning orasidagi ixtiyoriy $\mathbb{L}$ maydon uchun $H = \mathrm{Gal}(\mathbb{F}, \mathbb{L})$ gruppani olib, $\mathbb{F}_H$ maydonni qaraymiz. Ma’lumki, $\mathbb{L} \subset \mathbb{F}_H$ bo‘lib,

$$[\mathbb{F} : \mathbb{L}] = [\mathbb{F} : \mathbb{F}_H] \cdot [\mathbb{F}_H : \mathbb{L}]$$

tenglik o‘rinli.

Ikkinchi tomondan esa,

$$[\mathbb{F} : \mathbb{F}_H] = |\mathrm{Gal}(\mathbb{F}, \mathbb{F}_H)| = |H| = |\mathrm{Gal}(\mathbb{F}, \mathbb{L})| = [\mathbb{F} : \mathbb{L}]$$

ekanligidan $[\mathbb{F}_H : \mathbb{L}] = 1$ kelib chiqadi. Demak, biz quyidagi natijaga ega bo‘lamiz.

6.4.1-natija. *$H = Gal(\mathbb{F}, \mathbb{L})$ gruppa uchun $\mathbb{F}_H = \mathbb{L}$ bo'ladi.*

Demak, $\mathbb{K} \subset \mathbb{F}$ kengaytma orasidagi ixtiyoriy $\mathbb{L}$ maydonga $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ gruppaning $H = \mathrm{Gal}(\mathbb{F}, \mathbb{L})$ qism gruppasini, va aksincha $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining ixtiyoriy H qism gruppasiga $\mathbb{F}_H$ maydonni mos qo'yish mumkin. Bundan tashqari, turli $\mathbb{L}_1$ va $\mathbb{L}_2$ maydonlarga turli qism gruppalar mos keladi. Chunki, agar $\mathrm{Gal}(\mathbb{F}, \mathbb{L}_1) = \mathrm{Gal}(\mathbb{F}, \mathbb{L}_2)$ bo'lsa, u holda $\mathbb{L}_1 = \mathbb{F}_{\mathrm{Gal}(\mathbb{F}, \mathbb{L}_1)} = \mathbb{F}_{\mathrm{Gal}(\mathbb{F}, \mathbb{L}_2)} = \mathbb{L}_2$.

Shunday qilib biz guyidagi teoremaga ega bo'ldik.

6.4.1-teorema (Galua nazariyasining fundamental teoremasi). *$\mathbb{K} \subset \mathbb{F}$ separabel va normal kengaytmaning orasidagi maydonlar to'plami bilan $Gal(\mathbb{F}, \mathbb{K})$ Galua gruppasining qism gruppalari to'plami orasida o'zaro bir qiymatli moslik mavjud. Bunda $\mathbb{L}$ maydonga $Gal(\mathbb{F}, \mathbb{L})$ qism gruppa va $H \subset Gal(\mathbb{F}, \mathbb{K})$ qism gruppaga esa $\mathbb{F}_H$ maydon mos keladi. Bundan tashqari, $|Gal(\mathbb{F}, \mathbb{L})| = [\mathbb{F} : \mathbb{L}]$ va $[\mathbb{F} : \mathbb{F}_H] = |H|$.*

Ta'kidlash joizki, $\mathbb{K} \subset \mathbb{F}$ separabel va normal kengaytmaning orasidagi maydonlar to'plami bilan $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining qism gruppalari orasidagi ushbu moslikda $\mathbb{K}$ maydonga $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining o'zi mos kelsa, gruppaning faqat birlik elementdan tashkil topgan qism gruppasiga esa $\mathbb{F}$ maydon mos keladi. Bundan tashqari ushbu moslikda $\mathbb{F}$ maydonning $\mathbb{L}_1$ va $\mathbb{L}_2$ qism maydonlari uchun $\mathbb{L}_1 \subset \mathbb{L}_2$ munosabat o'rinli bo'lsa, u holda bu qism maydonlarga mos keluvchi H_1 va H_2 qism gruppalar uchun $H_1 \supset H_2$ bo'ladi.

6.4.1-misol. *Agar $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ kengaytmani qarasak, u holda 6.3.1-misolga ko'ra $|Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})| = 4$ bo'lib, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$ Galua gruppasi $\mathbb{Z}_4$ va $\mathbf{K}_4 = \{e, a, b, ab\}$ gruppalardan biriga izomorf bo'ladi. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ kengaytmaning orasida ikkita $\mathbb{Q}(\sqrt{2})$ va $\mathbb{Q}(\sqrt{3})$ maydonlar bo'lganligi uchun ushbu Galua gruppasining ham tartibi 2 ga teng bo'lgan kamida ikkita qism gruppasi mavjud. Bundan esa $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}) \simeq \mathbf{K}_4$ kelib chiqadi. Galua nazariyasining fundamental teoremasiga ko'ra qism maydonlar va qism gruppalar orasidagi quyidagicha moslikni o'rnatish mumkin*

$$\mathbb{Q} \leftrightarrow \mathbf{K}_4, \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}) \leftrightarrow \{e\},$$

$$\mathbb{Q}(\sqrt{2}) \leftrightarrow \{e, a\}, \quad \mathbb{Q}(\sqrt{3}) \leftrightarrow \{e, b\}, \quad \mathbb{Q}(\sqrt{6}) \leftrightarrow \{e, ab\}.$$

Endi $\mathbb{K} \subset \mathbb{F}$ kengaytma orasidagi $\mathbb{L}$ maydon $\mathbb{K}$ maydonning normal kengaytmasi bo'lgan holni qaraymiz.

Dastlab, quyidagi tasdiqni keltiramiz.

6.4.3-tasdiq. *$\mathbb{K} \subset \mathbb{F}$ separabel va normal kengaytmada $\alpha, \beta \in \mathbb{F}$ elementlar $\mathbb{K}$ maydonda qo'shma bo'lishi uchun, shunday $\varphi \in Gal(\mathbb{F}, \mathbb{K})$ avtomorfizm topilib, $\beta = \varphi(\alpha)$ bo'lishi zarur va yetarli.*

Isbot. Aytyaylik, $\beta = \varphi(\alpha)$ bo'lib, $f(x)$ ko'phad α elementning minimal ko'phadi bo'lsin. $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining ixtiyoriy avtomorfizmi $\mathbb{K}$ maydondagi ixtiyoriy ko'phad ildizini yana ildizga o'tkazganligi uchun $f(\beta) = 0$. Demak, α va β elementlar qo'shma bo'ladi.

Aksincha, aytaylik, α va β elementlar qo'shma bo'lsin. $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ gruppaning barcha elementlarini

$$\varphi_1 = \mathrm{id}, \varphi_2, \ldots, \varphi_n$$

deb olib,

$$\varphi_1(\alpha) = \alpha, \varphi_2(\alpha), \ldots, \varphi_n(\alpha) \tag{6.3}$$

elementlarni qaraymiz. Ixtiyoriy $\psi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ avtomorfizm uchun

$$\psi(\varphi_1(\alpha)), \psi(\varphi_2(\alpha)), \ldots, \psi(\varphi_n(\alpha)) \tag{6.4}$$

elementlarni qarasak, ushbu elementlar (6.3) elementlarning o'rinlarini almashtirishdan hosil bo'lgan elementlar bo'ladi. Demak,

$$g(x) = \prod_{i=1}^{n}(x - \varphi_i(\alpha))$$

ko'phadning barcha koeffitsiyentlari ixtiyoriy $\psi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ avtomorfizmda o'zgarishsiz qoladi, ya'ni $g(x)$ ko'phad $\mathbb{K}$ maydonda aniqlangan ko'phad bo'ladi. Berilgan α element $g(x)$ ko'phadning ildizi bo'lganligi uchun α elementning minimal $f(x)$ ko'phadi $g(x)$ ko'phadning bo'luvchisi bo'ladi. Bundan esa $f(x)$ ko'phadning β ildizi ham $g(x)$ ko'phadning ildizi ekanligi kelib chiqadi. $g(x)$ ko'phadning barcha ildizlari $\varphi_j(\alpha)$ ko'rinishida bo'lganligi uchun qanaydir j uchun $\beta = \varphi_j(\alpha)$. □

Quyidagi teoremada normal kengaytmaga aynan normal qism gruppa mos kelishi ko'rsatiladi.

6.4.2-teorema. *Agar $\mathbb{K} \subset \mathbb{F}$ separabel va normal kengaytmaning orasidagi $\mathbb{L}$ maydon $\mathbb{K}$ maydonning normal kengaytmasi bo'lsa, u holda $Gal(\mathbb{F}, \mathbb{L})$ gruppa $Gal(\mathbb{F}, \mathbb{K})$ Galua gruppasining normal qism gruppasi bo'ladi. Bundan tashqari, $Gal(\mathbb{F}, \mathbb{K})$ Galua gruppasining ixtiyoriy H normal qism gruppasiga mos keluvchi $\mathbb{F}_H$ maydon $\mathbb{K}$ maydonning normal kengaytmasi bo'ladi.*

Isbot. Aytaylik $\mathbb{K} \subset \mathbb{L}$ kengaytma normal bo'lsin. U holda 6.4.3-tasdiqqa ko'ra ixtiyoriy $\alpha \in \mathbb{L}$ element va $\varphi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ avtomorfizm uchun $\varphi(\alpha)$ element α bilan qo'shma bo'ladi. $\mathbb{K} \subset \mathbb{L}$ kengaytma normal bo'lganligi uchun α elementning qo'shmasi yana $\mathbb{L}$ maydonga tegishli, ya'ni $\varphi(\alpha) \in \mathbb{L}$. Demak, $\varphi : \mathbb{F} \to \mathbb{F}$ avtomorfizmni $\mathbb{L}$ maydonda aniqlangan deb qarash mumkin. Aniqroq qilib aytganda, $\mathbb{L}$ maydonda quyidagicha φ' akslantirishni aniqlaymiz.

$$\varphi'(\alpha) = \varphi(\alpha), \quad \forall \alpha \in \mathbb{L}.$$

Ushbu φ' akslantirish $\mathbb{L}$ maydondagi avtomorfizm bo‘lib, $\mathbb{K}$ maydonning elementlarini o‘zgarishsiz qoldiradi, ya’ni $\varphi' \in \mathrm{Gal}(\mathbb{L},\mathbb{K})$. Demak, biz $\mathrm{Gal}(\mathbb{F},\mathbb{K})$ gruppaning ixtiyoriy φ elementiga $\mathrm{Gal}(\mathbb{L},\mathbb{K})$ gruppaning φ' elementini mos qo‘ydik. Ushbu moslik, bu ikkita gruppa o‘rtasidagi gomomorfizmdir. Ya’ni $\Psi(\varphi) = \varphi'$ kabi aniqlangan $\Psi : \mathrm{Gal}(\mathbb{F},\mathbb{K}) \to \mathrm{Gal}(\mathbb{L},\mathbb{K})$ akslantirihsh uchun

$$\Psi(\varphi \circ \psi) = \Psi(\varphi) \circ \Psi(\psi)$$

munosabat o‘rinli. Ushbu Ψ gomomorfizmning yadrosi $\mathbb{L}$ maydonning barcha elementlarini o‘zgarishsiz qoldiradigan avtomorfizmlardan iborat bo‘ladi, ya’ni $\mathrm{Ker}\Psi = \mathrm{Gal}(\mathbb{F},\mathbb{L})$. Ixtiyoriy gomomorfizmning yadrosi normal qism gruppa bo‘lganligi uchun $\mathrm{Gal}(\mathbb{F},\mathbb{L})$ gruppa $\mathrm{Gal}(\mathbb{F},\mathbb{K})$ Galua gruppasining normal qism gruppasi ekanligini hosil qilamiz. Demak, teoremaning birinchi qismi isbotlandi.

