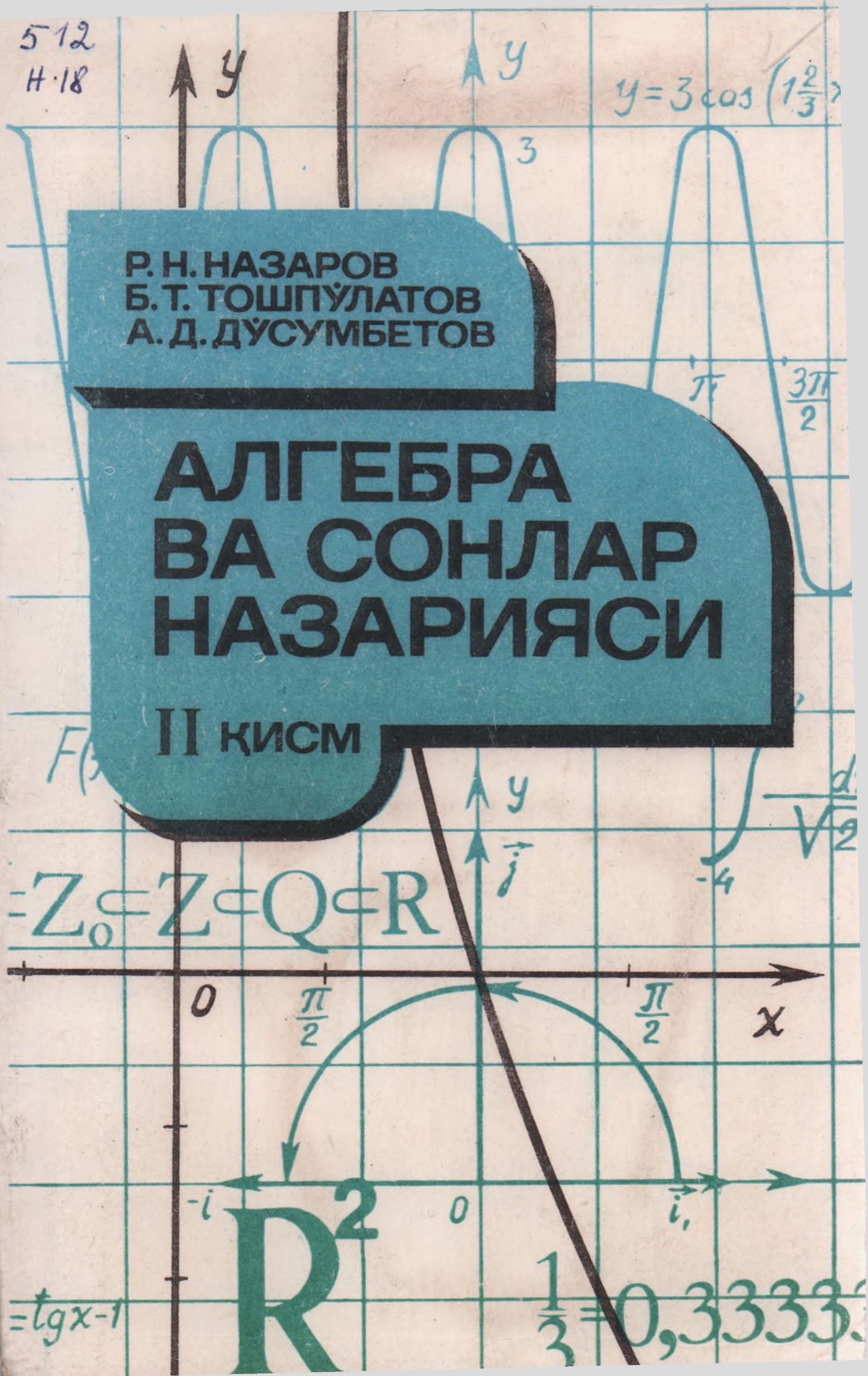


Р. Н. НАЗАРОВ
Б. Т. ТОШПЎЛАТОВ
А. Д. ДЎСУМБЕТОВ

АЛГЕБРА ВА СОНЛАР НАЗАРИЯСИ

II қисм

Р. Н. НАЗАРОВ, Б. Т. ТОШПЎЛАТОВ,
А. Д. ДЎСУМБЕТОВ

АЛГЕБРА ВА СОНЛАР НАЗАРИЯСИ

II ҚИСМ

Ўзбекистон Республикаси Халқ таълими вазирлиги
педагогика институтлари ва университетларининг физика
ва математика факультетлари талабалари учун ўқув қўлланма
сифатида тавсия этган

ТОШКЕНТ „ЎҚИТУВЧИ“ 1995

Махсус муҳаррир — Ўзбекистон Фанлар Академиясининг В. И Романовский номидаги математика илмий-тсқшириш институти катта илмий ходими, физика-математика фанлари номзоди **М. А. Бердиқулов.**

Тақризчилар: Ўзбекистон Фанлар Академиясининг мухбир аъзоси, физика-математика фанлари доктори, профессор **Ш. А. Аюпов**; Хоразм Давлат университети алгебра кафедраси мудири, физика-математика фанлари номзоди, доцент **И. Абдуллаев.**

Қўлланма „Алгебра ва сонлар назарияси" курсининг II қисми бўлиб, унда бутун сонлар ва бўлиниш назарияси, комплекс ва ҳақиқий сонлар майдони устида кўпҳадлар, ҳалқа, ҳалқаларнинг изоморфлиги, бутунлик соҳалари каби масалалар ёритилган. Бир қанча мисоллар ишлаб кўрсатилган.

Қўлланма педагогика институтлари ва университетлари талабалари учун мўлжалланган.

$Н \frac{1602030000-96}{353-04-95}$ 175 — 95

ISBN 5—645—02264—5

СЎЗ БОШИ

Ушбу ўқув қўлланма педагогика институтлари ва университетларининг физика ва математика факультетлари талабалари учун муаллифларнинг „Алгебра ва сонлар назарияси“ ўқув қўлланмаси I қисмининг давомидир. Бу қўлланма янги дастур бўйича ёзилган бўлиб, унда бутун сонлар ҳалқасида бўлиниш назарияси, таққосламалар назарияси, ҳалқа, бутунлик соҳалари, идеаллар, бир номаълумли кўпҳадлар, кўп номаълумли кўпҳадлар, рационал, ҳақиқий ва комплекс сонлар майдони устидаги кўпҳадлар, алгебраик ва трансцендент кенгайтмалар каби тушунчаларга катта эътибор берилди. Ҳар бир параграфда назарияни чуқур ўзлаштириш учун мисоллар келтирилди.

Ушбу ўқув қўлланмани синчиклаб ўқиб, фойдали маслаҳатларини берган Ўзбекистон Фанлар Академиясининг мухбир аъзоси, физика-математика фанлари доктори, профессор Ш. А. Аюпов, Ўзбекистон Фанлар Академиясининг В. И. Романовский номидаги математика илмий-текшириш институти катта илмий ходимлари, физика-математика фанлари номзодлари, доцентлар М. ,А. Бердиқулов ва И. А. Аллаков, Хоразм Давлат университети алгебра кафедраси мудири, физика-математика фанлари номзоди, доцент И. Абдуллаевларга ўз миннатдорчилигимизни изҳор этамиз.

Муаллифлар

I боб. БУТУН СОНЛАР ҲАЛҚАСИДА БЎЛИНИШ НАЗАРИЯСИ

1-§. Бутун сонлар ва улар устида амаллар

Натурал сонлар тўпламида ушбу

$$b+x=a \tag{1}$$

тенглама фақат $a>b$ бўлганда ва фақат шундагина $x=a-b$ ечимга эга бўлади ҳамда у a ва b сонларнинг *айирмаси* дейилади. Бошқача айтганда, $a>b$ бўлса, (1) тенгламанинг ечими бир жуфт (a; b) натурал сонлар ёрдамида аниқланади. Агар $a\leqslant b$ бўлса, (1) тенглама натурал сонлар тўпламида ечимга эга эмас. Натурал сонлар тўпламини шундай кенгайтириш керакки, у кенгайтмада (1) тенглама доимо ечимга эга бўлсин. Шу масалага батафсил тўхталиб ўтамиз.

Фараз қилайлик,

$$b+x=a \quad \text{ва} \quad d+y=c$$

тенгламаларнинг ечимлари мавжуд бўлиб, улар устма-уст тушсин. Бу иккита тенгламанинг ечимлари топилган деб фараз қилиб, биринчи тенгламанинг иккала томонига d ни, иккинчи тенгламанинг иккала томонига эса b ни қўшамиз:

$$d+b+x=d+a, \quad b+d+y=b+c.$$

Бу тенгламалардан кўринадики, агар x ва y лар биз қураётган кенгайтманинг битта элементи бўлса, у ҳолда бу кенгайтмада

$$d+a=b+c \tag{2}$$

тенглик бажарилиши керак. Фараз қилайлик

$$b+x=a \quad \text{ва} \quad d+y=c$$

тенгламаларнинг ечимлари мос равишда (a; b) ва (c; d) жуфтликлар ёрдамида аниқланган бўлсин. У ҳолда

$$(b+d)+(x+y)=a+c \tag{3}$$

тенглама ҳосил бўлади. Бундан x ва y нинг $x+y$ йиғиндиси ($a+c$; $b+d$) жуфтлик ёрдамида аниқланар экан.

Энди мос равишда (a; b) ва (c; d) жуфтликлар ёрдамида аниқланувчи x ва y элементларнинг $x\,y$ кўпайтмаси қандай жуфтлик ёрдамида аниқланишини излаймиз. Бунинг учун $b+x=a$, $d+y=c$ тенгламаларни ҳаллаб кўпайтирамиз. У ҳолда

$$bd+dx+by+xy=ac$$

тенглама ҳосил бўлади. Бу тенгламанинг иккала қисмига bd ни қўшиб, қуйидаги тенгламани ҳосил қиламиз:

$$bd+dx+bd+by+xy=ac+bd,$$
$$d(b+x)+b(d+y)+xy=ac+bd,$$
$$ad+bc+xy=ac+bd$$

Демак, $x\cdot y$ кўпайтма $(ac+bd,\ ad+bc)$ жуфтлик ёрдамида аниқланар экан.

Маълумки, натурал сонлар тўплами N тартибланган тўпламдир, яъни ҳар қандай $(a;\ b)$ натурал сонлар жуфтлиги учун $a=b$, $a>b$, $a<b$ муносабатлардан биттаси ва фақат биттаси ўринли бўлади.

1-таъриф. Агар $a=b$, $a>b$ ёки $a<b$ муносабатлар ўринли бўлса, у ҳолда $(a;\ b)$ жуфтлик мос равишда *ноль*, *мусбат* ёки *манфий жуфтлик* дейилади.

2-таъриф. Агар $a+d=b+c$ тенглик ўринли бўлса, у ҳолда $(a;\ b)$ ва $(c;\ d)$ жуфтликлар *эквивалент жуфтликлар* дейилади.

Бошқача айтганда, бу таърифга кўра

$$(\forall a,\ b,\ c,\ d\in N)\ (a+d=b+c)\Rightarrow((a;\ b)\backsim(c;\ d)).$$

Биз $(a;\ b)$ кўринишдаги барча жуфтликлар тўпламини Z орқали белгилаймиз. 2-таърифга кўра Z тўпламда эквивалентлик муносабати аниқланган.

Маълумки, эквивалентлик муносабати шу муносабат аниқланган тўпламни эквивалентлик синфларга ажратар эди (I қисм, I боб), яъни 2-таърифдаги эквивалентлик муносабати қаралаётган $(a;\ b)$ жуфтликлар ҳосил қилган эквивалент синфлар тўплами фактор-тўплам деб аталар эди. Шу фактор тўпламнинг элементларини бутун сонлар деб қабул қиламиз.

3-таъриф. $(a;\ b)$ кўринишдаги жуфтликларнинг ҳар бир эквивалентлик синфи *бутун сон* дейилади.

Бошқача айтганда $(a;\ b)$ жуфтликка $a-b$ бутун сон мос қўйилади. Ушбу $n\to\{(a+n;\ a)\}$ акслантириш натурал сонлар тўплами N, бутун сонлар тўплами Z нинг қисм тўплами эканини кўрсатади. N тўпламдаги қўшиш ва кўпайтириш амалига Z тўпламда аниқланган қўшиш ва кўпайтириш амаллари мос келади. Ҳақиқатан,

$$n+m \to \{(a+n+m;\ a)\},\quad n\cdot m \to \{(a+n\cdot m;\ a)\}.$$

Шундай қилиб, $(a+n;\ a)$ жуфтликлар синфига, бу синфнинг аниқланишига асосан, n натурал сон мос қўйилади. $(a;\ a)$ жуфтликлар синфини ноль билан белгилайлик. Аммо $(a+n;\ a)+(a;\ a+n)=(k;\ k)$ бўлгани учун $(a;\ a+n)$ жуфтлик $(a+n;\ a)$ жуфтликка *қарама-қарши элемент* дейилади ва $-n$ каби белгиланади ҳамда $-(-n)=n$ деб юритилади.

Шундай қилиб, бутун сонлар тўплами натурал сонлар тўпламининг кенгайтмасидан иборат бўлиб, бу тўпламда (1) тенглама доимо ечимга эга бўлар экан.

4-таъриф.

$$|a|=\begin{cases} a, \text{ агар } a\geqslant 0,\\ -a, \text{ агар } a<0\end{cases}$$

муносабат билан аниқланувчи $|a|$ сон a бутун соннинг *модули* дейилади.

Бутун сонлар тўплами тартибланган тўпламдир. Бунда тартиб муносабати қуйидагича киритилади.

Натурал сонларнинг табиий тартиби сақланади, яъни ҳар қандай натурал сон учун $n>0$, $-n<0$ бўлади. Ихтиёрий n ва k натурал сонлар учун $n>k$ бўлса, у ҳолда $-n<-k$ деб қабул қилинади.

Агар $(a\ \ b)$ жуфтликни $a-b$ билан алмаштирсак, бутун сонлар устидаги амаллар қуйидагидан иборат бўлади:

1. $(\forall n,\ k\in N)\ \ ((-n)+(-k)=-(n+k));$
2. $(n>0,\ k>0,\ n>k)\Rightarrow((-k)+n=n+(-k)=n-k);$
3. $(n>0,\ k>0,\ k>n)\Rightarrow((-k)+n=n+(-k)=-(k-n));$
4. $(\forall z\in Z,\ 0\in Z)\ \ (0+z=z+0=z);$
5. $n\cdot(-k)=(-n)\ k=-nk;$
6. $(-n)\cdot(-k)=nk;$
7. $z\cdot 0=0\cdot z=0.$

2-§. Бутун сонлар ҳалқасида бўлиниш муносабати ва унинг хоссалари

1-§ да кўриб ўтганимиздек, бутун сонлар тўпламида

$$b+x=a \tag{1}$$

тенглама доимо ечимга эга бўлади Лекин бутун сонлар тўплами бўлиш амалига нисбатан ёпиқ бўлмаганлигидан бу тўпламда

$$b\cdot x=a \qquad (2)$$

тенглама ҳар доим ҳам ечимга эга бўлавермайди. Масалан, $2x=7$ тенгламани тўғри тенгликка айлантирувчи бутун сон йўқ. Лекин шундай a ва b бутун сонлар мавжудки, улар учун $\frac{a}{b}$ нисбат доимо бутун сон бўлади. Масалан,

а) $b=\pm 1$ бўлса, у ҳолда $\frac{a}{b}=\pm a$ бўлади;

б) $a=0$ бўлиб, $b\neq 0$ бўлса, у ҳолда $\frac{a}{b}=0$ бўлади;

в) $a=bk$ бўлиб, k бутун сон ва $b\neq 0$ бўлса, у ҳолда $\frac{a}{b}$ бутун сон бўлади.

1-таъриф. Агар a, $b\neq 0$ сонлар учун

$$a=bq \qquad (3)$$

шартни қаноатлантирувчи q бутун сон мавжуд бўлса, у ҳолда *a сон b сонга бўлинади* ёки *b сон a ни бўлади* дейилади.

Агар a сон b га бўлинса, у ҳолда a/b ёки $a\vdots b$ кўринишларда белгиланади. Кўп ҳолларда a/b бўлса, b сон a соннинг *бўлувчиси* ҳам дейилади. (3) тенгликдаги a *бўлинувчи*, b *бўлувчи*, q эса *бўлинма* дейилади.

1-теорема. *Агар $a\neq 0$ ва $b\neq 0$ бўлиб, $a=bq$ тенгликни қаноатлантирувчи q сон мавжуд бўлса, у ягонадир.*

Исботи. Тескарисини фараз қиламиз, яъни (3) шартни қаноатлантирувчи камида иккита ва турли q_1 ва q_2 сонлар мавжуд бўлсин, яъни $a=bq_1$, $a=bq_2$ тенгликлар ўринли бўлсин. Бу тенгликлардан $bq_1=bq_2$ тенглик келиб чиқади. Бундан $b(q_1-q_2)=0$ бўлади. Лекин $b\neq 0$ бўлганидан ва Z да нолнинг бўлувчиси бўлмаганлигидан $q_1-q_2=0$, $q_1=q_2$ келиб чиқади. Бу эса қилган фаразимизга зид. Демак, q бўлинма ягона экан.

Бутун сонлар тўпламида киритилган бўлиниш муносабати қуйидаги хоссаларга эга:

1°. $(\forall a\in Z,\ a\neq 0)\ (0/a)$;

2°. $(\forall a\in Z,\ a\neq 0)\ (a/a)$ (рефлексивлик);

3°. $(\forall a \in Z)\ (a/1)$;

4°. $(\forall a,\ b,\ c \in Z,\ c \neq 0,\ b \neq 0)\ (a/b \wedge b/c \Rightarrow a/c)$ (транзитивлик);

5°. $(\forall a,\ b \in Z,\ a \neq 0,\ b \neq 0)\ (a/b \wedge b/a) \Rightarrow b = \pm a$;

6°. $(\forall a,\ b,\ c \in Z,\ c \neq 0)\ (a/c \Rightarrow ab/c)$;

7°. $(\forall b_i\ \ a \in Z,\ a \neq 0,\ (i = \overline{1,r}))\ b_1/a \wedge b_2/a \wedge \dots \wedge b_r/a$

бўлиб, $x_1,\ x_2,\ \dots,x_r$ ихтиёрий бутун сонлар бўлса, у ҳолда $(b_1x_1 + b_2x_2 + \dots + b_rx_r)/a$ бўлади.

Биз бу хоссалардан охиргисини исбот қилайлик. Бўлиниш таърифига асосан

$$b_i = aq_i\ (i = \overline{1,r}) \tag{4}$$

(4) тенгликлардан ҳар бирини мос равишда x_i га кўпайтириб, натижаларини ҳадлаб қўшсак,

$$\sum_{i=1}^{r} b_ix_i = a\sum_{i=1}^{r} q_ix_i$$

тенглик ҳосил бўлади. Охирги тенглик $\sum\limits_{i=1}^{r} b_ix_i$ нинг a сонга бўлинишини кўрсатади.

3-§. Қолдиқли бўлиш

Биз юқорида a ихтиёрий бутун сон, b эса натурал сон бўлганда $\frac{a}{b}$ нисбат ҳар доим бутун бўлавермаслигини эслатиб ўтган эдик. Лекин қуйидаги теорема доимо ўринли бўлади.

Теорема (қолдиқли бўлиш). *Ҳар қандай $a \in Z$ ва $b \in N$ учун шундай ягона $q \in Z$ ва ягона манфиймас r бутун сон топиладики, улар учун ушбу*

$$a = bq + r, \tag{1}$$

$$0 \leqslant r < b \tag{2}$$

муносабатлар ўринли бўлади.

Исботи. bq сон b нинг a дан катта бўлмаган энг катта карралиси бўлсин. У ҳолда $bq \leqslant a$ ва $a < bq + b$ муносабатлар ўринли бўлади (Архимед аксиомаси).

Бу икки боғланишдан $bq \leqslant a < b(q+1)$ муносабат келиб чиқади. Бу қўш тенгсизликнинг ҳар бир қисмига $(-bq)$ ни қўшсак, $0 \leqslant a - bq < b$ тенгсизлик ҳосил бўлади. Бу ерда $a - bq = r$ белгилаш киритсак, (1) ва (2) муносабатлар ўринли бўлади.

Энди q ва r ларнинг ягоналигини исбот қилайлик. Фараз қилайлик (1) ва (2) ни қаноатлантирадиган $q_1 (q_1 \neq q)$ ва $r_1 (r_1 \neq r)$ мавжуд, яъни

$$a = tq_1 + r_1, \qquad (3)$$

$$0 \leqslant r_1 < b \qquad (4)$$

муносабатлар бажарилсин. (1) ва (3) дан $bq + r = bq_1 + r_1$ ёки $r - r_1 = b(q - q_1)$ тенглик ҳосил бўлади. Охирги тенгликдан $(r - r_1)/b$ келиб чиқади. Лекин $|r - r_1| < b$ бўлганидан $(r - r_1)/b$ муносабат фақат ва фақат $r - r_1 = 0$ бўлгандагина бажарилади, яъни $r_1 = r$ келиб чиқади. $r - r_1 = b(q - q_1)$ тенгликдан $r_1 = r$ ва b нинг натурал сон эканлигини эътиборга олинса, у ҳолда $q - q_1 = 0$, яъни $q_1 = q$ эканлиги келиб чиқади. Демак, (1) ва (2) муносабатларни қаноатлантирувчи q ва r сонлари ягона экан. Агар $b \neq 0$ ихтиёрий бутун сон бўлса, у ҳолда (1) ва (2) муносабатлар $|b|$ учун ўринли бўлади.

4-§. Евклид алгоритми ва унинг татбиқи. Сонларнинг энг катта умумий бўлувчиси. Ўзаро туб сонлар

1-таъриф. a ва b бутун сонларнинг иккаласини ҳам бўладиган сон шу сонларнинг *умумий бўлувчиси* дейилади.

Биз фақат натурал бўлувчилар билангина шуғулланамиз. Умуман $a, b \in Z$ сонлар бир нечта умумий натурал бўлувчиларга эга бўлиши мумкин. Бу умумий бўлувчилар тўпламини биз $D_{a,b}$ орқали белгилайлик. Масалан, $a = 24$, $b = 18$ бўлсин, у ҳолда $D_{24,18} = \{1, 2, 3, 6\}$.

2-таъриф. a ва b натурал сонлар умумий бўлувчиларининг энг каттаси шу сонларнинг *энг катта умумий бўлувчиси* дейилади.

a ва b сонларнинг энг катта умумий бўлувчиси қисқача ЭКУБ деб ёзилиб, у $(a; b)$ кўринишда белгиланади.

3-таъриф. Агар $(a; b) = 1$ бўлса, у ҳолда a ва b натурал сонлар *ўзаро туб сонлар* дейилади.

Берилган сонларнинг ЭКУБини топиш учун аввало ҳар бир соннинг бўлувчилари тўпламини аниқлаймиз.

Агар A тўплам $a\in N$ соннинг бўлувчилари тўплами, b эса $b\in N$ соннинг бўлувчилари тўплами бўлса, $D_{a,b}=A\cap B$ эканлиги равшан.

$A\cap B$ кесишманинг энг катта элементи берилган a ва b сонларнинг ЭКУБ бўлади. Чунки A ва B тўпламлар чекли бўлганлигидан, $D_{a,b}$ тўплам ҳам чекли бўлади, ҳар қандай чекли тўплам эса доимо энг катта ва энг кичик элементга эга.

1-теорема. $(a/b)\Rightarrow[(D_{a,b}=D_b)\wedge((a;b)=b)]$.

Исботи. a ва b сонларнинг ҳар бир умумий бўлувчиси b ни ҳам бўлади a/b бўлгани учун b ни бўлувчи ҳар бир сон a ни ҳам бўлади. Шунинг учун $D_{a,b}=D_b$. Лекин b сонни бўлувчи сонларнинг энг каттаси b нинг ўзидир. Шунинг учун $(a;b)=b$,

Фараз қилайлак, a сон b га бўлинмасин. У ҳолда қолдиқли бўлиш ҳақидаги теоремага асосан қуйидаги тенгликлар системасини ёзиш мумкин:

$$\begin{array}{ll}
a=bq_1+r_2, & 0\leqslant r_2<b,\\
b=r_2q_2+r_3, & 0<r_3<r_2,\\
r_2=r_3q_3+r_4, & 0<r_4<r_3,\\
\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\\
r_{n-2}=r_{n-1}q_{n-1}+r_n, & 0<r_n<r_{n-1},\\
r_{n-1}=r_nq_n. &
\end{array}\qquad(1)$$

(1) системанинг ўнг томонидаги тенгсизликлар системасига эътибор берсак, қуйидаги муносабат кўзга ташланади:

$$b>r_2>r_3>\ldots>r_{n-1}>r_n>0,$$

бу ерда r_i $(i=\overline{2,n})$ ларнинг барчаси натурал сонлар. Лекин натурал сонлар қуйидан чегараланган, шунинг учун бирор n номердан бошлаб $r_{n+1}=0$ бўлади.

(1) тенгликлар системасининг биринчисига асосан a ва b нинг ихтиёрий умумий бўлувчиси r_2 ни бўлади (2-§ даги 7-хоссага қ.) ва аксинча $a=r_2-bq_1$ га асосан r_2 ва b нинг ҳар қандай умумий бўлувчиси a сонни бўлади. Демак, $(D_{a,b}=D_{b,r_2})\Rightarrow((a;b)=(b;r_2))$.

(1) системадаги иккинчи, учинчи ва ундан кейин келадиган тенгликлар ҳамда 1-теоремага асосан

$$D_{a,b}=D_{b,r_2}=D_{r_2,r_3}=\ldots=D_{r_{n-1},r_n}=D_{r_n},$$
$$(a;b)=r_n.\qquad(2)$$

борамиз. $1 \leqslant a < m$ бўлганда $a \in M$ бўлиб, $a = am^0$ тенглик биз излаётган тенглик бўлади. Фараз қилайлик (1) ёйилма a дан кичик бўлган барча натурал сонлар учун ўринли бўлсин. Унда қолдиқли бўлиш теоремасига асосан

$$a = mq + a_0 \ (a_0 \in M) \tag{2}$$

мавжуд бўлиб, $q < a$ бўлади. Фаразимизга асосан (1) ёйилма a дан кичик барча натурал сонлар учун мавжуд. Демак,

$$q = a_1 + a_2 m + \cdots + a_r m^{r-1} \tag{3}$$

ёйилма ҳам мавжуд. (3) ни (2) га қўямиз. У ҳолда

$$a = m(a_1 + a_2 m + \cdots + a_r m^{r-1}) + a_0 =$$
$$= a_0 + a_1 m + \cdots + a_r m^r.$$

Демак, (1) ёйилма a сон учун ҳам ўринли экан. Математик индукция принципига асосан, (1) ёйилма ҳар қандай натурал сон учун ҳам мавжуд бўлади.

1-таъриф. a натурал соннинг (1) кўриниши уни m нинг *даражалари бўйича ёйиш* дейилади.

Энди (1) ёйилманинг ягоналигини исбот қилайлик. Бунинг учун индукция принципидан фойдаланамиз. $a < m$ учун (1) ёйилма ўринли, чунки $a < m$ шартда a сон M тўпламнинг фақат битта элементига тенгдир. Фараз қилайлик, a соннинг ўзи учун (1) каби ёйилмадан бошқа яна битта қуйидаги ёйилма мавжуд бўлсин

$$a = a'_0 m^0 + a'_1 m + a'_2 m^2 + \cdots + a'_{r_1} m^{r_1} =$$
$$= a'_0 + m(a'_1 + a'_2 m + \cdots + a'_{r_1} m^{r-1}).$$

Бу тенгликни

$$a = a'_0 + mq_1 \tag{4}$$

шаклда ёзиб оламиз. Қолдиқли бўлишнинг ягоналигига асосан, (2)ва (4) дан қуйидагиларни ёза оламиз:

$$a_0 = a'_0, \ (q = q_1) \Rightarrow a_1 + a_2 m + \cdots + a_r m^{r-1} =$$
$$= a'_1 + a' m + \cdots + a_r m^{r-1}.$$

Лекин $q < a$ ва $q_1 < a$ бўлганидан индукция принципига асосан, $r_1 = r$ ва $a'_i = a_i$ $(i = \overline{1,r})$. Демак, (1) ёйилмани иккита бўлсин деб қилган фаразимиз нотўғри, яъни (1) ёйилма ягона.

Иккита соннинг ЭКУБ ни бу усулда топишни биринчи бўлиб Евклид кўрсатгани туфайли бу усул одатда Евклид алгоритми деб юритилади.

(2) га асосан $D_{a,b} = D_{r_n}$ ва $(a; b)=r_n$ бўлгани учун қуйидаги хулосани ёза оламиз:

a ва b сонларнинг умумий бўлувчилари тўплами $D_{a,b}$ шу сонлар ЭКУБ нинг бўлувчилари тўплами D_{r_n} билан устма-уст тушади ва бу сонларнинг ЭКУБ Евклид алгоритмидаги нолдан фарқли энг охирги қолдиққа тенг бўлади. Бу хулосани қисқача қуйидагича ёзиш мумкин: $(D_{a,b} = D_{(a,b)}) \wedge ((a; b) = r_n)$.

Мисол. 76501, 29719 сонларнинг ЭКУБ ни топинг.

Қуйидаги кетма-кетликлар системасини ҳосил қиламиз:

$$\begin{aligned}
76501 &= 29719\cdot 2+ 17063,\\
29719 &= 17063\cdot 1 + 12656,\\
17063 &= 12656\cdot 1 + 4407,\\
12656 &= 4407\cdot 2 + 3\ 42,\\
4407 &= 3842\cdot 1 + 565,\\
3842 &= 565\cdot 6 + 452,\\
565 &= 452\cdot 1 + 113,\\
452 &= 113\cdot 4.
\end{aligned}$$

Демак, (76501; 29719) = 113.

Натижа. a ва b сонларнинг ЭКУБ d бўлса, у ҳолда шундай u ва v бутун сонлар топиладики, улар учун $au + bv = d$ тенглик бажарилади.

Исботи. (1) системадаги охирги тенгликдан олдингисини, яъни $r_{n-2} = r_{n-1}q_n + r_n$ тенгликни олайлик. Бундан

$$r_{n-2} - r_{n-1}q_n = d \ (r_n = d) \tag{3}$$

тенгликни ҳосил қиламиз. $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$ тенгликдан r_{n-1} ни топиб, унинг қийматини (3) га қўямиз. Натижада $r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = d$, яъни

$$r_{n-2}(1 + q_{n-1}q_n) - r_{n-3}q_n = d \tag{4}$$

тенглик ҳосил бўлади. $r_{n-4} = r_{n-3}q_{n-2} + r_{n-2}$ тенгликдан r_{n-2} нинг қийматини (4) тенгликка қўямиз. Шу жараённи давом эттириб энг охирида $au+bv=d$ тенгликни ҳосил қиламиз.

Хусусий ҳолда $(a; b)=1$ бўлса, у ҳолда $au+bv=1$ бўлади.

Ўзаро туб сонлар қуйидаги хоссаларга эга:

1°. $((a;\ c)=1)\wedge((b;\ c)=1)\Rightarrow(a;\ b;\ c)=1$ (бунда $c\neq 0$);

2°. $(ab/c)\wedge((a;\ c)=1)\Rightarrow b/c$ (бунда $c\neq 0$);

3°. $(\forall n\in N)((a;\ b)=1)\Rightarrow((a^n;\ b^n)=1)$;

4°. $((a;\ b)=d)\Rightarrow\left(\left(\frac{a}{d};\ \frac{b}{d}\right)=1\right)$;

5°. $((a/b)\wedge(a/c)\wedge((b;\ c)=1))\Rightarrow(a/bc)$.

5-хоссани исботлайлик. Ҳақиқатан, a/b бўлгани учун $a=bk$ $(k\in Z)$ тенглик ўринли. У ҳолда a/c дан bk/c бўлади $(b;\ c)=1$ бўлгани учун 2-хоссага асосан k/c, яъни $k=ct$ $(t\in Z)$ тенглик ўринли. Демак, $a=bk=b(ct)=(bc)t$, яъни $a=(bc)t$ бўлиб, бундан a/bc муносабатнинг бажарилиши келиб чиқади.

Қолган хоссаларни исботлашни ўқувчига тавсия қиламиз.

5-§. Энг катта умумий бўлувчининг баъзи хоссалари

Агар Евклид алгоритмини ak ва bk сонларга татбиқ этсак, 4-§ нинг (1) системасидаги тенгликларнинг ҳар бири ҳади k марта ортади. Шунинг учун

$$(ak;\ bk)=(a;\ b\ k\ (k\in Z) \qquad (1)$$

бўлади. Бундан, қуйидаги хоссалар келиб чиқади:

1°. Агар берилган сонларнинг ҳар бири ўзгармас сонга кўпайтирилса, уларнинг ЭКУБ ҳам шу сонга кўпаяди.

2°. Агар a ва b сонларнинг ҳар бири бирор d сонга бўлинса, уларнинг ЭКУБ ҳам шу сонга бўлинади, яъни

$$\left(\frac{a}{d};\ \frac{b}{d}\right)=\frac{(a;\ b)}{d} \qquad (2)$$

тенглик ўринли бўлади.

Исботи. (1) га асосан қуйидагиларни ёза оламиз:

$$(a;\ b)=\left(\frac{a}{d}\cdot d;\ \frac{b}{d}\cdot d\right)=\left(\frac{a}{d};\ \frac{b}{d}\right)d.$$

Бунлан $\left(\frac{a}{d};\ \frac{b}{d}\right)=\frac{(a;\ b)}{d}$ тенглик келиб чиқади.

Хусусий ҳолда $(a;\ b)=d$ бўлса, (2) дан $\left(\frac{a}{(a,\ b)};\ \frac{b}{(a;\ b)}\right)=1$ келиб чиқади.

1-теорема. *Агар* $((a; c) = 1 \wedge (ab/c)) \Rightarrow b/c$, *яъни* $(a; c) = 1$ *бўлиб*, ab *кўпайтма* c *га бўлинса, у ҳолда* b *сон* c *га бўлинади.*

Исботи. $(a; c) = 1$ нинг иккала қисмини b га кўпайтириб, қуйидагига эга бўламиз: $(ab; bc) = b$. Теорема шартига кўра ab/c ва bc сон c га каррали бўлгани учун bc/c. У ҳолда 1-хосса ва (1) тенгликка асосан $(ab; bc)/c$. Лекин $(ab; bc) = b$ бўлгани учун b/c.

Биз юқорида, асосан, иккита соннинг ЭКУБ ни топиш билан шуғулландик. Бу тушунчани n та натурал. соннинг ЭКУБ ни топишга ҳам татбиқ этиш мумкин n та $a_1, a_2, \ldots, a_n$ соннинг ЭКУБни $(a_1, a_2, \ldots, a_n)$ орқали белгилайлик.

2-теорема. *Ихтиёрий* a, b, c *натурал сонлар учун* $(a; b; c) = ((a; b); c)$ *тенглик ўринли бўлади.*

Исботи. $(a; b) = d_1$, $(d_1; c) = d_2$, $(a; b; c) = d$ белгилашларни киритамиз. Белгилашларга асосан a/d_1, b/d_1, d_1/d_2, c/d_2. Булардан a/d_2, b/d_2, c/d_2 келиб чиқади. Демак, d_2 сон a, b, c сонларнинг умумий бўлувчиси ва d сон бу сонларнинг энг катта умумий бўлувчиси бўлгани учун

$$d/d_2 \tag{3}$$

муносабат ўринли. Евклид алгоритми натижасига асосан $d_1 = ak_1 + bk_2$, $d_2 = d_1k_3 + ck_4$ бўлади. Бу ерда $k_i \in \mathbf{Z}$ $(i = 1, 2, 3, 4)$.

Юқоридаги тенгликлардан

$$d_2 = k_3(ak_1 + bk_2) + ck_4 = ak_1k_3 + bk_2k_3 + ck_4. \tag{4}$$

(6) тенгликка асосан

$$d_2/d \tag{5}$$

муносабат келиб чиқади. (3) ва (5) муносабатлардан $d_2 = d$ тенглик келиб чиқади. Демак, $(a; b; c) = (a; b); c)$ экан.

Фараз қилайлик n та

$$a_1, a_2, \ldots, a_n \tag{6}$$

натурал сон берилган бўлсин. Бу сонларнинг ЭКУБ ни топиш учун биз аввало $(a_1; a_2) = d_2$ ни, сўнгра $(d_2; a_3) = d_3$, $(d_3; a_4) = d_4, \ldots, (d_{n-1}; a_n) = d_n$ ларни топамиз. У ҳолда $D_{a_1, a_2, \ldots, a_n} = D_{d_1, a_3, a_4, \ldots, a_n} = \ldots = D_{d_{n-1}, a_n} = D_{d_n}$ бўлгани учун $(a_1, a_2, \ldots, a_n) = d_n$ бўлади.

1-таъриф. Агар $(a_1, a_2, \ldots, a_n) = 1$ бўлса, у ҳолда $a_1, a_2, \ldots, a_n$ сонлар *ўзаро туб сонлар* дейилади.

2-таъриф. Агар $a_1, a_2, \ldots, a_n$ сонларнинг ихтиёрий иккитаси ўзаро туб бўлса, у ҳолда улар *жуфт-жуфти билан ўзаро туб* ёки *жуфтлама ўзаро туб сонлар* дейилади.

Агар (6) кетма-кетликдаги сонлар жуфт-жуфти билан ўзаро туб бўлса, улар ўзаро туб бўлади. Лекин тескариси тўғри эмас. Бу тасдиқнинг тўғрилигини юқорида келтирилган мисол тасдиқлайди. Чунки, $(3;\ 4;\ 9) = 1$, лекин $(3; 9) = 3$.

6-§. Энг кичик умумий каррали (бўлинувчи)

Ҳар бири нолдан фарқли бўлган a ва b бутун сонлар берилган бўлсин.

1-таъриф. a ва b сонларнинг иккаласига бўлинадиган сон шу сонларнинг *умумий карралиси* (*бўлинувчиси*) дейилади.

a ва b сонларнинг умумий карралилари чексиз кўп бўлади.

2-таъриф. a ва b сонлар умумий карралиларининг энг кичиги шу сонларнинг *энг кичик умумий карралиси* дейилади.

a ва b сонларнинг энг кичик умумий карралиси қисқача ЭКУК деб ёзилади. a ва b сонларнинг ЭКУК $[a;\ b]$ кўринишда белгиланади.

Мисол. Агар $a = 12$ ва $b = 16$ бўлса, у ҳолда $[12;\ 16] = 48$ бўлади.

Энди биз иккита соннинг ЭКУБ ва ЭКУК орасидаги боғланишни қарайлик. Фараз қилайлик, m сон a ва b сонларнинг бирор умумий карралиси бўлсин. Умумий карралининг таърифига асосан m/a ва m/b. m/a бўлганидан

$$m = ak \quad (k \in \mathbf{Z}). \tag{1}$$

Бундан ak/b деган хулосага келамиз. $(a;\ b) = d$, яъни $a = a_1 d$, $b = b_1 d$ ва $(a_1;\ b_1) = 1$ бўлади. $ak/b \Rightarrow a_1 kd/b_1 d$; $a_1 kd/b_1 d \Rightarrow a_1 k/b_1$, лекин $(a_1;\ b_1) = 1$ бўлгани учун k/b_1 бўлади. Демак,

$$k = b_1 t = \frac{b}{d} t \quad (t \in \mathbf{Z}) \tag{2}$$

(2) ни (1) га қўйсак

$$m = \frac{ab}{d} t \tag{3}$$

ган асарида бу масалани тўла очди. Бундан ташқари П. Л. Чебишев шу асарида $\pi(x)$ ва бошқа сонли функцияларнинг хоссаларини текшириш учун кучли элементар методларни кўрсатиб берди. У x нинг етарлича катта қийматларида $\pi(x)$ ни баҳолаш учун қуйидаги тенгсизликлар ўринли эканини исбот қилди:

$$0{,}92129 < \frac{\pi(x)}{\frac{x}{\ln x}} < 1{,}10555$$

ёки

$$0{,}92129 \frac{x}{\ln x} < \pi(x) < 1{,}10555 \frac{x}{\ln x}.$$

Адабиётларда бу тенгсизликлар Чебишев тенгсизликлари деб юритилади. Юқоридаги тенгсизликларнииг исботини келтириб ўтирмасдан, унинг геометрик талқинини баён этамиз.

Бу тенгсизликларга асосан, x етарлича катта қийматни қабул қилса, $\pi(x) : \frac{x}{\ln x}$ функциянинг графиги $y_1 = 0{,}92129$ ва $y_2 = 1{,}10555$ параллел тўғри чизиқлар орасида ётади.

П. Л. Чебишевнинг туб сонлар тақсимоти тўғрисидаги ишлари унинг замондошларига катта таъсир қилди. П. Л. Чебишевнинг қўлга киритган муваффақиятлари ҳақида сўзлаб инглиз математиги Сильвестр (1814—1894) 1881 йилда қуйидаги фикрни билдирган эди: „Сонлар назарияси соҳасида янада янги ютуқларга эришиш учун, ақл-заковати бўйича Чебишев олдий одамлардан қандай юқори турган бўлса, Чебишевдан шундай даражада юқори турадиган одам туғилишини кутиш мумкин“. Буюк немис математиги Ландау (1877—1938) ўзининг туб сонлар тақсимотига бағишлаган бир асарида Чебишев тўғрисида шундай деб ёзади: „Евклиддан сўнг „Туб сонлар масалалари“ни ҳал этиш учун тўғри йўл танланган ва муҳим муваффақиятларни қўлга киритган олим бу Чебишевдир“.

П. Л. Чебишевнинг ютуқлари туб сонлар тақсимотининг асимптотик қонунини исботлаш учун, яъни $\lim\limits_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}}$ нинг мавжудлигини кўрсатиш учун етарли эмас эди. Лекин у шу масалани ҳал қилишга уринган: агар лимит мавжуд бўлса, у 1 га тенг бўлишини исбот ҳосил бўлади. (3) кўринишдаги ҳар бир сон a ва b сонларнинг умумий карралиси бўлади.

a ва b сонларнинг ЭКУК ни топиш учун (3) тенгликда $t=1$ деб олиш кифоя. Демак,

$$[a;\ b]=\frac{a\cdot b}{d} \tag{4}$$

ва

$$m=[a;\ b]\cdot t\ (t\in Z). \tag{5}$$

Иккита соннинг ЭКУК қуйидаги хоссаларга эга:

1°. Иккита соннинг ЭКУК шу сонлар кўпайтмасини уларнинг ЭКУБ га бўлган нисбатига тенг.

2°. a ва b сонларга бўлинадиган ҳар бир m сони шу сонларнинг ЭКУК га ҳам бўлинади ((5) га асосан).

3°. $\frac{[a;\ b]}{a}$ ва $\frac{[a;\ b]}{b}$ сонлар ўзаро тубдир, чунки улар мос равишда $\frac{b}{d}=b_1$ ва $\frac{a}{d}=a_1$ бўлганидан b_1 ва a_1 лар ўзаро туб.

4°. Ўзаро туб сонларнинг ЭКУК шу сонлар кўпайтмасига тенг, яъни $((a;\ b)=1)\Rightarrow([a;\ b]=a\cdot b)$.

5°. Агар $k>0$ бўлса, у ҳолда $[ak;\ bk]=k[a;\ b]$.

6°. Агар a/k ва b/k бўлса, у ҳолда $\left[\frac{a}{k};\ \frac{b}{k}\right]=\frac{[a;\ b]}{k}$.

Иккитадан ортиқ сонларнинг ЭКУК ни топиш масаласи иккита соннинг ЭКУК ни топишдаги каби ҳал этилади. n та $a_1, a_2, \ldots, a_n$ сонларнинг ЭКУК ни $[a_1;\ a_2;\ldots;a_n]$ кўринишда белгилайлик.

Теорема. *Ихтиёрий a, b, c натурал сонлар учун $[a;\ b;\ c]=[[a;\ b];\ c]$ тенглик ўринли бўлади.*

Исботи. $[a;\ b;\ c]=m$, $[a;\ b]=m_1$, $[m_1;\ c]=m_2$ белгилашларни киритамиз. Белгилашларга асосан, m_2/m_1, m_2/c бўлади. Бу муносабатлардан m_2/a, m_2/b, m_2/c муносабатлар ҳосил бўлади, яъни m_2 сон a, b, c сонларнинг бўлинувчиси бўлади, шунинг учун

$$m_2/m \tag{6}$$

муносабат ўринли.

Иккинчидан, m/a, m/b ва m/m_1 бўлгани учун

$$m/m_2 \tag{7}$$

муносабат ўринли. (6) ва (7) муносабатларга асосан $m_2=m$ бўлади.

Фараз қилайлик

$$a_1,\ a_2,\ \ldots,\ a_n$$

натурал сонлар қатори берилган бўлиб, $[a_1; a_2]=m_2$, $[m_2; a_3]=m_3, \ldots, [m_{n-1}, a_n]=m_n$ бўлсин ЭКУК нинг 2-хоссасига асосан a_1 ва a_2 га бўлинадиган ҳар бир сон уларнинг ЭКУК га ҳам бўлинади. Бошқача айтганда a_1 ва a_2 нинг умумий карралилари шу сонлар ЭКУК ларининг умумий карралилари билан устма-уст тушади, яъни

$$[a_1, a_2, \ldots, a_n]=[m_2, a_3, a_4, \ldots, a_n]=$$
$$=[m_3, a_4, a_5, \ldots, a_n]=\ldots=[m_{n-1}, a_n]=m_n$$

бўлгани учун $[a_1; a_2; \ldots; a_n]=m_n$ бўлади.

Натижа. Жуфтлама ўзаро туб сонларнинг ЭКУК шу сонлар кўпайтмасига тенг, яъни $[a_1, a_2, \ldots, a_n]=$ $=a_1 \cdot a_2 \cdots a_n$.

7-§. Узлуксиз касрлар

4-§ даги (1) тенгликлар системасининг биринчи тенглигини b га, иккинчисини r_2 га, учинчисини r_3 га ва ҳоказо энг охиргисини r_n га бўлиб, қуйидагиларга эга бўламиз:

$$\frac{a}{b}=q_1+\frac{r_2}{b}=q_1+\frac{1}{\frac{b}{r_2}},$$

$$\frac{b}{r_2}=q_2+\frac{r_3}{r_2}=q_2+\frac{1}{\frac{r_2}{r_3}},$$

. . . .

$$\frac{r_{n-1}}{r_n}=q_n.$$

Бундан

$$\frac{a}{b}=q_1+\frac{1}{\frac{b}{r_2}}=q_1+\frac{1}{q_2+\frac{r_3}{r_2}}=q_1+\frac{1}{q_2+\frac{1}{q_3+\frac{r_4}{r_3}}}=\ldots$$

тенгликлар ҳосил бўлади. Агар $\frac{r_i}{r_{i+1}}=q_{i+1}+\frac{r_{i+2}}{r_{i+1}}$ нисбатларни 4-§ даги (1) системадан топиб, юқоридаги ифодаларга қўйсак, $\frac{a}{b}$ нисбат қуйидаги кўринишни олади:

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cdots + \cfrac{1}{q_n}}}} \qquad (1)$$

$\frac{a}{b}$ нисбатнинг (1) кўриниши уни узлуксиз (чекли занжирли) касрга ёйиш дейилади. Занжирли каср қуйидагича ҳам белгиланади:

$$\frac{a}{b} = (q_1, q_2, q_3, \ldots, q_n)$$

ёки

$$\frac{a}{b} = q_1 + \frac{1}{q_2} + \frac{1}{q_3} + \ldots + \frac{1}{q_n}.$$

$q_2, q_3, \ldots, q_n$ лар занжирли касрнинг *тўлиқсиз бўлинмалари* дейилиб, улар натурал сонлар ва $q_n > 1$ бўлади. q_1 эса $\frac{a}{b}$ рационал соннинг *бутун қисми* дейилади

Қуйидаги уч ҳол бўлиши мумкин:

а) $a > b$ бўлса, $q_1 > 0$ бўлади;

б) $a < b$ бўлганда эса, $q_1 = 0$ бўлади;

в) $a < 0$ бўлса, $\frac{a}{b}$ нисбатни $\frac{a}{b} = -k + \frac{r_1}{r}$ $(k > 0)$ кўринишда ёзиб оламиз. Бу ерда $\frac{r_1}{r}$ тўғри мусбат каср бўлади. Натижада қуйидаги ёйилма ҳосил бўлади:

$$\frac{a}{b} = -k + \frac{r_1}{r} = (\overline{-k, q_2, q_3, \ldots, q_n}).$$

1-эслатма. Ҳар қандай бутун сонни бир бўлакли узлуксиз каср деб қараш мумкин.

Масалан, $5 = (5)$. $\frac{1}{a}$ шаклдаги $(a > 1)$ каср эса икки бўлакли узлуксиз каср деб қаралади.

2-эслатма. Агар энг сўнгги q_n қисмий махражга ҳеч қандай шарт қўйилмаган бўлса, $\frac{a}{b}$ рационал соннинг узлуксиз касрга ёйилмаси иккита ҳар хил кўринишга эга бўлади.

1. Агар $q_n > 1$ бўлса, у ҳолда $\frac{a}{b} = (\overline{q_1, q_2, \ldots, q_n})$ ёйилма ягона бўлади.

2. Фараз қилайлик $q_n > 1$ шарти қўйилмаган бўлсин. У ҳолда $q_n = (q_n - 1) + \frac{1}{1}$ тенгликка асосан $\overline{(q_1, q_2, \ldots, q_n)} = \overline{(q_1, q_2, \ldots, q_n - 1, 1)}$ ни ёзиш мумкин. Бу ерда ўнг томондаги ёйилмада бўлаклар сони чапдаги ёйилма бўлаклари сонидан биттага ортиқдир.

Мисол. $$\frac{95}{42} = 2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{2}}}} = (2,\ 3,\ 1,\ 4,\ 2).$$

Энди соннинг бутун ва каср қисми устида тўхталиб ўтайлик. Қолдиқли бўлиш теоремасига асосан ҳар қандай $a \in \mathbf{Z}$ ва $m \in N$ лар учун

$$a = mq + r \quad (0 \leqslant r < m) \tag{2}$$

каби боғланиш мавжуд ва ягона эди. (2) нинг иккала қисмини m га бўлиб қуйидагини ҳосил қиламиз:

$$\frac{a}{m} = q + \frac{r}{m} \quad \left(0 \leqslant \frac{r}{m} < 1\right). \tag{3}$$

Демак, q сони $\frac{a}{m}$ каср сондан кичик бўлган бутун сонларнинг энг каттаси экан. Бу усулда аниқланган q сон $\frac{a}{m}$ рационал соннинг бутун қисми дейилади ва у $q = \left[\frac{a}{m}\right]$ каби белгиланади. $\frac{a}{m} - q = \frac{r}{m}$ сон эса $\frac{a}{m}$ рационал соннинг каср қисми дейилиб, у $\frac{r}{m} = \left\{\frac{a}{m}\right\}$ каби белгиланади.

Мисоллар. $\left[\frac{147}{17}\right] = 8$, $\left\{\frac{147}{17}\right\} = \frac{11}{17}$,

$$\left\{-\frac{79}{17}\right\} = \frac{6}{17},\ \{-7{,}25\} = 0{,}75,\ \{4\} = 0,\ \left\{\frac{13}{17}\right\} = \frac{13}{17}.$$

α соннинг бутун қисмини (3) қоида асосида аниқлаш *соннинг бутун қисмини ажратиш* деб аталади.

Агар α ҳақиқий сон бўлса, унинг бутун қисми қуйидаги шарт асосида ажратилади:

$$k \leqslant \alpha < k + 1, \text{ бу ерда } k = [\alpha].$$

Ҳар қандай α ҳақиқий сон учун қуйидаги тасдиқлар рост:

$$\{\alpha\} = \alpha - [\alpha],\ \alpha = [\alpha] + \{\alpha\},\quad 0 \leqslant \{\alpha\} < 1.$$

8-§. Муносиб касрлар ва уларнинг хоссалари

Биз юқорида ҳар бир рационал сонни чекли занжирли касрга ёйиш мумкинлигини кўриб ўтдик. Энди масалани аксинча қўямиз. Ҳар бир чекли занжирли каср бирор рационал сонни ифодалайдими? Бу масалани ҳал этишда $\frac{a}{b}$ рационал сонга *муносиб касрлар* деб аталувчи

$$\delta_1 = q_1,\quad \delta_2 = q_1 + \frac{1}{q_2},\quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}},\ \ldots \tag{1}$$

касрлар муҳим аҳамиятга эга.

$$\delta_n = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}}$$

бўлгани учун бу муносиб каср $\frac{a}{b}$ рационал соннинг ўзи бўлади, δ_k муносиб касрдан δ_{k+1} муносиб касрга ўтиш учун δ_k даги q_k ни $q_k + \frac{1}{q_{k+1}}$ билан алмаштириш лозимлиги (1) дан кўриниб турибди. Исталган муносиб касрни ҳисоблаш учун $\mathscr{P}_0 = 1$, $\mathscr{P}_1 = q_1$, $Q_0 = 0$, $Q_1 = 1$ белгилашлар киритиб қуйидагиларни ёзамиз:

$$\delta_1 = \frac{q_1}{1} = \frac{\mathscr{P}_1}{Q_1},$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_2q_1 + 1}{q_2} = \frac{q_2q_1 + 1}{q_2\cdot 1 + 0} = \frac{q_2\mathscr{P}_1 + \mathscr{P}_0}{q_2Q_1 + Q_0} = \frac{\mathscr{P}_2}{Q_2},$$

$$\delta_3 = \frac{\left(q_2 + \frac{1}{q_3}\right)\mathscr{P}_1 + \mathscr{P}_0}{\left(q_2 + \frac{1}{q_3}\right)Q_1 + Q_0} = \frac{q_3(q_2\mathscr{P}_1 + \mathscr{P}_0) + \mathscr{P}_1}{q_3(q_2Q_1 + Q_0) + Q_1} =$$

$$= \frac{q_3\mathscr{P}_2 + \mathscr{P}_1}{q_3Q_2 + Q_1} = \frac{\mathscr{P}_3}{Q_3}.$$

Математик индукция принципига асосан қуйидагини ёза оламиз:

$$\delta_k = \frac{\mathscr{P}_k}{Q_k} = \frac{q_k\mathscr{P}_{k-1} + \mathscr{P}_{k-2}}{q_kQ_{k-1} + Q_{k-2}} \tag{2}$$

Бу ерда

$$\begin{cases} \mathscr{P}_k = q_k\mathscr{P}_{k-1} + \mathscr{P}_{k-2}, \\ Q_k = q_kQ_{k-1} + Q_{k-2}. \end{cases} \qquad (3)$$

(2) боғланиш δ_k муносиб касрни ҳисоблаш учун хизмат қиладиган рекуррент формуладир. Қуйидаги схема исталган $\mathscr{P}_k$ ва Q_k сонларни ҳисоблашга имкон беради:

		q_1	q_2	q_3	$\cdots$	q_k	$\cdots$	q_n
$\mathscr{P}_k$	$\mathscr{P}_0 = 1$	$\mathscr{P}_1 = q_1$	$\mathscr{P}_2$	$\mathscr{P}_3$	$\cdots$	$\mathscr{P}_k$	$\cdots$	$\mathscr{P}_n$
Q_k	$Q_0 = 0$	$Q_1 = 1$	Q_2	Q_3	$\cdots$	Q_k	$\cdots$	Q_n

1-мисол. (2, 3, 1, 4, 2) га мос рационал сонни топинг.

		2	3	1	4	2
$\mathscr{P}_k$	1	2	$\mathscr{P}_2 = 3\cdot 2 + 1 = 7$	$\mathscr{P}_3 = 1\cdot 7 + 2 = 9$	$\mathscr{P}_4 = 4\cdot 9 + 7 = 43$	$\mathscr{P}_5 = 2\cdot 43 + 9 = 95$
Q_k	0	1	$Q_2 = 3\cdot 1 + 0 = 3$	$Q_3 = 1\cdot 3 + 1 = 4$	$Q_4 = 4\cdot 4 + 3 = 19$	$Q_5 = 2\cdot 19 + 4 = 42$

Демак, берилган узлуксиз каср учун

$$\delta_1 = \frac{2}{1},\ \delta_2 = \frac{7}{3},\ \delta_3 = \frac{9}{4},\ \delta_4 = \frac{43}{19},\ \delta_5 = \frac{95}{42}.$$

Бундан (2, 3, 1, 4, 2) $= \frac{95}{42}$.

Энди муносиб касрларнииг баъзи хоссаларини кўрсатиб ўтамиз.

1°. Фараз қилайлик, $\Delta_k = \mathscr{P}_kQ_{k-1} - \mathscr{P}_{k-1}Q_k$ бўлсин. (3) тенгликлардан фойдаланиб, Δ_k ни қуйидагича ёзамиз:

$$\Delta_k = \mathscr{P}_kQ_{k-1} - \mathscr{P}_{k-1}Q_k = (q_k\mathscr{P}_{k-1} + \mathscr{P}_{k-2})Q_{k-1} -$$
$$- \mathscr{P}_{k-1}(q_kQ_{k-1} + Q_{k-2}) =$$
$$= -(\mathscr{P}_{k-1}Q_{k-2} - \mathscr{P}_{k-2}Q_{k-1}) = -\Delta_{k-1}.$$

Демак, $\Delta_k = -\Delta_{k-1} = \Delta_{k-2} = -\Delta_{k-3} = \ldots$, яъни барча Δ_i лар бир хил абсолют қийматга эга. Лекин,

$$\Delta_1 = \mathscr{P}_1Q_0 - Q_1\mathscr{P}_0 = q_1\cdot 0 - 1\cdot 1 = -1, \quad \Delta_1 = (-1)^1$$

бўлганидан ҳар қандай $1 \leqslant k < n$ учун

$$\Delta\mathscr{P}_k = {}_kQ_{k-1} - Q_k\mathscr{P}_{k-1} = (-1)^k, \ \Delta_k = (-1)^k. \qquad (4)$$

(4) формула $(\mathscr{P}_k; Q_k) = 1$ эканини кўрсатади. Ҳақиқатан, $(\mathscr{P}_k; Q_k) = d > 1$ десак, (4) нинг ўнг томони ҳам d га бўлиниши лозим эди. Лекин $(-1)^k$ сони $d > 1$ га бўлинмайди.

$$2°. \ \delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_kQ_{k-1}}. \qquad (5)$$

Ҳақиқатан, $\delta_k - \delta_{k-1} = \frac{\mathscr{P}_k}{Q_k} - \frac{\mathscr{P}_{k-1}}{Q_{k-1}} =$

$$= \frac{\mathscr{P}_kQ_{k-1} - \mathscr{P}_{k-1}Q_k}{Q_kQ_{k-1}} = \frac{(-1)^k}{Q_kQ_{k-1}}.$$

Бундан

$$|\delta_k - \delta_{k-1}| = \frac{1}{Q_kQ_{k-1}}. \qquad (6)$$

Эслатма. Ҳар қандай иррационал сонни ҳам узлуксиз касрларга ёйиш мумкин. Бирор α иррационал сон берилган булиб, $[\alpha] = q_1$ бўлсин. У ҳолда α сонни $\alpha = q_1 + \frac{1}{\alpha_1}$ кўринишда ёзиш мумкин. Бу ерда $\alpha_1 > 1$ ва иррационал сон бўлгани учун $[\alpha_1] = q_2$ деймиз. Натижада $\alpha_1 = q_2 + \frac{1}{\alpha_2}$ бўлиб, α_2 иррационал сон. У ҳолда $\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{\alpha_2}}$ бўлади. Бу жараённи $\alpha_2, \alpha_3, \ldots$ иррационал сонларга нисбатан такрорлаб,

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdot_{\cdot_{\cdot_{+ \cfrac{1}{q_n + \cdot_{\cdot_{\cdot}}}}}}}}$$

га эга бўламиз. Шундай қилиб иррационал соннинг узлуксиз касрга ёйилмаси чексиз кўп булакка эга экан, деган хулосага келамиз.

2-мисол. $\sqrt{28}$ ни узлуксиз касрга ёйинг.

$\sqrt{28} = 5 + \frac{1}{\alpha}$, $\alpha > 1$ бўлгани учун

$$\alpha = \frac{1}{\sqrt{28} - 5} = \frac{\sqrt{28} + 5}{3} = 3 + \frac{1}{\beta}, \ \beta > 1,$$

$$\beta=\frac{3}{\sqrt{28}-4}=\frac{3(\sqrt{28}+4)}{12}=\frac{\sqrt{28}+4}{4}=2+\frac{1}{\gamma},$$

$$\gamma=\frac{4}{\sqrt{28}-4}=\frac{\sqrt{38}+4}{3}=3+\frac{1}{\nu},$$

$$\nu=\frac{3}{\sqrt{28}-5}=\sqrt{28}+5,\ \nu=10+\frac{1}{\mu},\ \mu=\frac{1}{\sqrt{28}-5}=\alpha\cdot$$

Бу ерда α каср такрорланади, яъни даврий каср ҳосил бўлди. Натижада қуйидагига эга бўлдик:

$$\sqrt{28}=5+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{10+\cfrac{1}{3+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{10+\ldots}}}}}}}}$$

9-§. Туб сонлар

1-таъриф. Фақат иккита турли натурал бўлувчига эга бўлган натурал сон *туб сон* дейилади.

2-таъриф. Натурал бўлувчилари сони иккитадан ортиқ бўлган натурал сон *мураккаб сон* дейилади.

Бу таърифларга кўра 2, 3, 5, 7, 11, 13,... сонлар туб сонлар, 4, 6, 8, 9, 10, 12, ... сонлар эса мураккаб сонлардир. 1 сони туб сон ҳам, мураккаб сон ҳам эмас. Чунки 1 сони туб ва мураккаб сонлар таърифларини қаноатлантирмайди. Туб ва мураккаб сонларнинг баъзи хоссаларини қуйида қараб чиқамиз.

1°. $a>1$ мураккаб соннинг 1 дан фарқли энг кичик натурал бўлувчиси p бўлса, у ҳолда p туб сон бўлади.

Ҳақиқатан, акс ҳолда p бирор q $(1<q<p)$ бўлувчига эга бўлиб, $p/q\wedge a/q\Rightarrow a/q$ ва $q<p$ бўлар эди. Бу эса p нинг энг кичик бўлувчи эканига зиддир.

2°. Ҳар қандай натурал a ва p туб сони ё ўзаро туб, ёки a сон p га бўлинади, яъни $(\forall a,\ p\in N,\ p-$ туб сон$)\Rightarrow((a;\ p)=1,\ \vee a/p)$.

Исботи. p туб соннинг натурал бўлувчилари 1 ва p дир. Шунинг учун $(a; p)=p$ ёки 1. Агар $(a, p)=p$ бўлса 4-§ даги 1-теоремага асосан a/p. Агар $(a, p)=1$ бўлса, a ва p лар ўзаро туб.

3°. Агар ab кўпайтма бирор p туб сонга бўлинса, у ҳолда кўпайтувчилардан камида биттаси p га бўлинади, яъни

$$(\forall a, b\in N)\ (ab/p)\Rightarrow(a/p\vee b/p).$$

Ҳақиқатан, агар $a\not/ p$, яъни a сон p га бўлинмаса, у ҳолда 2-хоссага асосан $(a; p)=1$ бўлади. У ҳолда 5-§ даги теоремага асосан b/p.

Бу хоссани математик индукция принципидан фойдаланиб кўпайтувчиларнинг сони уч ёки ундан ортиқ бўлган кўпайтмага нисбатан ҳам қўллаш мумкин. Бундан қуйидаги натижа келиб чиқади.

Натижа. Агар кўпайтма p га бўлиниб, унинг барча кўпайтувчилари туб сонлардан иборат бўлса, кўпайтувчилардан бири p га тенг бўлади.

10-§. Арифметиканинг асосий теоремаси

1-теорема. *Бирдан бошқа ихтиёрий натурал сон туб сон ёки туб сонлар кўпайтмаси шаклида ёзилади, агар бу кўпайтмада кўпайтувчиларнинг ўрни эътиборга олинмаса, у ҳолда бу кўпайтма ягона бўлади.*

Исботи. $a>1$ бўлганда ушбу

$$a=p_1\cdot p_2\cdots p_n\ (p_i\text{—туб сон, } i=\overline{1,n};\ n\geqslant 1)\qquad(1)$$

кўпайтманинг мавжудлиги ва ягоналигини кўрсатайлик.

Ихтиёрий натурал сонни (1) кўринишда ёзиш бу сонни *туб сонлар кўпайтмасига ёйиш* дейилади.

Маълумки, ҳар қандай натурал соннинг 1 дан фарқли энг кичик натурал бўлувчиси туб сон бўлади (9-§, 1-хосса). Демак,

$$a=p_1\cdot a_1\qquad(2)$$

тенглик ўринли. Агар (2) да a_1 туб сон бўлса, у ҳолда теорема исбот бўлади Агар a_1 мураккаб сон бўлса, унинг p_2 туб бўлувчиси бўлиб, у ҳолда $a_1=p_2\cdot a_2$ бўлади. Бундан $a=p_1\cdot p_2\cdot a_2$ тенглик ҳосил бўлади. Агар a_2 туб сон бўлса, у ҳолда теорема исбот бўлади.

Агар a_2 мураккаб сон бўлса, бу жараённи $a_n=1$ бўлган ҳолгача давом эттирамиз, яъни қуйидаги тенгликларни ҳосил қиламиз:

$$\begin{aligned} a &= p_1\cdot a_1, \\ a_1 &= p_2\cdot a_2, \\ a_2 &= p_3\cdot a_3, \\ &\cdots\cdots\cdots \\ a_{n-1} &= p_n\cdot a_n \end{aligned}$$

Бу тенгликларни ҳадлаб кўпайтирсак, $a=p_1\cdot p_2\cdots p_n$ (1) ёйилма ҳосил бўлади Энди (1) ёйилманинг ягоналигини исбот қилайлик. Фараз қилайлик a сон (1) дан бошқа

$$a=q_1\cdot q_2\cdots q_s \tag{3}$$

ёйилма а ҳам эга бўлсин. (1) ва (3) ларнинг чап томонларининг тенглигидан

$$p_1\cdot p_2\cdots p_n=q_1\cdot q_2\cdots q_s \tag{4}$$

тенгликни ҳосил қиламиз. (4) нинг чап томонидаги ҳар бир p_i $(i=\overline{1,n})$ туб сон, унинг ўнг томонини бўлади. Лекин барча q_j $(j=\overline{1,s})$ лар ҳам туб сондир.

9-§ даги натижага асосан q_j ларнинг бири бирорта p_i га ва аксинча p_k ларнинг бири бирорта q_l га тенг бўлади. Демак, (1) ва (4) ёйилмаларнинг ҳар бири тенг сондаги туб кўпайтувчилардан тузилган.

Улардаги бирор туб сон ёйилманинг маълум томонида иккинчи томондагига нисбатан кўпроқ қатнашсин десак, у ҳолда (4) ёйилманинг иккала томонини p га бир неча марта қисқартириб, унинг бир томонида p мавжуд, иккинчи томонида эса p қатнашмаган ҳолга келамиз. Бунинг бўлиши мумкин эмас. Демак, (1) ёйилма ягона экан.

(1) ёйилмада баъзи бир кўпайтувчилар ўзаро тенг бўлиши ҳам мумкин. Фараз қилайлик, (1) да p_1 туб сон α_1 марта, p_2 туб сон α_2 марта ва ҳ. к. p_k туб сон α_k марта қатнашсин. У ҳолда (1) ёйилма

$$a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_k^{\alpha_k} \tag{5}$$

кўринишда бўлади. (5) кўриниш a сонининг *каноник ёйилмаси* дейилади.

11 §. Туб сонлар тўплами

Теорема *Туб сонлар тўплами чексиздир.*

Қуйида бу теореманинг икки хил исботини берамиз.

1 Теореманинг Евклид исботини келтирайлик. Фараз қилайлик туб сонлар сони чекли бўлиб, улар ўсиш тартибида жойлашган $p_1, p_2, \ldots, p_n$ кўринишдаги туб сонлардан иборат бўлсин.

$$Q_n = p_1 \cdot p_2 \cdots p_n + 1$$

сонни оламиз. Бу соннинг энг кичик бўлувчисини p_m десак, у албатта туб сон бўлади (туб сонларнинг 1-хоссаси) ва у p_i ларнинг биронтасига ҳам тенг бўлмайди. p_m сон p_i $(i = \overline{1,n})$ туб сонларнинг бирортасига ҳам тенг бўла олмайди, акс ҳолда Q_n ва $p_1 \cdot p_2 \cdots p_n$ ларнинг p_m га бўлинишидан 1 нинг ҳам p_m га бўлиниши келиб чиқар эди. Бу эса мумкин эмас. Демак, фаразимиз нотўғри экан.

Q_n туб сон бўлса, у ҳолда $Q_n > p_i$ $(= \overline{1,n})$ ва янги туб сон ҳосил бўлади. Бу ҳолда ҳам фаразимиз нотўғри. Демак, туб сонларнинг сони чексиз, яъни туб сонлар тўплами чексиздир.

Евклиддан сўнг туб сонлар назариясини ривожлантиришда энг катта муваффақиятларни қўлга киритган математик Эйлердир. Эйлер математик анализ ёрдамида туб сонлар сони чексиз кўп эканини кўрсатди. Шундан сўнг сонлар назариясида янги соҳа—аналитик сонлар назарияси юзага келди.

2. Теореманинг Эйлер исботини келтирайлик. Чексиз камаювчи геометрик прогрессия ҳадлари йиғиндисини топиш формуласига асосан ихтиёрий p туб сон учун қуйидаги тенгликни ёза оламиз:

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \ldots \qquad (1)$$

Теоремани тескаридан исбот қилайлик. Туб сонлар сони чекли бўлиб, улар $p_1, p_2, \ldots, p_k$ бўлсин. Ҳар бир p_i $(i = \overline{1,k})$ учун (1) каби қуйидаги қаторни ёзиб оламиз:

$$\frac{1}{1-\frac{1}{p_i}} = 1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \ldots \quad (i = \overline{1,k}). \qquad (2)$$

(2) нинг ўнг томони яқинлашувчи қатордан иборат ва

чекли сондаги яқинлашувчи қаторларни ҳадлаб кўпайтириш мумкин. Математик анализдан маълумки, кўпайтиришдан ҳосил бўлган қатор (юқоридаги тасдиқларда) яна яқинлашувчи бўлади. Натижада қуйидаги тенглик ҳосил бўлади:

$$\prod_{i=1}^{k}\frac{1}{1-\frac{1}{p_i}}=\sum_{\alpha_1,\alpha_2,\ldots,\alpha_k}\frac{1}{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}}. \qquad (3)$$

Бу ерда йиғинди манфиймас $\alpha_1, \alpha_2, \ldots, \alpha_k$ ларнинг мумкин бўлган барча комбинациялари бўйича тузилади. (3) нинг ўнг томонидаги махраж мураккаб соннинг каноник кўринишидан иборат бўлиб, $p_1, p_2, \ldots, p_k$ лар эса унинг туб бўлувчиларидир. Фаразимиз бўйича p_i лардан бошқа туб сон йўқ. Демак, (3) нинг ўнг томонидаги махраж умуман барча натурал сонларни ифодалайди. Ҳосил бўлган яқинлашувчи қатор ҳадларини махражнинг ўсиши тартибида жойлаштириб (булар барчаси мусбат бўлгани учун шундай қила оламиз), $\sum\limits_{m=1}^{\infty}\frac{1}{m}$ каби гармоник қаторга эга бўламиз:

$$\sum_{m=1}^{\infty}\frac{1}{m}=\prod_{i=1}^{k}\frac{1}{1-\frac{1}{p_i}} \qquad (4)$$

(4) га асосан, гармоник қатор яқинлашувчи бўлиб, унинг йиғиндиси чекли $\prod\limits_{i=1}^{k}\frac{1}{1-\frac{1}{p_i}}$ сонга тенг. Лекин математик анализдан маълумки гармоник қатор узоқлашувчи эди. Биз қарама-қаршиликка учрадик Бу эса туб сонлар сони чекли деган фаразимизнинг нотўғри эканини кўрсатади.

12-§. Эратосфен ғалвири

Туб сонлар тўпламининг чексизлигини, биз юқорида кўрсатганимиздек, Эйлер ва Евклид исбот қилган. Агар берилган a сон етарлича катта бўлса, унинг туб ёки мураккаб эканини аниқлаш муҳим масалалардан биридир. Бу масалани ҳал этишда қуйидаги теореманинг моҳияти катта.

Теорема. *a натурал соннинг энг кичик туб бўлувчиси $\sqrt{a}$ дан катта эмас.*

Исботи. Фараз қилайлик p_1 туб сон a нинг энг кичик бўлувчиси бўлсин. У ҳолда $a=p_1 \cdot a_1$ бўлиб, $a_1 \geqslant p_1$ бўлади. Бундан $a=p_1 a_1 \geqslant p_1^2$ ёки $p_1 \leqslant \sqrt{a}$.

Бу теорема n дан катта бўлмаган туб сонларнинг жадвалини тузишга имкон беради. Бу усулни бириичи бўлиб грек математиги ва астрономи Эратосфен (эрамизгача 276—193 йиллар) кўрсатган. Бу усул қуйидагичадир: n гача бўлган барча натурал сонлар ёзиб борилади. Бу қаторда туб сонлар таърифини қаноатлантирувчи биринчи сон, яъни 2 ажратиб олинади. Сўнгра бу қатордаги 2 дан бошқа 2 га бўлинадиган сонлар ўчирилади. 2 дан бошқа биринчи ўчмаган сон 3 дир. Кейин 3 ни қолдириб, 3 га бўлинадиган сонларни ўчирамиз. 3 туб сон. Бу икки жараёндан сўнг ўчмай қолган биринчи сон (2 ва 3 дан ташқари) 5 дир. 5 ни қолдириб, 5 га бўлинадиган сонларни ўчирамиз. 5 туб сон. Бу жараённи $\sqrt{n}$ дан катта бўлмаган p туб сонгача давом эттириб p га бўлинадиган сонларни ўчирамиз. Натижада ўчирилмай қолган сонлар n дан катта бўлмаган туб сонлар бўлади. Бундай усул билан танлаб олинган туб сонлар жадвали „Эратосфен ғалвири“ номи билан маълумдир. Ўз усулини Эратосфен дастлаб қуйидагича ишлатган.

У n гача бўлган барча сонларни мум билан қопланган тахтачага ёзиб чиққан. Натижада тахтача ғалвирга ўхшаб қолган. Тахтачадаги тешилмай қолган ўринлардаги сонлар туб сонлардир. Эратосфен ўз усули билан минггача бўлган туб сонлар жадвалини тузган. Ҳозирги вақтда электрон ҳисоблаш машиналари ёрдамида исталган сонгача бўлган туб сонлар жадвалини тузиш мумкин.

Мисол. 2 дан 100 гача бўлган натурал сонлар орасидаги туб сонлар жадвалини тузинг.

Бунинг учун 2 дан 100 гача бўлган сонларни кетма-кет ёзиб чиқамиз.

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100.

Дастлаб 2 сонини олиб, кетма-кетликдаги 2 дан бошқа барча жуфт сонларни ўчирамиз. У ҳолда қуйидаги кетма-кетлик ҳосил бўлади:

2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99.

Энди мазкур кетма-кетликдан 3 нинг ўзидан бошқа унга бўлинадиган сонларни ўчирамиз. Натижада, ушбу

2, 3, 5, 7, 9, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97

кетма-кетликка эга бўламиз. Юқоридаги мулоҳазаларни 5 га нисбатан бажарсак,

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 91, 97

кетма-кетлик келиб чиқади. Ва ниҳоят сўнгги кетма-кетликда 7 нинг ўзидан бошқа унга бўлинадиган сонларни ўчирсак,

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 91, 97

кетма-кетликни ҳосил қиламиз. Бу кетма-кетликнинг барча элементлари туб сонлардан иборат экани ўз-ўзидан маълум. Демак, 100 гача бўлган натурал сонлар орасида 26 та туб сон бор экан.

13-§. Сонли функциялар. Натурал сон натурал бўлувчилари сони ва йиғиндиси

1-таъриф. Аниқланиш соҳаси ё қийматлар соҳаси, ёки ҳар иккаласи ҳам бутун сонлар тўплами бўлган функция *сонли функция* дейилади.

1. Берилган n натурал соннинг натурал бўлувчилари сонини $\tau(n)$ орқали белгилайлик Маълумки, (10-§, (5)) ҳар қандай $n>1$ натурал сонни

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad (1)$$

шаклда ёзиш мумкин эди. (1) шаклдаги соннинг барча натурал бўлувчилари

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \qquad (2)$$

кўринишга эга бўлади, бу ерда

$$0 \leqslant \beta_1 \leqslant \alpha, \quad 0 \leqslant \beta_2 \leqslant \alpha_2, \ldots, 0 \leqslant \beta_k \leqslant \alpha_k. \tag{3}$$

n соннинг барча бўлувчиларини топиш учун (2) даги β_i ларнинг мумкин бўлган барча қийматларини қараб чиқиш керак. Ҳар бир β_i, (3) га асосан, $\alpha_i + 1$ та қиймат қабул қилади

β_i ларнинг ҳар хил қийматларига мос келувчи қийматлар сони $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ га тенг. Демак, $\tau(n) = (\alpha_1 + 1\ (\alpha_2 + 1) \cdots (\alpha_k + 1)$.

1-мисол. $n = 504$ нинг натурал бўлувчилари сонини топинг.

$504 = 2^3 \cdot 3^2 \cdot 7$ бўлгани учун $\tau(504) = \tau(2^3 \cdot 3^2 \cdot 7) = (3 + 1)(2 + 1)\ 1 + 1)$, $\tau(504) = 24$ эканини топамиз.

2. Биз олдинги бандда n сонининг барча натурал бўлувчилари сонини ифодаловчи функцияни топдик. Энди шу натурал бўлувчиларнинг йиғинди и қайси формула орқали берилишини текширамиз.

n сонининг барча натурал бўлувчиларининг йиғиндисини $\sigma(n)$ ёки $\sum\limits_{|d} d$ орқали белгилайлик.

Қуйидаги кўпайтмани қарайлик:

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdots$$
$$\cdots (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k}) = \sum_{\beta_1, \beta_2, \ldots, \beta_k} p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}. \tag{4}$$

Бу ерда ҳар бир β_i $(i = \overline{1,k})$ бир-бирига боғлиқсиз равишда 0 дан α_i гача қийматларни қабул қилади. Геометрик прогрессия ҳадлари йиғиндисини топиш формуласидан фойдаланиб (4) йиғиндисини қуйидагича ёзамиз:

$$\sum_{\beta_1, \beta_2, \ldots, \beta_k} p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \tag{5}$$

Иккинчи томондан (5) нинг чап томонидаги ҳар бир $p_i^{\beta_i}$ $(i = \overline{1,k},\ 0 \leqslant \beta_i \leqslant \alpha_i)$ n соннинг бўлувчисидир. n сонинг ҳар бир бўлувчиси $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}$ кўринишда бўлади. Демак, (5) тенглик n сонининг натурал бўлувчилари йиғиндисини ифодаловчи формула экан, яъни

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

5°. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

Биз бу хоссани исбот қилиб ўтирмасдан ундан амалий машғулотларда фойдаланишнинг баъзи бир томонларини кўрсатиб ўтамиз.

а) $p \equiv 8m \pm 1$ шаклдаги туб сон бўлсин У ҳолда

$$\frac{p^2-1}{8}=\frac{(8m\pm1)^2-1}{8}=8m^2\pm 2m\equiv 0 \pmod 2$$

бўлгани учун $\left(\frac{2}{p}\right)=1$.

б) $p=8m\pm3$ шаклдаги туб сон бўлса, $\frac{p^2-1}{8}=$ $=\frac{(8m\pm3)^2-1}{8}=8m^2\pm6m+1\equiv1 \pmod 2$ бўлади. Демак, $p=8m\pm3$ шаклдаги сон бўлса, 2 сон p модуль бўйича квадратик чегирмамас бўлади, яъни $\left(\frac{2}{p}\right)=-1$.

6°. Ўзаролик қонуни.

Агар p ва q лар ҳар хил тоқ туб сонлар бўлса,

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{5}$$

тенглик ўринли бўлади.

Бу хоссани ҳам исбот қилмасдан унинг амалий машғулотларда қўлланилишини кўрсатамиз. Бунинг учун (5) нинг иккала қисмини $\left(\frac{p}{q}\right)$ га кўпайтирамиз:

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right), \tag{6}$$

бу ерда $\left(\frac{p^2}{q}\right)=1$.

(6) тенгликка асосан, p ёки q ларнинг камида биттаси $4m+1$ шаклдаги сон бўлса, $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=1$ бўлиб, $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$ ҳосил бўлади.

Агар p ва q ларнинг ҳар бири $4m+3$ шаклдаги туб сон бўлса, у ҳолда (-1) нинг даражаси тоқ сон бўлиб,

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$$

бўлади.

2-мисол. 504 нинг барча натурал бўлувчилари йиғиндисини топинг.

$$\sigma(504)=\sigma(2^3\cdot3^2\cdot7)=\frac{2^{3+1}-1}{2-1}\cdot\frac{2^{2+1}-1}{3-1}\cdot\frac{7^{1+1}-1}{7-1}=1560,$$

$$\sigma(504)=1560.$$

14-§ Туб сонларнинг тақсимот қонуни

Биз 11-§ да туб сонлар сонининг чексиз кўп эканини кўрсатиб ўтган эдик. Лекин туб сонларнинг натурал сонлар қаторида қандай жойланишини ўрганиш муҳим масалалардан биридир. Маълумки, (12-§ га қаранг) 1 дан 100 гача натурал сонлар орасида 26 та туб сон бор. 101 дан 200 гача натурал сонлар орасидаги туб сонлар сони 21 та эканига бевосита текшириш йўли билан ишонч ҳосил қилиш мумкин. Қуйидаги жадвални тузамиз:

...дан	...гача	туб сонлар сони
1	100	26
101	200	21
201	300	16
301	400	16
401	500	17
501	600	14
601	700	16
701	800	14
801	900	15
901	1000	14
1001	2000	168
2001	3000	127
3001	4000	120
4001	5000	119
5001	6000	114
6001	7000	117
7001	8000	107
8001	9000	110
9001	10000	112

Бу жадвалга асосан туб сонлар турли 100 ликлар орасида турлича жойлашган. Иккита натурал сон орасида жойлашган туб сонлар сонини бирор аналитик усулда ифодалаш, яъни уларнинг сонини ифодаловчи формулани топиш масаласи билан жуда кўп математиклар шуғулланган. Улар орасида биринчи бўлиб Гаусс империк (тажриба) усулида берилган x сонидан катта бўлмаган туб сонлар сони

$$\int_{2}^{x} \frac{1}{\ln x} dx$$

функция ёрдамида аниқланишини кўрсатиб берди. Биз бу масалага кейинроқ алоҳида тўхталамиз. Ҳозир эса сонлар назариясининг ривожланиши учун муҳим аҳамиятга эга бўлган баъзи масалалар устида тўхталиб ўтмокчимиз.