Aytaylik, $\mathrm{Gal}(\mathbb{F},\mathbb{K})$ Galua gruppasining ixtiyoriy H normal qism gruppasiga mos keluvchi $\mathbb{F}_H$ maydon berilgan bo‘lsin. H normal ekanligidan ixtiyoriy $\psi \in H$ va $\varphi \in \mathrm{Gal}(\mathbb{F},\mathbb{K})$ elementlar uchun $\varphi^{-1} \circ \psi \circ \varphi \in H$. Ya’ni ixtiyoriy $\alpha \in \mathbb{F}_H$ uchun $(\varphi^{-1} \circ \psi \circ \varphi)(\alpha) = \alpha$. Bundan esa, $\psi(\varphi(\alpha)) = \varphi(\alpha)$ tenglikni, ya’ni $\varphi(\alpha) \in \mathbb{F}_H$ ekanligini hosil qilamiz. Bu esa, $\mathbb{F}_H$ maydonning ixtiyoriy elementiga qo‘shma element yana shu maydonga tegishli ekanligini, ya’ni $\mathbb{F}_H$ maydonning normalligini bildiradi. □

Yuqoridagi teoremadan quyidagi natijani hosil qilamiz.

6.4.2-natija. *Agar $\mathbb{K} \subset \mathbb{F}$ separabel va normal kengaytmaning orasidagi $\mathbb{L}$ maydon $\mathbb{K}$ maydonning normal kengaytmasi bo‘lsa, u holda*

$$Gal(\mathbb{L},\mathbb{K}) \simeq Gal(\mathbb{F},\mathbb{K})/Gal(\mathbb{F},\mathbb{L}).$$

Isbot. Biz yuqoridagi teorema isbotida $\Psi : \mathrm{Gal}(\mathbb{F},\mathbb{K}) \to \mathrm{Gal}(\mathbb{L},\mathbb{K})$ gomomorfizm qurib, ushbu gomomorfizmning yadrosi $\mathrm{Gal}(\mathbb{F},\mathbb{L})$ ga teng ekanligini ko‘rsatdik. Agar biz ushbu gomomorfizmning syurektiv ekanligini ko‘rsatsak, u holda izomorfizm haqidagi birinchi teoremaga ko‘ra natijaning isbotiga ega bo‘lamiz. Ma’lumki,

$$|\Psi(\mathrm{Gal}(\mathbb{F},\mathbb{K}))| = [\mathrm{Gal}(\mathbb{F},\mathbb{K}) : \mathrm{Gal}(\mathbb{F},\mathbb{L})],$$

ya’ni Ψ gomomorfizm obrazining elementlari soni $\mathrm{Gal}(\mathbb{F},\mathbb{L})$ qism gruppaning $\mathrm{Gal}(\mathbb{F},\mathbb{K})$ gruppadagi indeksiga teng.

Ikkinchi tomindan gruppalar uchun Lagranj teoremasi va 6.1.4-tasdiqqa ko‘ra

$$[\mathrm{Gal}(\mathbb{F},\mathbb{K}) : \mathrm{Gal}(\mathbb{F},\mathbb{L})] = \frac{|\mathrm{Gal}(\mathbb{F},\mathbb{K})|}{|\mathrm{Gal}(\mathbb{F},\mathbb{L})|} = \frac{[\mathbb{F}:\mathbb{K}]}{[\mathbb{F}:\mathbb{L}]} = [\mathbb{L}:\mathbb{K}] = |\mathrm{Gal}(\mathbb{L},\mathbb{K})|$$

Bu esa, $\Psi(\mathrm{Gal}(\mathbb{F},\mathbb{K})) = \mathrm{Gal}(\mathbb{L},\mathbb{K})$ ekanligini, ya’ni Ψ gomomorfizmning syurektivligini bildiradi.

□

6.4.2-misol. *Aytaylik, $\mathbb{F}$ maydon $\mathbb{Q}$ maydonning x^3-2 ko'phad orqali yoyilgan maydoni bo'lsin. U holda*

$$x^3-2=(x-\sqrt[3]{2})(x+\frac{\sqrt[3]{2}}{2}(1-\sqrt{3}i))(x+\frac{\sqrt[3]{2}}{2}(1+\sqrt{3}i))$$

ekanligidan $\mathbb{F}=\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)$ kelib chiqadi. Agar $\mathbb{Q}\subset\mathbb{Q}(\sqrt[3]{2})\subset\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)$ kengaytmalarni qarasak, x^3-2 va $x^2+\sqrt[3]{2}x+\sqrt[3]{4}$ ko'phadlar mos ravishda $\mathbb{Q}\subset\mathbb{Q}(\sqrt[3]{2})$ va $\mathbb{Q}(\sqrt[3]{2})\subset\mathbb{Q}(\sqrt[3]{2},\sqrt{3}i)$ kengaytmalar uchun minimal ko'phadlar bo'lganligi uchun $[\mathbb{F}:\mathbb{Q}]=[\mathbb{F}:\mathbb{Q}(\sqrt[3]{2})]\cdot[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=6$. Demak, $|Gal(\mathbb{F},\mathbb{Q})|=6$.

Endi ushbu Galua gruppasining elementlarini aniqlaymiz. Buning uchun x^3-2 ko'phadning ildizlarini

$$r_1=\sqrt[3]{2},\quad r_2=\frac{\sqrt[3]{2}}{2}(-1+\sqrt{3}i),\quad r_3=\frac{\sqrt[3]{2}}{2}(-1-\sqrt{3}i)$$

kabi belgilab olsak, ixtiyoriy $\varphi\in Gal(\mathbb{F},\mathbb{Q})$ avtomorfizmni ushbu ildizlardagi qiymatlar orqali aniqlanash mumkin. Ya'ni barcha avtomorfizmlar r_1,r_2,r_3 elementlarning o'rinlarini almashtiruvchi aklantirishlardan iborat bo'ladi. Demak, $Gal(\mathbb{F},\mathbb{Q})$ Galua gruppasi S_3 o'rin almashtirishlar gruppasiga izomorf.

U holda S_3 o'rin almashtirishlar gruppasining xosmas qism gruppalari

$$H_1=\{e,(1,2)\},\quad H_2=\{e,(1,3)\},\quad H_3=\{e,(2,3)\},\quad H_4=\{e,(1,2,3),(1,3,2)\}$$

bo'lganligi uchun bu qism gruppalarga mos keluvchi oraliq maydonlar quyidagicha bo'ladi

$$\mathbb{L}_1=\mathbb{Q}(r_1),\quad \mathbb{L}_2=\mathbb{Q}(r_2),\quad \mathbb{L}_2=\mathbb{Q}(r_3),\quad \mathbb{L}_4=\mathbb{Q}(\sqrt{3}i).$$

H_1,H_2,H_3 qism gruppalar S_3 o'rin almashtirishlar gruppasining normal qism gurppasi bo'lmaganligi uchun $\mathbb{L}_1,\mathbb{L}_2,\mathbb{L}_3$ kengaytmalar ham normal emas, lekin H_4 gruppa normal qism gruppa bo'lib, unga mos keluvchi $\mathbb{L}_4=\mathbb{Q}(\sqrt{3}i)$ maydon ham $\mathbb{Q}$ maydonning normal kengaytmasi bo'ladi.

6.5 Tenglamalarning radikallarda yechilishi

Bizga $\mathbb{K}$ maydonda $f(x)$ separabel ko'phad berilgan bo'lib, $\mathbb{F}$ maydon esa $\mathbb{K}$ maydonning $f(x)$ ko'phad orqali yoyilgan maydoni bo'lsin.

6.5.1-ta'rif. *$\mathbb{K}$ maydondagi $f(x)$ ko'phadni Galua gruppasi deb, $Gal(\mathbb{F},\mathbb{K})$ gruppaga aytiladi, bu yerda $\mathbb{F}$ maydon $\mathbb{K}$ maydonning $f(x)$ ko'phad orqali yoyilgan maydoni.*

Aytaylik, $f(x)$ ko'pdanning ildizlari $\alpha_1,\alpha_2,\ldots,\alpha_n$ bo'lsin. Ma'lumki, Galua gruppasining har bir $\varphi\in Gal(\mathbb{F},\mathbb{K})$ elementi va ixtiyoriy α_i ildiz uchun $\varphi(\alpha_i)$

element yana $f(x)$ ko'phadning ildizi bo'ladi. φ avtomorfizm o'zari bir qiymatli akslantirish bo'lganligi va $\alpha_1, \alpha_2, \ldots, \alpha_n$ ildizlar turli xil ekanligi uchun ushbu φ avtomorfizmni S_n gruppaning elementi sifatida qarasa bo'ladi. Demak, darajasi n ga teng bo'lgan $f(x)$ ko'phadning Galua gruppasini S_n gruppaning qism gruppasi sifatida qarash mumkin.

Biz dastlab, xarakteristikasi 3 dan farqli bo'lgan ixtiyoriy maydonda berilgan kubik ko'phadning Galua gruppasini o'rganamiz. Ma'lumki, ixtiyoriy

$$f(x) = x^3 + \beta x^2 + \gamma x + \delta$$

kubik ko'phadni $x = u - \frac{\beta}{3}$ kabi almashtirish bajarib, $g(x) = x^3 + bx + c$ shaklga keltirish mumkin. Shuning uchun biz $g(x) = x^3 + bx + c$ ko'phadning Galua gruppasini o'rganish bilan chegaralanamiz.

Aytaylik, $g(x) = x^3 + bx + c$ ko'phad $\mathbb{K}$ maydon ustida keltirilmas bo'lsin, u holda ushbu ko'phad $\mathbb{K}$ maydonda ildizga ega bo'lmasdan, $\mathbb{K}$ maydonning $g(x)$ ko'phad orqali yoyilgan maydonida $\alpha_1, \alpha_2, \alpha_3$ ildizlarga ega bo'ladi. Demak,

$$g(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

hamda

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = b, \quad \alpha_1\alpha_2\alpha_3 = -c.$$

Quyidagi belgilashlarni kiritamiz

$$d = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2), \quad D = d^2 = (\alpha_2 - \alpha_1)^2(\alpha_3 - \alpha_1)^2(\alpha_3 - \alpha_2)^2.$$

U holda ixtiyoriy $\varphi \in Gal(\mathbb{F}, \mathbb{K})$ avtomorfizm uchun $\varphi(D) = D$ va $\varphi(d) = d$ yoki $\varphi(d) = -d$ bo'ladi. Bundan tashqari, $D = -4b^3 - 27c^2$ munosabat o'rinli.

6.5.1-teorema. *Aytaylik, $g(x) = x^3 + bx + c$ ko'phad $\mathbb{K}$ maydon ustida keltirilmas va seperabel bo'lib, $\mathbb{F}$ maydon $\mathbb{K}$ maydonning $f(x)$ ko'phad orqali yoyilgan maydoni bo'lsin. Agar D soni $\mathbb{K}$ maydonda biror sonning kvadrati shaklida ifodalansa, u holda $Gal(\mathbb{F}, \mathbb{K}) \simeq A_3$, aks holda $Gal(\mathbb{F}, \mathbb{K}) \simeq S_3$.*

Isbot. $D = -4b^3 - 27c^2$ bo'lganligi uchun $D \in \mathbb{K}$. Aytaylik, D soni $\mathbb{K}$ maydonda biror sonning kvadrati shaklida ifodalansin, ya'ni $d \in \mathbb{K}$ bo'lsin, u holda ixtiyoriy $\varphi \in Gal(\mathbb{F}, \mathbb{K})$ uchun $\varphi(d) = d$ bo'lib, $Gal(\mathbb{F}, \mathbb{K})$ gruppa S_3 o'rin almashtirishlar gruppasining faqat juft o'rin almashtirishlarini o'z ichiga oluvchi qism gruppasiga izomorf bo'ladi. $f(x)$ kop'hadning ildizlari turli xil bo'lganligi uchun $Gal(\mathbb{F}, \mathbb{K}) \neq \{e\}$. Demak, $Gal(\mathbb{F}, \mathbb{K}) \simeq A_3$.

Agar D soni $\mathbb{K}$ maydonda biror sonning kvadrati shaklida ifodalanmasa, u holda $d \notin \mathbb{K}$ bo'lib, $Gal(\mathbb{F}, \mathbb{K})$ Galua gruppasining tartibi 3 dan katta va u S_3

gruppaning toq o‘rin almashtirishlarni ham o‘z ichiga oluvchi qism gruppasiga izomorf. Demak, $Gal(\mathbb{F}, \mathbb{K}) \simeq S_3$. $\square$

Endi biror $\mathbb{K}$ maydonda $f(x) = x^n - 1$ ko‘phadni qaraymiz. Ma’lumki ushbu ko‘phadning ildizlari birning n**-darajali ildizlari** deb ataladi. Ushbu ko‘phad uchun

$$(x^n - 1) = (x - 1)(x^{n-1} + x^{n-2} + \cdots + 1)$$

tenglik o‘rinli bo‘lib, $x = 1$ element ushbu tenglamanin eng sodda ildizi, qolgan ildizlari esa $x^{n-1} + x^{n-2} + \cdots + 1$ ko‘phadning ildizlaridan iborat bo‘ladi.

Xususan, $\mathbb{K}$ maydon kompleks sonlar maydoning qism maydoni bo‘lsa, u holda $f(x) = x^n - 1$ ko‘phadning ildizlari

$$\xi_k = cos\frac{2\pi k}{n} + isin\frac{2\pi k}{n}, \quad k = 0, 1, \dots n - 1$$

ko‘rinishida bo‘ladi.

Kompleks sonlar maydoni ustida bo‘lgani kabi ixtiyoriy $\mathbb{K}$ maydondagi birning n-darajali ildizlari to‘plami ko‘paytirish amaliga nisbatan gruppa tashkil qiladi. Ushbu gruppaning tashkil qiluvchi elementlari esa birning n**-darajali boshlang‘ich ildizlari** deb ataladi. Demak, ζ element birning n-darajali boshlang‘ich ildizi bo‘lishi uchun $\{\zeta^k \mid 0 \leq k \leq n-1\}$ to‘plam birning barcha n-darajali ildizlarini to‘plami bilan ustma-ust tushishi zarur va yetarli. $\mathbb{K}$ maydonnni ζ boshlang‘ich oldiz bo‘yicha kengaytmasi $\mathbb{F} = \mathbb{K}(\zeta)$ maydon birning barcha n-darajali ildizlarini o‘z ichiga olganligi uchun, $\mathbb{K}(\zeta)$ maydon $\mathbb{K}$ maydonning $f(x) = x^n - 1$ ko‘phad orqali yoyilgan maydoni bo‘ladi.

6.5.1-tasdiq. *$f(x) = x^n - 1$ ko‘phadning Galua gruppasi kommutativdir.*

Isbot. Aytaylik, ζ element birning n-darajali boshlang‘ich ildizi bo‘lsin. U holda $f(x)$ ko‘phadning Galua gruppasi $\mathrm{Gal}(\mathbb{K}(\zeta), \mathbb{K})$ bo‘lib, ixtiyoriy $\psi \in \mathrm{Gal}(\mathbb{K}(\zeta), \mathbb{K})$ avtomorfizm uchun $\psi(\zeta)$ element yana $f(x)$ ko‘phadning ildizi bo‘ladi. Demak, qandaydir k soni uchun $\psi(\zeta) = \zeta^k$ tenglik o‘rinli. Agar ζ^k element boshlang‘ich ildiz bo‘lmasa, u holda qandaydir $m < n$ uchun $(\zeta^k)^m = 1$. Berilgan ψ avtomorfizmning teskarisini qarasak, $\zeta = \psi^{-1}(\zeta^k)$ bo‘lib, $\zeta^m = \psi^{-1}((\zeta^k)^m) = 1$. Bu esa, ζ elementning boshlang‘ich ildiz ekanligiga zid, ya’ni ζ^k element boshlang‘ich ildiz. Demak, k va n sonlari o‘zaro tub.

Shunday qilib biz har bir avtomorfizm uchun ζ boshlang‘ich ildizni ζ^k ga o‘tkazuvchi k elementni mos qo‘yamiz. Ushbu k soni n modul bo‘yicha aniqlanishini hisobga olsak, biz $\mathrm{Gal}(\mathbb{K}(\zeta), \mathbb{K})$ grupppasidan $\mathbb{U}_n$ gruppaga bo‘lgan $\Psi(\psi) = k$ kabi aniqlanuvchi gomomorfizmni hosil qilamiz, bu yerda $\mathbb{U}_n$ gruppa $\mathbb{Z}_n$ chegirmalar halqasining teskarilanuvchi elementlaridan iborat multiplikativ gruppa. $\Psi(\psi) = 1$ bo‘lishidan ψ avtomorfizmning ayniy ekanligi kelib chiqqanligi uchun

$\Psi : \mathrm{Gal}(\mathbb{K}(\zeta), \mathbb{K}) \to \mathbb{U}_n$ gomorfizm monomorfizm bo‘ladi. Demak, Galua gruppasi $\mathbb{U}_n$ gruppaning qism gruppasiga izomorf. $\mathbb{U}_n$ gruppa kommutativ ekanligidan $\mathrm{Gal}(\mathbb{K}(\zeta), \mathbb{K})$ Galua gruppasining ham kommutativligi kelib chiqadi. $\square$

6.5.1-tasdiq isbotidan ko‘rinadiki $f(x) = x^n - 1$ ko‘phadning Galua gruppasining tartibi $\mathbb{U}_n$ gruppa tartibining bo‘luvchisi bo‘ladi. $\mathbb{U}_n$ gruppaning tartibi $\varphi(n)-$Eyler funksiyasining qiymatiga tengligidan Galua gruppasining tartibi $\varphi(n)$ ning bo‘luvchisi ekanligi kelib chiqadi.

6.5.2-ta’rif. *Xarakteristikasi nolga teng $\mathbb{K}$ maydonning $f(x) = x^n - c$ ko‘phad bo‘yicha yoyilgan maydoni **sodda radikal kengaytma** deb ataladi, bu yerda $c \in \mathbb{K}$ va $c \neq 0$.*

Ta’kidlash joizki, $\mathbb{K}$ maydonning xarakteristikasi nolga teng bo‘lganligi uchun $f(x) = x^n - c$ ko‘phad separabel ko‘phad bo‘ladi. Ushbu $f(x)$ ko‘phadning ildizlari $\zeta^k\theta$ ko‘rinishida bo‘lib, $\mathbb{K}$ maydonning $f(x)$ ko‘phad bo‘yicha yoyilgan maydoni esa $\mathbb{F} = \mathbb{K}(\zeta, \theta)$ bo‘ladi, bu yerda ζ – birning n-darajali boshlang‘ich ildizi, θ esa $f(x)$ ko‘phadning biror fiksirlangan ildizi.

6.5.2-teorema. *Sodda radikal kengaytmaning Galua gruppasi yechiluvchan bo‘ladi.*

Isbot. Aytaylik, $\mathbb{F} = \mathbb{K}(\zeta, \theta)$ bo‘lsin. 6.5.1-tasdiqning isboti kabi ixtiyoriy $\psi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ avtomorfizm uchun $\psi(\zeta) = \zeta^k$ shartni qanoatlanturuvchi k sonini mos qo‘yish mumkin. Bundan tashqari, θ element $f(x)$ ko‘phadning ildizi bo‘lganligi uchun $f(\theta)$ ham shu ko‘phadning ildizi bo‘ladi. Bundan esa, $\psi(\theta) = \zeta^m\theta$ tenglik o‘rinli bo‘ladigan m soni mavjudligi kelib chiqadi. Demak, ixtiyoriy $\psi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ avtomorfizmga (k, m) juftlikni mos qo‘yish mumkin.

Endi bu moslikni har bir komponentasi bo‘yicha n-modul aniqligida yagona ekanligini ko‘rsatamiz. Aytaylik, (k, m) va (k_1, m_1) juftliklar bitta ψ avtomorfizmga mos kelsin. U holda

$$\psi(\zeta) = \zeta^k = \zeta^{k_1}, \quad \psi(\theta) = \zeta^m\theta = \zeta^{m_1}\theta.$$

Bundan esa, $\zeta^{k-k_1} = 1$ va $\zeta^{m-m_1} = 1$ ekanligi ya’ni $k - k_1$ va $m - m_1$ sonlari n ga bo‘linishi kelib chiqadi. Demak, $k \in \mathbb{U}_n$ va $m \in \mathbb{Z}_n$ bo‘lib, biz $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ gruppani $\mathbb{U}_n \times \mathbb{Z}_n$ to‘plamga otkazuvchi inyektiv akslantirishga ega bo‘lamiz. Endi $\mathbb{U}_n \times \mathbb{Z}_n$ to‘plamda quyidagicha amal aniqlaymiz

$$(k_1, m_1) \circ (k_2, m_2) = (k_1k_2, k_2m_1 + m_2).$$

Tekshirish qiyin emaski, $\mathbb{U}_n \times \mathbb{Z}_n$ to‘plam ushbu amalga nisbatan gruppa tashkil qiladi va bu gruppa odatda $\mathbf{M}_n$ kabi belgilanadi. Ushbu $\mathbf{M}_n$ gruppaning birlik elementi $(\overline{1}, \overline{0})$ bo‘lib, (k, m) elementning teskarisi esa $(k^{-1}, -k^{-1}m)$ bo‘ladi. Agar

$H = \{(\bar{1}, m) \mid m \in \mathbb{Z}_n\}$ to‘plamni qarasak, ushbu to‘plam $\mathbf{M}_n$ gruppaning normal qism gruppasi bo‘lib, u kommutativ bo‘ladi. Bundan tashqari, $\mathbf{M}_n/H \simeq \mathbb{U}_n$ ekanligidan faktor gruppaning ham kommutativ ekanligi kelib chiqadi. Demak, $\mathbf{M}_n$ gruppada

$$\mathbf{M}_n \supset H \supset e$$

yechiluvchan qator mavjud, ya’ni $\mathbf{M}_n$ gruppa yechiluvchan.

Demak, biz yuqorida $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasidan $\mathbf{M}_n$ yechiluvchan gruppaga inyektiv akslantirish qurgan ekanmiz. Agar biz bu inyektiv akslantirishning gomomorfizm ekanligini ko‘rsatsak, teoremaning isbotiga ega bo‘lamiz.

Aytaylik bizga ψ_1 va ψ_2 avtomorfizmlar berilgan bo‘lib, ularga (k_1, m_1) va (k_2, m_2) juftliklar mos kelsin. Ya’ni

$$\psi_1(\zeta) = \zeta^{k_1}, \quad \psi_1(\theta) = \zeta^{m_1}\theta, \qquad \psi_2(\zeta) = \zeta^{k_2}, \quad \psi_2(\theta) = \zeta^{m_2}\theta.$$

U holda $\psi_2 \circ \psi_1$ avtomorfizm uchun

$$(\psi_2 \circ \psi_1)(\zeta) = \psi_2(\zeta^{k_1}) = \big(\psi_2(\zeta)\big)^{k_1} = \zeta^{k_1 k_2},$$
$$(\psi_2 \circ \psi_1)(\theta) = \psi_2(\zeta^{m_1}\theta) = \psi_2(\zeta^{m_1})\psi_2(\theta) = \zeta^{k_2 m_1}\zeta^{m_2}\theta = \zeta^{k_2 m_1 + m_2}\theta.$$

Ushbu tengliklardan esa $\psi_2 \circ \psi_1$ avtomorfizmga $(k_1 k_2, k_2 m_1 + m_2)$ juftlik mos kelishini hosil qilamiz. Demak, $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasidan $\mathbf{M}_n$ yechiluvchan gruppaga qurilgan inyektiv akslantirish gomomorfizm, ya’ni monomorfizm bo‘lar ekan. $\mathbf{M}_n$ gruppa yechuluvchan bo‘lganligi uchun uning ixtiyoriy qism gruppasi ham yechiluvchan bo‘lib, bundan $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining ham yechiluvchan ekanligi kelib chiqadi. $\square$

6.5.3-ta’rif. *Agar $\mathbb{K} \subset \mathbb{F}$ kengaytmada shunday*

$$\mathbb{K} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_i \subset \mathbb{L}_{i+1} \subset \cdots \subset \mathbb{L}_s = \mathbb{F} \tag{6.5}$$

kengaytmalar ketma-ketligi topilib, har bir $\mathbb{L}_i \subset \mathbb{L}_{i+1}$ kengaytma sodda radikal kengaytma bo‘lsa, u holda $\mathbb{K} \subset \mathbb{F}$ kengaytma ***radikal kengaytma*** *deb ataladi.*

Radikal kengaytmadagi kengaytmalar ketma-ketligi esa, **radikal qator** deyiladi. Ta’kidlash joizki, radikal kengaytma bir nechta radikal qatorlarga ega bo‘lishi mumkin. Bundan tashqari, radikal qatorda $\mathbb{L}_i \subset \mathbb{L}_{i+1}$ kengaytmalar normal bo‘lganligi bilan $\mathbb{K} \subset \mathbb{F}$ kengaytma normal bo‘lmasligi mumkin. Bir vaqtning o‘zida ham normal ham radikal bo‘lgan kengaytmaga **normal radikal kengaytma** deb ataladi.