1. Камида битта туб сонни ўз ичига олувчи интервални аниқлаш. 1845 йилда француз математиги Бертран Жозеф Луи (1822—1900) $(2a>7)$ бўлганда a ва $2a-2$ сонлар орасида камида битта туб сон ётади деган фикрни айтган. Бу тасдиқни 1852 йилда П. Л. Чебишев исбот қилди. Дебов эса n^2 ва $(n+1)^2$ сонлар орасида камида иккита туб сон мавжуд деган фикрни айтган.

2. Эгизак туб сонлар. Натурал сонлар қаторида шундай p ва $p+2$ сонлар топиладики, уларнинг иккаласи ҳам туб сон бўлади. Бундай сонлар одатда *эгизак туб сонлар* деб юритилади.

Масалан, 11, 13; 17, 19; 29, 31; 41, 43; 59, 61. Бундай эгизак туб сони чексиз кўп деган фикр мавжуд, лекин бу фикр ҳозиргача исбот этилмаган.

3. Гольдбах проблемаси. Христиан Гольдбах (1690—1764) бутун математик ҳаётини Россияда ўтказган олим, Петербург Фанлар Академиясининг аъзоси. У 1742 йилда Эйлерга ёзган хатида қуйидаги тасдиқни келтирган эди: 6 дан кичик бўлмаган ҳар қандай натурал сонни учта туб сон йиғиндиси шаклида ифодалаш мумкин. Бу проблемани ҳал этиш учун математиклар қарийб 200 йил уриндилар. Уни 1937 йилда рус математиги академик Иван Матвеевич Виноградов ҳал қилди, яъни шундай p_0 тоқ сон мавжудки ундан катта бўлган ҳар қандай тоқ сон учта туб сон йиғиндисидан иборат бўлади.

4. Туб сонлардан иборат қийматларни қабул қилувчи сонли функциялар. Сонлар назарияси билан шуғулланган деярли ҳар бир математик $x \in N$ бўлганда қийматлари фақатгина туб сондан иборат бўлган $f(x)$ функцияни излаш билан шуғулланган. Леонард Эйлер (1707—1783) Петербург Академия-

сининг академиги (Швейцариялик) $x\in\{1, 2,\ldots,15\}$ бўлганда $f(x)=x^2+x+17$, $x\in\{0, 1, 2,\ldots,40\}$ бўлса, $f(x)=x^2-x+41$ функцияларнинг сонли қийматлари фақатгина туб сонлардан иборат эканини кўрсатди. Бундай хоссага $x\in\{0, 1, 2,\ldots,28\}$ бўлганда $2x^2+29$; $x\in\{0, 1, 2,\ldots,39\}$ бўлганда x^2+x+41 ва $x\in\{0, 1, 2,\ldots,79\}$ бўлганда $x^2-79x+1601$ каби функциялар ҳам эга бўлади. Бундай функцияларни кўплаб тузиш мумкин. Лекин, умуман олганда, биринчи бўлиб Х. Гольдбах томонидан айтилган қуйидаги мулоҳаза ўринли (исботсиз келтирамиз).

Теорема. *Агар $x\in N$ бўлса, барча қийматлари фақатгина туб сонлардан иборат бўлган бирорта ҳам $f(x)$ функция мавжуд эмас.*

5. Мукаммал сонлар.

1-таъриф. n натурал соннинг ўзидан бошқа натурал бўлувчилари унинг *хос бўлувчилари* дейилади.

n учун хос бўлувчиларнинг йиғиндиси $\sigma(n)-n$ га тенглиги ўз-ўзидан равшан.

2-таъриф. Агар a ва b натурал сонлар учун a нинг хос бўлувчилари йиғиндиси b га ва b нинг хос бўлувчилари йиғиндиси a га тенг бўлса, бундай сонлар *дўст сонлар* дейилади.

Таърифга асосан, қуйидагиларни ёза оламиз:

$$((\sigma(a)-a=b)\wedge(\sigma(b)-b=a))\Rightarrow(\sigma(a)=\sigma(b)=a+b).$$

1-мисол. 220 ва 284 сонлар дўст сонлардир.

3-таъриф. Агар n натурал соннинг хос бўлувчилари йиғиндиси n соннинг ўзига тенг бўлса, n *мукаммал сон* дейилади.

Бу таърифни қисқача қуйидагича ёзиш ҳам мумкин:

$$(n\in N)\ (\sigma(n)-n=n)\wedge(\sigma(n)=2n)$$

рост бўлса, n мукаммал сон дейилади.

2-мисол. $6=1+2+3$, $28=1+2+4+7+14$ бўлгани учун 6 ва 28 сонлар мукаммал сонлардир.

Электрон ҳисоблаш машиналари ёрдамида ҳозирги кунда бир қанча мукаммал сонлар топилган.

15-§. Туб сонлар тақсимотининг асимптотик қонуни

14-§ да биз туб сонларнинг турли юзликдаги турлича тақсимотини кўриб ўтган эдик. Туб сонлар натурал сонларнинг у ёки бу оралиғида қандай жойланишини текшириш билан жуда кўп математиклар шуғулланган. Бу масалани янада аниқроқ баён этамиз.

x дан ортиқ бўлмаган туб сонлар сонини $\pi(x)$ орқали белгилайлик. XIX аср математиклари $\pi(x)$ функциянинг ҳеч бўлмаганда тақрибий аналитик кўринишини топиш учун жуда катта иш қилишган. Улар агар $\pi(x)$ нинг аниқ кўринишини топиш мумкин бўлмаса, у ҳолда унга x нинг барча қийматларида жўда яқин бўлган $f(x)$ функцияни топиш масаласини ҳал қилишга уринишган. Бунинг учун $f(x)$ функцияни шундай танлаш лозим эдики, $\pi(x)$ ва $f(x)$ ларнинг нисбати, яъни $\frac{\pi(x)}{f(x)}$ нисбат x нинг етарлича катта қийматларида 1 га интилиши талаб қилинган, яъни

$$\lim_{x\to\infty}\frac{\pi(x)}{f(x)}=1 \qquad (1)$$

ўринли бўлиши лозим эди. (1) тенгликни қаноатлантирувчи функциялар одатда *асимптотик эквивалент функциялар* деб юритилади ва у қисқача $\pi(x)\sim f(x)$ кўринишда белгиланади.

Лимитнинг таърифига асосан (1) ни $\pi(x)=f(x)+R(x)$ каби ёзиш мумкин. Бу ерда $R(x)$ функция $x\to\infty$ да $f(x)$ га нисбатан чексиз кичик миқдордир, яъни $\lim\limits_{x\to\infty}\frac{R(x)}{f(x)}=0$ ўринли.

1808 йилда француз математики Андриен Мари Лежандр (1752—1833) туб сонлар жадвалини текшириб, $\pi(x)$ нинг тақрибий имперsection формуласини топди. Унинг фикрича x нинг етарлича катта қийматларида $\pi(x)$ функция тақрибан $\frac{x}{\ln x-\beta}$ га тенг экан, бу ерда $\beta=1{,}08366$ ўзгармас сон. Шу даврнинг ўзида немис математиги Гаусс $\pi(x)$ учун $\int\limits_2^x\frac{1}{\ln t}dt$ функцияни олиш мумкин деб айтди. Бу интегрални элементар функциялар орқали ифодалаб бўлмайди. Шунинг учун *интеграли логарифм* деб аталувчи қуйидаги интеграл билан алмаштирилади:

$$\mathrm{Li}\,x=\lim_{\eta\to+0}\left(\int\limits_0^{1-\eta}+\int\limits_{1+\eta}^{x}\right)\frac{1}{\ln t}\,dt.$$

Бу теореманинг моҳияти шундаки, унинг биринчи қисми (1) ёйилма коэффициентларини ҳисоблашнинг рекуррент боғланишини беради. (1) ёйилманинг ягоналиги эса, ихтиёрий натурал сонни m лик саноқ системасида ёйиш учун асос бўлади. m лик саноқ системасида ёзилган сон қисқача $(a_r a_{r-1} \cdots a_1 a_0)_m$ каби белгиланади. Бу ёзувда ҳар бир рақам ўзининг тутган ўрни билан характерланади. Масалан, 222 да 2 дан учта учрайди. Лекин улардан энг ўнг томонда жойлашгани 2 та бирликни, ўнгдан иккинчиси иккита ўнликни, яъни йигирмани, учинчиси эса иккита юзликни билдиради (бу ерда ўнлик саноқ системаси кўзда тутиляпти). Агар биз m лик система билан иш кўрганимизда эди юқоридаги учта иккилар мос равишда ўнгдан 2, $2m$, $2m^2$ ни билдирар эди.

2-таъриф. Бирор m асосга нисбатан қурилган саноқ системаси *позицион саноқ системаси* дейилади.

Позицион бўлмаган саноқ системалари ҳам бор. Масалан, рим рақамлари билан иш кўриладиган система позицион бўлмаган саноқ системасидир.

Ҳозирги вақтда электрон ҳисоблаш машиналари асосан иккилик саноқ системаси асосида ишлайди. $m=2$ бўлганда $M=\{0, 1\}$ бўлгани учун бу саноқ системасида ҳар қандай сон фақатгина иккита 0 ва 1 рақамлари ёрдамида ёзилади. Масалан, 119 сонини олсак, унинг $m=2$ нинг даражалари бўйича ёйилмаси, $119 = 1 \cdot 2^0 + 1 \cdot 2 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6$ бўлиб, бу соннинг кўриниши $(1110111)_2$ каби бўлади.

3-таъриф. Бирор m асосли саноқ системаси бўйича ёзилган сон *систематик сон* дейилади.

18-§. Систематик сонлар устида амаллар

Систематик сонлар устида баъзи бир амалларни бажаришдан олдин, уларни қуйидагича ёзиб оламиз:

$$a = a_0 m^0 + a_1 m^1 + \cdots + a_r m^r + 0 \cdot m^{r+1} + 0 \cdot m^{r+2} + \ldots = \sum_{r=0}^{\infty} a_r m^r. \qquad (1)$$

Демак, бирор $i>r$ номердан бошлаб барча a_i лар нолга тенг экан. Шундан сўнг исталган натурал сонни бир қанча кўринишда ёзиш мумкин. Масалан, $111 = 0111 = 00111 = \ldots$ сонларнинг барчаси иккилик саноқ системасида ўзаро тенгдир.

Энди m лик саноқ системасида берилган иккита сонни қўшиш амали устида тўхтаб ўтамиз.

$$a = \sum_{i=0}^{\infty} a_i m^i, \ 0 \leqslant a_i < m,$$

$$b = \sum_{i=0}^{\infty} b_i m^i, \ 0 \leqslant b_i < m \tag{2}$$

бўлганда $c = a + b$ ни m лик саноқ системасида қандай кўринишда ёзиш мумкинлиги билан шуғулланамиз.

$$a = a_0 + a_1 m + a_2 m^2 + \cdots + a_r m^r + \cdots \tag{3}$$

$$b = b_0 + b_1 m + b_2 m^2 + \cdots + b_r m^r + \cdots \tag{4}$$

бўлгани учун

$$c = a_0 + b_0 + (a_1 + b_1)m + (a_2 + b_2)m^2 + \cdots + (a_i + b_i)m^i + \\ + (a_{i+1} + b_{i+1})m^{i+1} + \cdots + (a_r + b_r)m^r + \cdots \tag{5}$$

бўлади. Иккинчидан ҳар қандай c сонниng m нинг даражали бўйича

$$c = c_0 + c_1 m + c_1 m^2 + \cdots + c_r m^r + \cdots \tag{6}$$

каби ёйилмаси мавжуд ва ягонадир.

Биз битта c сон учун (5) ва (6) каби икки хил ёйилмага эга бўлдик. Бу икки ёйилма умуман устма-уст тушмай қолиши мумкин. Бошқача қилиб айтганда, қуйидаги икки ҳол юз беради:

1. $(a_i + b_i < m) \Rightarrow (a_i + b_i = c_i)$ $(i = 0, 1, 2, \ldots)$

2. $a_k + b_k \geqslant m$ бўлса, $c_k = d_k$ бўлади, бу ерда d_k сон $a_k + b_k$ ни m га бўлгандаги қолдик. Демак, иккинчи ҳолда c_k коэффициент учун $a_k + b_k$ йиғиндини m га бўлгандаги қолдиқ олинар экан. Бундай ҳолда $a_k + b_k = d_k + m$ тенглик ўринли бўлганидан (5) ёйилмадаги k ва $k+1$ ҳадлар қуйидагича бўлади:

$$(a_k + b_k)m^k + (a_{k+1} + b_{k+1})m^{k+1} =$$
$$= (d_k + m)m^k + (a_{k+1} + b_{k+1})m^{k+1} =$$
$$= d_k m^k + (a_{k+1} + b_{k+1} + 1)m^{k+1}.$$

Лекин a_{k+1} ва b_{k+1} лар c_{k+1} коэффициентни аниқловчи қўшилувчилардир. Бошқача айтганда, $a_k + b_k \geqslant m$ бўлса, $k+1$ коэффициентга 1 бирлик қўшилар экан. Юқоридагиларни умумлаштириб, қуйидаги теоремани ёзамиз:

Теорема. *m лик саноқ системасида (3) ва (4) ёйилмалар орқали берилган a ва b сонлар*

$$a + b = c = c_0 + c_1 m + c_2 m^2 + \cdots + c_r m^r + \cdots \tag{7}$$

йиғиндисининг коэффициентлари қуйидаги рекуррент формулалар ёрдамида аниқланади: агар $a_0 + b_0 < m$ *бўлса,* $\varepsilon_0 = 0$ *акс ҳолда* $\varepsilon_0 = 1$ *деймиз.* $\varepsilon_i = 0 \Longleftrightarrow a_{i-1} + b_{i-1} + \varepsilon_{i-1} < m$, $\varepsilon_i = 1 \Longleftrightarrow a_{i-1} + b_{i-1} + \varepsilon_{i-1} \geqslant m$ *шартларда* ε_i *ни аниқлаймиз.*

Агар

$$\varepsilon_i + a_i + b_i < m \tag{8}$$

бўлса, у ҳолда $c_i = a_i + b_i + \varepsilon_i$ *бўлади; агар*

$$\varepsilon_i + a_i + b_i \geqslant m \tag{9}$$

бўлса, у ҳолда $c_i = d_i$, $a_i + b_i + \varepsilon_i - m$ $(i = \overline{0, +\infty})$ *бўлади.*

Исботни i нинг индукцияси асосида олиб борамиз. $i = 0$ да (5) ёйилмадаги $a_0 + b_0$ учун қуйидаги иккита ҳол бўлади:

а) $a_0 + b_0 < m$ бўлса, у ҳолда $c_0 = a_0 + b_0$ бўлади;

б) $a_0 + b_0 \geqslant m$ бўлса, $a_0 + b_0 = c_0 + m$ бўлгани учун c_1 коэффициентга 1 қўшилади. Демак, $i = 0$ да (8) ва (9) шартлар ўринли. Фараз қилайлик бу рекуррент формулалар c_{i-1} коэффициент учун ўринли бўлсин. У ҳолда i коэффициент $a_i + b_i + \varepsilon_i$ га тенг бўлиб, бу ерда $a_{i-1} + b_{i-1} + \varepsilon_{i-1} < m$ ёки $a_{i-1} + b_{i-1} + \varepsilon_{i-1} \geqslant m$ шартга қараб $\varepsilon_i = 0$ ёки $\varepsilon_i = 1$ бўлади.

1-мисол. Бешлик саноқ системасида $(342)_5$ ва $(134)_5$ сонларнинг йиғиндисини топинг.

Амалий машғулотларда бирор m асос бўйича сонни қўшиш учун жадвал тузиб олинади. $m = 5$ бўлганда бу жадвалнинг кўриниши қуйидагича бўлади:

„+“	1	2	3	4
1	2	3	4	10
2	3	4	10	11
3	4	10	11	12
4	10	11	12	13

яъни $1+1 = 2$, $1+2 = 3$, $1+3 = 4$, $1+4 = 10$ $(0 + 1 \cdot 5)$, $3 + 1 = 4$, $3 + 2 = 10$, $3 + 3 = 11$ $(1 + 1 \cdot 5)$, $4 + 4 = 13$ (чунки $8_{10} = 3 \cdot 5^0 + 1 \cdot 5$). Демак, $(342)_5 + (134)_5 = (1031)_5$

Айириш амали бир хонали сонларни айириш, қўшиш жадвалига асосан бажарилади. Кўп хонали сонларни айириш эса $m=10$ бўлган ҳолдаги сонларни айиришга ўхшайди. Агар камаювчининг бирор хона бирлиги айрилувчининг тегишли хона бирлигидан кичик бўлса, камаювчидан битта чапдаги хонанинг бир бирлиги, яъни m ундан ўнгда жойлашган хона рақамига қўшилиб, сўнгра айириш амали бажарилади. Масалан, $(5321)_7-(2651)_7$ ни бажаринг. Аввало ўнгдаги биринчи хонадаги сонлар тенг бўлгани учун $1-1=0$ Энди иккинчи хонасига ўтамиз. Лекин $2<5$. Шунинг учун ўнгдан учинчи хонанинг асосга тенг бўлган битта бирлигини иккинчи хонадаги сонга қўшамиз $(7+2=9)$. Шундан сўнг $9-5=4$. Энди учинчи хонада 2 қолди, лекин $2<6$ бўлгани учун ўнгдан тўртинчи хонанинг битта бирлигини учинчи хона сонига қўшамиз $(7+2==9)$. Шундан сўнг $9-6=3$ ва ниҳоят $4-2=2$. Демак, $(5321)_7-(2651)_7=(2340)_7$. Ҳақиқатан, $(2651)_7+$ $+(2340)_7=(5321)_7$.

Кўпайтириш. Ихтиёрий a натурал сонни m лик саноқ системасида (1) каби ёйилмасига ёйиб олгач, уларни кўпайтириш ўрта мактабда учраган кўпҳадни кўпҳадга кўпайтиришдаги каби бажарилади.

Агар коэффициентларни кўпайтириш пайтида кўпайтма саноқ системасининг асосидан катта бўлса, у ҳолда кўпайтмани асосга бўлиб кўпайтма ўрнига қолдиқ олинади ва у бўлинма шу сондан кейин келадиган хона рақамига қўшилади.

Кўпайтириш амали ҳам асосан жадвал ёрдамида бажарилади. Масалан, асос $g=6$ бўлганда кўпайтириш жадвали қуйидагича бўлади:

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	10	12	14
3	0	3	10	13	20	23
4	0	4	12	20	24	32
5	0	5	14	23	32	41

Бу жадвалдан фойдаланиб $(352)_6 \cdot (245)_6$ кўпайтмани топайлик:

$$\begin{array}{r}
\times\begin{array}{r}(352)_6\\(245)_6\end{array}\\
\hline
(3124)_6\\
(2332)_6\\
(1144)_6\\
\hline
(145244)_6
\end{array}$$

Исталган системада ёзилган сонларни бўлиш, худди $m = 10$ бўлган ҳолдаги бўлишдек бажарилади.

2-мисол. $m=6$ бўлганда $(145244)_6$ ни $(245)_6$ га бўлинг:

$$\begin{array}{r|l}
-\,145244_6 & 245_6\\
\cline{2-2}
1223_6 & 352_6\\
\cline{1-1}
-\,2254_6 & \\
2201_6 & \\
\cline{1-1}
-\,534_6 & \\
534_6 & \\
\cline{1-1}
0_6 &
\end{array}$$

19-§. Бир саноқ системасидан бошқа саноқ системасига ўтиш

Асоси m га тенг бўлган саноқ системасидан доимо бошқа бирор g асосга эга бўлган саноқ системасига ўтиш мумкин. Бунинг учун m системали сонни аввало ўнлик саноқ системасидаги сонга айлантириб, сўнгра охирги сонни g системадаги сонга айлантириш керак. Ўнлик системада берилган сондан g лик системага ($g < 10$) ўтиш учун берилган сонни g нинг даражалари бўйича ёзиб оламиз. Шу ёйилмадаги коэффициентлар (даражаларининг пасайиши тартибида олинади) g асосга нисбатан ёзилган соннинг рақамлари бўлади.

1-мисол. 3287 ни еттилик системасида ёзинг.

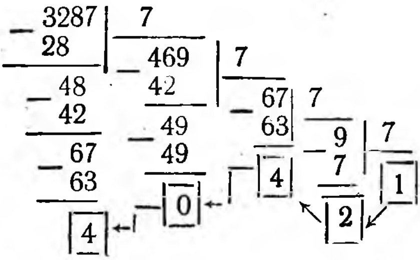
Бунинг учун қуйидаги кетма-кетликни бажарамиз:

$$\begin{aligned}
3287 &= 7\cdot 469 + 4,\\
469 &= 7\cdot 67 + 0,\\
67 &= 7\cdot 9 + 4,\\
9 &= 7\cdot 1 + 2.
\end{aligned}$$

Демак, 3287 сон қуйидаги ёйилмага эга экан:

$$3287 = 7(7\cdot 67) + 4 = 7^2\cdot 67 + 4 = 7^2(7\cdot 9 + 4) + 4 =$$
$$= 7^3\cdot 9 + 7^2\cdot 4 + 4 = 7^3(7 + 2) + 7^2\cdot 4 + 4 =$$
$$= 7^4\cdot 1 + 7^3\cdot 2 + 4\cdot 7^2 + 0\cdot 7 + 4\cdot 7^0 = (12404)_7,$$
$$3287 = (12404)_7.$$

Юқоридаги кетма-кет бўлишни қуйидаги усулда ҳам бажариш мумкин:



Охирги бўлинма ва қолдиқлар (энг сўнгги қолдиқдан бошлаб) дан тузилган сон биз излаган сон бўлади.

Энди бирор *m* асосли системадан ўнлик системага ўтиш масаласи билан шуғулланамиз ($m<10$)

$$N_m = (a_r a_{r-1} \cdots a_1 a_0)_m$$

берилган бўлсин. Ўнгдан биринчи хона бирлиги ўнли системада ҳам ўзгармайди, яъни $a_0 = a_0$. Ўнгдан иккинчи хонанинг бир бирлиги ўнлик системада $a_1 m$ қийматга, учинчи хона бирлиги $a_2 m^2$ ва ҳоказо, $r+1$ хона бирлиги эса $a_r m^r$ қийматга эга. Демак, N_m сон ўнлик системада қуйидаги ёйилма бўйича ёзилади:

$$N_m = a_0 + a_1 m + a_2 m^2 + \cdots + a_r m^r.$$

Юқоридагиларга асосан, қуйидаги қоидани ёза оламиз: *m* асос бўйича берилган сонни ўнлик системада ёзиш учун ўнгдан иккинчи рақамдан бошлаб ҳар бир сонни шу рақам жойлашган хона қийматига кўпайтириб, уларнинг йиғиндисини топиш керак.

2-мисол. $(25302)_7$ сонни ўнлик системада ёзинг.

Биринчи хонадаги сон $7^0 = 1$. Демак, $2\cdot 1 = 2$. Иккинчи хонадаги сон 7. Демак, $0\cdot 7 = 0$. Учинчи хонадаги сон $7^2 = 49$. Демак, $49\cdot 3 = 147$. Тўртинчи хонадаги сон $7^3 = 343$. Демак, $343\cdot 5 = 1715$. Бешинчи хонадаги сон $7^4 = 2401$. Демак, $2401\cdot 2 = 4802$. У ҳолда $2 + 0 + 147 + 1715 + 4802 = 6666$.

Амалий машғулотларда m асосли системадан ўнлик системага ўтиш учун юқоридаги жараён тескарисидан бажарилади, яъни энг юқори хона бирлиги (мисолимизда 2) асос бирлиги (мисолимизда 7) га кўпайтирилиб, кейинги хона бирлигига қўшилади, яъни $7 \cdot 2 + 5 = 19$. Ҳосил бўлган натижа яна асосга кўпайтирилиб, натижа кейинги хона бирлигига қўшилади ва ҳоказо. Шу усулни ҳозирги мисолга қўллайлик:

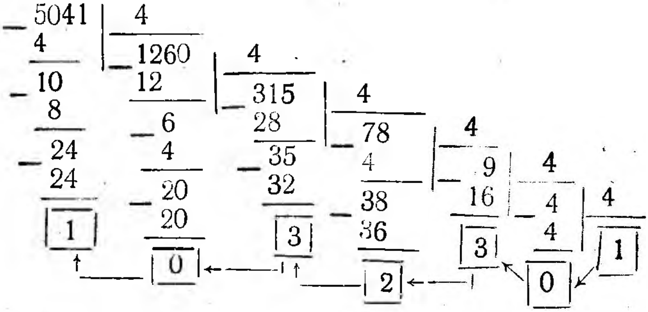
$$
\begin{aligned}
7 \cdot 2 + 5 &= 19,\\
19 \cdot 7 + 3 &= 136,\\
136 \cdot 7 + 0 &= 952,\\
952 \cdot 7 + 2 &= 6666.
\end{aligned}
$$

3-мисол. $(35201)_6 = x_4$ ни бажаринг. Бошқача айтганда олтилик системасидан тўртлик системага ўтинг.

Аввало юқорида айтиб ўтганимиздек, олтилик системадан ўнлик системага ўтамиз:

$$
\begin{aligned}
3 \cdot 6 + 5 &= 23,\\
23 \cdot 6 + 2 &= 140,\\
140 \cdot 6 + 0 &= 840,\\
840 \cdot 6 + 1 &= 5041.
\end{aligned}
$$

Энди ўнлик системадан тўртлик системага ўтамиз:



Демак, $5041 = (1032301)_4$ бўлиб, $(35201)_6 = (1032301)_4$ бўлади. Агар берилган асос 10 дан катта бўлса, у ҳолда янги символлар киритишга тўғри келади. Масалан, қаралаётган асосни 16 десак, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 рақамлардан ташқари (10), (11), (12), (13), (14), (15) символлар (рақамлар) киритилиб, 0 дан 16 ғача бўлган сонларни 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, (10), (11), (12), (13), (14), (15), 10 каби ёза оламиз.

4-мисол. $(12573)_{10}$ ни 16 асос бўйича ёзинг.

Ечиш.

$$12573 = 16\cdot 785 + 13,$$
$$785 = 16\cdot 49 + 1,$$
$$49 = 16\cdot 3 + 1.$$

Бу ерда 13 сони берилган 10 асосдан катта бўлганлиги учун уни (13) символ билан алмаштириб, қуйидагига эга бўламиз:

$$(12573)_{10} = (311\,(13))_{16}.$$

Фараз қилайлик бирор g асосга нисбатан ёзилган m сони берилган бўлсин. Биздан шу m сонини 10 лик системадан фойдаланмасдан туриб, исталган h асосга нисбатан ёзиш талаб этилсин.

Аввало h сонни g асосда ёзамиз, кейин қуйидаги амалларни бажарамиз:

а) m сонни h га бўлиб, қолдиқ b_0 сонни топамиз, яъни $m = hq_1 + b_0$ дан b_0 топилади;

б) b_0 қолдиқни h асосга ўтказамиз ва b_0 сон h асосли соннинг охирги рақами бўлади;

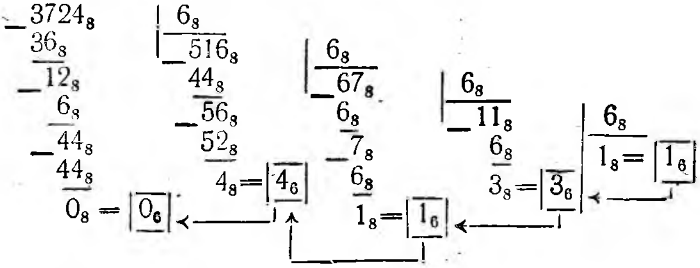
в) q_1 сонни h сонга бўлиб, қолдиқ b_1 сонни топамиз, яъни $q_1 = hq_2 + b_1$ дан b_1 топилади ва уни h асосга ўтказамиз;

г) бу жараённи бўлинма q_l сон h дан кичик бўлганча давом эттирамиз;

д) m соннинг h асосли биринчи рақами, охирги бўлинма q_l бўлади. Ундан кейинги рақам охирги қолдиқ ва шу тартибда қолдиқлар олинади. Бу сонлар m сонининг h асосли рақамлари бўлади.

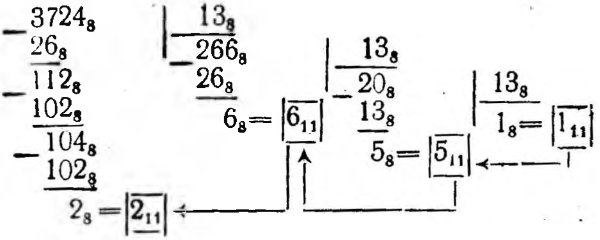
5-мисол. 3724_8 сонни олтилик ва ўнбирлик системаларида ёзинг.

а) $g = 8$ ва $h = 6$; $h = 6 = 6_8$.



Демак, $3724_8 = 13140_6$.

б) $g = 8$ ва $h = 11$; $h = 11 = 13_8$.



Демак, $2724_8 = 1562_{11}$.

Биз юқорида исталган бутун сонни $m > 1$ натурал асос бўйича ёзиш мумкинлигини кўрсатдик. Бу фикр исталган каср сон учун ҳам тўғри эканини баён қиламиз. Фараз қилайлик, бизга 1309,26 ўнли каср (10 асосга нисбатан) берилган бўлсин. Бу сонни 10 нинг даражалари бўйича қуйидагича ёзиб оламиз:

$$1309{,}26 = 1 \cdot 10^3 + 3 \cdot 10^2 + 0 \cdot 10^1 + 9 \cdot 10^0 + $$
$$+ 2 \cdot 10^{-1} + 6 \cdot 10^{-2}.$$

Агар қаралаётган каср бошқа асос бўйича берилган бўлса, у ҳолда уни ўнли асос орқали ёзиш мумкин.

Масалан, $(1254{,}7632)_8 = 1 \cdot 8^3 + 2 \cdot 8^2 + 5 \cdot 8^1 + + 4 \cdot 8^0 + 7 \cdot 8^{-1} + 6 \cdot 8^{-2} + 3 \cdot 8^{-3} + 2 \cdot 8^{-4}$ ёйилмада тегишли амаллар бажарилса, ҳосил бўлган сон 10 асосга нисбатан ёзилган бўлади.

Ўз-ўзидан маълумки каср сонларнинг барчаси ҳам чекли ўнли каср шаклида ёзилавермайди. Бу ҳол исталган саноқ системаси учун ҳам ўринли.

Лекин яна шундай ҳол юз бериши мумкинки, бир саноқ системасида чекли ёйилмага эга бўлган рационал сон бошқа саноқ системасида чексиз даврий касрга ёйилиши мумкин ва аксинча. Масалан, $\frac{1}{3}$ сони ўнлик системада 0,333. . . каби чексиз даврий ўнли касрга ёйилса, олтилик саноқ системада чекли бўлади, яъни $\left(\frac{1}{3}\right)_{10} = 0 \cdot 6 + 2 \cdot 6^{-1} = (0{,}2)_6$. Худди шундай $\left(\frac{1}{10}\right)_{10} = 0{,}1$ бўлгани ҳолда $\left(\frac{1}{10}\right)_{10} = (0{,}0333. . .)_6$ бўлади.

Умуман айтганда юқоридагиларга асосан исталган рационал M сонини m асос бўйича қуйидаги кўринишда ёзиш мумкин:

$$M_m = (a_k a_{k-1} \dots a_0,\ a_{-1} a_{-2} \dots a_{-s})_m.$$

Бунда $a_k, a_{k-1}, \dots, a_0$ лар M сонининг бутун қисмини, $a_{-1}, a_{-2}, \dots, a_{-s}$ лар эса унинг каср қисмини ифодалайди.

20-§. Арифметик прогрессияда туб сонлар

Қўлланмамизнинг 11-§ ида натурал сонлар тўпламида чексиз кўп туб сонлар мавжуд эканлигини кўрсатган эдик. Энди қуйидаги иккита арифметик прогрессияни қарайлик:

$$1,\ 4,\ 7,\ 10,\ 13,\ 16,\ 19,\ \dots$$
$$3,\ 7,\ 11,\ 15,\ 19,\ 23,\ 27,\ 31,\ \dots$$

Агар бу прогрессияларнинг ҳадларига эътибор берсак, уларнинг бир қанчаси туб сонлардан иборат эканлигини кўрамиз. Бир неча ҳадлари туб сонлар бўлган арифметик прогрессияларни доимо тузиш мумкин. Шунинг учун бизни $(a; d) = 1$ бўлганда $a,\ a+d,\ a+2d,\ \dots,\ a+nd,\ \dots$ прогрессиядаги туб сонларни топиш масаласи қизиқтиради. Бу масалани ҳал этиш учун бутун дунё олимлари узоқ вақт уринишди. Ниҳоят ўз замонасининг буюк математикларидан бири бўлган Лежен Дирихле (1805—1859) мазкур масалани тўла-тўкис ҳал қилади.

1-теорема (Дирихле теоремаси). *Агар $(a; d) = 1$ ва $n \in N$ бўлса, у ҳолда умумий ҳади $a + nd$ кўринишда бўлган прогрессияда чексиз кўп туб сонлар бўлади.*

Бу теоремани исботлаш учун математик анализ ва функциялар назариясининг мураккаб усулларидан фойдаланишга тўғри келгани туфайли биз уни исботлаб ўтирмасдан унинг қуйидаги баъзи бир махсус кўринишга эга бўлган прогрессияларини қараб ўтамиз:

2-теорема. $4n+1$ $(\forall n \in N)$ *кўринишдаги туб сонлар чаксиз кўп.*

1 дан катта ҳар қандай k натурал сон учун $k!$ жуфт сон бўлади. У ҳолда $(k!)^2 + 1$ тоқ сон бўлиб, унинг энг кичик бўлувчиси ҳам тоқ туб сондир. Бу тоқ туб сон ё $4n+1$, ёки $4n+3$ кўринишга эга бўлади, бу ерда n мусбат бутун сон.

Агар энг кичик туб бўлувчини p десак, $p > k$ бўлади. Акс ҳолда, яъни $p \leqslant k$ шартни қаноатлантирганда эди $(1 \cdot 2 \cdot 3 \cdot \ldots \cdot k)^2 + 1 = pt$ (t — мусбат бутун сон) тенгликда қавс ичидаги кўпайтувчилардан бири p га тенг бўлиб, бундан 1 нинг p га бўлиниши келиб чиқади. Бунинг бўлиши мумкин эмас, чунки p туб сон эди. Айтайлик $p = 4n + 3$ кўринишдаги туб сон бўлсин. У ҳолда $(k!)^2 = a$ десак, $(a^{2n+1} + 1) / a + 1 = ((k!)^{2(2n+1)} + 1)/(k!)^2 + 1$ келиб чиқади. Лекин $2(2n + 1) = 4n + 2 = (4n + 3) - 1 = p - 1$ бўлганидан ва $(k!)^2 + 1/p$ га кўра $(k!)^p + k!/p$ бажарилади.

Охирги муносабат $((k!)^p + k!)/p$ ўринли.эканини билдиради.

$((k!)^p - k!)/p$ муносабат ўринли. (Исботи 26- § даги Ферма теоремасидан келиб чиқади.) Демак, $(((k!)^p + k!)/p) \wedge ((k!)^p - k!)/p$ дан $((k!)^p + k!) - ((k!)^p - k!) = 2k!$ бўлиб, $2k!/p$ бўлади.

Охирги муносабатнинг бўлиши мумкин эмас, чунки $2k!$ жуфт сон бўлиб, p эса k дан катта тоқ туб сон. Демак, p туб сон $4n + 1$ кўрииишга эга экан. Шундай қилиб биз ҳар бир $n > 1$ натурал сонга битта $4n + 1$ кўринишдаги туб сон мос келишини кўрсатдик. Бу туб сон $(k!)^2 + 1$ нинг энг кичик туб бўлувчисидир. Лекин натурал сонлар тўплами чексиздир. Демак, $4n + 1$ кўринишдаги туб сонлар ҳам чексиз кўп экан.

3-теорема. $4n + 3$ $(\forall n \in N)$ *кўринишдаги прогрессияда туб сонлар чексиз кўп.*

Теоремани исботлашдан олдин қуйидаги иккита тасдиқни келтирамиз:

1) Ўз-ўзидан маълумки 2 дан катта бўлган ҳар бир туб сон тоқ сон бўлади. Акс ҳолда у иккига бўлинган бўларди.

2) Бундан ташқари $4n + 1$ шаклдаги ҳар қандай иккита соннинг кўпайтмаси яна $4n + 1$ кўринишда бўлади, чунки

$$(4a + 1)(4b + 1) = 16ab + 4a + 4b + 1 =$$
$$= 4(4ab + a + b) + 1 = 4k + 1,$$

бу ерда $k = 4ab + a + b$.

Энди 3-теоремани исботлайлик. Фараз қилайлик $4n + 3$ кўринишдаги туб сонлар сони n та бўлиб, улар $p_1, p_2, \ldots, p_n$ бўлсин. Бундай ҳолда қуйидаги ифодани тузамиз: $m = 4(p_1 \cdot p_2 \cdot \ldots \cdot p_n) - 1 = 4(p_1 \cdot p_2 \times$

$\times \ldots \cdot p_n - 1) + 3$. Бу ерда фақат қуйидаги икки ҳол юз бериши мумкин:

а) m — туб сон;

б) m — мураккаб сон.

а) m туб сон бўлса, уни q орқали белгилайлик. У ҳолда $4(\overline{p_1 \cdot p_2} \cdot \ldots \cdot p_n - 1) + 3$ бўлгани учун $q \neq p_i$ $(i = \overline{1, n})$ бўлади. Демак, $p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1 = n_1$ десак, у ҳолда $q = 4n_1 + 3$ кўринишдаги сон туб сон экан. Бу ҳолда фаразимиз нотўғри.

б) m мураккаб сон бўлсин. Бундай ҳолда $m = 4 \times (p_1 \cdot p_2 \cdot \ldots \cdot p_n - 1) + 3$ соннинг туб бўлувчиларининг барчаси ҳам $4n + 1$ шаклдаги сон бўлавермайди. Акс ҳолда m нинг ўзи ҳам $4n + 1$ кўринишдаги сон бўларди. Шунинг учун m нинг камида битта туб бўлувчиси $4n + 3$ кўринишда бўлиб, у $p_1, p_2, \ldots, p_n$ ларнинг бирортасига ҳам тенг эмас, акс ҳолда, $4(p_1 \times p_2 \cdot \ldots \cdot p_k \cdot \ldots \cdot p_n) - 1 = q_1 \cdot q_2 \cdot \ldots \cdot q_k \cdot \ldots \cdot qt$ бўлганда эди -1 сони $p_k = 4n_k + 3$ га бўлинган бўлар эди.

Шундай қилиб, биз икки ҳолда ҳам $p_1, p_2, \ldots, p_n$ лардан фарқли $4n + 3$ кўринишдаги туб сонни ҳосил қилдик. Бу эса фаразимизга зид.

Демак, $4n + 3$ кўринишдаги туб сонлар чексиз кўп экан.

Лемма. $6n + 5$ *кўринишдаги ҳар қандай натурал сон камида битта* $6m + 5$ *кўринишдаги туб бўлувчига эга бўлади.*

Исботи. 2 ва 3 га бўлинмайдиган ҳар қандай натурал сон ё $6t + 1$, ёки $6t + 5$ кўринишдаги сонга бўлинади. Иккинчи томондан $6n + 5$ нинг барча бўлувчилари фақатгина $6t + 1$ кўринишдаги сон бўлавермайди, акс ҳолда $(6t_1 + 1)(6t_2 + 1) = 36t_1 t_2 + 6t_1 + 6t_2 + 1 = 6(6t_1 \cdot t_2 + t_1 + t_2) + 1 = 6l + 1$ бўларди.

Демак, $6n + 5$ кўринишдаги натурал сон камида битта $6m + 5$ кўринишдаги туб бўлувчига эга экан.

4-теорема. $6n + 5$ *кўринишдаги туб сонлар чексиз кўп*

Исботи. Ихтиёрий k натурал сонни оламиз Агар $k = 1$ бўлса, $6 \cdot 1! - 1 = 5 = 6 \cdot 0 + 5$ тенглик бажарилади.

Фараз қилайлик $k > 1$ бўлсин. У ҳолда $k = 1 + m$ каби ёзиш мумкин бўлганидан $6k! - 1 = 6(1 + m)! - 1 = 6 - 6 + 6(1 + m)! - 1 = 6((1 + m)! - 1) + 5 = 6l + 5$, $6k! - 1 = 6l + 5$.

Демак, k ҳар қандай мусбат бутун сон бўлганда ҳам $6k! - 1$ доимо $6l + 5$ кўринишга эга экан. $6l + 5$ кўринишдаги сонларнинг 1 дан фарқли энг кичик мусбат бўлувчиси p туб сон эканлиги леммадан маълум. $6k! - 1 = 6(1 \cdot 2 \cdot 3 \cdot \ldots \cdot k) - 1 = pt$ бўлганидан (бу ерда t бутун мусбат сон) $p > k$ экани келиб чиқади.

Демак, ҳар бир k натурал сон учун k дан катта ва $6n + 5$ кўринишга эга p туб сон мавжуд экан. Натурал сонларнинг чексиз кўплигига биноан $6n + 5$ кўринишдаги туб сонлар ҳам чексиз кўп деган хулосага келамиз.

II боб.

ТАҚҚОСЛАМАЛАР НАЗАРИЯСИНИНГ АРИФМЕТИКАГА ТАТБИҚИ

21-§. Таққосламалар ва уларнинг хоссалари

Маълумки, қолдиқли бўлиниш ҳақидаги теоремага асосан ҳар қандай иккита a, $m>0$ бутун сон учун шундай ягона q_1 ва r сонлар топиладики, ушбу

$$a = mq_1 + r \tag{1}$$

тенглик бажарилади, бу ерда $0 \leqslant r < m$.

Бирор q_2 бутун сон учун

$$b = mq_2 + r \tag{2}$$

тенглик ўринли бўлган b сонни олайлик. (1) ва (2) тенгликлар a ва b сонларини m га бўлганда бир хил қолдиқ қолишини билдиради.

Таъриф. Агар иккита бутун a ва b сонни m натурал сонга бўлганда ҳосил бўлган қолдиқлар ўзаро тенг бўлса, у ҳолда a ва b сонлар m модуль бўйича *тенг қолдиқли сонлар* ёки m модуль бўйича *таққосланувчи сонлар* дейилади.

Агар a ва b сонлар m модуль бўйича таққосланса, у ҳолда қуйидагича белгиланади:

$$a \equiv b \pmod{m}. \tag{3}$$

(3) ни a ва b сонлари m модуль бўйича ўзаро таққосланади деб ўқилади. Энди (1) дан (2) ни айирайлик, у ҳолда $a - b = m(q_1 - q_2)$ ёки

$$a - b = mt \quad (t = q_1 - q_2) \tag{4}$$

тенглик ҳосил бўлади.

Юқоридаги мулоҳазаларни якунлаб қуйидаги хулосаларни чиқариш мумкин:

1. m модуль бўйича таққосланувчи сонларнинг айирмаси m сонига бўлинади.

2. Агар $a = b + mt$ бўлиб, b ни m га бўлгандаги қолдиқ r га тенг бўлса, a ни ҳам m га бўлгандаги қолдиқ r га тенг бўлади.

Ҳақиқатан, $b = mq_1 + r$ ни $a = b + mt$ га қўямиз. У ҳолда $a = mq_1 + r + mt = m(q_1 + t) + r = mq_2 + r$, яъни $a = mq_2 + r$ бўлади. Демак, $a = mq_2 + r$ бўлиб,

a ни m га бўлгандаги қолдиқ ҳам r га тенг экан. Шундай қилиб, $a \equiv b \pmod{m}$ таққосламани $a - b = mt$ ва $a = b + mt$ тенгликлар билан бир хил дейиш мумкин.

Агар $a = mq + r$ бўлса, у ҳолда уни $a \equiv r \pmod{m}$ каби ёзиш ҳам мумкин.

3. Агар a/m бўлса, у ҳолда $a \equiv 0 \pmod{m}$ бўлади.

Таққослама қуйидаги хоссаларга эга:

1°. Таққослама эквивалент бинар муносабат.

а) $a \equiv a \pmod{m}$, чунки $a - a = 0$ бўлиб, 0 сон m га бўлинади. Демак, таққослама рефлексивлик хоссасига эга.

б) $a \equiv b \pmod{m}$ ёки $a - b = mt$ бўлсин. Бундан $b - a = m(-t)$ тенгликни ёзиш мумкин. У ҳолда $b - a \equiv 0 \pmod{m}$ ёки $b \equiv a \pmod{m}$. Демак, таққослама симметриклик хоссасига эга

в) Агар $a \equiv b \pmod{m}$ ва $b \equiv c \pmod{m}$ бўлса, у ҳолда $a \equiv c \pmod{m}$ бўлади. Ҳақиқатан, $a = b + mt_1$, $b = c + mt_2$ тенгликларни ҳадлаб қўшсак, $a - c = mt$ тенглик ҳосил бўлади. Бунда $t = t_1 + t_2$. У ҳолда $a \equiv c \pmod{m}$ бўлади. Демак, таққослама транзитивлик хоссасига эга. Эквивалентлик ва бинар муносабатлари таърифига кўра, таққослама эквивалент бинар муносабат экан.

2°. Бир хил модулли таққосламаларни ҳадлаб қўшиш (айириш) мумкин. Ҳақиқатан ҳам,

$$\begin{gathered} a_1 \equiv b_1 \pmod{m}, \\ a_2 \equiv b_2 \pmod{m}, \\ \dots\dots\dots\dots \\ a_k \equiv b_k \pmod{m} \end{gathered}$$

бўлса, у ҳолда уларни

$$\begin{gathered} a_1 = b_1 + mt_1, \\ a_2 = b_2 + mt_2, \\ \dots\dots\dots \\ a_k = b_k + mt_k \end{gathered} \tag{5}$$

каби ёзиш мумкин. Бу тенгликларни ҳадлаб қўшиб (айириб)

$$a_1 \pm a_2 \pm \dots \pm a_k = b_1 \pm b_2 \pm \dots \pm b_k \pm m(t_1 + t_2 + \dots + t_k)$$

ёки

$$a_1 \pm a_2 \pm \dots \pm a_k = b_1 \pm b_2 \pm \dots \pm b_k \pm mt \tag{6}$$

тенгликка эга бўламиз. (6) ни

$$a_1 \pm a_2 \pm \dots \pm a_k \equiv b_1 \pm b_2 \pm \dots \pm b_k \pmod{m}$$

кўринишда ёзиш ҳам мумкин.

1-натижа. Таққосламанинг бир қисмидаги сонни иккинчи қисмига қарама-қарши ишора билан ўтказиш мумкин. Ҳақиқатан,

$$a + b \equiv c \pmod{m} \tag{7}$$

таққослама берилган бўлса, унга $-a \equiv -a \pmod{m}$ таққосламани қўшсак, $b \equiv c - a \pmod{m}$ таққослама ҳосил бўлади.

2-натижа. Таққосламанинг ихтиёрий қисмига модулга каррали сонни қўшиш мумкин. Ҳақиқатан, $a \equiv b \pmod{m}$ таққослама берилган бўлса, бу таққосламага $mk \equiv 0 \pmod{m}$ таққосламани қўшсак, $a + mk \equiv b \pmod{m}$ таққослама ҳосил бўлади.

3°. Бир хил модулли таққосламаларни ҳадлаб кўпайтириш мумкин. Ҳақиқатан, (5) даги тенгликларни ҳадлаб кўпайтириб, $a_1 \cdot a_2 \cdot \dots \cdot a_k = b_1 \cdot b_2 \cdot \dots \cdot b_k + mA$ тенгликка эга бўламиз. Бунда

$$A = b_1 b_2 b_4 \dots b_k t_2 + b_1 b_3 b_4 \dots b_k t_1 + \dots$$

бўлиб

$$a_1 a_2 \dots a_k \equiv b_1 b_2 \dots b_k \pmod{m} \tag{8}$$

таққослама ўринли.

Натижа. Таққосламаларнинг иккала қисмини (модулни ўзгартирмай) бир хил мусбат бутун даражага кўтариш мумкин.

Ҳақиқатан ҳам, $b_1 = b_2 = \dots = b_k = b$, $a_1 = a_2 = \dots = a_k = a$ бўлса, у ҳолда (8) га кўра $a^k \equiv b^k \pmod{m}$ таққослама ҳосил бўлади.

4°. Модулни ўзгартирмаган ҳолда таққосламанинг иккала қисмини бир хил бутун сонга кўпайтириш мумкин.

Ҳақиқатан, $a \equiv b \pmod{m}$ таққосламани $k \equiv k \pmod{m}$ таққослама билан ҳадлаб кўпайтириш натижасида $ak \equiv bk \pmod{m}$ га эга бўламиз.

5°. Агар $x \equiv y \pmod{m}$ бўлса, у ҳолда ихтиёрий бутун коэффициентли $f(x)$ ва $f(y)$ кўпҳадлар учун $f(x) \equiv f(y) \pmod{m}$, яъни

$$a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv a_0 y^n + a_1 y^{n-1} + \\ + \dots + a_n \pmod{m} \ (a_i \in Z)$$

таққослама ўринли бўлади.

Исботи. $x \equiv y \pmod{m}$ бўлганидан 3-хоссадаги натижага асосан

$$x^k \equiv y^k \pmod{m}. \qquad (9)$$

(9) нинг иккала қисмини 4-хоссага кўра a_{n-k} га кўпайтирамиз. Натижада $a_{n-k}x^k \equiv a_{n-k}y^k \pmod{m}$ ($k = \overline{0,\ n}$) таққосламалар ҳосил бўлади Булардан эса 2-хосса ёрдамида қуйидаги таққосламани топамиз:

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv a_0y^n + a_1y^{n-1} + \\ + \ldots + a_n \pmod{m}.$$

6°. Агар бир вақтда $a_i \equiv b_i \pmod{m}$ ($i = \overline{1,\ n}$) ва $x \equiv y \pmod{m}$ таққосламалар ўринли бўлса, у ҳолда

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv b_0y^n + b_1y^{n-1} + \\ + \ldots + b_n \pmod{m}$$

таққослама ўринли бўлади.

Натижа. Таққосламада қатнашувчи қўшилувчини ўзи билан тенг қолдиқли бўлган иккинчи сонга алмаштириш мумкин. Ҳақиқатан, $a + b \equiv c \pmod{m}$, $b \equiv d \pmod{m}$ бўлса, у ҳолда $a + d \equiv c \pmod{m}$ бўлади.

Таққосламани даражага нисбатан кўллаш мумкин эмас. Масалан, $3 \equiv 8 \pmod{5}$ учун $2^3 \not\equiv 2^8 \pmod{5}$ бўлади. Чунки $2^3 \equiv 3 \pmod{5}$ ва $2^8 \equiv 1 \pmod{5}$, аммо $1 \not\equiv 3 \pmod{5}$.

7°. Таққосламанинг иккала қисмини модуль билан ўзаро туб бўлган кўпайтувчига қисқартириш мумкин.

Исботи.

$$ad \equiv bd \pmod{m} \qquad (10)$$

бўлиб, $(d;\ m) = 1$ бўлсин. (10) таққослама $(ad - bd)/m$ муносабатга тенг кучли. У ҳолда $(a - b)d/m$ дан $(d;\ m) = 1$ бўлгани учун $(a - b)/m$ ёки $a \equiv b \pmod{m}$ бўлади.

Агар $(m;\ d) = k$ бўлиб, $k > 1$ бўлса, у ҳолда бу хосса ўринли эмас.

Мисол. $5 \cdot 4 \equiv 7 \cdot 5 \pmod{15}$, $(5;\ 15) = 5 \neq 1$ бўлгани учун бу таққосламанинг ҳар иккала томонини 5 га бўлиб, $4 \not\equiv 7 \pmod{5}$ хулосага келамиз.

8°. Таққосламанинг иккала қисмини ва модулини бир хил бутун мусбат сонга кўпайтириш, таққосламанинг иккала қисми ва модули умумий кўпайтувчига эга бўлса, у ҳолда бу таққосламанинг иккала қисми ва модулини умумий кўпайтувчига бўлиш мумкин.

Исботи. а) $a \equiv b \pmod{m}$ таққослама берилган бўлсин. $a = b + mt$ тенгликнинг иккала қисмини d бутун сонга кўпайтирсак, $ad = bd + mdt$ ёки $ad \equiv \equiv bd \pmod{md}$ таққослама ҳосил бўлади.

б) $ad \equiv bd \pmod{md}$ берилган бўлсин. У ҳолда бу таққосламани $(ad - bd)/md$ ёки $(a-b)\,d/md$ каби ёзишимиз мумкин. Бундан $a - b/m$, яъни $a \equiv b \pmod{m}$ таққослама келиб чиқади.

9°. Агар таққослама бир неча модуль бўйича ўринли бўлса, у ҳолда бу таққослама шу модулларнинг энг кичик умумий карралиси бўйича ҳам ўринли бўлади.

Исботи. $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$ бўлсин.

Таққослама таърифига асосан $a - b$ айирма бир вақтда m_1 ва m_2 ларга бўлинганидан бу айирма $m = [m_1; m_2]$ га ҳам бўлинади, яъни $a \equiv b \pmod{m}$ бўлади. Бу мулоҳазадан, агар таққослама $m_1, m_2, \ldots, m_n$ бўйича ўринли бўлса, $T = [m_1, m_2, \ldots, m_n]$ бўйича ҳам ўринли бўлади, деган хулосага келамиз.

10°. Агар таққослама бирор m модуль бўйича ўринли бўлса, у ҳолда шу таққослама модулнинг ихтиёрий бўлувчиси бўйича ҳам ўринли бўлади.

Ҳақиқатан, агар $a \equiv b \pmod{m}$ ёки $a - b = mt$ бўлиб $m = m_1 d$ бўлса, у ҳолда $a - b = m_1 dt$ дейиш мумкин. Бундан $a - b = m_1(dt)$ бўлади. Демак, $a \equiv b \pmod{m_1}$ экан.

11°. Таққосламанинг бир қисми ва модулининг энг катта умумий бўлувчиси билан унинг иккинчи қисми ва модулининг энг катта умумий бўлувчиси ўзаро тенг бўлади.

Ҳақиқатан, $a \equiv b \pmod{m}$ дан $a = b + mt$ ёки $a - - mt = b$ тенгликларни ёзиш мумкин.

$(a; m) = d$ ва $(b; m) = d_1$ бўлсин. Айтайлик, $a = da_1$ ва $m = dm_1$ бўлсин.

$a_1 d - m_1 dt = b$ нинг чап қисми d га бўлинганидан b ҳам d га бўлинади. d сон b ва m сонларнинг умумий бўлувчиси экан ва

$$d_1/d \tag{11}$$

$b = b_1 d$ бўлсин. У ҳолда $a = b_1 d_1 + m_2 d_1 t$ тенгликдан a/d_1 ва d_1 сон a ва m сонларнинг умумий бўлувчиси бўлгани учун

$$d/d_1 \tag{12}$$

бўлади. (11) ва (12) ларга кўра $d_1 = d$ бўлади.

22-§. Чегирмаларнинг тўла системаси. Чегирмалар синфларининг аддитив группаси ва ҳалқаси

Барча бутун сонларни бирор мусбат m бутун сонга бўлишдан 0, 1, 2, . . ., $m-1$ қолдиқлар ҳосил бўлади. Ҳар бир қолдиққа сонларнинг бирор синфи мос келади.

1-таъриф. m га бўлинганда бир хил қолдиқ берадиган бутун сонлар тўплами *m модуль бўйича чегирмалар синфи* дейилади.

m модуль бўйича чегирмалар синфларини

$$C_0, \overline{C_1}, \overline{C_2}, \ldots, \overline{C_{m-1}} \qquad (1)$$

кўринишда белгилайлик.

Бўлинма ва қолдиқнинг мавжудлиги ва ягоналиги ҳақидаги теоремага асосан чегирмаларнинг m модуль бўйича ҳар хил синфлари умумий элементга эга бўлмайди. Демак, бутун сонлар тўплами ўзаро кесишмайдиган синфларга ёйилади.

$\overline{C_r}$ синфнинг элементлари $mq+r$ шаклга эга бўлиб, q га ҳар хил бутун қийматлар бериш натижасида бу элементларнинг барчасини ҳосил қилиш мумкин. Масалан, $m=10$ бўлганда 3 қолдиқ ҳосил қиладиган сонлар $10q+3$ кўринишга эга ва $q=0, \pm 1, \pm 2, \ldots$ десак, $\{\ldots, -27, -17, -7, 3, 13, 23, \ldots\}$ синф ҳосил бўлади.

Иккита бутун сон m модуль бўйича таққосланувчи бўлиши учун улар шу модуль бўйича битта синфнинг элементи бўлиши кераклиги ўз-ўзидан маълум.

2-таъриф. Чегирмалар синфининг ихтиёрий элементи шу синфнинг *чегирмаси* дейилади.

3-таъриф. m модуль бўйича тузилган ҳар бир чегирмалар синфидан ихтиёрий равишда биттадан элемент олиб тузилган элементлар тўплами *m модуль бўйича чегирмаларнинг тўла системаси* дейилади.

Масалан, $m=10$ модуль бўйича $10q$, $10q+1$, . . ., $10q+9$ синфлар ҳосил бўлади. Шуларнинг ҳар бириддан ихтиёрий равишда биттадан олиб тузилган, 20, 31, 112, 13, 24, 135, 6, 147, -2, -31 сонлар системаси 10 модуль бўйича чегирмаларнинг тўла системаси бўлади.

Чегирмаларнинг манфиймас энг кичик тўла системасида $\{0, 1, 2, \ldots, m-1\}$ тўплам олинади. Баъзи ҳолларда абсолют қиймати бўйича энг кичик чегирмаларнинг m жуфт сон бўлса, 0, ± 1, ± 2, ..., $\pm \frac{m-2}{2}$, $\frac{m}{2}$; m тоқ сон бўлса, 0, ± 1, ± 2, ..., $\pm \frac{m-1}{2}$ кўринишдаги системаси олинади.

Юқоридаги мулоҳазаларга асосан, қуйидаги хулосага келамиз:

Берилган сонлар тўплами бирор m модуль бўйича чегирмаларнинг тўла системасини ҳосил қилиши учун қуйидаги иккита шартни қаноатлантириши керак экан:

1. Улар m модуль бўйича ҳар хил синфларнинг элементлари бўлиши керак.

2. Уларнинг сони m га тенг бўлиши керак.

1-теорема (чизиқли форма ҳақида). *Агар* $(a, m) = 1$ *ва* b *ихтиёрий бутун сон бўлиб,* x *ўзгарувчи* m *модуль бўйича чегирмаларнинг тўла системасини ташкил этса, у ҳолда* $ax + b$ *форма ҳам* m *модуль бўйича чегирмаларнинг тўла системасини ташкил этади.*

Исботи. Ҳақиқатан, ҳосил бўлган сонлар системаси:

1) m та сондан иборат, чунки x нинг ўрнига m та ҳар хил қиймат (m модуль бўйича чегирмаларнинг тўла системаси) қўйилади.

2) Ҳосил бўлган сонлар m модуль бўйича ҳар хил синфга тегишлидир.

Тескарисини фараз қилайлик, яъни улар ҳар хил синфга тегишли бўлмасин Бошқача айтганда, x нинг иккита ҳар хил x_1 ва x_2 қийматларида $ax_1 + b$, $ax_2 + b$ лар m модуль бўйича таққосланувчи, яъни $ax_1 + b \equiv ax_2 + b \pmod{m}$ бўлсин. У ҳолда $ax_1 \equiv ax_2 \equiv (\mathrm{mod}\, m)$ таққосламага эга бўламиз. Аммо $(a; m) = 1$ бўлгани учун бу таққосламанинг ҳар иккала қисмини a га қисқартириб $x_1 \equiv x_2 \pmod{m}$ таққосламани ҳосил қиламиз. Лекин бундай бўлиши мумкин эмас, чунки теорема шартига асосан x ўзгарувчи m модуль бўйича чегирмаларнинг тўла системасини ташкил этар эди, яъни $x_1 \not\equiv x_2 \pmod{m}$. Демак, фаразимиз нотўғри бўлиб, $ax + b$ форма m модуль бўйича ҳар хил синфнинг элементларидан иборат экан.

Энди (1) чегирмалар синфлари тўпламини Z/m орқали белгилайлик. Z/m тўпламда қўшиш ва кўпайтириш амалларини қуйидагича аниқлаймиз:

$$\overline{C}_i + \overline{C}_j = \overline{C}_r, \quad \overline{C}_i - \overline{C}_j = \overline{C}_t. \qquad (2)$$

Агар (2) да $i+j<m$ бўлса $r=i+j$, агар $i+j\geqslant m$ бўлса, $r=i+j-m$, агар $i-j\geqslant 0$ бўлса, $t=i-j$‘ агар $i-j<0$ бўлса, $t=m+i-j$ бўлади.

Таққосламалар хоссалари ва (2) тенгликларга кўра ихтиёрий $\overline{C_i}$ ва $\overline{C_j}$ синфлар учун уларнинг йиғиндиси $\overline{C_r}$ ва айирмаси $\overline{C_t}$ синфлар мавжуд.

Бутун сонларни қўшиш.амали коммутатив ва ассоциатив бўлгани учун чегирмалар синфларини қўшиш амали ҳам коммутатив ва ассоциатив бўлади.

$\overline{C_0}$ чегирмалар синфи қўшиш амалига нисбатан нейтраль элемент бўлади, яъни $\overline{C_i}+\overline{C_0}=\overline{C_i}$ тенглик ўринли. $-\overline{C_i}$ синф $\overline{C_i}$ синфга қарама-қарши синф бўлади, яъни $\overline{C_i}+(-\overline{C_i})=\overline{C_0}$ тенглик ўринли.

Бу мулоҳазалардан қуйидаги теореманинг ўринли экани келиб чиқади.

2-теорема. *$\langle Z/m, +, -\rangle$ — алгебра группа бўлади.*

4-таъриф. $\langle Z/m, +, -\rangle$ группа m модуль бўйича чегирмалар синфларининг *аддитив группаси* дейилади.

1-мисол. $Z/4$ тўплам аддитив группа ташкил қилишини кўрсатинг.

Модуль $m=4$ бўлгани учун $\overline{C_0}=\{\ldots, -4, 0, 4, \ldots\}$, $\overline{C_1}=\{\ldots, -3, 1, 5, \ldots\}$, $\overline{C_2}=\{\ldots, -2, 2, 6, \ldots\}$, $\overline{C_3}=\{\ldots, -1, 3, 7, \ldots\}$ бўлиб, бу синфлар учун $\overline{C_1}+\overline{C_3}=\overline{C_0}$, $\overline{C_2}+\overline{C_3}=\overline{C_1}$, $\overline{C_3}+\overline{C_3}=\overline{C_2}$, $\overline{C_3}-\overline{C_1}=\overline{C_2}$, $\overline{C_1}-\overline{C_2}=\overline{C_3}$, ... тенгликлар бажарилади. Бу тенгликлардан қўшиш амалининг коммутатив ва ассоциативлигини кўрсатиш мумкин. У ҳолда $Z/4=\{\overline{C_0}, \overline{C_1}, \overline{C_2}, \overline{C_3}\}$ тўплам аддитив группа ташкил қилади.

(1) даги чегирмалар синфларини кўпайтириш амали

$$\overline{C_i}\cdot\overline{C_j}=\overline{C_l} \tag{3}$$

кўринишда аниқланади, бунда $i\cdot j<m$ бўлса, $i\cdot j=l$, $i\cdot j\geqslant m$ бўлса, $i\cdot j=mq+l$, яъни $l=i\cdot j-mq$ бўлади.

Таққосламалар хоссалари ва (3) тенгликка асосан, ихтиёрий $\overline{C_i}$ ва $\overline{C_j}$ синфларга бир қийматли $\overline{C_l}$ синфи мос қўйилади.

Чегирмалар синфларини қўшиш ва кўпайтириш амаллари шу чегирмалар синфларидаги сонлар устида мос амалларни бажариш каби бўлади. Чегирмалар синфлари устида қўшиш ва кўпайтиришнинг коммутативлик, ассоциативлик ва қўшишга нисбатан кўпайтиришнинг дистрибутивлик хоссалари ўринли.

$\overline{C}_1$ синф кўпайтириш амалига нисбатан нейтрал элемент бўлади, яъни $\overline{C}_i \cdot \overline{C}_1 = \overline{C}_i$ тенглик ўринли.

Бу мулоҳазалардан қуйидаги теореманинг ўринли экани келиб чиқади:

3-теорема. $<Z/m, +, -, \cdot, 1>$ — *алгебра коммутатив ҳалқа бўлади.*

5-таъриф. $<Z/m, +, -, \cdot, 1>$ ҳалқа m модуль бўйича *чегирмалар синфларининг ҳалқаси* дейилади.

2-мисол. $Z/4$ тўплам ҳалқа ташкил этишини кўрсатинг.

$Z/4$ тўпламда кўпайтириш амали қуйидагича бўлади:

$$\overline{C}_3 \cdot \overline{C}_2 = \overline{C}_2, \quad \overline{C}_1 \cdot \overline{C}_3 = \overline{C}_3, \quad \overline{C}_3 \cdot \overline{C}_3 = \overline{C}_1, \quad \ldots$$

Кўпайтириш амали коммутатив ва ассоциатив (текшириб кўринг).

Дистрибутивлик хоссаси бажарилади. Ҳақиқатан,

$$(\overline{C}_2 + \overline{C}_3) \cdot \overline{C}_2 = \overline{C}_1 \cdot \overline{C}_2 = \overline{C}_2, \ \overline{C}_2 \cdot \overline{C}_2 = \overline{C}_0,$$
$$\overline{C}_3 \cdot \overline{C}_2 = \overline{C}_2,$$

$\overline{C}_2 \cdot C_2 + \overline{C}_3 \cdot \overline{C}_2 = \overline{C}_2$ бўлгани учун $(\overline{C}_2 + \overline{C}_3) \cdot \overline{C}_2 = \overline{C}_2 \times \overline{C}_2 + \overline{C}_3 \cdot \overline{C}_2$ бўлади.

$Z/4$ тўпламда айириш амали бажарилади (текшириб кўринг).

Демак, $Z/4$ тўплам ҳалқа экан.

23-§. Чегирмаларнинг келтирилган системаси, модуль билан ўзаро туб бўлган чегирмалар синфларининг мультипликатив группаси

Таққосламаларнинг 11-хоссасига асосан m модуль бўйича ўзаро таққосланувчи сонлар m модуль билан бир хил энг катта умумий бўлувчига эга эди. m модуль бўйича таққосланувчи сонлар битта синфнинг элементларидан иборатлигини биз юқорида кўрсатган эдик. Демак, синфнинг битта чегирмаси модуль билан ўзаро туб бўлса, бу синфнинг барча элементлари ҳам m билан ўзаро туб бўлади.

Шунинг учун m модуль билан ўзаро туб бўлган чегирмалар синфи тўғрисида гапириш мумкин. Бу синфлар тўплами сонлар назариясида муҳим роль ўйнайди.

1-таъриф. m модуль билан ўзаро туб бўлган барча чегирмалар синфларидан биттадан элемент олиб тузилган тўплам *чегирмаларнинг m модуль бўйича келтирилган системаси* дейилади.

Чегирмаларнинг келтирилган системасини шу чегирмаларнинг тўла системасидан ҳам тузиш мумкин. Бунинг учун тўла системада модуль билан ўзаро туб бўлган чегирмаларни ажратиб олиш кифоя.

Масалан, $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ тўплам, 10 модуль бўйича чегирмаларнинг тўла системаси бўлгани ҳолда 1, 3, 7, 9 эса 10 модуль бўйича чегирмаларнинг келтирилган системасидир. Худди шундай 1, 3, -3, -1 ҳам 10 модуль бўйича чегирмаларнинг келтирилган системаси бўлади. Чегирмаларнинг келтирилган системасидаги элементлар сонини аниқлаш учун Эйлер функцияси деб аталувчи қуйидаги $\varphi(m)$ функциядан фойдаланилади:

2-таъриф. Агар қуйидаги иккита шарт бажарилса, $\varphi(m)$ сонли функция *Эйлер функцияси* дейилади:

1. $\varphi(1)=1$;
2. $\varphi(m)$ функция m дан кичик ва m билан ўзаро туб бўлган сонлар сони.

Берилган сонлар системаси m модуль бўйича чегирмаларнинг келтирилган системаси бўлиши учун қуйидаги учта шарт бажарилиши керак:

1. Сонлар системасининг элементлари $\varphi(m)$ та бўлиши керак.
2. Сонлар системасидаги ихтиёрий иккита сон m модуль бўйича таққосланмаслиги, яъни m модуль бўйича ҳар хил синф элементлари бўлиши керак.
3. Сонлар системасидаги ихтиёрий сон m модуль билан ўзаро туб бўлиши керак.

1-теорема (чизиқли форма ҳақида). *Агар ax чизиқли формадаги x ўзгарувчи m модуль бўйича чегирмаларнинг келтирилган системасини ташкил этса ва $(a; m)=1$ бўлса, у ҳолда ax ҳам m модуль бўйича чегирмаларнинг келтирилган системасини ташкил этади.*

Теоремани исботлаш учун ax лар ҳам юқоридаги учта шартни қаноатлантиришини кўрсатиш лозим.

1. ax сонлар сони $\varphi(m)$ та бўлади. Чунки x нинг ўрнига биз кетма-кет $\varphi(m)$ та сон қўямиз.

2. 22-§ даги чизиқли форма ҳақидаги теоремага асосан $ax+b$ сони m модуль бўйича турли синф элементи эди. Демак, ax лар ҳам турли синф вакиллари бўлади, чунки x сони ҳар хил синфлардан олинган ва $(a;\ m)=1$.

3. Теорема шартига асосан, $(a;\ m)=1$ ва x ўзгарувчи m модуль бўйича чегирмаларнинг келтирилган системасининг элементи бўлганидан $(x;\ m)=1$ бўлади. Демак, $(ax;\ m)=1$ экан.

Эслатма. x ва ax чегирмалар m модуль бўйича алоҳида чегирмаларнинг келтирилган системасини ташкил қилса-да, x нинг бир хил қийматларида улар турли синф элементлари бўлади.

Ҳақиқатан, $(x;\ m)=1$ бўлгани учун $ax\equiv x \pmod{m}$ таққослама фақат ва фақат $a\equiv 1 \pmod{m}$ бўлгандагина рост бўлади. Агар x ва ax ларнинг m модуль бўйича энг кичик мусбат чегирмалари олинса, бу система бир хил элементлардан иборат бўлади. Бу системаларнинг мос элементлари (ўрин нуқтаи назаридан) m модуль бўйича турли синф элементлари бўлади.

1-мисол. $a=5$, $m=14$ бўлсин. У ҳолда $(5;\ 14)=1$ бўлиб, m модуль бўйича чегирмаларнинг келтирилган системаси $x=1,\ 3,\ 5,\ 9,\ 11,\ 13$ дан иборат бўлади.

$m=14$ модуль бўйича $5x$ ни ҳисоблаймиз:

$$5\cdot 1\equiv 5 \pmod{14},$$
$$5\cdot 3\equiv 1 \pmod{14},$$
$$5\cdot 5\equiv 11 \pmod{14},$$
$$5\cdot 9\equiv 3 \pmod{14},$$
$$5\cdot 11\equiv 13 \pmod{14},$$
$$5\cdot 13\equiv 9 \pmod{14}.$$

Демак, $5x$ ни 14 га бўлгандаги қолдиқлар мос равишда 5, 1, 11, 3, 13, 9 бўлар экан. 1, 3, 5, 9, 11, 13 ва 5, 1, 11, 13, 9 системалар бир-биридан фақат сонларнинг турган ўрни билан фарқ қилади, холос. Бу сонлар кўпайтмалари эса ўзаро тенг.

2-теорема. *m модуль билан ўзаро туб чегирмалар синфлари тўплами кўпайтириш амалига нисбатан абель группа ташкил қилади.*

Исботи. G_m тўплам m модуль билан ўзаро туб чегирмаларнинг барча синфлари тўплами бўлсин.

m модуль билан ўзаро туб чегирмалар синфларининг ихтиёрий иккитасининг кўпайтмаси яна модуль билан ўзаро туб чегирмалар синфи бўлади.

G_m даги синфларни кўпайтириш амали коммутативлик ва ассоциативлик хоссаларига эга.

$\overline{C}_1$ синф кўпайтириш амалига нисбатан нейтраль элемент бўлади.

Ихтиёрий $\overline{C}_i \in G_m$ синф учун тескари синф мавжудлигини кўрсатамиз. $G_m^* = \{\overline{C}_1, \overline{C}_2, \ldots, \overline{C}_{\varphi(m)}\}$ бўлсин. Бунда $\varphi(m)$ — Эйлер функцияси.

$a_1, a_2, \ldots, a_{\varphi(m)}$ лар m модуль бўйича чегирмаларнинг келтирилган системаси ва $a_i \in \overline{C}_i$ $(i = \overline{1, \varphi(m)})$ бўлсин.

1-теоремага асосан $a_i \cdot a_1, a_i \cdot a_2, \ldots, a_i \cdot a_{\varphi(m)}$ лар ҳам чегирмаларнинг келтирилган системасини ташкил қилади. Улар орасида m модуль бўйича 1 билан таққосланувчи $a_i a_k$ элемент мавжуд, яъни $a_i \cdot a_k \equiv 1 \pmod{m}$ ўринли.

У ҳолда $\overline{C}_i \cdot \overline{C}_k = \overline{C}_1$ тенглик ўринли бўлиб, $\overline{C}_k$ синф $\overline{C}_i$ синфга тескари синф бўлади. Демак, $\langle G_m, \cdot, ^{-1} \rangle$ алгебра абель группаси экан.

3-таъриф. $\langle G_m, \cdot, ^{-1} \rangle$ группа m модуль билан ўзаро туб чегирмалар синфларининг *мультипликатив группаси* дейилади.

2-мисол. $m = 6$ модуль бўйича $G_6 = \{\overline{C}_1, \overline{C}_5\}$ тўплам мультипликатив группа бўлади.

Ҳақиқатан, кўпайтириш амали қуйидагича аниқланади:

$$\overline{C}_1 \cdot \overline{C}_1 = \overline{C}_1, \quad \overline{C}_1 \cdot \overline{C}_5 = \overline{C}_5, \quad \overline{C}_5 \cdot \overline{C}_5 = \overline{C}_1.$$

Бу тенгликлардан кўринадики, $\overline{C}_1$ ва $\overline{C}_5$ синфлар ўзига-ўзи тескари синфлар, $\overline{C}_1$ синф эса нейтрал элемент бўлади. Демак, ассоциативлик хоссаси бажарилади (текшириб кўринг).

24-§. Эйлер функцияси ва унинг хоссалари

Таъриф. Натурал сонлар тўпламида аниқланган f функция учун $(m; n) = 1$ бўлганда

$$f(m \cdot n) = f(m) \cdot f(n) \qquad (1)$$

тенглик бажарилса, у ҳолда f функция *мультипликатив функция* дейилади.

Теорема. *Эйлер функцияси мультипликатив функциядир.*

Исботи. (1) ни исботлаш учун 1 дан nm гача бўлган сонларни қуйидаги жадвал шаклида ёзиб оламиз:

$$\begin{array}{cccccc} 1 & 2 & \ldots & k & \ldots & m \\ m+1 & m+2 & \ldots & m+k & \ldots & 2m \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ (n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+k & \ldots & (n-1)m+m=nm \end{array} \tag{2}$$

$\varphi(nm)$ ни ҳисоблаш учун (2) жадвалда $n \cdot m$ билан нечта ўзаро туб сон борлигини аниқлашимиз керак.

Бирор сон $n \cdot m$ билан ўзаро туб бўлиши учун у шу сонларнинг ҳар бири билан ўзаро туб бўлиши лозим. Шунинг учун (2) дан аввало m билан ўзаро туб бўлган сонларни ажратиб оламиз. Ажратилган сонлар орасидан эса n билан ўзаро тубларини танлаб оламиз. Жадвалнинг тузилишига асосан, ҳар бир устун элементлари m модулга нисбатан тенг қолдиқлар синфидан иборат. Шунинг учун ҳар бир устуннинг барча элементлари m модуль билан бир хил энг катта умумий бўлувчига эга, бу элементлардан биттаси m билан ўзаро туб бўлса, шу устуннинг барча элементлари ҳам m билан ўзаро туб бўлади. Демак, m модуль билан „ўзаро туб устунлар" тўғрисида гапириш мумкин. m билан „ўзаро туб устунлар" сонининг $\varphi(m)$ га тенглиги ўз-ўзидан кўриниб турибди. Энди жадвалнинг ихтиёрий бирор устунини оламиз. Мисол учун

$$k,\ m+k,\ 2m+k,\ \ldots,\ (n-1)m+k \tag{3}$$

ни қарайлик. Бу устуннинг элементларини x ўзгарувчи $0, 1, 2, \ldots, (n-1)$ қийматларни қабул қилгандаги $mx+k$ чизиқли форманинг қийматлари деб қараш мумкин. $(m; n)=1$ бўлгани учун (3) кетма-кетлик k га боғлиқ бўлмаган ҳолда n модуль бўйича чегирмаларнинг тўла системасини ташкил қилади. Демак, (3) даги n билан ўзаро туб сонлар $\varphi(n)$ дир. Шундай қилиб, (2) да m ҳамда n лар билан ўзаро туб сонлар сони $\varphi(n) \cdot \varphi(m)$ та экан. n ҳамда m билан ўзаро туб сон $m \cdot n$ билан ҳам ўзаро туб бўлади. Демак,

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m).$$

Бу хоссани чекли сондаги ўзаро туб сонлар кўпайтмаси учун ҳам умумлаштириш мумкин.

$\varphi(m)$ Эйлер функциясининг ҳисоблаш формулалари қуйидагилардан иборат.

а) $m = p$ туб сон бўлсин. У ҳолда $a < p$ бўлса, $(a; p) = 1$. Бундай сонлар 1, 2, 3, ..., $p - 1$ бўлгани учун $\varphi(p) = p - 1$ бўлади.

1-мисол. $p = 7$ бўлсин. 1, 2, 3, 4, 5, 6 сонларнинг ҳар бири 7 билан ўзаро тубдир. Шунинг учун $\varphi(7) = 6$ бўлади.

б) $m = p^{\alpha}$ бўлсин. $\varphi(p^{\alpha})$ ни ҳисоблаш учун 1 дан p^{α} гача сонларни қуйидагича ёзиб оламиз:

$$1, 2, 3, \ldots, p^{\alpha}. \tag{4}$$

Бу қатордаги $p, 2p, \ldots, p^{\alpha-1} \cdot p$ сонларнинг барчаси p га бўлингани учун p билан ўзаро туб эмас. p га бўлинадиган сонлар сони $p^{\alpha-1}$ тадир. (4) қаторда эса p^{α} та сон бор. Демак, (4) да p билан ўзаро туб сонлар сони

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p - 1), \text{ яъни}$$

$$\varphi(p^{\alpha}) = p^{\alpha-1}(p - 1)$$

та экан.

в) $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ бўлсин. Эйлер функцияси мультипликатив функция бўлгани учун

$$\varphi(m) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$$

тенгликни ёзиш мумкин. Ҳар бир кўпайтувчи учун б) ни қўллаб, қуйидагига эга бўламиз:

$$\varphi(m) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \ldots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right),$$

$$\varphi(m) = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \times$$

$$\times \ldots \cdot \left(1 - \frac{1}{p_k}\right),$$

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

ёки

$$\varphi(m) = p_1^{\alpha_1-1}(p_1 - 1) \cdot p_2^{\alpha_2-1}(p_2 - 1) \cdot \ldots \cdot p_k^{\alpha_k-1}(p_k - 1).$$

2-мисол. $\varphi(360)$ ни топинг.

$360 = 2^3 \cdot 3^2 \cdot 5$. У ҳолда $\varphi(360) = 2^2(2 - 1) \cdot 3(3 - 1)(5 - 1) = 96$, яъни $\varphi(360) = 96$.

25- §. Берилган соннинг барча бўлувчилари бўйича тузилган Эйлер функциялари қийматларининг йиғиндиси

Фараз қилайлик, m сони d та бўлувчига эга бўлсин. Бу бўлувчилар бўйича тузилган Эйлер функциялари қийматлари йиғиндисини $\sum\limits_{m|d}\varphi(d)$ каби белгилайлик.

$\sum\limits_{m|d}\varphi(d)$ нинг m га тенг эканлигини кўрсатамиз. Айтайлик

$$m=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ \ldots\ \cdot p_k^{\alpha_k} \qquad (1)$$

бўлсин. Бу ерда p_1, p_2, ..., p_k лар m нинг турли туб бўлувчиларидир. m нинг барча бўлувчилари $d=p_1^{\beta_1}\times\times p_2^{\beta_2}\cdot\ \ldots\ \cdot p_k^{\beta_k}$ кўринишдаги сонлар бўлади. Бу ерда

$$0\leqslant\beta_1\leqslant\alpha_1,\ 0\leqslant\beta_2\leqslant\alpha_2,\ \ldots,\ 0\leqslant\beta_k\leqslant\alpha_k. \qquad (2)$$

$\alpha_2=\alpha_3=\ldots=\alpha_k=0$ бўлганда m нинг бўлувчилари 1, p_1, p_1^2, ..., $p_1^{\alpha_1}$ лардан иборат. Демак, бундаги Эйлер функциялари қийматлари йиғиндиси $1+\varphi(p_1)+\varphi(p_1^2)+\ldots+\varphi(p_1^{\alpha_1})$ бўлади. $\varphi(p_1^{\beta_1})\cdot\varphi(p_2^{\beta_2})\cdot\ldots\times\varphi(p_k^{\beta_k})=\varphi(p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ \ldots\ \cdot p_k^{\beta_k})$ бўлгани учун $\sum\limits_{m|d}\varphi(d)=(1+\varphi(p_1)+\varphi(p^2)+\ldots+\varphi(p_1^{\alpha_1}))\cdot(1+\varphi(p_2)+\varphi(p_2^2)+\ldots+\varphi(p_2^{\alpha_2}))\cdot\ \ldots\ \cdot(1+\varphi(p_k)+\varphi(p_k^2)+\ldots+\varphi(p_k^{\alpha_k}))$ бўлади. Лекин $(1+\varphi(p_k)+\ldots+\varphi(p_k^{\alpha_k})=1+(p_k-1)+(p_k^2-p_k)+\ldots+(p_k^{\alpha_k}-p_k^{\alpha_k-1})=p_k^{\alpha_k}$. Демак, $\sum\limits_{m|d}\varphi(d)=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ \ldots\ \cdot p_k^{\alpha_k}=m$, яъни $\sum\limits_{m|d}\varphi(d)=m$.

26- §. Эйлер ва Ферма теоремалари

1-теорема (Эйлер теоремаси). *Агар* $(a;\ m)=1$ *бўлса, у ҳолда*

$$a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\ m) \qquad (1)$$

таққослама ўринлидир.

Исботи. 23-§ даги чизиқли форма ҳақидаги 1-теоремадан фойдаланамиз. ax формани олиб, ундаги x ўрнига m модуль бўйича чегирмаларнинг келтирилган системасидаги сонларни кетма-кет қўйиб чиқамиз. Чегирмаларнинг келтирилган системаси энг кичик мусбат чегирмалардан иборат бўлсин. Агар x ўзгарувчи $r_1, r_2, \ldots, r_k$ $(k=\varphi(m))$ каби чегирмаларни қабул қилса, ax форма ҳам мос равишда $r_1', r_2', \ldots, r_k'$ $(k=\varphi(m))$ каби чегирмаларни қабул қилади. Демак,

$$ar_1 \equiv r_1' \pmod m,$$
$$ar_2 \equiv r_2' \pmod m,$$
$$\cdots\cdots\cdots$$
$$ar_k \equiv ar_k' \pmod m.$$

Бу таққосламаларни ҳадлаб кўпайтирсак,

$$a^k \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_k \equiv r_1' \cdot r_2' \cdot \ldots \cdot r_k' \pmod m \qquad (2)$$

таққосламага эга бўламиз. Бунда $r_1 \cdot r_2 \ldots r_k$ кўпайтма билан $r_1' \cdot r_2' \ldots r_k'$ кўпайтма ўзаро тенг ва уларнинг ҳар бири модуль билан ўзаро туб, чунки $(r_i; m) = 1$ эди. (2) нинг иккала қисми $r_1 \cdot r_2 \ldots r_k = r_1' \times \times r_2' \ldots r_k'$ ларга қисқартирилгандан сўнг қуйидагига эга бўламиз:

$$a^k \equiv 1 \pmod m. \qquad (3)$$

Лекин $k=\varphi(m)$ эди. Шунинг учун $a^{\varphi(m)} \equiv 1 \pmod m$ бўлади.

1-мисол. $m=8$, $a=5$ бўлсин. $(8; 5)=1$ бўлиб, $5^{\varphi(8)} \equiv 1 \pmod 8$ бўлади.

$$\varphi(8) = \varphi(2^3) = 2^{3-1}(2-1) = 2^2 \cdot 1 = 4,$$
$$5^4 \equiv 625 \equiv 1 \pmod 8,\ 5^4 \equiv 1 \pmod 8.$$

2-теорема (Ферма теоремаси). *Агар a сон p сонга бўлинмаса ва p туб сон бўлса, у ҳолда $a^{p-1} \equiv \equiv 1 \pmod p$ таққослама ўринли бўлади.*

Исботи. a сон p сонга бўлинмаса ва p туб сон бўлса, у ҳолда $(a; p) = 1$ бўлади. Бундан Эйлер теоремасидаги таққосламада $m=p$ олинса ва $\varphi(p) = p - 1$ эканидан

$$a^{p-1} \equiv 1 \pmod p \qquad (4)$$

таққослама келиб чиқади. $(a; p) = 1$ бўлгани учун (4) нинг иккала қисмини a га кўпайтириш мумкин. У ҳолда $a^p \equiv a \pmod{p}$ таққослама ихтиёрий a учун тўғри бўлади.

2-мисол. $a = 8$, $p = 11$ бўлсин. $8 \equiv -3 \pmod{11}$ бўлганидан

$$8^{10} \equiv (-3)^{10} \pmod{11},$$
$$(-3) \equiv 9 \equiv -2 \pmod{11},$$
$$(-3)^{10} \equiv (-2)^5 \equiv -32 \equiv 1 \pmod{11}.$$

Демак, $8^{10} \equiv 1 \pmod{11}$ бўлади.

$a^{n-1} \equiv 1 \pmod{n}$ таққослама бажарилса, у ҳолда ҳар доим n туб сон бўлмаслиги мумкин.

Масалан, $a = 2$, $n = 341$, $\varphi(341) = 300$ бўлсин, У ҳолда $2^{340} \equiv 1 \pmod{341}$ таққослама ўринли. Лекин 341 мураккаб сон, яъни $341 = 11 \cdot 31$. Аммо $2^{10} \equiv 1 \pmod{341}$ бўлгани учун $2^{340} \equiv 1 \pmod{341}$ бўлади.

27-§. Бир номаълумли биринчи даражали таққосламалар

1-таъриф. Ушбу

$$ax \equiv b \pmod{m} \quad (1)$$

кўринишдаги таққослама *бир номаълумли биринчи даражали таққослама* дейилади (бу ерда a ва b — бутун сонлар, m — натурал сон).

2-таъриф. Агар (1) таққосламада $x = x_1$ бўлганда $ax_1 \equiv b \pmod{m}$ таққослама тўғри бўлса, у ҳолда x_1 сон (1) *таққосламани қаноатлантиради* дейилади.

Теорема. *Агар (1) таққосламани x_1 сон қаноатлантирса, у ҳолда (1) таққосламани $x_1 + mt$ (t — бутун сон) сонлар системаси қаноатлантиради.*

Ҳақиқатан, берилишига кўра $ax_1 \equiv b \pmod{m}$ таққослама тўғри. $x_1 + mt$ сонлар системасига тегишли ихтиёрий x_2 сонни олайлик. У ҳолда $x_2 \equiv x_1 \pmod{m}$ бўлиб, бундан 21-§ даги 5-хоссага кўра $f(x_2) \equiv f(x_1) \pmod{m}$ таққослама келиб чиқади. Бунда $f(x_1) \equiv 0 \pmod{m}$ ни эътиборга олсак, $f(x_2) \equiv 0 \pmod{m}$ таққосламага эга бўламиз, яъни x_2 сон (1) таққосламани қаноатлантиради. Демак, $x_1 + mt$ сонлар системасидаги ҳар бир сон (1) таққосламани қаноатлантирар экан.

$x_1 + mt$ сонлар системаси $\overline{x_1}$ ёки $[x_1]$ синф ҳам деб юритилади.

3-таъриф. Агар $\overline{x_1}$ сон (1) таққосламани қаноатлантирса, у ҳолда $\overline{x_1}$ синф (1) таққосламанинг *ечими* деб аталади.

(1) таққосламани қаноатлантирувчи сонларни 0, 1, 2, ..., $m-1$ сонлар ичидан қидириш керак.

(1) таққосламани ечишнинг қуйидаги иккита ҳолини кўрайлик:

1. $(a; m)=1$ бўлсин. Агар (1) таққослама ечимга эга бўлса, бу ечим m модуль бўйича чегирмаларнинг бирор синфи бўлади. Маълумки, чегирмаларнинг тўла системасидаги ҳар бир чегирмага битта синф мос келар эди. Демак, (1) да x сон чегирмаларнинг тўла системасини қабул қилар экан. У ҳолда чизиқли форма ҳақидаги теоремага кўра ax ҳам чегирмаларнинг тўла системасини қабул қилади. x нинг бирор x_0 қиймати топиладики, натижада ax_0 чегирма билан b сон битта синфга тегишли бўлади, яъни $ax_0 \equiv b \pmod m$ бўлиб, $x \equiv x_0 \pmod m$ бўлади. Бу ечим, юқорида айтилганидек, $\overline{x_0}$ ёки $[x_0]$ кўринишларда ҳам белгиланади.

2. $(a; m)=d>1$ бўлсин. (1) таққосламани унга тенг кучли $ax-b=my$ $(x, y \in \mathbf{Z})$ тенглик кўринишда ёзамиз. Бундан $ax-my=b$ бўлиб, $(a; m)=d$ га кўра $a/d \wedge m/d \Rightarrow b/d$. Демак, агар $b \not/ d$ ҳолда, яъни b сон d га бўлинмаса, (1) таққослама ечимга эга бўлмайди.

Фараз қилайлик, b сон d га бўлинсин, яъни $b=db_1$ бўлсин. Таққосламаларнинг хоссасига асосан (1) нинг иккала қисмини ва модулини d га бўлиб, қуйидагини ҳосил қиламиз:

$$a_1x \equiv b_1 \pmod{m_1}. \qquad (2)$$

(2) таққослама (1) таққосламага тенг кучли эканлигини кўрсатамиз. $\overline{x_1}$ — (2) таққосламанинг ихтиёрий ечими бўлсин. $a_1x_1 \equiv b_1 \pmod{m_1}$ таққосламанинг иккала қисмини ва модулини d га кўпайтирамиз.

$$da_1x_1 \equiv db_1 \pmod{dm_1} \Rightarrow ax_1 \equiv b \pmod m.$$

Демак, $\overline{x_1}$ — (1) таққосламанинг ечими экан. $\overline{x_0}$ — (1) таққосламанинг ихтиёрий ечими бўлсин. $ax_0 \equiv b \pmod m$ таққосламанинг иккала қисмини ва модулини d сонга бўламиз. У ҳолда $a_1x_0 \equiv b_1 \pmod{m_1}$ таққослама ҳосил бўлади, яъни $\overline{x_0}$ — (2) таққосламанинг ечими экан. Демак, (1) ва (2) таққосламалар тенг кучли экан. $(a_1;$

$m_1) = 1$ бўлганидан (1) ҳолга асосан (2) таққослама m_1 модуль бўйича қуйидаги ягона x_0 ечимга эга: $x \equiv x_0 (\bmod m_1)$ ёки $x = x_0 + m_1 k$ $(k \in Z)$. Бу ечим (1) ни ҳам қаноатлантиради, лекин (1) нинг ечимлари шу билан тугамайди. Берилган таққосламанинг ечимларини m модуль бўйича топиш учун қуйидагиларга эътибор берамиз:

$$x_1,\ x_1 + m_1,\ \ldots,\ x_1 + (d-1)\, m_1 \qquad (3)$$

чегирмаларнинг ҳар бири m_1 модуль бўйича тенг қолдиқлар бўлиб. $m_1 d = m$ модуль бўйича эса турли синфга тегишлидир Шу турли синфларнинг элементлари

$$x_1,\ x_1 + m_1,\ x_1 + 2m_1,\ \ldots,\ x_1 + (d-1)\, m_1 \qquad (4)$$

дан иборат. Ҳақиқатан, (4) нинг ҳар қандай иккита элементи m модуль бўйича таққосланувчи эмас. (3) синфнинг (4) га кирмаган ҳар бир элементи учун (4) да шундай элемент топиладики, уларнинг айирмаси $m_1 d = m$ га бўлинади. Шунинг учун улар битта синфнинг элементлари ҳисобланади. Демак, $(a;\ m) = d$ ва $(b;\ m) = d$ бўлса, (1) таққослама (4) орқали аниқланувчи d та ечимга эга экан. Юқоридагиларга асосан қуйидаги хулосани ёза оламиз:

1. Агар $(a;\ m) = 1$ бўлса, (1) нинг ечими мавжуд ва ягонадир.

2. $(a;\ m) = d > 1$ бўлганда

а) b/d бўлса, (1) нинг ечими мавжуд эмас;

б) $b \not/ d$ бўлса, (1) таққослама d та ечимга эга.

Мисоллар. 1. $3x \equiv 7 \pmod{11}$ таққосламани ечинг.

$(3;\ 11) = 1$ бўлгани учун ечим ягона бўлади. 11 модуль бўйича чегирмаларнинг системаси 0, ± 1, ± 2, ± 3, ± 4, ± 5 дан иборат. Бевосита текшириб кўриш билан $x \equiv -5 \pmod{11}$ ечим эканлигига ишонч ҳосил қиламиз.

2. $5x \equiv 7 \pmod{15}$ таққосламани ечинг.

$(5;\ 15) = 5$, лекин 7×5 бўлгани учун бу таққослама ечимга эга эмас.

3. $9x \equiv 6 \pmod{15}$ таққосламани ечинг.

$(9;\ 15) = 3$ ва $6/3$ бўлгани учун таққослама учта ечимга эга. Ҳақиқатан, таққосламани

$$3x \equiv 2 \pmod 5$$

шаклида ёзиб оламиз. $(3;\ 5) = 1$ бўлгани учун бу таққослама 5 модуль бўйича ягона $x \equiv -1 \pmod 5$ ечимга эга. У ҳолда берилган таққосламани -1, $-1+5$, $-1+2\cdot 5$ сонлар қаноатлантиради. Шунинг учун $x\equiv -1, 4, 9 \pmod{15}$ берилган таққосламанинг ечимлари бўлади.

28-§. Бир номаълумли биринчи даражали таққосламаларни ечиш усуллари

Ушбу

$$ax\equiv b \pmod{m} \qquad (1)$$

кўринишдаги бир номаълумли биринчи даражали таққосламаларни ечишнинг бир қанча усуллари мавжуд.

1. **Синаш усули.** Бу усулнинг моҳияти шундаки, (1) таққосламадаги x ўрнига m модулга кўра чегирмаларнинг тўла системасидаги барча чегирмалар кетма-кет қўйиб чиқилади. Улардан қайси бири (1) ни тўғри таққосламага айлантирса, ўша чегирма қатнашган синф ечим ҳисобланади. Биз 27-§ даги иккита мисолни шу усулда ечдик. Лекин коэффициентлар етарлича катта бўлганда бу усул унча қулай бўлмайди.

2. **Коэффициентларни ўзгартириш усули.** Амалий машғулотларда таққосламаларнинг хоссаларидан фойдаланиб, (1) да номаълум олдидаги коэффициентни ва b ни шундай ўзгартириш керакки, натижада таққосламанинг ўнг томонида ҳосил бўлган сон ax ҳаднинг коэффициентига бўлинсин.

1-мисол. $7x\equiv 5 \pmod{9}$ таққосламани ечинг.

$$7x\equiv 5+9 \pmod{9},$$
$$7x\equiv 14 \pmod{9}.$$

$(7; 14)=7$ ва $(7; 9)=1$ бўлганидан $x\equiv 2 \pmod{9}$ ечим келиб чиқади.

2-мисол. $17x\equiv 25 \pmod{28}$ таққосламани ечинг.

$$17x+28x\equiv 25 \pmod{28},$$
$$45x\equiv 25 \pmod{28}.$$

Бундан $9x\equiv 5 \pmod{28}$,

$$9x\equiv 5-140 \pmod{28}\equiv -135 \pmod{28},$$
$$9x\equiv -135 \pmod{28}, \quad x\equiv -15 \pmod{28},$$

$x\equiv 13 \pmod{28}$ ечим ҳосил бўлади.

3. **Эйлер теоремасидан фойдаланиш усули.** Маълумки, $(a; m)=1$ бўлса, у ҳолда $a^{\varphi(m)}\equiv 1 \pmod{m}$

таққослама ўринли эди. Бундан $a^{\varphi(m)} \cdot b \equiv b \pmod{m}$ таққосламани ёзиш мумкин. Охирги таққосламани $ax \equiv \equiv b \pmod{m}$ таққослама билан солиштириб, $x \equiv a^{\varphi(m)-1} \times \times b \pmod{m}$ эканига ишонч ҳосил қиламиз. Мисоллар ечишда $a^{\varphi(m)-1} \cdot b$ ифодани m модуль бўйича энг кичик мусбат чегирмага келтириш лозим.

3-мисол. $3x \equiv 7 \pmod{11}$ таққосламани ечинг.

$$x \equiv 3^{\varphi(11)-1} \cdot 7 \pmod{11}, \quad \varphi(11) = 10,$$
$$3^2 \equiv 9 \equiv -2 \pmod{11}, \quad 3^4 = 4 \pmod{11},$$

$3^5 = 12 \equiv 1 \pmod{11}$ бўлганидан $x = 3^9 \cdot 7 = 28 \equiv \equiv 6 \pmod{11}$, $x \equiv 6 \pmod{11}$ ечим ҳосил бўлади.

Таққосламанинг модули етарлича катта бўлса, қуйидаги усул анча фойдалидир.

4. **Узлуксиз касрлардан фойдаланиш усули.**

Ушбу

$$ax \equiv b \pmod{m} \qquad (1)$$

таққослама берилган бўлиб, $(a;\ m) = 1$ ва $a > 0$ бўлсин.

$\frac{m}{a}$ касрни узлуксиз касрга ёйиб, унинг муносиб касрларини $\frac{\mathscr{P}_k}{Q_k}$ $(k = \overline{1,\ n})$ каби белгилаймиз. $\frac{\mathscr{P}_k}{Q_k}$ қисқармас каср бўлганидан ${}_n = m$, $Q_n = a$ бўлади, у ҳолда 8-§ даги ${}_n Q_{n-1} - {}_{n-1} Q_n = (-1)^n$ тенглик $mQ_{n-1} - \mathscr{P}_{n-1} a = (-1)^n$ шаклни олади. Охирги тенгликдан $a\mathscr{P}_{n-1} = -(-1)^n + mQ_{n-1}$ ёки $a\mathscr{P}_{n-1} \equiv \equiv (-)1^{n-1} \pmod{m}$ ҳосил бўлади. Охирги таққосламанинг иккала қисмини $(-1)^{n-1} \cdot b$ ва кўпайтириб,

$$a(-1)^{n-1} \cdot b\mathscr{P}_{n-1} \equiv b \pmod{m} \qquad (2)$$

таққосламага эга бўламиз. (1) ва (2) ни солиштириб,

$$x \equiv (-1)^{n-1} \cdot b\mathscr{P}_{n-1} \pmod{m} \qquad (3)$$

таққосламани ҳосил қиламиз. Бу ерда $\mathscr{P}_{n-1}$ сон $\frac{m}{a}$ касрнинг $(n-1)$- муносиб касрининг суратидан иборат. (1) таққослама ягона ечимга эга бўлгани учун (3) ечим (1) нинг ечими бўлади.

4-мисол. $285x \equiv 117 \pmod{924}$ таққосламани ечинг.

$$(285;\ 924) = 3,\ 177/3$$

бўлганидан таққосламанинг модули ва иккала қисмини 3 га бўлиб, ушбу

$$95x \equiv 59 \pmod{308}$$

таққосламани ҳосил қиламиз. Энди $\frac{308}{95}$ касрни муносиб касрларга ёямиз. Бунинг учун кетма-кет бўлишни қуйидагича бажарамиз:

$$308 = 95 \cdot 3 + 23,$$
$$95 = 23 \cdot 4 + 3,$$
$$23 = 3 \cdot 7 + 2,$$
$$3 = 2 \cdot 1 + 1,$$
$$2 = 1 \cdot 2$$
$$q_1 = 3,\ q_2 = 4,\ q_3 = 7,\ q_4 = 1,\ q_5 = 2,$$

8-§ да баён қилинган усулга асосан қуйидаги жадвални тузамиз:

q_k		3	4	7	1	2
$\mathcal{P}_k$	1	3	13	94	107	308

Демак, $\mathcal{P}_{n-1} = \mathcal{P}_4 = 107$ экан. Бундан

$$x \equiv (-1)^4 \cdot 107 \cdot 59 \pmod{308}$$

ёки

$$x \equiv 153 \pmod{308}.$$

У ҳолда берилган таққослама ечимлари қуйидагилар бўлади:

$$x \equiv 153,\ 461,\ 769 \pmod{924}.$$

29-§. Туб модулли юқори даражали таққосламалар

Таққосламаларнинг 10-хоссасига асосан, ҳар қандай мураккаб модулли таққосламаларни доимо туб модулли таққосламаларга келтириш мумкин эди. Энди биз туб модулли таққосламалар билан шуғулланайлик.

Таъриф. $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_h$ кўпҳад $a_i \in Z$ ва $m > 1$ бўлиб, $a_0 \times m$ бўлса, у ҳолда ушбу

$$f(x) \equiv 0 \pmod m \qquad (1)$$

таққослама *n — даражали бир номаълумли таққослама* дейилади.

(1) таққосламани тўғри сонли таққосламага айлантирувчи $x_0 + mt$ $(t \in Z)$ синф шу *таққосламанинг ечими* дейилади. $x_0 + mt$ синфининг битта элементи бўлган x_0 сон m модуль бўйича тузилган чегирмаларнинг тўла системасига тегишлидир. Шунинг учун m модуль бўйича тузилган тўла системанинг чегирмалари (1) ни қаноатлантирса, бу таққосламанинг ечимлари сони ҳам шунча бўлади.

Ечимлари тўплами устма-уст тушган таққосламалар одатда *тенг кучли таққосламалар* деб аталади.

Агар (1) таққосламанинг иккала қисмига ихтиёрий кўпҳад қўшилса, у ҳолда ҳосил бўлган таққослама (1) таққосламага тенг кучли таққослама бўлади. Агар (1) таққосламанинг иккала қисми m модуль билан ўзаро туб бўлган k сонга кўпайтирилса, у ҳолда ҳосил бўлган таққослама (1) таққосламага тенг кучли бўлади. Агар (1) таққосламанинг иккала қисми ва модули k натурал сонга кўпайтирилса, у ҳолда ҳосил бўлган таққослама берилган таққосламага тенг кучли таққослама бўлади.

Фараз қилайлик, бизга коэффициентлари Z сонлар ҳалқасига тегишли бир номаълумли n- даражали таққослама берилган бўлиб, унинг модули туб сондан иборат бўлсин, яъни

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv$$
$$\equiv 0 \pmod p$$

(p — туб сон $a_0 \times p$) бўлсин.

Аввало барча a_i $(i = \overline{0, n})$ коэффициентларни p модулга кўра абсолют қиймат бўйича энг кичик қолдиқлар билан алмаштириб оламиз. Масалан,

$$25x^3 + 17x^2 - 13 \equiv 0 \pmod{11}$$

таққосламани $25 \equiv 3 \pmod{11}$, $17 \equiv -5 \pmod{11}$, $13 \equiv \equiv 2 \pmod{11}$ бўлгани учун

$$3x^3 - 5x^2 - 2 \equiv 0 \pmod{11} \qquad (2)$$

кўринишда ёзиш мумкин. $(a_0; p) = 1$ бўлганидан

$$a_0y \equiv 1 \pmod p \qquad (3)$$

таққослама доимо ягона ечимга эга бўлади. (3) таққосламани y га нисбатан ечиб, бу топилган ечимга (2) нинг иккала қисмини кўпайтирсак, x^n олдидаги коэффициент 1 га тенг бўлиб қолади. Ҳақиқатан, (2) таққосламанинг иккала қисмини $3y \equiv 1 \pmod{11}$ таққосламанинг ечими бўлган $y \equiv 4 \pmod{11}$ га кўпайтирсак, у $x^3 + 2x^2 + 3 \equiv 0 \pmod{11}$ кўринишни олади. Умуман олганда қуйидаги теорема ўринли:

1-теорема. *Даражаси n $(n > p)$ га тенг бўлган, p туб модулли таққослама даражаси $p-1$ дан катта бўлмаган таққосламага тенг кучли бўлади.*

Исботи. Қолдиқли бўлиш ҳақидаги теоремага асосан, $n \in N$ ва $p-1 \in N$ лар учун қуйидаги тенгликни ёза оламиз:

$$n = (p-1) \cdot k + r \quad (1 \leqslant r \leqslant p-1).$$

Биз бу ерда қолдиқни 0 дан $p-2$ гача олмасдан 1 дан $p-1$ гача олдик, чунки $p-1$ модуль бўйича чегирмаларнинг тўла системаси сифатида 0, 1, 2, ..., $p-2$ ёки 1, 2, 3, ..., $p-1$ системани олиш мумкин. Бундан ташқари Ферма теоремасига асосан,

$$x \equiv x^p \pmod{p}$$

таққослама ўринли. Бу таққосламанинг иккала қисмини кетма-кет

$$x^{r-1},\ x^{(p-1)\cdot 1+(r-1)},\ x^{(p-1)\cdot 2+(r-1)},\ \ldots,\ x^{(p-1)(k-1)+(r-1)}$$

га кўпайтирамиз. Унда қуйидаги таққосламалар ҳосил бўлади:

$$x^r \equiv x^{(p-1)\cdot 1+r} \pmod{p},$$
$$x^{(p-1)\cdot 1+r} \equiv x^{(p-1)\cdot 2+r} \pmod{p},$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$x^{(p-1)(k-1)+r} \equiv x^{(p-1)k+r} \pmod{p}.$$

Агар бу таққосламаларни ҳадлаб кўпайтирсак ва ҳосил бўлган таққосламанинг иккала қисмини умумий кўпайтувчига бўлсак, у ҳолда

$$x^r \equiv x^{(p-1)\cdot k+r} \pmod{p}, \quad 1 \leqslant r \leqslant p-1 \qquad (4)$$

таққослама ҳосил бўлади. $n = (p-1) \cdot k + r$ ва (2) таққосламага асосан

$$x^n = x^r \pmod{p}, \quad 1 \leqslant r \leqslant p-1$$

га эга бўламиз.

Мисол. $x^{19}+3x^{17}-3x^{11}-x^5+3x^2-1\equiv 0 \pmod 7$ таққослама берилган бўлсин. Бу ерда $7-1=6$ бўлгани учун юқоридаги таққосламани

$$x+3x^5-3x^5-x^5+3x^2-1\equiv 0 \pmod 7$$

ёки

$$x^5-3x^4-x+1\equiv 0 \pmod 7$$

шаклда ёзиш мумкин.

2-теорема. *Туб модулли n-даражали таққослама ечимлари сони n тадан ортиқ эмас.*

Исботи. Фараз қилайлик, (2) таққослама берилган бўлиб, $x\equiv x_1 \pmod p$ унинг ечими бўлсин, яъни

$$f(x_1)\equiv 0 \pmod p \tag{5}$$

таққослама ўринли бўлсин. У ҳолда Безу теоремасига асосан

$$f(x)=(x-x_1)f_1(x)+f(x_1)$$

бўлади, бу ерда $f_1(x)$ даражаси $n-1$ дан катта бўлмаган кўпҳад, $f(x_1)$ эса p га қолдиқсиз бўлинадиган сон. (5) га асосан (2) таққосламани

$$f(x)\equiv(x-x_1)f_1(x) \pmod p \tag{6}$$

кўринишда ёза оламиз. (2) ва (6) дан $(x-x_1)f_1(x)\equiv\equiv 0 \pmod p$ таққослама ҳосил бўлади.

Агар $f_1(x)\equiv 0 \pmod p$ таққослама бирор $x\equiv\equiv x_2 \pmod p$ каби ечимга эга бўлса, x нинг барча бутун қийматларида айнан бажарилувчи

$$f(x)\equiv(x-x_2)f_2(x) \pmod p$$

таққосламага эга бўламиз. Энди юқоридаги фикрларни $f_2(x)$ га нисбатан қўллаш мумкин. Бу жараённи давом эттириб, қуйидаги иккита тасдиқдан бири доимо ростлигига ишонч ҳосил қиламиз:

1. k қадамдан сўнг умуман ечимга эга бўлмаган $(n-k)$-даражали

$$f_k(x)\equiv 0 \pmod p \tag{7}$$

таққосламага эга бўламиз.

2. $a_0(x-x_n)\equiv 0 \pmod p$ кўринишдаги биринчи даражали таққосламага эга бўламиз.

1-ҳолда (2) таққосламани

$$f(x)\equiv(x-x_1)(x-x_2)\ \ldots\ (x-x_k)f_k(x) \pmod p \tag{8}$$

кўринишга, 2- ҳолда эса

$$f(x)\equiv a_0(x-x_1)(x-x_2)\dots(x-x_h)\ (\mathrm{mod}\,p)\qquad(9)$$

кўринишга келтирамиз. 1- ҳолда (2) таққослама x_1, x_2, ..., x_k лардан бошқа ечимга эга бўлмайди. Ҳақиқатан, $x\equiv x_{k+1}\ (\mathrm{mod}\,p)$ ечим мавжуд бўлиб, $x_{k+1}\not\equiv x_1$, x_2, ..., $x_k\ (\mathrm{mod}\,p)$ бўлса, у ҳолда

$$f_k(x_{k+1})=0\ \ (\mathrm{mod}\,p)$$

таққослама рост бўлади. Бу эса (7) таққосламанинг ечимга эга бўлмаслигига зиддир.

3-теорема. *Агар n- даражали туб модулли таққосламанинг ечимлари сони n дан ортиқ бўлса, у ҳолда унинг барча коэффициентлари p га бўлинади.*

Исботи. Фараз қилайлик, x_1, x_2, ..., x_n, x_{n+1} лар (2) таққосламанинг ечимлари бўлсин. $f(x)=a_0x^n+a_1x^{n-1}+\dots+a_n$ кўпҳадни $f(x)=a_0(x-x_1)(x-x_2)\dots(x-x_h)+b(x-x_1)(x-x_2)\dots(x-x_{n-1})+\dots+l(x-x_1)+m$ кўринишда ёзиш мумкин. Бу ерда x_i $(i=\overline{1,\ n})$ таққослама ечимлари. b, ..., l, m лар кўпҳадлар тенглиги таърифга асосланиб топилади.

$x=x_1$ бўлса, $f(x_1)=m$ бўлади ва m/p, чунки $f(x_1)/p$ $x=x_2$ бўлсин, у ҳолда $f(x_2)=l(x_2-x_1)+m$ га эга бўламиз. Бундан $f(x_2)/p$ ва m/p бўлгани учун $l(x_2-x_1)/p$ бўлади. Лекин $x_2-x_1\times p$ дан l/p бўлади. Шундай давом эттириб, $x=x_{n+1}$ қиймат берамиз.

$$f(x_{n+1})=a_0(x_{n+1}-x_1)\ x_{n+1}-x_2)\dots(x_{n+1}-x_n)\ (\mathrm{mod}\,p)$$

таққосламадан a_0/p.

a_1, a_2, ..., a_n лар a_0, b, ..., l, m сонларнинг алгебраик йиғиндиси бўлгани учун улар ҳам p га бўлинади.

Эслатма. Мураккаб модулли таққослама учун 1-теорема ўринли бўлмайди.

Масалан, $x^2-5x+6\equiv 0\ (\mathrm{mod}\ 6)$ таққослама $x\equiv 0, 2, 3, 5\ (\mathrm{mod}\ 6)$ лардан иборат тўртта ечимга эга.

4-теорема (исботсиз). *Бош коэффициенти 1 га тенг бўлган n $(n>p)$ даражали $f(x)=0\ (\mathrm{mod}\,p)$ таққослама p та ечимга эга бўлиш учун $f(x)$ ни x^p-x га бўлишдан ҳосил бўлган $r(x)$ қолдиқ кўпҳаднинг барча коэффициентлари p га бўлиниши зарур ва етарли.*

30-§. Квадратик чегирма ва квадратик чегирмамаслар

Иккинчи даражали бир номаълумли таққосламаларни ечиш икки номаълумли иккинчи даражали тенгламаларни бутун сонлар тўпламида ечиш масаласи билан узвий боғлиқдир.

1-таъриф. Ушбу

$$ax^2+bx+c\equiv 0 \pmod m \ (a\not\times m) \qquad (1)$$

кўринишдаги таққослама *иккинчи даражали (квадратик) бир номаълумли таққослама* дейилади.

(1) ни доимо

$$ax^2+bx+c=my \qquad (2)$$

шаклда ёзиш мумкин. (2) эса иккинчи даражали икки номаълумли тенгламанинг хусусий ҳолидир.

Теорема. (1) *кўринишдаги квадратик таққосламани ҳар доим*

$$x^2\equiv d \pmod{m_1} \qquad (3)$$

кўринишга келтириш мумкин.

Ҳақиқатан, таққосламанинг хоссасига асосан (1) нинг иккала қисмини ва модулини $4a$ га кўпайтирамиз, у ҳолда

$$4a^2x^2+4abx+4ac\equiv 0 \pmod{4ma}$$

ёки

$$(2ax+b)^2-b^2+4ac\equiv 0 \pmod{4ma},$$
$$2ax+b=y$$

десак, охирги таққослама

$$y^2\equiv b^2-4ac \pmod{4ma} \qquad (4)$$

кўринишга келади. Ниҳоят, $b^2-4ac=d$, $4ma=m_1$ белгилаш киритиб,

$$y^2\equiv d \pmod{m_1} \qquad (5)$$

таққосламани ҳосил қиламиз. (1) нинг ҳар бир ечими (4) ни ҳам қаноатлантиради. Лекин (4) нинг ҳар бир ечими (1) нинг ҳам ечими бўлавермайди. (4) нинг ечимлари орасидан (1) нинг ҳам ечими бўладиганларини танлаб олиш учун $x=\frac{y-b}{2a}$ га эътибор бериш лозим. Агар шу нисбат бутун сон бўлса, (4) ни қаноатлантирувчи ечим (1) нинг ҳам ечими бўлади.

Амалий машғулотларда (1) дан (5) га ўтиш учун юқоридаги барча жараёнларни бажариш шарт эмас. Унинг ўрнига, таққосламанинг чап қисмини бирор ифоданинг тўлиқ квадратига келтириб олиш лозим.

Мисоллар. 1. $4x^2-11x-3\equiv 0 \pmod{13}$. $11\equiv 24 \pmod{13}$, $3\equiv 16 \pmod{13}$ бўлгани учун $4x^2-24x-16\equiv 0 \pmod{13}$ бўлади. $(4; 13)=1$ бўлгани учун охирги таққосламадан

$$x^2-16x-4\equiv 0 \pmod{13},$$
$$(x-3)^2-13\equiv 0 \pmod{13},$$
$$(x-3)^2\equiv 0 \pmod{13},$$
$$x\equiv 3 \pmod{13}$$

келиб чиқади.

2.
$$3x^2+7x+8\equiv 0 \pmod{17},$$
$$3x^2+24x-9\equiv 0 \pmod{17},$$
$$x^2+8x-3\equiv 0 \pmod{17},$$
$$(x+4)^2\equiv 19 \pmod{17},$$
$$(x+4)^2\equiv 2 \pmod{17},$$
$$(x+4)^2\equiv 2+34 \pmod{17},$$
$$x+4\equiv \pm 6 \pmod{17}, \text{ яъни}$$
$$x+4\equiv 6 \pmod{17},$$
$$x+4\equiv -6 \pmod{17}.$$

Булардан $x_1\equiv 2 \pmod{17}$, $x_2\equiv -10 \pmod{17}$ келиб чиқади.

(5) кўринишдаги таққосламалар одатда икки ҳадли таққосламалар деб аталади.

2-таъриф Агар $(a; m)=1$ бўлганда $x^2\equiv a \pmod{m}$ таққослама ечимга эга бўлса, a га m *модуль бўйича квадратик чегирма*, акс ҳолда a га m *модуль бўйича квадратик чегирмамас* дейилади.

3-таъриф. Агар $(a; m)=1$ бўлганда $x^n\equiv a \pmod{m}$ таққослама ечимга эга бўлса, a га m модуль бўйича *n-даражали чегирма*, акс ҳолда *n-даражали чегирмамас* дейилади.

m_1 модуль мураккаб сон бўлса, у ҳолда (5) таққослама қуйидаги уч хил таққосламага келтирилади:

1. $x^2\equiv d \pmod{p}$ (p — тоқ туб сон);
2. $x^2\equiv d \pmod{p^\beta}$ (p — тоқ туб сон, $\beta>1$),
3. $x^2\equiv d \pmod{2^\alpha}$ ($\alpha\geqslant 1$).

31-§. Тоқ туб модулли иккинчи даражали таққосламаларни ечиш

Ушбу

$$x^2 \equiv a \pmod p \quad ((a; p) = 1,\ (2; p) = 1) \qquad (1)$$

икки ҳадли иккинчи даражали таққослама берилган бўлиб, унинг модули тоқ туб сон бўлсин.

Агар $a \equiv 0 \pmod p$ бўлса, берилган таққослама $x^2 \equiv 0 (\mathrm{mod}\, p)$ кўринишда бўлиб, бу таққосламанинг ечими $x \equiv 0 \pmod p$ бўлади. Шу ҳолда ва фақат шу ҳолдагина берилган таққослама ноль ечимга эга бўлади.

Модуль тоқ туб сон бўлгани учун (1) таққосламанинг ечими модуль бўйича чегирмаларнинг келтирилган системасига тегишли бўлади.

1-теорема. *Агар* $x \equiv x_1 \pmod p$ (1) *нинг ечими бўлса,* $x \equiv -x_1 (\mathrm{mod}\, p)$ ҳам (1) *нинг эчими бўлади.*

Исботи. $x_1^2 \equiv (-x_1)^2 \pmod r$ ўринли. Демак x_1 (1) ни қаноатлантирса, $(-x_1)$ ҳам (1) ни қаноатлантиради.

Маълумки, таққослама ечимининг аниқланишига асосан ҳар бир ечимга битта синф мос келади. Биз x_1 ва $-x_1$ лар p модуль бўйича турли синф вакиллари эканини кўрсатишимиз лозим.

Тескарисини фараз қилайлик, яъни x_1 ва $-x_1$ лар p модуль бўйича битта синфга тегишли бўлсин. Унда

$$(x_1 \equiv -x_1 (\mathrm{mod}\, p)) \Rightarrow (2x_1 \equiv 0 (\mathrm{mod}\, p)) \Rightarrow (x_1 \equiv 0 (\mathrm{mod}\, p)),$$

чунки $(2; p) = 1$. Лекин охирги таққослама $(a; p) = 1$, деган шартга зиддир. Демак, x_1 ва $(-x_1)$ лар p модуль бўйича турли синфларга тегишли.

Туб модулли иккинчи даражали таққосламаларни модуль етарлича кичик бўлганда синаш усули билан ечиш мақсадга мувофиқдир. Бунинг учун p модуль бўйича чегирмаларнинг келтирилган

$$\pm 1,\ \pm 2,\ \pm 3, \ldots, \pm \frac{p-1}{2} \qquad (2)$$

системасидаги ҳар бир чегирмани кетма-кет (1) га қўйиб ўтирмасдан x ни $1, 2, 3, \ldots, \frac{p-1}{2}$ лар билан алмаштириш кифоя. Бундай ҳолда чап томонда

$$1^2,\ 2^2,\ 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \qquad (3)$$

сонлар ҳосил бўлади.

2-теорема. (3) *сонларнинг ҳар бири p модуль бўйича турли синфларга тегишли бўлади.*

Исботи. Тескарисини фараз қилайлик, яъни $1 \leqslant k < l \leqslant \frac{p-1}{2}$ бўлганда $k^2 \equiv l^2 \ (\mathrm{mod}\, p)$ бўлсин.

$$k^2 - l^2 \equiv 0 \ (\mathrm{mod}\, p) \Rightarrow (k+l)(k-l) \equiv 0 \ (\mathrm{mod}\, p).$$

$0 < k+l < p$ ва $0 < l-k < p$ бўлгани учун охирги таққослама бажарилмайди.

1-натижа. p модуль бўйича тузилган чегирмаларнинг келтирилган системасидаги $\frac{p-1}{2}$ чегирма квадратик чегирма, $\frac{p-1}{2}$ таси эса квадратик чегирмамас бўлади.

Мисол. 11 модуль бўйича энг кичик мусбат квадратик чегирмаларни топинг.

Бу чегирмаларни топиш учун қуйидаги ҳисоблашларни бажарамиз.

$\frac{11-1}{2} = 5$ бўлганидан 1, 2, 3, 4, 5 ларнинг квадратларини қараб чиқамиз: $1^2 \equiv 1 \ (\mathrm{mob}\, 11)$, $2^2 \equiv 4 \ (\mathrm{mod}\, 11)$,

$$3^2 \equiv 9 \ (\mathrm{mod}\, 11), \ 4^2 \equiv 5 \ (\mathrm{mod}\, 11), \ 5^2 \equiv 3 \ (\mathrm{mod}\, 11).$$

Демак, 11 модуль бўйича квадратик чегирмалар 1, 4, 9, 5, 3 лар бўлиб, квадратик чегирмамаслар эса 2, 6, 7, 8, 10 лар бўлади.

2-натижа. Агар (1) таққослама ечимга эга бўлса, у ҳолда у фақат 2 та ечимга эга бўлади.

3-теорема (Эйлер критерийси). *Агар* $(a, p) = 1$ *бўлиб,* $a^{\frac{p-1}{2}} \equiv 1 \ (\mathrm{mod}\, p)$ *ўринли бўлса,* (1) *таққослама иккита ечимга эга бўлади,*

$$a^{\frac{p-1}{2}} \equiv -1 \ (\mathrm{mod}\, p) \qquad (4)$$

ўринли бўлганда эса (1) *таққослама бирорта ҳам ечимга эга бўлмайди.*

Исботи. Ферма теоремасига асосан, $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ таққослама рост. p тоқ сон бўлгани учун $a^{p-1} - 1 \equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$ ўринли Бундан $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \ (\mathrm{mod}\, p)$ таққослама ҳосил бўлади. Охирги таққосламага асосан, $a^{\frac{p-1}{2}} - 1$ ва $a^{\frac{p-1}{2}} + 1$ кўпайтувчилардан камида биттаси p га бўлиниши шарт. Бу иккала кўпайтувчи бир вақтда p га бўлинмайди, акс ҳолда уларнинг айирмаси бўлган ± 2 ҳам p га бўлинган бўларди, лекин p тоқ туб сон бўлгани учун $2 \times p$.

Агар a квадратик чегирма бўлса, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ бўлади. Ҳақиқатан, бундай ҳолда x нинг шундай қиймати мавжудки, бу қиймат учун $(x; p) = 1$ бўлганда $a \equiv x^2 \pmod{p}$ бўлади. Бундан $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \pmod{p} \Rightarrow x^{p-1} \equiv 1 \pmod{p}$ бўлиб, 1-натижага асосан p модуль бўйича $\frac{p-1}{2}$ та квадратик чегирма мавжуд. (1) таққослама туб модулли бўлгани учун унинг ечимлари сони таққослама даражасидан, яъни $\frac{p-1}{2}$ дан ортиқ бўла олмайди. Демак, (1) барча квадратик чегирмалар учунгина ўринли бўлади. У ҳолда $(a; p) = 1$ шартни қаноатлантирувчи квадратик чегирмамас a лар ва фақат шулар учун $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ ўринли бўлади.

32-§. Лежандр символи

Ушбу

$$x^2 \equiv a \pmod{p}, \quad (a; p) = 1 \tag{1}$$

таққосламанинг модули етарлича катта сон бўлганда Эйлер критерийсидан фойдаланиш унчалик қулай эмас. Бундай ҳолларда Лежандр символи деб аталувчи ва $\left(\frac{a}{p}\right)$ каби белгиланувчи символдан фойдаланилади.

Таъриф. Қуйидаги шартларни қаноатлантирувчи $\left(\frac{a}{p}\right)$ символ *Лежандр символи* дейилади:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{агар } a \text{ сон } p \text{ тоқ туб модуль бўйича квадратик чегирма бўлса;} \\ -1, & \text{агар } a \text{ сон } p \text{ тоқ туб модуль бўйича квадратик чегирмамас бўлса.} \end{cases}$$

$\left(\frac{a}{p}\right)$ символ a сондан p бўйича тузилган *Лежандр символи* деб аталади, бу ерда a Лежандр символининг *сурати*, p эса Лежандр символининг *махражи* дейилади.

Мисол. $\left(\frac{7}{19}\right)=1$, чунки Эйлер критерийсига асосан, $7^{\frac{19-1}{2}} \equiv 1 \pmod{19}$ бўлгани учун 7 сон 19 модуль бўйича квадратик чегирмадир. 5 сон 17 модуль бўйича квадратик чегирмамас бўлганлигидан $\left(\frac{5}{17}\right)=-1$ бўлади.

Маълумки, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ эканлигига қараб, a квадратик чегирма ёки квадратик чегирмамас бўларди. Демак, Лежандр символи ва Эйлер критерияларига асосан, қуйидагини ёза оламиз:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \qquad (2)$$

Энди Лежандр символининг қуйидаги баъзи бир хоссаларини кўриб ўтамиз:

$$1^\circ.\ a \equiv a_1 \pmod{p} \Rightarrow \left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right). \qquad (3)$$

Ҳақиқатан, битта синфнинг элементлари берилган модуль бўйича ё квадратик чегирма, ёки квадратик чегирмамас бўлади. Бунга асосан, (3) нинг тўғрилиги келиб чиқади. Бу хоссадан фойдаланиб, ҳар қандай $k \in Z$ учун қуйидагини ёза оламиз: $\left(\frac{a}{p}\right)=\left(\frac{kp+a_1}{p}\right)$, $\left(\frac{kp+a_1}{p}\right)=\left(\frac{a_1}{p}\right)$ бўлгани учун $\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$ бўлади.

$$2^\circ.\ \left(\frac{1}{p}\right)=1.$$

Ҳақиқатан, $x^2 \equiv 1 \pmod{p}$ таққослама доимо ечимга эга бўлиб, $x \equiv \pm 1 \pmod{p}$ унинг ечимидир.

$$3^\circ.\ \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

(2) таққосламага асосан қуйидагини ёза оламиз:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \qquad (4)$$

Лекин $\left(\frac{-1}{p}\right)$ ва $(-1)^{\frac{p-1}{2}}$ ларнинг қиймати ± 1 дан фарқли эмас. Шу билан бир вақтда p тоқ туб сон бўлгани учун 1 ва -1 лар шу модуль бўйича таққосланувчи бўла олмайди. Демак, $\left(\frac{-1}{p}\right)$ ва $(-1)^{\frac{p-1}{2}}$ лар бир вақтда 1 га ёки -1 га тенг бўлади.

Натижа. $p=4m+1$ шаклдаги сонлар учун -1 квадратик чегирма, $p=4m+3$ шаклдаги сонлар учун эса -1 квадратик чегирмамас бўлади.

Ҳақиқатан,

$$\left(-\frac{1}{4m+1}\right)=(-1)^{2m}=1,$$

$$\left(-\frac{1}{4m+3}\right)=(-1)^{2m+1}=-1,$$

4°. $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right).$

Исботи. (2) таққосламага асосан қуйидагини ёзиш мумкин:

$$\left(\frac{a\cdot b}{p}\right)\equiv(a\cdot b)^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}}\cdot b^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\pmod{p}$$

ёки

$$\left(\frac{a\cdot b}{p}\right)\equiv\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\ (\mathrm{mod}\,p).$$

$a^{\frac{p-1}{2}}\cdot b^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(\mathrm{mod}\,p)$ таққосламанинг иккала қисми a ва b лар p модуль бўйича квадратик чегирма ёки квадратик чегирмамас бўлса, 1 га, a ва b ларнинг бири p модуль бўйича квадратик чегирма, иккинчиси эса квадратик чегирмамас бўлса, -1 га тенг. Шунинг учун $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$ тенгликни ёза оламиз.

Бу хоссадан қуйидаги натижалар келиб чиқади:

1-натижа. $\left(\frac{a^2}{p}\right)=1,\ \left(\frac{a\cdot b^2}{p}\right)=\left(\frac{a}{p}\right).$

2-натижа. Жуфт сондаги квадратик чегирмалар ёки квадратик чегирмамаслар кўпайтмаси доимо квадратик чегирма бўлади. Тоқ сондаги квадратик чегирмамаслар кўпайтмаси яна квадратик чегирмамас бўлади.

Мисол. $x^2 \equiv 426 \pmod{491}$ таққослама ечимга эгами?

Бу саволга жавоб бериш учун $\left(\frac{426}{491}\right)$ Лежандр символини тузамиз. $426 = 2 \cdot 3 \cdot 71$ шаклдаги сон бўлгани учун 4-хоссага асосан қуйидагича ёзамиз:

$$\left(\frac{426}{491}\right)=\left(\frac{2}{491}\right)\left(\frac{3}{491}\right)\cdot\left(\frac{71}{491}\right).$$

1. $\left(\frac{2}{491}\right) = -1$, чунки $491 \equiv 3 \pmod 8$.

2. $\left(\frac{3}{491}\right) = -\left(\frac{491}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$, чунки $491 \equiv 3 \pmod 4$ ва $3 \equiv 3 \pmod 4$ ҳамда $3 \equiv 3 \pmod 8$.

3. $\left(\frac{71}{491}\right) = -\left(\frac{491}{71}\right) = -\left(\frac{65}{71}\right) = -\left(\frac{5}{71}\right)\cdot\left(\frac{13}{71}\right) = -\left(\frac{71}{5}\right)\cdot\left(\frac{71}{13}\right) = -\left(\frac{1}{5}\right)\cdot\left(\frac{6}{13}\right) = -\left(\frac{2}{13}\right)\cdot\left(\frac{3}{13}\right) = -(-1)\left(\frac{13}{3}\right) = 1\cdot\left(\frac{1}{3}\right) = 1,$

чунки $491 \equiv 3 \pmod 4$, $71 \equiv 3 \pmod 4$, $491 \equiv 65 \pmod{71}$, $5 \equiv 1 \pmod 4$, $13 \equiv 1 \pmod 4$, $13 \equiv 5 \pmod 8$.

Демак, $\left(\frac{426}{491}\right) = (-1)\cdot 1 \cdot 1 = -1$, $\left(\frac{426}{491}\right) = -1$, бўлгани учун берилган таққослама ечимга эга эмас.

33-§. Бошланғич илдизлар ва кўрсаткичга тегишли сонлар

Эйлер теоремасига кўра $(a;\ m) = 1$ бўлганда

$$a^{\varphi(m)} \equiv 1 \pmod m \qquad (1)$$

таққослама ўринли. (1) таққосламанинг иккала қисмини k-даражага кўтариб

$$a^{k\varphi(m)} \equiv 1 \pmod m \qquad (2)$$

га эга бўламиз. (1) ва (2) ни умумлаштириб қуйидаги хулосага келамиз: агар $(a;\ m) = 1$ бўлса, ҳар доим шундай γ натурал сон топиладики,

$$a^{\gamma} \equiv 1 \pmod m \qquad (3)$$

таққослама ўринли бўлади ((1) га асосан).

Биз ушбу қўлланманинг биринчи қисмида натурал сонлар системасини қурганда ҳар қандай натурал сонлар тўплами доимо энг кичик элементга эга эканини кўрган эдик. Шунга кўра (3) таққосламани қаноатлантирувчи натурал сонлар тўпламининг энг кичик элементи мавжуд. Уни δ орқали белгилайлик, яъни $\delta = \min \gamma$ бўлсин.

1-таъриф. Агар $(a; m) = 1$ бўлганда

$$a^{\delta} \equiv 1 \pmod{m} \qquad (4)$$

таққослама ўринли бўлса, у ҳолда δ сон *а сонининг т модулга кўра кўрсаткичи ёки т модуль бўйича а сонига тегишли кўрсаткич* дейилади.

Бу таърифга асосан, $\delta \leqslant \varphi(m)$ бўлади.

2-таъриф. Агар $(a; m) = 1$ бўлиб, $\delta = \varphi(m)$ бўлса, у ҳолда a сон m модуль бўйича *бошланғич илдиз* дейилади.

m модуль бўйича бирор a сонига тегишли кўрсаткични топишни қуйидаги мисолларда кўриб ўтамиз:

1-мисол. $m = 7$ модуль бўйича 2, 3, 5 сонларга тегишли бўлган кўрсаткичларни топинг.

а) $a = 2$ бўлсин, $\varphi(7) = 6$ бўлгани учун $2^1, 2^2, 2^3, 2^4, 2^5, 2^6$ даражаларни 7 модуль бўйича кўриб чиқамиз:

$$2 \equiv 2 \pmod 7,$$
$$2^2 \equiv 4 \pmod 7,$$
$$2^3 \equiv 1 \pmod 7.$$

Демак, таърифга кўра 2 сон 7 модуль бўйича 3 кўрсаткичга тегишли.

б) $a = 3$ бўлсин. У ҳолда

$$3 \equiv 3 \pmod 7,$$
$$3^2 \equiv 2 \pmod 7,$$
$$3^3 \equiv -1 \pmod 7,$$
$$3^4 \equiv 4 \pmod 7,$$
$$3^5 \equiv 5 \pmod 7,$$
$$3^6 \equiv 1 \pmod 7.$$

Демак, 3 сонининг 7 модуль бўйича кўрсаткичи 6 га тенг экан.

в) $a = 5$ бўлсин. У ҳолда

$$5 \equiv 5 \pmod 7,$$
$$5^2 \equiv 4 \pmod 7,$$
$$5^3 \equiv 20 \equiv -1 \pmod 7,$$
$$5^4 \equiv 16 \equiv 2 \pmod 7,$$
$$5^5 \equiv 24 \equiv 3 \pmod 7,$$
$$5^6 \equiv 1 \pmod 7.$$

Бундан 5 сонининг 7 модуль бўйича кўрсаткичи ҳам 6 га тенг. б) ва в) ларда $\varphi(7)=6$ бўлгани учун 3 ва 5 сонлари 7 модуль бўйича бошланғич илдизни ташкил этади. Демак, битта модуль бўйича ҳар хил бошланғич илдизлар мавжуд экан.

1-теорема. *Бирор m модуль бўйича тузилган битта синфнинг чегирмалари шу модуль бўйича бир хил кўрсаткичга тегишли бўлади.*

Исботи. Теоремани тескаридан исбот қилайлик, a ва a_1 чегирмалар m модуль бўйича битта чегирмалар синфидан олинган бўлсин.

$a \equiv a_1 (\bmod m)$ бўлиб, $a^{\delta} \equiv 1 (\bmod m)$ ва $a_1^{\delta_1} \equiv (1 \bmod m)$ ҳамда $\delta \neq \delta_1$ бўлсин. Аниқлик учун $\delta < \delta_1$ (ёки $\delta > \delta_1$) деб оламиз. $\delta < \delta_1$ бўлиши мумкин эмас, чунки $a^{\delta} \equiv 1 (\bmod m)$ ва $a \equiv a_1 (\bmod m)$ лигидан охирги таққосламани δ даражага кўтариб, $a^{\delta} \equiv a_1^{\delta} (\bmod m)$ га эга бўламиз. У ҳолда $a^{\delta} \equiv 1 (\bmod m)$ эканидан $a_1^{\delta} \equiv 1 (\bmod m)$ бўлади. a_1 сон δ_1 кўрсаткичга тегишли бўлгани учун, таърифга асосан, $\delta_1 \leqslant \delta$ га эга бўламиз. Бу эса $\delta < \delta_1$ шартга зид. Энди $\delta > \delta_1$ деб фараз қиламиз ва $a \equiv a_1 (\bmod m)$ нинг иккала қисмини δ_1 даражага кўтарамиз:

$$a^{\delta_1} \equiv a_1^{\delta_1} (\bmod m) \Rightarrow a^{\delta_1} \equiv 1 (\bmod m).$$

a сон m модуль бўйича δ кўрсаткичга тегишли бўлгани учун

$$\delta \leqslant \delta_1$$

$$(\delta \leqslant \delta_1) \wedge (\delta_1 \leqslant \delta) \Rightarrow \delta_1 = \delta.$$

Демак, агар бирор a сон m модуль бўйича бирор δ кўрсаткичга тегишли бўлса, a билан m модуль бўйича тенг қолдиқлар синфининг барча элементлари ҳам шу кўрсаткичга тегишли бўлади, яъни берилган модуль бўйича битта кўрсаткичга тегишли бўлган сонлар синфи тўғрисида гапириш мумкин.

m модуль бўйича δ кўрсаткичга тегишли бўлган ҳар бир a сони m билан ўзаро туб бўлиши лозим, акс ҳолда, яъни $(a; m) = d > 1$ бўлса, $a^{\gamma} \equiv 1 (\bmod m)$ таққослама ўринли бўлмайди.

Агар a сони m модуль бўйича бошланғич илдиз бўлса, у ҳолда биз бошланғич илдизлар синфи ҳақида фикр юритамиз.

2-теорема. *Агар $(a; m) = 1$ бўлганда*

$$a^{\delta} \equiv 1 (\bmod m) \tag{5}$$

бўлса, у ҳолда

$$a^0, a^1, \ldots, a^{\delta-1} \qquad (6)$$

сонлар системаси m модуль бўйича ўзаро таққосланмайди.

Исботи. Исботни тескарисини фараз қилиш усули билан бажарамиз. Фараз қилайлик, k ва l лар ихтиёрий натурал сонлар бўлганда $a^k \equiv a^l \pmod m$ таққослама рост бўлиб, бунда $\delta - 1 \geqslant l > k \geqslant 0$ бўлсин. $(a^k; m) = 1$ бўлгани учун юқоридаги таққосламанинг иккала қисмини a^k га бўлиб

$$a^{l-k} \equiv 1 \pmod m \quad (0 < l - k < \delta)$$

таққосламага эга бўламиз. Лекин бу таққосламанинг ўринли бўлиши мумкин эмас, чунки a сон m модуль бўйича δ кўрсаткичга тегишли.

1-натижа. $\delta = \varphi(m)$ бўлганда (3) система m модуль бўйича чегирмаларнинг келтирилган системасини ташкил қилади.

Ҳақиқатан, 1. (6) системада $\varphi(m)$ та элемент мавжуд;

2. $(a; m) = 1 \Rightarrow (a^k; m) = 1$;

3. a^k элементларнинг ҳар бири 2-теоремага асосан, m модуль бўйича турли синфларга тегишли. Бу учта шарт (6) нинг келтирилган чегирмалар системасини билдиради.

2-натижа. Агар m модуль туб сон бўлса, яъни $m = p$ бўлиб ва a сон p модуль бўйича бошланғич илдиз бўлса, у ҳолда (6) қатор

$$a^0. a^1, \ldots, a^{p-2} \qquad (7)$$

кўринишда бўлади.

2-мисол. 7 модуль бўйича 5 бошланғич илдиз учун (7) кўринишдаги системани тузинг.

$1 = 3^0, 3, 3^2, 3^3, 3^4, 3^5$ ни тузамиз ва ҳар бир даражани 7 модуль бўйича энг кичик мусбат чегирмалар билан алмаштирамиз. Улар қуйидагилардан иборат (1-б мисол):

$$1, 3, 2, 6, 4, 5.$$

Ҳақиқатан, бу система 7 модуль бўйича чегирмаларнинг келтирилган системасидан иборатдир.

3-теорема. *a сон m модуль бўйича δ кўрсаткичга тегишли бўлса, у ҳолда ушбу*

$$a^{\gamma} \equiv a^{\gamma_1} \pmod m \qquad (8)$$

таққосламанинг ўринли бўлиши учун

$$\gamma = \gamma_1 (\bmod \delta) \qquad (9)$$

таққосламанинг ўринли бўлиши зарур ва етарлидир.

Исботи. 1) Зарурийлиги. a сон m модуль бўйича δ кўрсаткичга тегишли ва $a^{\gamma} \equiv a^{\gamma_1} (\bmod m)$ таққослама ўринли бўлсин. У ҳолда γ ва γ_1 ларни қуйидагича ёзиб оламиз:

$$\gamma = \delta q + r, \ \gamma_1 = \delta q_1 + r_1 \ (0 \leqslant r < \delta, \ 0 \leqslant r_1 \quad \delta)$$

ва $r = r_1$ эканини кўрсатамиз. γ ва γ_1 ларнинг бу қийматларини (7) га қўямиз. У ҳолда

$$a^{\delta q + r} \equiv a^{\delta q_1 + r_1} (\bmod m) \Rightarrow (a^{\delta})^{q} \cdot a^{r} \equiv (a^{\delta})^{q_1} \cdot a^{r_1} (\bmod m)\cdot$$

Лекин $a^{\delta} \equiv 1 \ (\bmod m)$ бўлгани учун охирги таққослама $a^{r} \equiv a^{r_1} (\bmod m)$ кўринишни олади.

Юқорида кўриб ўтилган 2-теоремага асосан охирги таққослама фақатгина $r = r_1$ бўлгандагина ўринли бўлади. Демак, $r = r_1$ ва $\gamma \equiv \gamma_1 \ (\bmod m)$.

2. Етарлилиги. $a^{\delta} \equiv 1 (\bmod m)$ ва $\gamma \equiv \gamma_1 (\bmod \delta)$ таққосламалар ўринли бўлсин. Иккинчи таққосламани тенглик ёрдамида қуйидагича ёзиш мумкин:

$$\gamma = \delta q + r, \ \ \gamma_1 = \delta q_1 + r \ \ (0 \leqslant r < \delta)$$

a сон m модуль бўйича δ кўрсаткичга тегишли бўлганидан

$$((a^{\delta p} \equiv 1 \ (\bmod m)) \wedge (a^{\delta p_1} \equiv 1 \ (\bmod m)) \Rightarrow (a^{\delta})^{q} \equiv$$
$$\equiv (a^{\delta})^{q_1} (\bmod m) \Rightarrow a^{\delta q} \cdot a^{r} \equiv a^{\delta q_1} \cdot a^{r} (\bmod m) \Rightarrow$$
$$\Rightarrow a^{\delta p + r} \equiv a^{\delta p_1 + r} (\bmod m) \Rightarrow a^{\gamma} \equiv a^{\gamma_1} (\bmod m).$$

3-натижа. $\gamma \equiv 0 (\bmod \delta)$ бўлганда ва фақат шу ҳолдагина $a^{\gamma} \equiv 1 \ (\bmod m)$ таққослама ўринли бўлади.

Ҳақиқатан, агар $\gamma \equiv \gamma_1 \ (\bmod \delta)$ ва $\gamma_1 = 0$ десак, $a^{\gamma} \equiv a^{0} \equiv 1 \ (\bmod m)$ ҳосил бўлади. Бошқача айтганда γ / δ бажарилса, $a^{\gamma} \equiv 1 (\bmod m)$ бўлади.

4-натижа. a сонининг m модуль бўйича δ кўрсаткичи $\varphi(m)$ нинг бўлувчиси бўлади. (Агар a бошланғич илдиз бўлса, δ кўрсаткич $\varphi(p) = p - 1$ ни бўлади) δ кўрсаткични топиш учун $a^{0}, a^{1}, \ldots, a^{\delta - 1}$ системадаги барча даражаларни ҳисоблаб чиқиш шарт эмас, унинг ўрнига даража кўрсаткичи $\varphi(m)$ ни бўладиган даражаларни ҳисоблаймиз.

Масалан, 7 модуль бўйича 5 сон тегишли бўлган кўрсаткични топиш учун $\varphi(7)=6$ бўлганидан 1, 2, 3 ва 6 кўрсаткичларни текшириш кифоя.

3-мисол. 17 модуль бўйича 7 сони тегишли бўлган кўрсаткични топинг.

$\varphi(17)=16$ бўлиб, 16 нинг бўлувчилари 1, 2, 4, 8, 16 бўлади. Шунинг учун қуйидагиларни ҳисоблаймиз:

$$7^1 \equiv 7 \pmod{17},\ 7^2 \equiv -2 \pmod{17},$$
$$7^4 \equiv 4 \pmod{17},\ 7^8 \equiv -1 \pmod{17},$$
$$7^{16} \equiv 1 \pmod{17}.$$

Демак, 7 сони 17 модуль бўйича бошланғич илдиз экан.

5-натижа. Агар a сон m модуль бўйича δ кўрсаткичга тегишли бўлса, a^k сони шу модуль бўйича $\frac{\delta}{(\delta;\ k)}$ кўрсаткичга тегишли бўлади.

Исботи. a^k сон m модуль бўйича γ кўрсаткичга тегишли бўлсин, яъни $a^{k\gamma} \equiv 1 \pmod{m}$ бажарилсин. 3-натижага асосан, охирги таққослама фақат $k\gamma \equiv 0 \pmod{\delta}$ бўлгандагина ўринли бўлади.

Таққосламаларнинг хоссасига асосан охирги таққосламани қуйидаги кўринишда ёзамиз:

$$\gamma \equiv 0 \left(\mathrm{mod}\, \frac{\delta}{(\delta;\ k)}\right).$$

6-натижа. Агар $(\delta;\ k)=1$ бўлса, у ҳолда a^k сон δ кўрсаткичга тегишли бўлади.

4-мисол. 3 сони 7 модуль бўйича 6 кўрсаткичга тегишли. Чунки $3^4 = 81$ сони $\frac{6}{(6;\ 4)} = \frac{6}{2} = 3$ бўлгани учун 7 модуль бўйича 3 кўрсаткичга тегишли бўлади. Ҳақиқатан,

$$81 \equiv -3 \pmod{7},\ 81^2 \equiv 2 \pmod{7},\ 81^3 \equiv 1 \pmod{7}.$$

34-§. Кўрсаткичга тегишли синфларнинг мавжудлиги ва сони. Туб модуль бўйича бошланғич илдизнинг мавжудлиги

Айтайлик, бирор a сон δ кўрсаткичга тегишли бўлсин. Чегирмаларнинг келтирилган системасидаги сонлардан шу δ кўрсаткичга тегишли бўлганларини топиш билан шуғулланамиз. Маълумки, p модуль бўйича δ

кўрсаткичга тегишли чегирмалар

$$x^{\delta} \equiv 1 \pmod{p} \qquad (1)$$

таққосламаларнинг ечимлари ичида ётади. (1) таққосламанинг ечимлари эса чегирмалари

$$a^0, a^1, a^2, \ldots, a^k, \ldots, a^{\delta-1} \qquad (2)$$

дан ва p модуль бўйича тузилган синфлардан иборат.

Ҳақиқатан, 1) $(a^k)^{\delta} \equiv (a^{\delta})^k \equiv 1 (\mathrm{mod}\, p)$ бўлгани учун (2) система (1) ни қаноатлантиради.

2) (2) қаторнинг ҳар бир элементи 33-§ даги 2-теоремага асосан, p модуль бўйича турли синфларга тегишлидир.

3) (2) да бу чегирмалар сони δ га тенг.

(1) таққосламада модуль туб бўлгани учун унинг ечимлари сони δ дан ортиқ эмас. Энди биз топилган ечимлар ичидан кўрсаткичга тегишли бўлганларини излаймиз.

Маълумки, 33-§ даги 1- теоремада бир хил кўрсаткичга тегишли бўлган чегирмалар синфи ҳақида гап борган эди, яъни ҳар бир синфнинг барча чегирмалари битта кўрсаткичга тегишли бўлиб, бу кўрсатгич $\varphi(m)$ нинг бўлувчисидан иборат бўларди. Энди масалани аксинча қўямиз:

$\varphi(m)$ нинг ҳар бир бўлувчиси m модуль бўйича тузилган бирор синфнинг кўрсаткичи бўладими? Ҳар қандай m модуль бўйича бошланғич илдиз мавжудми? Бу саволларга қуйидаги лемма ёрдамида жавоб бериш мумкин.

Лемма. *p туб сон ва δ сон $p-1$ соннинг бўлувчиси бўлсин. p модуль бўйича чегирмаларнинг келтирилган синфлар системасида δ кўрсатгичга тегишли синфлар сони $\varphi(\delta)$ та бўлади.*

Исботи. Маълумки, p модуль бўйича чегирмалар келтирилган системасининг ҳар бир чегирмаси битта кўрсаткичга тегишли (33-§ га қаранг) ва ҳар бир чегирмага эса битта синф мос келади.

p модуль бўйича тузилган чегирмаларнинг келтирилган системасидаги чегирмалардан берилган кўрсаткичга тегишли бўлган чегирмалар сонини $\psi(\delta)$ деб белгилайлик. Бунда қуйидаги икки ҳол бўлади:

а) δ кўрсаткичга тегишли бўлган чегирма мавжуд эмас, яъни $\psi(\delta) = 0$;

б) келтирилган системанинг камида битта чегирмаси δ кўрсаткичга тегишли, яъни $\psi(\delta) > 0$.

Биз б) ҳолни атрофлича қараб чиқайлик. 33-§ даги 6-натижага асосан $(\delta; k) = 1$ шартни қаноатлантирувчи барча a^k лар δ кўрсаткичга тегишли бўлади. (2) қатордаги $(\delta; k) = 1$ шартни қаноатлантирувчи чегирмалар сони $\varphi(\delta)$ бўлади. Чунки k ўзгарувчи $0, 1, 2, \ldots, \delta - 1$ ларни қабул қилади. Бу кетма-кетликда δ билан ўзаро туб чегирмалар сони $\varphi(\delta)$ дир. $\varphi(\delta)$ эса δ модуль бўйича тузилган чегирмаларнинг келтирилган системасидаги чегирмалар сонидан иборат. Демак, $\varphi(\delta) = \psi(\delta)$.

Мисол. 19 модуль бўйича 4 сони тегишли бўлган кўрсаткични топинг ва 19 модуль бўйича кўрсаткичга тегишли бўлган чегирмаларнинг келтирилган системасини тузинг.

Аввало, бевосита ҳисоблаш усули билан 4 сони 19 модуль бўйича қайси кўрсаткичга тегишли эканини топамиз. 4 нинг барча даражаларини текшириб ўтирмай, унинг фақат 1, 2, 3, 6, 9, 18 даражаларини текширамиз (33-§, 4-натижа).

$$4 \equiv 4 \pmod{19},\ 4^2 \equiv 16 \pmod{19},\ 4^3 \equiv 7 \pmod{19},$$
$$4^6 \equiv 11 \pmod{19},\ 4^9 \equiv 1 \pmod{19}.$$

Демак, 4 сон 19 модуль бўйича 9 кўрсаткичга тегишли экан.

Энди 19 модуль бўйича кўрсаткичга тегишли бўлган сонларни излаймиз. Леммага асосан бундай сонлар сони $\varphi(9) = 6$ та. 1, 2, 4, 5, 7, 8 система 9 модуль бўйича чегирмаларнинг келтирилган системасидан иборатдир.

Демак, биз излаган сонлар $4, 4^2, 4^4, 4^5, 4^7, 4^8$ лар бўлади. Бу сонларни 19 модуль бўйича энг кичик мусбат чегирмалар билан алмаштирамиз ва уларни ўсиш тартибида ёзиб, 4, 5, 6, 9, 16, 17 системага эга бўламиз.

Теорема. *p туб модуль бўйича тузилган $p - 1$ сонннинг ҳар бир δ бўлувчиси $\varphi(\delta)$ та синфнинг кўрсаткичи бўлади. Хусусий ҳолда $\varphi(p - 1)$ та бошланғич илдизлар синфи мавжуд.*

Исботи. Фараз қилайлак $\delta_1, \delta_2, \ldots, \delta_k$ лар $p - 1$ нинг бўлувчилари бўлсин. p модуль бўйича тузилган $1, 2, 3, \ldots, p - 1$ чегирмалар келтирилган системасининг барча элементларини шу сонларнинг ҳар бири тегишли бўлган кўрсаткичлар бўйича гуруҳларга ажратиб чиқамиз. У ҳолда δ_1 га тегишли сонлар сони $\psi(\delta_1)$; δ_2 га тегишли сонлар сони $\psi(\delta_2)$ ва ниҳоят δ_k га тегишли сонлар сони $\psi(\delta_k)$ бўлади. Барча гуруҳларга тақсимланган чегирмалар сони $p-1$ та бўлгани учун

$$\psi(\delta_1)+\psi(\delta_2)+\ldots+\psi(\delta_k)=p-1 \qquad (3)$$

бўлади.

Иккинчи томондан 25-§ да кўриб ўтганимиздек, бирор соннинг бўлувчилари бўйича тузилган Эйлер функцияларининг йиғиндиси

$$\sum_{p-1/\delta_l} \varphi(\delta_l)=p-1 \qquad (4)$$

эди. Демак,

$$\sum_{p-1/\delta_l} \psi(\delta_l)=\sum_{p\ 1/\delta_l} \varphi(\delta_l). \qquad (5)$$

Леммага асосан

$$\psi(\delta_l)=\varphi(\delta_l) \qquad (6)$$

тенгликка эга бўламиз. Лекин $\psi(\delta_l)$ сон p модуль бўйича δ_l кўрсаткичга тегишли бўлган чегирмалар сони эди. (6) га асосан $\psi(\delta_l)$ ларнинг сони $\varphi(\delta_l)$ экан.

Хусусий ҳолда, $\delta_k=p-1$ бўлса, у ҳолда $p-1$ кўрсаткичга тегишли сон бошланғич илдиз бўлади. Демак, p туб модуль бўйича $\varphi(p-1)$ та бошланғич илдизлар синфи мавжуд экан.

Бошланғич илдизлар фақатгина $m=2,4$, p^α ва $2p^\alpha$, сонлар учунгина мавжуддир (бу ерда p — тоқ туб сон, $\alpha \geqslant 1$ натурал сон).

Бошланғич илдизлар бевосита ҳисоблаш усули билан топилади. Ҳозирги кунгача уларни топишга ёрдам берувчи бирорта алгоритм ишлаб чиқилмаган.

35-§. Индекслар ва уларнинг хоссалари.

Биз 33-§ да ҳар қандай p туб модуль бўйича бошланғич илдиз мавжудлигини кўрсатган эдик. Маълумки, g сон p модуль бўйича бошланғич илдиз бўлса,

$$g^0,\ g^1,\ g^2,\ \ldots,\ g^{p-2} \qquad (1)$$

сонлар қатори шу p модуль бўйича чегирмаларнинг келтирилган системасини ташкил қилади. (1) қаторнинг ҳадлари p билан ўзаро туб бўлиб, улар p модуль бўйича $\varphi(p) = p - 1$ та синфнинг вакилларидан иборатдир.

Демак, $(a; p) = 1$ бўлса, у ҳолда (1) қаторда p модуль бўйича a сон билан таққосланувчи ягона элемент топилади, яъни

$$a \equiv g^{\gamma}(\bmod p) \qquad (2)$$

таққослама ўринли бўлади.

Таъриф. Агар g сон p туб модуль бўйича бошланғич илдиз бўлиб, $(a; p) = 1$ бўлганда (2) таққослама ўринли бўлса, $\gamma \geqslant 0$ сон a соннинг p модуль бўйича g асосга нисбатан *индекси* дейилади ва у $\gamma = \operatorname{ind}_g a$ каби белгиланади.

Агар асос аввалдан берилган бўлса, a нинг индекси $\operatorname{ind} a$ орқали белгиланади.

Бу таърифдан фойдаланиб (2) ни қуйидагича ёзиш мумкин:

$$a \equiv g^{\operatorname{ind} a}(\bmod p). \qquad (3)$$

Юқоридагиларга асосан, ҳар бир $(a; p) = 1$ шартни қаноатлантирувчи a сон берилган g асос бўйича

$$0, 1, 2, \ldots, p - 2 \qquad (4)$$

сонларнинг биттаси билан аниқланувчи индексга эга экан. Асоснинг ўзгариши билан индекс ҳам ўзгаради. Масалан, 7 модуль бўйича 1, 2, 3, 4, 5, 6 сонлари ва улар билан, шу 7 модуль бўйича таққосланувчи барча сонлар 3 асосга кўра

$$3^0 \equiv 1\,(\bmod 7),\ 3^2 \equiv 2\,(\bmod 7),\ 3 \equiv 3\,(\bmod 7),$$
$$3^4 \equiv 4(\bmod 7),\ 3^5 \equiv (\bmod 7),$$
$$3^3 \equiv -1(\bmod 7)$$

бўлгани учун мос равишда 0, 2, 1, 4, 5, 3 каби индексларга эга. Энди асос $a = 5$ бўлсин. У ҳолда асос бўйича тузилган индекслар 33-§ даги мисолнинг в) сига асосан мос равишда 0, 4, 5, 2, 1, 3 сонларга тенг.

g сон p модуль бўйича бошланғич илдиз бўлгани учун, бошланғич илдизнинг таърифига асосан

$$g^{p-1} \equiv 1(\bmod p) \qquad (5)$$

таққослама ўринли бўлади. Бу таққосламанинг иккала қисмини $k > 0$ даражага кўтариб

$$1 \equiv g^{k(p-1)}\,(\bmod p) \qquad (6)$$

га эга бўламиз. Энди (2) ва (6) таққосламаларни ҳадлаб кўпайтириб,

$$a\equiv g^{\gamma+k(p-1)}(\mathrm{mod}\, p) \qquad (7)$$

таққосламага эга бўламиз.

(7) таққослама эса ҳар бир $(a;\ p)=1$ шартни қаноатлантирувчи a сони g бошланғич илдиз бўйича чексиз кўп индексга эга эканини кўрсатади. Бу индексларнинг барчаси

$$g^{\gamma}\equiv g^{\gamma_1}(\mathrm{mod}\, p) \qquad (8)$$

таққосламани қаноатлантиради. (8) нинг ўринли бўлиши учун

$$\gamma\equiv\gamma_1(\mathrm{mod}\, p-1) \qquad (9)$$

таққосламанинг бажарилиши зарур ва етарли. Демак, p модуль бўйича тузилган ва p билан ўзаро туб бўлган ҳар бир синфга (9) таққослама билан аниқланувчи индекслар тўплами мос келади ва аксинча.

Бу тушунчаларга кўра ($a\equiv b(\mathrm{mod}\, p)$ бўлса, у ҳолда

$$\mathrm{ind}\, a\equiv \mathrm{ind}\, b(\mathrm{mod}\, p-1). \qquad (10)$$

(2) ва (3) га асосан

$$g^{\gamma}\equiv g^{\mathrm{ind}\, a}\,(\mathrm{mod}\, p). \qquad (11)$$

Бундан

$$\gamma\equiv \mathrm{ind} a(\mathrm{mod}\, p-1) \qquad (12)$$

Индекслар қуйидаги хоссаларга эга:

1°. Кўпайтманинг индекси $p-1$ модуль бўйича кўпайтувчилар индексларининг йиғиндиси билан таққосланади, яъни

$$\mathrm{ind}(a\cdot b\ \ldots\ l)\equiv \mathrm{ind}\, a+\mathrm{ind} b+\ \ldots\ +\mathrm{ind}\, l\ (\mathrm{mod}\, p-1).$$

Исботи. Индекснинг таърифига асосан, қуйидаги таққосламаларни ёзиб оламиз:

$$a\equiv g^{\mathrm{ind} a}\,(\mathrm{mod}\, p),$$
$$b\equiv g^{\mathrm{ind} b}\,(\mathrm{mod}\, p),$$
$$\ldots\ldots\ldots,$$
$$l\equiv g^{\mathrm{ind} l}\,(\mathrm{mod}\, p).$$

Буларни ҳадлаб кўпайтирамиз. У ҳолда

$$a\cdot b\ .\ .\ .\ l\equiv g^{\mathrm{ind} a+\mathrm{inb} b+\ldots+\mathrm{ind} l}(\mathrm{mod}\, p)$$

таққослама ҳосил бўлади. Бундан (2) ва (12) га асосан

$$\mathrm{ind}(a\cdot b\ .\ .\ .\ l)\equiv \mathrm{ind} a+\mathrm{ind} b+\ .\ .\ .\ +$$
$$+\mathrm{ind}\, l(\mathrm{mod}\, p-1). \qquad (13)$$

2°. Натурал кўрсаткичли даражанинг индекси $p-1$ модуль бўйича асос индекси ва даража кўрсаткичининг кўпайтмаси билан таққосланади, яъни

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod{p-1}.$$

Исботи. Фараз қилайлик, $a=b=\ldots=l$ бўлсин. У ҳолда 1-хоссага асосан

$$\operatorname{ind}(a \cdot a \ldots a) \equiv \operatorname{ind} a + \operatorname{ind} a + \ldots + \\ + \operatorname{ind} a \pmod{p-1}$$

ёки

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod{p-1}$$

ҳосил бўлади.

3°. p ихтиёрий туб сон бўлганда p модуль бўйича 1 нинг индекси нолга, асос g нинг индекси эса 1 га тенг бўлади.

Ҳақиқатан, $g^0 \equiv 1 \pmod{p}$ ва $g^1 \equiv g \pmod{p}$ бўлганидан $\operatorname{ind} 1 \equiv 0 \pmod{p-1}$ ва $\operatorname{ind} g \equiv 1 \pmod{p-1}$ дир. Демак, индекслар ҳам логарифмлар каби хоссаларга эга экан.

36-§. Индекслар жадвали

Логарифмик жадваллар мавжуд бўлганидек, ихтиёрий p туб модуль бўйича индекслар жадвалини тузиш мумкин. Индексларнинг асоси қилиб p сонниг бирорта бошланғич илдизи олинади. Дастлабки индекслар жадвалини рус математиги М. В. Остроградский тузган. У 1837 йилда 200 гача бўлган туб модуллар учун индекслар жадвалини тузди. Ҳозирги кунда бундай жадваллар 10000 гача туб модуллар учун тузилган.

Ҳар бир жадвал қуйидаги 2 та қисмдан иборат бўлади:

1) берилган n сон бўйича I индексни топиш;

2) берилган I индекс бўйича n сонни топиш.

Бирор p модуль бўйича индекслар жадвалини тузиш учун аввало p модуль бўйича g бошланғич илдизни топиш лозим. Сўнгра

$$g^0,\ g^1,\ \ldots,\ g^{p-2}$$

даражалар p модуль бўйича энг кичик мусбат чегирмаларга алмаштирилади. Масалан, $p=11$ модуль бўйича индекслар ва уларга мос сонлар жадвалини тузайлик. Бевосита ҳисоблаш усули билан 2, 6, 7, 8 лар

11 модуль бўйича бошланғич илдиз эканига ишонч ҳосил қиламиз.

Ҳақиқатан, $\varphi(11)=10$ бўлгани учун

$$2\equiv 2 \pmod{11},\ 2^3\equiv 8 \pmod{11},$$
$$2^4\equiv 5 \pmod{11},\ 2^2\equiv 4 \pmod{11},$$
$$2^5\equiv 10 \pmod{11},\ 2^{10}\equiv 1 \pmod{11},$$
$$2^9\equiv 6 \pmod{11},\ 2^6\equiv 9 \pmod{11},$$
$$2^7\equiv 7 \pmod{11},\ 2^8\equiv 3 \pmod{11}$$

ларга асосан 2 бошланғич илдиздир.

$$6\equiv 6 \pmod{11},\ 6^3\equiv 7 \pmod{11},\ 6^{10}\equiv 1 \pmod{11},$$
$$6^2\equiv 3 \pmod{11},\ 6^5\equiv 10 \pmod{11}.$$

Демак, 11 модуль бўйича 6 ҳам бошланғич илдиз экан.