6.5.3-teorema. *Ixtiyoriy $\mathbb{K} \subset \mathbb{F}$ radikal kengaytma uchun shunday $\overline{\mathbb{F}}$ ($\mathbb{K} \subset \mathbb{F} \subset \overline{\mathbb{F}}$) maydon mavjudki, $\mathbb{K} \subset \overline{\mathbb{F}}$ kengaytma normal radikal kengaytma bo‘ladi. Ya’ni ixtiyoriy radikal kengaytma qandaydir normal radikal kengaytmaning ichida yotadi.*

Isbot. Isbotni radikal qatorning uzunligi bo‘yicha induksiya metodini qo‘llab amalga oshiramiz. Agar $s = 1$ bo‘lsa, u holda $\mathbb{K} = \mathbb{L}_0 \subset \mathbb{L}_1 = \mathbb{F}$ bo‘lib, $\mathbb{K} \subset \mathbb{F}$ kengaytma normal radikal bo‘ladi, ya’ni $\overline{\mathbb{F}} = \mathbb{F}$ deb olish yetarli.

Tasdiqni usunligi s ga teng bo‘lgan radikal qatorlar uchun o‘rinli bo‘lsin deb faraz qilib, $s+1$ uchun ko‘rsatamiz. Agar

$$\mathbb{K} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_s \subset \mathbb{L}_{s+1} = \mathbb{F}$$

qatorni qarasak, induksiya faraziga ko‘ra $\mathbb{K} \subset \mathbb{L}_s$ kengaytmani o‘z ichiga olivchi $\overline{\mathbb{L}}_s$ ($\mathbb{K} \subset \mathbb{L}_s \subset \overline{\mathbb{L}}_s$) normal radikal kengaytma mavjud, ya’ni qandaydir

$$\mathbb{K} = \mathbb{P}_0 \subset \mathbb{P}_1 \subset \dots \mathbb{P}_{t-1} \subset \mathbb{P}_t = \overline{\mathbb{L}}_s \tag{6.6}$$

radikal qator mavjud.

Ikkinchi tomondan esa, $\mathbb{L}_s \subset \mathbb{F}$ kengaytma sodda radikal kengaytma bo‘lganligi uchun $\mathbb{F} = \mathbb{L}_s(\zeta, \theta)$, bu yerda ζ – birning n-darajali boshlang‘ich ildizi, θ esa $x^n - c,\ c \in \mathbb{L}_s$ tenglamaning birorta fiksirlangan ildizi.

Aytaylik, ushbu $c \in \mathbb{L}_s$ elementning $\mathbb{K}$ maydon ustidagi minimal ko‘phadi $g(x)$ bo‘lsin. $\mathbb{K} \subset \overline{\mathbb{L}}_s$ kengaytma normal bo‘lib, $c \in \overline{\mathbb{L}}_s$ bo‘lganligi uchun, $g(x)$ ko‘phadning barcha ildizlari $\overline{\mathbb{L}}_s$ maydonda yotadi. Bundan esa, ζ boshlang‘ich ildizning ham $\overline{\mathbb{L}}_s$ maydonda yotishi kelib chiqadi. Ushbu $g(x)$ ko‘phadning ildizlari $\beta_1 = c, \beta_2, \dots, \beta_r$ uchun $\overline{\mathbb{L}}_s$ maydonda quyidagi tenglamalarni qaraymiz

$$x^n - \beta_i = 0, \quad 1 \leq i \leq r.$$

Bu r ta tenglamaning har biridan bittadan $\alpha_1 = \theta, \alpha_2, \dots, \alpha_r$ ildizlarni olib, $\overline{\mathbb{L}}_s$ maydon va ushbu α_i ildizlarni o‘z ichiga oluvchi $\overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \dots, \alpha_r)$ maydonni qarasak, $\zeta, \theta \in \overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \dots, \alpha_r)$ ekanligidan $\mathbb{F} \subset \overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \dots, \alpha_r)$ kelib chiqadi.

Endi quyidagi

$$\overline{\mathbb{L}}_s \subset \overline{\mathbb{L}}_s(\alpha_1) \subset \overline{\mathbb{L}}_s(\alpha_1, \alpha_2) \subset \cdots \subset \overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \dots, \alpha_r) \tag{6.7}$$

qatorni qarasak, ushbu qator radikal qator bo‘ladi. Bundan esa, (6.6) va (6.7) qatorlarni birlashtirish natijasida $\mathbb{K}$ maydondan boshlanib, $\overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \dots, \alpha_r)$ maydonda tugovchi radikal qatorning mavjudligini keltirib chiqazamiz. Ya’ni $\mathbb{K} \subset \overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \dots, \alpha_r)$ kengaytma radikal kengaytma bo‘ladi.

Endi uchbu kengaytmaning normal ekanligini ko‘rsatamiz. Buning uchun

$$G(x) = g(x^n) = (x^n - \beta_1)(x^n - \beta_2) \dots (x^n - \beta_r)$$

ko‘phadni qarasak, $\alpha_1, \alpha_2, \dots, \alpha_r$ elementlar $G(x)$ ko‘phadning ildizlari bo‘ladi. Demak, $\mathbb{K}$ maydonning $G(x)$ ko‘phad orqali yoyilgan maydoni $\overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \dots, \alpha_r)$ maydonni o‘z ichiga oladi. Ikkinchi tomondan esa, $G(x)$ ko‘phadning qolgan ildizlari $\alpha_1, \alpha_2, \ldots, \alpha_r$ elementlarga birning n-darajali boshlang'ich ildizi ζ ning darajalariga ko'paytmalari orqali hosil qilinadi. Bu esa $G(x)$ ko'phadning barcha ildizlari $\overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \ldots, \alpha_r)$ maydonda yotishini, ya'ni $\overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \ldots, \alpha_r)$ maydon $\mathbb{K}$ maydonning $G(x)$ ko'phad orqali yoyilgan maydoni bilan ustma-ust tushushini anglatadi. Demak, $\mathbb{K} \subset \overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \ldots, \alpha_r)$ kengaytma normal radikal kengaytma bo'ladi. $\overline{\mathbb{F}} = \overline{\mathbb{L}}_s(\alpha_1, \alpha_2, \ldots, \alpha_r)$ deb olsak, teorema isbotini hosil qilamiz. □

Endi xarakteristikasi no'lga teng bo'lgan $\mathbb{K}$ maydonda

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \tag{6.8}$$

tenglamani qaraymiz.

6.5.4-ta'rif. *Agar* (6.8) *tenglamaning θ ildizi $\mathbb{K}$ maydonning qandaydir radikal kengaytmasiga tegishli bo'lsa, u holda θ ildiz* ***radikallarda ifodalanadi*** *deyiladi. Agar tenglamaning barcha ildizlari radikallarda ifodalansa, u holda ushbu tenglama* ***radikallarda yechiladi*** *deb ataladi.*

Ta'kidlash joizki, θ ildizning radikallarda ifodalanishi uning $\mathbb{K}$ maydon elementlari ustida to'rtta arifmetik amal va n-darajali ildiz chiqazish orqali hosil qilinishi bilan teng kuchli.

6.5.2-tasdiq. *Agar $f(x)$ keltirilmas ko'phadning hech bo'lmaganda bitta ildizi radikallarda ifodalansa, u holda $f(x) = 0$ tenglama radikallarda yechiladi.*

Isbot. Aytaylik, $f(x)$ keltirilmas ko'phad bo'lib, θ uning radikallarda ifodalanuvchi ildizi bo'lsin. U holda $\mathbb{K} \subset \mathbb{F}$ radikal kengaytma mavjud bo'lib, $\theta \in \mathbb{F}$. O'z navbatida 6.5.3-teoremaga ko'ra $\mathbb{F}$ maydonni o'z ichiga olivchi $\overline{\mathbb{F}}$ maydon mavjud bo'lib $\mathbb{K} \subset \overline{\mathbb{F}}$ kengaytma normal radikal kengaytma bo'ladi. $\theta \in \overline{\mathbb{F}}$ bo'lganligi va $\mathbb{K} \subset \overline{\mathbb{F}}$ kengaytmaning normalligidan, $f(x) = 0$ tenglamaning barcha ildizlari $\overline{\mathbb{F}}$ maydonda yotishi kelib chiqadi. Demak, $f(x) = 0$ tenglama radikallarda yechiladi. □

6.5.3-tasdiq. *Ixtiyoriy normal radikal kengaytmaning Galua gruppasi yechiluvchan bo'ladi.*

Isbot. Aytaylik, $\mathbb{K} \subset \mathbb{F}$ normal radikal kengaytma berilgan bo'lsin. U holda Galua nazariyasining fundamental teoremasiga ko'ra

$$\mathbb{K} = \mathbb{L}_0 \subset \mathbb{L}_1 \subset \cdots \subset \mathbb{L}_{s-1} \subset \mathbb{L}_s = \mathbb{F}$$

radikal qatorga $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining quyidagi qism gruppalari ketma-ketligi mos keladi

$$\mathrm{Gal}(\mathbb{F}, \mathbb{K}) = H_0 \supset H_1 \supset \cdots \supset H_{s-1} \supset H_s = E, \tag{6.9}$$

bu yerda $H_i = \mathrm{Gal}(\mathbb{F}, \mathbb{L}_i)$.

Ixtiyoriy i $(1 \leq i \leq s)$ uchun $\mathbb{L}_{i-1} \subset \mathbb{L}_i$ kengaytma normal kengaytma ekanligidan $H_i = \mathrm{Gal}(\mathbb{F}, \mathbb{L}_i)$ qism gruppaning $H_{i-1} = \mathrm{Gal}(\mathbb{F}, \mathbb{L}_{i-1})$ qism gruppada normal bo'luvchi ekanligini hosil qilamiz. Bundan tashqari, H_{i-1}/H_i faktor gruppa $\mathrm{Gal}(\mathbb{L}_i, \mathbb{L}_{i-1})$ gruppaga izomorf bo'lib, $\mathbb{L}_{i-1} \subset \mathbb{L}_i$ kengaytma sodda radikal kengaytma bo'lganligi uchun 6.5.2-teoremaga ko'ra H_{i-1}/H_i faktor gruppa yechiluvchan bo'ladi. Demak, (6.9) qator normal qator bo'lib, uning har bir H_{i-1}/H_i faktor gruppalari yechiluvchan. Bundan esa $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining yechiluvchan ekanligi kelib chiqadi. $\square$

Ta'kidlash joizki, 6.5.3-tasdiqning teskarisi umuman olganda o'rinli emas, ya'ni Galua gruppasi yechiluvchan bo'lgan ixtiyoriy normal kengaytma radikal bo'lavermaydi. Lekin Galua gruppasi yechiluvchan bo'lgan ixtiyoriy normal kengaytmani o'z ichiga oluvchi normal radikal kengaytma mavjud. Biz ushbu fakt isbotini keyingi paragrafda keltirib o'tamiz (6.6.2-teoremaga qarang). Galua teoremasi deb yuritiladigan quyidagi asosiy teoremaning isbotida esa biz ushbu faktdan foydalanamiz.