Энди асос 2 бўлганда қуйидаги жадвалларни тузамиз:

n	1	2	3	4	5	6	7	8	9	10
I	10	1	8	2	4	9	7	3	6	5

I	1	2	3	4	5	6	7	8	9	10
n	2	4	8	5	10	9	7	3	6	1

Биринчи жадвалга асосан, сон берилса, индекс топилади, иккинчи жадвалга асосан эса индексга қараб сон топилади.

$p=43$ модуль бўйича 3, 5, 12, 18, 19, 20, 26, 28, 30, 33, 34 сонлар бошланғич илдиздир. $g=28$ бўлганда қуйидаги жадвалларга эга бўламиз:

n	0	1	2	3	4	5	6	7	8	9
0		42	39	17	36	5	4	7	33	34
1	2	6	11	40	4	22	30	16	31	29
2	41	24	3	20	8	10	37	9	1	25
3	19	32	27	23	13	12	28	35	26	5
4	38	18	21							

n

I	0	1	2	3	4	5	6	7	8	9
0		28	10	22	14	5	11	7	24	27
1	25	12	35	34	6	39	17	3	41	30
2	23	42	15	33	21	29	38	32	36	14
3	16	18	31	8	9	37	4	26	40	2
4	13	20	1							

Бу жадваллардаги сатрлар ва устунлар мос равишда сон (индекс) нинг ўнлик ва бирлик хонасини билдириб, уларнинг кесишган жойида изланаётган индекс (сон) туради.

Мисол. 43 модуль бўйича 37 соннинг индексини топинг.

Биринчи жадвалдаги 3-сатр ва 7-устуннинг кесишган жойида 35 сони жойлашган. Демак, $\mathrm{ind}_{28}37=35$. Энди аксинча 43 модуль бўйича индекси 18 га тенг сонни топинг.

$$\mathrm{ind}\, n\equiv 18 (\mathrm{mod}\, 42).$$

Иккинчи жадвалга асосан биринчи сатр ва 8-устуннинг кесишган жойига 41 сони мос келади. Демак, $n=41$.

Агар изланаётган сон (ёки индекс) жадвалдаги энг катта сондан ҳам катта бўлса, бу сон қаралаётган p ёки $p-1$ модуль бўйича энг кичик мусбат чегирма билан алмаштириб олинади.

Бошланғич илдизи мавжуд бўлган ҳар қандай модуль бўйича индекслар жадвалини тузиш мумкин. Чунки бундай ҳолда ҳам бошланғич илдизнинг даражалари m модуль бўйича чегирмаларнинг келтирилган системасини ташкил қилади.

37-§. Индекслар ёрдамида таққосламаларни ечиш

Индексларнинг хоссаларидан фойдаланиб, икки ҳадли таққосламаларни осонгина ечиш мумкин. Бундай мисолларни ечиш учун берилган сон бўйича унинг индексини (маълум асосга кўра) ва аксинча берилган индексга қараб, унга мос келувчи сонни топишга тўғри келади. Шунинг учун мазкур қўлланманинг охирида 1 дан 100 гача туб сонларнинг индекслари жадвали келтирилган.

Фараз қилайлик,

$$ax^n \equiv b (\mathrm{mod}\, p) \qquad (1)$$

таққослама берилган бўлиб, $(a;\ p)=1$ ва p тоқ туб сон бўлсин. Индекслар тушунчасидан фойдаланиб, (1) ни унга тенг кучли

$$\mathrm{ind}\, a + n\, \mathrm{ind}\, x \equiv \mathrm{ind}\, b (\mathrm{mod}\, p-1)$$

$$n\, \mathrm{ind}\, x \equiv \mathrm{ind}\, b - \mathrm{ind}\, a (\mathrm{mod}\, p-1) \qquad (2)$$

таққослама билан алмаштирамиз. Энди, $\mathrm{ind}\, x$ ни номаълум сифатида қараб, (2) таққосламани ечамиз. Агар бу таққослама умуман ечимга эга бўлса, қуйидаги икки ҳолдан бири бўлиши мумкин:

1. $(n;\ p-1)=1$;
2. $(n;\ p-1)=d>1$.

Агар 1- ҳол ўринли бўлса, 27- § га асосан (2) таққослама $\mathrm{ind}\, x$ га нисбатан ягона ечимга эга бўлади

Агар $\mathrm{ind}\, x=c$ ечим бўлса, индекслар жадвалидан фойдаланиб, x ни топамиз. x нинг топилган қиймати p модуль бўйича берилган таққосламанинг ечими бўлади.

2- ҳол ўринли бўлсин, яъни $(n;\ p-1)=d>1$ бўлсин. Унда қуйидаги 2 та ҳол юз беради:

а) $(\mathrm{ind}\, b-\mathrm{ind}\, a)\underset{\cdot}{\times} d$, яъни $\mathrm{ind}\, b-\mathrm{ind}\, a$ сон d га бўлинмайди. Бундай ҳолда таққосламаларнинг хоссасига асосан (2) ечимга эга бўлмайди.

(1) ва (2) тенг кучли бўлгани учун (1) ҳам ечимга эга бўлмайди.

б) $(\mathrm{ind}\, b-\mathrm{ind}\, a)\underset{\cdot}{\times} d$, яъни $\mathrm{ind}\, b-\mathrm{ind}\, a$ сон d га бўлинсин. У ҳолда (2) таққосламани қуйидагича ёзиш мумкин:

$$\frac{n}{d}\, \mathrm{ind}\, x \equiv \frac{\mathrm{ind}\, b-\mathrm{ind}\, a}{d} \left(\mathrm{mod}\, \frac{p-1}{d}\right). \qquad (3)$$

Бунда $\left(\frac{n}{d};\ \frac{p-1}{d}\right)=1$ бўлгани учун охирги таққослама $\frac{p-1}{d}$ модуль бўйича фақат битта ечимга эга бўлади. Яна (2) таққослама $p-1$ модуль бўйича d та ечимга ҳам эга булади. Бу ечимларни $\mathrm{ind}\, x$ лар бўйича топиб, индекслар жадвали ёрдамида эса (1) нинг ечимларини топамиз.

Индекслар одатда бирор бошланғич илдизга нисбатан тузилгани учун ҳар бир таққослама ечимини албатта дастлаб берилган модуль бўйича топиш керак. Чунки биз бошланғич илдизлар ўзгариши билан индекслар ҳам ўзгаришини кўриб ўтган эдик.

1-мисол. $x^5 \equiv 14 (\mathrm{mod} 41)$ таққосламани ечинг.

Бу таққосламанинг иккала қисмини индекслаймиз. У ҳолда

$$5 \operatorname{ind} x \equiv \operatorname{ind} 14 (\mathrm{mod}\, 40).$$

Жадвалга асосан, $\operatorname{ind} 14 = 25$. Демак, $5 \operatorname{ind} x \equiv 25 (\mathrm{mod}\ 40)$ ёки $\operatorname{ind} x \equiv 5 (\mathrm{mod}\, 8)$.

$(5;40)=5$ бўлгани учун берилган таққослама 41 модуль бўйича 5 та ечимга эга бўлади. У ечимлар

$$\operatorname{ind} x_1 \equiv 5 (\mathrm{mod}\, 40),\ \operatorname{ind} x_2 \equiv 13 (\mathrm{mod}\, 40),\ \operatorname{ind} x_3 \equiv 21 (\mathrm{mod} 40),$$
$$\operatorname{ind} x_4 \equiv 29 (\mathrm{mod}\, 40),\ \operatorname{ind} x_5 \equiv 37 (\mathrm{mod}\, 40)$$

таққосламалардан индекслар бўйича

$$x_1 \equiv 27 (\mathrm{mod}\, 41),\ x_2 \equiv 24 (\mathrm{mod}\, 41),\ x_3 \equiv 35 (\mathrm{mod}\, 41),$$
$$x_4 \equiv 22 (\mathrm{mod}\, 41),\ x_5 \equiv 15 (\mathrm{mod}\, 41).$$

Энди $x^n \equiv a (\mathrm{mod}\, p)$ таққосламанинг ечилиш шартини кўрсатамиз.

Бу таққосламанинг ечилиш шартини келтириб чиқариш учун унинг иккала қисмини индекслаб,

$$n \operatorname{ind} x \equiv \operatorname{ind} a (\mathrm{mod}\, p-1) \tag{4}$$

таққосламага эга бўламиз.

$(n; p-1)=d$ бўлганда охирги таққосламанинг ечимга эга бўлиши учун $\operatorname{ind} a$ нинг d га бўлиниши зарур ва етарлидир, яъни

$$\operatorname{ind} a \equiv 0 (\mathrm{mod}\, d) \tag{5}$$

бажарилиши керак. (5) ни p ва d лар орасидаги боғланиш орқали ифодалайлик. Бунинг учун (5) нинг иккала қисмини ва модулини $\frac{p-1}{d}$ га кўпайтирамиз. У ҳолда (5) таққослама билан тенг кучли бўлган $\frac{p-1}{d}$ $\operatorname{ind} a \equiv 0 (\mathrm{mod}\, p-1)$ таққослама ҳосил бўлади. Индекслар тушунчасидан фойдаланиб, бу таққосламани

$$\operatorname{ind} a^{\frac{p-1}{d}} \equiv 0 (\mathrm{mod}\, p-1)$$

кўринишда ёзамиз. $0 \equiv \operatorname{ind} 1 (\mathrm{mod}\, p-1)$ бўлганидан ва юқоридаги таққосламага мувофиқ қуйидагини ёза оламиз:

$$a^{\frac{p-1}{d}} \equiv 1(\mathrm{mod}\, p). \qquad (6)$$

Ҳосил бўлган (6) таққослама (3) таққосламанинг ечилиш шарти. (6) да $n=2$ бўлганда бизга маълум бўлган Эйлер шарти келиб чиқади. Ҳақиқатан, бундай ҳолда p тоқ туб сон бўлгани учун $d=(2;\ p-1)=2$, яъни $d=2$ бўлиб, (6) таққослама

$$a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$$

кўринишни олади. Бу эса $x^2 \equiv a(\mathrm{mod}\, p)$ таққосламанинг ечилиш шарти эди.

Ушбу

$$a^x \equiv b(\mathrm{mod}\, p) \qquad (7)$$

кўринишдаги таққослама *кўрсаткичли таққослама* дейилади. Бу таққосламани ечиш учун унинг ҳар иккала қисмини индекслаб,

$$x\, \mathrm{ind}\, a \equiv \mathrm{ind}\, b(\mathrm{mod}\, p-1) \qquad (8)$$

таққосламани ҳосил қиламиз. Бу таққослама эса биринчи даражали бир номаълумли таққослама бўлиб, бундай таққосламаларни ечишни 28- § да кўриб ўтган эдик.

2-мисол. $11^x \equiv 17(\mathrm{mod}\, 31)$ таққосламани ечинг.

Бунинг учун берилган таққосламанинг иккала қисмини индекслаб $x\, \mathrm{ind}\, 11 \equiv \mathrm{ind}\, 17(\mathrm{mod}\, 30)$ таққосламага эга бўламиз. $\mathrm{ind}\, 11=23$, $\mathrm{ind}\, 17=7$ эканидан $23x \equiv 7(\mathrm{mod}\, 30)$ ёки $x=29(\mathrm{mod}\, 30)$ таққосламани ҳосил қиламиз. Бундан $x=29(\mathrm{mod}\, 30)$ ечим берилган таққосламанинг ечими экани келиб чиқади.

38-§. Таққосламалар назариясининг арифметикага татбиқлари

I. Бўлиниш аломатлари. Бутун сонлар тўпламига тегишли ихтиёрий a ва $m>0$ сонлари берилган бўлсин. Кўп ҳолларда a сонни m сонга бўлишдан ҳосил бўлган энг кичик қолдиқни топиш талаб этилади. Бу масалани ҳал этишнинг умумлашган усулини дастлаб француз математиги Б. Паскаль кўрсатган эди.

Биз ҳозир шу усулни ўнлик, юзлик ва минглик саноқ системалари учун баён этамиз.

Фараз қилайлик, a натурал сон ўнлик саноқ системада берилган бўлсин. Унда бу a сонини ўннинг даражалари бўйича қуйидагича ёзиш мумкин:

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n.$$

m модуль бўйича 10^k сон тегишли бўлган чегирмалар синфининг энг кичик абсолют чегирмаси r_k, яъни

$$10^k \equiv r_k (\mathrm{mod}\, m) \quad (k = \overline{0,\ n};\ r_0 = 1)$$

бўлсин. Унда a сонини қуйидагича ёзиш мумкин:

$$a \equiv a_0 r_0 + a_1 r_1 + a_2 r_2 + \ldots + a_n r_n (\mathrm{mod}\, m). \qquad (1)$$

Агар $R_m = a_0 r_0 + a_1 r_1 + \ldots + a_n r_n$ десак, (1) ушбу

$$a \equiv R_m (\mathrm{mod}\, m)$$

кўринишда бўлади. Шундай қилиб, a сони ундан кичик бўлган R_m сони билан алмаштирилади. Бошқача қилиб айтганда, (1) таққослама ўнлик системада Паскалнинг бўлиниш (ёки тенг қолдиқлилик) аломатини билдиради. Агар $R_m = 0$ бўлса, a сон m га қолдиқсиз бўлинади, агар $R_m \neq 0$ бўлса, у ҳолда $r = R_m$ бўлади.

Бўлиниш аломатининг қуйидаги баъзи хусусий ҳолларини кўриб ўтамиз:

1. $m = 9$ бўлсин. Биз ихтиёрий натурал соннинг 9 га бўлиниш аломатини келтириб чиқарамиз.

Ушбу $10 \equiv 1 (\mathrm{mod}\, 9)$ таққосламанинг иккала қисмини k даражага кўтарсак,

$$10^k \equiv 1 (\mathrm{mod} 9)$$

таққослама ҳосил бўлади. Бундан кўринадики, барча r_k лар 1 га тенг экан. Унда R_m қуйидаги кўринишни олади:

$$R_9 = a_0 + a_1 + a_2 + \ldots + a_n$$

Бу эса ўрта мактабда бизга маълум бўлган аломатнинг ўзидир, яъни берилган соннинг рақамлари йиғиндиси 9 га бўлинса, у ҳолда бу натурал сон 9 га бўлинади.

2. $m = 11$ бўлсин. У ҳолда $10 \equiv -1 (\mathrm{mod}\, 11) \Rightarrow 10^k \equiv (-1)^k (\mathrm{mod}\, 11)$ га асосан

$$R_{11} = (a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots)$$

тенглик ўринли бўлади, яъни R_{11} сон 11 га бўлинса, у ҳолда берилган сон 11 га бўлинади.

1-мисол. $a = 3568921$ сонни 11 га бўлганда ҳосил бўладиган қолдиқни топинг.

$$R_{11} = (1+9+6+3)-(2+8+5)=19-15=4,$$
$$R_{11}=4.$$

Демак, 3568921 сонни 11 га бўлганда қоладиган қолдиқ 4 га тенг.

3. $m=7$ бўлсин. У ҳолда

$$10^0 \equiv 1 \pmod 7),\ 10 \equiv 3 \pmod 7),\ 10^2 \equiv 2 \pmod 7),$$
$$10^3 \equiv -1 \pmod 7),\ 10^4 \equiv -3 \pmod 7),\ 10^5 \equiv -2 \pmod 7),$$
$$10^6 \equiv 1 \pmod 7)$$

бўлгани учун $R_7 = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6$ бўлади. Фараз қилайлик, 10 сони m модуль бўйича δ кўрсаткичга тегишли бўлсин. Унда кўрсаткичнинг таърифига асосан, $10^0 \equiv 1 \pmod m)$ бўлгани учун $r_\delta = 1$ бўлиб, $r_{\delta+1} = r_1$, $r_{\delta+2} = r_2, \ldots, r_{2\delta} = r_\delta = 1$ бўлади, яъни қолдиқлар δ та қадамдан сўнг такрорланади. У ҳолда R_m қуйидаги кўринишни олади:

$$R_m = a_0 + a_1 r_1 + a_2 r_2 + \ldots + a_{\delta-1} r_{\delta-1} + a_\delta + a_{\delta+1} r_1 + \ldots$$

Маълумки, ихтиёрий сонни ихтиёрий саноқ системасида ёзиш мумкин. Фараз қилайлик, саноқ системасининг асоси 10^δ бўлиб, бу асосга кўра a сонининг ёйилмаси

$$a = d_0 + d_1 \cdot 10^\delta + d_2 \cdot 10^{2\delta} + \ldots + d_n \cdot 10^{n\delta}$$

бўлсин. $(10)^n = 1 \pmod m)$ бўлгани учун (1) таққослама $a = d_0 + d_1 + d_2 + \ldots + d_n$ кўринишни олади.

Демак, 10 асосли системада берилган соннинг m га бўлиниш аломати ўнлик системада берилган соннинг 9 га бўлиниш аломати каби бўлар экан. Шуни алоҳида таъкидлаш керакки, берилган a сонининг 10^δ асос бўйича m га бўлиниш аломатини келтириб чиқариш учун уни ўнгдан чапга қараб δ хоналарга ажратиб чиқиш лозим.

2-мисол. a сонининг 100 лик системада 11 га бўлиниш аломатини келтириб чиқаринг.

Аввало a ни юзлик системада қуйидагича ёзиб оламиз:

$$a = b_0 + b_1 \cdot 100 + b_2 \cdot 100^2 + b_3 \cdot 100^3 + \ldots + b_n \cdot 100^n.$$

Аммо $100^k \equiv 1 (\bmod 11)$ бўлгани учун $a \equiv b_0 + b_1 + b_2 + \ldots + b_n (\bmod m)$ бўлиб, $R_{11} = b_0 + b_1 + b_2 + \ldots + b_n$, $a = 3568921$ сонини юзлик системада 11 га бўлишидан ҳосил бўлган қолдиқ

$$R_{11} = 21 + 89 + 56 + 3 = 169, \quad R_{11} = 169 \equiv 4 (\bmod 11).$$

3-мисол. 37 модуль бўйича 10 сони 3 кўрсаткичга тегишли, яъни $10^3 \equiv 1 (\bmod 37)$ бўлгани учун берилган a сони минглик системасида

$$a = c_0 + c_{11} \cdot 1000 + c_2 \cdot 1000^2 + \ldots + c_n \cdot 1000^n$$

кўринишда ёзилган бўлса, у ҳолда

$$a \equiv c_0 + c_1 + c_2 + \ldots + c_n (\bmod 37)$$

бўлганидан минглик системада 37 га бўлиниш аломати

$$R_{37} \equiv c_0 + c_1 + c_2 + \ldots + c_n (\bmod 37)$$

бўлади. $a = 83576289$ сонини 1000 лик системада 37 га бўлганда ҳосил бўлган қолдиқни топинг.

$$R_{37} = 289 + 576 + 83 \equiv 23 (\bmod 37),$$

бўлгани учун қолдиқ 23 га тенг.

Энди даражани бўлишдан чиққан қолдиқни ҳисоблайлик.

$$a \equiv r (\bmod m) \Rightarrow a^k \equiv r^k (\bmod m)$$

бўлгани учун a^k даража r^k даража билан алмаштирилади $(r;\ m) = 1$ бўлганда Эйлер теоремасидан фойдаланиш мақсадга мувофиқдир. Ҳақиқатан, $(r;\ m) = 1$ бўлганда $r^{\varphi(m)} \equiv 1 (\bmod m)$ эди $k = \varphi(m) \cdot q + l (0 \leqslant l < \varphi(m))$ тенгликка асосан

$$r^k \equiv (r^{\varphi(m)})^q \cdot r^l \equiv r^l \bmod m)$$

ни ёза оламиз.

4-мисол. 1277^{261} ни 28 га бўлишдан ҳосил бўлган қолдиқни топинг.

$$1277 \equiv 17 (\bmod 28), \quad 1277^{261} \equiv 17^{261} (\bmod 28).$$

Бунда $(17;\ 28) = 1$ бўлгани учун $17^{\varphi(28)} \equiv 1 (\bmod 28) \Rightarrow 17^{12} \equiv 1 (\bmod 28)$.

$261 = 12 \cdot 21 + 9$ бўлгани учун $17^{261} \equiv 17^9 (\bmod 28)$ бўлади $17 \equiv 17 (\bmod 28)$ айний таққослама олайлик. У ҳолда

$$17^2 \equiv 9 (\bmod 28), \quad 17^4 \equiv -3 (\bmod 28),$$
$$17^8 \equiv 9 (\bmod 28), \quad 17^9 \equiv 13 (\bmod 28).$$

Демак, $1277^{261}\equiv 17^{261}\equiv 17^{9}\equiv 13 \pmod{28}$, $1277^{261}\equiv 13 \pmod{28}$, яъни 1277^{261} сонни 28 га бўлганда қоладиган қолдиқ 13 бўлар экан.

II. Оддий касрни ўнлик асрга айлантиришда ҳосил бўладиган давр узунлигини аниқлаш. Маълумки, махражи 2 ва 5 га бўлинмайдиган ҳар қандай қисқармайдиган $\frac{a}{b}$ касрни ўнли касрга айлантирганда, бу ўнли каср чексиз даврий ўнли каср бўлади.

1-таъриф. Ўнли касрнинг бутун қисми унинг *характеристикаси*, каср қисми эса *мантиссаси* дейилади. Агар ўнли касрнинг мантиссаси чексиз бўлиб, унда маълум узунликдаги ўнли улушлар такрорланиб келса, у ҳолда бундай ўнли каср *даврий ўнли каср*, такрорланадиган ўнли улушларнинг кичиги *давр*, бу даврдаги рақамлар сони *давр узунлиги* дейилади.

2-таъриф. Агар даврий касрда давр бевосита вергулдан кейин келса, у ҳолда бундай каср *соф даврий каср*, агар вергул билан давр орасида бошқа рақамлар бўлса у ҳолда бундай даврий каср *аралаш даврий каср* дейилади.

Ҳар бир даврий ўнли касрнинг давр узунлигини топиш мумкин. Бунинг учун қуйидаги икки ҳол бўлиши мумкин:

1-ҳол. Қисқармайдиган тўғри (акс ҳолда касрнинг бутун қисмини ажратиб олган бўлардик) $\frac{a}{b}$ касрнинг махражида 2 ва 5 каби бўлувчилар мавжуд эмас, яъни $(a; b)=1$, $(b, 10)=1$ бўлсин.

Қуйидаги тенгликлар кетма-кетлигини қараймиз:

$$\begin{aligned}
10a &= bq_1+r_1 \qquad (0<r_1<b);\\
10r_1 &= bq_2+r_2 \qquad (0<r_2<b);\\
10r_2 &= bq_3+r_3 \qquad (0<r_3<b);\\
&\cdots\cdots\cdots\cdots\cdots\\
10r_{m-1} &= bq_m+r_m \qquad (0<r_m<b).
\end{aligned} \tag{1}$$

$b>a$, $b>r_1,\dots,b>r_{m-1}$ бўлгани учун $q_1<10$, $q_2<10,\dots,q_m<10$ бўлади.

Қуйидаги тасдиқлар рост бўлади:

$$(10;\ b)=1\wedge(a;\ b)=1\Rightarrow(10a;\ b)=1;$$
$$(10a;\ b)=1\Rightarrow(r_1;\ b)=1;$$

$$((10;\, b)=1 \wedge (r_1;\, b)) = 1 \Rightarrow (r_2;\, b)=1;$$

. . . .

Шундай қилиб, $(r_i;\, b)=1$ эканига ишонч ҳосил қиламиз. Демак, турли $r_i(i=\overline{1,\, n})$ лар b модуль бўйича чегирмаларнинг келтирилган системасини ташкил этади. Маълумки, b модуль бўйича чегирмаларнинг келтирилган системасидаги чегирмалар сони $\varphi(b)$ га тенг.

Шунинг учун кўпи билан $\varphi(b)$ қадамдан сўнг барча қолдиқлар ва улар б лан биргаликда q_i чала бўлинмалар яна такрорлана бошлайди. $q_1, q_2, \ldots, q_m$ рақамлар эса $\frac{a}{b}$ қисқармайдиган касрнинг даври дейилиб, бу касрнинг давр узунлиги $\varphi(b)$ дан катта бўла олмайди.

Даврдаги рақамлар сонини топиш учун (1) тенгликларни b модуль бўйича қуйидаги таққосламаларга алмаштирамиз:

$$\begin{aligned} 10\,a &\equiv r_1 (\mathrm{mod}\, b); \\ 10\,r_1 &\equiv r_2 (\mathrm{mod}\, b); \\ 10\,r_2 &\equiv r_3 (\mathrm{mod}\, b); \\ &\ldots\ldots \\ 10\,r_{m-1} &\equiv r_m (\mathrm{mod}\, b). \end{aligned} \qquad (2)$$

Бу таққосламаларни ҳадлаб кўпайтирамиз, у ҳолда

$$10^m a \cdot r_1 \cdot r_2 \ldots r_{m-1} \equiv r_1 \cdot r_2 \ldots r_m (\mathrm{mod}\, b)$$

ҳосил бўлади. $(r_1 \cdot r_2 \ldots r_{m-1};\, b)=1$ бўлгани учун охирги таққосламанинг иккала қисмини $r_1 \cdot r_2 \ldots r_{m-1}$ кўпайтмага бўлиб, ушбу

$$10^m a \equiv r_m (\mathrm{mod}\, b) \qquad (3)$$

таққосламани ҳосил қиламиз

Айтайлик, 10 сони b модуль бўйича m кўрсаткичга тегишли бўлсин. У ҳолда сон тегишли кўрсаткичнинг таърифига асосан, ушбу

$$10^m \equiv 1 (\mathrm{mod}\, b) \qquad (4)$$

таққослама ўринли бўлади. (4) га асосан (3) ни қуйидагича ёзиш мумкин:

$$a \equiv r_m (\mathrm{mod}\, b). \qquad (5)$$

Маълумки, ($0<a<b$ ва $0<r_m<b$) ҳар бири b дан кичик бўлган иккита мусбат сон b модуль бўйича тенг қолдиқли бўлиши учун улар тенг бўлиши, яъни $a=r_m$ бўлиши лозим.

Демак, m та қадамдан сўнг ҳосил бўладиган қолдиқ берилган касрнинг суратига тенг бўлади, бошқача айтганда m та қадамдан кейин қолдиқлар (ва демак, бўлинмалар ҳам) такрорланиб келади:

$$r_{m+1}=r_1,\ r_{m+2}=r_2,\ r_{m+3}=r_3,\ \ldots$$

m сони (5) таққослама ўринли бўлган индексларнинг энг кичигидир. Чунки m индекс b модуль бўйича a сони тегишли бўлган кўрсаткичдир. Тегишли кўрсаткич эса унинг таърифига асосан, (4) таққосламани қаноатлантирувчи даража кўрсаткичларидан энг кичигидир. Бундан m сони $\frac{a}{b}$ касрнинг давр узунлиги экан деган хулосага келамиз.

Шундай қилиб, (4) таққослама ўринли бўлганда $\frac{a}{b}$ каср $(a;\ b)=1$ бўлганда соф даврий касрга ёйилади, даврдаги рақамлар сони (давр узунлиги) фақатгина касрнинг махражига боғлиқ.

(1) даги тенгликларнинг ҳар икки қисмини b га бўлиб, қуйидагиларни ҳосил қиламиз:

$$\frac{a}{b}=\frac{q_1}{10}+\frac{r_1}{10b},$$

$$\frac{r_1}{b}=\frac{q_2}{10}+\frac{r_2}{10b},$$

$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

$$\frac{r_{m-1}}{b}=\frac{q_m}{10}+\frac{r_m}{10b}.$$

Бу тенгликларга асосан, қуйидаги ёйилмага эга бўламиз:

$$\frac{a}{b}=\frac{q_1}{10}+\frac{q_2}{10^2}+\frac{q_3}{10^3}+\ldots+\frac{q_m}{10^m}+\frac{r_m}{10^m b}.$$

Лекин $r_m=a$. Демак,

$$\frac{a}{b}=\frac{q_1}{10}+\frac{q_2}{10^2}+\frac{q_3}{10^3}+\ldots+\frac{q_m}{10^m}+\frac{a}{10^m b}$$

бўлиб, $\frac{a}{b}$ касрнинг даври $(q_1, q_2, q_3, \ldots, q_m)$ бўлади.

Юқоридаги тенгликлар кетма-кетлигига асосан $\frac{r_1}{b}$ нинг даври $(q_2, q_3, \ldots, q_m, q_1)$, $\frac{r_2}{b}$ нинг даври $(q_3, q_4, \ldots, \ldots, q_m, q_1, q_2)$, умуман $\frac{r_k}{b}$ касрнинг даври $(q_{k+1}, \ldots, \ldots, q_m, q_1, \ldots, q_k)$ бўлишига ишонч ҳосил қиламиз.

Шундай қилиб, 10 сони b модуль бўйича m кўрсаткичга тегишли бўлса, $\frac{a}{b}$, $\frac{r_1}{b}$, $\frac{r_2}{b}$, $\ldots$, $\frac{r_{m-1}}{b}$ касрлар соф даврий касрлар бўлиб, улар бир-биридан даврдаги рақамларнинг циклик алмашиб келиши билан фарқ қилади

5-мисол. $\frac{5}{37}$ касрни ўнли касрга айлантириб, унинг давр узунлигини топинг.

10 сони 37 модуль бўйича 3 кўрсаткичга тегишли эканини биз олдинги мавзуда кўриб ўтган эдик, бошқача айтганда,

$$10^3 \equiv 1 \pmod{37}.$$

Демак, юқоридаги касрнинг даври учта рақамдан ташкил топади. Ҳозир шу рақамларни топамиз.

$$5 \cdot 10 = 37 \cdot 1 + 13,$$
$$13 \cdot 10 = 37 \cdot 3 + 19,$$
$$19 \cdot 10 = 37 \cdot 5 + 5$$

тенгликларга асосан, $\frac{5}{37} = 0,\ (135)$, $\frac{13}{37} = 0,\ (351)$, $\frac{19}{37} = 0,\ (513)$.

Агар 10 сони b модуль бўйича бошланғич илдиз бўлса, $m = \varphi(b)$ бўлади. У ҳолда ўнли касрнинг давридаги рақамлар сони $m = \varphi(b)$ га тенг. Лекин бошланғич илдиз ҳар қандай сонлар учун мавжуд бўлавермаслигини биз кўриб ўтган эдик.

Айтайлик, 10 сони b модуль бўйича бошланғич илдиз бўлмасин. Унда 10 сони тегишли бўлган кўрсаткич $\varphi(b)$ дан кичик бўлади. Бундай ҳолда $\varphi(b) = md$ каби тенгликни ёза оламиз Демак, суратлари 1 дан $\varphi(b)$ гача бўлган сонларни қабул қилувчи, махражлари эса b га тенг бўлган касрлар тўплами d та касрлар системасига ажралар экан. Бу касрлар системасини биз қуйидагича ёзиб оламиз:

$$\frac{r_0}{b}, \frac{r_1}{b}, \frac{r_2}{b}, \ldots, \frac{r_{m-1}}{b};$$

$$\frac{s_0}{b}, \frac{s_1}{b}, \frac{s_2}{b}, \ldots, \frac{s_{m-1}}{b};$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\frac{t_0}{b}, \frac{t_1}{b}, \frac{t_2}{b}, \ldots, \frac{t_{m-1}}{b}.$$

Бунда ҳар бир йўлдаги касрларнинг даври бири иккинчисидан фақатгина рақамларининг циклик алмашиниши билан фарқ қилишини биз юқорида кўриб ўтган эдик.

Айтайлик, $s_0 \neq r_i$ бўлсин. У ҳолда иккинчи йўл касрлари ҳосил бўлиб, уларнинг даври ҳам m га тенг бўлади. s_i ва $r_i(i = \overline{0, m-1})$ лардан фарқли бирор $c_0 < \varphi(b)$ ни олсак, учинчи касрлар системаси ҳосил бўлади. Бу жараённи давом эттириб, биз d та касрлар системасига эга бўламиз. Бу айтилган фикрларни юқоридаги мисолга қўллаб кўрайлик: $\varphi(37) = 36$ бўлиб, $36 = 3 \cdot 12$ эканидан 12 та касрлар системасига эга бўламиз

Ҳақиқатан, 5, 13, 19 ларга тенг бўлмаган бирор сонни, масалан, 2 ни олайлик, у ҳолда

$$2 \cdot 10 = 37 \cdot 0 + 20,$$
$$20 \cdot 10 = 37 \cdot 5 + 15,$$
$$15 \cdot 10 = 37 \cdot 4 + 2$$

тенгликларга асосан, $\frac{2}{37} = 0,(054)$, $\frac{20}{37} = 0, (540)$, $\frac{15}{37} = 0, (405)$ касрлар системасига эга бўламиз. Қолган касрлар системалари мос равишда қуйидагича бўлади:

$$\frac{10}{37}, \frac{26}{37}, \frac{1}{37}, \; 0, (027) = \frac{10}{37};$$

$$\frac{30}{37}, \frac{4}{37}, \frac{3}{37}, \; 0, (081) = \frac{30}{37};$$

$$\frac{6}{37}, \frac{23}{37}, \frac{8}{37}, \; 0, (162) = \frac{6}{37};$$

$$\frac{7}{37}, \frac{33}{37}, \frac{34}{37}, \; 0, (189) = \frac{7}{37};$$

$$\frac{9}{37},\ \frac{16}{37},\ \frac{12}{37},\ 0,(243)=\frac{9}{37};$$
$$\frac{11}{37},\ \frac{36}{37},\ \frac{27}{37},\ 0,(297)=\frac{11}{37};$$
$$\frac{13}{37},\ \frac{19}{37},\ \frac{5}{37},\ 0,(351)=\frac{13}{37};$$
$$\frac{14}{37},\ \frac{29}{37},\ \frac{31}{37},\ 0,(378)=\frac{14}{37};$$
$$\frac{17}{37},\ \frac{22}{37},\ \frac{35}{37},\ 0,(459)=\frac{17}{37};$$
$$\frac{21}{37},\ \frac{25}{37},\ \frac{28}{37},\ 0,(567)=\frac{21}{37};$$
$$\frac{24}{37},\ \frac{32}{37},\ \frac{18}{37},\ 0,(486)=\frac{18}{37}.$$

Шуни алоҳида эслатиб ўтиш лозимки, турли касрлар системасининг даври бири иккинчисидан циклли алмаштириш ёрдамида ҳосил бўлмайди.

Агар тўғри касрнинг махражи берилган бўлса, бу касрга тенг бўлган ўнли касрнинг давр узунлигини индекслар ёрдамида топиш мумкин. Буни қуйидаги мисолда кўриб ўтамиз:

6-мисол. Махражи $b=41$ бўлган қисқармас касрни ўнли касрга айлантирганда ҳосил бўлган касрнинг давр узунлигини топинг.

Тегишли кўрсаткичнинг таърифига асосан, бу кўрсаткич

$$10^x\equiv 1 \pmod{41}$$

таққосламани қаноатлантирувчи кўрсаткичларнинг энг кичигидир. Бу таққосламани индекслар ёрдамида ечамиз: $x\,\mathrm{ind}\,10\equiv\mathrm{ind}\,1 \pmod{40}$, $\mathrm{ind}\,10=8$ бўлгани учун $8x\equiv 0 \pmod{40}$, $x\equiv 0 \pmod{5}$.

Охирги таққосламани қаноатлантирувчи энг кичик мусбат сон $x=5$ дир. Демак, махражи 41 га тенг бўлган қисқармас касрларнинг давр узунлиги 5 га тенг.

2-ҳол. Қисқармайдиган $\frac{a}{b}$ каср махражининг каноник ёйилмасида 2 ёки 5 қатнашсин, яъни $(b;\ 10)=1$ бўлмай, балки $b=2^{\alpha}\cdot 5^{\beta}\cdot b_1$ бўлсин. Бу ерда $(b_1;\ 10)=1$ бўлиши равшан. α ва β ларнинг энг каттасини n деб белгилайлик.

Қуйидаги нисбатни қараймиз:

$$\frac{10^n a}{b} = \frac{10^n a}{2^\alpha\cdot 5^\beta\cdot b_1} = \frac{2^{n-\alpha}\cdot 5^{n-\beta}\cdot a}{b_1} = \frac{a_1}{b_1}.$$

$$((b_1;\ 10)=1)\wedge((a,\ b_1)=1)\Rightarrow(a_1;\ b_1)=1.$$

Энди $(b_1;\ 10)=1$ бўлгани учун $\frac{a_1}{b_1}$ қисқармас касрни ўнли касрга айлантириш мумкин. У ҳолда қуйидаги тенглик ҳосил бўлади:

$$\frac{10^n a}{b} = \frac{a_1}{b_1} = H,\ (q_1,\ q_2,\ \ldots,\ q_n).$$

Бундан $\frac{a}{b} = \frac{H}{10^n}(q_1,\ q_2,\ \ldots,\ q_m)$ келиб чиқади. Агар $H=\overline{k\ k_1\ k_2 \ldots k_n}$ бўлса, у ҳолда $\frac{H}{10^n} = k,\ \overline{k_1\ k_2 \ldots k_n}$ бўлади, бу ерда $\overline{kk_1k_2\ldots k_n} = k\cdot 10^n + k_1\cdot 10^{n-1} + \ldots + k_{n-1}\cdot 10 + k_n$. Демак, $\frac{a}{b} = k,\ k_1k_2\ldots k_n(q_1,\ q_2,\ \ldots,\ q_m)$ экан. Шундай қилиб, $(b;\ 10)\neq 1$ бўлганда $\frac{a}{b}$ касрни ўнли касрга айлантирганда аралаш даврий каср ҳосил бўлиб, унинг давр узунлиги 10 сони b_1 модуль бўйича тегишли бўлган m кўрсаткичга тенг бўлади. Вергулдан кейинги давргача бўлган рақамлар сони эса $\lambda = \max(\alpha;\ \beta)$ орқали аниқланади.

III боб. ҲАЛҚА

39-§. Ҳалқанинг таърифи. Ҳалқага мисоллар

Айтайлик, бирор бўш бўлмаган K тўплам элементлари учун иккита алгебраик амал аниқланган бўлсин, яъни тартибланган $(a; b)$ жуфтликка ягона c элемент мос қўйилган бўлиб, $c \in K$ бўлсин.

Бу алгебраик амалларни биз *қўшиш* ва *кўпайтириш* деб атаймиз.

1-таъриф. Қўшиш ва кўпайтириш амаллари аниқланган K тўплам элементлари учун қуйидаги аксиомалар ўринли бўлса, у ҳолда K тўплам *ҳалқа* дейилади:

1. Қўшиш қонунлари:

а) $\forall a, b, c \in K \quad a+(b+c)=(a+b)+c$ (қўшишнинг ассоциативлиги);

б) $\forall a, b \in K \quad a+b=b+a$ (қўшишнинг коммутативлиги).

с) $\forall a, b \in K, \exists x \in K \quad a+x=b.$

2. Кўпайтириш қонунлари:

$\forall a, b, c \in K \quad a \cdot (b \cdot c)=(a \cdot b) \cdot c$ (кўпайтиришнинг ассоциативлиги);

3. Тақсимот (дистрибутивлик) қонуни:

а) $\forall a, b, c \in K \quad a \cdot (b+c)=a \cdot b+a \cdot c;$

б) $\forall a, b, c \in K \quad (b+c) \cdot a=b \cdot a+c \cdot a.$

K тўплам ҳосил қилган ҳалқани $\mathscr{K}$ ҳарфи орқали белгилаймиз. Агар $\mathscr{K}$ ҳалқанинг ихтиёрий a ва b элементлари учун $a \cdot b=b \cdot a$ тенглик бажарилса, у ҳолда $\mathscr{K}$ ҳалқа *коммутатив ҳалқа* дейилади.

Энди юқоридаги аксиомалардан келиб чиқадиган баъзи бир хулосаларни кўриб ўтамиз

Дастлабки учта аксиома $\mathscr{K}$ ҳалқанинг қўшиш амалига нисбатан абель группаси эканлигини билдиради.

Демак, абель группаси учун ўринли бўлган хоссалар ҳалқада ҳам ўринли бўлади, яъни ҳалқада қуйидаги хоссалар ўринли:

1°. $\mathscr{K}$ ҳалқанинг ихтиёрий a элементи учун $a+\theta=a$ тенгликни қаноатлантирувчи ноль элемент мавжуд ва у ягонадир.

2°. $\mathscr{K}$ ҳалқанинг ихтиёрий a элементи учун шу ҳалқада шундай $-a$ элемент топиладики, $a+(-a)=\theta$ бўлади.

Бунда $-a$ элемент a га *қарама-қарши элемент* дейилади.

3°. $\mathscr{K}$ ҳалқада $a+x=b$ тенглама ечимга эга ва у ягонадир. Бу ечим $x=-a+b$ бўлиб, биз уни $x=b-a$ орқали белгилаймиз.

2-таъриф. Агар $\mathscr{K}$ ҳалқанинг ихтиёрий a элементи учун $ae=ea=a$ бўлса, у ҳолда e элемент ҳалқанинг *бирлик элементи* дейилади.

4°. $a-b=a+(-b)$ бўлгани учун қуйидаги тенгликни ёзиш мумкин:

$$\forall a,\ b,\ c\in K\ (a-b)-c=(a-c)-b.$$

5°. $-(-a)=a$ ва $a-a=\theta$.

3-таъриф. Қаралаётган амал қўшиш бўлганда n та a нинг йиғиндиси $a+a+\ldots+a=na$ каби белгиланиб, na ни *a элементнинг бутун мусбат n коэффициентли карралиси* деб аталади.

6°. $\mathscr{K}$ ҳалқадаги ихтиёрий a ва ихтиёрий n натурал сон учун $n(-a)=-(na)=-na$ тенглик ўринли.

Ҳақиқатан, қўшилувчиларни гуруҳлаб, қуйидагига эга бўламиз: $na+n(-a)=n(a+c-a)=n\theta=\theta$, $na+n(-a)=\theta$. Бундан $n(-a)=-na$ бўлади.

Биз бу хоссаларнинг исботини „Группалар" мавзусида кўриб ўтган эдик.

Ассоциативлик қонунининг ўринлилиги қуйидагиларни талаб этади:

Қаралаётган элементлар сони иккитадан ортиқ бўлганда улар устида бажарилган алгебраик амал кўпайтувчи (қўшилувчи) ларнинг гуруҳланишларига боғлиқ бўлиб қолиши мумкин, бошқача айтганда, $u=bc$, $v=ab$ бўлганда $au=vc$ тенглик бажарилмаслиги мумкин. Ҳалқадаги ассоциативлик қонуни эса шу иккита элементнинг тенг, яъни $a(bc)=(ab)c$ эканлигини билдиради.

Ҳалқада аниқланган ассоциативлик қонуни ҳар қандай чекли сондаги элементлар учун ҳам ўринли бўлади. Бу тасдиқнинг исботини математик индукция принципи асосида олиб борамиз. $n=3$ да 2-аксиомага асосан тасдиқ ўринли.

Айтайлик, $n>3$ бўлганда бу фикримиз n дан кичик сондаги элементлар учун рост бўлсин, яъни

$$a_1(a_2\cdot a_3\ldots a_k)\ \text{ва}\ (a_{k+1}a_{k+2}\ldots a_{n-1})\cdot a_n$$

ларнинг натижалари қавсларнинг қўйилишига боғлиқ бўлмасин. Биз бу иккита ифодани кўпайтириб, кўпайтманинг ҳам қавсга боғлиқ эмаслигини кўрсатамиз. Ҳар бир кўпайтувчидаги элементлар сони n дан кичик бўлгани туфайли уларнинг ҳар бири ҳам бир қийматли усулда аниқланган.

Шунинг учун биз ҳар кандан k ва l учун рост

$$(a_1 \cdot a_2 \ldots a_k)(a_{k+1} \cdot a_{k+2} \ldots a_n) =$$
$$= (a_1 \cdot a_2 \ldots a_l)(a_{l+1} a_{l+2} \ldots a_n)$$

тенгликнинг $l = k + 1$ учун ўринли эканлигини кўрсатсак кифоя. Агар $l = k + 1$ бўлганда

$$a_1 \cdot a_2 \ldots a_k = b, \quad a_{k+2} \cdot a_{k+3} \ldots a_n = c$$

десак, учта элемент кўпайтмасининг ассоциативлигига кўра $b \cdot (a_{k+1} \cdot c) = (b \cdot a_{k+1}) \cdot c$ бўлади. Тасдиқ исбот этилди.

4-таъриф. Агар кўпайтувчи элементлар n та бўлиб, улар ўзаро тенг бўлса, $a \cdot a \ldots a$ ҳосил бўлиб, бу кўпайтма a^n кўринишда белгиланади ва унга *бутун мусбат даражали элемент* дейилади.

Энди дистрибутивлик қонунидан келиб чиқадиган баъзи бир натижаларни кўриб ўтамиз.

Бу қонуннинг чекли сондаги қўшилувчилар учун ўринли эканлиги математик индукция принципи асосида исботланади ва бу қонун айириш амалига нисбатан ҳам сақланади.

Ҳақиқатан, айирманинг аниқланишига асосан $b - a$ элемент учун

$$a + (b - a) = b$$

тенглик ўринли. Унинг иккала томонини c га кўпайтирамиз ва қўшишнинг кўпайтиришга нисбатан дистрибутивлигидан

$$ac + (b - a) \cdot c = bc$$

ни ҳосил қиламиз.

Бундан $(b - a)c$ элемент bc дан ac нинг айирмаси эканлиги келиб чиқади.

$$(b - a) \cdot c = bc - ac \text{ ёки } c(b - a) = cb - ca.$$

Охирги тенгликдан хусусий ҳолда $b = a$ бўлса, $c \cdot \theta = c \cdot (b - b) = cb - cb = \theta$, $c \cdot \theta = \theta$ келиб чиқади.

Демак, ҳалқада кўпайтувчиларнинг бири ноль элемент бўлса, кўпайтма ҳам ноль элемент бўлар экан.

Лекин баъзи ҳолларда бу тасдиқнинг тескариси ўринли бўлмайди. Масалан,

$$A=\begin{pmatrix}2 & 0\\ 0 & 0\end{pmatrix},\ B=\begin{pmatrix}0 & 0\\ 0 & 3\end{pmatrix}$$

матрицаларни олсак, уларнинг ҳар бири ноль матрица эмас. Аммо уларнинг кўпайтмаси ноль матрицадир.

$$A\cdot B=\begin{pmatrix}2 & 0\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix}0 & 0\\ 0 & 3\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}.$$

5-**таъриф.** Ҳалқада $a\neq 0$, $b\neq 0$ бўлганда $a\cdot b=0$ ўринли бўлса, у ҳолда a ва b элементлар *нолнинг бўлувчилари* дейилади.

Одатда, ҳалқанинг ноль элементи ҳам нолнинг бўлувчиси деб юритилади.

6-таъриф. Агар ҳалқада нолнинг ўзидан бошқа нолнинг бўлувчилари мавжуд бўлмаса, яъни

$$\forall a,\ b\in\mathscr{K}\ a\cdot b=0\Rightarrow a=0\vee b=0$$

бўлса, бундай ҳалқа *нолнинг бўлувчиларига эга бўлмаган ҳалқа* дейилади.

Мисоллар. 1. Барча бутун сонлар тўплами коммутатив ҳалқа бўлади, чунки бу тўплам қўшиш амалига кўра абель группасидан иборат бўлиб, унда кўпайтириш амали ёпиқ ва бутун сонларни кўпайтириш ассоциатив ҳамда бу амал қўшишга нисбатан дистрибутивдир.

2. Барча жуфт сонлар тўплами ҳалқа бўлади.

3. Барча тоқ сонлар тўплами ҳалқа бўлмайди, чунки иккита тоқ сон йиғиндиси бу тўпламга тегишли эмас.

4. Комплекс сонлар тўплами коммутатив ҳалқа бўлади, чунки бу тўпламда ҳам ҳалқанинг барча аксиомалари ўринли бўлади.

Бу ҳалқалар одатда *сонли ҳалқалар* деб аталади. Сонли ҳалқаларнинг бирортаси ҳам нолнинг бўлувчиларига эга эмас.

5. F тўплам $(-1;\ 1)$ оралиқда аниқланган ва узлуксиз функциялар тўплами бўлсин. Агар

$$f(x)=\begin{cases}0, & \text{агар } x\geqslant 0,\\ x, & \text{агар } x<0;\end{cases}\quad g(x)=\begin{cases}0, & \text{агар } x<0,\\ x, & \text{агар } x\geqslant 0\end{cases}$$

бўлса, у ҳолда $f(x) \neq 0$, $g(x) \neq 0$ бўлиб, $f(x) \cdot g(x) = 0$ тенглик бажарилади (текширинг).

Шунингдек, $(-1; 1)$ оралиқдаги узлуксиз функциялар тўплами ҳалқа ташкил қилишини осонгина аниқлаш мумкин. Демак, F нолнинг бўлувчиларига эга бўлган ҳалқа экан.

6. $A = \{0, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ тўплам ҳам нолнинг бўлувчиларига эга бўлган ҳалқадир. Бу ерда $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$ лар $m = 6$ модуль бўйича чегирмалар синфларидан иборат. Бу фикрни текшириб кўришни ўқувчига ҳавола қиламиз.

40-§. Ҳалқанинг характеристикаси

1-таъриф. $\mathcal{K}$ ҳалқа учун бирор M қисм тўплам $\mathcal{K}$ да аниқланган қўшиш ва купайтириш амалларига нисбатан ҳалқа бўлса, у ҳолда M қисм тўплам $\mathcal{K}$ ҳалканинг *қисм ҳалқаси* дейилади ва у $M \subset \mathcal{K}$ кўринишда белгиланади.

Масалан, жуфт сонлар тўплами бутун сонлар ҳалқаси учун қисм ҳалқа бўлиб, бутун сонлар тўплами эса рационал сонлар ҳалқасининг қисм ҳалқасидир.

Қуйидаги теорема $\mathcal{K}$ ҳалқанинг бирор M қисм тўплами ҳалқа бўлиш-бўлмаслигини аниқлашда муҳим аҳамиятга эга.

Теорема. *$\mathcal{K}$ ҳалқанинг бирор бўш бўлмаган M қисм тўплами қисм ҳалқа бўлиши учун M га тегишли a ва b элементларнинг йиғиндиси, айирмаси ва кўпайтмаси яна қисм тўпламга тегишли бўлиши зарур ва етарли.*

Исботи. 1) Зарурийлик шарти. Фараз қилайлик, $\forall a, b \in M$ бўлганда $a + b \in M$, $a - b \in M$, $a \times b \in M$ бўлсин. $M \subset \mathcal{K}$ эканлигини кўрсатамиз. Ҳақиқатан, ҳар қандай $a \in M$ ва $b \in M$ учун $a + b \in M$ ва $a \cdot b \in M$ бўлгани сабабли мос равишда $a + b$, $a \cdot b$ ни M даги a ва b элементларни қўшиш ва кўпайтириш амаллари деб олишимиз мумкин.

Энди M тўпламнинг ҳалқа эканлигига ишонч ҳосил қилиш учун унда ҳалқанинг барча аксиомалари бажарилишини кўрсатиш кифоя. M тўплам $\mathcal{K}$ нинг қисм тўплами бўлганлигидан унда ҳалқа таърифининг I гуруҳ аксиомаларидаги с) қисмидан бошқа барчаси ўринли. Биз ҳозир с) аксиоманинг ҳам ўринли эканлигини кўрсатамиз.

Теорема шартига асосан $a \in M$ ва $b \in M$ эканлигидан $b - a = c \in M$, иккинчидан $\mathcal{K}$ ҳалқада $a + (b - a) = b$ ёки $a + c = b$ бўлади. Шундай қилиб, с) аксиома ҳам ўринли.

Демак, M тўплам $\mathcal{K}$ ҳалқанинг қисм ҳалқаси экан.

Эслатма. $a + b = a - (-b)$ бўлгани учун теоремадаги биринчи шартни, яъни $a + b \in M$ шартни олмасдан, қолган иккита шарт билан қаноатлансак ҳам M қисм ҳалқа бўлади.

2) Етарлилик шарти. M қисм ҳалқа бўлсин. У ҳолда M да теоремадаги учта шартнинг бажарилиши ҳалқа аксиомаларига асосан келиб чиқади.

Бирлик элементга эга бўлган $\mathcal{K}$ ҳалқа берилган бўлсин. Биз ўз олдимизга бирлик элементни ичига олувчи ва бошқа барча қисм ҳалқалар учун қисм ҳалқа бўладиган, яъни энг кичик қисм ҳалқани топиш вазифасини қўямиз. Бу қисм ҳалқада e бирлик элемент бўлса, у ҳолда $-e$ элемент ҳам бўлади. У ҳолда $ne = \underbrace{e + e + \ldots + e}_{n \text{ та}}$ ва $-ne = \underbrace{(-e) + (-e) + \ldots + (-e)}_{n \text{ та}}$ ҳам бу қисм ҳалқага тегишли бўлади $ne - me = (n - m)e$ ва $(ne) \cdot (me) = n \cdot m(e \cdot e) = nme$ бўлгани учун e элементнинг карралилари тўплами яна ҳалқа бўлади.

Агар биз бу қисм ҳалқани $\mathcal{K}_1$ десак, у $\mathcal{K}$ даги e ни ўз ичига олувчи энг кичик қисм ҳалқа бўлади. Бунда қуйидаги икки ҳол бўлиши мумкин:

а) барча натурал n лар учун $ne \neq 0$;

б) бирорта натурал n учун $ne = 0$.

Натурал сонларнинг исталган тўплами доимо энг кичик элементга эга бўлганлигидан $me = 0$ шартни қаноатлантирувчи натурал сонлар ичида энг кичик натурал m сон мавжуд.

2-таъриф. Агар барча $n \neq 0$ лар да $ne \neq 0$ бўлса, $\mathcal{K}_1$ ҳалқа *ноль характеристикали*, бирорта $m \neq 0$ да $me = 0$ бўлганда эса $\mathcal{K}_1$ ҳалқа *m характеристикали ҳалқа* дейилади.

Сонли ҳалқаларнинг барчаси ноль характеристикали ҳалқа эканлиги ўз-ўзидан аён.

Мисоллар. 1. Бутун сонлар тўплами рационал сонлар ҳалқаси учун қисм ҳалқа бўлади.

2. a ва b бутун сонлар бўлганда $a+b\sqrt{p}$ (p—туб сон) кўринишдаги элементлар тўплами ҳақиқий сонлар ҳалқасининг қисм ҳалқаси бўлади.

Ҳақиқатан, а) $(a_1+b_1\sqrt{p})(a_2+b_2\sqrt{p}) = (a_1a_2 + b_1b_2p) + (a_1b_2+a_2b_1)\sqrt{p} = a + b\sqrt{p}$. (Бунда $a_1a_2 + b_1b_2p = a$, $a_1b_2 + a_2b_1 = b$.)

б) $(a_1+b_1\sqrt{p}) - (a_2+b_2\sqrt{p}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{p} = c + d\sqrt{p}$. (Бунда $a_1 - a_2 = c$, $b_1 - b_2 = d$.)

Бу ҳалқани биз $\mathbf{Z}[\sqrt{p}]$ деб юритамиз.

41-§. Бутунлик соҳаси

39-§ да кўриб ўтганимиздек, ҳалқалар икки хил ва уларнинг баъзилари нолнинг бўлувчиларига эга, баъзилари эса нолнинг бўлувчиларига эга бўлмас эди.

Таъриф. Нолнинг бўлувчиларига эга бўлмаган коммутатив ҳалқа *бутунлик соҳаси* дейилади.

Бутунлик соҳаси ҳалқа бўлгани туфайли у бирлик элементга эга бўлиши ҳам, эга бўлмаслиги ҳам мумкин.

Барча сонли ҳалқалар бутунлик соҳасига мисол бўлади. $\mathcal{K}$ бутунлик соҳаси қуйидаги муҳим хоссага эга: агар $a \neq 0$ бўлса, у ҳолда $ab = ac$ тенгликдан $b = c$ тенглик келиб чиқади.

Биз бу фикрни исботлаш учун $ab = ac$ ни $ab - ac = \theta$ каби ёзиб оламиз. Бундан $a(b - c) = \theta$ тенгликда $a \neq \theta$ бўлганидан ва $\mathcal{K}$ да нолнинг бўлувчилари мавжуд эмаслигидан $b - c = \theta$, яъни $b = c$ келиб чиқади.

Мисоллар. 1. Ҳар қандай майдон бутунлик соҳаси бўлади.

Ҳақиқатан. P майдон бўлгани учун $a \neq \theta$ шартда a^{-1} мавжуд. Агар $a \cdot b = \theta$ бўлса, у ҳолда тенгликнинг иккала томонини a^{-1} га кўпайтириб, $b = \theta$ га эришамиз. Демак, майдонда $a \cdot b = \theta \Rightarrow a = \theta \vee b = \theta$ шарт бажарилганлиги туфайли майдон бутунлик соҳаси бўлади.

2. Барча сонли ҳалқалар бутунлик соҳаси бўлади. Чунки бу ҳалқалар коммутатив бўлиб, нолнинг бўлувчиларига эга эмас.

3. 39-§ даги 5-мисолда кўриб ўтилган $\mathcal{F}$ ҳалқа бутунлик соҳаси бўла олмайди.

4. Мураккаб модуль бўйича тузилган чегирмалар синфлари ҳам бутунлик соҳаси бўлмайди, чунки улар нолнинг бўлувчиларига эга.

42-§. Бутунлик соҳасида аниқланган бўлиниш муносабатининг хоссалари

Биз 41-§ да $\mathcal{K}$ бутунлик соҳаси бўлса, унда

$$\forall a,\ b,\ c \in \mathcal{K} \quad ((a \neq \theta) \wedge (ab = ac)) \Rightarrow (b = c)$$

хосса ўринли эканлигини кўриб ўтган эдик.

1-таъриф. Агар $\mathcal{K}$ бутунлик соҳасида берилган ҳар қандай a ва $b \neq 0$ элементлар учун $\mathcal{K}$ да шундай q элемент мавжуд бўлсаки, натижада $a = bq$ тенглик бажарилса, у ҳолда *a элемент b элементга бўлинади* дейилади*.

Агар a элемент b элементга бўлинса, у ҳолда у a/b кўринишда белгиланади.

2-таъриф Ҳалқадаги a элемент учун $ab = e$ (e— ҳалқанинг бирлик элементи) тенглик ўринли бўлса, у ҳолда *b элемент a га тескари элемент* дейилади. Тескари элементга эга бўлган элемент одатда *тескариланувчан* деб юритилади ва у ε орқали белгиланади. Тескариланувчан элементлар баъзан *бирнинг бўлувчилари* ҳам дейилади.

1-теорема. *Агар a/b ва ε тескариланувчан элемент бўлса, $a/b\varepsilon$ ва $a\varepsilon/b$ бўлади.*

Исботи. Таърифга кўра $a/b \Rightarrow a = bq$. ε тескариланувчан бўлгани учун $\mathcal{K}$ да $\varepsilon \cdot \varepsilon_1 = e$ шартни қаноатлантирувчи ε_1 элемент мавжуд. Бундай ҳолда

$$a = bq \Rightarrow a = (b\varepsilon \cdot \varepsilon_1)\, q \Rightarrow a = (b\varepsilon) \cdot \varepsilon_1 q$$

бўлгани учун $a/b\varepsilon$ ўринли. Иккинчидан, a/b ва ихтиёрий $\varepsilon \in \mathcal{K}$ учун $a\varepsilon/b$ ўринлидир.

3-таъриф. $\mathcal{K}$ бутунлик соҳасининг a ва b элементлари учун $a = b \cdot \varepsilon$ ўринли бўлса, бу элементлар ўзаро *ассоцирланган элементлар* дейилади.

2-теорема. *$\mathcal{K}$ бутунлик соҳасида a/b ва b/a муносабатлар бажарилиши учун a ва b ўзаро ассоцирланган бўлиши зарур ва етарли.*

---

* $\mathcal{K}$ бутунлик соҳасида берилган бўлиниш муносабати бутун сонларнинг бўлиниши каби хоссаларга эга.

Исботи. 1) **Етарлилик шарти.** a ва b элементлар ассоцирланган, яъни $a = b\varepsilon$ ва $b = a\varepsilon_1$ бўлсин. Бу тенгликларнинг биринчиси a/b ни, иккинчиси эса b/a ни билдиради.

2) **Зарурийлик шарти.** a/b ва b/a бўлсин. У ҳолда

$$a/b \Rightarrow a = bq, \qquad (1)$$
$$b/a \Rightarrow b = aq_1 \qquad (2)$$

келиб чиқади. (2) дан фойдаланиб (1) ни қуйидагича ёзамиз:

$$a = bq \Rightarrow a(e - qq_1) = \theta.$$

$\mathcal{K}$ бутунлик соҳаси бўлгани учун $a(e - qq_1) = \theta$ ни $e - qq_1 = 0$ каби ёзиш мумкин Охирги тенгликка асосан $qq_1 = e$. Демак, q ва q_1 тескариланувчан элементлар экан. Бошқача айтганда; a ва b ўзаро ассоцирланган элементлардир.

Мисоллар. 1. 1 ва -1 сонлар бутун сонлар ҳалқасида тескариланувчандир.

2. $Z[i] = \{a + bi/a, b \in Z\}$ сонлар тўпламида тўртта элемент, яъни $1, -1, i, -i$ тескариланувчан бўлади.

3. Бутун сонлар ҳалқасидаги -7 ва 7 сонлар ассоцирланган сонлардир.

4. $Z[\sqrt{3}]$ ҳалқада $(2 - \sqrt{3})(2 + \sqrt{3}) = 1$ бўлгани учун $5 + 2\sqrt{3}$ ва $4 - \sqrt{3}$ элементлар ўзаро ассоцирланган элементлар бўлади. Ҳақиқатан, $4 - \sqrt{3} = (5 + 2\sqrt{3})(2 - \sqrt{3})$.

43-§. Гомоморф ва изоморф ҳалқалар

Биз ушбу қўлланманинг биринчи қисмида группаларнинг гомоморфлиги, чизиқли фазо ва чизиқли алгебраларнинг изоморфлиги тўғрисида фикр юритган эдик. Энди ҳалқаларнинг гомоморфлиги ва изоморфлиги устида тўхталиб ўтамиз.

Таъриф. $\mathcal{A}$ ва $\mathcal{B}$ ҳалқалар элементлари орасида бирор мослик ўрнатилган бўлиб, бу мослик бир қийматли (ўзаро бир қийматли) бўлса ҳамда қуйидаги шартлар бажарилса $\mathcal{A}$ ҳалқа $\mathcal{B}$ га *гомоморф (изоморф)* дейилади:

1. $\forall a, b \in \mathscr{A}, \forall a', b' \in \mathscr{B}\, a \overset{\varphi}{\to} a' \wedge b \overset{\varphi}{\to} b' \Rightarrow$

$\Rightarrow a + b \overset{\varphi}{\to} a' + b'$;

2. $\forall a, b \in \mathscr{A}, \forall a', b' \in \mathscr{B}\, a \overset{\varphi}{\to} a' \wedge b \overset{\varphi}{\to} b' \Rightarrow$

$\Rightarrow ab \overset{\varphi}{\to} a'b'$.

$\mathscr{A}$ ҳалқанинг $\mathscr{B}$ ҳалқага гомоморфлиги (изоморфлиги) $\mathscr{A} \simeq \mathscr{B}$ ($\mathscr{A} \cong \mathscr{B}$) каби белгиланади.

1-теорема. *Ихтиёрий $\mathscr{K}$ ҳалқа ва қўшиш ҳамда кўпайтириш амаллари аниқланган K' тўплам учун $\mathscr{K} \simeq K'$ бўлса, у ҳолда K' тўплам ҳалқа бўлади.*

Исботи. Теорема шарти бўйича $\mathscr{K} \simeq K'$ бўлиб, $\mathscr{K}$ ҳалқадир. K' да иккита алгебраик амал аниқланган ва ёпиқ бўлсин. Биз K' нинг ҳам ҳалқа эканлигини кўрсатишимиз керак. Бунинг учун K' дан ихтиёрий учта a', b', c' элементларни олиб, улар учун ҳалқанинг барча аксиомалари ўринли эканлигини кўрсатамиз.

Биз шулардан қуйидаги иккитасини келтирамиз:

1. $a' \odot (b' \oplus c') = a' \odot b' \oplus a' \odot c'$ — кўпайтиришнинг қўшишга нисбатан дистрибутивлиги.

2. $a' \oplus x' = b'$ тенгламанинг ечимга эгалиги.

1. $\mathscr{K}$ ҳалқа бўлгани учун $a(b + c) = ab + ac$ шарт бажарилади. $a \xrightarrow{\varphi} a'$, $b \xrightarrow{\varphi} b'$, $c \xrightarrow{\varphi} c'$ бўлсин. Бу мослик $\mathscr{K}$ нинг K' га гомоморфлигига асосан қўшиш ва кўпайтиришда ҳам сақланади. Шунинг учун $(a \overset{\varphi}{\to} a') \wedge$ $\wedge (b \overset{\varphi}{\to} b') \wedge (c \overset{\varphi}{\to} c') \wedge (a(b + c) = ab + ac) \Rightarrow a' \odot (b' \oplus$ $\oplus c') = a' \odot b' \oplus a' \odot c'$.

2. $(a \to a') \wedge (b \to b') \wedge (x \to x') \Rightarrow (a + x = b) \to$ $\to (a' \oplus x' = b')$ $(x \in \mathscr{K}, x' \in K')$.

Бошқа аксиомалар ҳам худди шу усулда исбот қилинади. Демак, K' тўплам ҳалқа экан.

2-теорема. *$\mathscr{K}$ ҳалқа бўлиб, $\mathscr{K} \simeq K'$ бўлса,*

1. $(\theta \overset{\varphi}{\to} \theta') \wedge ((-a) \to (-a'))$ $(\theta; -a \in \mathscr{K}, 0';$ $-a' \in K')$.

2. *$\mathscr{K}$ бирлик элементга эга бўлса, K' ҳам бирлик элементга эга бўлади ва $e \overset{\varphi}{\to} e'$ $(e \in \mathscr{K}, e' \in K')$ бўлади.*

Теоремани исботлашни ўқувчиларга тавсия қиламиз.

44-§. Ҳалқа идеаллари

Биз 40-§ да қисм ҳалқа тушунчаси билан танишиб ўтган эдик. $\mathcal{K}$ ҳалқанинг бирор H қисм тўплами $\mathcal{K}$ нинг қисм ҳалқаси бўлиши учун H тўплам a ва b элементлар билан биргаликда уларнинг айирмаси ва кўпайтмасини ҳам ўз ичига олиши зарур ва етарли эди. Энди қисм ҳалқа тушунчасини аниқловчи иккинчи шарт, ($\forall a, b \in H \Rightarrow a \cdot b \in H$) ни бироз ўзгартириб қуйидаги тушунчани киритамиз:

1-таъриф. Агар $\mathcal{K}$ ҳалқанинг бирор бўш бўлмаган I қисм тўплами учун қуйидаги иккита шарт бажарилса, яъни

а) $\forall a, b \in I \Rightarrow a - b \in I$;

б) $\forall r \in \mathcal{K}, \forall a \in I \Rightarrow ar \in I$

бўлса, у ҳолда I тўплам $\mathcal{K}$ ҳалқанинг ўнг идеали дейилади.

2-таъриф Агар 1-таърифдаги а) шарт билан биргаликда

с) $\forall r \in \mathcal{K}, \forall a \in I \Rightarrow ra \in I$

бўлса, у ҳолда I тўплам $\mathcal{K}$ ҳалқанинг *чап идеали* дейилади.

3-таъриф Агар а), б) ва с) шартлар бажарилса, яъни I идеал ҳалқанинг чап ва ўнг идеали бўлса, у ҳолда I тўплам $\mathcal{K}$ ҳалқанинг *идеали* дейилади.

4-таъриф. $\mathcal{K}$ ҳалқанинг a элементига каррали бўлган барча элементлар тўплами $\mathcal{K}$ ҳалқанинг *бош идеали* дейилади ва у (a) орқали белгиланади.

Юқоридаги таърифлардан кўринадики, берилган ҳалқанинг ҳар қандай идеали шу ҳалқа учун қисм ҳалқа бўлади. Лекин бу тасдиқнинг таскариси ўринли бўлмаслиги мумкин. Масалан, Z тўплам Q ҳалқа учун қисм ҳалқа, лекин идеал эмас, чунки исталган r рационал сон ва исталган a бутун сон учун ra бутун сон бўлмаслиги мумкин.

Мисоллар. 1. Ихтиёрий $\mathcal{K}$ ҳалқанинг ўзи ва унинг $\{0\}$ қисм тўплами $\mathcal{K}$ ҳалқа учун идеал бўлади. Бу идеаллар одатда *тривиал* ёки *бирлик* ва *ноль идеаллар* деб юритилади ҳамда улар мос равишда (e) ва (0) каби белгиланади. $\mathcal{K}$ ҳалқа бошқа идеалларга эга бўлса, улар *нотривиал идеаллар* деб юритилади.

2. Бутун сонлар ҳалқасининг исталган бутун сонга (нолдан ташқари) каррали бўлган қисм тўпламлари бутун сонлар ҳалқасининг идеаллари бўлади.

3. Ихтиёрий $\mathcal{K}$ ҳалқа берилган бўлсин. Бу ҳалқадан бирор a ва ихтиёрий r элементларни олиб, $ra+na$ кўринишдаги элементлар тўпламини (a) каби белгилайлик, яъни

$$(a)=\{ra+na\,|\,r,\ a\in\mathcal{K},\ n\in Z\}.$$

(a) тўплам $\mathcal{K}$ ҳалқанинг чап идеали бўлади. Ҳақиқатан,

а) $(r_1a+n_1a)-(r_2a+n_2a)=(r_1-r_2)a+(n_1-n_2)a=$ $=ra+na\in(a)$. Бунда $r_1-r_2=r$, $n_1-n_2=n$ деб олинди

б) $\forall s\in\mathcal{K}$ ва $ra+na\in(a)$ учун $s(ra+na)=$ $=sra+sna=(sr+sn)a=r'a+0\cdot a\in(a)$. Бунда $r'=$ $=sr+sn$

Шундай қилиб, (a) тўплам учун идеал бўлишликнинг иккала шарти ҳам бажарилар экан

(a) идеал одатда *$\mathcal{K}$ ҳалқанинг a элементи ёрдамида ҳосил қилинган чап идеали* деб юритилади.

$ra+na$ йиғиндидаги na кўпайтмани ҳар доим ҳам $\mathcal{K}$ ҳалқа иккита элементининг кўпайтмаси деб қараш мумкин эмас, чунки бу ерда n бутун сон бўлгани учун ҳар доим ҳам $\mathcal{K}$ га тегишли бўлавермаслиги мумкин. Хусусий ҳолда, яьни $\mathcal{K}$ ҳалқа бирлик элементга эга бўлса, na ни қаралаётган ҳалқа иккита элементининг кўпайтмаси деб қараш мумкин. Дарҳақиқат, бундай пайтда

$$ra+na=ra+n\cdot ea=(r+ne)a=r'a$$

бўлиб, $r'=r+ne\in\mathcal{K}$, $a\in\mathcal{K}$ бўлади.

4) $\{a_1, a_2, \ldots, a_k\}$ тўплам $\mathcal{K}$ ҳалқанинг бирор қисм тўплами бўлсин. Бу қисм тўпламнинг элементлари ёрдамида қуйидаги тўпламни тузамиз:

$$A=\{r_1a_1+r_2a_2+\ldots+r_ka_k+n_1a_1+n_2a_2+\ldots+n_ka_k\,|\,r_i,\ a_i\in\mathcal{K},\ n_i\in Z,\ i=1,\ k\}.$$

Бевосита текшириш натижасида A тўплам ҳам $\mathcal{K}$ ҳалқанинг чап идеали эканлигига ишонч ҳосил қиламиз. Ҳақиқатан,

а) $(r_1a_1+r_2a_2+\ldots+r_ka_k+n_1a_1+n_2a_2+\ldots+n_ka_k)-$ $-(r_1'a_1+r_2'a_2+\ldots+r_k'a_k+n_1'a_1+n_2'a_2+\ldots+n_k'a_k)=$

$$= (r_1 - r_1')a_1 + \ldots + (r_k - r_k')a_k + (n_1 - n_1')a_1 +$$
$$+ \ldots + (n_k - n_k')a_k \in A;$$

б) $\forall s \in \mathcal{K}$ учун $s(r_1a_1 + \ldots + r_ka_k + n_1a_1 + \ldots + n_ka_k) = (sr_1)a_1 + \ldots + (sr_k)a_k + n_1(sa_1) + \ldots + n_k(sa_k) \in A$

шартлар бажарилгани учун юқоридаги усулда аниқланган A тўплам $a_1, a_2, \ldots, a_k$ элементлар ёрдамида ҳосил қилинган чап идеал бўлади ва у $(a_1, a_2, \ldots, a_k)$ каби белгиланади. $a_1, a_2, \ldots, a_k$ эса $(a_1, a_2, \ldots, a_k)$ идеалнинг базиси деб ҳам юритилади.

Агар берилган $\mathcal{K}$ ҳалқа бирлик элементга эга бўлса, у ҳолда ушбу тенглик ўринли:

$$r_1a_1 + r_2a_2 + \ldots + r_ka_k + n_1a_1 + n_2a_2 + \ldots + n_ka_k =$$
$$= r_1a_1 + r_2a_2 + \ldots + r_ka_k + n_1ea_1 + n_2ea_2 + \ldots + n_kea_k =$$
$$= (r_1 + n_1e)a_1 + (r_2 + n_2e)a_2 + \ldots + (r_k + n_ke)a_k =$$
$$= r_1'a_1 + r_2'a_2 + \ldots + r_k'a_k,$$

бу ерда $r_i + n_ie = r_i'$ $(i = \overline{1, k})$.

Демак, $\mathcal{K}$ ҳалқа бирлик элементга эга бўлганда $(a_1, a_2, \ldots, a_k)$ идеални аниқлаш учун $r_1a_1 + r_2a_2 + \ldots + r_ka_k)$ кўринишдаги йиғиндилар тўплами билан чегараланиш мумкин экан

45-§. Идеалларнинг баъзи бир содда хоссалари

$\mathcal{K}$ ҳалқанинг иккита I_1 ва I_2 идеали берилган бўлсин.

1-теорема. *$\mathcal{K}$ ҳалқа иккита идеалининг кесишмаси яна шу ҳалқанинг идеали бўлади.*

Исботи. I_1 ва I_2 лар $\mathcal{K}$ ҳалқанинг идеаллари бўлиб, уларнинг кесишмасини $I_1 \cap I_2$ орқали белгилайлик.

Фараз қилайлик, $a \in I_1 \cap I_2$ ва $b \in I_1 \cap I_2$ бўлсин. У ҳолда кесишманинг таърифига асосан $a \in I_1$, $a \in I_2$, $b \in I_1$, $b \in I_2$ бўлади. I_1 ва I_2 тўпламлар $\mathcal{K}$ да идеал бўлгани учун $a - b \in I_1$ ҳамда $a - b \in I_2$ бўлади. Охирги икки муносабатдан $a - b \in I_1 \cap I_2$ эканлиги келиб чиқади. Энди $(a \in I_1 \cap I_2) \wedge (r \in \mathcal{K}) \Rightarrow ar \in I_1 \cap I_2$ эканлигини келтириб чиқарамиз. $a \in I_1 \cap I_2 \Rightarrow a \in I_1$, $a \in I_2$ бўлиб, I_1, I_2 идеал бўлганидан $ra \in I_1$, $ra \in I_2$ бўлади.

Демак, $ra \in I_1 \cap I_2$ экан. Шундай қилиб, $I_1 \cap I_2$ тўплам a ва b элементлар билан бирликда уларнинг айирмаси ва $ra (r \in \mathcal{K})$ кўпайтмани ўз ичига олгани учун $I_1 \cap I_2$ тўплам ҳалқанинг идеали бўлади.

Бу теоремани чекли сондаги идеаллар кесишмаси учун ҳам исботлаш мумкин. Бу исбот худди юқоридаги усулда бажарилади

$\mathcal{K}$ ҳалқанинг идеаллари учун яна қўшиш, кўпайтириш, бўлиш ва илдиз чиқариш тушунчаларини ҳам киритиш мумкин. Бу амаллар билан танишишни истаган ўқувчиларга О. Зарицкий ва Н. Самюэлларнинг „Коммутативная алгебра“ китобини ҳавола қиламиз.

Энди $\mathcal{K}$ ҳалқанинг энг кичик идеали деган тушунчани киритамиз. Фараз қилайлик, $A \subset \mathcal{K}$ бўлсин. A тўпламни ўз ичига олувчи барча идеаллар кесишмасини $I(A)$ деб белгилаймиз ва $I(A)$ ни *A тўпламни ўз ичига олган энг кичик идеал* деб юритамиз. $I(A)$ ҳам 1-теоремага асосан идеал бўлади.

2-теорема. *$\mathcal{K}$ ҳалқанинг A тўпламни ўз ичига олувчи энг кичик $I(A)$ идеали A тўплам ёрдамида тузилган (A) идеал билан устма-уст тушади.*

Исботи. $A \subset (A)$ бўлгани учун (A) идеал A тўпламни ўз ичига олувчи идеаллардан биридир. Демак, $I(A) \subset (A)$. Иккинчидан, $A \subset (A)$ га кўра A тўпламнинг барча $a_1, a_2, \ldots, a_k$ элементлари ва $r_i \in \mathcal{K}$ бўлганда $r_1a_1 + r_2a_2 + \ldots + r_ka_k$ йиғиндилар $I(A)$ га тегишлидир. $\sum_{i=1}^{k} r_ia_i$ кўринишдаги элементлар тўплами эса (A) ни беради. Демак, $(A) \subset I(A)$ экан. У ҳолда юқоридаги тушунчалардан ушбу хулосага келамиз:

$$(I(A) \subset (A)) \wedge ((A) \subset I(A)) \Rightarrow (A) = I(A).$$

3-теорема. *Агар $\mathcal{K}$ ҳалқа бирлик элементга эга бўлиб, бу бирлик элемент идеалга тегишли бўлса, у ҳолда $I = \mathcal{K}$ булади.*

Исботи. Идеал таърифидаги б) қисмга асосан $\mathcal{K}$ ҳалқанинг исталган r элементи ва I идеалнинг ҳар қандай a элементи учун $ra \in I$ бўлиши керак эди. Агар $a = e$ десак, $re = r$ бўлади. Бу эса

$$\mathcal{K} \subseteq I \tag{1}$$

эканлигини билдиради. Идеал таърифига асосан эса

$$I \subseteq \mathscr{K}. \tag{2}$$

(1) ва (2) дан $\mathscr{K} = I$ бўлади.

4-теорема. *Нотривиал идеалларга эга бўлмаган ҳалқа майдон бўлади.*

Исбот. Фараз қилайлик, $\mathscr{K}$ ҳалқа фақатгина иккита (e) ва (0) идеалга эга бўлсин. $\mathscr{K}$ ҳалқадан бирор $a \neq 0$ элементни оламиз. $a \neq 0$ бўлгани учун бош идеал таърифига асосан

$$(a) \neq (0) \tag{3}$$

бажарилади. $\mathscr{K}$ ҳалқа фақатгина иккита идеалга эга бўлганидан (3) га кўра $(a) = (e)$ бўлади. Демак, $\mathscr{K}$ ҳалқада шундай a^{-1} элемент мавжудки натижада $a \times a^{-1} = e$ тенглик ўринли.

a элемент $\mathscr{K}$ ҳалқанинг нолдан фарқли ихтиёрий элементи эди. Нолдан фарқли ихтиёрий элемент тескариланувчан бўлгани учун $\mathscr{K}$ ҳалқа майдон бўлади.

46-§. Идеал бўйича таққослама ва чегирмалар синфлари. Фактор-ҳалқалар. Эпиморфизм ҳақида теорема

$\mathscr{K}$ ҳалқанинг исталган идеали шу ҳалқанинг аддитив группасининг қисм группаси бўлади. Аддитив группанинг исталган қисм группаси эса шу группанинг нормал бўлувчиси бўлади. Демак, группалар назариясида нормал бўлувчи тушунчаси қандай аҳамиятга эга булса, ҳалқалар назариясида идеаллар тушунчаси ҳам шундай аҳамиятга эгадир.

Ҳалқа идеалининг таърифига асосан $a, a_1 \in I$ бўлганда $a - a_1 \in I$ бўлар эди. Биз энди $a - a_1 \in I$ бўлганда

$$a \equiv a_1 \pmod{I} \tag{1}$$

каби ёзувни (белгилашни) киритамиз ва бу ёзувни a a_1 элементлар I модуль бўйича таққосланади деб ўқиймиз. (1) таққосламани қаноатлантирувчи барча элементлар тўпламини $\bar{a} = a_1 + I$ каби ёзиш мумкин. (1) муносабат ёрдамида $\mathscr{K}$ ҳалқа эквивалент синфларга ажралади. Шунинг учун $\bar{a} = a_1 + I$ синфга тегишли бўлмаган бирор b_1 элементни олсак, $b = b_1 + I$ синф ҳам мавжуд бўлади. Энди бу эквивалент синфлар тўпламини

$$\mathcal{K}/I = \{I,\ a_1 + I,\ b_1 + I,\ \ldots\}$$

деб оламиз ва унинг ҳалқа эканлигини кўрсатамиз. Бунинг учун $\mathcal{K}/I$ тўплам элементлари учун қўшиш ва кўпайтириш амалларини қуйидагича киритамиз:

$$\bar{a} + \bar{b} = a_1 + b_1 + I, \qquad (2)$$

$$\bar{a} \cdot \bar{b} = a_1 \cdot b_1 + I, \qquad (3)$$

яъни иккита синфни қўшиш (кўпайтириш) учун шу синфлардан ихтиёрий равишда биттадан олинган иккита элементни қўшиш (кўпайтириш) кифоя. Таққосламаларда бўлгани каби ҳар бир синфнинг ихтиёрий элементи шу *синфнинг I модулга кўра чегирмаси* дейилади. Яна шуни эслатиб ўтамизки, иккита синфни қўшиш ёки кўпайтириш бу синфларнинг қайси чегирмасини олишга боғлиқ эмас. Дарҳақиқат, $\bar{a}$ ва $\bar{b}$ синфлардан a_1 ва b_1 дан бошқа мос равишда яна биттадан a_2 ва b_2 элементларни олайлик. a_1, $a_2 \in \bar{a}$ ҳамда b_1, $b_2 \in \bar{b}$ бўлганидан $a_2 \equiv a_1 \pmod{I}$ ҳамда $b_2 \equiv b_1 \pmod{I}$ бўлади. Агар охирги иккита таққосламани қўшсак ва кўпайтирсак,

$$a_2 + b_2 \equiv a_1 + b_1 \pmod{I},$$

$$a_2 \cdot b_2 \equiv a_1 \cdot b_1 \pmod{I}$$

таққосламаларга эга бўламиз. Демак, I модуль бўйича тузилган синфларни қўшиш ва кўпайтириш бир қийматли усулда аниқланар экан.

Энди $\mathcal{K}$ ҳалқанинг элементлари учун φ акслантиришни қуйидагича аниқлаймиз:

(1) таққосламани қаноатлантирувчи ихтиёрий $a \in \mathcal{K}$ элементни φ мослик $\bar{a} = a + I$ синфга акслантирсин. Натижада, φ акслантириш $\mathcal{K}$ ҳалқани I модуль бўйича тузилган эквивалент синфлар тўпламига гомоморф акслантиради. Ҳалқанинг гомоморф тасвири яна ҳалқа бўлгани учун $\mathcal{K}/I$ ҳам ҳалқа бўлади. Ана шу ҳалқа *I модуль бўйича тузилган фактор-ҳалқа* деб аталади.

Мисол. Z ҳалқада $I = (5)$ идеал бўйича

$$\bar{0} = \{5k | k \in Z\},\quad \bar{1} = \{5k + 1 | k \in Z\},\quad \bar{2} = \{5k + 2 | k \in Z\}$$

$$\bar{3} = \{5k + 3 | k \in Z\},\quad \bar{4} = \{5k + 4 | k \in Z\}$$

бўлиб, $Z/(5) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ тўплам $I = (5)$ идеал бўйича фактор-ҳалқа бўлади.

Таъриф. h акслантириш $\mathscr{K}$ ҳалқани $\mathscr{K}'$ ҳалқа устига гомоморф акслантирсин, $\mathscr{K}'$ ҳалқанинг ноль элементига акслантирувчи $\mathscr{K}$ ҳалқанинг барча элементлари тўплами *h гомоморфлик ядроси* (ўзаги) дейилади ва у $I = \operatorname{Ker} h$ каби белгиланади.

Теорема (эпиморфизм ҳақидаги теорема). *$\mathscr{K}$ ҳалқа h акслантириш ёрдамида бирор $\mathscr{K}'$ ҳалқа устига гомоморф акслансин. I тўплам $\mathscr{K}$ нинг шундай элементлари тўплами бўлсинки, h акслантириш I нинг барча элементларини $\mathscr{K}'$ нинг ноль элементига акслантирсин. У ҳолда $\mathscr{K}'$ ҳалқа $\mathscr{K}/I$ га изоморф булади ва I тўплам $\mathscr{K}$ ҳалқанинг идеали булади.*

Исботи. I нинг идеал эканлигини кўрсатамиз. Ҳақиқатан,

1) $\forall m_1, m_2 \in I$ бўлганда, бу элементларнинг ҳар бири h акслантириш ёрдамида $0' \in \mathscr{K}'$ га ўтгани учун

$$h(m_1 - m_2) = h(m_1) - h(m_2) = 0' - 0' = 0' \in \mathscr{K}';$$

2) $\forall r \in \mathscr{K}$, $\forall m \in I$ учун $h(mr) = h(m) \cdot h(r) = 0' \times \times r' = 0' \in \mathscr{K}'$ шартлар бажарилганлиги учун I тўплам $\mathscr{K}$ ҳалқанинг идеалидир.

Энди $\mathscr{K}'$ ҳалқанинг битта a' элементига h ёрдамида аксланадиган $\mathscr{K}$ ҳалқа элементлари тўпламини $M_{a'}$ дейлик ва бу тўплам элементлари қандай хоссаларга эга эканлигини кўриб ўтайлик. Бунинг учун $M_{a'}$ тўпламдан бирор a, b элементларни олиб

$$a + x = b \tag{4}$$

тенгламани тузамиз. $M_{a'} \subseteq \mathscr{K}$ ва $\mathscr{K}$ ҳалқа бўлгани учун (4) тенглама доимо $\mathscr{K}$ га тегишли ягона ечимга эга. Шу ечимни биз m деб белгилайлик. У ҳолда

$$a + m = b \tag{5}$$

тенглик ўринли. Энди (5) тенгликнинг иккала томонига h акслантиришни татбиқ этамиз. Натижада

$$a' \oplus m' = b' \tag{6}$$

тенглик ҳосил бўлади.

Энди b элемент $M_{a'}$ қисм тўпламга тегишли бўлган ҳолни қараб ўтайлик. Бундай ҳолда h акслантириш b ни ҳам $a' \in \mathcal{K}'$ элементга ўтказгани учун (6) тенглик

$$a' \oplus m' = a' \tag{7}$$

кўринишни олади. Охирги тенгликдан $m' = 0'$ эканлиги аён. Демак, $m \in I$ экан. Агар, $M_{e'}$ қисм тўплам элементларига эътибор берсак, уларнинг барчаси $k \in Z$ бўлганда $a + km$ кўринишдаги элементлар тўпламидан, бошқача айтганда $\bar{a} = a + I$ синф элементларидан иборат. Демак, h акслантириш ёрдамида I модуль бўйича тузилган ҳар бир синфнинг барча элемантлари $\mathcal{K}'$ нинг битта элементига аксланади, ҳар хил синфлар эса $\mathcal{K}'$ нинг ҳар хил элементларига ўтади.

Энди $f : \mathcal{K}/I \to \mathcal{K}'$ акслантиришни қуйидагича киритамиз. $a' \in \mathcal{K}'$, $\bar{a} = a + I$ синфнинг ихтиёрий вакили (чегирмаси) бўлганда $f(\bar{a}) = h(a)$ деб оламиз. Юқорида кўриб ўтганимизга биноан $h : \mathcal{K} \to \mathcal{K}'$ устига гомоморф акслантириш (эпиморф акслантириш) бўлгани учун f ҳам эпиморф акслантириш бўлади.

Энди шу акслантиришнинг изоморф акслантириш эканлигини кўрсатамиз. $a \in \bar{a}$ ва $b \in \bar{b}$ бўлганда $f(\bar{a}) = f(\bar{b})$ бўлсин. Биз $\bar{a} = \bar{b}$ эканлигини кўрсатишимиз керак. Ҳақиқатан, $f(\bar{a}) = f(\bar{b})$ бўлганидан $h(a) = h(b)$. Бундан $0' = h(a) - h(b) = h(a - b)$ бўлгани учун $a - b \in I$. Демак, $a \equiv b \pmod{I}$, яъни $\bar{a} = \bar{b}$ экан. Шундай қилиб, f акслантириш изоморф акслантириш экан.

47-§. Коммутатив ҳалқада бўлиниш муносабати. Бутунлик соҳасининг туб ва мураккаб элементлари

Айтайлик, $\mathcal{K}$ бирлик элементга эга бўлган коммутатив ҳалқа (бутунлик соҳаси) бўлсин. Исталган майдонни бутунлик соҳаси деб қараш мумкин. Майдоннинг $a \neq 0$ ва ихтиёрий b элементлари учун

$$ax = b \tag{1}$$

тенглама доимо ягона ечимга эга бўлар эди. Агар қаралаётган бутунлик соҳаси майдон бўлмаса, (1) тенглама ечимга эга бўлмаслиги ёки унинг ечимлари сони бир нечта бўлиши мумкин. Бундай ҳолатларни атрофлича ўрганиш учун мос равишда ҳалқада бўлиниш муносабати ҳамда нолнинг бўлувчилари тушунчалари киритилади.

1-таъриф. Агар $\mathscr{K}$ ҳалқанинг исталган $a \neq 0$ ва b элементлари учун (1) тенглама $\mathscr{K}$ да ечимга эга бўлса, у ҳолда *a элемент b элементни бўлади* дейилади ва у b/a ёки $b \vdots a$ каби белгиланади.

b/a белги баъзан b элемент a га бўлинади, b элемент a элементнинг карралиси деб ўқилади. Юқоридаги таърифни предикатлар ёрдамида қуйидаги кўринишда ёзиш мумкин:

$$y/x \Leftrightarrow \exists z\,(xz = y). \qquad (2)$$

Агар 1-таърифни қаноатлантирувчи элемент мавжуд бўлмаса, *a элемент b ни бўлмайди* (*b элемент a га бўлинмайди*) деб юритилади ва у $b \times a$ каби белгиланади.

Теорема. *$\mathscr{K}$ бутунлик соҳасида аниқланган бўлиниш муносабати қуйидаги хоссаларга эга*:

а) $\forall a \in \mathscr{K}$ $(a \neq 0)$ *учун* $0/a$; a/e; a/a *дир* (*бунда* 0 *ва* e *лар мос равишда* $\mathscr{K}$ *нинг ноль ва бирлик элементларидир*);

б) $a \neq 0 \Rightarrow a \times 0 \wedge 0/a$;

в) $\forall a, b, c \in \mathscr{K}$ $(a/b \wedge b/c \Rightarrow a/c)$ $(b, c \neq 0)$;

г) $\forall a, b, c, d \in \mathscr{K}$ $(a/b \wedge c/d \Rightarrow ac/bd)$ $(b, d \neq 0)$;

д) $\forall a, b, 0 \neq c \in \mathscr{K}$ $(bc/ac \Rightarrow b/a)$;

е) $\forall a, a_i \in \mathscr{K}$ $(i = \overline{1, n})$ $(a_i/a \Rightarrow \sum\limits_{i=1}^{n} a_i r_i/a)$,

бу ерда $r_1, r_2, \ldots, r_n \in \mathscr{K}$.

Биз бу хоссалардан фақатгина д) ва е) қисмларини исбот қиламиз, қолганларини исботлашни эса ўқувчига тавсия қиламиз.

д) Ихтиёрий $c \neq 0$ учун bc/ac жумла (2) га биноан

$$bc = ac \cdot d \qquad (3)$$

кўринишда ёзилади. (3) тенгликни эса

$$c\,(b - ad) = 0 \qquad (4)$$

кўринишда ёзиш мумкин. Бутунлик соҳаси нолнинг бўлувчиларига эга бўлмагани учун (4) тенглик, фақатгина

$$b = ad \qquad (5)$$

бўлгандагина бажарилади. Охирги тенглик эса b/a эканлигини билдиради.

е) нинг исботи. a_i/a $(i=\overline{1, n})$ бўлгани учун яна (2) га асосан

$$\begin{aligned} a_1 &= ab_1, \\ a_2 &= ab_2, \\ &\dots\dots \\ a_n &= ab_n \end{aligned} \tag{6}$$

тенгликлар системасини ёза оламиз. Бў тенгликларни мос равишда $r_1, r_2, \dots, r_n$ га кўпайтириб, қўшсак,

$$\sum_{i=1}^{n} a_i r_i = a \sum_{i=1}^{n} b_i r_i \tag{7}$$

ҳосил бўлади. Бу тенглик эса $\sum\limits_{i=1}^{n} a_i r_i/a$ эканлигини билдиради.

Рационал сонлар ҳалқасида нолдан фарқли барча элементлар бирнинг бўлувчилари бўлади.

Ҳалқаниг ихтиёрий a элементи ε (тескариланувчи элемент) ва $a\varepsilon$ га доимо бўлинади. ε ва $a\varepsilon$ элементлар одатда a нинг *тривиал* (*энг содда*) *бўлувчилари* деб юритилади.

$a \in \mathcal{K}$ нинг қолган барча бўлувчилари (агар шундай элементлар мавжуд бўлса) унинг *тривиал бўлмаган бўлувчилари* дейилади.

Масалан, Z тўпламда 8 нинг тривиал бўлувчилари -1, 1 ва -8, 8 бўлиб, тривиал бўлмаган бўлувчилари эса -4, -2, 2, 4 дан иборат.

2-таъриф. Бирлик элементга эга бўлган $\mathcal{K}$ бутунлик соҳасининг нолдан, бирнинг бўлувчиларидан фарқли бирор p элементи фақатгина тривиал бўлувчиларга эга бўлса, у ҳолда бундай p элемент $\mathcal{K}$ бутунлик соҳасининг *туб* ёки *ёйилмайдиган элементи* дейилади.

3-таъриф. Бирлик элементга эга бўлган $\mathcal{K}$ бутунлик соҳасининг бирор a элементи нолдан ва бирнинг бўлувчиларидан фарқли бўлиб, тривиал бўлмаган бўлувчиларга эга бўлса, у ҳолда a элемент $\mathcal{K}$ бутунлик соҳасининг *мураккаб* (*ёйилувчи*) *элементи* дейилади.

Мисол. Z тўпламнинг ± 2, ± 3, ± 5, ± 7, ± 11, ... элементлари туб элементлар, ± 4, ± 6, ± 8, ... элементлари эса мураккаб элементлардир.

3-таърифга асосан p туб элемент бўлиб, $p = a \cdot b$ тенглик бажарилса, ё a, ёки b бирнинг бўлувчилари бўлади. $p = a \cdot b$ тенгликда a ва b нинг иккаласи ҳам бирнинг бўлувчилари бўлмаса, p элемент мураккаб бўлади.

Натижа. Исталган майдон ҳеч қандай туб ёки мураккаб элементларга эга бўлмайди.

48-§. Бош идеаллар ҳалқаси. Евклид ҳалқаси

Маълумки, бутун сонлар ҳалқаси элементлари учун энг катта умумий бўлувчиси (ЭКУБ), энг кичик умумий каррали (ЭКУК), мураккаб ва туб сонлар, исталган мураккаб сонни туб сонлар кўпайтмаси шаклида ёзиш каби тушунчалар мавжуд эди. Бундай тушунчалар исталган ҳалқа элементлари учун ҳам ўринли бўлавермайди. Бу тушунчалар фақатгина бош идеаллар ҳалқаси деб аталувчи ҳалқа элементлари учунгина ўринли бўлади.

1-таъриф. Ҳар бир идеали бош идеалдан иборат бўлган ҳалқалар *бош идеаллар ҳалқаси* дейилади.

Мисоллар. **1.** Ҳар қандай $\mathscr{P}$ майдон бош идеаллар ҳалқаси бўлади, чунки майдон фақатгина иккита идеалга эга. Улар (0) ва $(e) = \mathscr{P}$ бош идеаллардир.

2. Бутун сонлар ҳалқаси бош идеаллар ҳалқасидир (исбот қилинг).

2-таъриф. Агар бирлик элементга эга бўлган $\mathscr{B}$ бутунлик соҳаси берилган бўлиб, унинг барча элементларини манфиймас бутун сонлар тўплами N_0^+ га бир қийматли акслантирувчи шундай φ акслантириш мавжуд бўлсаки, унинг учун қуйидаги шартлар бажарилса, яъни

1) $\mathscr{P}$ нинг исталган a ва b элементлари учун шундай бир жуфт $q, r \in \mathscr{P}$ элементлар топилсаки, улар учун

$$a = bq + r \qquad (1)$$

тенглик ўринли;

2) (1) тенгликда $r=0$ ёки $\varphi(r)<\varphi(q)$ бўлса, у ҳолда, $\mathcal{K}$ бутунлик соҳаси *Евклид ҳалқаси* дейилади.

Мисоллар. 1. Z ҳалқа Евклид ҳалқаси бўлади. Ҳақиқатан, $\forall x \in Z$ учун $\varphi(x)=|x|$ десак, Евклид ҳалқаси таърифидаги иккита шарт бажарилади.

2. Ҳар қандай майдон Евклид ҳалқаси бўлади (исбот қилинг).

1-теорема. *$\mathcal{K}$ бош идеаллар ҳалқасининг камида биттаси нолдан фарқли бўлган $a_1, a_2, \ldots, a_n$ элементлари учун ЭКУБ мавжуд ва у бирнинг бўлувчиси кўпайтмаси аниқлигида ягонадир. $d \in \mathcal{K}$ элемгнт $a_1, a_2, \ldots, a_n$ элементларнинг ЭКУБи бўлиши учун*

$$a_i=dq_i \ (i=\overline{1, n}) \tag{2}$$

$$d=a_1r_1+a_2r_2+\ldots+a_nr_n \tag{3}$$

тенгликлар $\mathcal{K}$ ҳалқанинг баъзи бир $q_1, q_2, \ldots, q_n$ ва $r_1, r_2, \ldots, r_n$ элеменшлари учрн бажарилиши зарур ва етарли.

Исботи. 1. Зарурийлик шарти. Фараз қилайлик, $\mathcal{K}$ ҳалқанинг бирор A қисм тўплами элементлари (3) кўринишга эга бўлсин. Бундай ҳолда A идеал эканлиги бизга маълум. $\mathcal{K}$ ҳалқа бош идеаллар ҳалқаси бўлгани учун унинг ҳар бир идеали, шу жумладан, A ҳам бош идеалдир. Демак, шундай $d \in \mathcal{K}$ топиладики, $A=(d)$ бўлади.

Энди $d \in \mathcal{K}$ элемент $a_1, a_2, \ldots, a_n$ элементлар учун ЭКУБ бўлишини кўрсатамиз.

Агар $r_i=e$ ва $k \neq i$ да $r_k=0$ десак, $a_1r_1+a_2r_2+ +\ldots+a_nr_n$ йиғинди a_i кўринишни олади. Демак, $a_i \in A$ бўлиб, $A=(d)$ эканлигига асосан a_i элемент d га бўлинади, яъни (2) ҳосил бўлади. Теорема шартига биноан a_i $(i=\overline{1, n})$ лардан камида биттаси нолдан фарқли эди. Бундан $d \neq 0$ деган хулосага келамиз. $d \in A$ бўлгани учун (3) тенглик ўринли бўлади.

2. Етарлилик шарти. (2) ва (3) тенгликларни қаноатлантирувчи ҳар қандай $d \in \mathcal{K}$ элемент $a_1, a_2, \ldots, a_n$ элементлар учун ЭКУБ бўлади. Ҳақиқатан, (2) тенгликлар барча a_i $(i=\overline{1, n})$ ларнинг d га бўлинишини кўрсатади, яъни d — умумий бўлувчи. Иккинчидан, бирор $b \in \mathcal{K}$ бошқа бирор умумий бўлувчи бўлса,

$d \in \mathcal{K}$ элемент b га бўлинади, чунки $a_i = bq_i'$ бўлса, (3) тенгликка асосан

$$d = b(q_1'r_1 + q_2'r_2 + \ldots + q_n'r_n)$$

тенглик ўринли.

Энди ЭКУБ бирнинг бўлувчиси кўпайтмаси аниқлигида ягона эканлигини кўрсатамиз. Агар $\varepsilon \in \mathcal{K}$ бирнинг бўлувчиси бўлса, у ҳолда (2) тенгликни

$$a_i = (\varepsilon d)\cdot(\varepsilon^{-1}q_i) \ (i = \overline{1,\ n}) \qquad (2')$$

каби ёзиш мумкин. Бундай ҳолда (3) тенглик

$$\varepsilon d = a_1(r_1\varepsilon) + a_2(r_2\varepsilon) + \ldots + a_n(r_n\varepsilon) \qquad (3')$$

каби бўлади. (2′) ва (3′) тенгликлар εd нинг ҳам a_1, a_2, ..., a_n лар учун ЭКУБ бўлишини кўрсатади. d ва εd эса бир-биридан бирнинг бўлувчиси кўпайтмасига фарқ қилади, холос.

Мазкур теорема бош идеаллар ҳалқасининг чекли сондаги элементлари учун ЭКУБ нинг мавжудлигини кўрсатади.

a_1, a_2, ..., a_n элементларнинг ЭКУБ ни топиш масаласини иккита элементнинг ЭКУБ ни топиш масаласига келтириш мумкин. Ҳақиқатан, $d_1 = (a_1, a_2)$ бўлса, юқоридаги теоремага биноан шундай r_1, $r_2 \in \mathcal{K}$ лар топиладики, натижада $d_1 = a_1r_1 + a_2r_2$ бўлади. Фараз қилайлик, a_1, a_2, a_3 элементлар ЭКУБ ни d_2 деб олайлик. d_2 элемент a_1 ва a_2 элементларни бўлгани учун у d_1 ни ҳам бўлиши керак.

Демак, d_1 ва a_3 нинг ЭКУБ a_1, a_2, a_3 элементларнинг ЭКУБ билан бир хил бўлади. Бу фикрни давом эттирсак

$$d_k = (a_1, a_2, \ldots, a_k) = (d_{k-1}, a_k)$$

тенгликка келамиз, бу ерда $d_{k-1} = (a_1, a_2, \ldots, a_{k-1})$ дир. Демак, n та элементнинг ЭКУБ ни топиш масаласи иккита элементнинг ЭКУБ ни топиш масаласига келтирилди. Евклид ҳалқаларида иккита элемент ЭКУБ ни топиш Евклид алгоритми деб аталувчи кетма-кет бўлиш усули ёрдамида топилади. $\mathcal{K}$ Евклид ҳалқаси ва унинг иккита a ва b элементи берилган бўлсин. Бунда қуйидаги икки ҳол бўлади:

а) Агар $b = 0$ бўлса, $(a;\ 0) = a$;

б) Агар $b \neq 0$ бўлса, a ни b га, b ни эса қолдиққа, сўнгра олдинги қолдиқларни кейинги қолдиқларга бўлиш натижасида қуйидаги кетма-кетликлар системаси ҳосил қилинади:

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\cdots\cdots \\ r_{k-2} &= r_{k-1}q_k + r_k, \\ r_{k-1} &= r_kq_{k+1}. \end{aligned} \tag{4}$$

(4) тенгликлар бажарилганда

$$\varphi(r_k) < \varphi(r_{k-1}) < \ldots < \varphi(r_1) < \varphi(b)$$

бўлар эди. $\varphi(r_i)$ $(i = \overline{1, k})$ лар манфиймас бутун сонлардир. Ҳар қандай манфиймас бутун сонлар тўплами эса доимо қуйидан чегараланган. Шунинг учун k қадамдан сўнг $r_{k+1} = 0$ бўлади. Бундай ҳолда $r_k \neq 0$ бўлиб, у биз излаган ЭКУБ бўлади.

$d = r_k$ учун ЭКУБ нинг иккала шарти бажарилишини текшириб кўришни ўқувчига тавсия қиламиз.

2-теорема. *Евклид ҳалқаси бош идеаллар ҳалқаси бўлади.*

Исботи. Фараз қилайлик, $\mathscr{K}$ Евклид ҳалқаси бўлиб, A унинг бирор идеали бўлсин. A нинг бош идеал эканлигини кўрсатамиз. Бу ерда қуйидаги икки ҳол бўлиши мумкин:

а) A тўплам фақат биттагина ноль элементга эга. Унда $A = (0)$ бош идеалдир.

б) $A \neq (0)$ бўлсин. $\mathscr{K}$ ҳалқа Евклид ҳалқаси бўлгани учун $\mathscr{K}$ даги ҳар қандай нолдан фарқли a элементни манфиймас бутун сонга акслантирувчи ҳамда

$$a = bq + r$$

ва $r = 0$ ёки $\varphi(r) < \varphi(b)$ шартларни қаноатлантирувчи $\varphi: \mathscr{K} \to N_0^+$ акслантириш мавжуд. Лекин манфиймас бутун сонларнинг ҳар қандай қисм тўплами қуйидан чегараланган. Демак, φ акслантириш ёрдамида энг кичик манфиймас бутун сонга акслантирувчи $d \in A$ элемент мавжуд. Натижада A тўпламнинг ихтиёрий a элементини

$$a = dq + r,\ 0 \leqslant \varphi(r) < \varphi(d) \tag{5}$$

каби ёза оламиз.

Энди A дан олинган ихтиёрий a элементнинг d га бўлинишини кўрсатамиз. $a = dq + r \Rightarrow a - dq = r$. Бунда $r \in A$, чунки $a \in A$ ва $d \in A$ эди. Шунинг учун $r \neq 0$ бўлса, $\varphi(d) > \varphi(r)$ бўлар эди, бу эса $\varphi(d)$ нинг энг кичик манфиймас бутун сон эканлигига зид. Шунинг учун $r = 0$ бўлиб, a элемент d га бўлинади, яъни $A = (d)$ бош идеал бўлади.

49-§. Бутунлик соҳасининг нисбатлар майдони

Маълумки, ҳалқалар икки хил бўлар эди: 1) нолнинг бўлувчиларига эга бўлган ҳалқалар; 2) нолнинг бўлувчисига эга бўлмаган ҳалқалар.

Нолнинг бўлувчисига эга бўлмаган коммутатив ҳалқа бутунлик соҳаси дейилар эди.

Барча сонли ҳалқалар бутунлик соҳаси бўлади. Ҳалқа элементларидан жуфтликлар тузиб, бу жуфтликлар тўпламида қўшиш ва кўпайтириш амалларини қуйидагича киритамиз:

$$<a;\ b> + <c;\ d> = <ad + bc;\ bd>,$$
$$<a;\ b> \cdot <c;\ d> = <ac;\ bd>.$$

Агар ҳалқалар тушунчасига эътибор берсак, ҳалқаларнинг баъзи бирларини қандайдир майдон ичига жойлаш мумкинлигини пайқаймиз. Масалан, Z ҳалқа Q майдон учун қисм тўпламдир. Қандай ҳалқаларни майдон ичига жойлаш мумкин деган саволга қуйидаги теорема орқали жавоб бериш мумкин:

Теорема. *Ҳар қандай бутунлик соҳасини майдон ичига жойлаш мумкин.*

Исботи. $\mathcal{K}$ бутунлик соҳаси берилган бўлсин. $\mathcal{K}$ нинг элементлари ёрдамида мумкин бўлган барча $<a;\ b>$ жуфтликлар тўпламини тузиб, $(b \neq 0)$ бу тўпламни P деб олайлик, яъни

$$P = \{<a;\ b> \mid a,\ b \in \mathcal{K},\ b \neq 0\}$$

бўлсин. P тўплам элементлари учун қуйидагича аниқланган муносабатни киритайлик:

$$<a;\ b> \sim <a_1;\ b_1> \Longleftrightarrow ab_1 = a_1 \cdot b. \qquad (1)$$

Бу муносабат (унинг рефлексив, симметрик ва транзитив эканлигини текшириб кўринг) эквивалентлик муносабати бўлади ва P тўпламни ўзаро кесишмайдиган эквивалентлик синфларига ажратади.

Таъриф. $\mathscr{F}$ майдон ва $\mathscr{K}$ бутунлик соҳаси берилган бўлса, у ҳолда қуйидаги шартларни қаноатлантирган $\mathscr{F}$ майдон бутунлик соҳасининг нисбатлар майдони дейилади:

1) $\mathscr{K}$ бутунлик соҳаси $\mathscr{F}$ майдоннинг қисм ҳалқаси;

2) $\mathscr{F}$ даги ихтиёрий x элемент учун $\mathscr{K}$ да $x = a \cdot b^{-1}$ тенгликни қаноатлантирадиган a ва b элементлар мавжуд бўлса, $<a; b>$ жуфтлик ва унга эквивалент бўлган барча жуфтликлар синфини $\overline{a; b>}$ каби белгилайлик. Барча эквивалентлик синфлари тўпламини 7 орқали белгилаймиз ва унинг элементлари (синфлар) учун қўшиш ва кўпайтириш амалларини қуйидагича киритамиз:

$$\overline{<a; b>} + \overline{<c; d>} = \overline{<ad+bc; bd,>} \qquad (2)$$

$$\overline{<a; b>} \cdot \overline{<c; d>} = \overline{<ac; bd} >. \qquad (3)$$

Шундай қилиб, иккита эквивалентлик синфлари йиғиндиси ва кўпайтмаси яна эквивалентлик синфи бўлар экан.

Лекин бу йиғинди ва кўпайтмалар ягона усулда аниқланадими? Бошқача айтганда, улар синфлардан олинган жуфтликларнинг танланишга боғлиқ бўладими? Ҳозир шу масалани ҳал қилишга ўтамиз. Бунинг учун

$$<a; b> \sim <a_1; b_1> \Longleftrightarrow ab_1 = a_1 b, \qquad (1)$$

$$<c; d> \sim <c_1; d_1> \Longleftrightarrow cd_1 = c_1 d \qquad (4)$$

муносабатларни олиб, улар учун

$$<ad + bc; \; bd> \sim <a_1 d_1 + b_1 c_1; \; b_1 d_1>, \qquad (5)$$

$$<ac; \; bd> \sim <a_1 c_1; \; b_1 d_1> \qquad (6)$$

эквивалентликлар бажарилишини кўрсатамиз. (5) ва (6) эса ўз навбатида

$$<ad + bc> b_1 d_1 = <a_1 d_1 + b_1 c_1> bd, \qquad (5')$$

$$ac \cdot b_1 d_1 = bd \cdot a_1 c_1 \qquad (6')$$

га тенг кучли.

Аввало (5) тенгликнинг ўринли эканлигини кўрсатамиз. Бунинг учун унинг чап томонини

$$adb_1 d_1 + bcb_1 d_1 \qquad (7)$$

шаклда ёзиб оламиз ва (4) га асосан (7) даги ab_1 ни a_1b билан ҳамда cd_1 ни c_1d билан алмаштирамиз. У ҳолда

$$a_1bdd_1 + bb_1c_1d = bd\,(a_1d_1 + b_1c_1)$$

тенгликка эга бўламиз. Демак, (5) тенглик ўринли экан ((6) нинг ўринли эканлигини мустақил ҳолда текширинг). $b \neq 0$ бўлганда $(\overline{0; b})$ синф T тўпламнинг ноль элементини, $(\overline{b; b})$ синф эса T нинг нейтрал элементини ташкил этади. Ҳақиқатан,

а) $<\overline{c; d}> + <\overline{0; b}> = <\overline{bc + 0 \cdot d; bd}> = <\overline{c; d}>$,

б) $<\overline{c; d}> \cdot <\overline{b; b}> = <\overline{cb; db}> = (\overline{c; d})$.

Булардан ташқари, в) T тўпламнинг исталган нолмас $<\overline{a; b}>$ $(a \neq 0,\ b \neq 0)$ синфи учун $<\overline{b; a}>$ каби тескари элемент мавжуд.

г) $<\overline{a; b}>$, $<\overline{c; d}>$, $<\overline{e; f}> \in T$ учун

$$(<\overline{a; b}> + <\overline{c; d}>) \cdot <\overline{e; f}> =$$
$$= <\overline{a; b}><\overline{e; f}> + <\overline{c; d}> \cdot <\overline{e; f}> \qquad (8)$$

тенглик бажарилади. Чунки (8) нинг чап томонини оладиган бўлсак, уни қуйидагича ёзиш мумкин:

$$((\overline{a; b}) + (\overline{c; d}))(\overline{e; f}) = (\overline{ad + bc; bd}) \cdot (\overline{e; f}) =$$
$$= <\overline{ade + bce; bdf}>. \qquad (9)$$

(8) нинг ўнг томони эса $<\overline{a; b}> \cdot <\overline{e; f}> + <\overline{c; d}> \times$ $\times <\overline{e; f}> = <\overline{ae; bf}> + <\overline{ce; df}> = <\overline{aedf + bfce; bdf^2}> =$ $= (\overline{ade + bce; bdf})$, $(f \neq 0)$ бўлгани учун (8) тенглик ўринли.

д) $<\overline{a; b}>$ синф учун $<\overline{-a; b}>$ синф қарама-қарши синф бўлади (текшириб кўринг).

е) Учта синфни қўшиш амали ассоциатив бўлади (текшириб кўринг). Шундай қилиб, T тўплам майдон экан. Энди $\mathscr{K}$ ҳалқани T майдон ичига жойлаш мумкин эканлигини кўрсатамиз Бунинг учун $\mathscr{K}$ нинг элементлари T нинг қандайдир элементларига айнан мос келишини кўрсатиш кифоя. Бу мосликни қуйидагича киритамиз: $\mathscr{K}$ ҳалқанинг ихтиёрий c элементига T майдонининг $(\overline{bc; b})$ синфини мос қўямиз (бу ерда $b \neq 0$). Бу мослик ўзаро бир қийматли бўлади. Ҳақиқатан, а) агар $c \to \overline{<cb_1;\ b_1>}$ каби бўлиб, c га яна бирорта синф мос келади десак, бу синфлар устма-уст тушади, чунки $cb_1b = cbb_1$, бундан $<bc; b> \sim <cb_1; b_1>$ муносабатдан $\overline{<bc;\ b>} = \overline{<b_1c;\ b_1>}$ тенглик келиб чиқади:

б) ҳар хил c ва c_1 ларга ҳар хил синфлар мос келади, чунки $c \to \overline{<cb; b>}$ ва $c_1 \to \overline{<c_1b_1, b_1>}$ бўлиб, $\overline{<cb; b>} = \overline{(c_1b_1;\ b_1)}$ бўлганда эди,

$$cbb_1 = c_1b_1b \Rightarrow c = c_1\ (b \neq 0,\ b_1 \neq 0)$$

бўлар эди. Бу эса $c \neq c_1$ деган фаразга зид.

$c \to \overline{<bc;\ b>}$ мосликнинг изоморфизм эканини, яъни қуйидаги тенгликлар бажарилишини кўрсатамиз;

$$\overline{<ad;\ a> + <bc;\ b>} = \overline{<ad,\ a>} + \overline{<bc;\ b>}, \qquad (10)$$

$$\overline{<ad; a> \cdot \quad bc;\ b>} = \overline{<ad;\ a>} \cdot \overline{bc;\ b>}. \qquad (11)$$

Ҳақиқатан, $<ad;\ a> + <bc; b> = <adb + abc; ab> = <kd + kc;\ k>$ (бунда $ab = k$ каби белгиладик) бўлганидан $c + d \to <kd + kc;\ k>$ мослик ўринли ва (10) тенглик бажарилади.

$<ad; a> \cdot <bc; b> = <ad \cdot bc; ab>$ тенгликка асосан, $cd \to \overline{(ad \cdot bc;\ ab)}$ мослик ўринли бўлади ва (11) тенглик бажарилади.

T майдондаги барча $\overline{<bc; b>}$ кўринишдаги элементларни c элемент билан, қолган барча элементларни ўзини-ўзига алмаштирамиз. Натижада ҳосил бўлган тўпламни T' билан белгиласак, юқоридаги акслантиришга асосан T майдон T' тўпламга изоморф акслана-ди ва T майдон бўлгани учун T' ҳам майдон ташкил қилади ҳамда T' майдон $\mathcal{K}$ бутунлик соҳасини ўз ичига олади.

IV боб. БИР НОМАЪЛУМЛИ КЎПҲАДЛАР

50-§. Ҳалқанинг оддий трансцендент кенгайтмаси

Айталик $\mathscr{K}$ ва L коммутатив ҳалқалар бўлсин.

1-таъриф. Агар қуйидаги иккита шарт бажарилса, у ҳолда L ҳалқа x элемент бўйича $\mathscr{K}$ ҳалқанинг *оддий кенгайтмаси* дейилади:

1) $\mathscr{K}$ ҳалқа L ҳалқанинг қисм ҳалқаси;

2) L даги ихтиёрий a элемент

$$a = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \, (\alpha_i \in \mathscr{K}, \ i = \overline{0, n})$$

кўринишда ифодаланади,

Келгусида L ҳалқа x элемент бўйича $\mathscr{K}$ ҳалқанинг оддий кенгайтмаси эканлиги $L = \mathscr{K}[x]$ кўринишда белгиланади.

2-таъриф. Агар $L = \mathscr{K}[x]$ оддий кенгайтмада $\mathscr{K}$ ҳалқанинг ихтиёрий $\alpha_0, \alpha_1, \ldots, \alpha_n$ элементлари учун $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n = 0$ тенгликдан $\alpha_0 = 0$, $\alpha = 0$, $\ldots$, $\alpha_n = 0$ экани келиб чиқса, у ҳолда $L = \mathscr{K}[x]$ ҳалқа $\mathscr{K}$ ҳалқанинг *оддий трансцендент кенгайтмаси* дейилади

3-таъриф Агар $L = \mathscr{K}[x]$ ҳалқа x элемент бўйича $\mathscr{K}$ ҳалқанинг оддий кенгайтмаси бўлса ва x элемент 2-таърифдаги шартни қаноатлантирса, у ҳолда x элемент $\mathscr{K}$ га нисбатан L нинг *трансцендент элементи* дейилади.

4-таъриф. Агар $\mathscr{K}[x]$ ҳалқа x элемент бўйича $\mathscr{K}$ ҳалқанинг оддий трансцендент кенгайтмаси бўлса, у ҳолда $\mathscr{K}[x]$ ҳалқа *$\mathscr{K}$ устида x элемент бўйича тузилган кўпҳадлар ҳалқаси* дейилади. $\mathscr{K}[x]$ ҳалқанинг элементлари $\mathscr{K}$ устида *x нинг кўпҳадлари ёки $\mathscr{K}$ устида кўпҳадлар дейилади* ва унинг элементлари

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

$$(a_i \in \mathscr{K}, \ i = \overline{0, n}, \ \forall n \in N)$$

кўринишда ёзилади.

51-§. Кўпҳадлар устида амаллар

Айтайлик, $\mathscr{K}$ бутунлик соҳаси берилган бўлсин. $\mathscr{K}$ га тегишли бўлмаган x элементни олиб, ушбу ифодани тузамиз:

$$a_0+a_1x+a_2x^2+\ldots+a_nx^n=\sum_{\nu=0}^{n}a_\nu x^\nu$$

$$(a_\nu\in\mathscr{K},\ \nu=\overline{0,\ n};\ \forall n\in N). \qquad (1)$$

1-таъриф. Агар $a_n\neq0$ бўлса, у ҳолда (1) ифода *бир номаълумли n-даражали кўпҳад* дейилади, бунда $a_\nu x^\nu$ $(\nu=\overline{0,\ n})$ лар *кўпҳаднинг ҳадлари*, a_ν $(\nu=\overline{0,\ n})$ лар эса бу *кўпҳаднинг коэффациентлари* дейилади.

Таърифга асосан $7x^3-5\sqrt{x}+2x^2-3$ ва $\frac{1}{x^5}-3x^2+7x-5$ ифодалар кўпҳад бўлмайди.

Кўпҳадлар баъзан номаълум даражаларининг пасайиш тартибида

$$a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=\sum_{\nu=0}^{n}a_\nu x^{n-\nu}$$

каби ҳам ёзилади.

Бир номаълумли кўпҳадлар одатда $f(x)$, $g(x)$, $\varphi(x)$, ... каби белгиланади.

Айтайлик, $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ бирор кўпҳад бўлсин.

2-таъриф. $a_n\neq0$ бўлганда a_nx^n ҳад $f(x)$ кўпҳаднинг *бош ҳади*, a_0 эса *озод ҳади* дейилади.

Энди иккита кўпҳаднинг формал-алгебраик маънодаги тенглик тушунчасини киритамиз.

Иккита кўпҳаднинг нолли (коэффициентлари нолга тенг) ҳадларидан бошқа барча мос номерли ҳадлари бир-бирига тенг бўлганда ва фақат шундагина улар ўзаро тенг деб аталади.

Масалан, $3+0\cdot x+0\cdot x^2+0\cdot x^3+x^4+2x^5$, $3+x^4+2x^5$ кўпҳадлар ўзаро тенгдир.

Кўпҳадлар тенглиги символик равишда қуйидагича ёзилади:

$$(\forall a_\nu,\ b_\nu\in\mathscr{K})\ a_\nu=b_\nu\Longleftrightarrow\left(\sum_{\nu=0}^{n}a_\nu x^\nu=\sum_{\nu=0}^{n}b_\nu x^\nu\right).$$

Иккита

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = \sum_{k=0}^{n} a_kx^k,$$

$$\varphi(x) = b_0 + b_1x + b_2x^2 + \ldots + b_sx^s = \sum_{l=0}^{s} b_lx^l$$

кўпҳаднинг йиғиндиси деб

$$f(x) + \varphi(x) = \sum_{\nu=0}^{t} c_\nu x^\nu$$

кўпҳадни тушунамиз, бу ерда $t = \max(n; s)$, $c_\nu = a_\nu + b_\nu$ бўлиб, агар $n > s$ бўлса $b_{s+1} = b_{s+2} = \ldots = b_n = 0$. Агар $s > n$ бўлса, $a_{n+1} = a_{n+2} = \ldots = a_s = 0$ деб олинади.

Яна шуни таъкидлаймизки, $a_\nu, b_\nu \in \mathcal{K} \Rightarrow a_\nu + b_\nu \in \mathcal{K}$ ва йиғинди кўпҳаднинг даражаси қўшилувчи кўпҳадларнинг даражасидан катта эмас. Агар $a_n \neq -b_n$ $(n \geqslant s)$ бўлса, йиғиндининг даражаси қўшилувчи кўпҳадларнинг даражасидан катта эмас, чунончи ҳатто кичик ҳам бўлиши мумкин, масалан, $a_n = -b_n$ $(n = s)$ бўлган ҳол.

Кўпҳадлар тўпламида айириш амали ўринли. Бу тўпламда ноль элемент деб барча коэффициентлари ноллардан иборат кўпҳад олинади.

$f(x)$ кўпҳад учун

$$-f(x) = -a_0 - a_1x - a_2x^2 - \ldots - a^nx^n$$

кўпҳад *қарама-қарши кўпҳад* дейилади.

Энди $f(x)$ ва $\varphi(x)$ кўпҳадларнинг кўпайтмаси тушунчасини киритамиз. $f(x)$ ва $\varphi(x)$ кўпҳадлар *кўпайтмаси* деб коэффициентлари

$$d_\nu = \sum_{k+l=\nu} a_kb_l \quad (\nu = \overline{0; n+s})$$

тенглик билан аниқланувчи кўпҳадни айтилади. Бу ерда

$$d_0 = a_0b_0,\ d_1 = a_0b_1 + a_1b_0,\ d_2 = a_0b_2 + a_1b_1 + a_2b_0, \ldots$$
$$d_s = a_0b_s + a_1b_{s-1} + \ldots + a_sb_0, \ldots$$

Кўпҳадларнинг коэффициентлари $\mathcal{K}$ бутунлик соҳасига тегишли бўлгани учун $a_n \neq 0$ ва $b_s \neq 0$ бўлганда

$a_n b_s = d_{n+s} \neq 0$ бўлиб, кўпҳадлар кўпайтмасининг даражаси улар даражаларининг $n+s$ йиғиндисига тенг бўлади.

Теорема. *Кўпҳадлар тўплами ҳалқа бўлади.*

Исботи. Иккита кўпҳаднинг йиғиндиси ва кўпайтмаси яна кўпҳад эканлигини биз юқорида кўриб ўтдик. Энди кўпҳадлар тўплами учун ҳалқанинг қолган шартлари бажарилишини кўрсатамиз. Ҳақиқатан,

1) агар a_ν ва b_ν лар $f(x)$ ва $\varphi(x)$ кўпҳадларнинг коэффициентлари бўлса, у ҳолда

$$(\forall a_\nu,\ b_\nu \in \mathcal{K})\ a_\nu + b_\nu = b_\nu + a_\nu$$

бўлгани учун

$$f(x) + \varphi(x) = \sum_{\nu=0}^{t}(a_\nu + b_\nu)x^\nu = \sum_{\nu=0}^{t}(b_\nu + a_\nu)x^\nu =$$

$$= \sum_{\nu=0}^{s} b_\nu x^\nu + \sum_{\nu=0}^{n} a_\nu x^\nu = \varphi(x) + f(x)$$

бўлади, яъни кўпҳадларни қўшиш коммутативдир.

2) $f(x)\varphi(x) = \varphi(x)\cdot f(x)$ (кўпайтириш амали коммутативдир). Кўпҳадларнинг коэффициентлари $\mathcal{K}$ бутунлик соҳасига тегишли бўлганлиги ҳамда $\sum\limits_{k+l=\nu} a_k b_l = \sum\limits_{l+k=\nu} b_l a_k$ бўлгани учун $f(x)\varphi(x) = \varphi(x)\cdot f(x)$ тенглик ўринлидир.

3) Кўпҳадларни кўпайтириш ассоциативдир, яъни

$$f(x)(\varphi(x)\cdot g(x)) = (f(x)\cdot\varphi(x))\cdot g(x). \qquad (2)$$

Бу тенгликни исботлаш учун яна бир

$$g(x) = c_0 + c_1x + c_2x^2 + \ldots + c_tx^t \quad (c_t \neq 0)$$

кўпҳадни оламиз. $f(x)$, $\varphi(x)$ ва $g(x)$ мос равишда n, s ва t даражали бўлганидан $(f(x)\cdot\varphi(x))\cdot g(x)$ кўпҳаддаги $x^i = (i = 0, 1, 2, \ldots, n+s+t)$ нинг коэффициенти

$$\sum_{j+m=i}\left(\sum_{k+l=j} a_k b_l\right)\cdot c_m = \sum_{k+l+m=i} a_k b_l c_m$$

йиғинди орқали аниқланади. $f(x)(\varphi(x)\cdot g(x))$ кўпҳаддаги x^i ($i=0, 1, 2, \ldots, n+s+t$) нинг коэффициенти эса

$$\sum_{k+j=i} a_k \Big(\sum_{l+m=j} b_l c_m\Big) = \sum_{k+l+m=i} a_k b_l c_m$$

йиғинди орқали аниқланади Уларнинг тенглигига асосан (2) тенглик ҳам бажарилади.

4) Шунингдек $f(x)(\varphi(x)+g(x)) = f(x)\varphi(x) + f(x)g(x)$ бўлади, яъни кўпҳадларни кўпайтириш қўшиш амалига нисбатан дистрибутивдир.

Бу тасдиқнинг тўғрилиги

$$\sum_{\nu+k=\mu} (b_\nu + c_\nu) a_k = \sum_{k+\nu=\mu} a_k b_\nu + \sum_{k+\nu=\mu} a_k c_\nu$$

тенглик ўринли эканлигидан келиб чиқади. Чунки, бу тенгликнинг ўнг томони $f(x)\varphi(x) + f(x)g(x)$ кўпҳаднинг x^i олдидаги коэффициентидан, чап томони эса $f(x)(\varphi(x)+g(x))$ кўпҳаднинг x^i олдидаги коэффициентидан тузилган.

Демак, коэффициентлари $\mathcal{K}$ бутунлик соҳасига тегишли бўлган бир номаълумли кўпҳадлар тўплами ҳалқа бўлар экан. Бу ҳалқа одатда $\mathcal{K}[x]$ каби белгиланади.

52-§. Кўпҳадларнинг қолдиқли бўлиниши

Айтайлик, $\varphi(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$ кўпҳад берилган бўлсин. Даражаси n га тенг ва бош коэффициенти $b_n \neq 0$ бўлган ҳар қандай $\varphi(x)$ кўпҳаднинг бош коэффициентини доимо 1 га келтириб олиш мумкин. Бунинг учун $\frac{\varphi(x)}{b_n} = g(x)$ кўпҳадни қараш кифоя.

$g(x)$ кўпҳаддан бошқа бош коэффициенти ихтиёрий бўлган $m \geqslant n$ даражали $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_mx^m$ кўпҳад берилган бўлсин.

Агар $f(x)$ кўпҳад n-даражали кўпҳад бўлса, у дар $f(x) = n$ каби ёзилади.

Теорема. *Ҳар қандай* $f(x)$ *ва* $g(x) \neq 0$ *кўпҳадлар учун шундай ягона* $h(x)$ *ва* $r(x)$ *кўпҳадлар мавжудки, улар учун* дар $r(x) <$ дар $g(x)$ *ва* дар $h(x) <$ дар $f(x)$ *бўлиб, ушбу тенглик бажарилади:*

$$f(x) = g(x)\,h(x) + r(x). \tag{1}$$

Исботи. Агар $f(x)$ кўпҳаддан $a_m x^{m-n} g(x)$ кўпҳадни айирсак, $f(x) - a_m x^{m-n} g(x) = r_1(x)$ кўпҳадда $a_m x^m$ ҳад бўлмайди. Бу ерда қуйидаги иккита ҳол бўлиши мумкин:

а) $r_1(x)$ нинг даражаси $g(x)$ нинг даражасидан кичик;

б) $r_1(x)$ нинг даражаси $g(x)$ даражасидан катта ёки унга тенг.

Агар а) ҳол юз берса, $h(x) = a_m x^{m-n}$; $r(x) = r_1(x)$ бўлиб, теорема исботланган бўлади. Биз б) ҳол устида тўхталиб ўтамиз. Фараз қилайлик, дар $r_1(x) \geqslant$ дар $g(x)$ бўлиб, $r_1(x) = c_0 + c_1x + c_2x^2 + \ldots + c_kx^k$ кўринишга эга бўлсин.

Энди $g(x)$ кўпҳадни $c_k x^{k-n}$ га кўпайтириб, натижасини $r_1(x)$ дан айирамиз. У ҳолда $r_1(x) - c_k x^{k-n} \times g(x) = r_2(x)$ бўлиб, $r_2(x)$ кўпҳадда $c_k x^k$ ҳад бўлмайди.

$r_2(x) = d_0 + d_1x + d_2x^2 + \ldots + d_lx^l$ бўлсин. Бу ерда яна юқоридаги икки ҳолдан бири юз бериши мумкин:

1) агар $l \geqslant n$ бўлса, ушбу айирмани тузамиз:

$$r_2(x) - d_l x^{l-n} \cdot g(x) = r_3(x),$$

жараённи давом эттириб, бирор ν қадамдан сўнг дар $r_\nu(x) <$ дар $g(x)$ га эришамиз. Бошқача айтганда, $r_{\nu-1}(x) - t_\mu x^{\mu-n} g(x) = r_\nu(x)$ тенгликда дар $r_\nu(x) <$ дар $g(x)$ бўлади.

Энди ушбу тенгликларни ҳадлаб қўшамиз:

$$\begin{aligned} f(x) - a_m x^{m-n} g(x) &= r_1(x), \\ r_1(x) - c_k x^{k-n} \cdot g(x) &= r_2(x), \\ r_2(x) - d_l x^{l-n} \cdot g(x) &= r_3(x), \\ \ldots\ldots\ldots\ldots\ldots & \\ r_{\nu-1}(x) - t_\mu x^{\mu-n} \cdot g(x) &= r_\nu(x). \end{aligned}$$

Унда $f(x) - (a_m x^{m-n} + c_k x^{k-n} + d_l x^{l-n} + \ldots + t_\mu x^{\mu-n}) \times g(x) = r_\nu(x)$ ҳосил бўлади. Бу ерда $a_m x^{m-n} + c_k x^{k-n} + \ldots + t_\mu x^{\mu-n} = h(x)$ ва $r_\nu(x) = r(x)$ десак, $f(x) = g(x) \cdot h(x) + r(x)$ тенглик ҳосил бўлади.

$f(x) = g(x) \cdot h(x) + r(x)$ тенгликдаги $f(x)$ бўлинувчи, $g(x)$ бўлувчи, $h(x)$ чала бўлинма, $r(x)$ эса қолдиқ кўпҳадлар дейилади.

Энди (1) тенгликнинг ягоналигини исботлаймиз.

Айтайлик, (1) шартни қаноатлантирувчи яна бир жуфт $h'(x)$ ва $r'(x)$ кўпҳад мавжуд, яъни

$$f(x) = g(x) \cdot h'(x) + r'(x) \qquad (2)$$

тенглик ўринли бўлсин. (1) ва (2) тенгликларни ҳадлаб айириб

$$0 = g(x)(h(x) - h'(x)) + (r(x) - r'(x))$$

ёки

$$g(x) \cdot (h(x) - h'(x)) = r'(x) - r(x) \qquad (3)$$

ни ҳосил қиламиз. Бу ерда $r(x)$ ва $r'(x)$ нинг аниқланишига асосан дар$(r'(x) - r(x)) <$ дар $g(x)$ бўлади. Агар чап томонда $h(x) - h'(x) \neq 0$ бўлса, $r'(x) - r(x)$ нинг даражаси (3) га асосан $g(x)$ нинг даражасидан кичик эмас. Бу эса $r(x)$ ва $r'(x)$ нинг аниқланишига зиддир. Шунинг учун $h(x) = h'(x)$ бўлади. Бунга кўра (3) дан $r(x) = r'(x)$ келиб чиқади.

Бу теоремани баъзан $f(x)$ кўпаҳадни $g(x)$ кўпҳадга қолдиқли бўлиш теоремаси деб юритилади.

53-§. Кўпҳад илдизлари Кўпҳадни иккиҳадга бўлиш

$\mathscr{K}$ бирлик элементга эга бўлган бутунлик соҳаси бўлсин.

1-таъриф. Агар $\mathscr{K}$ бутунлик соҳасининг бирор α элементи учун $f(\alpha) = 0$ тенглик бажарилса, у ҳолда α элемент $f(x)$ *кўпҳаднинг илдизи* дейилади.

Q майдон устида бир номаълумли биринчи даражали $f(x) = ax + b$ кўпҳад $a \neq 0$ бўлганда рационал сонлар тўпламида доимо илдизга эга, чунки $f\left(-\frac{b}{a}\right) = -b + b = 0$, яъни $f\left(-\frac{b}{a}\right) = 0$ бўлади.

Даражаси $n \geqslant 1$ бўлган ҳар қандай кўпҳад илдизларга эга бўлган кенгайтма майдон доимо мавжуд бўлади. Биз буни кейинроқ исботлаймиз.

Нолинчи даражали $f(x) = a \neq 0$ кўпҳаднинг илдизи йўқ, чунки x га қандай қийматни бермайлик, барибир $f(\alpha = a \neq 0$ бўлади. Биз ноль кўпҳадни эътиборга олмаймиз, бундай кўпҳад x нинг ҳар бир қийматида нолга тенг.

1-теорема (Безу теоремаси). *$f(x)$ кўпҳадни $x - \alpha$ иккиҳадга бўлишдан чиққан қолдиқ $f(\alpha)$ га тенг.*

Исботи. Бўлувчи $x-\alpha$ нинг даражаси 1 га тенг бўлгани учун қолдиқ $r(x)$ ё нолинчи даражали кўпҳад, ёки ноль бўлиши керак, яъни

$$f(x)=(x-\alpha)h(x)+r \qquad (1)$$

бўлиб, бу тенгликда $x=\alpha$ десак, $f(\alpha)=r$ ни ҳосил қиламиз.

2-теорема. *$x=\alpha$ элемент $f(x)$ кўпҳаднинг илдизи бўлиши учун $f(x)$ нинг $x-\alpha$ иккиҳадга бўлиниши зарур ва етарли.*

Исботи. 1. Зарурийлиги. $x=\alpha$ ни $f(x)$ нинг илдизи дейлик. Бу ҳолда $f(\alpha)=0$ бўлади. 1-теоремага асосан $f(x)$ ни $x-\alpha$ га бўлишдан чиққан қолдиқ $f(\alpha)$ га тенг. Лекин $f(\alpha)=0$ бўлгани учун $r=0$ дир. Демак, $f(x)$ кўпҳад $x-\alpha$ иккиҳадга қолдиқсиз бўлинади.

2. Етарлилиги. $f(x)$ кўпҳад $x-\alpha$ га қолдиқсиз бўлинсин; $f(x)=(x-\alpha)h(x)$, яъни қолдиқ $r=0$ бўлсин. 1-теоремага кўра $f(\alpha)=r$. Бунда $r=0$ бўлгани учун $f(\alpha)=0$. Демак, $x=\alpha$ қиймат $f(x)$ кўпҳаднинг илдизи экан.

3-теорема. *Агар $\alpha_1, \alpha_2, \ldots, \alpha_k$ лар $f(x)$ кўпҳаднинг турли илдизлари бўлса, у ҳолда $f(x)$ кўпҳад $(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)$ кўпайтмага бўлинади.*

Исботи. Теореманинг исботини магематик индукция принципи асосида олиб борамиз $k=1$ да теореманинг ростлигини биз юқорида кўриб ўтдик. Айтайлик, теорема $n=k-1$ ҳол учун рост, яъни

$$f(x)=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_{k-1})g(x) \qquad (2)$$

бўлсин.

Бу тенгликка $x=\alpha_k$ ни қўямиз. У ҳолда α_k илдиз бўлгани туфайли $f(\alpha_k)=0$. Демак, $x=\alpha_k$ да $0=(\alpha_k-\alpha_1)(\alpha_k-\alpha_2)\ldots(\alpha_k-\alpha_{k-1})g(\alpha_k)$ ҳосил бўлади. $\mathcal{K}$ бутунлик соҳаси нолнинг бўлувчиларига эга бўлмаганлигидан ва $\alpha_1\neq\alpha_2\neq\ldots\neq\alpha_k$ шартга асосан $g(\alpha_k)=0$, яъни α_k сон $g(x)$ кўпҳаднинг илдизи экан. Унда 1-теоремага асосан

$$g(x)=(x-\alpha_k)h(x) \qquad (3)$$

бўлади. Энди (3) ни (2) га қўямиз. У ҳолда

$$f(x)=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)h(x)$$

бўлиб, бу эса $f(x)$ нинг $(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)$ га бўлинишини билдиради.

Эслатма. Баъзи ҳолларда бир неча ёки барча илдизлар устма-уст тушиб қолиши мумкин Унда (2) формула қуйидаги кўринишни олади:

$$f(x) = (x - \alpha)^l (x - \beta)^m h(x) \quad (l + m = k).$$

Бундай ҳолдаги α ва β илдизларни мос равишда l ва m каррали илдизлар дейилади.

Натижа. Нолдан фарқли m-даражали кўпҳад $(m \geqslant 1)$ $\mathcal{K}$ бутунлик соҳасида m дан ортиқ илдизга эга эмас.

Бу фикр нолнинг бўлувчиларига эга бўлган ҳалқада ўринли эмас. Масалан, 16 модуль бўйича тузилган чегирмалар синфлари ҳалқасида $f(x) = x^2$ кўпҳад 0, 4, 8, 12 илдизларга эга.

54-§. Кўпҳадларнинг бўлиниши

Айтайлик, $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ кўпҳаднинг коэффициентлари бирор $\mathcal{P}$ майдонга тегишли бўлсин. Бундай ҳолда $f(x)$ кўпҳад $\mathcal{P}$ майдон устида берилган кўпҳад дейилади.

Масалан, $f(x) = 3x^3 - 7x^2 - \sqrt{5}x - 3$, $g(x) = ix^7 - 3x^2 + ix - 7$ кўпҳадлар мос равишда ҳақиқий сонлар майдони устида ва комплекс сонлар майдони устида берилган кўпҳадлар бўлади.

Агар 52-§, (1) тенгликда $r(x) = 0$ бўлса, у ҳолда

$$f(x) = \varphi(x) \cdot g(x)$$

тенглик ҳосил бўлади. Бу эса $f(x)$ нинг $\varphi(x)$ га қолдиқсиз бўлинишини кўрсатади. Биз уни қисқача $f(x)/\varphi(x)$ каби белгилаймиз. Қаралаётган барча кўпҳадларни битта $\mathcal{P}$ майдон устида берилган деб фараз қилсак, кўпҳадларнинг бўлиниши қуйидаги хоссаларга эга:

1°. $((f(x)/\varphi(x)) \wedge (\varphi(x)/\psi(x))) \Rightarrow (f(x)/\psi(x))$.

Исботи. $f(x)/\varphi(x)$ эканлигидан

$$f(x) = \varphi(x) \cdot g_1(x), \tag{1}$$

$\varphi(x)/\psi(x)$ эканлигидан эса

$$\varphi(x) = \psi(x) \cdot g(x). \tag{2}$$

(1) ва (2) дан: $f(x) - \psi(x)\, g_9(x)\, g(x) = \psi(x) \cdot h(x)$, бунда $g_1(x) \cdot g(x) = h(x)$ деб олинади.

$f(x) = \psi(x)\cdot h(x)$ тенглик $f(x)$ нинг $\psi(x)$ га бўлинишини кўрсатади.

2°. $f_i(x)/\varphi(x)$ $(i=\overline{1,\ m}) \Rightarrow (f_1(x)\pm f_2(x)\pm\ldots\pm f_m(x))/\varphi(x)$.

Исботи. $((f_1(x)=\varphi(x)g_1(x))\wedge(f_2(x)=\varphi(x)\times g_2(x))\wedge\ldots\wedge(f_m(x)=\varphi(x)g_m(x)))\Rightarrow(f_1(x)\pm f_2(x)\pm\ldots\pm f_m(x))=\varphi(x)(g_1(x)\pm g_2(x)\pm\ldots\pm g_m(x))\Rightarrow(f_1(x)\pm f_2(x)\pm\ldots\pm f_m(x)/\varphi(x)$.

3°. $f_i(x)$ $(i=\overline{1,\ m})$ кўпҳадлардан камида биттаси $\varphi(x)$ га бўлинса, у ҳолда уларнинг кўпайтмаси ҳам $\varphi(x)$ га бўлинади.

Исботи. Фараз қилайлик, $f_1(x)/\varphi(x)$ бўлсин. Унда $f_1(x)=\varphi(x)\cdot g_1(x)$ бўлиб, бу тенгликдан

$$f_1(x)f_2(x)\ldots f_m(x)=\varphi(x)\cdot g_1(x)\cdot f_2(x)\ldots f_m(x)=\\=\varphi(x)\cdot g(x),$$

бундан 3-хоссанинг исботи кўриниб турибди.

4°. Агар $f_i(x)$ $(i=\overline{1,\ m})$ кўпҳадларнинг ҳар бири $\varphi(x)$ га бўлиниб, $g_i(x)$ лар ихтиёрий кўпҳадлар бўлса, у ҳолда

$$f_1(x)g_1(x)\pm f_2(x)g_2(x)\pm\ldots\pm f_m(x)g_m(x)/\varphi(x).$$

Исботи. 3-хоссага асосан ҳар бир $f_i(x)g_i(x)$ $(i=\overline{1,\ m})$ ҳад $\varphi(x)$ га бўлинади. 2-хоссага асосан эса уларнинг алгебраик йиғиндиси ҳам $\varphi(x)$ га бўлинади.

5°. Исталган $f(x)$ кўпҳад ҳар қандай нолинчи даражали кўпҳадга бўлинади.

Агар $\varphi(x)=a\neq 0$ десак, $f(x)=a:g(x)$ тенглик хоссани исботлайди, бунда $(0\neq a\in\mathscr{P})$.

6°. $f(x)/\varphi(x)\Rightarrow f(x)/a\varphi(x)$ $(0\neq a\in\mathscr{P})$.

Исботи. $f(x)=\varphi(x)g(x)\Rightarrow f(x)=a\cdot\varphi(x)\times a^{-1}g(x)$. Хусусий ҳолда $f(x)\neq 0$ ўз-ўзига бўлингани учун $af(x)$ га ҳам бўлинади.

7° $f(x)\neq 0$ ва $\varphi(x)\neq 0$ кўпҳадлар бир-бирига бўлинса, улар бир-биридан ўзгармас $a\neq 0$ кўпайтувчи билангина фарқ қилади

Исботи. Шарт бўйича $f(x)=\varphi(x)\cdot g_1(x)$ ва $\varphi(x)=f(x)\cdot g_2(x)$ берилган. Бу тенгликлардан $f(x)=f(x)g_1(x)\cdot g_2(x)$ ёки $1=g_1(x)g_2(x)$ тенглик ҳосил бўлади. Сўнгги тенглик $g_1(x)g_2(x)$ кўпайтманинг нолинчи даражали кўпҳадлигини кўрсатади. Бу ҳол эса $g_1(x)$ ва $g_2(x)$ нинг ҳар қайсиси нолинчи даражали кўпҳад бўлгандагина юз бериши мумкин. Демак, кўпҳадларнинг ўзаро тенглик шартига кўра $g_2(x) = a \neq 0$ ва $\varphi(x) = af(x)$ бўлади.

Теорема. $\mathscr{P}$ *сонлар майдони устида берилган кўпҳадлар бош идеаллар ҳалқаси бўлади.*

Исботи. $\mathscr{P}$ сонлар майдони бўлгани учун $\mathscr{P}[x]$ ҳалқа нолнииг бўлувчиларига эга бўлмаган коммутатив ҳалқа, яъни бутунлик соҳаси бўлади. Бу бутунлик соҳаси ўз ичига бирлик $f(x) = a^0x^0 = 1$ элементни олади. Энди $\mathscr{P}[x]$ ҳалқадаги ҳар бир идеалнинг бош идеал эканлигини кўрсатайлик.

Кўпҳадлар ҳалқасининг идеалини I билан белгилаймиз ва уни $I \neq 0$ деб оламиз. Энди I идеалдаги энг кичик даражали кўпҳадни $d(x)$ деб белгилаб, I даги ихтиёрий $f(x)$ ни $d(x)$ га бўламиз:

$$f(x) \in I,\ d(x) \in I \Rightarrow f(x) - d(x)\,g(x) = r(x) \in I$$

(бу ерда дар $d(x) >$ дар $r(x)$). $r(x) \in I$ га асосан $r(x) = 0$ тенглик рост. Акс ҳолда $d(x)$ кўпҳад I даги энг кичик даражали кўпҳад бўлмай, бундай кўпҳад $r(x)$ бўлар эди. Демак, I идеалдаги ихтиёрий $f(x)$ кўпҳад $d(x)$ га қолдиқсиз бўлингани учун I идеал ош идеал экан, яъни $I = (d(x))$ бўлиб, ҳалқа бош идеаллар ҳалқаси бўлади.

55-§. Евклид алгоритми. Энг катта умумий бўлувчи

Бутун сонлар учун маълум бўлган Евклид алгоритми ва унинг натижаларини кўпҳадларга ҳам татбиқ этилишини кўриб ўтайлик. $f(x) \neq 0$ бўлиб, $f(x)$ кўпҳаднинг даражаси $\varphi(x) \neq 0$ кўпҳаднинг даражасидан кичик эмас деб фараз қиламиз ва $f(x)$ ни $\varphi(x)$ га бўламиз. Ҳосил бўлган бўлинма ва қолдиқни мос равишда $g_1(x)$ ва $r_1(x)$ билан белгилаймиз. Маълумки, $r_1(x)$ нинг даражаси $\varphi(x)$ нинг даражасидан кичикдир. Энди $\varphi(x)$ ни $r_1(x)$ га бўлиб, бўлинма ва қолдиқни $g_2(x)$ ва $r_2(x)$ орқали белгилаймиз. Яна $r_2(x)$ нинг даражаси $r_1(x)$ нинг даражасидан кичиклигини эътиборга олиб, $r_1(x)$ ни $r_2(x)$ га бўламиз ва ҳосил бўлган бўлинма ва қолдиқни $g_3(x)$ ва $r_3(x)$ билан белгилаймиз ва ҳ. к. ҳар бир қолдиқни ундан кейинги қолдиққа бўламиз. Натижада даражалари камайиб борувчи $r_1(x)$, $r_2(x)$, $r_3(x)$, $r_4(x)$, . . . кўпҳадлар (қолдиқлар) ҳосил бўлади.

Бу қолдиқларнинг сони албатта чеклидир, чунки уларнинг даражалари камайиб борувчи (лекин манфий эмас) бутун сонлар кетма-кетлигини ҳосил қилади, бундай қатор эса чексиз бўла олмаслиги равшан. Шу сабабли юқоридаги бўлиш жараёни чекли бўлиб, биз шундай $r_k(x)$ қолдиққа келамизки, унга олдинги $r_{k-1}(x)$ қолдиқ бўлинадиган бўлади. Натижада ушбу тенгликлар системасини ҳосил қиламиз:

$$\begin{aligned} f(x) &= \varphi(x) g_1(x) + r_1(x), \\ \varphi(x) &= r_1(x) g_2(x) + r_2(x), \\ r_1(x) &= r_2(x) g_3(x) + r_3(x), \qquad (1) \\ &\cdots\cdots\cdots\cdots \\ r_{k-2}(x) &= r_{k-1}(x) g_k(x) + r_k(x), \\ r_{k-1}(x) &= r_k(x) g_{k+1}(x). \end{aligned}$$

Бу кетма-кет бўлиш жараёни одатда Евклид алгоритми дейилади. Энди кўпҳадларнинг умумий бўлувчилари тушунчасини қарайлик.

1-таъриф. Агар $f(x)$ ва $\varphi(x)$ кўпҳадлар $g(x)$ кўпҳадга бўлинса, у ҳолда $g(x)$ кўпҳад $f(x)$ ва $\varphi(x)$ кўпҳадларнинг *умумий бўлувчиси* дейилади.

$f(x)$ ва $\varphi(x)$ кўпҳаднинг бир неча умумий бўлувчилари мавжуд бўлиши мумкин. Масалан, $f(x) = x^4 + x^3 - 7x^2 - x + 6$ ва $\varphi(x) = x^4 - 5x^2 + 4$ кўпҳадлар учун $g_1(x) = x - 1$, $g_2(x) = x + 1$, $g_3(x) = x - 2$, $g_4(x) x^2 - 1$, $g_5(x) = x^2 - 3x + 2$, $g_6(x) = x^2 - x - 2$, $g_7(x) = x^3 - 2x^2 - x + 2$ кўпҳадларнинг ҳар қайсиси умумий бўлувчидир (буни текшириб кўринг).

2-таьриф. Агар $d(x)$ кўпҳад $f(x)$ ва $\varphi(x)$, кўпҳадларнинг умумий бўлувчиси бўлиб, у бу иккита кўпҳаднинг ихтиёрий умумий бўлувчисига бўлинса, у ҳолда $d(x)$, бўлувчини $f(x)$ ва $\varphi(x)$ кўпҳадларнинг *энг катта умумий бўлувчиси* (ЭКУБ) дейилади.

Масалан, юқоридаги мисолдаги $f(x)$ ва $\varphi(x)$ кўпҳадларнинг энг катта умумий бўлувчиси $g_7(x) = x^3 - 2x^2 - x + 2$ бўлади (текшириб кўринг).

$f(x)$ ва $\varphi(x)$ кўпҳадларнинг ЭКУБ $(f(x), \varphi(x))$ кўринишда белгиланади.

3-таъриф. Агар $f(x)$ ва $\varphi(x)$ кўпҳадларнинг энг катта умумий бўлувчиси нолинчи даражали кўпҳад бўлса, у ҳолда $f(x)$ ва $\varphi(x)$ кўпҳадлар *ўзаро туб кўпҳадлар* дейилади.

1-теорема. *$f(x)$ ва $\varphi(x)$ кўпҳадларнинг энг катта умумий бўлувчиси (1) тengликлардаги энг сўнгги $r_k(x)$ қолдиқ бўлади.*

Исботи. Аввало $f(x)$ ва $\varphi(x)$ учун $r_k(x)$ умумий бўлувчи эканини кўрсатамиз. Шу мақсадда (1) дан

$$r_{k-2}(x) = r_{k-1}(x)\,g_k(x) + r_k(x) \qquad (2)$$

тенгликни олиб, бу тенгликнинг ўнг томони $r_k(x)$ га бўлингани учун[*] $r_{k-2}(x)$ ҳам $r_k(x)$ га бўлинишини кўрсатамиз. Ундан кейин (1) да (2) дан юқорида турган

$$r_{k-3}(x) = r_{k-2}(x)\,g_{k-1}(x) + r_{k-1}(x)$$

тенгликни олиб, худди ўша йўл билан $r_{k-3}(x)$ нинг ҳам $r_k(x)$ га бўлинишини топамиз. Шу хилда (1) даги ҳар бир тенгликдан юқоридаги тенгликка ўтиб, ниҳоят $f(x)$ ва $\varphi(x)$ нинг $r_k(x)$ га бўлинишини кўрамиз. Демак, $f(x)$, $\varphi(x)$ кўпҳадлар учун $r_k(x)$ умумий бўлувчидир.

Энди, $f(x)$ ва $\varphi(x)$ нинг исталган умумий бўлувчисини $g(x)$ билан белгилаб, (1) даги биринчи

$$f(x) - \varphi(x)\,g_1(x) = r_1(x)$$

тенгликнинг чап томони $g(x)$ га бўлинганини кўрамиз. Шу сабабли бу тенгликнинг ўнг томонидаги $r_1(x)$ ҳам $g(x)$ га бўлинади. Кейинги

$$\varphi(x) - r_1(x)\,g_2(x) = r_2(x)$$

тенгликка нисбатан ҳам юқоридаги мулоҳазани такрорлаб, $r_2(x)$ нинг $g(x)$ га бўлинишини топамиз ва ҳоказо. Шу хилда, (1) нинг ҳар бир тенглигидан кейинги тенглигига ўтиб, ниҳоят $r_k(x)$ нинг $g(x)$ га бўлинишини кўрамиз. Демак, $f(x)$ ва $\varphi(x)$ учун $r_k(x)$ энг катта умумий бўлувчидир.

2-теорема. *Агар $d(x)$ кўпҳад $f(x)$ ва $\varphi(x)$ кўпҳадларнинг энг катта умумий бўлувчиси бўлса, $ad(x)$ ҳам $f(x)$ ва $\varphi(x)$ нинг энг катта умумий бўлувчиси бўлади,* (бунда a — нолинчи даражали исталган кўпҳад).

Исботи. Кўпҳадлар бўлинишининг 6°-хоссасига биноан $f(x)$ ва $\varphi(x)$ кўпҳадлар $ad(x)$ га бўлинади. Демак, $ad(x)$ кўпҳад бу кўпҳадларнинг умумий бў-

---

[*] Чунки $r_{k-1}(x)$ кўпҳад $r_k(x)$ га бўлинади.

лувчиси. Энди $g(x)$ ни $f(x)$ ва $\varphi(x)$ нинг исталган умумий бўлувчиси десак, $g(x)$ га $ad(x)$ бўлинади, чунки $d(x)=g(x)\,h(x)$ дан $ad(x)=g(x)\cdot(ah(x))$ келиб чиқади.

Демак, энг катта умумий бўлувчи $ad(x)$ кўринишга эга бўлса, биз уни a га қисқартира оламиз.

Аксинча, $d(x)$ ва $d_1(x)$ кўпҳадларни $f(x)$ ва $\varphi(x)$ нинг энг катта умумий бўлувчилари десак, улар бир-биридан фақат ўзгармас кўпайтувчи, яъни нолинчи даражали кўпҳадга тенг кўпайтувчи билангина фарқ қилиши мумкин.

Ҳақиқатан, $d(x)$ ни энг катта умумий бўлувчи ва $d_1(x)$ ни умумий бўлувчи деб қарасак, $d(x)$ нинг $d_1(x)$ га бўлинишини топамиз; $d_1(x)$ га нисбатан ҳам шу мулоҳазани такрорлаб, унинг $d(x)$ га бўлинишини кўрамиз. Демак, қолдиқли бўлинишнинг 7-хоссасига мувофиқ $d_1(x)=ad(x)$ бўлади.

Юқорида баён этилганларга кўра, ўзгармас кўпайтувчига эътибор қилмаганимиздагина $f(x)$ ва $\varphi(x)$ кўпҳадлар ягона энг катта умумий булувчига эга дейишимиз мумкин.

Мисоллар. 1. $f(x)=x^4-1$ ва $\varphi(x)=2x^3+x^2-2x-1$ кўпҳадларнинг энг катта умумий бўлувчисини топинг.

Авал, юқорида айтганимизга биноан, $f(x)$ ни 2 га кўпайтириб (бўлиш жараёнида каср коэффициентлар пайдо бўлмаслиги учун), сўнгра $\varphi(x)$ га бўламиз:

$$\begin{array}{l|l}
2x^4-2 & 2x^3+x^2-2x-1 \\
\underline{2x^4+x^3-2x^2-x} & \hline x \\
-x^3+2x^2+x-2 &
\end{array}$$

Яна $-x^3+2x^2+x-2$ бўлинувчини -2 га кўпайтирамиз ва сўнг бўлишни давом эттирамиз:

$$\begin{array}{l|l}
-\,2x^4-2 & 2x^3+x^2-2x-1 \\
\underline{2x^4+x^3-2x^2-x} & \hline x+1 \\
-x^3+2x^2+x-2 & \\
-\,2x^3-4x^2-2x+4 & \\
\underline{2x^3+x^2-2x-1} & \\
-5x^2+5 &
\end{array}$$

Биз ўзгармас кўпайтувчи аниқлигида биринчи

$$r_1(x) = -5x^2 + 5$$

қолдиқни топдик.

Энди $\varphi(x)$ ни $r_1(x)$ га бўламиз (аввал $r_1(x)$ ни -5 га қисқартириб):

$$\begin{array}{r|l} -\,2x^3 + x^2 - 2x - 1 & x^2 - 1 \\ \cline{2-2} 2x^3 \qquad - 2x \qquad & 2x + 1 \\ \cline{1-1} -\,x^2 - 1 \qquad & \\ x^2 - 1 \qquad & \\ \cline{1-1} 0 \qquad & \end{array}$$

Кетма-кет бўлиш жараёни тугади. Демак, нолдан фарқли сўнгги қолдиқ $x^2 - 1$ бўлиб, у $f(x)$ ва $\varphi(x)$ нинг энг катта умумий бўлувчисини ифодалайди, яъни $(f(x); \varphi(x)) = x^2 - 1$ бўлади.

2. $f(x) = x^4 + x^3 - 7x^2 - x + 6$ ва $\varphi(x) = x^4 - 5x^2 + 4$ кўпҳадларнинг энг катта умумий бўлувчисини топинг.

Бунинг учун $f(x)$ ни $\varphi(x)$ га бўламиз:

$$\begin{array}{r|l} x^4 + x^3 - 7x^2 - x + 6 & x^4 - 5x^2 + 4 \\ \cline{2-2} x^4 \qquad - 5x^2 \qquad + 4 & 1 \\ \cline{1-1} \multicolumn{2}{c}{x^3 - 2x^2 - x + 2 = r_1(x)} \end{array}$$

$\varphi(x)$ ни $r_1(x)$ га бўламиз:

$$\begin{array}{r|l} -\quad x^4 - 5x^2 + 4 \qquad & x^3 - 2x^2 - x + 2 \\ \cline{2-2} x^4 - 2x^3 - x^2 + 2x \qquad & x + 2 \\ \cline{1-1} -\quad 2x^3 - 4x^2 - 2x + 4 & \\ 2x^3 - 4x^2 - 2x + 4 & \\ \cline{1-1} 0 \qquad\qquad & \end{array}$$

Демак, биз излаган энг катта умумуй бўлувчи $d(x) = x^3 - 2x^2 - x + 2$ бўлади.

3. $f(x) = x^4 - 2x^3 - 4x^2 + 4x - 3$, $\varphi(x) = 2x^3 - 5x^2 - 4x + 3$ кўпҳадларнинг энг катта умумий бўлувчисини топинг.

$f(x)$ ни $\varphi(x)$ га бўламиз:

$$\begin{array}{r|l} -\,2x^4 - 4x^3 - 8x^2 + 8x - 6 & 2x^3 - 5x^2 - 4x + 3 \\ \cline{2-2} 2x^4 - 5x^3 - 4x^2 + 3x \qquad & x + 1 \\ \cline{1-1} x^3 - 4x^2 + 5x - 6 & \\ -\,2x^3 - 8x^2 + 10x - 12 & \\ 2x^3 - 5x^2 - 4x + 3 & \\ \cline{1-1} \multicolumn{2}{l}{-3x^2 + 14x - 15 = r_1(x).} \end{array}$$

Энди, $\varphi(x)$ ни $r_1(x)$ га бўламиз:

$$\begin{array}{r|l}
6x^3-15x^2-12x+9 & -3x^2+14x-15 \\
\underline{6x^3-28x^2+30x} & \overline{-2x-13} \\
13x^2-42x+9 & \\
-39x^2-126x+27 & \\
\underline{39x^2-182x+195} & \\
56x-168, & \qquad r_2(x)=x-3
\end{array}$$

Ниҳоят, $r_1(x)$ ни $r_2(x)$ га бўламиз:

$$\begin{array}{r|l}
-3x^2+14x-15 & x-3 \\
-3x^2+9x & \overline{-3x+5} \\
-\;5x-15 & \\
\underline{5x-15} & \\
0 &
\end{array}$$

Шундай қилиб, $f(x)$ ва $\varphi(x)$ нинг энг катта умумий бўлувчиси $d(x)=x-3$ бўлади.

4. $f(x)=x^4+x^3+x^2+x+1$, $\varphi(x)=3x^3+x^2+3x-1$ кўпҳадларнинг энг катта умумий бўлувчисини топинг.

1)
$$\begin{array}{r|l}
-\;3x^4+3x^3+3x^2+3x+3 & 3x^3+x^2+3x-1 \\
\underline{3x^4+x^3+3x^2-x} & \overline{x+2} \\
2x^3+4x+3 & \\
-\;6x^3+12x+9 & \\
\underline{6x^3+2x^2+6x-2} & \\
-2x^2+6x+11=r_1(x) &
\end{array}$$

2)
$$\begin{array}{r|l}
-\;6x^3+2x^2+6x-2 & -2x^2+6x+11 \\
\underline{6x^3-18x^2-33x} & \overline{-3x-10} \\
-\;20x^2+39x-2 & \\
\underline{20x^2-60x-110} & \\
99x+108 & \\
r_2(x)=11x+12. &
\end{array}$$

3)
$$\begin{array}{r|l}
-\;22x^2-66x-121 & 11x+12 \\
\underline{22x^2+24x} & \overline{2x+90} \\
-90x-121 & \\
-\;990x+1331 & \\
\underline{990x+1080} & \\
250 &
\end{array}$$

Демак, $f(x)$ ва $\varphi(x)$ нинг энг катта умумий бўлувчиси $d(x)=1$ бўлиб, бу кўпҳадлар ўзаро тубдир,

Евклид алгоритми $\mathscr{P}$ майдон устидаги икки $f(x)$ ва $\varphi(x)$ кўпҳаднинг энг катта умумий бўлувчиси $d(x)$ яна шу майдон устидаги кўпҳад бўлишини кўрсатади.

3-теорема. *$\mathscr{P}$ майдон устида берилган $f(x)$ ва $\varphi(x)$ кўпҳадларнинг энг катта умумий бўлувчиси $d(x)$ бўлса, у ҳолда бу майдонда улар учун ушбу*

$$f(x)\cdot g(x)+\varphi(x)\cdot h(x)=d(x) \qquad (3)$$

тенгликни қаноатлантирувчи $g(x)$ ва $h(x)$ кўпҳадлар мавжуд.