6.5.4-teorema (Galua teoremasi). *$f(x) = 0$ tenglama radikallarda yechilishi uchun uning Galua gruppasi yechiluvchan bo'lishi zarur va yetarli.*

Isbot. ***Zaruriyligi.*** Aytaylik, $\mathbb{K}$ maydon ustida berilgan $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$ ko'phad uchun $f(x) = 0$ tenglama radikallarda yechilsin, u holda $\mathbb{K}$ maydonning tenglamani barcha ildizlarini o'z ichiga oluvchi normal radikal kengaytma mayjud va u $\mathbb{K}$ maydonning $f(x)$ ko'phad orqali yoyilgan maydonini o'z ichiga oladi. Ya'ni agar $\mathbb{F}$ maydon tenglamaning barcha ildizlarini o'z ichiga oluvchi normal radikal kengaytma, $\mathbb{L}$ esa $\mathbb{K}$ maydonning $f(x)$ ko'phad orqali yoyilgan maydoni bo'lsa, u holda $\mathbb{K} \subset \mathbb{L} \subset \mathbb{F}$.

6.5.3-tasdiqqa ko'ra $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ yechiluvchan gruppa bo'lib, uning $\mathrm{Gal}(\mathbb{F}, \mathbb{L})$ qism gruppasi ham yechiluvchan bo'ladi. $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ gruppa esa $\mathrm{Gal}(\mathbb{F}, \mathbb{K})/\mathrm{Gal}(\mathbb{F}, \mathbb{L})$ faktor gruppaga izomorf bo'lganligi uchun u ham yechiluvchan bo'ladi.

Yetarliligi. Aytaylik, $\mathbb{L}$ maydon $\mathbb{K}$ maydonning $f(x)$ ko'phad orqali yoyilgan maydoni bo'lib, $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ Galua gruppasi yechiluvchan bo'lsin. U holda yuqorida aytilgan faktga asosan (6.6.2-teoremaga qarang) $\mathbb{L}$ maydonni o'z ichiga oluvchi normal radikal kengaytma mavjud. Bundan esa, $f(x) = 0$ tenglama radikallarda yechilishi kelib chiqadi. $\square$

6.5.1-misol. *Ratsional sonlar maydoni ustida berilgan $f(x) = x^4 - 2$ ko'phadning Galua gruppasini toping.*

Yechish. Ma'lumki, $f(x) = x^4 - 2$ ko'phad ratsional sonlar maydoni ustida keltirilmas bo'lib, kompleks sonlar maydoni ustida quyidagi ko'rinishda chiziqli ko‘paytuvchilarga ajraladi.

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

Bundan ko‘rinadiki, $\mathbb{Q}$ ratsional sonlar maydonining $f(x)$ ko‘phad orqali yoyilgan maydoni $\mathbb{Q}(i, \sqrt[4]{2})$ maydondan iborat. Agar $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(i, \sqrt[4]{2})$ ekanligidan foydalansak,

$$[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}].$$

Endi $x^4 - 2$ ko‘phad $\mathbb{Q}$ maydonda $\sqrt[4]{2}$ element uchun minimal, $x^2 + 1$ ko‘phad esa $\mathbb{Q}(\sqrt[4]{2})$ maydonda i uchun minimal bo‘lganligi uchun $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ va $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 2$ bo‘lib, $[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$ ekanligi kelib chiqadi.

Demak, $|\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2}), \mathbb{Q})| = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = 8$, ya’ni $f(x)$ ko‘phad Galua gruppasining tartibi 8 ga teng. Bundan esa, $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2}), \mathbb{Q})$ Galua gruppasi $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, Q_8 va D_4 gruppalardan biriga izomorf ekanligi kelib chiqadi.

Ta’kidlash joizki, $f(x)$ ko‘phadning barcha ildizlari $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$ bo‘lganligi uchun ixtiyoriy $\varphi \in \mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2}), \mathbb{Q})$ avtomorfizmni aniqlash uchun uning ildizlardagi qiymatlarini aniqlash kifoya. Bundan tashqari, $\varphi(\alpha) = \alpha, \alpha \in \mathbb{Q}$ ekanligidan $\varphi(-\sqrt[4]{2}) = -\varphi(\sqrt[4]{2})$ va $\varphi(-i\sqrt[4]{2}) = -\varphi(i\sqrt[4]{2})$. Bulardan foydalanib, $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2}), \mathbb{Q})$ Galua gruppasining barcha elementlarini quyidagi jadval oqrali ifodalashimiz mumkin.

	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6	φ_7	φ_8
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-i\sqrt[4]{2}$
$-\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}$	$\sqrt[4]{2}$	$\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$i\sqrt[4]{2}$
$i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$
$-i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$\sqrt[4]{2}$

Ko‘rinib turibdiki, ushbu gruppa kommutativ emas, chunki $\varphi_2 \circ \varphi_5 \neq \varphi_5 \circ \varphi_2$.

Bundan tashqari, Q_8 kvaternion gruppasi tartibi 2 ga teng bo‘lgan yagona qism gruppaga ega bo‘lib, $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2}), \mathbb{Q})$ Galua gruppasida esa bunday qism gruppalar $H_1 = \{\varphi_1, \varphi_2\}, H_2 = \{\varphi_1, \varphi_3\}, H_3 = \{\varphi_1, \varphi_4\}$. Demak, Galua gruppasi Q_8 gruppaga ham izomorf emas. Bundan esa, $\mathrm{Gal}(\mathbb{Q}(i, \sqrt[4]{2}), \mathbb{Q})$ Galua gruppasi D_4 Diedr gruppasiga izomorf ekanligini kelib chiqadi. $\square$

6.6 Qo‘shimcha tushuncha va teoremalar

Bizga $\mathbb{K}_1$ va $\mathbb{K}_2$ maydonlar berilgan bo‘lib, $\mathbb{P}$ esa ushbu $\mathbb{K}_1$ va $\mathbb{K}_2$ maydolarni o‘z ichiga oluvchi eng kichik maydon bo‘lsin. Masalan, agar $\mathbb{K}_1 = \mathbb{K}(\theta_1)$ va $\mathbb{K}_2 =$

$\mathbb{K}(\theta_2)$ bo'lsa, u holda ushbu maydonlarni o'z ichiga oluvchi eng kichik maydon $\mathbb{K}(\theta_1, \theta_2)$ bo'ladi.

6.6.1-tasdiq. *Agar $\mathbb{P}$ maydon $\mathbb{K}_1$ va $\mathbb{K}_2$ maydonlarni o'z ichiga oluvchi eng kichik maydon bo'lib, $\mathbb{K}_2 = \mathbb{K}(\theta_1, \theta_2, \dots, \theta_n)$ bo'lsa, u holda $\mathbb{P} = \mathbb{K}_1(\theta_1, \theta_2, \dots, \theta_n)$ bo'ladi.*

Isbot. Aytaylik, $\mathbb{P}$ ushbu $\mathbb{K}_1$ va $\mathbb{K}_2$ maydolarni o'z ichiga oluvchi eng kichik maydon bo'lsin. $\mathbb{K} \subset \mathbb{K}_1$ bo'lganligi uchun $\mathbb{K}(\theta_1, \theta_2, \dots, \theta_n) \subset \mathbb{K}_1(\theta_1, \theta_2, \dots, \theta_n)$, ya'ni $\mathbb{K}_2 \subset \mathbb{K}_1(\theta_1, \theta_2, \dots, \theta_n)$. Bundan tashqari, $\mathbb{K}_1 \subset \mathbb{K}_1(\theta_1, \theta_2, \dots, \theta_n)$ bo'lib, $\mathbb{P}$ maydonning eng kichik ekanligidan $\mathbb{P} \subset \mathbb{K}_1(\theta_1, \theta_2, \dots, \theta_n)$ kelib chiqadi.

Ikkinchi tomondan esa, $\mathbb{K}_1 \subset \mathbb{P}$ va $\theta_1, \theta_2, \dots, \theta_n \in \mathbb{P}$ ekanligidan $\mathbb{K}_1(\theta_1, \theta_2, \dots, \theta_n) \subset \mathbb{P}$ kelib chiqadi. Demak, $\mathbb{P} = \mathbb{K}_1(\theta_1, \theta_2, \dots, \theta_n)$. $\square$

Ushbu tasdiqdan quyidagi natijaga ega bo'lamiz.

6.6.1-natija. *Agar $\mathbb{K}$ maydonning $\mathbb{K}_1$ va $\mathbb{K}_2$ kengaytmalaridan hech bo'lmaganda bittasi chekli bo'lsa, u holda ushbu maydolarni o'z ichiga oluvchi eng kichik maydonning ixtiyoriy elementi*

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_s\beta_s$$

ko'rinishida bo'ladi, bu yerda $\alpha_1, \alpha_2, \dots, \alpha_s \in \mathbb{K}_1$, $\beta_1, \beta_2, \dots, \beta_s \in \mathbb{K}_2$.

Isbot. Aytaylik, $\mathbb{K} \subset \mathbb{K}_2$ kengaytma chekli bo'lsin. U holda ushbu kengaytma algebraik hosil qilingan kengaytma bo'lib, $\mathbb{K}$ maydonda algebraik bo'lgan $\theta_1, \theta_2, \dots, \theta_n$ elementlar uchun $\mathbb{K}_2 = \mathbb{K}(\theta_1, \theta_2, \dots, \theta_n)$. Ushbu elementlar $\mathbb{K}_1$ maydonda ham algebraik bo'lib, $\mathbb{P} = \mathbb{K}_1(\theta_1, \theta_2, \dots, \theta_n)$ maydonning ixtiyoriy elementini $\theta_1, \theta_2, \dots, \theta_n$ elementlar va $\mathbb{K}_1$ maydonning elementlari orqali

$$\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_s\beta_s$$

kabi ifodalash mumkin. $\square$

Aytaylik, $\mathbb{K}$ maydonning $\mathbb{K}_1$ va $\mathbb{K}_2$ kengaytmalari hamda $\mathbb{K} \subset \mathbb{F}$ normal va seperabel kengaytma berilgan bo'lib, ushbu $\mathbb{K}_1$ va $\mathbb{K}_2$ maydonlarni o'z ichiga oluvchi eng kichik $\mathbb{P}$ maydon uchun $\mathbb{K} \subset \mathbb{P} \subset \mathbb{F}$ bo'lsin. U holda

$$\mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{P} \subset \mathbb{F} \quad \text{va} \quad \mathbb{K} \subset \mathbb{K}_2 \subset \mathbb{P} \subset \mathbb{F}$$

bo'lib, $\mathrm{Gal}(\mathbb{F}, \mathbb{P})$, $\mathrm{Gal}(\mathbb{F}, \mathbb{K}_1)$ va $\mathrm{Gal}(\mathbb{F}, \mathbb{K}_2)$ gruppalar $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining qism gruppalari bo'ladi. Ushbu qism gruppalar uchun quyidagi tasdiq o'rinli.

6.6.2-tasdiq. *$Gal(\mathbb{F}, \mathbb{P}) = Gal(\mathbb{F}, \mathbb{K}_1) \cap Gal(\mathbb{F}, \mathbb{K}_2)$*

Isbot. $\mathrm{Gal}(\mathbb{F}, \mathbb{K}_1)$ va $\mathrm{Gal}(\mathbb{F}, \mathbb{K}_2)$ gruppalar mos ravishda $\mathbb{K}_1$ va $\mathbb{K}_2$ maydon elementlarini o'z joyida qoldiruvchi avtomorfizmlardan iborat bo'lib, ixtiyoriy $\varphi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K}_1) \cap \mathrm{Gal}(\mathbb{F}, \mathbb{K}_2)$ avtomorfizm $\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_s\beta_s$ ko'rinishidagi elementlarni o'z joida qoldiradi. Bundan esa, φ avtomorfizm $\mathbb{P}$ maydonning ham ixtiyoriy elementini o'z joyida qoldirishi kelib chiqadi. Demak, $\varphi \in \mathrm{Gal}(\mathbb{F}, \mathbb{P})$, ya'ni $\mathrm{Gal}(\mathbb{F}, \mathbb{K}_1) \cap \mathrm{Gal}(\mathbb{F}, \mathbb{K}_2) \subset \mathrm{Gal}(\mathbb{F}, \mathbb{P})$.