Исботи. (1) даги охиридан иккинчи турган тенгликда $r_k(x)=a\cdot d(x)$ эканини эътиборга олиб, уни қуйидагича ёзамиз:

$$r_{k-2}(x)-r_{k-1}(x)\,g_k(x)=a\cdot d(x) \qquad (4)$$

Яна (1) га мурожаат қилиб, биз олган тенгликдан юқоридаги тенгликдан $r_{k-1}(x)$ ни аниқлаймиз:

$$r_{k-1}(x)=r_{k-3}(x)-r_{k-2}(x)\,g_{k-1}(x)$$

ва бу ифодани (4) га қўямиз. Бунинг натижасида келиб чиқадиган тенгликни аввал a га бўлиб, сўнгра ундаги $r_{k-2}(x)$ ва $r_{k-3}(x)$ га кўпайтирилган кўпҳадларни қисқача $g_1(x)$ ва $h_1(x)$ билан белгилаб, ушбу тенгликни ҳосил қиламиз:

$$r_{k-2}(x)\,g_1(x)+r_{k-3}(x)\cdot h_1(x)=d(x). \qquad (5)$$

Энди, яна (1) га қайтиб, сўнгги олган тенглигимизнинг юқорисида турувчи тенгликдан $r_{k-2}(x)$ ни аниқлаб, (5) га қўямиз ва ҳоказо. Хуллас, шу йўл билан ҳосил бўла борган тенгликларга кетма-кет яна

$$r_{k-3}(x).\ r_{k-4}(x),\ \ldots,\ r_2(x),\ r_1(x)$$

нинг ифодаларини қўя борсак ва бундай тенгликларнинг энг кейингисидан $f(x)$ ни $\varphi(x)$ га кўпайтирилган кўпҳадларни қисқача $g(x)$ ва $h(x)$ билан белгиласак, (3) тенглик ҳосил бўлади. Равшанки, $g(x)$ ва $h(x)$ кўпҳадлар худди $\mathscr{P}$ майдон устидаги кўпҳадлар сифатида ҳосил бўлади.

Хусусий ҳолда, яъни $f(x)$ ва $\varphi(x)$ кўпҳадлар ўзаро туб бўлганда, уларнинг $d(x)$ энг катта умумий бўлувчиси нолинчи даражали кўпҳаддан иборат бўлиб, (3) тенглик

$$f(x)\,g(x)+\varphi(x)\cdot h(x)=a$$

ёки

$$f(x)r(x)+\varphi(x)s(x)=1 \qquad (6)$$

кўринишни олади, бунда $r(x)=a^{-1}g(x)$ ва $s(x)=a^{-1}h(x)$.

(3) тенгликни ҳосил қилишда (1) тенгликлардаги қолдиқларгина эмас, балки бўлинмалар ҳам иштирок этади. Шу сабабли бу ҳолда Евклид алгоритми бўйича кетма-кет бўлишларни аниқ (бўлинувчиларни ёки бўлувчини ҳеч қандай сонларға кўпайтирмай) бажариш лозим.

Мисоллар. 1. $f(x)=x^4-1$ ва $\varphi(x)=2x^3+x^2-2x-1$ кўпҳадлар учун (3) тенгликни қаноатлантирувчи $g(x)$ ва $h(x)$ кўпҳадларни топинг.

Евклид алгоритмига асосан

$$x^4-1=(2x^3+x^2-2x-1)\left(\frac{1}{2}x-\frac{1}{4}\right)+\left(\frac{5}{4}x^2-\frac{5}{4}\right)$$

$$2x^3+x^2-2x-1=\left(\frac{5}{4}x^2-\frac{5}{4}\right)\left(\frac{8}{5}x+\frac{4}{5}\right).$$

Кўрамизки, бу мисолда Евклид алгоритми фақат иккита тенгликни беради. Уларнинг биринчисига қараб, $f(x)$ ва $\varphi(x)$ нинг энг катта умумий бўлувчиси $\frac{5}{4}x^2-\frac{5}{4}$ эканини топамиз.

Биринчи тенгликдан

$$(x^4-1)-(2x^3+x^2-2x-1)\left(\frac{1}{2}x-\frac{1}{4}\right)=\frac{5}{4}x^2-\frac{5}{4}$$

ҳосил бўлади. Агар энг катта умумий бўлувчининг ўзгармас кўпайтувчигача аниқлик билан топилишини эсга олсак, сўнгги тенгликни 4 га кўпайтириш мумкин бўлиб, ушбуни ҳосил қиламиз:

$$4(x^4-1)-(2x^3+x^2-2x-)(2x-1)=5x^2-5,$$

Демак, бунда $g(x)=4$ ва $h(x)=-2x+1$.

2. $f(x)=x^5-x^2-x+1$ ва $\varphi(x)=x^4-2x^3-4x^2+2x+3$ кўпҳадлар учун (3) тенгликни қаноатлантирувчи $g(x)$ ва $h(x)$ кўпҳадларни топинг.

Евклид алгоритмига кўра

$$x^5-x^2-x+1=(x^4-2x^3-4x^2+2x+3)(x+2)+$$
$$+(8x^3+5x^2-8x-5),$$

$$x^4-2x^3-4x^2+2x+3=(8x^3+5x^2-8x-5)\left(\frac{1}{8}x-\right.$$
$$\left.-\frac{21}{64}\right)+\left(\frac{-87}{64}x^2+\frac{87}{64}\right),\quad 8x^3+5x^2-8x-5=\left(-\frac{87}{64}x^2+\right.$$
$$\left.+\frac{87}{64}\right)\left(-\frac{512}{87}x-\frac{320}{87}\right).$$

Иккинчи тенгликдан $f(x)$ ва $\varphi(x)$ нинг энг катта умумий бўлувчиси $-\frac{87}{64}x^2+\frac{87}{64}$ экани кўринади. Иккинчи тенгликни -64 га кўпайтириб, қуйидагини ёзамиз:

$$-64(x^4-2x^3-4x^2+2x+3)+(8x^3+5x^2-8x-5)\times$$
$$\times(8x-21)=87x^2-87.$$

Биринчи тенгликдан $8x^3+5x^2-8x-5$ ни аниқлаб, сўнгги тенгликка қуйсак:

$$87x^2-87=(x^5-x^2-x+1)(8x-21)+(x^4-2x^3-$$
$$-4x^2+2x+3)(-8x^2+5x-22)$$

ҳосил бўлиб, бунда $g(x)=8x-21$ ва $h(x)=-8x^2+$ $+5x-22$ бўлади.

Энди ўзаро туб кўпҳадларга доир теоремаларни исботлайлик,

4-теорема. *Агар $f_1(x)$, $f_2(x)$, ..., $f_n(x)$ кўпҳадларнинг ҳар бири $\varphi(x)$ кўпҳад билан ўзаро туб бўлса, у ҳолда $f_1(x)$, $f_2(x)$, ..., $f_n(x)$ кўпайтма ҳам $\varphi(x)$ билан ўзаро туб бўлади.*

Исботи. 1) Теоремани аввал иккита $f_1(x)$ ва $f_2(x)$ кўпҳад учун исботлайлик. $f_1(x)$ ва $\varphi(x)$ ўзаро туб бўлганидан $r(x)$ ва $s(x)$ кўпҳадлар мавжуд бўлиб,

$$f_1(x)\cdot r(x)+\varphi(x)\cdot s(x)=1$$

тенглик бажарилади. Бу тенгликнинг иккала томонини $f_2(x)$ га кўпайтириб, ушбуни ҳосил қиламиз:

$$f_1(x)f_2(x)r(x)+\psi(x)f_2(x)s(x)=f_2(x). \qquad (7)$$

Агар $f_1(x)\cdot f_2(x)$ ва $\varphi(x)$ нинг энг катта умумий бўлувчисини $d(x)$ десак, (7) нинг чап томони ва, демак, ўнг томони, яъни $f_2(x)$ ҳам $d(x)$ га бўлинади. Шундай қилиб, $f_2(x)$ ва $\varphi(x)$ учун $d(x)$ кўпҳад умумий бўлувчидир. Лекин, $f_2(x)$ ва $\varphi(x)$ ўзаро туб бўлгани сабабли $d(x)=1$ деган натижага келамиз. Демак, $f_1(x)\cdot f_2(x)$ ва $\varphi(x)$ кўпҳадлар ўзаро туб экан.

2) Энди $f_1(x)\cdot f_2(x)$ ва $f_3(x)$ нинг ҳар қайсиси $\varphi(x)$ билан ўзаро туб бўлгани учун, юқоридаги исботга асосан

$$f_1(x)\cdot f_2(x)\cdot f_3(x)$$

кўпайтма ҳам $\varphi(x)$ билан ўзаро тубдир ва ҳ. к. Шу мулоҳазани давом эттириб, индукция усули бўйича $f_1(x)\cdot f_2(x)\dots f_n(x)$ ва $\varphi(x)$ нинг ўзаро тублигини топамиз.

5-теорема. *Агар $f(x)$ ва $\varphi(x)$ кўпҳадлар ўзаро туб бўлиб, $f(x)\cdot g(x)$ кўпайтма $\varphi(x)$ га бўлинса, у ҳолда $g(x)$ кўпҳад $\varphi(x)$ га бўлинади.*

Исботи. Евклид алгоритми натижасига кўра $f(x)$ ва $\varphi(x)$ учун шундай $r(x)$ ва $s(x)$ кўпҳадлар топиладики, натижада ушбу

$$f(x)\,r(x)+\varphi(x)\cdot s(x)=1$$

тенглик ўринли бўлади. Бу тенгликнинг иккала томонини $g(x)$ га кўпайтириб, қуйидагини ҳосил қиламиз:

$$f(x)\,g(x)\,r(x)+\varphi(x)\,g(x)\,s(x)=g(x).$$

Сўнгги тенгликнинг чап томони (берилганига кўра) $\varphi(x)$ га бўлингани учун унинг ўнг томони, яъни $g(x)$ ҳам $\varphi(x)$ га бўлинади.

6-теорема. *Агар $f(x)$ кўпҳад бир вақтда ҳам $\varphi(x)$, кўпҳадга, ҳам $h(x)$ кўпҳадга бўлинса ва $(\varphi(x); h(x))=1$ бўлса, у ҳолда $f(x)$ кўпҳад $\varphi(x)\cdot h(x)$ кўпҳадга бўлинади.*

Исботи. $f(x)/\varphi(x)\Rightarrow f(x)=\varphi(x)\cdot g_1(x)$ ва $\varphi(x)\times g_1(x)/h(x)$. Аммо $(\varphi(x); h(x))=1$, бўлгани учун $g_1(x)/h(x)$, яъни $g_1(x)=h(x)\cdot g_2(x)$ бўлади. Демак, $f(x)=\varphi(x)\,g_1(x)$ ёки $f(x)=\varphi(x)\,h(x)\cdot g_2(x)$.

56-§. Келтириладиган ва келтирилмайдиган кўпҳадлар

Таъриф. Агар $\mathcal{P}$ майдон устида берилган ва даражаси, нолга тенг бўлмаган $f(x)$ кўпҳадни шу $\mathcal{P}$ майдон устидаги ва даражалари $f(x)$ нинг даражасидан кичик иккита $g(x)$ $h(x)$ кўпҳад кўпайтмаси сифатида ифодалаш (кўпайтмага келтириш) мумкин бўлса, $f(x)$ ни $\mathcal{P}$ майдон устида *келтириладиган кўпҳад*, ва аксинча, агар бундай кўпайтма сифатида ифодалаш (бундай кўпайтмага келтириш) мумкин бўлмаса, у $\mathcal{B}$ майдон устида ***келтирилмайдиган кўпҳад*** дейилади.

Масалан, рационал сонлар майдони устидаги $f(x) = x^5 + 2x^3 + x^2 + x + 1$ кўпҳад шу майдон устида келтириладиган кўпҳад, чунки

$$x^5 + 2x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^2 + 1)$$

бўлади.

Рационал сонлар майдони устидаги $f(x) = x^2 - 3$ кўпҳад эса бу майдон устида келтирилмайдиган кўпҳаддир. Ҳақиқатан, бу кўпҳадни рационал сонлар майдони устида келтириладиган десак,

$$f(x) = g(x) \cdot h(x) \tag{1}$$

тенглик бажарилиб, $g(x)$ ва $h(x)$ нинг даражалари 2 дан кичик ва коэффициентлари рационал сон бўлиши лозим. Демак, $g(x)$ ва $h(x)$ биринчи даражали кўпҳадлар бўлгандагина (1) тенглик бажарилиши мумкин. Шу сабабли

$$x^2 - 3 = (ax + b)(cx + d)$$

тенглик ўринли бўлиб, a, b, c, d рационал сонлар бўлиши керак. Сўнгги тенгликнинг ўнг томони ва, демак, чап томони ҳам $x = -\frac{b}{a}$ қийматда нолга айланади, яъни $\frac{b^2}{a^2} - 3 = 0$, бунда $\pm\frac{b}{a} = \sqrt{3}$. Лекин бундай тенглик ўринли эмас, чунки $\sqrt{3}$ иррационал сон $\pm\frac{b}{a}$ рационал сонга тенг бўла олмайди.

Ҳар қандай $\mathcal{P}$ сонлар майдони устидаги биринчи даражали исталган кўпҳад шу майдон устида келтирилмайдиган кўпҳад бўлади. Ҳақиқатан, даражаси 1 дан кичик кўпҳад фақат нолинчи даражали бўлиши мумкин. Лекин биринчи даражали кўпҳадни иккита нолинчи даражали кўпҳаднииг кўпайтмаси қилиб ёзиш ҳеч ҳам мумкин эмас.

Даражаси бирдан юқори бўлиб, $\mathcal{P}$ майдон устида келтирилмайдиган $f(x)$ кўпҳад $\mathcal{P}$ ни ўз ичига олган бошқа (кенгроқ) майдон устида келтириладиган бўлиши мумкин. Масалан, рационал сонлар майдони устида келтирилмайдиган $x^2 - 3$ кўпҳад ҳақиқий сонлар майдони устида келтириладиган кўпҳад бўлади, чунки $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$. Шунингдек, ҳақиқий сонлар майдони устида келтирилмайдиган $x^2 + 1$ кўпҳад комплекс сонлар майдони устида келтириладиган кўпҳад бўлади, чунки $x^2+1=(x-i)(x+i)$. Шу сабабли $f(x)$ кўпҳаднинг келтириладиганлиги ёки келтирилмаслигини бирор майдонни кўзда тутибгина гапириш мумкин.

Келтирилмайдиган кўпҳадлар қуйидаги хоссаларга эга:

1°. Агар келтирилмайдиган $p(x)$ кўпҳад келтирилмайдиган иккинчи $g(x)$ кўпҳадга бўлинса, $p(x)$ ва $g(x)$ бир-биридан ўзгармас кўпайтувчи билангина фарқ қилади.

Исботи. Берилганига кўра $p(x)/g(x)$, яъни $p(x)=$ $=g(x)h(x)$ эди. Бунда $h(x)$ нолинчи даражали кўпҳад бўлиши керак, акс ҳолда $p(x)$ келтириладиган кўпҳадни ифодалайди. Демак, $h(x)=a$ ва $p(x)=ag(x)$.

2°. Исталган $f(x)$ кўпҳад келтирилмайдиган ихтиёрий $p(x)$ кўпҳадга ё бўлинади, ёки у билан ўзаро туб бўлади.

Исботи. $f(x)$ ва $p(x)$ нинг энг катта умумий бўлувчисини $d(x)$ дейлик. У ҳолда $p(x)=d(x)\cdot h(x)$ тенглик ўринли бўлади. $p(x)$ келтирилмайдиган кўпҳад бўлгани учун $h(x)=a$ ёки $d(x)=a$ бўлиши керак.

$h(x)=a$ бўлган ҳолда $p(x)=ad(x)$ тенгликка қараб, $f(x)$ нинг $d(x)$ га бўлинишини топамиз, чунки $f(x)$ нинг $d(x)$ га бўлинишидан, унинг $ad(x)$ га ҳам бўлиниши келиб чиқади.

$d(x)=a$ тенгликнинг бажарилиши $f(x)$ ва $p(x)$ ларнинг ўзаро тублигини кўрсатади.

3°. Агар $f_1(x)$, $f_2(x)$, ..., $f_m(x)$ кўпҳадларнинг ҳеч бири келтирилмайдиган $p(x)$ кўпҳадга бўлинмаса, уларнинг $f_1(x)\cdot f_2(x)\cdot \ldots \cdot f_m(x)$ кўпайтмаси ҳам $p(x)$ га бўлинмайди.

Исботи. 2-хоссага асосан $f_1(x)$, $f_2(x)$, ..., $f_m(x)$ кўпҳадларнинг ҳар бири $p(x)$ билан ўзаро туб бўлиб, 55-§ даги 4-теоремага мувофиқ, $f_1(x)\cdot f_2(x)\cdot \ldots \times$ $\times f_m(x)$ кўпайтма ҳам $p(x)$ билан ўзаро туб бўлади. Демак, бу кўпайтма $p(x)$ га бўлинмайди.

4°. Агар $f_1(x)\cdot f_2(x)\ldots f_m(x)$ кўпайтма келтирилмайдиган $p(x)$ кўпҳадга бўлинса, $f_1(x)$, $f_2(x)$, ..., $f_m(x)$ кўпҳадларнинг ақалли биттаси $p(x)$ га бўлинади.

5°. $p(x)$ келтирилмайдиган кўпҳад бўлса, $ap(x)$ ҳам келтирилмайдиган кўпҳад бўлади.

Исботи. $ap(x)$ келтириладиган кўпҳад бўлса,

$$ap(x)=g(x)\cdot h(x)$$

тенглик ўринли бўлиб, бундан

$$p(x) = a^{-1}g(x) \cdot h(x)$$

тенглик келиб чиқади. Бу эса $p(x)$ нинг юқорида айтилишига мувофиқ, келтирилмайдиган бўлишига зиддир.

Теорема. *$\mathcal{F}$ майдон устида берилган ва даражаси 1 дан кичик бўлмаган ҳар бир $f(x)$ кўпҳад шу майдон устида келтирилмайдиган кўпҳад ёки келтирилмайдиган купҳадлар кўпайтмасига ёйилади, яъни*

$$f(x) = p_1(x) \cdot p_2(x) \dots p_r(x) \qquad (2)$$

бўлиб, бу ёйилма кўпайтувчилари ўзгармас кўпайтувчиларгача аниқлик даражасида ягонадир.

Исботи. Теорема келтирилмайдиган $f(x)$ кўпҳад учун равшандир, чунки бундай кўпҳад ягона йўл билан қуйидагича ифодаланади:

$$f(x) = f(x).$$

Энди теоремани кўпҳаднинг даражасига нисбатан математик индукция усулини қўллаб исботлаймиз. Биринчи даражали кўпҳад келтирилмайдиган кўпҳад бўлгани сабабли, бундай кўпҳад учун теорема ўринлидир. Даражалари n дан кичик кўпҳадлар учун теоремани ўринли деб ҳисоблаб, уни n- даражали $f(x)$ кўпҳад учун исботлайлик.

Шундай қилиб, n- даражали $f(x)$ кўпҳад берилган бўлсин ($n > 1$).

$f(x)$ келтирилмайдиган кўпҳад бўлган ҳолни юқорида кўриб ўтдик. Шу сабабли $f(x)$ ни келтириладиган кўпҳад дейлик. Бу вақтда

$$f(x) = f_1(x) \cdot f_2(x) \qquad (3)$$

тенглик бажарилади.

$f_1(x)$ ва $f_2(x)$ нинг даражалари нолдан катта, лекин n дан кичик бўлгани сабабли, бу кўпҳадлар учун теорема ўринлидир, яъни улар келтирилмайдиган кўпҳадлар кўпайтмасига қуйидагича ёйилади:

$$f_1(x) = p_1(x) \cdot p_2(x) \dots p_k(x),$$
$$f_2(x) = p_{k+1}(x) \cdot p_{k+2}(x) \dots p_r(x).$$

Бу ифодаларни (3) га қўйиб,

$$f(x) = p_1(x) \cdot p_2(x) \dots p_r(x) \qquad (4)$$

ни ҳосил қиламиз.

Энди (4) ёйилманинг ягоналигини исботлашгина қолди. Фараз қилайлик, $f(x)$ кўпҳад (4) дан бошқа яна қуйидаги келтирилмайдиган кўпҳадлар кўпайтмасига ёйилган бўлсин:

$$f(x) = g_1(x)\, g_2(x) \ \dots \ g_s(x) \tag{5}$$

(4) ва (5) ни тенглаштириб, ушбу тенгликни ҳосил қиламиз:

$$p_1(x)\, p_2(x) \ \dots \ p_r(x) = g_1(x)\, g_2(x) \ \dots \ g_s(x). \tag{6}$$

(6) тенгликнинг чап томони $p_1(x)$ га бўлингани учун унинг ўнг томони ҳам $p_1(x)$ га бўлинади. Бундан 56-§ даги 4-хоссага асосан $g_i(x)$ кўпҳадларнинг ақалли биттаси, масалан, $g_1(x)$ кўпҳад $p_1(x)$ га бўлинади деган хулосага келамиз.

56-§ даги 1°-хоссага асосан ушбу тенгликка эга бўламиз:

$$g_1(x) = c_1 p_1(x). \tag{7}$$

Бу қийматни (6) га қўйсак,

$$p_1(x) \cdot p_2(x) \ \dots \ p_r(x) = c_1 p_1(x)\, g_2(x) \ \dots \ g_s(x)$$

ёки $p_1(x)$ га қисқартирсак

$$p_2(x) \cdot p_3(x) \ \dots \ p_r(x) = c_1 g_2(x)\, g_3(x) \ \dots \ g_s(x) \tag{8}$$

тенглик ҳосил бўлади.

(8) тенгликнинг чап ва ўнг томони $g(x) = \frac{f(x)}{p_1(x)}$ кўпҳаднинг келтирилмайдиган кўпҳадлар кўпайтмасига ёйилишидан иборат. Бунда $g(x)$ кўпҳаднинг даражаси нолдан катта ва n дан кичик эканини эътиборга олсак, фаразимиз бўйича, бу кўпҳад учун теорема тўғри, яъни (8) ёйилма ўзгармас кўпайтувчилар аниқлигида ягонадир деган хулосага келамиз. Бошқача айтганда $r - 1 = s - 1$ бўлиб, бундан $r = s$, яъни

$$c_1 g_2(x) = c_2 c_1 p_2(x), \quad g_3(x) = c_3 p_3(x), \ \dots, \\ g_r(x) = c_r p_r(x)$$

тенгликларни ҳосил қиламиз. Бу тенгликларни (7) билан бирга олиб, ушбу $r = s$,

$$g_1(x) = c_1 p_1(x), \quad g_2(x) = c_2 p_2(x), \ \dots, \\ g_r(x) = c_r p_r(x)$$

натижага келамиз.

Эслатма. (4) ёйилмада баъзи $p_l(x)$ кўпҳадлар бир неча марта такрорланиб келиши мумкин. Масалан, $p_1(x)$ кўпҳад α_1 марта, $p_2(x)$ кўпҳад α_2 марта, ниҳоят, $p_l(x)$ кўпҳад α_l марта такрорланса, (4) ёйилма

$$f(x) = ap_1^{\alpha_1}(x) \cdot p_2^{\alpha_2}(x) \ \dots \ p_l^{\alpha_l}(x) \tag{9}$$

кўринишни олади*. Бу ерда $\alpha_1 + \alpha_2 + \dots + \alpha_l = n$ экани равшан.

57-§. Кўпҳаднинг ҳосиласи

Мазкур мавзуни баён этишдан олдин қуйидаги ёрдамчи тушунчаларни киритамиз:

1-теорема. *Майдон нолнинг бўлувчиларига эга эмас.*

Исботи. Тескарисини фараз қилайлик, яъни майдон нолнинг бўлувчиларига эга бўлсин. Майдонда ушбу

$$ax = b \tag{1}$$

тенглама $a \neq 0$ бўлганда ягона ечимга эга бўлар эди. Шунга асосан

$$ax = 0 \tag{2}$$

тенглама ҳам $a \neq 0$ бўлганда ечимга эга. $a \neq 0$ бўлгани учун (2) нинг иккала томонини a^{-1} га кўпайтирамиз. Унда $a^{-1} \cdot ax = a^{-1} \cdot 0 \Rightarrow x = 0$ бўлади. Демак, $a \cdot b = 0$ муносабат майдонда $a = 0$ ёки $b = 0$ бўлгандагина ўринли экан, яъни майдон нолнинг бўлувчиларига эга эмас.

2-теорема. *Ихтиёрий $\mathscr{P}$ майдон учун қуйидаги иккита тасдиқдан биттаси ва фақат биттаси доимо ўринли бўлади:*

а) $\forall n \in N, \ \forall a \in \mathscr{P} \, (a \neq 0 \wedge n \neq 0) \Rightarrow (na \neq 0)$;

б) $\forall a \in \mathscr{P}, \ \exists p \in N$ (p — туб сон) $\Rightarrow pa = 0$

ва бундай туб сон ягона.

Исботи. Фараз қилайлик, а) ҳол ўринли бўлмасин. Унда б) ҳол ўринли эканини кўрсатамиз. Ихтиёрий $b \in \mathscr{P}$ элемент учун шундай $q \in N$ элемент топиладики, натижада $aq = b$ муносабат ўринли бўлади.

Майдонда кўпайтириш амалининг ассоциативлигидан $nb = n(aq) = (n \cdot a)q = 0 \cdot q = 0$, яъни $nb = 0$ ҳо-

---

* (4) ёйилмада бир-биридан ўзгармас кўпайтувчилар билангина фарқ қилган кўпҳадлар мавжуд бўлганидан a кўпайтувчи пайдо бўлади.

сил бўлади. Бу ерда b элемент $\mathscr{P}$ майдоннинг ихтиёрий элементи бўлганидан б) тасдиқни майдоннинг бирлик элементи e учун бажарилишини кўрсатиш кифоя.

Ҳозиргина кўрганимиздек, $ne = 0$. Бундан $(-n)e = 0$ бўлади. n ва $-n$ дан бири мусбат. Демак, $ke = 0$ шартни қаноатлантирувчи k натурал сон мавжуд. Лекин, натурал сонларнинг ихтиёрий қисм тўплами доим энг кичик элементга эга. Айтайлик, $k \cdot e = 0$ муносабатни қаноатлантирувчи k ларнинг энг кичиги p бўлсин. p нинг туб сон эканлигини кўрсатамиз. $p \neq 1$, чунки акс ҳолда $1 \cdot e = e \cdot 1 = e = 0$ бўлиб қолар эди. Аммо майдонда $e \neq 0$.

Агар p мураккаб сон бўлса, у ҳолда $p = q \cdot r$ тенглик бажарилиб, бу ерда $1 < q < p$, $1 < r < p$ бўлар эди. У ҳолда кўпайтириш амалининг ассоциативлигидан қуйидаги тенгликни ҳосил қиламиз:

$$pe = (q \cdot r) \cdot e = (q \cdot e)(r \cdot e) = 0, \; pe = 0.$$

Майдон нолнинг бўлувчиларига эга бўлмаганлигидан $qe = 0$ ёки $re = 0$. Бу тенгликларнинг биттаси ҳам ўринли бўлмаслиги керак, чунки $ke = 0$ муносабатни қаноатлантирувчи k ларнинг энг кичиги p эди. Демак, p туб сон экан.

Энди $k \cdot e = 0$ муносабат бажарилганда k нинг p га бўлинишини кўрсатамиз. Ҳар қандай k учун қолдиқли бўлиш теоремасига асосан ушбу муносабатни ҳосил қиламиз.

$$k = pq + r \quad (0 \leqslant r < p). \tag{3}$$

(3) нинг иккала томонини e га кўпайтирамиз, яъни $ke = (pq + r)e$ тенгликни ҳосил қилиб, бунда $k \cdot e = 0$ бўлганидан $(pq)e + r \cdot e = 0$ тенгликни ёза оламиз.

Майдон коммутатив бўлгани учун $0 = (p \cdot q)e + re = q(pe) + re = q \cdot 0 + r \cdot e = 0 + r \cdot e$ ёки $re = 0$ тенгликни ҳосил қилдик. Бу тенгликда $e \neq 0$ бўлгани учун $r = 0$ бўлади.

Демак, $k = pq$ бўлиб, k/p бўлади. Бундан p нинг $pe = 0$ муносабатни қаноатлантирувчи ягона туб сонлиги келиб чиқади.

1-таъриф. Агар $\mathscr{P}$ майдоннинг ҳар қандай a элементи ва нолдан фарқли ихтиёрий n бутун сон учун $na \neq 0$ бўлса, у ҳолда $\mathscr{P}$ майдон *ноль характеристикали майдон*, бирор p туб сон учун $pa = 0$ бўлганда эса $\mathcal{P}$ майдон *p характеристикали майдон* дейилади.

Барча сонли майдонлар ноль характеристикали майдон бўлади, чунки $n \cdot 1 = n$ бўлиб, $n \cdot 1 = 0$ тенглик фақат ва фақат $n = 0$ дагина бажарилади.

Мисол. $\mathcal{K} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ тўплами $m = 5$ модуль бўйича тузилган синфлар ҳалқаси бўлсин. Бу ҳалқада $\overline{a}\, x = \overline{b}$ тенглама $\overline{a} \neq \overline{0}$ бўлганда доимо ечимга эга Демак, $\mathcal{K}$ ҳалқа майдон экан. Бу ерда $\mathcal{K}$ майдон $p = 5$ характеристикали майдон, чунки $\overline{1} \in \mathcal{K}$ учун $5 \cdot \overline{1} = \overline{5} = \overline{0}$.

Мураккаб модуль бўйича тузилган ҳалқа майдон бўлмайди, чунки $m = 6$ бўлганда $\mathcal{K} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ ҳалқа $\overline{2} \cdot \overline{3} = \overline{0}$ бўлгани учун нолнинг бўлувчиларига $(\overline{2} \neq \overline{0}, \overline{3} \neq \overline{0})$ эга. Майдон эса нолнинг бўлувчиларига эга эмас эди.

Энди кўпҳадлар ҳосиласи тушунчасига қайтамиз.

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

кўпҳаднинг коэффициентлари ноль характеристикали $\mathcal{P}$ майдондан олинган бўлсин.

Бу кўпҳаднинг биринчи тартибли ҳосиласи деб

$$f'(x) = n a_0 x^{n-1} + (n-1) a_1 x^{n-2} + \ldots + 2a_{n-2} x + a_{n-1} \tag{4}$$

кўпҳадни айтилади. Биринчи тартибли ҳосиладан олинган ҳосила иккинчи тартибли ҳосила дейилади ва у $f''(x)$ каби белгиланади. Ҳар қандай n- тартибли ҳосила $(n-1)$- тартибли ҳосила орқали аниқланади.

Нолинчи даражали ва ноль кўпҳадлар ҳосиласи одатда нолга тенг деб олинади.

Агар n- даражали кўпҳаднинг кетма-кет n марта ҳосиласини олсак, $f^{(n)}(x) = n! a_0$ бўлиши аниқ. Охирги кўпҳад нолинчи даражали кўпҳад бўлганлигидан $f^{(n+1)}(x) = 0$ бўлади.

Демак, n- даражали кўпҳаднинг $(n+1)$- тартибли ҳосиласи нолга тенг экан.

Кўпҳад ҳосиласи тушунчасидан фойдаланиб, қуйидагиларни исботлаш мумкин:

1. $(f(x) + g(x))' = f'(x) + g'(x)$ (йиғиндининг ҳосиласи);

2. $(f(x)\cdot g(x))'=f'(x)g(x)+f(x)g'(x)$ (кўпайтманинг ҳосиласи).

Биз бу тенгликлардан иккинчисининг исботини келтирамиз. Фараз қилайлик.

$$g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_{m-1}x+b_m \qquad (5)$$

бўлсин. У ҳолда $g(x)$ нинг биринчи тартибли ҳосиласи деб биз қуйидаги кўпҳадни тушунамиз.

$$g'(x)=mb_0x^{m-1}+(m-1)b_1x^{m-2}+\ldots+$$
$$+2b_{m-2}x+b_{m-1}. \qquad (6)$$

$f(x)$ ва $g(x)$ нинг кўпайтмаси

$$f(x)\cdot g(x)=a_0b_0x^{m+n}+(a_0b_1+a_1b_0)x^{m+n-1}+$$
$$+(a_0b_2+a_1b_1+a_2b_0)x^{m+n-2}+\ldots+(a_nb_{m-2}+$$
$$+a_{n-1}b_{m-1}+a_{n-2}b_m)x^2+(a_nb_{m-1}+a_{n-1}b_m)x+a_nb_m$$

бўлиб, бу кўпайтманинг ҳосиласи

$$(f(x)\cdot g(x))'=(n+m)a_0b_0x^{n+m-1}+(n+m-$$
$$-1)(a_0b_1+a_1\cdot b_0)x^{n+m-2}+\ldots+2(a_nb_{m-2}+$$
$$+a_{n-1}b_{m-1}+a_{n-2}b_m)x+(a_hb_{m-1}+a_{n-1}b_m) \qquad (7)$$

каби бўлади.

Иккинчидан, (5), (3) ва (6) ни ҳадлаб кўпайтириб, натижаларини қўшсак,

$$f'(x)g(x)+f(x)g'(x)=(m+n)a_0b_0x^{n+m-1}+$$
$$+(n+m-1)(a_0b_1+a_1b_0)x^{n+m-2}+\ldots+$$
$$+2(a_hb_{m-2}+a_{n-1}b_{m-1}+a_{n-2}b_m)x+$$
$$+(a_hb_{m-1}+a_{n-1}b_m) \qquad (8)$$

тенгликка эга бўламиз. Энди (7) ва (8) ни солиштирсак,

$$(f(x)\cdot g(x))'=f'(x)g(x)+f(x)g'(x)$$

эканлиги келиб чиқади.

58-§. Горнер схемаси

Агар $x=\alpha$ сон $f(x)$ кўпҳаднинг илдизи бўлса, Безу теоремасига асосан $f(x)$ кўпҳаднинг $x=\alpha$ даги қиймати $r=f(\alpha)=0$ бўлар эди. Қолдиқли бўлиш теоремасига кўра

$$f(x)=(x-\alpha)\varphi(x)+r$$

тенгликдаги $\varphi(x)$ нинг коэффициентларини ва r қолдиқ ҳадни ҳисоблашнинг бир усули билан танишайлик. Бунинг учун $\varphi(x)$ ва r ни номаълум коэффициентлар ёрдамида қуйидагича ёзиб оламиз:

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_h = (x - \alpha)(A_0x^{n-1} + A_1x^{n-2} + \ldots + A_{n-2}x + A_{n-1}) + r.$$

Тенгликларнинг ўнг томонидаги қавсларни очиб, икки кита кўпҳаднинг тенглиги таърифига асосан, қуйидагиларга эга бўламиз:

$$a_0 = A_0,\ a_1 = A_1 - \alpha A_0,\ a_2 = A_2 - \alpha A_1,\ \ldots,$$
$$a_k = A_k - \alpha A_{k-1},\ \ldots,\ a_{n-1} = A_{n-1} - \alpha A_{n-2},$$
$$a_n = r - \alpha A_{n-1}.$$

Бу тенгликлардан A_i $(i = \overline{0, n})$ ларни ва r ни қуйидагича аниқлаймиз:

$$A_0 = a_0,\ A_1 = a_1 + \alpha A_0,\ A_2 = a_2 + \alpha A_1,\ \ldots,$$
$$A_k = a_k + \alpha A_{k-1},\ \ldots,\ A_{n-1} = a_{n-1} + \alpha A_{n-2},$$
$$r = a_n + \alpha A_{n-1}.$$

Бу ҳисоблашларни қуйидаги Горнер схемаси деб аталувчи схема ёрдамида ҳам бажариш мумкин:

	a_0	a_1	a_2	...	a_k	...	a_{n-1}	a_n
α	A_0	A_1	A_2	...	A_k	...	A_{n-1}	r

Ҳар бир A_k коэффициентни топиш учун схемада унинг юқорисидаги a_k га A_k дан олдин турган A_{k-1} ни α га кўпайтириб қўшиш керак. Агар $\varphi(x)$ кўпҳадни яна бирор $x - \beta$ иккиҳадга бўлиш талаб этилса, бу схемани пастга қараб давом эттириш мумкин. Умуман олганда, кўпҳаднинг каррали илдизларини топишда ҳам шу усулдан фойдаланилади (53- § га қаранг).

Мисоллар. 1. $x^3 + 2x - 5$ учҳадни $x - 2$ иккиҳаднинг даражалари бўйича ёзинг.

Қуйидаги схемани тузиб оламиз:

	1	0	2	−5
2	1	2	6	7
2	1	4	14	
2	1	6		
2	1			

Бу жадвалнинг биринчи сатри $x^3+2x-5=(x-2)\times\times(x^2+2x+6)+7$ ни, иккинчи сатр эса $x^2+2x+6=(x-2)(x+4)+14$ ни билдиради. Буларга асосан, $x^3+2x-5=(x+4)(x-2)^2+14(x-2)+7$ ёки $x++4=(x-2)+6$ дан фойдалансак, $x^3+2x-5==(x-2)^3+6\cdot(x-2)^2+14(x-2)+7$ ҳосил бўлади.

2. $x^5-7x^4+12x^3+16x^2-64x+48$ кўпҳад учун $x=2$ неча каррали илдиз эканлигини аниқланг.

Бу мисол учун ҳам юқоридаги каби қуйидаги схемани тузамиз:

	1	−7	12	16	−64	48
2	1	−5	2	20	−24	0
2	1	−3	−4	12	0	
2	1	−1	−6	0		
2	1	1	−4			

Демак, $x=2$ уч каррали илдиз бўлиб, берилган кўпҳадни

$$x^5-7x^4+12x^3+16x^2-64x+48=$$
$$=(x-2)^3(x^2-x-6)$$

шаклда ёзиш мумкин. Бу ерда $x^2-x-6=(x-2)\times\times(x+1)-4$.

59-§. Каррали кўпайтувчиларни ажратиш

Таъриф. Агар $f(x)$ кўпҳад $\varphi^{\alpha}(x)$ кўпҳадга бўлиниб, лекин $\varphi^{\alpha+1}(x)$ кўпҳадга бўлинмаса, у ҳолда $\varphi(x)$ кўпҳад $f(x)$ кўпҳаднинг каррали кўпайтувчиси дейилади*,

Бу таърифга асосан, $f(x)$ кўпҳадни

$$f(x) = \varphi^{\alpha}(x) \cdot g(x) \qquad (1)$$

кўринишда ёзиш мумкин. Бунда $g(x)$ кўпҳад $\varphi(x)$ га бўлинмайди, чунки акс ҳолда $g(x) = \varphi(x) \cdot h(x)$ ифодани (1) га қўйиб, ушбуни ҳосил қиламиз: $f(x) = \varphi^{\alpha+1}(x) \cdot h(x)$. Бу эса $f(x)$ нинг $\varphi^{\alpha+1}(x)$ га бўлинишини кўрсатади.

Масалан, $f(x) = x^5 + x^4 + x^3 - x^2 - x - 1$ кўпҳад учун $\varphi(x) = x^2 + x + 1$ кўпҳад икки каррали кўпайтувчидир, чунки $f(x)$ кўпҳад $(x^2 + x + 1)^2$ га бўлинади, лекин $(x^2 + x + 1)^3$ га бўлинмайди. Демак, $f(x) = (x + x + 1)^3 (x - 1)^2$ бўлади.

$f(x) = x^4 + 2x^3 + 2x^2 + 3x - 2$ учун $\varphi(x) = x^3 + 2x - 1$ бир каррали кўпайтувчи, чунки

$$f(x) = (x^3 + 2x - 1)(x + 2).$$

$f(x) = 5(x^2 - 4)^4 (2x^3 + x - 1)^3 (x + 1)(x^4 - 3x^3 + 1)^5$ кўпҳад учун $\varphi_1(x) = x^2 - 4$ кўпҳад тўрт каррали кўпайтувчи, $\varphi_2(x) = 2x^3 + x - 1$ кўпҳад уч каррали кўпайтувчи, $\varphi_3(x) = x + 1$ бир каррали кўпайтувчи ва $\varphi_4(x) = x^4 - 3x^3 + 1$ кўпҳад беш каррали кўпайтувчи эканлиги равшан.

Теорема. *Агар келтирилмайдиган $p(x)$ кўпҳад $f(x)$ кўпҳад учун α каррали кўпайтувчи бўлса, унинг $f'(x)$ ҳосиласи учун $p(x)$ кўпҳад $\alpha - 1$ каррали кўпайтувчи бўлади.*

Исботи. Таърифга кўра $f(x) = p^{\alpha}(x) g(x)$ бўлиб, бунда $g(x)$ кўпҳад $p(x)$ га бўлинмайди. Энди $f(x)$ нинг ҳосиласини оламиз:

$$f'(x) = \alpha p^{\alpha-1}(x) p'(x) g(x) + p^{\alpha}(x) g'(x) =$$
$$= p^{\alpha-1}(x)(\alpha p'(x) g(x) + p(x) g'(x)).$$

---

* Таърифдан $\varphi(x)$ нолинчидан юқори даражали кўпҳад эканлиги кўринади, чунки $\varphi(x) = a$ бўлса, $f(x)$ кўпҳад $\varphi(x)$ нинг исталган даражасига бўлинар эди.

Қавслар ичидаги йиғинди $p(x)$ га бўлинмайди. Ҳақиқатан, бу йиғиндини $h(x)$ билан белгиласак,

$$p'(x)g(x) = \alpha^{-1}h(x) - \alpha^{-1}p(x)g'(x)$$

тенглик ҳосил бўлади. $p'(x)$ ва $g(x)$ айрим-айрим $p(x)$ га бўлинмагани учун 56-§ даги 3°-хоссага асосан бу кўпҳадларнинг кўпайтмаси ҳам $p(x)$ га бўлинмайди. Ўнг томондаги йиғиндининг $-\alpha^{-1}p(x)g'(x)$ қўшилувчиси $p(x)$ га бўлинади, агар $\alpha^{-1}h(x)$ қўшилувчи ҳам $p(x)$ га бўлинса, тенгликнинг ўнг томони, ва демак, чап томони $p'(x)g(x)$ ҳам $p(x)$ га бўлинар эди. Шундай қилиб, $h(x)$ кўпҳад $p(x)$ га бўлинмайди ва $f'(x) = p^{\alpha-1}(x)h(x)$ тенглик теоремани исботлайди.

Бу теоремадан $f(x)$ нинг бир каррали $p(x)$ кўпайтувчиси $f'(x)$ ҳосила учун кўпайтувчи эмаслигини кўрамиз.

Қуйида $f(x)$ кўпҳаднинг каррали кўпайтувчиларини ажратиш усули билан танишамиз. $f(x)$ кўпҳад келтирилмайдиган кўпҳадлар кўпайтмасига қуйидагича ёйилган бўлсин:

$$f(x) = ap_1^{\alpha_1}(x)\cdot p_2^{\alpha_2}(x)\ \ldots\ p_r^{\alpha_r}(x). \qquad (2)$$

Бу ёйилмадаги ҳамма бир каррали келтирилмайдиган кўпҳадларнинг кўпайтмасини X_1 орқали, биттадан олинган ҳамма икки каррали келтирилмайдиган кўпҳадларнинг кўпайтмасини X_2 орқали, биттадан олинган ҳамма уч каррали келтирилмайдиган кўпҳадларнинг кўпайтмасини X_3 орқали белгилаймиз ва ҳ. к. ниҳоят, келтирилмайдиган кўпҳадлар орасида энг юқори s каррали кўпҳадларнинг биттадан олиб тузилган кўпайтмасини X_s орқали белгилаймиз. Агар ёйилмада бирон k каррали кўпҳадлар бўлмаса, $X_k = 1$ деб ҳисоблаймиз. Шундай қилиб, юқоридаги ёйилма ушбу кўринишни олади:

$$f(x) = a\cdot X_1\cdot X_2^2\cdot X_3^3\ \ldots\ X_s^s.$$

Масалан, $f(x)$ кўпҳаднинг Q майдон устида келтирилмайдиган кўпҳадларга ёйилмаси

$$f(x) = 4(x^2-3)^3(x-1)(x-2)(3x^3+1)^5\times$$
$$\times(2x^2+1)^5(x+7)^8$$

кўринишда бўлса, бунда

$$X_1 = (x-1)(x-2),\ X_2 = 1,\ X_3 = x^2-3,\ X_4 = 1,$$
$$X_5 = (3x^3+1)(2x^2+1),\ X_6 = 1,\ X_7 = 1,\ X_8 = x+7$$

бўлади. Демак, бу мисолда

$$f(x) = 4X_1 \cdot X_2^2 \cdot X_3^3 \cdot X_4^4 \cdot X_5^5 \cdot X_6^6 \cdot X_7^7 \cdot X_8^8$$

бўлади.

$f(x)$ нинг (2) ёйилмасидаги ҳар бир $p_i(x)$ кўпайтувчи $f'(x)$ ҳосила учун битта кам каррали кўпайтувчи бўлади (юқоридаги теоремага мувофиқ). Шу сабабли, $f'(x)$ учун X_1 кўпайтувчи бўлмайди, X_2 эса бир каррали кўпайтувчи, X_3 икки каррали кўпайтувчи бўлади ва ҳоказо. Демак,

$$f'(x) = aX_2 \cdot X_3^2 \cdot X_4^3 \ldots X_s^{s-1} \cdot \varphi_1(x)$$

бўлиб, бунда $\varphi_1(x)$ орқали $f(x)$ га кирмайдиган кўпайтувчиларнинг кўпайтмасини белгиладик.

$f(x)$ ва $f'(x)$ нинг энг катта умумий бўлувчиси $d_1(x)$ бу икки кўпҳад учун умумий бўлган кўпайтувчилардангина тузилади. Шу сабабли у

$$d_1(x) = a_1X_2 \cdot X_3^2 \ldots X_s^{s-1}$$

кўринишда бўлади.

Худди юқоридаги мулоҳазани такрорлаб, $d_1(x)$ нинг ҳосиласи

$$d_1'(x) = a \cdot X_3 \cdot X_4^2 \ldots X_s^{s-2} \cdot \varphi_2(x)$$

кўринишга эга деган хулосага келамиз. $d_1(x)$ ва $d_1'(x)$ нинг энг катта умумий бўлувчиси эса қуйидагидан иборат бўлади:

$$d_2(x) = a_2 \cdot X_3 \cdot X_4^2 \ldots X_s^{s-2}.$$

Сўнгра $d_2(x)$ ва унинг

$$d_2'(x) = aX_4 \cdot X_5^2 \ldots X_s^{s-3} \cdot \varphi_3(x)$$

ҳосиласи учун энг катта умумий бўлувчи

$$d_3(x) = a_3X_4 \cdot X_5^2 \ldots X_s^{s-3}$$

эканини топамиз ва ҳоказо. Шу йўл билан, энг охирида,

$$d_{s-1}(x) = a_{s-1}X_s, \quad d_s(x) = 1$$

кўпҳадларни ҳосил қиламиз.

Энди қуйидаги нисбатларни тузамиз:

$$E_1(x) = \frac{f(x)}{d_1(x)} = a_1' X_1 \cdot X_2 \cdot X_3 \ldots X_{s-1} \cdot X_s,$$

$$E_2(x)=\frac{d_1(x)}{d_2(x)}=a_2'X_2X_3\ \dots\ X_{s-1}\cdot X_s,$$

$$E_3(x)=\frac{d_2(x)}{d_3(x)}=a_3'X_3X_4\ \dots\ X_{s-1}X_s,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$E_{s-1}(x)=\frac{d_{s-2}(x)}{d_{s-1}(x)}=a_{s-1}'X_{s-1}X_s,$$

$$E_s(x)=\frac{d_{s-1}(x)}{d_s(x)}=a_s'X_s.$$

Натижада, каррали кўпайтувчилар қуйидагича ажралади:

$$\frac{E_1}{E_2}=X_1,\quad \frac{E_2}{E_3}=X_2,\ \dots,\ \frac{E_{s-}}{E_s}=X_{s-1},\quad E_s=X_s.$$

Мисол. $f(x)=x^4+x^3-3x^2-5x-2$ кўпҳаднинг каррали кўпайтувчиларини ажратайлик. Аввал $f(x)$ дан ҳосила оламиз.

Энди Евклид алгоритми ёрдами билан $f(x)$ ва $f'(x)$ нинг энг катта умумий бўлувчисини топамиз:

$$\begin{array}{r|l}
4x^4+4x^3-12x^2-20x-8 & 4x^3+3x^2-6x-5 \\ \cline{2-2}
\underline{4x^4+3x^3-\ \ 6x^2-\ \ 5x} & x+1 \\
x^3-6x^2-15x-8 & \\
4x^3-24x^2-60x-32 & \\
\underline{4x^3+\ \ 3x^2-\ \ 6x-\ \ 5} & \\
-27x^2-54x-27 & \\
x^2+2x+1 &
\end{array}$$

Демак, $(f(x),\ f'(x))=d_1(x)=x^2+2x+1$ бўлади $d_1(x)$ ва $d_1'(x)=2x+2$ ҳосиланинг энг катта умумий бўлувчисини топамиз:

$$\begin{array}{r|l}
-\ x^2+2x+1 & 2x+2 \\ \cline{2-2}
\underline{x^2+\ \ x} & \frac{1}{2}x+\frac{1}{2} \\
-\ x+1 & \\
\underline{x+1} & \\
0 &
\end{array}$$

Бундан, $(d_1(x),\ d_1'(x))=2x+2=d_2(x)$, $d_2(x)=2x+2$ бўлади. Ниҳоят, $d_2(x)$, $d_3(x)=2$ ларнинг энг катта умумий бўлувчиси $d_3(x) = d_2(x)$, $(d_2'(x)) = 2$, $d_3(x) = 2$ топилади.

Буларга асосан

$$E_1 = \frac{f(x)}{d_1(x)} = x^2 - x - 2, \quad E_2 = \frac{d_1(x)}{d_2(x)} = x + 1,$$

$$E_3 = \frac{d_2(x)}{d_3(x)} = x + 1$$

бўлиб,

$$X_1 = \frac{E_1}{E_2} = x - 2, \quad X_2 = \frac{E_2}{E_3} = 1, \quad X_3 = E_3 = x + 1,$$

яъни $X_1 = x - 2$, $X_2 = 1$, $X_3 = x + 1$ бўлади. Демак, $f(x) = X_1 \cdot X_2^2 \cdot X_3^3$, яъни $f(x) = (x - 2)(x + 1)^3$.

V боб. КЎП НОМАЪЛУМЛИ КЎПҲАДЛАР

60-§. Кўп номаълумли кўпҳадлар ҳалқаси. Бутунлик соҳасининг трансцендент кенгайтмаси

L ҳалқа нолнинг бўлувчисига эга бўлмаган коммутатив ҳалқа, яъни бутунлик соҳаси бўлсин. $\mathcal{K}$ ҳалқа L коммутатив ҳалқанинг нолмас қисм ҳалқаси ва $x_1, x_2, \ldots, x_m$ лар L ҳалқанинг элементлари бўлсин.

1-таъриф. L ҳалқанинг қисм ҳалқаси ва L даги $x_1, x_2, \ldots, x_m$ элементларни ўз ичига олувчи $\mathcal{K}$ ҳалқанинг минимал кенгайтмаси $\mathcal{K}$ ҳалқа ва $x_1, x_2, \ldots, x_m$ элементлар яратган L ҳалқанинг *қисм ҳалқаси* дейилади ва у $\mathcal{K}[x_1, x_2, \ldots, x_m]$ каби белгиланади.

$\mathcal{K}[x_1, x_2, \ldots, x_m]$ ҳалқа $\mathcal{K}$ нинг қисм ҳалқаси сифатида ва $x_1, x_2, \ldots, x_m$ элементларни ўз ичига олувчи L ҳалқанинг барча қисм ҳалқалари кесишмаси бўлади.

2-таъриф. Қуйидаги индуктивлик формулалари ёрдамида аниқланадиган $\mathcal{K}[x_1][x_2]\ldots[x_m]$ ҳалқани $\mathcal{K}$ ҳалқанинг *т каррали кенгайтмаси* дейилади:

1) $\mathcal{K}[x_1][x_2] = (\mathcal{K}[x_1])[x_2]$;

2) $\mathcal{K}[x_1][x_2]\ldots[x_m] = (\mathcal{K}[x_1][x_2]\ldots[x_{m-1}])\times$ $\times[x_m]$.

1-теорема. *$\mathcal{K}$ ҳалқа L ҳалқанинг коммутатив қисм ҳалқаси ва $x_1, x_2, \ldots, x_m \in L$ бўлса, у ҳолда*

$$\mathcal{K}[x_1, x_2, \ldots, x_m] = \mathcal{K}[x_1][x_2]\ldots[x_m] \qquad (1)$$

тенглик ўринли бўлади.

Исботи. $m = 1$ бўлганда теорема ўринли. $\mathcal{K}$ ҳалқага $m-1$ та элемент киритилганда ҳам теоремани рост дейлик ва унинг m та элемент учун ростлигини исботлайлик.

Таърифга асосан $\mathcal{K}[x_1, x_2, \ldots, x_{m-1}] \subset \mathcal{K}[x_1, x_2, \ldots, x_m]$ ва $x_m \in \mathcal{K}[x_1, x_2, \ldots, x_m]$ бўлгани учун

$$(\mathcal{K}[x_1, x_2, \ldots, x_{m-1}])[x_m] \subset \mathcal{K}[x_1, x_2, \ldots, x_m] \qquad (2)$$

муносабат бажарилади. Сўнгра

$$x_1, x_2, \ldots, x_m \in (\mathscr{K}[x_1, x_2, \ldots, x_{m-1}])[x_m]$$

бўлгани учун

$$\mathscr{K}[x_1, x_2, \ldots, x_m] \subset (\mathscr{K}[x_1, x_2, \ldots, x_{m-1}])[x_m] \quad (3)$$

муносабат ўринли. (2) ва (3) га асосан,

$$\mathscr{K}[x_1, x_2, \ldots, x_m] = \mathscr{K}[x_1, x_2, \ldots, x_{m-1}][x_m]. \quad (4)$$

Индуктивлик фаразига асосан,

$$\mathscr{K}[x_1, x_2, \ldots, x_{m-1}] = \mathscr{K}[x_1][x_2] \ldots [x_{m-1}] \quad (5)$$

келиб чиқади. (4) ва (5) тенгликлардан эса

$$\mathscr{K}[x_1, x_2, \ldots, x_m] = \mathscr{K}[x_1][x_2] \ldots [x_m]$$

тенгликка эга бўламиз.

3-таъриф. Агар $\{1, 2, \ldots, m\}$ тўпламнинг ихтиёрий s элементи учун $\mathscr{K}[x_1, x_2, \ldots, x_s]$ ҳалқа x_s элемент орқали $\mathscr{K}[x_1, x_2, \ldots, x_{s-1}]$ ҳалқанинг оддий трансцендент кенгайтмаси бўлса, у ҳолда $\mathscr{K}[x_1, x_2, \ldots, x_m]$ ҳалқани $\mathscr{K}$ ҳалқанинг *m каррали трансцендент кенгайтмаси* дейилади.

Эслатма. $m = 1$ бўлганда $\mathscr{K}$ ҳалқанинг m каррали трансцендент кенгайтмаси $\mathscr{K}$ ҳалқанинг оддий трансцендент кенгайтмаси бўлади.

4-таъриф. $\mathscr{K}$ бутунлик соҳасининг m каррали трансцендент кенгайтмаси бўлган $\mathscr{K}[x_1, x_2, \ldots, x_m]$ ҳалқани *кўпҳадлар ҳалқаси*, унинг элементини $x_1, x_2, \ldots, x_m$ *номаълумли кўпҳад* дейилади.

5-таъриф. Камида иккита номаълумга боғлиқ бўлган кўпҳад кўп *номаълумли кўпҳад* дейилади.

Кўп номаълумли кўпҳадлар 2, 3, 4, ..., n номаълумли бўлиши мумкин. n номаълумли кўпҳад $x_1^{\alpha_i} x_2^{\beta_i} \ldots x_n^{\delta_i}$ кўринишдаги чекли сондаги ҳадларнинг алгебраик йиғиндисидан иборат бўлиб, бу ерда $\alpha_i, \beta_i, \ldots, \delta_i \geqslant 0$ $(i = \overline{1, n})$ лар $\mathscr{P}$ сонлар майдонига тегишли бўлган бутун сонлардир. n номаълумли кўпҳаднинг кўриниши қуйидагича бўлади:

$$a_1 x_1^{\alpha} x_2^{\beta_1} \ldots x_n^{\delta_1} + a_2 x_1^{\alpha_2} x_2^{\beta_2} \ldots x_n^{\delta_2} + \ldots + \\ + a_n x_1^{\alpha_n} x_2^{\beta_n} \ldots x_n^{\delta_n}. \quad (6)$$

n номаълумли кўпҳад $f(x_1, x_2, \ldots, x_n)$, $g(x_1, x_2, \ldots, x_n)$, ... каби белгиланади.

$a_i \in \mathscr{P}$ $(i = \overline{1, n})$ лар (6) кўпҳад ҳадларининг коэффициентлари дейилади.

(6) кўпҳадни $f(x_1, x_2, \ldots, x_h) = \sum\limits_{i=1}^{n} a_i x_1^{\alpha_i} x_2^{\beta_i} \ldots x_n^{\delta_i}$ кўринишда ҳам ёзилади.

Агар $a_i \neq 0$ бўлса, у ҳолда (6) йиғиндидаги ҳар бир $a_i x_1^{\alpha_i} x_2^{\beta_i} \ldots x_n^{\delta_i}$ қўшилувчи кўпҳаднинг ҳади, $\alpha_i + \beta_i + \ldots + \delta_i$ йиғинди эса бу ҳаднинг даражаси деб аталади.

n номаълумли кўпҳаднинг даражаси деб шу кўпҳаддаги қўшилувчи ҳадлар даражаларининг энг каттасига айтилади.

Масалан,рационал сонлар майдони устидаги $x_1^2 \cdot x_2 \cdot x_3^3 - 7x_2^4 x_4 + 5x_3^2 x_4 - x_1$ кўпҳадда биринчи $x_1^2 \cdot x_2 \cdot x_3^3 = x_1^2 \cdot x_2 \cdot x_3^3 \cdot x_4^0$ ҳаднинг даражаси $2+1+3+0=6$, иккинчи $-7x_2^4 \cdot x_4$ ҳаднинг даражаси $0+4+0+1=5$, учинчи $5x_3^2 \cdot x_4^3$ ҳаднинг даражаси $0+0+2+3=5$, тўртинчи $-x_1$ ҳаднинг даражаси $1+0+0+0=1$ бўлади. Кўпҳаднинг даражаси эса 6 га тенг.

(6) кўпҳаднинг баъзи ёки ҳамма коэффициентлари, шунингдек, баъзи ёки барча $\alpha_i, \beta_i, \ldots, \delta_i$ даража кўрсаткичлари нолга тенг бўлиши мумкин. Масалан, $a_2 = a_3 = \ldots = a_n = 0$, $\alpha_1 = \beta_1 = \ldots = \delta_1 = 0$ бўлиб. a_1 коэффициент $\mathscr{P}$ майдоннинг исталган элементини билдирса, (6) кўпҳад

$$f(x_1, x_2, \ldots, x_n) = a_1$$

кўринишни олади. Демак, $\mathscr{P}$ майдоннинг ҳамма элементлари ҳам n ўзгарувчили кўпҳад деб ҳисобланади. Хусусий ҳолда $a_1 = a_2 = \ldots = a_n = 0$ бўлса, у ҳолда ноль кўпҳад ҳосил бўлади. Биз уни $f(x_1, x_2, \ldots, x_n) = 0$ кўринишда белгилаймиз. $a_1 \neq 0$ бўлса, у ҳолда $f(x_1, x_2, \ldots, x_n) = a_1$ ни нолинчи даражали кўпҳад дейилади. Ноль кўпҳаднинг даражаси аниқланмаган.

(6) кўпҳаддаги $x_1, x_2, \ldots, x_n$ номаълумлар бир-бирига боғлиқ эмас, уларни исталган сон қийматни қабул қила олади деб ҳисоблаймиз. Бошқача айтганда, ҳар бир x_i номаълумнинг қийматлари қолган номаълум-

ларнинг қийматлари билан боғлиқ эмас, яъни x_i номаълум қолган номаълумларнинг функцияси эмас. Бундай ўзгарувчилар, одатда, эркин ўзгарувчилар деб аталади.

Айтилганлардан қуйидаги натижа чиқади: ҳамма $a_1, a_2, \ldots, a_n$ коэффициентлардан ақалли биттаси нолга тенг бўлмаса, (6) кўпҳад ҳам ноль кўпҳад бўла олмайди. Ҳақиқатан,

$$a_1 x_1^{\alpha_1} x_2^{\beta_1} \ldots x_n^{\delta_1} + a_2 x_1^{\alpha_2} x_2^{\beta_2} \ldots x_n^{\delta_2} + \ldots +$$
$$+ a_n x_1^{\alpha_n} x_2^{\beta_n} \ldots x_n^{\delta_n} = 0$$

тенгликдан x_i қолган номаълумларнинг ошкормас функцияси эканини кўрамиз.

Демак, $a_1 = a_2 = \ldots = a_n = 0$ шартдагина (6) кўпҳад айнан нолга тенг.

5-таъриф. $f(x_1, x_2, \ldots, x_n)$ ва $\varphi(x_1, x_2, \ldots, x_n)$ кўпҳадлардан ҳар бирининг исталган

$$a_i x_1^{\alpha_i} x_2^{\beta_i} \ldots x_n^{\delta_i}$$

ҳади учун иккинчисининг ҳам худди шундай (айнан тенг) ҳади мавжуд бўлсагина, бу *икки кўпҳад бир-бирига тенг* дейилади.

6-таъриф. (6) кўпҳаднинг ҳамма ҳадлари бир хил даражали бўлса, у ҳолда бундай кўпҳад *бир жинсли кўпҳад* ёки *форма* дейилади.

Масалан, $f(x_1, x_2, x_3) = 2x_1 x_2^3 x_3^2 - x_1^2 x_3^4 + 7x_2 x_3^5 - 4x_1^3 x_2^2 x_3$ кўпҳад 6- даражали формадир.

Биринчи даражали форма чизиқли форма, иккинчи даражалиси квадратик форма, учинчи даражалиси кубик форма деб аталади.

Энди $\mathcal{P}$ сонлар майдони устида берилган n номаълумли иккита кўпҳад учун қўшиш ва кўпайтириш амалларини киритамиз:

$f(x_1, x_2, \ldots, x_n)$, $\varphi(x_1, x_2, \ldots, x_n)$ кўпҳадларни қўшиш деб, улардаги мос ҳадларнинг коэффициентларини қўшишни тушунамиз:

$k_i = t_i$ $(i = 1, n)$ бўлганда

$$a x_1^{k_1} \cdot x_2^{k_2} \ldots x_n^{k_n} \tag{7}$$

ва

$$b x_1^{t_1} x_2^{t_2} \ldots x_n^{t_n} \tag{8}$$

ҳадлар мос ёки ўхшаш ҳадлар деб юритилади.

Агар бирор ҳад $f(x_1, x_2, \dots, x_n)$ ва $\varphi(x_1, x_2, \dots, x_n)$ кўпҳадларнинг фақатгина биттасида учраса иккинчи кўпҳадлаги бу ҳаднинг коэффициенти ноль деб тушунилади.

(7) ва (8) каби ҳадларнинг кўпайтмаси деб

$$abx_1^{k_1+t_1} \cdot x_2^{k_2+t_2} \dots x_n^{k_n+t_n} \tag{9}$$

ифодани тушунамиз. Демак, $f(x_1, x_2, \dots, x_n)$ кўпҳадни $\varphi(x_1, x_2, \dots, x_n)$ кўпҳадга кўпайтириш учун $f(x_1, x_2, \dots, x_n)$ нинг ҳар бир ҳадини $\varphi(x_1, x_2, \dots, x_n)$ нинг барча ҳадларига кўпайтириш, кейин эса бир хил ҳадларни ихчамлаш керак.

Масалан, комплекс сонлар майдони устидаги $f(x_1, x_2, x_3) = (1+i)x_1x_2 - ix_2x_3^2 + x_2$ ва $\varphi(x_1, x_2, x_3) = 3x_1x_2 + ix_3$ кўпҳадларнинг йиғиндиси, айирмаси ва кўпайтмаси қуйидагича:

1. $f(x_1, x_2, x_3) + \varphi(x_1, x_2, x_3) = (4+i)\, x_1x_2 - ix_2 \times x_3^2 + x_2 + ix_3$;

2. $f(x_1, x_2, x_3) - \varphi(x_1, x_2, x_3) = (-2+i)\, x_1x_2 - ix_2x_3^2 + x_2 - xi_3$;

3. $f(x_1, x_2, x_3) \cdot \varphi(x_1, x_2, x_3) = (3+3i)\, x_1^2x_2^2 + (i-1)\, x_1x_2x_3 - 3ix_1x_2^2x_3^2 + x_2x_3^3 + 3x_1x_2^2 + ix_2x_3$.

2-теорема. *n номаълумли кўпҳадлар тўплами ҳалқа бўлади.*

Исботи. Теореманинг исботини кўпҳаддаги номаълумлар сони бўйича индукция усули асосида олиб борамиз.

$n = 1$ да биз бир номаълумли кўпҳадлар тўпламига эга бўламиз. Маълумки, 50-§ га асосан бу кўпҳадлар тўплами ҳалқа ташкил этар эди ва бу ҳалқа нолнинг бўлувчиларига эга бўлмас эди. Фараз қилайлик, теорема $k = n - 1$ учун тўғри бўлсин. Бошқача айтганда, барча $n - 1$ номаълумли кўпҳадлар тўплами нолнинг бўлувчиларига эга бўлмаган ҳалқа бўлсин.

Теореманинг $k = n$ учун тўғрилигини исботлаймиз. $\mathscr{P}$ сонлар майдони устида берилган n номаълумли кўпҳадни битта номаълумли кўпҳад деб қараш мумкин. Бу кўпҳад коэффициентларининг ҳар бири $x_1, x_2, \dots, x_{n-1}$ номаълумли кўпҳадлар бўлади. Агар коэффициентлар тўпламини $R[x_1, \dots, x_{n-1}]$ десак, фаразимизга асосан $R[x_1, x_2, \dots, x_n]$ нолнинг бўлувчиларига эга бўлмаган ҳалқадир.

Иккинчидан, битта x_n номаълумли кўпҳадлар тўплами $R[x_1, x_2, \ldots, x_{n-1}]$ да ҳалқа ташкил этади. Бу ҳалқа биз излаган n номаълумли кўпҳадлар ҳалқаси бўлиб, у одатда $\mathcal{K}[x_1, x_2, \ldots, x_{n-1}, x_n]$ каби белгиланади. $\mathcal{K}[x_1, x_2, \ldots, x_{n-1}]$ нолнинг бўлувчиларига эга бўлмаган коммутатив ҳалқа бўлганлигидан, $\mathcal{K}[x_1, x_2, \ldots, x_n]$ ҳам $\mathcal{F}$ сонлар майдони устида қурилган нолнинг бўлувчиларига эга бўлмаган коммутатив ҳалқадир. Маълумки, бундай ҳалқалар бутунлик соҳасини ташкил қилар эди.

Демак, n номаълумли кўпҳадлар тўплами бутунлик соҳасидан иборат экан.

61-§. Кўп номаълумли кўпҳадни лексикографик тартибда ёзиш

Биз бир номаълумли кўпҳадларни одатда икки усулда, яъни номаълумнинг даражалари ўсиши ва камайиши тартибида ёзар эдик. n номаълумли кўпҳаднинг бир неча ҳадлари бир хил даражада қатнашиши мумкин. Шунинг учун уни номаълумлар даряжаларининг ўсиши ёки камайиши тартибида ёзиш мумкин эмас. Бундай кўпҳадларни маълум бир тартибда ёзиш учун қуйидагича иш тутилади: n ўзгарувчили $f(x_1, x_2, \ldots, x_n)$ кўпҳад берилган бўлиб, бу кўпҳаднинг икки ҳадидан қайси бирида x_1 нинг даражаси катта бўлса, ўша ҳадни юқори деб ҳисоблаймиз. Бу ҳадлардаги x_1 нинг даражалари тенг бўлган ҳолда эса қайси бирида x_2 нинг даражаси кагта бўлса, ўша ҳадни юқори деймиз ва ҳ. к. Бошқача айтганда, $a_l \cdot x_1^{\mu_1} \cdot x_2^{\mu_2} \ldots x_n^{\mu_n}$ ва $a_j x_1^{\nu_1} \times$ $\times x_2^{\nu_2} \ldots x_n^{\nu_n}$ иккита ҳад учун нолдан фарқли $\mu_k - \nu_k$ айирмаларнинг биринчиси мусбат бўлса, биринчи ҳад иккинчи ҳаддан юқори деб аталади.

Масалан, $4x_1 x_2^3 x_3 x_4^2$ ва $-2x_2^5 x_3^2 x_4$ ҳадларда биринчиси иккинчидан юқори, $x_1 x_2^4 x_3 x_4$ ва $x_1 x_2^4 x_3 x_4^5$ ҳадларда эса иккинчиси биринчисидан юқори.

$f(x_1, x_2, \ldots, x_n)$ кўпҳадни ёзишда биринчи ўринга энг юқори ҳадни, иккинчи ўринга қолган ҳадлар орасида энг юқори бўлган ҳадни, учинчи ўринга қолган ҳадлар орасида энг юқори бўлган ҳадни ва шу жараён охирги ҳад учун ёзилса, у ҳолда $f(x_1, x_2, \ldots, x_n)$ кўпҳад лексикографик ёзилган дейилади.

Масалан, $f(x_1, x_2, x_3, x_4) = 2x_1 - 4x_2^6 x_3 + x_1 x_2 + 3x_1 x_2^3 - x_2^4 + 6x_3^4 x_4 - x_2^6 x_3 x_4 + x_2^2$ кўпҳаднинг лексикографик ёзилиши қуйидагича бўлади:

$$f(x_1, x_2, x_3, x_4) = 3x_1 x_2^3 + x_1 x_2 + 2x_1 - x_2^6 x_3 x_4 - 4x_2^6 x_3 + x_2^2 + 6x_3^4 x_4 - x_3^4.$$

Теорема. *Кўп номаълумли кўпҳадлар кўпайтмасининг энг юқори ҳади бу кўпҳадлар энг юқори ҳадлари кўпайтмасига тенг.*

Исботи. Теоремани $f(x_1, x_2, \ldots, x_n)$ ва $\varphi(x_1, x_2, \ldots, x_n)$ кўпҳад учун исботлайлик.

$$ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \ldots x_n^{\alpha_n} \tag{1}$$

ҳад $f(x_1, x_2, \ldots, x_n)$ кўпҳаднинг энг юқори ҳади,

$$kx_1^{\mu_1} \cdot x_2^{\mu_2} \ldots x_n^{\mu_n} \tag{2}$$

эса унинг исталган ҳади бўлсин:

$$bx_1^{\beta_1} \cdot x_2^{\beta_2} \ldots x_n^{\beta_n} \tag{3}$$

ҳад $\varphi(x_1, x_2, \ldots, x_n)$ кўпҳаднинг энг юқори ҳади,

$$tx_1^{\nu_1} \cdot x_2^{\nu_2} \ldots x_n^{\nu_n} \tag{4}$$

эса унинг исталган ҳади бўлсин.

Ушбу

$$a \cdot b x_1^{\alpha_1+\beta_1} \cdot x_2^{\alpha_2+\beta_2} \ldots x_n^{\alpha_n+\beta_n} \tag{5}$$

ва

$$k \cdot t x_1^{\mu_1+\nu_1} \cdot x_2^{\mu_2+\nu_2} \ldots x_n^{\mu_n+\nu_n} \tag{6}$$

ҳадларнинг қайси бири юқори ҳад эканлигини аниқлайлик. (1) ва (3) ҳадлар, мос равишда, (2) ва (4) ҳадлардан юқори бўлгани учун $\alpha_1 \geqslant \mu_1$ ва $\beta_1 \geqslant \nu_1$. Бундан $\alpha_1 + \beta_1 \geqslant \mu_1 + \nu_1$.

Агар $\alpha_1 + \beta_1 > \mu_1 + \nu_1$ бўлса, (5) ҳад (6) ҳаддан юқори: $\alpha_1 + \beta_1 = \mu_1 + \nu_1$ бўлса $(\alpha_1 - \mu_1) + (\beta_1 - \nu_1) = 0$ келиб чиқади. Аммо $\alpha_1 - \mu_1$ ва $\beta_1 - \nu_1$ амаллар манфий бўлмагани учун (чунки $\alpha_1 \geqslant \mu_1$ ва $\beta_1 \geqslant \nu_1$) $\alpha_1 - \mu_1 = 0$ ва $\beta_1 - \nu_1 = 0$ ёки $\alpha_1 = \mu_1$ ва $\beta_1 = \nu_1$ деган натижага келамиз. У ҳолда $\alpha_2 \geqslant \mu_2$ ва $\beta_2 \geqslant \nu_2$ бажарилиб, $\alpha_2 + \beta_2 \geqslant \mu_2 + \nu_2$ ни ҳосил қиламиз. Агар $\alpha_1 + \beta_1 = \mu_1 + \nu_1$ бўлиб $\alpha_2 + \beta_2 > \mu_2 + \nu_2$ бўлса, (5) ҳад (6) ҳаддан юқори-дир; $\alpha_2+\beta_2=\mu_2+\nu_2$ бўлганда эса, юқоридагидек, $\alpha_2=\mu_2$ ва $\beta_2=\nu_2$ эканини топамиз ва ҳ. к. Бу жараённи давом эттириб, (5) ҳаднинг (6) дан юқорилигини исботлаймиз.

Агар i нинг барча қийматларида $\alpha_i+\beta_i=\mu_i+\nu_i$ тенгликлар бажарилса, (2) ҳад (1) га ва (4) ҳад (3) га айнан тенг бўлади. Агар (2) ва (4) ҳадлардан ақалли биттаси (1) ва (3) га тенг бўлмаса, бирор i учун албатта $\alpha_i+\beta_i>\mu_i+\nu_i$ тенгсизлик бажарилади. Шундай қилиб, $f(x_1, x_2, \ldots, x_n)$ ва $\varphi(x_1, x_2, \ldots, x_n)$ нинг энг юқори ҳадларини кўпайтириш билан тузилган (5) ҳад $f(x_1, x_2, \ldots, x_n)\cdot\varphi(x_1, x_2, \ldots, x_n)$ кўпайтманинг энг юқори ҳадини ифодалайди.

Теорема иккитадан ортиқ кўпҳадлар кўпайтмаси учун математик индукция усули билан исботланади.

62-§. Рационал касрлар майдони

Бир номаълумли кўпҳадларнинг $\mathscr{P}[x]$ ҳалқаси берилган бўлсин.

Биз ўз олдимизга $\mathscr{P}[x]$ ҳалқани ўз ичига олувчи бирор майдонни қуриш вазифасини қўямиз. Бу майдонда қўшиш ва кўпайтириш амалларини шундай танлаймизки, бу амаллар $\mathscr{P}[x]$ даги мос амаллар билан бир хил бўлсин. Бошқача айтганда, $\mathscr{P}[x]$ биз қурмоқчи бўлган майдоннинг қисм ҳалқаси бўлиши керак.

Теорема. *Ҳар қандай бутунлик соҳасини ўз ичига олувчи коммутатив майдон мавжуд.*

Исботи. Теоремани кўпҳадлар ҳалқаси учун исботлаймиз. Бир номаълумли кўпҳадларнинг $\mathscr{P}[x]$ ҳалқаси бутунлик соҳаси эканлиги бизга маълум. Шунинг учун келгусида фақат кўпҳадлар ҳалқаси тўғрисида сўз юритамиз. $\mathscr{P}[x]$ ҳалқани ўз ичига олувчи майдонни қуриш учун $\varphi(x)\neq 0$ бўлгандаги тартибланган $(f;\ \varphi)$ жуфтликлар тўпламини қараймиз. Бу жуфтликларнинг бирор $\mathscr{P}(x)$ тўплами майдон бўлиши учун уларни қандай қоидалар асосида қўшиш ва кўпайтиришни билишимиз керак. Бу қоидаларни биз қуйидагича киритамиз;

$$\begin{aligned}&1.\ fg=\varphi\psi \Longleftrightarrow (f;\ \varphi)=(\psi;\ g);\\&2.\ (f;\ \varphi)+(\psi;\ g)=(fg+\varphi\psi;\ \varphi g);\qquad\qquad (1)\\&3.\ (f;\ \varphi)\cdot(\psi;\ g)=(f\psi;\ \varphi g).\end{aligned}$$

Жуфтликларнинг юқоридаги усулда киритилган таққослаш қоидаси рефлексив, симметрик ва транзитив бўлади.

Ҳақиқатан,

а) $(f;\ \varphi)=(f;\ \varphi)$, чунки $f\varphi=\varphi f$ бўлади;

б) $(f;\ \varphi)=(\psi;\ g)\Rightarrow(\psi;\ g)=(f;\ \varphi)$, чунки $\mathcal{P}[x]$ коммутатив бўлгани учун ва 1-шартга асосан

$$fg=\varphi\psi\Rightarrow\psi\varphi=gf;$$

в) $((f;\ \varphi)=(\psi;\ g)\wedge(\psi;\ g)=(h;\ \theta))\Rightarrow(f;\ \varphi)=(h;\ \theta)$.

1) шартга кўра в) боғланишнинг чап томонини қуйидагича ёзиш мумкин: $(fg=\varphi\psi)\wedge(\psi\theta=gh)$.

Биринчи тенгликнинг иккала қисмини θ га, иккинчи тенгликнинг иккала қисмини φ га кўпайтирсак, $fg\theta=\varphi\psi\theta$ ва $\psi\theta\varphi=gh\varphi$ тенгликларга эга бўламиз. Демак, $fg\theta=gh\varphi$. $\mathcal{P}[x]$ бутунлик соҳаси бўлгани учун бу тенгликни $f\theta=\varphi h$ каби ёзиш мумкин. Бу тенгликни 1) қоидага асосан $(f;\ \varphi)=(h;\ \theta)$ каби ёзамиз. Энди $(f;\ \varphi)$ жуфтликни қўшиш ва кўпайтириш амаллари бир қийматли эканлигини кўрсатамиз:

$$((f;\ \varphi)=(f_1;\ \varphi_1)\wedge(\varphi;\ g)\equiv(\varphi_1;\ g_1))\Rightarrow$$
$$\Rightarrow((f;\ \varphi)+(\varphi_1;\ g)\equiv(f_1;\ \varphi_1)+(\varphi_1;\ g_1))\wedge$$
$$\wedge((f;\ \varphi)\cdot(\varphi;\ g)=(f_1;\ \varphi_1)\cdot(\varphi_1;\ g_1));$$
$$(f;\ \varphi)=(f_1;\ \varphi_1),\ (\varphi;\ g)=(\varphi_1;\ g_1).$$

Бу таққослашларни мос равишда

$$f\cdot\varphi_1=\varphi\cdot f_1,\quad \varphi\cdot g_1=g\cdot\varphi_1 \tag{2}$$

каби ёзиш мумкин. Энди

$$(f;\ \varphi)+(\psi;\ g)=(fg+\varphi\psi;\ \varphi g),$$
$$(f;\ \varphi)\cdot(\psi;\ g)=(f\psi;\ \varphi g)$$

тенгликлардаги жуфтликларни $(f_1;\varphi_1)$ ва $(\varphi_1;g_1)$ жуфтликлар билан алмаштирамиз. Унда

$$(f_1;\ \varphi_1)+(\psi_1;\ g)=(f_1g_1+\varphi_1\psi_1;\ \varphi_1g_1),$$
$$(f_1;\ \varphi_1)\cdot(\varphi_1;\ g_1)=(f_1\cdot\varphi_1;\ \varphi_1g_1)$$

тенгликлар ҳосил бўлади. Бу тенгликларга асосан, иккита тенг жуфтликнинг йиғинди ва кўпайтмаси таққосланар экан, яъни

$$(fg+\varphi\psi)\varphi_1g_1=(f_1g_1+\varphi_1\psi_1)\varphi g, \tag{3}$$
$$f\psi\cdot\varphi_1g_1=\varphi g\cdot f_1\psi_1. \tag{4}$$

Биз бу тенгликлардан биринчисини текширамиз. Бунинг учун унинг чап томонидаги қавсларни очсак,

$$(fg\varphi_1 g_1 + \varphi\psi\varphi_1 g_1) \Rightarrow (f\varphi_1 \cdot gg_1 + \varphi g_1 \cdot \psi\varphi_1).$$

Агар (2) тенгликлардан фойдалансак, уни

$$\varphi f_1 \cdot gg_1 + g\varphi_1 \cdot \varphi\psi_1 = (f_1 g_1 + \varphi_1\psi_1)\,\varphi g$$

каби ёзиш мумкин. Бу тенгликнинг ўнг томони (3) нинг ўнг томонидан иборат. (4) тенгликни текширишни ўқувчига тавсия қиламиз.

Энди бу жўфтликлар майдон аксиомаларини қаноатлантиришини кўрсатамиз.

1. $(f; \varphi) + (\psi; g) = (fg + \varphi\psi;\ \varphi g) = (\varphi\psi + fg;\ \varphi g) = (\psi\varphi + gf;\ g\varphi) = (\psi; g) + (f; \varphi)$ (қўшиш коммутатив);

2. $(f; \varphi) \cdot (\psi; g) = (f\psi;\ \varphi g) = (\psi f;\ g\varphi) = (f; \varphi)$ (кўпайтириш коммутатив);

3. $((f; \varphi) + (\psi; g)) + (h; \theta) = (fg + \varphi\psi;\ \varphi g) + (h; \theta) = ((fg + \varphi\psi)\theta + \varphi gh; \varphi g\theta) = (fg\theta + \varphi\psi\theta + \varphi gh; \varphi g\theta) = (fg\theta + \varphi(\psi\theta + gh);\ \varphi g\theta) = (f; \varphi) + \varphi(\theta + gh;\ g\theta) = (f; \varphi) + ((\psi; g) + (h; \theta))$ (қўшиш ассоциатив).

Кўпайтириш амалининг ассоциативлиги ҳам шу усулда текширилади. Бу тўплам $(0; \theta)$ кўринишдаги ноль элементга эга бўлиб, $\theta \neq 0$ бўлади. Ҳақиқатан,

$$(f;\ \varphi) + (0;\ \theta) = (f\theta + 0\varphi;\ \ \varphi\theta) = (f\theta;\ \varphi\theta).$$

$(f\theta;\ \varphi\theta) \equiv (f;\ \varphi)$ ни 1-шартга асосан

$$((f\varphi\theta = \varphi f\theta) \Rightarrow (f\varphi = \varphi f)) \Rightarrow (f;\ \varphi) \equiv (f;\ \varphi)$$

кўринишда ёза оламиз. Демак,

$$(f;\ \varphi) + (0;\ \theta) = (f;\ \varphi).$$

$(f;\ \varphi) + (-f;\ \varphi) = (0;\ \varphi^2) = 0$ бўлгани учун $(-f;\ \varphi)$ жуфтлик $(f;\ \varphi)$ жуфтлик учун қарама-қарши элемент бўлади. Бу тўпламнинг бирлик элементи $(\theta;\ \theta) = e$ жуфтликдан иборат. Ҳақиқатан, $(f; \varphi) \cdot (\theta;\ \theta) = (f\theta;\ \varphi\theta) \equiv (f; \varphi)$. Тўпламда бирлик элемент мавжуд бўлгани сабабли унинг $(f;\ \varphi) \neq 0$ элементи учун тескари элемент ҳам мавжуд бўлиб, у $(\varphi;\ f)$ дан иборат. Чунки

$$(f;\ \varphi) \cdot (\varphi;\ f) = (f\varphi;\ \varphi f) = (f\varphi;\ f\varphi) = e.$$

Кўпайтириш амалининг қўшишга нисбатан дистрибутивлигини ҳам кўрсатиш мумкин. Буни ўқувчига тавсия қиламиз. Демак, $(f; \varphi)$ жуфтликларнинг $\mathscr{P}(x)$ тўплами коммутатив майдон бўлар экан.

Биз юқоридаги жуфтликлар учун киритилган муносабат рефлексивлик, симметриклик ва транзитивлик хоссаларга эга эканлигини кўрсатдик. Маълумки, агар бирор ρ муносабат рефлексив, симметрик ва транзитив бўлса, бундай муносабат эквивалентлик муносабати дейилар эди.

Эквивалентлик муносабати $(f; \varphi)$ жуфтликлар тўпламини эквивалентлик синфларига ажратади.

Таъриф. ρ эквивалент муносабат ёрдамида ҳосил қилинган $(f; \varphi)$ жуфтликлар тўпламининг ихтиёрий синфи *рационал каср дейилади* ва уни $\frac{f(x)}{\varphi(x)}$ $(f(x), \varphi(x) \in$ $\in \mathscr{P}(x), \varphi(x) \neq 0)$ кўринишда белгиланади.

Энди $\mathscr{P}(x)$ майдонда $\mathscr{P}[x]$ ҳалқа билан изоморф бўлган $\overline{\mathscr{P}}[x]$ ҳалқа мавжудлигини кўрсатамиз. Бу ерда $\overline{\mathscr{P}}[x]$ ҳалқанинг ҳар бир элементи шу ҳалқа иккита элементининг нисбатидан иборат бўлиши керак.

Бошқача айтганда, $\mathscr{P}[x]$ майдон элементлари орасидан $f(x) = \varphi(x) \cdot \psi(x)$ кўринишга эга бўлган $\varphi(x)$ элементлар тўпламини $\overline{\mathscr{P}}[x]$ деб белгилаймиз.

$\overline{\mathscr{P}}[x] \cong \mathscr{P}[x]$ ни кўрсатиш учун $\mathscr{P}[x]$ нинг $f(x)$ элементига $\overline{\mathscr{P}}[x]$ нинг $\frac{f(x)}{1}$ элементини мос қўямиз. Бу мослик ўзаро бир қийматли бўлиб, бу мослик элементларни қўшиш ва кўпайтиришда ҳам сақланади. Ҳақиқатан,

а) $\left(\frac{f(x)}{1} = \frac{\varphi(x)}{1}\right) \Rightarrow (f(x) \cdot 1 = \varphi(x) \cdot 1) \Rightarrow (f(x) = \varphi(x));$

б) $\frac{f(x)}{1} + \frac{\varphi(x)}{1} = \frac{f(x) \cdot 1 + \varphi(x) \cdot 1}{1^2} = \frac{f(x) + \varphi(x)}{1};$

в) $\frac{f(x)}{1} \cdot \frac{\varphi(x)}{1} = \frac{f(x) \cdot \varphi(x)}{1}.$

Шундай қилиб, $\frac{f(x)}{1}$ кўринишдаги касрларга тенг касрлар синфи $\mathscr{P}(x)$ майдонда $\mathscr{P}[x]$ ҳалқага изоморф қисм ҳалқа ташкил қилади.

Агар $g(x) \neq 0$ бўлса, $\frac{1}{g(x)}$ касрларга тенг касрлар синфи $\frac{g(x)}{1}$ касрларга тенг касрлар синфига тескари бўлади.

$$\frac{f(x)}{1} \cdot \frac{1}{g(x)} = \frac{f(x)}{g(x)}$$

тенгликдан $\mathscr{P}(x)$ майдоннинг барча элементларини $\mathscr{P}[x]$ ҳалқадаги кўпҳадлар нисбати дейиш мумкин.

Ихтиёрий $\mathscr{P}$ майдон устида $\mathscr{P}(x)$ рационал касрлар майдонини туздик. Кўпҳадлар ҳалқаси ўрнига бутун сонлар ҳалқасини олсак, ўша усул билан рационал сонлар майдонини тузиш мумкин. Бу иккита ҳолни бирлаштириб, ҳар қандай бутунлик соҳаси бирор майдоннинг қисм ҳалқаси бўлади деган тасдиқни ҳосил қиламиз.

Эслатма. Бир неча ўзгарувчили кўпҳадларнинг рационал касрлари тўплами ҳам майдон бўлади ва $\mathscr{P}[x_1, x_2, \ldots, x_k]$ ҳалқа $\mathscr{P}(x_1, x_2, \ldots, x_k)$ майдоннинг қисм тўплами бўлади. Бу тасдиқнинг исботи худди юқоридаги каби усулда бажарилади.

63-§. Кўп номаълумли кўпҳадларни келтирилмайдиган кўпҳадлар кўпайтмасига ёйиш

Биз бир номаълумли кўпҳадлар учун келтириладиган ва келтирилмайдиган бўлишлик ҳақида гапириб ўтган эдик. Кўпҳадларнинг келтириладиган ёки келтирилмайдиган бўлишлиги бир неча номаълумли кўпҳадлар учун ҳам ўринли.

Бундан сўнг $f(x_1, x_2, \ldots, x_k)$ кўпҳаднинг ўзгарувчиларини ёзиб ўтирмасдан, уни f орқали белгилаймиз.

1-таъриф. Агар $\mathscr{P}[x_1, x_2, \ldots, x_n]$ ҳалқада $= \varphi\psi$ тенглик бажарилса, *f кўпҳад φ кўпҳадга бўлинади* дейилади.

Кўп номаълумли кўпҳадларнинг бўлиниши ҳам бир номаълумли кўпҳадларнинг бўлиниши ҳақидаги барча хоссаларга эга.

2-таъриф. Даражаси $k \geqslant 1$ га тенг бўлган кўп номаълумли кўпҳадни $\mathscr{P}[x_1, x_2, \ldots, x_k]$ ҳалқанинг ҳар бирининг даражаси бирдан кичик бўлмаган камида иккита кўпҳад кўпайтмаси шаклида ёзиш мумкин бўлса, f кўпҳад *$\mathscr{P}$ майдон устида келтириладиган*, акс ҳолда $\mathscr{P}$ *майдон устида келтирилмайдиган кўпҳад* дейилади.

1-теорема. *$\mathscr{P}[x_1, x_2, \ldots, x_n]$ ҳалқанинг даражаси бирдан кичик бўлмаган ҳар бир кўпҳади келтирилмайдиган кўпҳадлар кўпайтмасига ёйилади ва бу ёйилма нолинчи даражали кўпҳад аниқлигида ягонадир.*

Теореманинг исботини кўпҳаддаги номаълумлар сони бўйича индукция принципи асосида олиб борамиз. Бир ўзгарувчили кўпҳад учун теореманинг исботини биз олдин кўриб ўтган эдик. Фараз қилайлик, теорема n номаълумли кўпҳад учун ўринли бўлсин. Унинг тўғрилигини $n+1$ номаълумли кўпҳадлар учун кўрсатамиз. $n+1$ та $x, x_1, x_2, \ldots, x_n$ номаълумли кўпҳадни $\varphi(x)$ орқали белгилаймиз. Бу кўпҳаднинг коэффициентлари $\mathscr{P}[x_1, x_2, \ldots, x_n]$ ҳалқага тегишлидир. Теоремани исботлаш учун қуйидаги ёрдамчи тушунчалардан фойдаланамиз.

3-таъриф. Агар $\varphi(x)$ кўпҳаднинг барча коэффициентлари ўзаро туб бўлса, у ҳолда $\varphi(x)$ *примитив кўпҳад* дейилади.

Бу таърифга асосан $\varphi(x)$ нинг барча коэффициентлари $\mathscr{P}[x_1, x_2, \ldots, x_n]$ да бирорта ҳам келтирилмайдиган умумий кўпайтувчига эга эмас.

2-теорема. *$\mathscr{P}[x_1, x_2, \ldots, x_n]$ ҳалқадан олинган иккита f ва φ кўпҳаднинг $f\cdot\varphi$ кўпайтмаси бирор келтирилмайдиган p кўпҳадга бўлинса, у ҳолда f ва φ кўпҳадларнинг камида биттаси p га бўлинади.*

Исботи. Тескарисини фараз қилайлик, яъни f ва φ нинг бирортаси ҳам p га бўлинмасин. У ҳолда кўпайтма иккита ёйилмага эга бўлиб, уларнинг бири p га бўлинади, иккинчиси эса p га бўлинмайди. Бундай бўлиши мумкин эмас. Демак, фаразимиз нотўғри экан.

1-лемма (Гаусс леммаси). *Иккита примитив кўпҳаднинг кўпайтмаси яна примитив кўпҳад бўлади.*

Исботи. Фараз қилайлик, коэффициентлари $\mathscr{P}[x_1, x_2, \ldots, x_n]$ ҳалқадан олинган иккита

$$f(x)=a_0x^k+a_1x^{k-1}+\ldots+a_ix^{k-i}+\ldots+a_k, \quad (1)$$

$$g(x)=b_0x^l+b_1x^{l-1}+\ldots+b_jx^{l-j}+\ldots+b_l \quad (2)$$

примитив кўпҳад берилган бўлиб, уларнинг кўпайтмаси

$$f(x) \cdot g(x) = c_0 x^{k+l} + c_1 x^{k+l-1} + \ \ldots \ + c_{i+j} x^{k+l-(i+j)} + \\ + \ldots + c_{k+l} \qquad (3)$$

кўринишда бўлсин.

Тескарисини фараз қиламиз, яъни (1) ва (2) примитив бўлиб, (3) примитивмас кўпҳад бўлсин.

$f(x)$ ва $\varphi(x)$ примитив бўлгани учун улардаги коэффициентларнинг камида биттаси (масалан, a_i ва b_j) келтирилмайдиган $p = p(x_1, x_2, \ldots, x_n)$ кўпҳадга бўлинмайди. (3) кўпайтма примитив бўлмагани учун, унинг барча коэффициентлари $p(x_1, x_2, \ldots, x_n)$ га бўлинади. Бу ерда $x^{k+l-(i+j)}$ ўзгарувчининг коэффициенти c_{i+j} қуйидаги кўринишга эга:

$$c_{i+j} = a_i b_j + a_{i-1} b_{j+1} + \ldots + a_{i+1} b_{j-1} + \\ + a_{i+2} b_{j-2} + \ldots \qquad (4)$$

Фаразимизга асосан (4) тенгликнинг чап томони ва унинг ўнг томонидаги биринчи ҳаддан бошқа барча ҳадлари келтирилмайдиган $p(x_1, x_2, \ldots, x_n)$ кўпҳадга бўлинади. Демак, $a_i b_j$ ҳам $p(x_1, x_2, \ldots, x_n)$ га бўлинади. Бу эса $f(x)$ ва $g(x)$ нинг примитив кўпҳадлар эканлигига зиддир. Бу зиддиятлик биз қилган фаразнинг нотўғрилигини билдиради. Демак, $f(x) \cdot g(x)$ примитив кўпҳад экан.

Бир неча ўзгарувчили кўпҳадлардан тузилган рационал касрлар тўплами майдон бўлиши бизга маълум. Агар бу майдонни $\mathscr{P}(x_1, x_2, \ldots, x_n)$ деб белгиласак, бу майдон (62-§ га асосан) $\mathscr{P}[x_1, x_2, \ldots, x_n]$ ҳалқани ўз ичига олади. Энди $\mathscr{P}(x_1, x_2, \ldots, x_n) = Q$ деб, $Q[x]$ кўпҳадлар ҳалқасини қараймиз. Коэффициентлари $Q[x]$ ҳалқага тегишли бўлган ҳар қандай $\varphi(x)$ кўпҳадни қуйидагича ёза оламиз:

$$\varphi(x) = \frac{a}{b} f(x), \qquad (5)$$

(5) да b маҳраж $\varphi(x)$ кўпҳад коэффициентларининг умумий махражи, a эса бу коэффициентлар суратларининг умумий кўпайтувчиси бўлиб, $f(x)$ примитив кўпҳаддир.

Юқоридаги тенглик ўринли бўлган ҳолда $\varphi(x)$ ни $f(x)$ га мос деб оламиз. У ҳолда қуйидаги лемма ўринли.

2-лемма. *Ҳар қандай $\varphi(x)$ кўпҳад учун унга мос примитив $f(x)$ кўпҳад мавжуд ва у $\mathscr{P}(x_1, x_2, \ldots, x_n)$ майдондан олинган кўпайтувчи аниқлигича ягонадир.*

Биз юқорида $f(x)$ кўпҳад мавжудлигини кўрсатган эдик, энди унинг ягоналигини кўрсатамиз. Тескарисири фараз қилайлик, яъни $\varphi(x)$ учун ушбу

$$\varphi(x) = \frac{c}{a} g(x) \tag{6}$$

тенглик ўринли бўлиб. $g(x)$ примитив кўпҳад бўлсин. (5) ва (6) дан

$$adf(x) = bcg(x) \tag{7}$$

келиб чиқади. (7) тенгликдаги ad ва bc лар $\mathscr{P}[x_1, x_2, \ldots, x_n]$ ҳалқадаги биргина $\varphi(x)$ кўпҳад коэффициентларининг умумий кўпайтувчисидан иборат. Бу кўпайтмалардаги ҳар бир кўпайтувчи n номаълумли бўлганлигидан асосий теорема булар учун тўғри бўлиб, улар бир-биридан нолинчи даражали кўпайтувчи билангина фарқ қилади. Демак, $f(x)$ ва $g(x)$ примитив кўпҳадлар ҳам шу нолинчи даражали кўпҳад билан бир-биридан фарқ қилади.

3-лемма. *$Q[x]$ ҳалқадан олинган иккита кўпҳад кўпайтмасига бу кўпҳадларга мос келувчи примитив кўпҳадлар кўпайтмаси мос келаси*

Исботи. 2-леммага асосан ҳар қандай иккита $\varphi(x)$ ва $\psi(x)$ кўпҳад учун

$$\varphi(x) = \frac{a}{b} f(x) \text{ ва } \psi(x) = \frac{c}{d} g(x)$$

тенгликлар рост бўлиб, бу ерда $f(x)$ ва $g(x)$ примитив кўпҳадлардир. Агар буларни ҳадлаб кўпайтирсак,

$$\varphi(x)\psi(x) = \frac{ac}{bd} f(x) \cdot g(x)$$

тенглик ҳосил бўлиб, бу ерда Гаусс леммасига асосан $f(x) \cdot g(x)$ примитив кўпҳад бўлади.

4-лемма. *Агар $Q[x]$ ҳалқанинг бирор $\varphi(x)$ кўпҳади Q майдон устида келтирилмайдиган бўлса, унга мос келувчи $f(x)$ примитив кўпҳад ҳам шу майдон устида келтирилмайдиган кўпҳад бўлади ва аксинча.*

Исботи. Тескарисини фараз қилайлик, яъни $\mathscr{P}(x_1, x_2, \ldots, x_n)$ майдонда f кўпҳад келтириладиган бўлиб, $f = f_1 \cdot f_2$ тенглик ўринли бўлсин. Бунда f_1 ва f_2 нинг ҳар бири x ўзгарувчига боғлиқ бўлади, акс ҳолда f кўпҳад Q майдонда примитив бўлмас эди.

$f(x)$ кўпҳад $\varphi(x)$ га мос келувчи примитив кўпҳад бўлгани учун

$$\varphi(x) = \frac{a}{b} f(x) = \left(\frac{a}{b} f_1\right) \cdot f_2$$

тенглик тўғри. Бу тенглик $\varphi(x)$ нинг Q устида келтириладиган кўпҳад эканлигини билдиради. Бу эса натижа шартига зид. Демак, $f(x)$ ни келтириладиган кўпҳад деб қилган фаразимиз нотўғри экан.

Агар $\varphi(x)$ кўпҳад Q майдон устида келтириладиган бўлса, унда $\varphi(x) = \varphi_1(x) \cdot \varphi_2(x)$ тенглик ўринли бўлиб, $\varphi_1(x)$ ва $\varphi_2(x)$ га мос келувчи примитив $f_1(x)$ ва $f_2(x)$ кўпҳадларнинг ҳар бири ўзгарувчининг функциясидан иборат. Бу кўпҳадлар кўпайтмаси, 2-леммада кўриб ўтганимиздек, $\mathscr{P}$ майдон элементи кўпайтмаси аниқлигида ягонадир.

5-лемма. *Примитив кўпҳаднинг келтирилмайдиган кўпҳадлар кўпайтмасига ёйилмаси $\mathscr{P}$ сонлар майдонидан олинган ўзгармас кўпайтувчи аниқлигида ягонадир.*

Исботи. f примитив кўпҳад ёйилмаси қуйидаги кўринишда бўлсин:

$$f = f_1 \cdot f_2 \ldots f_n. \tag{8}$$

Бу ёйилмадаги ҳар бир f_i $(i = \overline{1, n})$ кўпайтувчи n та ўзгарувчига боғлиқ бўлиб, улар алоҳида-алоҳида примитив кўпҳад бўлади. Акс ҳолда f ҳам примитив кўпҳад бўлмас эди.

Бу ёйилмани примитив $f(x)$ кўпҳаднинг $Q = \mathscr{P}(x_1, x_2, \ldots, x_n)$ майдон устидаги келтирилмайдиган кўпҳадларга ёйилмаси деб қараш мумкин. Бир номаълумли кўпҳадлар учун ёйилманинг ягоналигини биз биламиз. Бу ягоналик Q майдондан олинган кўпайтувчи аниқлигичалиги бизга маълум. Лекин, f_i лар примитив кўпҳадлар бўлганлиги учун бу кўпайтувчи ўзгармас сондан иборат. Демак, (8) ёйилма $\mathscr{P}$ сонлар майдонидан олинган ўзгармас кўпайтувчи аниқлигида ягона экан.

Энди асосий теореманинг исботига ўтамиз:

$\mathscr{P}[x_1, x_2, \ldots, x_k]$ ҳалқанинг ҳар қандай келтирилмайдиган кўпҳади $\mathscr{P}[x_1, x_2, \ldots, x_k]$ ҳалқада келтирилмайдиган кўпҳад ёки келтирилмайдиган примитив кўпҳад бўлади. Демак, $\varphi(x_1, x_2, \ldots, x_n)$ кўпҳад келтирилмайдигац кўпҳадлар кўпайтмасига ёйилган бўлса, уни 2-леммага асосан

$$\varphi(x) = a(x_1, x_2, \ldots, x_n)\cdot f(x, x_1, \ldots, x_n)$$

кўринишда ёзиш мумкин бўлиб, бу ерда a кўпайтувчи x га боғлиқ бўлмай, f эса примитив кўпҳаддир.

Индуктивлик қонунига асосан теорема $a(x_1, x_2, \ldots, x_k)$ учун рост. 5-леммага кўра $n+1$ та номаълумли примитив $f(x)$ кўпҳаднинг келтирилмайдиган кўпҳадлар кўпайтмасига ёйилмаси ҳам майдондан олинган ўзгармас кўпайтувчи аниқлигида ягонадир. Шундай қилиб, теорема тўла исбот этилди.

Биз биламизки, даражаси иккидан кичик бўлмаган бир номаълумли $f(x)$ кўпҳад бирор $\mathscr{P}$ майдон устида келтирилмайднган бўлса, бу кўпҳад $\mathscr{P}$ учун кенгайтма майдон бўлган $\mathscr{P}'$ да келтириладиган бўлар эди. Бир неча номаълумли кўпҳадлар учун бу тасдиқ тўғри эмас. Бошқача айтганда, қуйидаги мулоҳаза ўринли:

Ҳар қандай майдонда ҳам келтирилмайдиган кўп номаълумли кўпҳад доимо мавжуд. Масалан, агар $\varphi(x)$ кўпҳад $\mathscr{P}$ майдон устида берилган бир номаълумли кўпҳад бўлса, $f(x; y) = \varphi(x) + y$ кўпҳад $\mathscr{P}$ нинг ҳар қандай $\mathscr{P}'$ кенгайтмаси устида ҳам келтирилмайдиган кўпҳад бўлади. Агар тескарисини фараз қиласак, $\mathscr{P}'$ майдон устида

$$f(x; y) = g(x; y)\cdot h(x; y)$$

тенглик ўринли бўларди. Бу ерда $g(x; y)$ ва $h(x; y)$ нинг камида биттаси y номаълумга боғлиқ бўлмаслиги керак. Акс ҳолда $f(x; y)$ кўпҳад y^2 га боғлиқ бўлар эди. Шунинг учун

$$g(x; y) = a_0(x)\,y + a_1(x),$$
$$h(x; y) = b_0(x)$$

десак. $a_0(x)\cdot(b_0 x) = 1$ бўлиб, $a_0(x)$ ва $b_0(x)$ нолинчи даражали кўпҳад бўлади. $b_0(x)$ нолинчи даражали кўпҳад бўлганлигидан бу кўпҳад x га ҳам боғлиқ эмас.

Бундан $h(x;\ y)$ нинг x га ҳам боғлиқ эмаслиги келиб чиқади. Демак, $h(x;\ y)$ кўпҳад нолинчи даражали кўпҳад экан.

64-§. Симметрик кўпҳадлар

1-таъриф. Агар кўп номаълумли кўпҳаддаги ихтиёрий иккита номаълумнинг ўринларини алмаштирганда кўпҳад ўзгармаса, у ҳолда бундай кўпҳад *симметрик кўпҳад* дейилади.

1-мисол. $f(x_1,\ x_2,\ x_3) = x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2$ кўпҳад симметрик кўпҳаддир, чунки бу кўпҳаддаги x , x_2, x_3 номаълумларнинг ҳамма 6 та ўринларини алмаштириб чиқсак, кўпҳад ўзгармайди. Чунончи, x_1 ва x_2 номаълумларни бир-бири билан алмаштирсак, $x_2x_1x_3 + x_2x_1x_3^2 + x_2x_1x_3^2$ кўпҳад ҳосил бўлиб, бу эса ўша кўпҳаднинг ўзгинасидир. Шунга ўхшаш, x_2 ва x_3 ни алмаштириб, $x_1^2x_3x_2 + x_1x_3x_2^2 + x_1x_3x_2^2$ кўпҳадни ҳосил қиламиз. Бу эса яна берилган кўпҳаднинг ўзидир.

n та номаълумли симметрик кўпҳадларнинг алгебраик йиғиндиси ва кўпайтмаси яна n та номаълумли симметрик кўпҳадлар бўлади. Ҳақиқатан, номаълумларнинг исталган ўрин алмаштиришида ҳар қайси симметрик кўпҳад ўзгармаса, равшанки, уларнинг алгебраик йиғиндиси ва кўпайтмаси ҳам ўзгармайди. Масалан, $f_1(x_1,\ x_2,\ x_3) = x_1 + x_2 + x_3$ ва $f_2(x_1,\ x_2,\ x_3) = x_1x_2x_3$ симметрик кўпҳадларнинг қуйидаги алгебраик йиғиндиси ва кўпайтмаси яна симметрик кўпҳадлардир:

$$f_1 \pm f_2 = x_1 + x_2 + x_3 \pm x_1x_2x_3;$$
$$f_1 \cdot f_2 = x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2,$$

2-таъриф. $x_1,\ x_2, \ldots, x_n$ номаълумлардан тузилган.

$$\begin{aligned} \tau_1 &= x_1 + x_2 + \ldots + x_n, \\ \tau_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ \tau_n &= x_1x_2 \cdots x_n \end{aligned} \qquad (1)$$

симметрик кўпҳадлар *асосий (элементар) симметрик кўпҳадлар* деб аталади.

Юқоридаги мисолни $f(x_1,\ x_2,\ x_8) = (x_1 + x_2 + x_8) \times \times x_9x_2x_3$ кўринишда ёзиб, $\tau_1 = x_1 + x_2 + x_8$, $\tau_3 = x_1x_2x_3$

эканини эътиборга олсак, у ҳолда $f=\tau_1\cdot\tau_3$ тенглик ҳосил бўлади. Шундай қилиб, берилган симметрик кўпҳад асосий симметрик кўпҳадлар орқали ифодаланади.

Яна

$$f(x_1,\ x_2,\ x_3)=x_1^2+3x_1x_3+3x_1x_3+x_2^2+3x_2x_3+$$
$$+x_3^2-3x_1x_2x_3$$

симметрик кўпҳадни

$$f(x_1,\ x_2,\ x_3)=(x_1+x_2+x_3)^2+(x_1x_2+x_1x_3+x_2x_3)-$$
$$-3x_1x_2x_3$$

кўринишда олиб

$$\tau_1=x_1+x_2+x_3,\quad \tau_2=x_1x_2+x_1x_3+x_2x_3,\quad \tau_3=x_1x_2x_3$$

эканини ҳисобга олсак, у ҳолда

$$f(x_1,\ x_2,\ x_3)=\tau_1^2+\tau_2-3\tau_3$$

тенгликни ҳосил қиламиз. Демак, бу ҳолда ҳам симметрик кўпҳад асосий симметрик кўпҳадлар орқали ифодаланади.

1-теорема. *$\mathscr{P}$ майдон устидаги $\tau_1,\ \tau_2, \ldots, \tau_n$ асосий симметрик кўпҳадларнинг*

$$a_1\tau_1^{\alpha_1}\tau_2^{\alpha_2}\cdots\tau_n^{\alpha_n}+a_2\tau_1^{\beta_1}\tau_1^{\beta_2}\cdots\tau_n^{\beta_n}+\ldots$$
$$\ldots+a_k\tau_1^{W_1}\cdot\tau_2^{W_2}\cdots\tau_n^{W_n} \qquad (2)$$

кўпҳади фақат $a_1=a_2=\ldots=a_k=0$ бўлгандагина нолга тенг бўла олади, бу ерда $\alpha_i,\ \beta_i, \ldots, W_i$ манфиймас бутун сонлардир.

Исботи. (2) кўпҳаднинг ҳар бир

$$a\ \tau_1^{\gamma_1}\tau_2^{\gamma_2}\cdots\tau_n^{\gamma_n} \qquad (3)$$

ҳади, маълумки, $x_1,\ x_2, \ldots, x_n$ номаълумларнинг бирор кўпҳадидан иборат, чунки (3) га

$$\tau_1=x_1+x_2+\ldots+x_n,$$
$$\tau_2=x_1x_2+x_1x_3+\ldots+x_{n-1}x_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\tau_n=x_1x_2\cdots x_n$$

қийматларни қўйиб, кўрсатилган амалларни бажарсак, худди айтилган кўпҳад келиб чиқади.

Бу (3) кўпҳаднинг энг юқори ҳадини топамиз. τ_1, $\tau_2, \ldots, \tau_n$ нинг энг юқори ҳадлари мос равишда,

$$x_1,\ x_1x_2,\ x_1x_2x_3, \ldots, x_1x_2\cdots x_n$$

бўлгани учун (3) кўпайтманинг энг юқори ҳади

$$a_l x_1^{\gamma_1}(x_1x_2)^{\gamma_2}\cdot(x_1x_2x_3)^{\gamma_3}\cdots(x_1x_2\cdots x_n)^{\gamma_n} =$$
$$= a_l x_1^{\gamma_1+\gamma_2+\ldots+\gamma_n}\cdot x_2^{\gamma_2+\gamma_3+\ldots+\gamma_n}\cdot x_3^{\gamma_3+\gamma_4+\ldots+\gamma_n}\cdots x_n^{\gamma_n} \qquad (4)$$

бўлади. Худди шу йўл билан (3) йиғиндидаги ҳар бир қўшилувчининг энг юқори ҳадини аниқлаб чиқамиз. Бу юқори ҳадлар орасида бир-бирига ўхшаш ҳадлар йўқ. Ҳақиқатан, агар (4)' бирор бошқа юқори ҳадни бир-бирига ўхшаш десак,

$$\begin{aligned}\gamma_1+\gamma_2+\ldots+\gamma_n &= \delta_1+\delta_2+\ldots+\delta_n,\\ \gamma_2+\ldots+\gamma_n &= \delta_2+\ldots+\delta_n,\\ \ldots\ldots&\ldots\ldots\\ \gamma_n &= \delta_n\end{aligned}$$

тенгликлардан $\gamma_1=\delta_1$, $\gamma_2=\delta_2,\ldots,\gamma_n=\delta_n$ ни топамиз. Бу эса (3) кўпҳаднинг

$$a_l\tau_1^{\gamma_1}\cdot\tau_2^{\gamma_2}\cdots\tau_n^{\gamma_n} \text{ ва } a_j\tau_1^{\delta_1}\cdot\tau_2^{\delta_2}\cdots\tau_n^{\delta_n}$$

ҳадлари ўхшаш эканини кўрсатади. Аммо, бизга маълумки, кўпҳаднинг ўхшаш ҳадлари йўқ деб фараз қила оламиз.

Энди айтилган юқори ҳадлар орасида энг юқориси, масалан,

$$a_l x_1^{\alpha_1+\alpha_2+\ldots+\alpha_n}\cdot x_2^{\alpha_2+\alpha_3+\ldots+\alpha_n}\cdots x_n^{\alpha_n} \qquad (5)$$

бўлсин. Бу вақтда, равшанки, (2) ни $x_1, x_2,\ldots,x_n$ нинг кўпҳади деб қарасак, (5) ҳад унинг энг юқори ҳади бўлади. Шу сабабли (2) ни

$$a_1 x_1^{\alpha_1+\alpha_2+\ldots+\alpha_n}\cdot x_2^{\alpha_2+\alpha_3+\ldots+\alpha_n}\cdots x_n^{\alpha_n}+Q \qquad (6)$$

кўринишда ёзиш мумкин. Бунда Q—қолган ҳамма ҳадларнинг йиғиндиси. $a_1\neq 0$ ҳолда, (6) йиғинди ва, демак, (2) ҳам нолга тенг бўла олмайди. $a_1=0$ бўлган ҳолда, (2) кўпҳад

$$a_2\tau_1^{\beta_1}\cdot\tau_2^{\beta_2}\cdots\tau_n^{\beta_n}+\ldots+a_k\tau_1^{W_1}\cdot\tau_2^{W_2}\cdots\tau_n^{W_n}$$

кўринишни олади. Юқоридаги мулоҳазани такрорлаб, $a_l\neq 0$ ҳолда бу кўпҳаднинг нолга тенг бўла олмаслигини исботлаймиз ва ҳ. к.

Бу теоремага асосан, икки $f(\tau_1, \tau_2,\ldots,\tau_n)$ ва $\varphi(\tau_1, \tau_2,\ldots,\tau_n)$ кўпҳаддан ҳар бирининг ҳадлари иккинчисининг ҳадларига айнан тенг бўлган ҳолдагина бу кўпҳадлар бир-бирига тенг деган натижага келамиз.

Ҳақиқатан, бир кўпҳадда $a\tau_1^{\alpha_1}\cdot\tau_2^{\alpha_2}\cdots\tau_n^{\alpha_n}$ ҳад мавжуд бўлиб, иккинчисида бўлмаса, иккинчи кўпҳадга $0\cdot\tau_1^{\alpha_1}\times$ $\times\tau_2^{\alpha_2}\cdots\tau_n^{\alpha_n}$ ҳадни қўшиш мумкинлигини назарда тутиб, бу икки кўпҳадни

$$f(\tau_1, \tau_2, \dots, \tau_n) = a_1\tau_1^{\alpha_1}\cdot\tau_2^{\alpha_2}\cdots\tau_n^{\alpha_n} + \\ + a_2\tau_1^{\beta_1}\cdot\tau_2^{\beta_2}\cdots\tau_n^{\beta_n} + \dots + a_k\tau_1^{\gamma_1}\cdot\tau_2^{\gamma_2}\cdots\tau_n^{\gamma_n}$$

ва

$$\varphi(\tau_1, \tau_2, \dots, \tau_n) = b_1\tau_1^{\alpha_1}\cdot\tau_2^{\alpha_2}\cdots\tau_n^{\alpha_n} + \\ + b_2\tau_1^{\beta_1}\cdot\tau_2^{\beta_2}\cdots\tau_n^{\beta_n} + \dots + b_k\tau_1^{\gamma_1}\cdot\tau_2^{\gamma_2}\cdots\tau_n^{\gamma_n}$$

кўринишда ёзайлик. Энди, кўпҳадларни бир-бирига тенглаштиргандан кейин ушбу тенгликка келамиз:

$$(a_1 - b_1)\tau_1^{\alpha_1}\cdot\tau_2^{\alpha_2}\cdots\tau_n^{\alpha_n} + (a_2 - b_2)\tau_1^{\beta_1}\cdot\tau_2^{\beta_2}\cdots\tau_n^{\beta_n} + \\ + \dots + (a_k - b_k)\tau_1^{\gamma_1}\cdot\tau_2^{\gamma_2}\cdots\tau_n^{\gamma_n} = 0.$$

Бундан, юқорида исботланганга мувофиқ, $a_i - b_i = 0$ ёки $a_i = b_i$ $(i = 1, 2, \dots, k)$ ҳосил бўлади.

2-теорема (симметрик кўпҳадлар ҳақидаги асосий теорема). $\mathcal{F}$ *майдон устидаги ҳар қандай симметрик кўпҳад шу майдон устида элементар симметрик кўпҳадлар орқали ягона ифодаланади.*

Исботи. Фараз қилайлик, $f(x_1, x_2, \dots, x_n)$ симметрик кўпҳад ва унинг энг юқори ҳади

$$a_1x_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdots x_n^{\alpha_n} \tag{7}$$

бўлсин. (7) ҳаднинг даража кўрсаткичлари $\alpha_1 \geqslant \alpha_2 \geqslant \dots \geqslant \alpha_n$ тенгсизликларни қаноатлантиради. Ҳақиқатан, симметрик кўпҳадда x_1 ва x_2 нинг ўринларини алмаштирсак, маълумки, функция ўзгармайди. Бу алмаштириш натижасида (7) ҳад шу симметрик кўпҳаднинг $ax_1^{\alpha_2}x_2^{\alpha_1}x_3^{\alpha_3}\cdots x_n^{\alpha_n}$ ҳадига ўтади. Аммо (7) энг юқори ҳад бўлгани учун, $\alpha_1 \geqslant \alpha_2$. Шунингдек, симметрик кўпҳадда x_2 ва x_3 ни ўзаро алмаштирсак, (7) ҳад кўпҳаднинг $a_1x_1^{\alpha_1}\cdot x_2^{\alpha_3}\cdots x_n^{\alpha_n}$ ҳадига ўтади ва бундан $\alpha_2 \geqslant \alpha_3$ ҳосил бўлади ва ҳ. к.

$x_1, x_2, \dots, x_n$ номаълумларнинг $\tau_1, \tau_2, \dots, \tau_n$ асосий симметрик кўпҳадларини олиб, шу номаълумларнинг симметрик кўпҳади бўлган ушбу

$$a\tau_1^{\alpha_1-\alpha_2}\cdot\tau_2^{\alpha_2-\alpha_3}\cdots\tau_{n-1}^{\alpha_{n-1}-\alpha_n}\cdot\tau_n^{\alpha_n} \tag{8}$$

кўпайтмани тузамиз. $\tau_1, \tau_2, \ldots, \tau_n$ нинг энг юқори ҳадлари, мос равишда x_1; x_1x_2; $x_1x_2x_3; \ldots; x_1x_2\cdots x_n$ бўлгани сабабли (8) кўпайтманинг энг юқори ҳади

$$ax_1^{\alpha_1-\alpha_2}\cdot(x_1\,x_2)^{\alpha_2-\alpha_3}\cdots(x_1\cdot x_2\cdots x_n)^{\alpha_n}=$$
$$=ax_1^{\alpha_1}\cdot x_2^{\alpha_2}\cdots x_n^{\alpha_n}$$

бўлади. Бунда $f(x_1, x_2, \ldots, x_n)$ кўпҳаднинг энг юқори ҳади келиб чиққанини кўрамиз. Шу сабабли, иккита симметрик кўпҳаднинг айирмаси бўлган

$$f(x_1,\ x_2, \ldots, x_n)-a\tau_1^{\alpha_1-\alpha_2}\cdot\tau_2^{\alpha_2-\alpha_3}\cdots\tau_n^{\alpha_n}=$$
$$=f_1(x_1,\ x_2, \ldots, x_n)$$

симметрик кўпҳадда (8) ҳад бўлмайди. Шу мулоҳазани $f_1(x_1, x_2, \ldots, x_n)$ га нисбатан такрорлаб,

$$f_1(x_1,\ x_2, \ldots, x_n)-b\tau_1^{\beta_1-\beta_2}\cdot\tau_2^{\beta_2-\beta_3}\cdots\tau_n^{\beta_n}=$$
$$=f_2(x_1,\ x_2, \ldots, x_n)$$

симметрик кўпҳадни тузамиз. Унинг ҳадлари $f(x_1, x_2, \ldots, x_n)$ иинг энг юқори ҳадидан кичикдир ва ҳ. к. Бу жараён чекли равишда давом этади. Ҳақиқатан, f_1 f_2, $f_3, \ldots$ симметрик кўпҳадлардан исталганининг юқори ҳадини

$$m\,x_1^{\lambda_1}\cdot x_2^{\lambda_2}\cdots x_n^{\lambda_n} \tag{9}$$

орқали белгиласак, $\alpha_1 \geqslant \lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n$ тенгсизликларга эга бўламиз. Аммо бу тенгсизликларни фақат чекли сон $\lambda_1, \lambda_2, \ldots, \lambda_n$ кўрсаткичлар (манфиймас бутун сонлар) қаноатлантириши мумкин. Демак, (9) кўринишдаги юқори ҳадларнинг, шунингдек, f_1, f_2, $f_3, \ldots$ кўпҳадларнинг сони фақат чекли бўла олади.

Шундай қилиб, чекли сондаги қадамлардан кейин $f(x_1, x_2, \ldots, x_n)$ симметрик кўпҳад $\tau_1, \tau_2, \ldots, \tau_n$ нинг ўша $\mathscr{P}$ майдон устидаги кўпҳади сифатида ифодаланади, яъни

$$f(x_1,\ x_2, \ldots, x_n)=g(\tau_1,\ \tau_2, \ldots, \tau_n) \tag{10}$$

тенглик ўринли.

Энди (10) ифодаланишнинг ягона эканини исботлаймиз. Фараз қилайлик, $f(x_1, x_2, \ldots, x_n)$ симметрик кўпҳад (10) дан бошқа яна $\tau_1, \tau_2, \ldots, \tau_n$ нинг иккинчи кўпҳади билан ушбу

$$f(x_1,\ x_2, \ldots, x_n)=\psi(\tau_1,\ \tau_2, \ldots, \tau_n) \tag{11}$$

кўринишда ифодалансин. (10) ва (11) нинг чап томонлари бир хил эканлигидан $g(\tau_1, \tau_2, \dots, \tau_n) = \psi(\tau_1, \tau_2, \dots, \tau_n)$ тенгликни ҳосил қиламиз. Бу тенглик эса $g(\tau_1, \tau_2, \dots, \tau_n)$ ва $\psi(\tau_1, \tau_2, \dots, \tau_n)$ кўпҳадлардан ҳар бирининг ҳадлари айнан тенг, яъни бу кўпҳадлар аслида битта кўпҳад эканини кўрсатади. Демак, (10) ифодаланиш ягона экан.

2-мисол. Рационал сонлар майдони устидаги

$$f(x_1, x_2, x_3) = x_1^2x_2 + x_1^2x_3 + x_2^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2x_3^2$$

симметрик кўпҳадни асосий симметрик кўпҳадлар орқали ифодаланг.

$f(x_1, x_2, x_3)$ нинг энг юқори ҳади $x_1^2x_2$ бўлгани учун, $\alpha_1 = 2$, $\alpha_2 = 1$, $\alpha_3 = 0$. Теоремага асосан қуйидаги айирмани тузамиз:

$$f(x_1, x_2, x_3) - \tau_1^{\alpha_1-\alpha_2} \cdot \tau_2^{\alpha_2-\alpha_3} \cdot \tau_3^{\alpha_3} =$$

$$= (x_1^2x_2 + x_1^2x_3 + x_2^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2x_3^2) - \tau_1\tau_2 =$$

$$= (x_1^2x_2 + x_1^2x_3 + x_2^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2x_3^2) -$$

$$- (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) = -3x_1x_2x_3.$$

Бунда $x_1x_2x_3 = \tau_3$, Демак, $f(x_1, x_2, x_3) = \tau_1\tau_2 - 3\tau_3$ бўлади.

Симметрик кўпҳадларни асосий симметрик кўпҳадлар орқали ифодалашнинг амалий жиҳатдан қулай усулини кўриб ўтамиз. Бу *аниқмас коэффициентлар усули* дейилади. Усулнинг моҳияти қуйидагидан иборат.

Берилган симметрик кўпҳад формалар йиғиндисига ажратилади (равшанки, ҳар бир форма ўз навбатида симметрик кўпҳадни ифодалайди*) сўнгра аниқмас коэффициентлар усули билан ҳар бир форма асосий симметрик кўпҳадлар орқали ифодаланади.

3-мисол. Рационал сонлар майдони устидаги

$$f(x_1, x_2, x_3) = x_1^3x_2^2x_3 + x_1^2x_2^3x_3 + x_1^2x_2x_3^3 +$$

$$+ x_1^3x_2x_3^2 + x_1x_2^2x_3^2 + x_1x_2^3x_3^2 + x_1^3 + x_2^3 + x_2^3$$

симметрик кўпҳадни асосий симметрик кўпҳадлар орқали ифодаланг.

Берилган кўпҳад қуйидаги иккита форма йиғиндисига ажралади:

---

* Чунки ўзгарувчиларнинг ўринларини алмаштирганда ҳадларнинг даражалари ўзгармайди.

$$f(x_1, x_2, x_3) = \varphi_1(x_1, x_2, x_3) + \varphi_2(x_1, x_2, x_3) =$$
$$= (x_1^3 x_3^2 x_3 + x_1^2 x_2^3 x_3 + x_1^2 x_2 x_3^3 + x_1^3 x_2 x_3^2 +$$
$$+ x_1 x_2^2 x_3^3 + x_1 x_2^3 x_3^2) + (x_1^3 + x_2^3 + x_3^3)$$

Аввал биринчи

$$\varphi_1(x_1, x_2, x_3) = x_1^3 x_2^2 x_3 + x_1^2 x_2^3 x_3 + x_1^2 x_2 x_3^3 +$$
$$+ x_1^3 x_2 x_3^2 + x_1 x_2^2 x_3^3 + x_1 x_2^3 x_3^2$$

формани олиб асосий симметрик кўпҳадлар орқали ифодалаймиз.

2-теореманинг исботида айтилган ҳамма $f_1, f_2, f_3, \ldots$ симметрик кўпҳадларнинг энг юқори ҳадларини ҳисобга оламиз. Бунда φ_1 кўпҳад 6-даражали форма бўлгани учун $f_1, f_2, f_3, \ldots$ симметрик кўпҳадлар ҳам 6-даражали формалардан иборат бўлиши керак. Шу билан бирга, ҳар бир юқори ҳаднинг $\alpha_1, \alpha_2, \alpha_3$ даража кўрсаткичлари $\alpha_1 \geqslant \alpha_2 \geqslant \alpha_3$ ва $\alpha_1 + \alpha_2 + \alpha_3 = 6$ шартларни қаноатлантириши кераклигини ҳам назарда тутишимиз лозим. Бунда φ_1 кўпҳаднинг энг юқори ҳади $x_1^3 x_2^2 x_3$ бўлиб, даража кўрсаткичлар 3, 2, 1 системани тузади. Кейинги f_1 кўпҳаднинг энг юқори ҳади φ_1 нинг юқори ҳадидан кичик бўлиши керак. Шу сабабли, бу иккинчи юқори ҳаднинг даража кўрсаткичлари учун фақат 2, 2, 2 системани ҳосил қиламиз, чунки шундан бошқа система $\alpha_1 \geqslant \alpha_2 \geqslant \alpha_3$ ва $\alpha_1 + \alpha_2 + \alpha_3 = 6$ шартларни бир вақтда қаноатлантира олмайди. Шу билан жараён тугайди, чунки кейинги f_2 симметрик кўпҳаднинг энг юқори ҳади учун $\alpha_1 \geqslant \alpha_2 \geqslant \alpha_3$ ва $\alpha_1 + \alpha_2 + \alpha_3 = 6$ шартларни қаноатлантирувчи даража кўрсаткичлар системаси йўқ*. Энди қуйидаги жадвални тузамиз:

Энг юқори ҳадларнинг даража кўрсаткичлари системаси	Энг юқори ҳадлари	Асосий симметрик кўпҳадлардан тузиладиган тегишли кўпайтмалар
3 2 1	$x_1^3 x_2^2 x_3$	$\tau_1^{3-2} \tau_2^{2-1} \cdot \tau_3 = \tau_1 \tau_2 \tau_3$
2 2 2	$a x_1^2 x_2^2 x_3^2$	$a\tau_1^{2-2} \tau_2^{2-2} \cdot \tau_3^2 = a\tau_3^2$

Бу жадвалдан қуйидаги тенглик ҳосил бўлади:

$$\varphi_1(x_1, x_2, x_3) = \tau_1 \tau_2 \tau_3 + a\tau_3. \tag{12}$$

---

* f_2 нинг энг юқори ҳади f_1 нинг юқори ҳадларидан паст бўлиш шарти билан.

Номаълум a коэффициентни аниқлаймиз. Шу мақсадда, (12) тенгликни мукаммал

$$x_1^3x_2^2x_3+x_1^2x_2x_3^3+x_1^2x_2^3x_3+x_1^3x_2x_3^2+$$
$$+x_1x_2^2x_3^3+x_1x_2^3x_3^2=(x_1+x_2+x_3)(x_1x_2+ \quad (13)$$
$$+x_1x_3+x_2x_3)(x_1x_2x_3)+a(x_1x_2x_3)^4$$

кўринишда ёзиб, x_1, x_2, x_3 га шундай ихтиёрий қийматлар берамизки, уларнинг ёрдами билан a нинг қийматини аниқлаш мумкин бўлсин*.

Масалан, $x_1=2$, $x_2=-1$, $x_3=-1$ десак, (13) дан $-12=0+4a$ ёки $a=-3$ келиб чиқади. Демак,

$$\varphi(x_1,\ x_2,\ x_3)=\tau_1\tau_2\tau_3-3\tau_3^2$$

тенглик ҳосил бўлади. Энди худди шу усул билан иккинчи $\varphi_2(x_1,\ x_2,\ x_3)=x_1^3+x_2^3+x_3^3$ форма учун жадвал тузамиз:

Энг юқори ҳадларнинг курсаткичлари системаси	Энг юқори ҳадлар	Асосий симметрик кўпҳадлардан тузилган тегишли кўпайтмалар
3 0 0	x_1^3	$\tau_1^{3-0}\tau_2^{0-0}\tau_3^0=\tau_1^3$
2 1 0	$ax_1^2x_2$	$a\tau_1^{2-1}\tau_2^{1-0}\tau_3^0=a\tau_1\tau_2$
1 1 1	$bx_1x_2x_3$	$b\tau_1^{1-1}\tau_2^{1-1}\tau_3^1=b\tau_3$

Жадвалга асосан қуйидагини топамиз:

$$\varphi(x_1,\ x_2,\ x_3)=\tau_1^3+a\tau_1\tau_2+b\tau_3$$

ёки

$$x_1^3+x_2^3+x_3^3=(x_1+x_2+x_3)^3+a(x_1+x_2+x_3)\times$$
$$\times(x_1x_2+x_1x_3+x_2x_3)+bx_1\cdot x_2\cdot x_3. \quad (14)$$

Агар ўзгарувчиларга $x_1=x_2=1$, $x_3=0$ қийматлар берсак, (14) дан $2=8+2a$, $a=-3$ ҳосил бўлади. Сўнгра $x_1=x_2=x_3=1$ қийматларда (14) дан $a=-3$ эканини эътиборга олиб, $3=27-27+b$, $b=3$ ни топамиз. Демак,

$$\varphi_2(x_1,\ x_2,\ x_3)=\tau_1^3-3\tau_1\tau_2+3\tau_3$$

тенглик ҳосил бўлади. Шундай қилиб, берилган $f(x_1,$

---

* (13) айният бўлгани учун у ўзгарувчиларнинг ҳар қандай қийматларида ҳам ўринлидир.

x_2, x_3) симметрик кўпҳад асосий симметрик кўпҳадлар орқали ушбу кўринишда ифодаланади:

$$f(x_1, x_2, x_3) = \tau_1\tau_2\tau_3 - 3\tau_3^2 + \tau_1^3 - 3\tau_1\tau_2 + 3\tau_3.$$

65-§. Касрнинг махражидаги иррационалликни йўқотиш

Симметрик кўпҳадлар тушунчасидан келиб чиқадиган баъзи натижаларни кўриб ўтамиз.

1-натижа. Фараз қилайлик, $\mathscr{P}$ сонлар майдони устида бош коэффициенти 1 га тенг.

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n \qquad (1)$$

кўпҳад берилган бўлиб, $\alpha_1, \alpha_2, \ldots, \alpha_n$ унинг илдизлари бўлсин. У ҳолда $\mathscr{P}$ сонлар майдони устида берилган ҳар қандай n номаълумли $f(x_1, x_2, \ldots, x_n)$ кўпҳаднинг $x_i = \alpha_i$ $(i = \overline{1,n})$ даги $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ қиймати $\mathscr{P}$ сонлар майдонига тегишли бўлади.

Исботи. Симметрик кўпҳадлар ҳақидаги асосий теоремага кўра $f(x_1, x_2, \ldots, x_n) = \varphi(\tau_1, \tau_2, \ldots, \tau_n)$ бўлади. $\alpha_1, \alpha_2, \ldots, \alpha_n$ лар $f(x)$ кўпҳаднинг илдизлари бўлгани учун $f(x)$ ни

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \qquad (2)$$

кўринишда ёзиш мумкин*. (2) нинг ўнг томонини ҳадлаб кўпайтирсак,

$$f(x) = x^n - (\alpha_1 + \alpha_2 + \ldots + \alpha_n)x^{n-1} + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n)x^{n-2} - (\alpha_1\alpha_2\alpha_3 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n)x^{n-3} + \ldots + (-1)^n\alpha_1\alpha_2\cdots\alpha_n \qquad (3)$$

га эга бўламиз. (1) ва (3) нинг ўнг томонларини солиштириб, *Виет формулалари* деб аталувчи қуйидаги формулаларни ҳосил қиламиз:

$$\begin{aligned} &\alpha_1 + \alpha_2 + \ldots + \alpha_n = -a, \quad \tau_1 = -a_1; \\ &\alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n = a_2, \quad \tau_2 = a_2; \\ &\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n = -a_3, \quad \tau_3 = -a_3; \qquad (4) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\alpha_1\alpha_2\alpha_3 \cdot \ldots \cdot \alpha_n = (-1)^n a_n, \quad \tau_n = (-1)^n a_n \end{aligned}$$

---

* Агар бирор α_k илдиз m каррали бўлса, $x-\alpha_k$ кўпайтувчи (2) тенгликда m марта такрорланади.

(4) тенгликдаги асосий симметрик кўпҳадларнинг қийматларини $f(x_1, x_2, \ldots, x_n) = \varphi(\tau_1, \tau_2, \ldots, \tau_n)$ тенгликка қўйсак, $f(\alpha_1, \alpha_2, \ldots, \alpha_n) = \varphi(-a_1, a_2, \ldots, (-1)^n a_n)$ келиб чиқади. $f(x)$ ва $f(x_1, x_2, \ldots, x_n)$ кўпҳадларнинг коэффициентлари $\mathscr{P}$ сонлар майдонига тегишли бўлганлигидан

$$\varphi(-a_1, a_2, \ldots, (-1)^n a_n) = b \in \mathscr{P}.$$

2-натижа. Касрнинг махражидаги иррационалликни йўқотиш мумкин, яъни $\mathscr{P}$ сонлар майдони устида келтирилмайдиган n-даражали

$$(n \geqslant 2)\ P(x) = x^n + a_1x^{n-1} + a_1x^{n-2} + \ldots + a_{n-1}x + a_n$$

кўпҳад берилган бўлиб, $x = \alpha$ унинг илдизи бўлса, у ҳолда

$$\frac{f(\alpha)}{\psi(\alpha)} \quad (\psi)\alpha(\neq 0) \tag{5}$$

каср-рационал ифодани шундай ўзгартириш мумкинки, натижада унинг махражи бутун рационал ифодага айланади.

Исботи. Фараз қилайлик,

$$\frac{f(\alpha)}{\psi(\alpha)} = h(\alpha)$$

бўлсин. Ҳар қандай n-даражали кўпҳад комплекс сонлар майдони устида доимо n та илдизга эга бўлади. (Биз буни кейинроқ кўрсатамиз.) Шунинг учун $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ ни $P(x)$ кўпҳаднинг илдизлари деб оламиз. (5) ифоданинг сурат ва махражини $\psi(\alpha_2)\cdot\psi(\alpha_3)\cdots\psi(\alpha_n)$ га кўпайтириб,

$$\frac{f(\alpha)}{\psi(\alpha)} = \frac{f(\alpha_1)\,\psi(\alpha_2)\,\psi(\alpha_3)\cdots\psi(\alpha_n)}{\psi(\alpha_1)\,\psi(\alpha_2)\,\psi(\alpha_3)\cdots\psi(\alpha_n)}$$

ни ҳосил қиламиз. $\psi(x_1)\,\psi(x_2)\cdots\psi(x_n)$ кўпайтма $\mathscr{P}$ сонлар майдони устида $x_1, x_2, \ldots, x_n$ номаълумли симметрик кўпҳад бўлгани учун 1-натижага кўра $\psi(\alpha_1)\times\psi(\alpha_2)\cdots\psi(\alpha_n) = b$ бўлиб, бу ерда $b \in \mathscr{P}$ дир.

Демак,

$$\frac{f(\alpha)}{\psi(\alpha)} = \frac{1}{b}\, f(\alpha_1)\,\psi(\alpha_2)\,\psi(\alpha_3)\cdots\psi(\alpha_n)$$

бўлади.

Энди мақсад $\psi(\alpha_2)\psi(\sigma_3)\cdots\psi(\alpha_n)$ кўпайтмани α орқали ифодалашдан иборат. $\psi(\alpha_2)\,\psi(\alpha_3)\cdots\psi(\alpha_n)$ кўпайтма $\mathscr{P}$ сонлар майдони устида $n-1$ та $x_2, x_3, \ldots, x_n$ номаълумли симметрик кўпҳад бўлганидан, уни

$$\bar{\tau}_1 = x_2 + x_3 + \ldots + x_n,$$
$$\bar{\tau}_2 = x_2x_3 + x_2x_4 + \ldots + x_{n-1}x_n,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\bar{\tau}_n = x_2x_3x_4\cdots x_n$$

каби асосий симметрик кўпҳадлар орқали ифодалаймиз. Иккинчидан,

$$\bar{\tau}_1 = \tau_1 - x_1,$$
$$\bar{\tau}_2 = \tau_2 - x_1\bar{\tau}_1 = \tau_2 - \tau_1x_1 + x_1^2,$$
$$\bar{\tau}_3 = \tau_3 - x_1\bar{\tau}_2 = \tau_3 - \tau_2x_1 + \tau_1x_1^2 - x_1^3$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

га эгамиз. (4) тенгликлардан фойдаланиб, қуйидагиларни ҳосил қиламиз:

$$\bar{\tau}_1 = -a_1 - \alpha, \quad \bar{\tau}_2 = a_2 + a_1\alpha + \alpha^2,$$
$$\bar{\tau}_3 = -a_3 - a_2\alpha - a_1\alpha^2 - \alpha^2$$

ва ҳ. к. Умуман олганда, $\psi(\alpha_j)$ $(j=\overline{1,n})$ ларнинг барчаси $\alpha_1=\alpha$ ва $P(x)$ кўпҳаднинг коэффициентлари орқали ифодаланади, яъни $\psi(\alpha_2)\cdot\psi(\alpha_3)\cdots\psi(\alpha_n) = k(\alpha)$ десак,

$$\frac{f(\alpha)}{\psi(\alpha)} = \frac{1}{b}\,f(\alpha)\,k(\alpha$$

ҳосил бўлиб, (5) касрнинг махражидаги иррационаллик йўқолади.

66-§. Результант

Комплекс сонлар майдонида бир ўзгарувчили иккита кўпҳад берилган бўлсин:

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \quad (a_0 \neq 0),$$
$$\varphi(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m \quad (b_0 \neq 0).$$

Бу кўпҳадларнинг илдизларини, мос равишда, $\alpha_1, \alpha_2, \ldots, \alpha_n$ ва $\beta_1, \beta_2, \ldots, \beta_m$ билан белгилайлик.

1-таъриф. Ушбу

$$R(f;\ \varphi) = a_0^m\,\varphi(\alpha_1)\,\varphi(\alpha_2)\cdots\varphi(\alpha_n) \tag{1}$$

кўринишдаги ифода $f(x)$ ва $\varphi(x)$ кўпҳадларнинг *результанти* деб аталади.

Бу таърифга асосан, аксинча, $\varphi(x)$ ва $f(x)$ кўпҳадларнинг результанти

$$R(\varphi;\ f)=b^n f(\beta_1)f(\beta_2)\cdots f(\beta_m) \qquad (2)$$

кўринишга эга бўлади.

Энг аввал биз шуни кўрамизки, $f(x)$ ва $\varphi(x)$, шунингдек, $\varphi(x)$ ва $f(x)$ кўпҳадларнинг результанти сондан иборат, чунки (1) ва (2) лар сонларнинг кўпайтмаларидир.

1-теорема. *Ушбу тенглик ўринлидир*:

$$R(\varphi;\ f)=(-1)^{m\cdot n}R(f;\ \varphi). \qquad (3)$$

Исботи. $\varphi(x)=b_0(x-\beta_1)(x-\beta_2)\cdots(x-\beta_m)$ ифодада x нинг ўрнига кетма-кет $\alpha_1, \alpha_2, \ldots, \alpha_n$ ни қўйиб, қуйидагини ҳосил қиламиз:

$$\begin{gathered}
\varphi(\alpha_1)=b_0(\alpha_1-\beta_1)(\alpha_1-\beta_2)\cdots(\alpha_1-\beta_m),\\
\varphi(\alpha_2)=b_0(\alpha_2-\beta_1)(\alpha_2-\beta_2)\cdots(\alpha_2-\beta_m),\\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\\
\varphi(\alpha_n)=b_0(\alpha_n-\beta_1)(\alpha_n-\beta_2)\cdots(\alpha_n-\beta_m).
\end{gathered}$$

Бу қийматларни (1) га қўйсак:

$$\begin{aligned}
R(f;\ \varphi)=a_0^m b_0^n\prod_{j=1}^{m}(\alpha_1-\beta_j)\cdot\prod_{j=1}^{m}(\alpha_2-\beta_j)\cdots\\
\cdots\prod_{j=1}^{m}(\alpha_n-\beta_j) \qquad (4)
\end{aligned}$$

келиб чиқади. (4) да $\prod$ белги кўпайтма белгисидир.

Кўпайтма белгисидан фойдаланиб, (4) ифодани яна ҳам қисқароқ қуйидаги шаклда ёзиш мумкин:

$$R(f;\ \varphi)=a_0^m b_0^n\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j).$$

Кўпинча $\prod\limits_{i=1}^{n}\prod\limits_{j=1}^{m}$ белги ўрнига битта $\prod\limits_{\substack{i=\overline{1,n}\\ j=\overline{1,m}}}$ белгининг ёзилишини эътиборга олиб, сўнгги ифодани

$$R(f;\ \varphi)=a_0^m b_0^n\prod_{\substack{i=\overline{1.n}\\ j=\overline{1,m}}}(\alpha_i-\beta_j) \qquad (5)$$

кўринишга келтирамиз.

Худди шунга ўхшаш, $f(x)=a_0(x-\alpha_1)(x-\alpha_2)\cdots$ $\cdots(x-\alpha_n)$ да x нинг ўрнига навбат билан $\beta_1, \beta_2, \ldots$ $\ldots, \beta_m$ ни қўйиб ва (2) дан фойдалаииб,

$$R(\varphi;\ f)=a_0^m b_0^n \prod_{\substack{i=\overline{1,n}\\ j=\overline{1,m}}} (\beta_j-\alpha_i) \tag{6}$$

ифодани ҳосил қиламиз.

Энди (6) дан (3) тенгликка келамиз:

$$R(\varphi;\ f)=a_0^m b_0^n \prod_{\substack{i=\overline{1,n}\\ j=\overline{1,m}}} (\beta_j-\alpha_i)=$$

$$=(-1)^{mn}a_0^m b_0^n \prod_{\substack{i=\overline{1,n}\\ j=\overline{1,m}}} (\alpha_i-\beta_j)=(-1)^{mn}R(f;\ \varphi).$$

2-теорема. *$f(x)$ ва $\varphi(x)$ кўпҳадлар умумий илдизга эга бўлиши учун бу кўпҳадлар $R(f;\ \varphi)$ результантининг нолга тенг бўлиши зарур ва етарли.*

Исботи. I. Агар $f(x)$ ва $\varphi(x)$ кўпҳадлар умумий α_i илдизга эга бўлса, $\varphi(\alpha_i)=0$ тенгликка асосан,

$$R(f;\ \varphi)=a_0^m\varphi(\alpha_1)\varphi(\alpha_2)\cdots\varphi(\alpha_i)\cdots\varphi(\alpha_n)=0.$$

II. Аксинча, $R(f;\ \varphi)=a_0^m\varphi(\alpha_1)\cdots\varphi(\alpha_i)\cdots\varphi(\alpha_n)=0$ тенгликдан, $a_0^m\neq0$ бўлгани сабабли, қолган кўпайтувчиларнинг камида бири нолга тенг, яъни $\varphi(\alpha_i)=0$ деган натижага келамиз. Бу сўнгги тенглик эса камида битта α_i нинг $\varphi(x)$ учун ҳам илдиз эканини кўрсатади.

Мисоллар. 1. $f(x)=x^3-6x^2+11x-6,$
$\varphi(x)=x^3+6x^2+11x+6$

кўпҳадларнинг илдизлари, мос равишда, ±1; ±2; ±3. Бу кўпҳадларнинг $R(f;\ \varphi)$ результантини топайлик. Аввал $\varphi(1)=1+6+11+6=24$, $\varphi(2)=8+24+22+6=60$, $\varphi(3)=27+54+33+6=120$ қийматларни аниқлаб ва $a_0=1$ эканини эътиборга олиб, (1) га асосан, $R(f;\ \varphi)=$ $=24\cdot60\cdot120=137600$, $R(f;\ \varphi)=137600$ ни ҳосил қиламиз.

(3) тенгликка асосан $\varphi(x)$ ва $f(x)$ нинг результанти $R(\varphi;\ f)=(-1)^{3\cdot3}\cdot R(f;\varphi)=-137600$, $R(\varphi;f)=-137600$ ҳосил бўлади.

Бевосита ҳисоблаганимизда ҳам шунинг ўзини топамиз. Ҳақиқатан, $f(-1)=-1-6-11-6=-24$, $f(-2)=-8-24-22-6=-60$, $f(-3)=-27-54-$ $-33-6=-120$.

Энди $b_0=1$ бўлгани учун (2) га асосан $R=(\varphi;\ f)=$ $=(-24)(-60)(-120)=-137600$, $R(\varphi;\ f)=-137600$ бўлади.

2. $f(x)=x^2-3x+2$, $\varphi(x)=x^2+x-2$ кўпҳадларнинг илдизлари, мос равишда, 1; 2 ва 1; -2, $R(f;\ \varphi)$ ни ҳисоблаймиз. Бунда $\varphi\ (1)=0$ ва $\varphi(2)=4+2-2=4$, $\varphi(2)=4$. Демак, $R(f;\ \varphi)=0\cdot 4=0$, $R(f;\ \varphi)=0$, яъни результанти нолга тенг, чунки кўпҳадлар 1 дан иборат умумий илдизга эга.

Биз ҳозирга қадар результант тушунчасини берганимизда

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n,$$
$$\varphi(x)=b_0x^m+b_1x^{m-1}+\ldots+b_{m-1}x+b_m \tag{7}$$

кўпҳадларнинг бош коэффициентлари $a_0\neq 0$ ва $b=0$ бўлган ҳолни кўрдик. Чунки $f(x)$ ва $\varphi(x)$ нинг результанти, шунингдек, $\varphi(x)$ ва $f(x)$ нинг результанти ҳақида сўзлаганда биз учун бу кўпҳадлар нечта илдизга эга ва кўпҳадларнинг даражалари қандай бўлиши муҳим эди.

Энди $f(x)$ ва $\varphi(x)$ кўпҳадларнинг бош коэффициентлари қандай (нолдан фарқли ёки нолга тенг) бўлишини эътиборга олмай туриб, результантга таъриф берайлик.

2-таъриф. $f(x)$ ва $\varphi(x)$ кўпҳадларнинг $R(f;\ \varphi)$ *результанти* деб ушбу

$$R(f;\ \varphi)=\left|\begin{array}{llllll}
a_0 & a_1 & \cdots & a_n & & 0\\
0 & a_0 & \cdots & a_{n-1} & a_n & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot\\
0 & 0 & \cdots & a_0 & a_1\cdots & a_n\\
b_0 & b_1 & \cdots & b_m & & 0\\
0 & b_0 & \cdots & b_{m-1} & b_m & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot\\
0 & 0 & \cdots & b_0 & b_1\cdots & b_m
\end{array}\right|
\begin{array}{l}\left.\begin{array}{l}\\ \\ \\ \\ \end{array}\right\}m\\ \left.\begin{array}{l}\\ \\ \\ \\ \end{array}\right\}n\end{array}
\tag{8}$$

Сильвестер детерминантига айтилади.

Бу ҳолда $\varphi(x)$ ва $f(x)$ результанти

$$R(\varphi;\ f)=\begin{vmatrix} b_0 & b_1 & \cdots & b_m & 0 & & \\ 0 & b_0 & \cdots & b_{m-1} & b_m & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots b_0 & b_1 & b_2 & \cdots & b_m \\ a_0 & a_1 & \cdots & a_n & 0 & & \\ 0 & a_0 & \cdots & a_{m-1} & a_m & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots a_0 & a_1 & a_2 & \cdots & a_n \end{vmatrix}\begin{matrix}\left.\begin{matrix}\\ \\ \\ \\ \end{matrix}\right\}n\\ \left.\begin{matrix}\\ \\ \\ \\ \end{matrix}\right\}m\end{matrix} \tag{9}$$

кўринишда бўлади.

$a_0\neq0$ ва $b_0\neq0$ бўлган ҳолда, 2-таъриф 1-таърифга тенг кучлидир, чунки юқорида $a_0^m\varphi(\alpha_1)\varphi(\alpha_2)\cdots\varphi(\alpha_n)$ нинг (8) детерминантга тенглигини исботладик. Шунингдек, бу ҳолда $b_0^n f(\beta_1)f(\beta_2)\cdots f(\beta_n)$ худди (9) детерминантга тенг.

Результантнинг 2-таърифида ҳам

$$R(\varphi;\ f)=(-1)^{mn}R(f;\ \varphi)$$

тенглик ўринлидир.

Ҳақиқатан, (9) детерминантда $(n+1)$-сатрни биринчи ўринга, $(n+2)$-сатрни иккинчи ўринга, $(n+m)$-сатрни m-ўринга қўйсак, худди (8) детерминант ҳосил бўлади. Бунинг учун сатрларни иккитадан, ҳаммаси бўлиб, $m\cdot n$ марта ўзаро алмаштириш керак. Бундан $R(f;\ \varphi)$ ва $R(\varphi;\ f)$ детерминантлар бир-биридан $(-1)^{mn}$ кўпайтувчигагина фарқ қилиши аниқланади.

67-§. Системани номаълумларни йўқотиш усули билан ечиш

Бу параграфда системадан номаълумларни йўқотиш (чиқариш) назариясининг асосий татбиқи бўлган юқори даражали тенгламалар системасини ечиш билан шуғулланамиз. Биз $\mathscr{P}$ майдон устидаги иккита номаълумли иккита

$$f(x;\ y)=0,\ \varphi(x;\ y)=0 \tag{10}$$

алгебраик тенглама системасинигина текширамиз. Бундай системани ечиш қуйидаги теоремага асосланади.

1-теорема. *Агар* 66-§ *даги* (7) *кўпҳадларнинг* (8) *результанти нолга тенг бўлса,* (7) *кўпҳадлар* *умумий илдизга эга ёки уларнинг a_0 ва b_0 бош коэффициентлари нолга тенг ва аксинча, (7) кўпҳадлар умумий илдизга эга ёки уларнинг a_0 ва b_0 бош коэффициентлари нолга тенг бўлса, у ҳолда бу кўпҳадларнинг (8) результанти нолга тенг бўлади.*

Исботи. I. Фараз қилайлик, (8) результант нолга тенг бўлсин. Бу ҳол (8) детерминантнинг биринчи устунидаги ҳамма элементлари, демак, a_0 ва b_0 ҳам нолга тенг бўлганда юз бериши мумкин.

Агар коэффициентларнинг ақалли биттаси, аниқлик учун a_0 нолга тенг эмас десак, (8) результант учун (1) тенглик ўринли бўлиб,

$$R(f;\ \varphi) = a_0^m\varphi(\alpha_1)\varphi(\alpha_2)\cdots\varphi(\alpha_n)=0$$

бажарилади. Бундан, $a_0^m \neq 0$ бўлгани сабабли $\varphi(\alpha_n) = 0$ келиб чиқади, яъни α_i умумий илдиз бўлади.

II. Аксинча, $a_0 = b_0 = 0$ бўлса, (8) детерминантнинг нолга тенглиги равшан. Шу сабабли $f(x)$ ва $\varphi(x)$ кўпҳадлар α_i умумий илдизга эга бўлсин. Бу вақтда $a_0 = b_0 = 0$ бўлса, юқорида айтилганидек, (8) детерминант албатта нолга тенг бўлади. Агар a_0 ва b_0 нинг ақалли биттаси, масалан, a_0 нолдан фарқли десак,

$$R(f;\ \varphi) = a_0^m\varphi(\alpha_1)\varphi(\alpha_2)\cdots\varphi(\alpha_n)$$

ифода ўринли бўлиб, $\varphi(\alpha_i) = 0$ га асосан, $R(f;\ \varphi) = 0$ ни ҳосил қиламиз.

Энди (10) системага қайтайлик. $f(x;\ y)$ ва $\varphi(x;\ y)$ кўпҳадларни x нинг даражалари бўйича ёзиб, (10) системанинг чап томонларини

$$f(x;\ y) = F(x) = a_0(y)x^k + a_1(y)x^{k-1} + \cdots + \\ + a_{k-1}(y)x + a_k(y),\ (a_0(y) \neq 0) \qquad (11)$$

ва

$$\varphi(x;\ y) = \Phi(x) = b_0(y)x^l + b_1(y)x^{l-1} + \cdots + \\ + b_{l-1}(y)x + b_l(y),\quad (b_0(y) \neq 0)$$

кўринишга келтирамиз. $F(x)$ ва $\Phi(x)$ кўпҳадларнинг результантини Сильвестер детерминанти шаклида ёзамиз:

$$\psi(y)=\left|\begin{matrix} a_0(y) & a_1(y) & \cdots & a_{k-1}(y) & a_k(y) & 0 & \cdots & 0 \\ 0 & a_0(y) & \cdots & a_{k-2}(y) & a_{k-1}(y) & a_k(y) & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & a_0(y) & a_1(y) & & \cdots & a_k(y) \\ b_0(y) & b_1(x) & \cdots & b_{l-1}(y) & b_l(y) & 0 & \cdots & 0 \\ 0 & b_0(y) & \cdots & b_{l-2}(y) & b_{l-1}(y) & b_l(y) & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & b_0(x) & & \cdots & b_l(y) \end{matrix}\right| \begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} l \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} k \end{matrix} \qquad (12)$$

Равшанки, бу детерминант y га нисбатан $\mathscr{P}$ майдон устидаги кўпҳадни ифодалайди.

2-теорема. *Агар* (10) *система* $x=\alpha$ *ва* $y=\beta$ *ечимга эга бўлса,* $y=\beta$ *қиймат* $\psi(y)=0$ *тенглама учун илдиз бўлади. Аксинча,* $\psi(y)=0$ *тенгламанинг илдизи учун* $a_0(\beta)\neq 0$ *ва* $b_0(\beta)\neq 0$ *муносабатлардан ақалли биттаси бажарилса,* (10) *система* $k=\alpha$, $y=\beta$ *ечимга эга бўлади.*

Исботи. I. Фараз қилайлик, (10) система $x=\alpha$, $y=\beta$ ечимга эга бўлсин. Агар $y=\beta$ қийматни (11) кўпҳадларга қўйсак, x га нисбатан қуйидаги кўпҳадлар ҳосил бўлади:

$$f(x;\ \beta)=F(x)=a_0(\beta)x^k+a_1(\beta)x^{k-1}+\ldots+a_k(\beta),$$
$$\varphi(x;\ \beta)=\Phi(x)=b_0(\beta)x^l+b_1(\beta)x^{l-1}+\ldots+b_l(\beta). \qquad (13)$$

Бу кўпҳадларнинг результанти

$$\psi(\beta)=\left|\begin{matrix} a_0(\beta) & a_1(\beta) & \cdots & a_{k-1}(\beta) & a_k(\beta) & 0 & \cdots & 0 \\ 0 & a_0(\beta) & \cdots & a_{k-2}(\beta) & a_{k-1}(\beta) & a_k(\beta) & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & a_0(\beta) & a_1(\beta) & a_2(\beta) & \cdots & a_k(\beta) \\ b_0(\beta) & b_1(\beta) & \cdots & b_{l-1}(\beta) & b_l(\beta) & 0 & \cdots & 0 \\ 0 & b_0(\beta) & \cdots & b_{l-2}(\beta) & b_{l-1}(\beta) & b_l(\beta) & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 & 0 & b_0(\beta) & \cdots & b_l(\beta) \end{matrix}\right|$$

бўлади. Юқоридаги (13) кўпҳадлар умумий $x=\alpha$ илдизга эга бўлгани учун 1-теоремага асосан уларнинг результанти нолга тенг, яъни $\psi(\beta)=0$. Шундай қилиб, β сон $\varphi(y)=0$ тенглама учун илдиздир.

II. Аксинча, β сон $\psi(y)$ тенгламанинг илдизларидан бири бўлсин ва бу илдиз учун $a_0(\beta)\neq 0$ ва $b_0(\beta)\neq 0$ тенгсизликларнинг ақалли биттаси бажарилсин.

Шундай қилиб, $\psi(\beta)=0$ ёки, бошқача айтганда, (13) кўпҳадларнинг результанти нолга тенг. Демак, биринчи теоремага мувофиқ, (13) кўпҳадлар, яъни $f(x;\ \beta)$ ва $\varphi(x;\ \beta)$ умумий илдизга эга, яъни

$$f(\alpha;\ \beta)=0,\quad \varphi(\alpha;\ \beta)=0$$

бўлади. Бу эса (10) системанинг $x=\alpha$, $y=\beta$ ечими борлигини кўрсатади.

Агар $\psi(y)=0$ нинг $y=\beta$ илдизи учун $a_0(\beta)=0$ ва $b_0(\beta)=0$ бўлиб қолса, (10) система ечимга эга бўлиши ва, шунингдек, бўлмаслиги ҳам мумкин. Буни аниқлаш учун $a_0(\beta)=0$, $b_0(\beta)=0$ шартни қаноатлантирувчи ҳар бир β сонни алоҳида текшириб кўриш лозим.

Мисоллар. 1. Ушбу системани ечинг:

$$\begin{cases} x^2y+3xy+2y+3=0, \\ 2xy-2x+2y+3=0. \end{cases} \tag{14}$$

Ечиш. Иккала тенглама y га нисбатан биринчи даражали бўлгани учун системадан y ни чиқариб x га нисбатан битта тенгламага келиш қулайроқ. Шу мақсадда системани

$$\begin{cases} (x^2+3x+2)y+3=0, \\ (2x+2)y+(3-2x)=0 \end{cases} \tag{15}$$

кўринишда ёзиб,

$$\varphi(x)=\begin{vmatrix} x^2+3x+2 & 3 \\ 2x+2 & 3-2x \end{vmatrix}$$

результантни тузамиз. Бу детерминантни ҳисоблаб, қуйидаги тенгламани ҳосил қиламиз:

$$x(2x^2+3x+1)=0. \tag{16}$$

Бу тенгламанинг $x_1=0$ илдизи учун

$$a_0(0)=0^2+3\cdot0+2=2,\ a_0(0)=2,$$
$$b_0(0)=2\cdot0+2=2,\ b_0(0)=2$$

бўлади.

Шу сабабли, (15) дан $x_1=0$ қийматда ҳосил бўладиган

$$\begin{cases} 2y+3=0, \\ 2y+3=0 \end{cases}$$

система $y = -\frac{3}{2}$ умумий илдизга эга. Демак, (11) системанинг ечимларидан бири $x = 0$, $y = -\frac{3}{2}$ экан.

(16) тенгламанинг $x_2 = -1$ илдизи учун $a_0(-1) = 0$ ва $b_0(-1) = 0$ бўлади.

Демак, (15) дан $3 = 0$ ва $3 - 2x = 0$ ҳосил бўлиб, бу система умумий илдизга эга эмас (умуман $3 = 0$ мумкин бўлмаган тенглик).

Ниҳоят, (16) тенгламанинг $x_3 = -\frac{1}{2}$ илдизи учун $a_0\left(-\frac{1}{2}\right) = \frac{3}{4}$ ва $b_0\left(-\frac{1}{2}\right) = 1$. Демак, (15) дан $x = -\frac{1}{2}$ қийматда ҳосил бўладиган

$$\begin{cases} \frac{3}{4} y + 3 = 0, \\ y + 4 = 0 \end{cases}$$

система $y = -4$ умумий илдизга эга. Шундай қилиб, системанинг иккинчи ечими $x = -\frac{1}{2}$, $y = -4$ бўлади.

2. Ушбу системани ечинг:

$$\begin{cases} -xy + 2x + y - 2 = 0, \\ 2x^2y - 4x^2 - x + 1 = 0. \end{cases}$$

Ечиш. Бунинг учун системани

$$\begin{cases} (2 - y)x + (y - 2) = 0, \\ (2y - 4)x^2 - x + 1 = 0 \end{cases} \tag{17}$$

шаклда ёзиб, ушбу тенгламани тузамиз:

$$\psi(y) = \begin{vmatrix} 2 - y & y - 2 & 0 \\ 0 & 2 - y & y - 2 \\ 2y - 4 & -1 & 1 \end{vmatrix} =$$

$$= (y - 2)^2 \begin{vmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 2(y-2) & -1 & 1 \end{vmatrix} =$$

$$= (y - 2)^2 \begin{vmatrix} -1 & 1 & 1 \\ 0 & 0 & 1 \\ 2(y - 2) & 0 & 1 \end{vmatrix} =$$

$$= 2(y - 2)^3 = 0, \quad \psi(y) = 2(y - 2)^3 = 0.$$

$2(y-2)^3=0$ ни ечиб, $y=2$ илдизни топамиз. Бу $y=2$ қийматда $a_0(2)=0$ ва $b_0(2)=0$ бўлиб, (17) дан $\begin{cases}0=0,\\ -x+1=0\end{cases}$ бўлади. Бундан $x=1$ топилади. Демак, берилган система учун $x=1$, $y=2$ ечимдир.

68-§. Кўпҳад илдизининг мавжудлиги

Биз майдон тушунчаси билан китобнинг I қисмида танишган эдик. Бу параграфда эса майдон кенгайтмаси тўғрисида фикр юритамиз.

1-таъриф. $\mathscr{G}$ майдоннинг барча қисм майдонлари кесишмаси *минимал майдон* дейилади.

2-таъриф. Агар бирор $\mathscr{P}'$ тўплам $\mathscr{R}$ майдоннинг қисм майдони бўлса, $\mathscr{P}$ майдон $\mathscr{T}'$ майдоннинг *кенгайтмаси* дейилади.

Бирор кўпҳад $\mathscr{P}$ майдон устида илдизга эга бўлмаса, бу кўпҳаднинг кенгайтмаси бўлган $\overline{\mathscr{P}}$ устида илдизга эга бўладими? Оддий мисоллар билан иш кўрганда бу савол ижобий жавобга эга эканлигига ишонч ҳосил қилиш мумкин. Масалан, $f(x)=x^2-2$ кўпҳад рационал сонлар майдонида илдизга эга бўлмагани ҳолда, бу майдон учун кенгайтма ҳисобланган ҳақиқий сонлар майдонида илдизга эгадир. $f(x)=x^2+5$ кўпҳад эса ҳақиқий сонлар майдонида илдизга эга бўлмай, балки комплекс сонлар майдонида $x=\pm i\sqrt{5}$ илдизга эга бўлади.

Қуйидаги теорема ўринли.

1-теорема. *$\mathscr{R}$ майдон устида келтирилмайдиган ҳар қандай*

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n \qquad (n\geqslant 1)$$

кўпҳад учун $\mathscr{P}$ нинг шундай $\overline{\mathscr{P}}$ кенгайтмаси мавжудки, унда $f(x)$ кўпҳад илдизга эга ҳамда $\mathscr{P}$ майдонни ва $f(x)$ нинг бирор илдизини ўз ичига олган барча минимал майдонлар ўзаро изоморф бўлади.

Исботи. Даражаси $n\geqslant 2$ бўлган ва $\mathscr{P}$ майдон устида келтирилмайдиган $f(x)$ кўпҳад берилган бўлсин. Агар кўпҳад келтириладиган бўлса, уни келтирилмайдиган кўпҳадлар кўпайтмасига ёйиб, ихтиёрий кўпайтувчи кўпҳад илдизини оламиз. Бу илдиз $f(x)$ учун ҳам илдиз бўлишлиги ўз-ўзидан маълум.