Ikkinchi tomondan esa, ixtiyoriy $\psi \in \mathrm{Gal}(\mathbb{F}, \mathbb{P})$ avtomorfizm $\mathbb{K}_1$ va $\mathbb{K}_2$ maydonlarning elementlarini ham o'z joyida qoldiradi. Demak, $\mathrm{Gal}(\mathbb{F}, \mathbb{P}) \subset \mathrm{Gal}(\mathbb{F}, \mathbb{K}_1) \cap \mathrm{Gal}(\mathbb{F}, \mathbb{K}_2)$ bo'lib, bundan esa tasdiqning isboti kelib chiqadi. $\square$

6.6.2-natija. *$\mathbb{F} = \mathbb{P}$ bo'lishi uchun $Gal(\mathbb{F}, \mathbb{K}_1) \cap Gal(\mathbb{F}, \mathbb{K}_2) = E$ bo'lishi zarur va yetarli.*

6.6.3-natija. *Agar $\mathbb{K} \subset \mathbb{F}$ normal va separabel, $\mathbb{K} \subset \mathbb{K}_1$ normal va $\mathbb{K} \subset \mathbb{K}_2$ kengaytmalar berilgan bo'lib, $\mathbb{F}$ maydon $\mathbb{K}_1$ va $\mathbb{K}_2$ maydonlarni o'z ichiga oluvchi eng kichik maydon bo'lsa, u holda $Gal(\mathbb{F}, \mathbb{K}_2)$ Galua gruppasi $Gal(\mathbb{K}_1, \mathbb{K})$ Galua gruppasining qandaydir qism gruppasiga izomorf bo'ladi.*

Isbot. 6.4.2-natijaga ko'ra $\mathrm{Gal}(\mathbb{K}_1, \mathbb{K}) \simeq \mathrm{Gal}(\mathbb{F}, \mathbb{K})/\mathrm{Gal}(\mathbb{F}, \mathbb{K}_1)$, ya'ni

$$\Psi : \mathrm{Gal}(\mathbb{F}, \mathbb{K}) \to \mathrm{Gal}(\mathbb{K}_1, \mathbb{K})$$

epimorfizm mayjud bo'lib, $\mathrm{Ker}\Psi = \mathrm{Gal}(\mathbb{F}, \mathbb{K}_1)$.

Bundan tashqari, $\mathrm{Gal}(\mathbb{F}, \mathbb{K}_1) \cap \mathrm{Gal}(\mathbb{F}, \mathbb{K}_2) = E$ ekanligidan esa ushbu Ψ epimorfizmning $\mathrm{Gal}(\mathbb{F}, \mathbb{K}_2)$ gruppada monomorfizmligi kelib chiqadi. Demak, $\mathrm{Gal}(\mathbb{F}, \mathbb{K}_2)$ gruppa $\mathrm{Gal}(\mathbb{K}_1, \mathbb{K})$ gruppaning qandaydir qism gruppasiga izomorf bo'ladi. $\square$

Endi siklik kengaytma tushunchasini kiritamiz.

6.6.1-ta'rif. *Agar $Gal(\mathbb{F}, \mathbb{K})$ gruppa siklik gruppa bo'lsa, u holda $\mathbb{K} \subset \mathbb{F}$ kengaytma **siklik kengaytma** deb ataladi.*

Agar $\mathbb{K}$ maydonning $f(x) = x^n - c$ ko'phadga mos keluvchi sodda radikal kengaytmasida birning n-darajali boshlang'ich ildizi $\mathbb{K}$ maydonga tegishli bo'lsa, u holda ushbu sodda radikal kengaytma siklik kengaytma bo'ladi. Haqiqatdan ham, agar $\mathbb{F} = \mathbb{K}(\zeta, \eta)$ bo'lib, $\zeta \in \mathbb{K}$ bo'lsa, u holda $\mathbb{K}(\zeta, \eta) = \mathbb{K}(\eta)$ bo'lib, 6.5.2-teorema isbotidagi kabi $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ gruppadan $\mathbf{M}_n$ gruppaga qurilgan monomorfizmning obrazi $H = \{(\overline{1}, m) \mid m \in \mathbb{Z}_n\}$ to'plamdan iborat bo'ladi. Ushbu H to'plam $\mathbf{M}_n$ gruppaning siklik qism gruppasi bo'lganligi uchun $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining ham siklik ekanligi kelib chiqadi.

Shunday qilib biz, agar birning n-darajali boshlang'ich ildizi $\mathbb{K}$ maydonga tegishli bo'lsa, u holda ixtiyoriy sodda radikal kengaytmaning siklik kengaytma bo'lishini hosil qildik. Bizning maqsadimiz ushbu tasdiqning teskarisi ham o'rinli ekanligini ko'rsatishdan iborat. Buning uchun dastlab, bir qancha zaruriy lemmalarni isbotlab olamiz.

Demak, bizga xarakteristikasi nolga teng bo'lgan maydonning $\mathbb{K} \subset \mathbb{F}$ siklik kengaytmasi berilgan va $[\mathbb{F} : \mathbb{K}] = n$. Aytaylik, ζ – birning n-darajali boshlang'ich ildizi va $\varphi \in \mathrm{Gal}(\mathbb{F}, \mathbb{K})$ avtomorfizm siklik gruppaning hosil qiluvchi elementi bo‘lib, $\zeta \in \mathbb{K}$ bo‘lsin. Ixtiyoriy $\alpha \in \mathbb{K}$ element va t butun son uchun quyidagi qatorni qaraymiz

$$(\zeta^t, \alpha) = \alpha + \zeta^t \cdot \varphi(\alpha) + \zeta^{2t} \cdot \varphi^2(\alpha) + \cdots + \zeta^{(n-1)t} \cdot \varphi^{n-1}(\alpha)$$

6.6.1-lemma. *Shunday $\alpha \in \mathbb{K}$ element mavjudki, $(\zeta, \alpha) \neq 0$.*

Isbot. Xarakteristikasi nolga teng bo‘lgan maydon cheksiz maydon bo‘lganligi va $\mathbb{K} \subset \mathbb{F}$ kengaytma chekli ekanligi uchun 6.2.1-teoremaga ko‘ra shunday θ element topilib, $\mathbb{F} = \mathbb{K}(\theta)$ bo‘ladi. Bundan tashqari, $[\mathbb{F} : \mathbb{K}] = n$ bo‘lgani uchun θ element darajasi n ga teng bo‘lgan keltirilmas ko‘phadning ildizidir. Biz quyidagi elementlarni qarab,

$$(\zeta, \theta), \quad (\zeta, \theta^2), \quad \ldots, (\zeta, \theta^{n-1})$$

ulardan hech bo‘lmaganda bittasi noldan farqli ekanligini ko‘rsatamiz.

Teskarisini faraz qilaylik, ya’ni $(\zeta, \theta) = (\zeta, \theta^2) = \cdots = (\zeta, \theta^{n-1}) = 0$ bo‘lsin, u holda

$$\begin{cases} \theta + \zeta \cdot \varphi(\theta) + \zeta^2 \cdot \varphi^2(\theta) + \cdots + \zeta^{n-1} \cdot \varphi^{n-1}(\theta) = 0 \\ \theta^2 + \zeta \cdot \varphi(\theta^2) + \zeta^2 \cdot \varphi^2(\theta^2) + \cdots + \zeta^{n-1} \cdot \varphi^{n-1}(\theta^2) = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \theta^{n-1} + \zeta \cdot \varphi(\theta^{n-1}) + \zeta^2 \cdot \varphi^2(\theta^{n-1}) + \cdots + \zeta^{n-1} \cdot \varphi^{n-1}(\theta^{n-1}) = 0 \end{cases}$$

Bundan tashqari, ζ – birning n-darajali boshlang‘ich ildizi ekanligidan foydalansak, $0 = \zeta^n - 1 = (\zeta - 1)(1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1})$ tenglikdan

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = 0$$

kelib chiqadi.

U holda $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ elementlar oldidagi koeffitsiyentlardan tuzilgan determinantning qiymati nolga teng bo‘ladi, ya’ni

$$\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ \theta & \varphi(\theta) & \varphi^2(\theta) & \ldots & \varphi^{n-1}(\theta) \\ \theta^2 & \varphi(\theta^2) & \varphi^2(\theta^2) & \ldots & \varphi^{n-1}(\theta^2) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \theta^{n-1} & \varphi(\theta^{n-1}) & \varphi^2(\theta^{n-1}) & \ldots & \varphi^{n-1}(\theta^{n-1}) \end{vmatrix} = 0.$$

Endi φ akslantirishning avtomorfizm ekanligidan foydalansak, $\varphi^i(\theta^j) =$

$\left(\varphi^i(\theta)\right)^j$ bo‘lib, yuqoridagi determinant quyidagi ko‘rinishga keladi

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ \theta & \varphi(\theta) & \varphi^2(\theta) & \dots & \varphi^{n-1}(\theta) \\ \theta^2 & \left(\varphi(\theta)\right)^2 & \left(\varphi^2(\theta)\right)^2 & \dots & \left(\varphi^{n-1}(\theta)\right)^2 \\ \dots & \dots & \dots & \dots & \dots \\ \theta^{n-1} & \left(\varphi(\theta)\right)^{n-1} & \left(\varphi^2(\theta)\right)^{n-1} & \dots & \left(\varphi^{n-1}(\theta)\right)^{n-1} \end{vmatrix} = 0.$$

Ko‘rinib turibdiki, ushbu determinant $\theta, \varphi(\theta), \varphi^2(\theta), \dots, \varphi^{n-1}(\theta)$ elementlarga nisbatan Vandermond determinanti bo‘lib, uning qiymati nolga teng ekanligidan elementlarning ichida o‘zaro tenglari mavjudligi kelib chiqadi. Ya’ni qandaydir i, j $(0, \leq i, j, \leq n-1)$ uchun $\varphi^i(\theta) = \varphi^j(\theta)$. Bundan esa $\varphi^i = \varphi^j$ kelib chiqib, bu esa φ avtomorfizmning hosil qiluvchi element ekanligiga zid. Ushbu ziddiyatdan (ζ, θ), (ζ, θ^2), $\dots, (\zeta, \theta^{n-1})$ elementlarning ichida noldan farqlisi mavjud ekanligi, ya’ni lemmaning isboti kelib chiqadi. □

6.6.2-lemma. *Agar* $(\zeta, \alpha) \neq 0$ *bo‘lsa, u holda* $\mathbb{F} = \mathbb{K}(\alpha)$.

Isbot. $\alpha \in \mathbb{F}$ bo‘lganligi uchun $\mathbb{K}(\alpha) \subset \mathbb{F}$ bo‘lib, $H = \mathrm{Gal}(\mathbb{F}, \mathbb{K}(\alpha))$ gruppa $\mathrm{Gal}(\mathbb{F}, \mathbb{K})$ Galua gruppasining qism gruppasi bo‘ladi. Siklik gruppaning qism gruppasi yana siklik bo‘lganligi uchun H gruppa ham siklik.

Aytaylik, $|H| = m$ bo‘lsin, u holda $|\mathrm{Gal}(\mathbb{F}, \mathbb{K})| = n$ ekanligi uchun $m|n$ bo‘lib, H qism gruppaning indeksi $d = \frac{n}{m}$ bo‘ladi. Demak, H gruppaning ψ hosil qiluvchi elementi uchun $\psi = \varphi^d$ tenglik o‘rinli. $\alpha \in \mathbb{K}(\alpha)$ bo‘lganligi uchun $\varphi^d(\alpha) = \alpha$ bo‘lib, bundan ixtiyoriy i, j uchun $\varphi^{id+j}(\alpha) = \varphi^j(\alpha)$ kelib chiqadi. Quyidagi tengliklarni qaraymiz

$$(\zeta, \alpha) = \sum_{k=0}^{n-1} \zeta^k \cdot \varphi^k(\alpha) = \sum_{i=0}^{m-1} \sum_{j=0}^{d-1} \zeta^{id+j} \cdot \varphi^{id+j}(\alpha) =$$

$$= \sum_{i=0}^{m-1} \sum_{j=0}^{d-1} \zeta^{id+j} \cdot \varphi^j(\alpha) = \sum_{j=0}^{d-1} \zeta^j \cdot \varphi^j(\alpha) \cdot \sum_{i=0}^{m-1} \zeta^{id}.$$

Agar $d \neq n$ bo‘lsa u holda $\zeta^d \neq 1$ bo‘lib, $\zeta^n = 1$ ekanligini hisobqa olgan holda quyidagini hosil qilamiz

$$\sum_{i=0}^{m-1} \zeta^{id} = 1 + \zeta^d + \zeta^{2d} + \dots + \zeta^{(n-1)d} = \frac{1 - \zeta^{md}}{1 - \zeta^d} = \frac{1 - \zeta^n}{1 - \zeta^d} = 0.$$

Demak, $d \neq n$ bo‘lgan holda $(\zeta, \alpha) = 0$. Lemma shartiga ko‘ra $(\zeta, \alpha) \neq 0$ bo‘lganligi uchun $d = n$, ya’ni $m = 1$ kelib chiqadi. Bu esa, $H = E$ ekanligini, ya’ni $\mathbb{F} = \mathbb{K}(\alpha)$ bo‘lishini bildiradi. □

Biz yuqoridagi lemmada agar $(\zeta,\alpha)\neq 0$ bo‘lsa, u holda $\mathbb{F}=\mathbb{K}(\alpha)$ bo‘lishini ko‘rsatdik. Lekin buning teskarisi har doim ham o‘rinli bo‘lavermaydi. Ya’ni $\mathbb{F}=\mathbb{K}(\alpha)$ bo‘lib, $(\zeta,\alpha)=0$ bo‘lishi ham mumkin.

Endi $(\zeta,\alpha)\neq 0$ bo‘lsa, $\beta=(\zeta,\alpha)$ kabi belgilab, (ζ^t,α) ifodalarni organamiz.

6.6.3-lemma. *Ixtiyoriy t natural son uchun quyidagi munoisabat o‘rinli*

$$(\zeta^t,\alpha)\in\mathbb{K}(\beta),$$

bu yerda $\beta=(\zeta,\alpha)\neq 0$.

Isbot. Agar

$$(\zeta^t,\alpha)=\alpha+\zeta^t\cdot\varphi(\alpha)+\zeta^{2t}\cdot\varphi^2(\alpha)+\cdots+\zeta^{(n-1)t}\cdot\varphi^{n-1}(\alpha)$$

ifodaga φ avtomorfizmni qo‘llab, $\varphi(\zeta)=\zeta$ ekanligini hisobga olsak, quyidagiga ega bo‘lamiz

$$\varphi(\zeta^t,\alpha)=\varphi(\alpha)+\zeta^t\cdot\varphi^2(\alpha)+\cdots+\zeta^{(n-2)t}\cdot\varphi^{n-1}(\alpha)+\zeta^{(n-1)t}\cdot\varphi^n(\alpha)=$$

$$=\zeta^{-t}\big(\zeta^t\varphi(\alpha)+\zeta^{2t}\cdot\varphi^2(\alpha)+\cdots+\zeta^{(n-1)t}\cdot\varphi^{n-1}(\alpha)+\alpha\big)=\zeta^{-t}(\zeta^t,\alpha).$$

Demak, ixtiyoriy t uchun

$$\varphi(\zeta^t,\alpha)=\zeta^{-t}(\zeta^t,\alpha) \tag{6.10}$$

tenglikka ega bo‘lamiz, xususan $t=1$ bo‘lganda $\varphi(\zeta,\alpha)=\zeta^{-1}(\zeta,\alpha)$.

Ushbu tenglikning ikkala tomonini t darajaga oshirsak,

$$\varphi\big((\zeta,\alpha)^t\big)=\zeta^{-t}(\zeta,\alpha)^t. \tag{6.11}$$

Yuqoridagi (6.10) va (6.11) tengliklarni bo‘lsak,

$$\varphi\left(\frac{(\zeta^t,\alpha)}{(\zeta,\alpha)^t}\right)=\frac{(\zeta^t,\alpha)}{(\zeta,\alpha)^t}$$

tenglikka ega bo‘lamiz, ya’ni φ avtomorfizm $\frac{(\zeta^t,\alpha)}{(\zeta,\alpha)^t}$ elementni o‘zgarishsiz qoldiradi. φ avtomorfizm $\mathrm{Gal}(\mathbb{F},\mathbb{K})$ siklik gruppaning yasovchisi ekanligidan $\frac{(\zeta^t,\alpha)}{(\zeta,\alpha)^t}$ element ixtiyoriy avtomorfizmda ham o‘zgarishsiz qolishi kelib chiqadi. Demak, $\frac{(\zeta^t,\alpha)}{(\zeta,\alpha)^t}\in\mathbb{K}$, ya’ni ixtiyoriy t uchun shunday $c_t\in\mathbb{K}$ element topilib, $\frac{(\zeta^t,\alpha)}{(\zeta,\alpha)^t}=c_t$. Boshqacha qilib aytganda $(\zeta^t,\alpha)=c_t(\zeta,\alpha)^t=c_t\beta^t$, ya’ni $(\zeta^t,\alpha)\in\mathbb{K}(\beta)$ □

6.6.4-lemma. *Agar $\beta=(\zeta,\alpha)\neq 0$ bo‘lsa, u holda $\mathbb{F}=\mathbb{K}(\beta)$.*

Isbot. Quyidagi yig'indini qaraymiz

$$\sum_{t=0}^{n-1}(\zeta^t,\alpha)=\sum_{t=0}^{n-1}\sum_{j=0}^{n-1}\zeta^{jt}\varphi^j(\alpha)=\sum_{j=0}^{n-1}\left(\varphi^j(\alpha)\sum_{t=0}^{n-1}\zeta^{jt}\right).$$

Agar $j=0$ da $\sum\limits_{t=0}^{n-1}\zeta^{jt}=n$ va $j=1$ da $\sum\limits_{t=0}^{n-1}\zeta^{jt}=\frac{\zeta^{jn}-1}{\zeta^j-1}=0$ ekanligini hisobga olsak,

$$\sum_{t=0}^{n-1}(\zeta^t,\alpha)=n\alpha$$

tenglikka ega bo'lamiz. 6.6.3-lemmaga ko'ra, tenglikning chap tomonida turgan ifodalar $\mathbb{K}(\beta)$ maydonga tegishli bo'lganligi uchun, o'ng tomondagi ifoda ham shu maydonga tegishli bo'ladi, ya'ni $\alpha\in\mathbb{K}(\beta)$. 6.6.2-lemmaga ko'ra $\mathbb{K}=\mathbb{K}(\alpha)$ ekanligidan, $\mathbb{F}\subset\mathbb{K}(\beta)$ kelib chiqadi. Ikkinchi tomondan esa, $\beta\in\mathbb{K}$ bo'lganligi uchun $\mathbb{K}(\beta)\subset\mathbb{F}$. Demak, biz $\mathbb{F}=\mathbb{K}(\beta)$ ekanligiga ega bo'ldik. □

Endi siklik kengaytma bilan sodda radikal kengaytma orasidagi bog'lanishni beruvchi asosiy teoremani keltiramiz.

6.6.1-teorema. *Agar xarakteristikasi nolga teng bo'lgan $\mathbb{K}$ maydon birning n-darajali boshlang'ich ildizini o'z ichiga olsa, u holda uning ixtiyoriy n-darajali siklik kengaytmasi $f(x)=x^n-c$ ko'phad orqali aniqlanuvchi sodda radikal kengaytma bo'ladi.*

Isbot. Aytaylik, xarakteristikasi nolga teng bo'lgan maydonning n-darajali $\mathbb{K}\subset\mathbb{F}$ siklik kengaytmasi berilgan bo'lib, ζ – birning n-darajali boshlang'ich ildizi $\mathbb{K}$ maydonga tegishli va $\varphi\in\mathrm{Gal}(\mathbb{F},\mathbb{K})$ avtomorfizm siklik gruppaning hosil qiluvchi elementi bo'lsin. U holda 6.6.1-lemmaga ko'ra shunday $\alpha\in\mathbb{F}$ element topilib, $(\zeta,\alpha)\neq 0$. Agar $\beta=(\zeta,\alpha)$ va $\gamma=\beta^n$ kabi belgilab olsak, u holda (6.11) tenglikka ko'ra

$$\varphi(\gamma)=\varphi((\zeta,\alpha)^n)=\zeta^{-n}(\zeta,\alpha)^n=(\zeta,\alpha)^n=\gamma.$$

Bundan esa, $\gamma\in\mathbb{K}$ ekanligi kelib chiqadi. Demak, β element $x^n-\gamma$ keltirilmas ko'phadning ildizi. 6.6.4-lemmaga ko'ra $\mathbb{F}=\mathbb{K}(\beta)$ bo'lganligi uchun $\mathbb{K}\subset\mathbb{F}$ kengaytmaning sodda radikal kengaytma ekanligini hosil qilamiz. □

Endi Galua teoremasining yetarliligi isbotini beruvchi teoremani keltiramiz.

6.6.2-teorema. *Agar xarakteristikasi nolga teng bo'lgan maydonda $\mathbb{K}\subset\mathbb{L}$ normal kengaytmaning Gal$(\mathbb{L},\mathbb{K})$ Galua gruppasi yechiluvchan bo'lsa, u holda $\mathbb{L}$ maydon $\mathbb{K}$ maydonning qandaydir normal radikal kengaytmasining ichida yotadi.*

Isbot. Dastlab, Galua gruppasi siklik bo‘lgan holni qaraymiz, ya’ni aytaylik, $\mathbb{K} \subset \mathbb{L}$ normal kengaytmaning darajasi m ga teng bo‘lib, $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ gruppa siklik bo‘lsin. U holda birning m-darajali boshlang‘ich ildizi ξ uchun $\mathbb{F} = \mathbb{L}(\xi)$ maydonni qaraymiz.

Ushbu $\mathbb{F}$ maydon $\mathbb{K}$ maydonning normal kengaytmasi hamda $\mathbb{L}$ va $\mathbb{K}(\xi)$ maydonlarni o‘z ichiga olivchi eng kichik maydon bo‘lib, 6.6.3-natijaga ko‘ra $\mathrm{Gal}(\mathbb{F}, \mathbb{K}(\xi))$ gruppa $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ gruppaning qandaydir qism gruppasiga izomorf bo‘ladi. Bundan esa $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ gruppa siklik bo‘lganligi uchun $\mathrm{Gal}(\mathbb{F}, \mathbb{K}(\xi))$ gruppaning ham siklikligi kelib chiqadi.

Agar $|\mathrm{Gal}(\mathbb{F}, \mathbb{K}(\xi))| = n$, ya’ni $[\mathbb{F} : \mathbb{K}(\xi)] = n$ bo‘lsa, u holda $n|m$ bo‘lib, birning n-darajali boshlang‘ich ildizi ζ birning m-darajali boshlang‘ich ildizi ξ ning qandaydir darajasidan iborat bo‘ladi. Bu esa, $\zeta \in \mathbb{K}(\xi)$ ekanligini bildiradi.

Shunday qilib biz $\mathbb{K}(\xi) \subset \mathbb{F}$ kengaytma siklik kengaytma bolib, birning n-darajali boshlang‘ich ildizi ζ uchun $\zeta \in \mathbb{K}(\xi)$ ekanligini ko‘rsatdik. U holda 6.6.1-teoremaga ko‘ra ushbu $\mathbb{K}(\xi) \subset \mathbb{F}$ kengaytma sodda radikal kengaytma bo‘lib, $\mathbb{K} \subset \mathbb{K}(\xi) \subset \mathbb{F}$ bo‘lganligi uchun $\mathbb{F}$ maydon $\mathbb{K}$ maydoning radikal kengaytmasi bo‘ladi. Ushbu kengaytmaning normal ekanligi va $\mathbb{L} \subset \mathbb{F}$ bo‘lishi $\mathbb{F}$ maydonning qurilishidan kelib chiqadi. Demak, Galua gruppasi siklik bo‘lgan hol uchun teorema isbotlandi.

Endi umumiy holga o‘tamiz, ya’ni $\mathbb{K} \subset \mathbb{L}$ normal kengaytma berilgan bo‘lib, $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ Galua gruppasi yechiluvchan bo‘lsin. U holda quyidagicha yechiluvchan qator mavjud

$$\mathrm{Gal}(\mathbb{L}, \mathbb{K}) = H_0 \supset H_1 \supset \cdots \supset H_{i-1} \supset H_i \supset \cdots \supset H_s \supset E.$$

Isbotni s bo‘yicha induksiya orqali amalga oshiramiz. Agar $s = 1$ bo‘lsa, u holda $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ gruppa siklik bo‘lib, yuqorida isbotlangan holga kelamiz. Demak, $s = 1$ uchun teorema o‘rinli. Endi Galua gruppasi uzunligi $s - 1$ ga teng bo‘lgan yechiluvchan qatorga ega bo‘lgan maydonlar uchun teorema o‘rinli deb faraz qilib, $\mathbb{L}$ maydonning Galua gruppasi yechiluvchan qatorining uzunligi s ga teng bo‘lsin deb olamiz. Ushbu qatordagi H_1 normal qism gruppga mos keluvchi $\mathbb{L}_{H_1}$ maydonni qarasak, $\mathbb{K} \subset \mathbb{L}_{H_1}$ kengaytma ham normal bo‘lib, $\mathrm{Gal}(\mathbb{L}_{H_1}, \mathbb{K})$ Galua gruppasi $\mathrm{Gal}(\mathbb{L}, \mathbb{K})/H_1$ faktor gruppaga izomorf bo‘ladi. Bundan esa $\mathrm{Gal}(\mathbb{L}_{H_1}, \mathbb{K})$ gruppaning siklik ekanligi kelib chiqadi. U holda $\mathbb{L}_{H_1}$ maydon qandaydir normal radikal kengaytmaning ichida yotadi.

Aytaylik, $\mathbb{L}_{H_1}$ maydonni o‘z ichiga oluvchi normal radikal kengaytma $\mathbb{P}$ bo‘lsin. $\mathbb{L}$ va $\mathbb{P}$ maydonlarni o‘z ichiga oluvchi eng kichik maydonni $\overline{\mathbb{L}}$ kabi belgilasak, 6.6.3-natijaga ko‘ra $\mathrm{Gal}(\overline{\mathbb{L}}, \mathbb{P})$ gruppa $\mathrm{Gal}(\mathbb{L}, \mathbb{L}_{H_1})$ gruppaning qandaydir qism gruppasiga izomorf bo‘ladi. Endi $\mathrm{Gal}(\mathbb{L}, \mathbb{L}_{H_1}) = H_1$ ekanligini hisobga olsak, H_1 gruppa uzuligi $s - 1$ ga teng bo‘lgan yechiluvchan qatorga ega bo‘lganligi uchun uning ixtiyoriy qism gruppasi ham, xususan $\mathrm{Gal}(\overline{\mathbb{L}}, \mathbb{P})$ gruppa ham uzuligi $s - 1$

ga teng bo‘lgan yechiluvchan qatorga egaligi kelib chiqadi. Bundan esa, induksiya faraziga ko‘ra, $\overline{\mathbb{L}}$ maydon $\mathbb{P}$ maydonning qandaydir normal radikal kengaytmasi ichida yotishi kelib chiqadi. $\overline{\mathbb{L}}$ maydonni o‘z ichiga olib, $\mathbb{P}$ maydonning normal radikal kengaytmasi bo‘lgan uchbu maydonni $\mathbb{F}$ kabi belgilasak, $\mathbb{K} \subset \mathbb{P} \subset \mathbb{F}$ ketma-ketlikdagi har bir kengaytma radikal kengaytma bo‘lganligi uchun $\mathbb{F}$ maydon $\mathbb{K}$ maydonning radikal kengaytmasi bo‘ladi. 6.5.3-teoremaga ko‘ra esa $\mathbb{K} \subset \mathbb{F}$ radikal kengaytmani o‘z ichiga oluvchi $\overline{\mathbb{F}}$ normal radikal kengaytma mavjud.

Shunday qilib biz $\mathbb{L}$ maydonni o‘z ichiga oluvchi $\mathbb{K} \subset \overline{\mathbb{F}}$ normal radikal kengaytma mavjudligini ko‘rsatdik. □

6.7 Mustaqil ishlash uchun misol va masalalar

1. Quyidagi kengaytmalarning darajalarini toping va bazislarini aniqlang.
   - $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3})$.
   - $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{5})$.
   - $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{7})$.
   - $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.
   - $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{7})$.
   - $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
   - $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3} + \sqrt{5})$.
   - $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt[3]{2})$.

2. Quyidagi ko‘phadlarning ko‘rsatilgan maydonlarda keltirilmas ekanligini isbotlang.
   - $f(x) = x^2 - 5, \quad \mathbb{F} = \mathbb{Q}(\sqrt{2})$.
   - $f(x) = x^2 - 7, \quad \mathbb{F} = \mathbb{Q}(\sqrt{3})$.
   - $f(x) = x^4 + 3x^2 - 7x + 1, \quad \mathbb{F} = \mathbb{Q}$.
   - $f(x) = x^4 + x + 1, \quad \mathbb{F} = \mathbb{Z}_2$.
   - $f(x) = x^3 + 3x + 2, \quad \mathbb{F} = \mathbb{Z}_5$.

3. $\mathbb{Q}$ ratsional sonlar maydoni ustida quyidagi sonlarga mos keluvchi minimal ko‘phadlarni toping.
   - $\sqrt{2} + \sqrt{3}$.
   - $\sqrt{2 + \sqrt{5}}$.
   - $\sqrt{2 - \sqrt{2}}$.

- $\sqrt{6+3\sqrt{2}}$.

4. Quyidagi maydonlarning berilgan ko‘phad orqali yoyilgan maydonlarini aniqlang va yoyilmaning darajasini toping.
   - $\mathbb{K}=\mathbb{Q}, \quad f(x)=x^4-2$.
   - $\mathbb{K}=\mathbb{Q}, \quad f(x)=x^4+4$.
   - $\mathbb{K}=\mathbb{Q}, \quad f(x)=x^3-3$.
   - $\mathbb{K}=\mathbb{Q}, \quad f(x)=x^4-5x^2+6$.
   - $\mathbb{K}=\mathbb{Q}, \quad f(x)=x^4-10x^2+21$.
   - $\mathbb{K}=\mathbb{Q}, \quad f(x)=x^4+x^2+1$.
   - $\mathbb{K}=\mathbb{Q}, \quad f(x)=x^6+x^3+1$.
   - $\mathbb{K}=\mathbb{Z}_2, \quad f(x)=x^2+1$.
   - $\mathbb{K}=\mathbb{Z}_5, \quad f(x)=x^2+x+1$.
5. $\mathrm{Gal}(\mathbb{C},\mathbb{R})$ Galua gruppasining tartibini aniqlang, bu yerda $\mathbb{C}$ va $\mathbb{R}$ mos ravishda kompleks va haqiqiy sonlar maydonilari.
6. $\mathbb{Q}(\sqrt[3]{5})=\mathbb{Q}(\sqrt[3]{25})$ ekanligini ko‘rsating.
7. Agar $\mathbb{F}=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ bo‘lsa, $\mathrm{Gal}(\mathbb{F},\mathbb{Q})$ Galua gruppasining tartibini aniqlang.
8. $\mathbb{Q}\subset\mathbb{Q}(i,\sqrt{3})$ maydonlar orasidagi barcha mayonlarni aniqlang.
9. Ratsional sonlar maydoni ustida berilgan quyidagi ko‘phadlarning Galua gruppalarini toping.
   - $f(x)=x^2-x+1$.
   - $f(x)=x^4-1$.
   - $f(x)=x^3-x-1$.
   - $f(x)=x^3-3x+1$.
   - $f(x)=x^3-2$.
   - $f(x)=x^3-7$.
   - $f(x)=(x^2-2)(x^2-5)$.
   - $f(x)=x^4+x^3+x^2+x+1$.
   - $f(x)=x^4+x^2+1$.
   - $f(x)=(x^2-3x+1)(x^3-2)$.
10. Ratsional sonlar maydoni ustida berilgan $f(x)=x^5-10x^4+2x^3-24x^2+2$ ko‘phadning Galua gruppasi S_5 ga izomorf ekanligini ko‘rsating.

Foydalanilgan adabiyotlar ro‘yxati

1. Xodjiyev D.X., Faynleyb A.S. ***Algebra va sonlar nazaryasi kursi***. “O‘zbekiston”, 2001 y. 304 b.
2. Artin M. ***Algebra***. 2nd Edition, “Pearson Education”, 2018, p. 560.
3. Ash R.B. ***Abstract Algebra***. “Dover Publication”, 2006, p. 674.
4. Dummit D.S., Foote R.M. ***Abstract Algebra***. 3rd Edition. “Wiley”, 2003, p. 944.
5. Fraleigh J.B., Brand N. ***A First Course in Abstract Algebra***. 8th Edition. “Pearson Education”, 2020, p. 443.
6. Grillet P.A. ***Abstract Algebra***. “Springer”, 2007, p. 674.
7. Hungerford T.W. ***Algebra***. “Springer”, 1974, p. 504.
8. Lang S. ***Algebra***. “Springer”, 2002, p. 933.
9. Malik D.S., Mordeson J.N., Sen M.K. ***Fundamentals of abstract algebra***. “WCB McGrew-Hill”, 1997, p.636.
10. Ван-дер-Варден Б.Л.. ***Алгебра***. “Мир”, 1976, 648 с.
11. Винберг Э.Б. ***Курс алгебры***. “Факториал пресс”, 2001, 544 с.
12. Каргаполов М.И., Мерзляков Ю.И. ***Основы теории групп***. “Наука”, 1982, 288 с.
13. Кострикин А.И. ***Введение в алгебру***. Часть I. Основы алгебры. “Физматлит”, 1994, 320 с.
14. Кострикин А.И. ***Введение в алгебру***. Часть III. Основные структуры. “Физматлит”, 2004, 272 с.
15. Курош А.Г. ***Лекции по общей алгебре***. “Физматлит”, 1973, 400 с.
16. Курош А.Г. ***Теория групп***. “Наука”, 1967, 648 с.
17. Постников М.М. ***Теория Галуа***. “Факториал пресс”, 2003, 304 с.
18. Проскуряков И.Л. ***Сборник задач по линейной алгебре***. “Лань”, 2010 г. 480 с.
19. Скорняков Л.А. ***Элементы общей алгебры***. “Наука”, 1983, 272 с.
20. ***Сборник задач по алгебре***. Под редакцией, Кострикина А.И. “Физматлит”, 2001. 464 с.

Tushuncha va atamalarning qisqacha lug'ati

O'zbekcha	Ruscha	Inglizcha
birlamchi ideal	первичный идеал	prime ideal
bosh ideal	главный идеал	principal ideal
buralish	кручение	torsion
butunlik sohasi	область целостности	integral domain
davriy gruppa	периодическая группа	periodic group (torsion group)
davriy qism	периодическая часть	periodic part (torsion part)
diedr	диедр	dihedral
erkin gruppa	свободная группа	free group
hosilaviy qator	производный ряд	derived series
invariant faktorlar	инвариантные факторы	invariant factors
ichki to'g'ri ko'paytma	внутреннее прямое произведение	internal direct product
jism	тело	division ring
kamayuvchi zanjir	убивающая цепь	descending chain
keltirilmas element	неприводимый элемент	irreducible element
markaziy qator	центральный ряд	central series
moslik teoremasi	теорема о соответствии	correspondence theorem
primar ideal	примарный идеал	primary ideal
primar komponenta	примарная компонента	primary component
quyi qator	нижний ряд	descending series
sodda gruppa	простая группа	simple group
stabilizator	стабилизатор	stabilizer
tashqi to'g'ri ko'paytma	внешнее прямое произведение	external direct product
ta'sir	действие	action
tub element	простой элемент	prime element
yechiluvchan	разрешимый	solvable
yoyilgan maydon	поле разложение	splitting field
yuqori qator	верхний ряд	ascending series
o'zuvchi zanjir	возрастающая цепь	ascending chain