$f(x)$ нинг бирор α илдизини ўз ичига олувчи ва $\mathscr{P}$ учун кенгайтма бўладиган $\mathscr{P}$ майдонни қуйидаги усулда қурамиз. Кўпҳадларнинг $\mathscr{P}[x]$ ҳалқасини олиб, бу ҳалқадаги барча кўпҳадларни $f(x)$ га бўлиб чиқамиз ва $\mathscr{P}[x]$ ҳалқани ҳосил бўлган қолдиқлар бўйича синфларга ажратамиз. Бошқача айтганда, $\varphi(x) \equiv \psi(x) \pmod{f(x)}$ шартни қаноатлантирувчи $\varphi(x)$ ва $\psi(x)$ ни битта синфга киритамиз. Бу синфларни A, B, $C, \ldots$ каби белгилаймиз. $\varphi_1(x) \in A$ ва $\psi_1(x) \in B$ элементларнинг йиғиндиси ва кўпайтмасини

$$\chi_1(x) = \varphi_1(x) + \psi_1(x), \quad \theta_1(x) = \varphi_1(x) \cdot \psi_1(x)$$

каби белгилайлик.

Энди A ва B синфларда мос равишда бошқа бирор $\varphi_2(x)$ ва $\psi_2(x)$ кўпҳадларни олиб, улар учун

$$\chi_2(x) = \varphi_2(x) + \psi_2(x), \quad \theta_2(x) = \varphi_2(x) \cdot \psi_2(x)$$

каби белгилайлик. Шарт бўйича

$$\varphi_1(x) \equiv \varphi_2(x) \pmod{f(x)}, \tag{1}$$

$$\psi_1(x) \equiv \psi_2(x) \pmod{f(x)} \tag{2}$$

бўлгани учун

$$\varphi_1(x) + \psi_1(x) \equiv \varphi_2(x) + \psi_2(x) \pmod{f(x)}$$

бўлади. Бу таққосламага асосан

$$\chi_1(x) \equiv \chi_2(x) \pmod{f(x)}. \tag{3}$$

Бошқача айтганда, $\chi_1(x) - \chi_2(x)$ ҳам $f(x)$ га қолдиқсиз бўлинади, яъни $\chi_1(x)$ ва $\chi_2(x_2)$ лар битта синфнинг элементлари бўлади. Худди шундай, (1) ва (2) ни ҳадлаб кўпайтирсак,

$$\varphi_1(x) \cdot \psi_1(x) \equiv \varphi_2(x) \psi_2(x) \pmod{f(x)}$$

ёки

$$\theta_1(x) \equiv \theta_2(x) \pmod{f(x)} \tag{4}$$

ҳосил бўлади. $\varphi_i(x)$ ва $\psi_i(x)$ $(i = 1, 2)$ лар A ва B синфларнинг ихтиёрий элементлари эди. (3) таққослама ёрдамида аниқланувчи $\chi_1(x)$ ва $\chi_2(x)$ лар A ва B синфларнинг ихтиёрий иккита элементи йиғиндиларидир. Бу йиғинди бирор C синфнинг элементи эканлиги аниқ. Шу синфни A ва B синфларнинг йиғиндиси деймиз ва уни $C = A + C$ каби белгилаймиз. (4) таққослама ёрдамида аниқланадиган синфни эса A ва B синфлар кўпайтмаси деб атаймиз ва уни $D = A \cdot B$ каби белгилаймиз.

Энди $A, B, C, \ldots$ синфлар тўпламининг майдон бўлишини кўрсатамиз.

Ҳақиқатан, $\mathscr{P}[x]$ ҳалқада кўпҳадларни қўшиш, учта кўпҳадни ўзаро кўпайтириш ва иккита кўпҳад йиғиндисини учинчи кўпҳадга кўпайтириш ассоциатив ва дистрибутив бўлганидан, бу хоссалар мазкур кўпҳадларга мос келувчи синфлар учун ҳам сақланади. Бундан ташқари,

$$\varphi(x) \cdot \psi(x) = \psi(x) \cdot \varphi(x)$$

бўлганидан синфлар ҳалқаси коммутативдир.

Қаралаётган халқанинг ноль элементи $k \cdot f(x) \equiv 0(\mathrm{mod}\, f(x))$ га мос келувчи синфдан, яъни $f(x)$ га қолдиқсиз бўлинадиган кўпҳадлар, кўпҳадлар тўпламидан иборат.

Ноль элемент одатда 0 каби белгиланади. $\varphi(x) = r(x)\,(\mathrm{mod}\, f(x))$ бўлиб, $\varphi(x) \in A$ бўлса, $-\varphi(x) \equiv -r(x)\,(\mathrm{mod}\, f(x))$ эканлигидан $-\varphi(x) \in A$ бўлади. Чунки, $\varphi(x + (-\varphi(x)) \equiv 0\,(\mathrm{mod}\, f(x))$ таққослама доимо ўринлидир. Шундай қилиб, $A, B, C, \ldots$ синфлар тўпламида айириш амали аниқланган ва у бир қийматлидир.

Энди $A, B, C, \ldots$ синфлар тўпламида бўлиш амали ўринли эканлигини кўрсатамиз. Бунинг учун унда бирлик элемент ва нолдан фарқли ҳар бир A синф учун $A \cdot B = E$ шартни қаноатлантирувчи B синф мавжудлигини кўрсатамиз. $f(x)$ га бўлганда қолдиқда 1 ҳосил бўладиган кўпҳадлар синфи берилган тўпламнинг бирлик элементи бўлади; уни E орқали белгилайлик.

A синф нолдан фарқли синф бўлсин. У ҳолда A синфдан олинган ихтиёрий $\varphi(x)$ кўпҳад $f(x)$ кўпҳадга қолдиқли бўлинади (бунда қолдиқ нолга тенг эмас). Лекин $f(x)$ кўпҳад келтирилмайдиган кўпҳад бўлгани учун $\varphi(x)$ ва $f(x)$ кўпҳадлар ўзаро туб бўлади. Бундан

$$\varphi(x)u(x) + f(x)v(x) = 1 \qquad (5)$$

шартни қаноатлантирувчи $u(x)$ ва $v(x)$ кўпҳадлар топилади. (5) тенгликни $\varphi(x)u(x) = 1 - f(x)v(x)$ кўринишда ёзиб олсак, ундан $f(x)$ модуль бўйича

$$\varphi(x)u(x) \equiv 1(\mathrm{mod}\, f(x)) \qquad (6)$$

таққослама ҳосил бўлади.

Агар $\varphi(x)$, $u(x)$ ва 1 га $f(x)$ модуль бўйича мос келувчи синфларни мос равишда A, B ва E деб белгиласак, (6) дан $A \cdot B = E$ тенглик ҳосил бўлиб, бундан $B = A^{-1}$ бўлади. Демак, биз қараётган A, B, $C, \ldots$ синфлар тўплами майдон бўлар экан. Бу майдонни $\overline{\mathscr{F}}$ орқали белгилайлик; у $\mathscr{F}$ майдоннинг кенгайтмасидан иборат бўлади. $\overline{\mathscr{F}}$ майдон $\mathscr{F}$ нинг кенгайтмаси эканлигини кўрсатиш учун $\mathscr{F}$ майдоннинг a элементига $f(x)$ га бўлганда ҳосил бўладиган қолдиқ a га тенг бўлган кўпҳадлар синфини мос қуямиз. Бу синфни $\mathscr{F}|a|$ орқали белгилаймиз. Ўз-ўзидан маълумки, a ҳам шу синф элементи бўлади. Бу ерда ҳар бир $a \in \mathscr{F}$ элементга $\mathscr{F}(a)$ га тегишли битта синф ва аксинча b қолдиққа мос келувчи ҳар бир $\mathscr{F}(b)$ синфга битта $b \in \mathscr{F}$ элемент мос келади, бошқача айтганда, $\mathscr{F} \cong \cong \mathscr{F}(t)$ $(t = a, b, \ldots)$ бўлади ва бу изоморфлик $\mathscr{F}(t)$ синфларини қўшиш ва кўпайтиришда ҳам сақланади, яъни $\mathscr{F}(t) \subseteq \overline{\mathscr{F}}$ бўлади.

Энди $\mathscr{F}[x]$ ҳалқа элементларидан $f(x)$ га бўлганда қолдиқда x ҳосил бўладиган кўпҳадлар тўпламини X деб белгилаймиз ва бу синф $(f)x$ кўпҳад учун илдиз эканлигини кўрсатамиз.

$a_i \in \mathscr{F}$ $(i = 0, 1, 2, \ldots)$ элементларга мос келувчи $\overline{\mathscr{F}}$ элементлари (синфлар)ни A_i деб белгилаймиз.

$$(X \subseteq \overline{\mathscr{F}}) \wedge) A_i \subseteq \overline{\mathscr{F}}) \Rightarrow$$

$$\Rightarrow (A_0X^n + A_1X^{n-1} + \ldots + A_{n-1}X + A_n \subseteq \overline{\mathscr{F}}).$$

A_i $(i = 0, 1, 2, \ldots)$ синфни X^k $(k = \overline{0,n})$ синфга кўпайтириш ёки A_iX^{n-i} синфни A_jX^{n-j} синфга қўшиш учун уларнинг тегишли вакилларини кўпайтириш ёки қўшиш кераклигини биз юқорида кўриб ўтган эдик.

$f(x)$ кўпҳад a_i ҳамда x^{n-i} лар кўпайтмасининг алгебраик йиғиндисидан иборат бўлгани учун бу кўпҳад

$$T = A_0X^n + A_1X^{n-1} + \ldots + A_{n-1}X + A_n$$

синфга тегишли бўлади. Лекин $f(x)/f(x)$ эди. Демак, T синфда A_i коэффициентларни $a_i \in \mathscr{F}$ лар билан алмаштирсак,

$$a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n = 0$$

бўлиб, X синф $f(x)$ кўпҳаднинг илдизидан иборат бўлади. Шундай қилиб, теореманинг биринчи қисми исбот этилди.

Энди теореманинг иккинчи қисмини исботлайлик. $\mathscr{P}$ майдон устида келтирилмайдиган $f(x)$ кўпҳад берилган бўлсин. У ҳолда теореманинг биринчи қисмига асосан $f(x)$ нинг бирор α илдизини ўз ичига олувчи $\overline{\mathscr{P}}$ кенгайтма майдон мавжуд бўлади. Бунда қуйидаги леммадан фойдаланамиз.

Лемма. *Агар α элемент $\mathscr{P}$ майдон устида келтирилмайдиган $f(x)$ ва $\mathscr{P}\,[x[$ ҳалқадан олинган бирор $g(x)$ кўпҳадларнинг илдизи бўлса, унда $g(x)/f(x)$ яъни $g(x)$ кўпҳад $f(x)$ га бўлинади.*

Ҳақиқатан, Безу теоремасига кўра $g(x)=(x-\alpha)g_1(x)$ эди. $g(x)$ ихтиёрий кўпҳад, $f(x)$ эса $\mathscr{P}$ майдон устида келтирилмайдиган кўпҳад бўлгани ва улар ўзаро туб бўлмагани учун $g(x)/f(x)$ бўлади.

Энди $\overline{\mathscr{P}}$ майдоннинг шундай минимал қисм майдонини излаймизки, у ўз ичига $\mathscr{P}$ майдонни ва α элементни олсин. Бу майдонни $\mathscr{F}\,(\alpha)$ орқали белгилайлик.

$\alpha \in \mathscr{P}\,(\alpha)$ бўлиб, $b_i \in \mathscr{P}$ $(i=\overline{0,\ n-1})$ бўлгани учун

$$\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} \in \mathscr{P}\,(\alpha) \qquad (7)$$

бўлади.

$\overline{\mathscr{F}}$ майдоннинг ҳар бир элементи учун (7) ёйилма ягонадир. Ҳақиқатан, агар тескарисини фараз қилсак, у ҳолда

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1}$$

тенглик бирорта k номер учун $c_k \neq \beta_k$ бўлганда ҳам ўринли бўлиши керак. Бундай ҳолда $x=\alpha$ элемент

$$g(x) = (b_0 - c_0) + (b_1 - c_1)x + (b_2 - c_2)x^2 + \ldots +$$
$$+ (b_{n-1} - c_{n-1})x^{n-1}$$

кўпҳаднинг илдизи бўлади. Бу эса $\text{дар}\, g(x) < \text{дар}\, f(x)$ бўлганлиги учун юқоридаги лемма шартига зиддир. Шунинг учун барча k $(k=\overline{0,\ n-1})$ лар учун $c_k = b_k$ экан.

Агар $b_1 = b_2 = \ldots = b_{n-1} = 0$ десак, $b_0 \in \mathscr{T}$ эканлигига асосан (7) дан $\mathscr{T}$ майдоннинг элементлари $b_0=0$, $b_1 = 0$, $b_2 = 0, \ldots, b_{n-1} = 0$ бўлганда α эламент ҳосил бўлади.

$\mathscr{P}(\alpha)$ нинг ҳақиқатан майдон эканлигини кўрсатиш учун унинг (7) ва

$$\gamma = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1} \qquad (8)$$

элементлари тўплами майдоннинг барча аксиомаларини қаноатлантиришини кўрсатишимиз керак.

Ҳақиқатан, $\overline{\mathscr{P}}$ майдондаги иккита синфни қўшишга асосан

$$\beta \pm \gamma = (b_0 \pm c_0) + (b_1 \pm c_1)\alpha + \ldots + (b_{n-1} \pm c_{n-1})\alpha^{n-1}$$

бўлиб, $\beta \pm \gamma \in \mathscr{P}(\alpha)$ бўлади. Иккинчидан, $\overline{\mathscr{P}}$ майдонда $f(\alpha)=0$ шартга асосан

$$0 = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n$$

ёки $a_0\alpha^n = -a_1\alpha^{n-1} - \ldots - a_{n-1}\alpha - a_n$ бўлиб, α^n, α^{n+1}, α^{n+2}, ... лар α нинг n дан кичик даражалари орқали ифодаланади. Бу тасдиққа асосан

$$\beta\cdot\gamma = d_0 + d_1\alpha + d_2\alpha^2 + \ldots + d_{n-1}\alpha^{n-1}$$

бўлиб, $\beta\cdot\gamma \in \mathscr{P}(\alpha)$ бўлади.

Энди $\mathscr{P}(\alpha)$ нинг ҳар бир $\beta \neq 0$ элементи тескари β^{-1} элементга эга эканлигини кўрсатамиз. Бунинг учун $\mathscr{P}[x]$ ҳалқадан олинган

$$\varphi(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1}$$

кўпҳад билан $\mathscr{P}$ да келтирилмайдиган $f(x)$ кўпҳадларни қараймиз. $f(x)$ кўпҳад келтирилмайдиган ва дар $f(x) >$ дар $\varphi(x)$ бўлгани учун $f(x)$ ва $\varphi(x)$ ўзаро тубдир. У ҳолда $\mathscr{P}[x]$ ҳалқада $\varphi(x)u(x)+f(x)v(x)=1$ тенгликни қаноатлантирувчи $u(x)$ ва $v(x)$ топилиб, дар $u(x) >$ дар $v(x)$ бўлади.

Бу тенгликда $x=\alpha$ десак, $f(\alpha)=0$ га асосан $\varphi(\alpha) \times u(\alpha)=1$ бўлади. Лекин, $\varphi(\alpha)=\beta$ эди. Шундай қилиб, $u(\alpha)=\beta^{-1}$ экан. Демак, $\beta^{-1} = u(\alpha) = s_0 + s_1(\alpha) + s_2\alpha^2 + \ldots + s_{n-1}\alpha^{n-1}$ кўринишга эга. Шундай қилиб, $\mathscr{P}(\alpha) \subset \overline{\mathscr{P}}$ экан.

1-эслатма. (7) ёки (8) кўринишдаги элементларни одатда *алгебраик элементлар* дейилади.

2-теорема. *Алгебраик сонлар тўплами майдон бўлади.*

Исботи. (7) ва (8) кўринишдаги γ ва β ни қўшиш ёки кўпайтириш учун улардаги α нинг коэффициентлари билангина иш кўрилишини биз биламиз. Демак, қуйидаги хулоса ўринли бўлади.

Агар $f(x)$ кўпҳаднинг бошқа бирор α' илдизини ва $\mathscr{P}$ ни ўз ичига олувчи $\overline{\mathscr{P}}'$ кенгайтма мавжуд бўлса ҳамда $\mathscr{P}(\alpha')$ майдон $\overline{\mathscr{P}}'$ нинг $\mathscr{P}$ ва α ларни ўз ичига олувчи минимал қисм майдони бўлса, у ҳолда $\mathscr{P}(\alpha) \cong \mathscr{P}(\alpha')$ бўлади.

Бу изоморфликни ўрнатиш учун $\beta \in \mathscr{P}(\alpha)$ нинг α бўйича бўлган ёйилмасидаги α нинг b_i $(i = \overline{0, n-1})$ коэффициентларига $\beta' \in \mathscr{P}(\alpha')$ нинг α' бўйича ёйилмасида шу b'_i коэффициентларни мос қўйиш кифоядир.

2-эслатма. Ҳар қандай $x-c$ шаклдаги чизиқли кўпайтувчи келтирилмайдиган бўлгани учун бу кўпайтувчи $f(x)$ кўпҳаднинг келтирилмайдиган кўпайтувчиларидан бири бўлади.

$\mathscr{P}$ майдонда келтирмайдиган кўпҳад $\overline{\mathscr{P}}$ да келтириладиган ва илдизга эга бўлганлиги учун у $\overline{\mathscr{P}}$ да чизиқли кўпайтувчилар кўпайтмасига ёйилиши мумкин. Агар $(x-c)^k$ чизиқли кўпайтувчини k та кўпайтувчи деб ҳисобласак, у ҳолда қуйидаги натижа ўринли:

1-натижа. Даражаси n га тенг бўлган кўпҳаднинг $\mathscr{P}$ майдондаги илдизлари сони n тадан ортиқ эмас.

3-таъриф Агар $\mathscr{P}$ майдоннинг шундай Q кенгайтмаси мавжуд бўлсаки, унда n-даражали $f(x)$ кўпҳад n та илдизга эга бўлса, Q майдон $f(x)$ кўпҳад учун ёйилма майдон дейилади.

Таърифга асосан n-даражали $f(x)$ кўпҳад Q майдонда n та чизиқли кўпайтувчи кўпайтмасига ёйилади. Демак, бундан сўнг Q ни ҳеч қандай усулда кенгайтириш мумкин бўлмайди, бошқача айтганда, $f(x)$ нинг янги илдизларини ўз ичига олувчи кенгайтмаси мавжуд эмас.

3-теорема. *$\mathscr{P}[x]$ ҳалқада берилган ҳар қандай n-даражали кўпҳад учун* ($n \geqslant 1$ бўлганда) *ёйилма майдон мавжуд.*

Исботи. Қуйидаги икки ҳол бўлади:

а) $f(x)$ кўпҳад $\mathscr{P}$ да n та илдизга эга. Бундай ҳолда $\mathscr{P}$ майдон кўпҳад учун ёйилма майдондир.

б) $f(x)$ кўпҳад $\mathscr{P}$ да чизиқли кўпайтувчилар кўпайтмасига ёйилмайди, яъни $f(x)$ кўпҳаднинг барча илдизлари $\mathscr{P}$ га тегишли эмас.

У ҳолда $f(x)$ ёйилмасининг $\mathscr{P}$ даги бирорта келтирилмайдиган $\varphi(x)$ кўпайтувчисини олиб, $\mathscr{P}$ нинг шундай $\mathscr{P}'$ кенгайтмасини тузамизки, унда $\varphi(x)$ кўпҳад илдизга эга бўлади. $\mathscr{P}'$ да $f(x)$ нинг бирорта келтирилмайдиган кўпайтувчисини олиб $\mathscr{P}'$ ни яна кенгайтирамиз. Илдизнинг мавжудлиги ҳақидаги теоремага асосан $\mathscr{P}$ нинг кенгайтмасида $f(x)$ илдизга эга бўлади. Бу жараённи давом эттириб, $\mathscr{P}'$ нинг шундай Q кенгайтмасини топамизки, бу кенгайтмада $f(x)$ кўпҳад чизиқли кўпҳадлар кўпайтмасига ёйилади. Бу Q майдон $f(x)$ учун ёйилма майдон бўлади.

VI боб. КОМПЛЕКС ВА ҲАҚИҚИЙ СОНЛАР МАЙДОНИ УСТИДА КЎПҲАДЛАР

69-§. Кўпҳад бош ҳадининг модули. Алгебранинг асосий теоремаси Кўпҳадни чизиқли кўпайтувчиларга ёйиш. Комплекс сонлар майдонининг алгебраик ёпиқлиги

Таъриф. Агар $\mathscr{P}$ майдон устида $\mathscr{P}[x]$ ҳалқадан олинган ихтиёрий мусбат даражали $p(x)$ кўпҳад камида битта илдизга эга бўлса, у ҳолда $\mathscr{P}$ *алгебраик ёпиқ майдон* дейилади.

1-лемма (Даламбер леммаси). *Комплекс сонлар майдони C устида мусбат даражали $f(x)$ кўпҳад берилган бўлиб, $a \in C$ учун $f(a) \neq 0$ бўлса, у ҳолда, шундай C комплекс сон топиладики, натижада $|f(c)| < |f(a)|$ тенгсизлик ўринли бўлади.*

2-лемма (Вейрштрасс леммаси). *$C(z)$ ҳалқадан олинган ихтиёрий $f(z)$ кўпҳаднинг модули C майдонда бирор z_0 нуқтада энг кичик қийматни қабул қилади.*

Бу леммаларни исботсиз келтирдик.

Теорема. *Комплекс сонлар майдони алгебраик ёпиқ майдон.*

Исботи. C майдонда $f(x)$ кўпҳаднинг модули x_0 нуқтада энг кичик қийматга эга бўлсин (2-леммага асосан бундай x_0 сон топилади). x_0 сон $f(x)$ кўпҳаднинг илдизи эканини кўрсатамиз.

Фараз қилайлик, x_0 сон $f(x)$ кўпҳаднинг илдизи бўлмасин. У ҳолда, $f(x_0) \neq 0$ бўлади. 1-леммага асосан шундай c комплекс сон мавжудки, $|f(c)| < |f(x_0)|$ тенгсизлик бажарилади. Бу тенгсизлик $|f x)|$ нинг энг кичик қийматга x_0 да эга деган фаразимизга зид. Демак, фаразимиз нотўғри, яъни x_0 сон $f(x)$ кўпҳаднинг илдизи экан,

Биз алгебранинг асосий теоремаси деб аталувчи теореманинг исботини ва унинг ҳар хил татбиқларини кўриб ўтамиз. Бунинг учун аввало қуйидаги кўпҳад бош ҳадининг модули ҳақидаги леммани кўриб ўтамиз.

3-лемма. *Коэффициентлари комплекс сонлар майдонидан олинган, даражаси 1 дан кичик бўлмаган*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \qquad (1)$$

кўпҳад ва ихтиёрий мусбат ҳақиқий k сон берилганда, модули етарлича катта бўлган x номаълум учун ушбу

$$|a_0x^n| > k|a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n| \qquad (2)$$

тенгсизлик ўринли бўлади.

Исботи. Фараз қилайлик, $A = \max(|a_1|, |a_2|, \ldots, |a_n|)$ бўлсин. Китобнинг биринчи қисмида

$$|a + b| \leqslant |a| + |b|, \ |a \cdot b| = |a| \cdot |b|, \ |a^n| = |a|^n$$

эканлигини кўрсатиб ўтган эдик. Шунга асосан қуйидагини ёза оламиз:

$$|a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n| \leqslant$$

$$\leqslant |a_1x^{n-1}| + |a_2\,x^{n-2}| + \ldots + |a_{n-1}x| + |a_n| =$$

$$= |a|_1|x|^{n-1} + |a_2||x|^{n-2} + \ldots + |a_{n-1}||x| + |a_n| \leqslant$$

$$A(|x|^{n-1} + |x|^{n-2} + \ldots + |x| + 1) = A\frac{|x|^n - 1}{|x| - 1}$$

$$(|x| \neq 1). \qquad (3)$$

Лемма шартига асосан $|x|$ ни етарлича катта деб олиш мумкин. Шунинг учун $|x| > 1$ деб фараз қилсак,

$$\frac{|x|^n - 1}{|x| - 1} < \frac{|x|^n}{|x| - 1} \qquad (4)$$

(3) ва (4) дан

$$|a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n| < A\frac{|x|^n}{|x| - 1} \qquad (5)$$

ни ҳосил қиламиз. (2) тенгсизлик ўринли бўлиши учун x номаълум $|x| > 1$ шарт билан биргаликда

$$k \cdot A\frac{|x|^n}{|x| - 1} \leqslant |a_0x^n| = |a_0| \cdot |x|^n$$

тенгсизликни қаноатлантириши керак. Бу тенгсизликни $|x|$ га нисбатан ечсак,

$$\left(k \cdot A\frac{|x|^n}{|x| - 1} \leqslant |a_0| \cdot |x|^n\right) \Rightarrow$$

$$\Rightarrow \left(k \cdot A\frac{1}{|x| - 1} \leqslant |a_0|\right) \Rightarrow \left(|x| \geqslant \frac{k \cdot A}{|a_0|} + 1\right) \qquad (6)$$

тенгсизлик ҳосил бўлади.

1-натижа. Ҳақиқий сонлар майдони устида берилган $f(x)$ кўпҳаднинг ишораси x нинг модули етарлича катта бўлганда бош ҳад ишораси билан бир хил булади.

Исботи. Фараз қилайлик, $f(x)$ кўпҳаднинг барча коэффициентлари ва x номаълумнинг қабул қиладиган қийматлари ҳақиқий сонлар бўлсин. Агар (2) тенгсизликда $k = 1$ десак, қуйидаги тенгсизлик ҳосил бўлади:

$$|a_0x^n| > |a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n|.$$

$$f|x| = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

ва охирги тенгсизликка асосан $f(x)$ нинг ишораси a_0x^n нинг ишораси билан бир хил бўлади.

2-натижа. Ҳақиқий сонлар майдони устида берилган ихтиёрий тоқ даражали кўпҳад камида битта ҳақиқий илдизга эга бўлади.

Исботи. $f(x)$ кўпҳадда a_0 коэффициентни доимо мусбат қилиб олиш мумкин. x нинг етарлича катта қийматларида $f(x)$ нинг ишораси a_0x^n нинг ишораси билан бир хил бўлишини биз юқорида кўриб ўтдик.

Демак, $x = -m$ (m—етарлича катта мусбат сон) да $f(-m)<0$ ва $f(m)>0$ бўлади. $f(x)$ кўпҳадни $(n+1)$ та узлуксиз функциянинг йиғиндиси деб қараш мумкин. У ҳолда математик анализда кўриб ўтилган узлуксиз функциялар ҳақидаги теоремаларга асосан $f(x)$ ҳам узлуксиз функция бўлади.

Иккинчидан, $[-m\ m]$ оралиқда узлуксиз бўлиб, $f(-m)<0$ ва $f(m)>0$ шартларни қаноатлантирувчи функциянинг шу оралиқда ноль қийматни қабул қилиши, яъни $f(c)=0$ шартни қаноатлантирувчи $x = c \in [-m; m]$ мавжудлиги ҳам бизга математик анализ курсидан маълум. Демак, $x = c$ сон $f(x)$ кўпҳаднинг илдизи экан.

Теорема (алгебранинг асосий теоремаси). Даражаси 1 дан кичик бўлмаган комплекс коэффициентли ҳар қандай кўпҳад камида битта комплекс илдизга эга.

Исботи. Биз юқорида тоқ даражали кўпҳад доимо илдизга эга эканлигини кўриб ўтдик. Шунинг учун теореманинг исботини жуфт даражали кўпҳадлар учун кўрсатамиз.

Фараз қилайлик, n-даражали $f(x)$ кўпҳад берилган бўлиб, унда $n=2^k\cdot m$ бўлсин (бу ерда $k\geqslant 1$ бўлиб, m— тоқ сон). Исботни k нинг индукцияси асосида олиб борамиз.

$m=1$ ва $k=0$ бўлса, ($n=1$) теорема тўғри. Энди теоремани $l=k-1$ учун ўринли деб фараз қиламиз.

Маълумки, ҳар қандай кўпҳад учун ёйилма майдон мавжуд эди. Шунга кўра бирор $\mathscr{F}$ майдонни $f(x)$ кўпҳад учун комплекс сонлар майдонидаги ёйилма майдон деб олайлик. $f(x)$ кўпҳад ёйилма майдонда n та α_i илдизларга эга бўлганидан $\alpha_i\in\mathscr{F}$ $(i=\overline{1, n})$ бўлади.

Энди $\mathscr{F}$ майдоннинг α_i ва $\alpha_j(i>j)$ элементлари ва ихтиёрий ҳақиқий c сондан фойдаланиб,

$$\beta_{ij}=\alpha_i\alpha_j+c(\alpha_i+\alpha_j) \tag{7}$$

кўринишда тузилган элементларни қараймиз. Ўз-ўзидан маълумки, $\beta_{ij}\in\mathscr{F}$ бўлиб, β_{ij} ларнинг сони n элементдан 2 тадан группалашлар сонига, яъни $\frac{n(n-1)}{2}$ га тенг.

Иккинчидан,

$$\frac{n(n-1)}{2}=\frac{2^k\cdot m(2^k\cdot m-1)}{2}=2^{k-1}\cdot m(2^k\cdot m-1)=$$
$$=2^{k-1}\cdot q' \tag{8}$$

Бу ерда m ва 2^km-1 лар тоқ сон бўлганидан $q'=$ $=m\cdot(2^km-1)$ ҳам тоқ сондир.

Энди илдизлари фақатгина β_{ij} элементлардан иборат бўлганда

$$g(x)=\prod_{i<j}^{\frac{n(n-1)}{2}}(x-\beta_{ij})$$

кўпҳадни тузиб оламиз. Бу кўпҳаднинг коэффициентлари β_{ij} лардан тузилган элементар симметрик кўпҳадлардан иборат бўлади. Агар β_{ij} ларни (7) билан алмаштирсак, $g(x)$ нинг коэффициентлари ҳам α_1, α_2, ..., α_n га боғлиқ бўлган симметрик кўпҳадлар бўлиб, бу симметрик кўпҳадларнинг коэффициентлари ҳақиқий сонлар бўлади.

У ҳолда 65-§ даги 1-натижага асосан $g(x)$ нинг коэффициентларининг ўзи ҳам ҳақиқий сонлар бўлади.

$g(x)$ кўпҳаднинг даражаси β_{ij} илдизлар сонига тенг бўлгани учун ва (8) га асосан бу даража 2^{k-1} га бўлиниб, лекин 2^k га бўлинмайди. Индуктив фаразимизга асосан теорема $l = k-1$ да ўринли, яъни $g(x)$ нинг $\beta_{ij}(i<j=\overline{1, n})$ илдизларидан камида биттаси комплекс сон эди.

Демак, $\beta_{ij} = \alpha_i\alpha_j + c(\alpha_i+\alpha_j)(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ элементлар учун шундай бир жуфтлик $(i_1;\ j_1)$ мавжуд эканки, бу жуфтликка мос келувчи $\beta_{i_1j_1}$ комплекс сон экан

Иккинчидан, $\mathscr{P}$ майдон комплекс сонлар майдони учун кенгайтма майдон эди. Агар $c \neq c_1$ ҳақиқий сонни оладиган бўлсак, c_1 га мос келувчи комплекс сон мавжуд бўлади ва унга мос келувчи $(i_2;\ j_2)$ жуфтлик ҳам $(i_1;\ j_1)$ билан бир хил бўлмайди. Бизнинг имкониятимизда $\frac{n(n-1)}{2}$ та $(i;\ j)$ жуфтликлар мавжуд. Ҳақиқий сонлар эса чексиз кўп. Демак, шундай ўзаро ҳар хил $c_1 \neq c_2$ ҳақиқий сонлар мавжудки, буларга бир хил $(i;\ j)$ жуфтликлар мос келади, яъни

$$\begin{cases} \alpha_i\alpha_j + c_1(\alpha_i + \alpha_j) = a, \\ \alpha_i\alpha_j + c_2(\alpha_i + \alpha_j) = b \end{cases} \qquad (9)$$

бўлиб, a ва b комплекс сонлардир. (9) системадан

$$(c_1 - c_2)(\alpha_i + \alpha_j) = a - b$$

ҳосил бўлиб, бундан эса $\alpha_i + \alpha_j = \frac{a-b}{c_1-c_2}$ келиб чиқади.

Демак, $\alpha_i+\alpha_j$ йиғинди ва $\alpha_i \cdot \alpha_j$ кўпайтма ҳам комплекс сонлар экан.

Виет теоремасига асосан α_i, α_j лар

$$x^2 - (\alpha_i + \alpha_j)x + \alpha_i\alpha_j = 0$$

квадрат тенгламанинг илдизлари бўлади. Коэффициентлари комплекс сонлардан иборат бўлган квадрат тенглама илдизи ҳам комплекс сон эканлигини биз китобнинг I қисмида кўриб ўтган эдик. Шундай қилиб, $f(x)$ кўпҳаднинг илдизларидан ҳатто иккитаси комплекс сон эканлигини исбот қилдик. Шу билан теорема тўла исбот этилди.

Энди қуйида алгебра асосий теоремасининг баъзи бир натижаларини кўриб ўтайлик.

1-натижа. Комплекс сонлар майдонидаги n-даражали кўпҳаднинг n та илдизи мавжуд.

Исботи. 4-теоремага асосан $f(x)$ нинг ақалли битта комплекс илдизи мавжуд, Безу теоремасига кўра $f(x)$ кўпҳад $x-\alpha_1$ га бўлинади, яъни

$$f(x)=(x-\alpha_1)f(x_1) \tag{10}$$

тенглик ўринли.

$(n-1)$-даражали $f_1(x)$ кўпҳадга нисбатан юқоридаги мулоҳазани қўллаб,

$$f_1(x)=(x-\alpha_2)f_2(x) \tag{11}$$

тенгликни ҳосил қиламиз, бунда $f_2(x)$ кўпҳад $(n-2)$-даражалидир ва ҳоказо, бу жараённи давом эттириб, ниҳоят, биринчи даражали $f_{n-1}(x)$ кўпҳадга келамиз ва

$$f_{n-1}(x)=(x-\alpha_n)r_0 \tag{12}$$

тенгликка эга бўламиз, бунда r_0—ўзгармас сон.

Ҳосил бўлган (10), (11), (12) ва ҳоказо тенгликлардан

$$f(x)=r_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \tag{13}$$

ёйилмага келамиз. Бу (13) ифодага қараб. $\alpha_1, \alpha_2, \ldots, \alpha_n$ сонлар $f(x)$ кўпҳаднинг илдизлари эканини кўрамиз, чунки $\alpha_i(i=\overline{1, n})$ ни x нинг ўрнига қўйсак, $f(\alpha_i)=0$ келиб чиқади.

(13) ёйилмадаги $x-\alpha_i$ иккиҳадлар биринчи даражали ва улар келтирилмайдиган кўпҳадлар бўлгани учун $f(x)$ ни келтирилмайдиган кўпҳадлар кўпайтмасига ёйиш ҳақидаги теоремага биноан бу $x-\alpha_i$ иккиҳадлар ўзгармас кўпайтувчилар аниқлигида ягонадир. Бу ҳол эса $f(x)$ кўпҳаднинг $\alpha_1, \alpha_2, \ldots, \alpha_n$ дан бошқа илдизлари йўқлигини билдиради.

(13) ёйилмадаги $x-\alpha_i$ иккиҳадларни бир-бирига ва r_0 га кўпайтириб чиқсак, ҳосил бўлган кўпҳаднинг бош коэффициенти r_0 га тенглигини кўрамиз. Лекин бу кўпҳад $f(x)$ нинг ўзгинаси бўлгани учун $r_0=a_0$ деган натижага келамиз, бунда a_0 орқали $f(x)$ нинг бош коэффициентини белгиладик. Шундай қилиб, (13) тенглик қуйидагича ёзилади:

$$f(x)=a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n). \tag{14}$$

Бу ёйилма $f(x)$ кўпҳаднинг чизиқли (биринчи даражали) кўпайтувчиларга ёйилмаси дейилади.

Умуман, илдизларнинг баъзилари ўзаро тенг бўлиши ҳам мумкин. Шу сабабли, ҳар хил илдизларни α_1, α_2,

. . . , α_k билан белгилаб (14) тенгликни ушбу кўринишда ёза оламиз:

$$f(x)=a_0(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\dots(x-\alpha_k)^{m_k},$$

бунда $m_1+m_2+\dots+m_k=n$, $m_1, m_2, \dots, m_k$ бутун мусбат сонлар мос равишда $\alpha_1, \alpha_2, \dots, \alpha_k$ илдизларнинг *карралик белгилари* дейилади. Бошқача айтганда α_1 ни m_1 каррали илдиз деб атаймиз. Демак, n-даражали $f(x)$ кўпҳаднинг илдизлари бир каррали, икки каррали ва ҳоказо k каррали бўлиши мумкин. Шундай қилиб, комплекс сонлар майдони устидаги даражаси бирдан юқори ҳар бир $f(x)$ кўпҳад бу майдон устида келтириладигандир.

Ҳақиқатан, α_i бундай кўпҳаднинг исталган илдизи бўлса. $f(x)$ ни $x-\alpha_i$ га бўлиб, қуйидагини ҳосил қиламиз:

$$f(x)=(x-\alpha_i)\varphi(x).$$

Бу кўпайтма айтганимизни тасдиқлайди.

2-натижа. n-даражали $f(x)$ кўпҳад x нинг n тадан ортиқ ҳар хил қийматларида нолга тенг бўлса, $f(x)$ ноль кўпҳад бўлади.

Исботи. n-даражали

$$f(x)=a_0x^n+a_1x^{n-1}+\dots+a^{n-1}x+a_n$$

кўпҳад x нинг қуйидаги m та ($m>n$) ҳар хил

$$\alpha_1, \alpha_2, \dots, \alpha_n, \alpha^{n+1}, \dots, \alpha_m \tag{15}$$

қийматларида нолга тенг деб фараз қилайлик. У ҳолда бу сонлардан, масалан, дастлабки n таси $f(x)$ нинг илдизлари бўлиб, (13) тенглик ўринлидир:

$$f(x)=a_0(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n).$$

Берилгани бўйича, $f(\alpha_i)=0$, яъни

$$a_0(\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\dots(\alpha_i-\alpha_n)=0$$

бўлади. Бунда α_i қолган $\alpha_{n+1}, \alpha_{n+2}, \dots, \alpha_m$ сонлардан исталганини ифодалайди.

Энди $\alpha_i-\alpha_k\neq0$ ($k=1, 2, \dots, n$) бўлгани учун $a_0=0$ деган натижага келамиз. Демак, кўпҳад қуйидаги кўринишни олади:

$$f(x)=a_1x^{n-1}+a_2x^{n-2}+\dots+a_{n-1}x+a_n.$$

Бу кўпҳад ҳам n дан кичик даражали бўлиб, x нинг (15) қийматларида нолга айланади ва, шу сабабли, юқоридаги мулоҳазани такрорлаб, $a_1 = 0$ эканини топамиз ва ҳоказо бу жараённи охиригача давом эттириб, $f(x) = a_n$ га келамиз. Шарт бўйича $f(a_i) = a_n = 0$. Демак, $a_0 = a_1 = \ldots = a_{n-1} = a_n = 0$ бўлгани учун $f(x) = 0$ экан.

3-натижа. Даражалари n дан юқори бўлмаган $f(x)$ ва $\varphi(x)$ кўпҳадлар x нинг n тадан ортиқ ҳар хил қийматларида бир-бирига тенг бўлса, $f(x)$ ва $\varphi(x)$ ўзаро тенг кўпҳадлар бўлади.

Исботи. Даражаси n дан юқори бўлмаган $g(x) = f(x) - \varphi(x)$ кўпҳад x нинг n тадан ортиқ ҳар хил қийматларида нолга айланади. Демак, юқоридаги теоремага биноан, $g(x) = f(x) - \varphi(x) = 0$ ёки $f(x) = \varphi(x)$ бўлади.

70-§ Ҳақиқий сонлар майдони устида келтирилмайдиган кўпҳадлар. Ҳақиқий коэффициентли кўпҳад мавҳум илдизининг қўшмалилиги

1-теорема. *Ҳақиқий сонлар майдони устидаги $f(x)$ кўпҳад x нинг қўшма комплекс қийматларида қўшма комплекс қийматларни қабул қилади.*

Исботи. a ҳақиқий сонни оламиз ва Тейлор формуласига асосан $f(a+h)$ ни h нинг даражалари бўйича қуйидагича ёямиз:

$$f(a+h) = f(a) + f'(a)h + \frac{f''(a)}{2!}h^2 + \ldots + \frac{f^n(a)}{n!}h^n.$$

Бу ёйилманинг коэффициентлари ҳақиқий сонлар бўлиб, биз уларни ушбу кўринишда белгилайлик:

$$f(a) = A_0,\ f'(a) = A_1, \frac{f''(a)}{2!} = A_2, \ldots, \frac{f^n(a)}{n!} = A_h.$$

У ҳолда юқоридаги ёйилма

$$f(a+h) = A_0 + A_1h + A_2h^2 + \ldots + A_nh^n$$

кўринишни олади. Агар ўз ичига h нинг жуфт ва тоқ даражаларини олган ҳадларни айрим-айрим гуруҳларга ажратсак,

$$f(a+h) = (A_0 + A_2h^2 + A_4h^4 + \ldots) + \\ + (A_1 + A_3h^2 + A_5h^4 + \ldots)h \qquad (1)$$

тенглик ҳосил бўлади. Энди бу тенгликка $h = bi$ (b— ҳақиқий сон) қийматни қўйиб қуйидагини ҳосил қиламиз:

$$f(a+bi) = (A_0 - A_2b^2 + A_4b^4 - \dots) + \\ + (A_1 - A_3b^2 + A_5b^4 - \dots)bi$$

ёки

$$f(a+bi) = M + Ni,$$

бунда $M = A_0 - A_2b^2 + A_4b^4 - \dots$ ва $N = b(A_1 - A_3b^2 + A_5b^4 - \dots)$ ҳақиқий сонлар.

Агар (1) тенгликка $h = -bi$ қийматни қўйсак,

$$f(a-bi) = (A_0 - A_2b^2 + A_4b^4 - \dots) - \\ - bi(A_1 - A_3b^2 + A_5b^4 - \dots)$$

ёки $f(a-bi) = M - Ni$ тенглик келиб чиқади.

Шундай қилиб, x нинг $a+bi$ ва $a-bi$ қийматларида $f(x)$ кўпҳад $M+Ni$ ва $M-Ni$ қийматларни қабул қилади.

1-натижа. Ҳақиқий сонлар майдони устидаги $f(x)$ кўпҳад учун $a+bi$ комплекс сон илдиз бўлса, у ҳолда унга қўшма $a-bi$ ($b \neq 0$) комплекс сон ҳам илдиз бўлади.

Исботи. $a+bi$ комплекс сон $f(x)$ нинг илдизи бўлгани учун $f(a+bi) = M+Ni = 0$, $M+Ni = 0$. Демак, $M = N = 0$. Шунинг учун $f(a-bi) = M - Ni = 0 - 0i = 0, f(a-bi) = 0$. Бу эса $a-bi$ сон $f(x)$ нинг илдизи эканини кўрсатади.

2-натижа. Ҳақиқий сонлар майдони устидаги $f(x)$ кўпҳаднинг мавҳум* илдизлари сони жуфт бўлади.

Ҳақиқатан, 1-натижага биноан, ҳар бир $a+bi$ комплекс илдиз учун яна $a-bi$ илдиз мавжуд.

3-натижа. Ҳақиқий сонлар майдони устида жуфт даражали $f(x)$ кўпҳаднинг ҳақиқий илдизлари сони жуфт бўлади.

Ҳақиқатан, $f(x)$ нинг даражасини n ва мавҳум илдизларнинг сонини m десак, ҳақиқий илдизларнинг сони $k = n - m$ бўлади. n ва m жуфт сонларни ифодалагани учун k ҳам жуфт сондир. Бу m ва k сонлардан биттаси 0 га тенг бўлиши, яъни $f(x)$ нинг ё мавҳум, ёки ҳақиқий илдизлари бўлмаслиги мумкин.

---

*Мавҳум илдиз деб $b \neq 0$ шартни қаноатлантирувчи $a+bi$ илдизни тушунамиз.

4-натижа. Ҳақиқий сонлар майдони устида тоқ даражали $f(x)$ кўпҳаднинг ҳақиқий илдизлари сони тоқ бўлади.

Ҳақиқатан, n тоқ ва m жуфт бўлса, $k = n - m$ тоқ бўлади. Шундай қилиб, $f(x)$ нинг энг камида битта илдизи ҳақиқий бўлади. $m = 0$ бўлса, унинг ҳамма илдизлари ҳақиқий бўлади.

5-натижа. Ҳақиқий сонлар майдони устидаги ҳар бир $f(x)$ кўпҳадни шу майдон устидаги биринчи ва иккинчи даражали келтирилмайдиган кўпҳадлар кўпайтмасига ёйиш мумкин.

Ҳақиқатан, $f(x)$ нинг илдизларини $\alpha_1, \alpha_2, \ldots, \alpha_n$ десак,

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

ёйилма ҳосил бўлади, бунда a_0 — ҳақиқий сон. Агар α_1 ҳақиқий илдиз бўлса, $x - \alpha_1$ ҳакиқий сонлар майдони устидаги биринчи даражали (демак келтирилмайдиган) кўпҳадни ифодалайди. Агар $\alpha_2 = a + bi$ комплекс илдизни билдирса, $f(x)$ нинг илдизларидан биттаси $a - bi$ қўшма комплекс сондан иборат бўлада. Айтайлик $\alpha_3 = a - bi$ бўлсин. У ҳолда ҳақиқий сонлар майдони устидаги иккинчи даражали келтирилмайдиган

$$(x - \alpha_2)(x - \alpha_3) = (x - a - bi)(x - a + bi) =$$
$$= (x - a)^2 + b^2 = x^2 - 2ax + a^2 + b^2$$

кўпҳадни ҳосил қиламиз.

Демак, $f(x)$ кўпҳад ҳақиқий сонлар майдони устидаги биринчи ва иккинчи даражали келтирилмайдиган кўпҳадлар кўпайтмасига ёйилади. Кўпҳад ҳақиқий (ёки мавҳум) илдизларга эга бўлмаса, бу ёйилмада биринчи (ёки иккинчи) даражали келтирилмайдиган кўпайтувчилар бўлмайди.

Хулоса. Ҳақиқий сонлар майдони устида иккинчидан юқори даражали ҳар бир $f(x)$ кўпҳад шу майдон устида келтириладиган кўпҳаддир. Ҳақиқатан, юқорида айтилган ёйилмани ҳақиқий сонлар майдони устидаги ва даражалари $f(x)$ нинг даражасидан кичик иккита кўпҳад кўпайтмасига келтириш мумкин.

Масалан, $f(x) = x^4 + 1$ кўпҳадни олайлик. У ҳолда

$$x = \sqrt[4]{-1} = \sqrt[4]{\cos\pi + i\sin\pi} = \cos\frac{2k+1}{4}\pi + i\sin\frac{2k+1}{4}\pi$$

бўлиб, унинг илдизлари қуйидагилар бўлади:

$$\alpha_1 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2};$$

$$\alpha_2 = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2};$$

$$\alpha_3 = \cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = -\frac{\sqrt{2}}{3} - i\frac{\sqrt{2}}{2};$$

$$\alpha_4 = \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}.$$

Шу сабабли $f(x) = (x-\alpha_1)\ (x-\alpha_2)\ (x-\alpha_3)\ (x-\alpha_4)$ бўлади.

Бунда

$$(x-\alpha_1)\ (x-\alpha_4) = \left(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\times$$
$$\times\left(x - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = x^2 - \sqrt{2}\,x + 1,$$

$$(x-\alpha_2)\ (x-\alpha_3) = \left(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\left(x + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) =$$
$$= x^2 + \sqrt{2}x + 1.$$

Шундай қилиб, қуйидагини ҳосил қиламиз:

$$f(x) = x^4 + 1 = \left(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\cdot\left(x - \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)\times$$
$$\times\left(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\right)\left(x + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) =$$
$$= (x^2 - \sqrt{2}\,x + 1)\,(x^2 + \sqrt{2}x + 1)$$

71-§. Учинчи даражали тенглама

Комплекс сонлар майдони устидаги ушбу

$$ax^3 + bx^2 + cx + d = 0\ (a \neq 0) \qquad (1)$$

кўринишдаги тенглама учинчи даражали бир номаълумли тенглама дейилади. (1) тенгламанинг ҳар икки томонини a га бўлиб, ушбу тенгламага эга бўламиз:

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0. \qquad (2)$$

(2) да $x = y - \frac{3b}{a}$ алмаштиришни киритиб,

$$\left(y - \frac{3b}{a}\right)^3 + \frac{b}{a}\left(y - \frac{3b}{a}\right)^2 + \frac{c}{a}\left(y - \frac{3b}{a}\right) + \frac{d}{a} = 0 \qquad (3)$$

тенгламани ҳосил қиламиз. (3) тенгламани соддалаштиргандан кейин

$$y^3+py+q=0 \tag{4}$$

кўринишдаги тенгламага эга бўламиз. (4) тенгламадаги y ўзгарувчи ўрнига иккита u ва v ўзгарувчини $y=u+v$ тенглик ёрдамида киритамиз.

Натижада $(u+v)^3+p(u+v)+q=0$ ёки

$$u^3+v^3+q+(3uv+p)\cdot(u+v)=0 \tag{5}$$

тенгламага эга бўламиз. (5) да u ва v ни шундай танлайликки, натижада

$$3uv+p=0 \tag{6}$$

шарт бажарилсин. Бундай талаб қўйишимиз ўринли, чунки

$$\begin{cases} u+v=y, \\ uv=-\dfrac{p}{3} \end{cases}$$

тенгламалар системаси y берилганда ягона ечимга эга бўлади. (6) шартни эътиборга олсак, (5) тенглама қуйидаги кўринишда бўлади:

$$u^3+v^3=-q. \tag{7}$$

(6) дан $u^3v^3=-\frac{p^3}{27}$ бўлгани учун u^3 ва v^3 Виет теоремасига асосан бирор $z^2+qz-\frac{p^3}{27}=0$ кўринишдаги квадрат тенгламанинг илдизлари бўлади. Бу квадрат тенгламани ечишдан

$$z_1=u^3=-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}},\quad z_2=v^3= \\ =-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}} \tag{8}$$

ни ҳосил қиламиз (8) дан

$$u=\sqrt{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},\quad v=\sqrt{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$$

топилиб, u ва v нинг ҳар бирига учта қиймат, y ўзгарувчи учун эса тўққизта қиймат топилади. Улардан

(6) шартни қаноатлантирганларини оламиз. У ҳолда (4) тенгламанинг барча ечимлари топилади.

Агар u, $u\varepsilon$, $u\varepsilon^2$ (бунда ε сон 1 дан чиқарилган илдиз, яъни $\varepsilon^3=1$) z_1 нинг учинчи даражали илдизларининг қийматлари бўлса, унга мос z_2 нинг учинчи даражали илдизлари қийматлари v^2, $v\varepsilon^2$, $v\varepsilon$ бўлади. Натижада (4) тенглама ушбу

$$y_1 = u + v,\ y_2 = u\varepsilon + v\varepsilon^2,\ y_3 = u\varepsilon^2 + v\varepsilon \tag{9}$$

илдизларга эга бўлиб, унда $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ бўлганидан

$$y_1 = u + v,\ y_2 = -\frac{1}{2}(u+v) + i\frac{\sqrt{3}}{2}(u-v),$$

$$y_3 = -\frac{1}{2}(u+v) - i\frac{\sqrt{3}}{2}(u-v) \tag{10}$$

ечим ҳосил бўлади.

(10) ва $x = y - \frac{3b}{a}$ ни эътиборга олиб, (1) тенгламанинг $x_1 = y_1 - \frac{3b}{a}$, $x_2 = y_2 - \frac{3b}{a}$ ва $x_2 = y_3 - \frac{3b}{a}$ илдизлари топилади.

Энди ҳақиқий коэффициентли учинчи даражали тенглама илдизларини текширайлик.

Қуйидаги теорема учинчи даражали тенгламанинг ҳақиқий ва мавҳум илдизлари сонини аниқлайди.

Теорема. *Агар*

$$x^2 + px + q = 0 \tag{11}$$

тенглама ҳақиқий коэффициентли тенглама бўлиб, $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$ *бўлса, у ҳолда қуйидаги мулоҳазалар ўринли бўлади:*

а) *агар* $\Delta > 0$ *бўлса,* (11) *тенглама битта ҳақиқий ва иккита ўзаро қўшма мавҳум илдизларга эга бўлади;*

б) *агар* $\Delta = 0$ *бўлса,* (11) *тенгламанинг барча илдизлари ҳақиқий ва камида битта илдизи каррали бўлади;*

с) *агар* $\Delta < 0$ *бўлса,* (11) *тенгламанинг барча илдизлари ҳақиқий ва турлича бўлади.*

Исботи. а) $\Delta > 0$ бўлса, у ҳолда z_1 ва z_2 илдизлар ҳақиқий ва ҳар хил бўлади. Демак, илдизлардан камида биттаси, масалан z_1, нолдан фарқли бўлади. $u=\sqrt[3]{z_1}$ сон z_1 нинг арифметик илдизи бўлсин. Шунинг учун u ҳақиқий сон бўлади. $uv=-\frac{p}{3}$ тенгликка асосан, v ҳам ҳақиқий сон бўлади $z_1\neq z_2$ бўлгани учун $u^3\neq v^3$ бўлади. Бундан $u\neq v$ муносабат ўринли эканлиги равшан. (10) га асосан эса

$$x_1=u+v,\quad x_2=-\frac{1}{2}(u+v)+i\frac{\sqrt{3}}{2}(u-v),\quad x_3= =-\frac{1}{2}(u+v)-i\frac{\sqrt{3}}{2}(u-v) \qquad (12)$$

бўлиб, u ва v ҳақиқий ҳамда турли сонлар бўлгани учун (12) да x_1 ҳақиқий, x_2 ва x_3 лар ўзаро қўшма мавҳум сонлар бўлади.

б) $\Delta=0$ бўлсин. Агар $\Delta=0$ ва $q\neq0$ бўлса, у ҳолда $z_1=z_2=-\frac{q}{2}\neq0$ бўлади.

$u=\sqrt[3]{-\frac{q}{2}}$ сон $-\frac{q}{2}$ нинг арифметик илдизи бўлсин. $uv=-\frac{p}{3}$ ҳақиқий сон бўлгани учун $v=\sqrt[3]{-\frac{q}{2}}$ ҳақиқий сон бўлади, яъни $u=v\neq0$ бўлади.

(12) формулага асосан $x_1=2u\neq0$, $x_2=x_3=-u$ бўлади. Шундай қилиб, $q\neq0$ бўлганда, (11) тенглама учта ҳақиқий илдизга эга ва улардан биттаси каррали бўлади.

Агар $\Delta=0$ ва $q=0$ бўлса, у ҳолда $p=0$ бўлади. Бу ҳолда (11) тенглама $x^3=0$ кўринишда бўлиб, $x_1=x_2=x_3=0$ бўлади.

с) $\Delta<0$ бўлсин. У ҳолда $z_1=-\frac{q}{2}+\sqrt{\Delta}$, $z_2=-\frac{q}{2}-\sqrt{\Delta}$ бўлади. Демак, z_1 ва z_2 сонлар ўзаро қўшма мавҳум сонлар экан. Шунинг учун

$$|z_1|=|z_2|\neq0 \qquad (13)$$

ва

$$z_1\neq z_2 \qquad (14)$$

муносабатлар ўринли.

(6) ва (8) га кўра

$$u^3 = z_1,\ v^3 = z_2,\ uv = -\frac{p}{3} \qquad (15)$$

бўлгани учун (13) ва (15) дан $|u|^3 = |v|^3 \neq 0$ бўлиб, бундан

$$|u| = |v| \neq 0 \qquad (16)$$

келиб чиқади. (14) га асосан, $u \neq v$ муносабат ҳам ўринлидир. (6) га асосан $uv = -\frac{p}{3}$ бўлиб, бундан $|u| \cdot |v| = -\frac{p}{3}$ келиб чиқади (чунки с) шартга асосан $p < 0$ эди). (16) га кўра

$$-\frac{p}{3|u|^2} = 1 \qquad (17)$$

тенглик бажарилади. (15) ва (17) ларга асосан

$$v = -\frac{p}{3u} = -\frac{p}{3u\bar{u}} \cdot \bar{u} = -\frac{p}{3|u|^2} \cdot \bar{u} = \bar{u},$$

яъни

$$v = \bar{u} \qquad (18)$$

тенглик ўринлидир.

(12) формуладаги v ни $\bar{u}$ билан алмаштирсак ва $u \neq v$ ни эътиборга олсак, x_1, x_2 ва x_3 илдизлар ҳақиқий ва ҳар хил экани маълум бўлади. Ҳақиқатан, (12) формуладан $x_2 \neq x_3$ келиб чиқади. Фараз қилайлик, $x_1 = x_2$ бўлсин. У ҳолда (9) га асосан $u + v = u\varepsilon + v\varepsilon^2$ бўлиб, бундан $u(1-\varepsilon) = v(\varepsilon^2 - 1)$ ёки $u = v\varepsilon^2$ келиб чиқади.

Бундан $z_1 = z_2$ ва $\Delta = 0$ тенгликлар келиб чиқади. Бу эса $\Delta < 0$ шартга қарама-қарши.

Худди шунингдек, $x_1 \neq x_3$ эканлигини ҳам кўрсатиш мумкин.

72-§. Тўртинчи даражали тенглама

Тўртинчи даражали тенгламани ечишнинг Феррари усулини кўрайлак. Бу усул бўйича тўртинчи даражали тенгламани ечиш бирор ёрдамчи учинчи даражали тенгламани ечишга келтирилади.

Комплекс коэффициентли тўртинчи даражали тенглама ушбу

$$x^4+ax^3+bx^2+cx+d=0 \tag{1}$$

кўринишда берилган бўлсин.

(1) дан $x^4+ax^3=-bx^2-cx-d$ ни ёзиб олиб, унинг иккала томонига $\frac{a^2x^2}{4}$ ҳадни қўшамиз ва ушбу кўринишдаги тенгламани ҳосил қиламиз:

$$\left(x^2+\frac{ax}{2}\right)^2=\left(\frac{a^2}{4}-b\right)x^2-cx-d. \tag{2}$$

(2) тенгламанинг иккала томонига $\left(x^2+\frac{ax}{2}\right)y+\frac{y^2}{4}$ ҳадни қўшиб, ушбу

$$\left(x^2+\frac{ax}{2}+\frac{y}{2}\right)^2=\left(\frac{a^2}{4}-b+y\right)x^2+\left(\frac{ay}{2}-c\right)x+\left(\frac{y^2}{4}-b\right) \tag{3}$$

тенгламани ҳосил қиламиз. (3) нинг чап томонида тўла квадрат ҳосил бўлди.

(3) нинг ўнг томонидаги учҳад эса y параметрга боғлиқ. (3) да y параметрни шундай танлаб оламизки, натижада (3) нинг ўнг томони тўла квадрат бўлсин. $Ax^2+Bx+C=0$ учҳад тўла квадраг бўлиши учун эса $B^2-4AC=0$ бўлиши етарли.

Ҳақиқатан, бу шарт бажарилса,

$$Ax^2+Bx+C=Ax^2+2\sqrt{AC}x+C=(\sqrt{A}x+\sqrt{C})^2,$$

яъни

$$Ax^2+Bx+C=(\sqrt{A}x+\sqrt{C})^2$$

тенгламага эга бўламиз.

Демак, y ни шундай танлаб оламизки, натижада

$$\left(\frac{ay}{2}-c\right)^2-4\left(\frac{a^2}{4}-b+y\right)\left(\frac{y^2}{4}-d\right)=0 \tag{4}$$

шарт бажарилсин, яъни y га нисбатан учинчи даражали тенглама ҳосил бўлади.

(4) шарт бажарилса, у ҳолда (3) нинг ўнг томони тўла квадратга айланади.

(4) тенгамани ечиб, унинг битта y_0 илдизини топамиз. Кейин y_0 ни (3) тенгламадаги y ўрнига қўямиз ва

$$\left(x^2+\frac{ax}{2}+\frac{y_0}{2}\right)^2=(\alpha x+\beta)^2 \tag{5}$$

тенгламани ҳосил қиламиз. (5) тенгламани ечганда қуйидаги квадрат тенгламалар системаси ҳосил бўлади:

$$\left|\begin{array}{l} x^2 + \frac{ax}{2} + \frac{y_0}{2} = \alpha x + \beta, \\ x^2 + \frac{ax}{2} + \frac{y_0}{2} = -\alpha x - \beta. \end{array}\right.$$

Бу системани ечиб, берилган (1) тенгламанинг барча ечимларини топамиз.

VII боб. РАЦИОНАЛ СОНЛАР МАЙДОНИ УСТИДАГИ КЎПҲАДЛАР ВА АЛГЕБРАИК СОНЛАР

73-§. Бутун коэффициентли кўпҳаднинг бутун ва рационал илдизлари

Рационал сонлар майдони устида берилган ҳар қандай $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ кўпҳаднинг илдизи

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = O \qquad (1)$$

тенгламанинг ҳам илдизи бўлади. Шунинг учун бундан сўнг биз фақатгина n-даражали тенгламанинг рационал илдизларини топиш билан шуғулланамиз.

1°. Каср коэффициентли тенгламани бутун коэффициентли тенглама билан алмаштириш мумкин.

Исботи. Бунинг учун (1) тенгламанинг икки томонини барча a_0, a_1, a_2 . . . , a_{n-1}, a_n коэффициентларнинг умумий махражига кўпайтириш кифоя.

2°. Бутун коэффициентли тенгламани бош коэффициенти 1 га тенг бутун коэффициентли тенглама билан алмаштириш мумкин.

Исботи. (1) тенгламанинг коэффициентларини бутун деб ҳисоблаб, $x = \frac{y}{a_0}$ алмаштиришни бажарсак, (1) тенглама

$$\frac{y^n}{a_0^{n-1}} + \frac{a_1y^{n-1}}{a_0^{n-1}} + \frac{a_2y^{n-2}}{a_0^{n-2}} + \ldots + \frac{a_{n-1}y}{a_0} + a_n = 0$$

кўринишни олади. Бундан ушбуни ҳосил қиламиз:

$$y^n + a_0a_1y^{n-1} + a_0a_2y^{n-2} + \ldots + a_0^{n-2}a_{n-1}y + a_0^{n-1}a = 0.$$

3°. Бутун коэффициентли

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = 0 \quad (2)$$

тенгламанинг рационал илдизлари фақат бутун сонлар бўлади.

Исботи. (2) тенглама $\alpha = \frac{a}{b}$ илдизга эга бўлсин (a ва b — бутун сонлар, $b \neq 0$); бу касрни қисқармайдиган деб ҳисоблаш мумкин; $\alpha = \frac{a}{b}$ илдизни (2) тенгламага қўйиб,

$$\frac{a^n}{b^n} + a_1 \frac{a^{n-1}}{b^{n-1}} + \ldots + a_{n-1}\frac{a}{b} + a^n = 0$$

ёки

$$\frac{a^n}{b^n} = -(a_1 a^{n-1} + a_2 a^{n-1} b + \ldots + a_n b^{n-1}) \qquad (8)$$

тенгликни ҳосил қиламиз. $\frac{a}{b}$ қисқармайдиган касрдир. Шу сабабли, (3) тенгликнинг бўлиши мумкин эмас, чунки қисқармайдиган каср бутун сонга тенг бўла олмайди.

4°. (2) тengламанинг бутун илдизи озод ҳаднинг бўлувчисидир.

Исботи. a ни (2) тенгламанинг бутун илдизи десак,

$$a^n + a_1 a^{n-1} + a_2 a^{n-2} + \ldots + a_{n-1} a + a_n = 0$$

ёки

$$a_n = a(-a^{n-1} - a_1 a^{n-2} - \ldots - a_{n-1})$$

тенгликка эга бўламиз; бу эса a_n нинг a га бўлинишини кўрсатади.

5°. (2) тенгламанинг чап томонини $x - a$ (a — бутун сон) га бўлишдан чиққан бўлинма бутун коэффициентли кўпҳаддир.

Исботи. Горнер схемаси бўйича бўлинманинг коэффициентлари қуйидаги бутун сонларга тенг:

$$b_0 = a_0 = 1,\ b_1 = a_1 + a,\ b_2 = a_2 + ab_1,\ \ldots,$$
$$b_{n-1} = a_{n-1} + ab_{n-1}.$$

6°. Агар a бутун сон (2) тенгламанинг илдизи бўлса, $\frac{f(1)}{a-1}$ ва $\frac{f(-1)}{a+1}$ ҳам бутун сонлар бўлади

Исботи. Ҳақиқатан, $f(x) = (x - a)\varphi(x)$ тенгликдан $\frac{f(x)}{a-x} = -\varphi(x)$ ҳосил бўлади, бунда, 5°-хоссага биноан, $\varphi(x)$ бутун коэффициентли кўпҳад. Демак, $\frac{f(1)}{a-1} = -\varphi(1)$, $\frac{f(-1)}{a+1} = -\varphi(-1)$ — бутун сонлар.

7°. a бутун сон (2) тенгламанинг илдизи бўлиши учун

$$q_{n-1}=\frac{a_n}{a},\ q_{n-1}=\frac{a_{n-1}+q_{n-1}}{a},\ \ldots,$$

$$q_1=\frac{a_2+q_2}{a}.\ q_0=\frac{a_1+q_1}{a}=1 \qquad (4)$$

нисбатлар бутун сон бўлиши зарур ва етарли.

Исботи. Зарурийлиги. a—тенгламанинг бутун илдизи бўлсин. Горнер схемасидан фойдаланиб, $f(x)$ ни $x-a$ га бўламиз. Бу ҳолда бўлинманинг коэффициентлари $b_0=1$, $b_1=a_1+a$, $b_2=a_2+cb_1, \ldots, b_{n-1}=$ $=a_{n+1}+ab_{n-2}$ тенгликлар билан аниқланиб, қолдиқ нолга тенг бўлади, яъни $0=a_n+ab_{n-1}$. Бу тенгликлардан

$$-b_{n-1}=\frac{a_n}{a}\ -b_{n-2}=\frac{a_{n-1}-b_{n-1}}{a}, \ldots, -1=\frac{a_1-b_1}{a}$$

келиб чиқади. Агар $-b_{n-1}=q_{n-1}$, $-b_{n-2}=q_{n-2}, \ldots,$ $-1=q_0$ деб белгиласак, (4) тенгликларни ҳосил қиламиз.

Етарлилиги. Энди, a бутун сон бўлгани учун (4) тенгликлар кучга эга дейлик. Бу тенгликларнинг сўнггисидан $a_1+a=-q_1$ ни топамиз. Горнер схемасига асосан, $a_1+a=b_1$. Демак, $-q_1=b_1$. Иккинчи тенгликдан $-q_2=a_2-aq_1=a_2+ab$ ҳосил бўлади. Демак, яна Горнер схемаси бўйича топиладиган $b_2=a_2+ab_1$ тенгликка асосан, $-q_2=b_2$. Бу жараённи давом эттириб, биринчи тенгликдан $a_n-aq_{n-1}=a_n+ab_{n-1}=0$ ни ҳосил қиламиз. Аммо Горнер схемаси бўйича $r=a_n+$ $+ab_{n-1}$. Шу сабабли $r=0$. Демак, $f(x)$ ни $x-a$ га бўлишдан чиққан қолдиқ нолга тенг бўлганидан, a бутун сон (2) тенгламанинг илдизини ифодалайди.

Шундай қилиб, рационал сонлар майдони устидаги тенгламанинг рационал илдизларини ҳисоблаш жараёни қуйидагидан иборат:

1) Аввал тенгламани (2) кўринишга келтирамиз;

2) Озод ҳаднинг бўлувчиларини олиб текширамиз;

3) Агар a озод ҳаднинг бўлувчиси бўлса, $f(1)$ ва $f(-1)$ нинг $a-1$ ва $a+1$ га бўлиниш-бўлинмаслигини текширамиз;

4) $\frac{f(1)}{a-1}$ ва $\frac{f(-1)}{a+1}$ нисбатлардан биронтаси бутун сон

бўлмаса, a илдиз бўлмайди. Синовдан ўтган a ни олиб, 7°-хоссанинг бажарилишини текширамиз. Бунинг учун қуйидаги схемани тузамиз:

a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	1
q_{n-1}	q_{n-2}	q_{n-3}	$\ldots$	q_0	

Бунда $q_{n-1}, q_{n-2}, \ldots, q_1, q_0$ сонлар (4) тенгликларга асосан топилади. Агар q_i бутун сон ва $q_0 = -1$ бўлсагина, a илдиз бўлади.

Мисол. Ушбу тенгламани қарайлик:

$$x^5 - \frac{7}{10}x^4 + \frac{11}{10}x^3 - \frac{17}{10}x^2 + \frac{4}{5}x - \frac{1}{10} = 0.$$

Аввал бутун коэффициентли тенгламага алмаштирмиз:

$$10x^5 - 7x^4 + 11x^3 - 17x^2 + 8x - 1 = 0.$$

Сўнгра тенгламани $x = \frac{y}{10}$ алмаштириш билан (2) кўринишга келтирамиз:

$$f(y) = y^5 - 7y^4 + 110y^3 - 1700y^2 + 8000y - 10000. \quad (5)$$

Бунда 10000 озод ҳаднинг бўлувчилари жуда кўп. Шу сабабли ҳисоблашни қисқартириш учун аввал ҳақиқий илдизларнинг чегараларини топамиз.

Мусбат илдизларнинг чегаралари 0 ва 16 эканини аниқлаймиз. (5) тенгламанинг манфий илдизлари йўқ, чунки $y = -z$ алмаштириш натижасида ҳосил бўлган

$$z^5 + 7z^4 + 110z^3 + 1700z^2 + 8000z + 10000 = 0$$

тенгламанинг чап томони z нинг мусбат қийматларида ноль бўламагани учун тенгламанинг мусбат илдизлари йўқ. Шундай қилиб, 10000 нинг 1, 2, 4, 5, 8, 10, 16 бўлувчилари билан чегараланиш кифоя.

Энди $f(-1) = 3596$, $f(1) = 19818$ эканини топамиз.

4 сони илдиз бўла олмайди, чунки $f(-1)$ сон $a + 1 = 4 + 1 = 5$, $a + 1 = 5$ га бўлинмайди. Шунга ўхшаш, 8, 10, 16 ҳам илдиз бўла олмайди. 2 ва 5 ни олганимизда $f(1)$ ва $f(-1)$, мос равишда, $a - 1 = 2 - 1 = 1$, $a - 1 = 1$, $a - 1 = 5 - 1 = 4$, $a - 1 = 4$ га ва $a + 1 = 2 + 1 = 3$, $a + 1 = 5 + 1 = 6$ га бўлинади. Шу сабабли, 2 ва 5 учун 7°-хоссани текшириб кўрамиз.

−10000	8000	−1700	110	−7	1
−5000	1500	−100	5	−1	

−10000	8000	−1700	110	−7	1
−2000	1200	−100	2	−1	

Демак, (5) тенглама $y_1=2$ ва $y_2=5$ дан иборат иккита бутун илдизга эга. Шу сабабли, берилган тенгламанинг рационал илдизлари $x_1=\frac{1}{5}$ ва $x_2=\frac{1}{2}$ бўлади.

74- §. Эйзенштейннинг кўпҳадлар учун келтирилмаслик аломати

Теорема (Эйзенштейн аломати). *Берилган бутун коэффициентли* $f(x)=c_0+c_1x+\ldots+c_nx^n$ *кўпҳаднинг бош ҳади коэффициенти* c_n *дан бошқа барча коэффициентлари p туб сонга бўлиниб, озод ҳад* c_0 *эса* p^2 *га бўлинмаса, у ҳолда* $f(x)$ *кўпҳад Q рационал сонлар майдони устида келтирилмайдиган кўпҳад бўлади.*

Исботи. Фараз қилайлик, $f(x)$ кўпҳад Q майдон устида келтириладиган кўпҳад, яъни $f(x)=g(x)\cdot h(x)$ тенглик ўринли бўлиб, $g(x)$, $h(x)$ кўпҳадларнинг коэффициентлари бутун сонлар бўлсин. Айтайлик,

$$g(x)=a_0+a_1x+\ldots+a_kx^k\ (a_k\neq 0),$$
$$h(x)=b_0+b_1x+\ldots+b_mx^m\ (b_m\neq 0)$$

берилган бўлсин.

Юқоридаги тенгликка кўра $1\leqslant k$, $m<n$ бўлганда

$$f(x)=c_0+c_1x+\ldots+c_nx^n=$$
$$=(a_0+a_1x+\ldots+a_kx^k)(b_0+b_1x+\ldots+b_mx^m)\quad(1)$$

муносабат келиб чиқади. Бунда

$$c_0=a_0b_0,\quad(2)$$
$$c_n=a_kb_m.\quad(3)$$

Теорема шартига асосан,

$$c_0/p, \; c_0 \times p^2 \tag{4}$$

ўринли.

(2), (4) муносабатлардаги a_0 ва b_0 сонлардан фақат биттаси p га бўлинади. Айтайлик,

$$a_0/p, \; b \times p \tag{5}$$

бўлсин. Теорема шартига асосан $c_n \times p$. Бундан (3) га асосан

$$a_k \times p. \tag{6}$$

$g(x)$ кўпҳад коэффициентларининг a_k дан бошқа яна бир нечта коэффициентлари p га бўлинмаслиги мумкин.

$g(x)$ кўпҳад коэффициентларининг p га бўлинмайдиганларидан биринчиси a_s бўлсин, яъни a_0, a_1, ..., a_{s-1} лар p га бўлиниб, a_s сон p га бўлинмасин. Бунда $s \leqslant k < n$ дир. Кўпҳадларни кўпайтириш қоидасига асосан x^s олдидаги c_s коэффициент қуйидаги кўринишда ёзилади:

$$c_s = a_sb_0 + (a_{s-1}b_1 + a_{s-2}b_2 + \ldots + a_0b_s), \; (s < n).$$

a_0, a_1, ..., a_{s-1} сонлар p га бўлингани учун юқоридаги қавс ичидаги ифода p га бўлинади. $a_s \times p$ ва $b_0 \times p$ бўлгани учун c_s сон p га бўлинмайди. Теорема шартига кўра $s \leqslant k < n$ бўлгани учун c_s сон p га бўлиниши керак эди. Бу қарама-қаршилик фаразимизнинг нотўғрилигини кўрсатади. Демак, берилган $f(x)$ кўпҳад Q рационал сонлар майдони устида келтирилмайдиган кўпҳад бўлади.

75-§. Алгебраик ва трансцендент сонлар

Биз юқорида кўриб ўтганимиздек, рационал коэффициентли n-даражали ҳар қандай кўпҳад комплекс сонлар майдонида n та илдизга эга бўлади. Бу илдизлардан баъзи бирлари ҳақиқий сонлардан, баъзилари эса $a + bi$ $(b \neq 0)$ шаклдаги мавҳум сондан иборат бўлади.

Энди масалани бошқача қуймоқчимиз. Ҳар қандай ҳақиқий сон бирорта рационал коэффициентли n-даражали тенгламанинг илдизи бўла оладими? Кейинчалик бу савол ижобий жавобга эга эмаслигини кўриб ўтамиз, яъни ҳеч қандай рационал коэффициентли алгебраик тенгламанинг илдизи бўла олмайдиган ҳақиқий сонлар мавжуд.

1-таъриф. Агар α сон коэффициентлари рационал сонлардан иборат кўпҳаднинг ёки алгебраик тенгламанинг илдизи бўла олса, у ҳолда α сон *алгебраик сон*, акс ҳолда *трансцендент сон* дейилади.

Мисоллар. 1. Барча рационал сонлар алгебраик сонлар бўлади. Ҳақиқатан, $\frac{m}{n}$ $(n \neq 0)$ кўринишдаги рационал сон $mx - n = 0$ тенглама инг илдизи бўлади.

2. Рационал сонларнинг ихтиёрий k-даражали илдизи ҳам алгебраик сондир, чунки, бу сонлар $mx^k - n = 0$ тенглама илдизи бўлади

3. $2 - 3i$ сон $x^2 - 4x + 13 = 0$ алгебраик тенгламанинг илдизи Демак, $2 - 3i$ алгебраик сон экан.

4. i сон $x^2 + 1 = 0$ алгебраик тенгламанинг илдизи. Демак, мавҳум сонларнинг бир қисми ҳам алгебраик сонлар экан.

5. π, e сонлари трансцендент сонлардир.

1-таъриф. Агар α сон коэффициентлари $\mathcal{P}$ майдонга тегишли бирор алгебраик тенгламанинг илдизи бўлса, у ҳолда α сон *$\mathcal{P}$ майдонга нисбатан алгебраик сон*, акс ҳолда α сон *$\mathcal{P}$ майдонга нисбатан трансцендент сон* дейилади.

Теорема. *Илдизи α дан иборат бўлган келтирилмайдиган кўпҳад нолинчи даражали кўпҳад аниқлигида ягонадир.*

Исботи. Фараз қилайлик, илдизи α дан иборат бўлган иккита $f(x)$ ва $g(x)$ кўпҳадлар мавжуд ва уларнинг ҳар бири келтирилмайдиган кўпҳадлар бўлсин. Бундай ҳолда бу кўпҳадларнинг энг катта умумий бўлувчиси 1 дан фарқли. Иккинчидан, улар $\mathcal{P}$ сонлар майдони устида келтирилмайдиган бўлганлиги туфайли бу кўпҳадлар бир-биридан нолинчи даражали кўпҳад билангина фарқланади.

3-таъриф. $\mathcal{P}$ майдон устида бош коэффициенти 1 га тенг ва келтирилмайдиган $f(x)$ кўпҳад α илдизга эга бўлса, бу кўпҳаднинг даражаси $\mathcal{P}$ майдонга нисбатан *α алгебраик соннинг даражаси* дейилади. $f(x)$ кўпҳад эса $\mathcal{P}$ сонлар майдони устидаги *минимал кўпҳад* дейилади.

4-таъриф. $\mathcal{P}$ майдон устида келтирилмайдиган $f(x)$ кўпҳаднинг барача илдизлари *ўзаро қўшма сонлар* дейилади.

Рационал сонлар ўз-ўзига қўшма деб ҳисобланади. Рационал бўлмаган ҳар қандай сон, даражаси иккидан кичик бўлмаган кўпҳаднинг илдизидан иборат бўлгани учун улар қўшма алгебраик сонларга эга*.

76- §. Майдоннинг оддий алгебраик кенгайтмасини қуриш

α элемент $\mathscr{P}$ майдонга нисбатан алгебраик элемент бўлсин. Элементлари $d_0+d_1\alpha+\ldots+d_l\alpha^l$ кўринишдаги ҳалқани $\mathscr{F}[\alpha]$, элементлари $\frac{c_0+c_1\alpha+\ldots+c_k\alpha^k}{d_0+d_1\alpha+\ldots+d_l\alpha^l}$ (бунда $d_0+d_1\alpha+\ldots+d_l\alpha^l\neq 0$) кўринишдаги тўпламни эса $\mathscr{B}(\alpha)$ орқали белгилайлик.

1-теорема. *Агар α элемент $\mathscr{P}$ майдонга нисбатан алгебраик элемент бўлса, у ҳолда $\mathscr{P}(\alpha)=\mathscr{P}[\alpha]$ тенглик ўринла бўлади.*

Исботи. Ушбу

$$\mathscr{P}(\alpha)=\left\{\frac{c_0+c_1\alpha+\ldots+c_k\alpha^k}{d_0+d_1\alpha+\ldots+d_l\alpha^l}\Big/ c_i, d_i\in\mathscr{P},\ k,\ l=0,\ 1,\ 2\ldots\right\} \qquad (1)$$

тўплам майдон ташкил этади.

Агар (1) да $d_0=1,\ d_1=d_2=\ldots=d_l=0$ бўлса, у ҳолда $\mathscr{F}(\alpha)$ тўпламнинг элементлари $\mathscr{P}(\alpha)$ нинг элементлари каби бўлади, яъни ушбу муносабат ўринли:

$$\mathscr{P}[\alpha]\subset\mathscr{R}[\alpha] \qquad (2)$$

α алгебраик элемент бўлгани учун у $\mathscr{F}$ майдон устида келтирилмайдиган бирор $p(x)=p_0+p_1x+\ldots+p_nx^n\ (p_i\in\mathscr{P})$ кўпҳаднинг илдизи, яъни $p(\alpha)=0$ бўлади, $A\beta\in\mathscr{P}(\alpha)$ бўлиб $\beta=f(\alpha)=c_0+c_1\alpha+\ldots+c_k\alpha^k\ (ci\in\mathscr{P})$ бўлсин.

Қолдиқли бўлиш теоремасига кўра

$$f(x)=p(x)\,g(x)+r(x),\ (g(x),\ r(x)\in\mathscr{P}[x]) \qquad (3)$$

тенгликни ёзамиз. (3) да $x=\alpha$ бўлса, у ҳолда $f(\alpha)=p(\alpha)\,g(\alpha)+r(\alpha)$ ёки $f(\alpha)=r(\alpha)$ бўлиб, $\beta=r(\alpha)$ тенглик ўринли бўлади.

$r(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ бўлса, у ҳолда $\beta=a_0+a_1x+\ldots a_{n-1}x^{n-1}$ ни ёзиш мумкин. Бундан

---

* Қўшма комплекс сон тушунчаси билан қўшма алгебраик сонлар тушунчасини аралаштириб юбормаслик лозим.

кўринадики, $k>0$ бўлганда ҳамма вақт β нинг даражасини n дан кичик қилиб олиш мумкин экан. Энди

$$\frac{f(\alpha)}{g(\alpha)}=\frac{a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}}{b_0+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1}}\in\mathscr{P}(\alpha)$$

бўлсин. Бунда $g(\alpha)\neq 0$, $g(x)\neq 0$. $g(x)$ кўпҳад $p(x)$ кўпҳадга бўлинмайди. Чунки $g(x)$ нинг даражаси $p(x)$ нинг даражасидан кичик. $p(x)$ кўпҳад келтирилмайдиган кўпҳад бўлгани учун $(p(x);\ g(x))=1$ бўлади. У ҳолда шундай $u(x)$ ва $v(x)$ кўпҳадлар мавжудки, натижада $g(x)u(x)+p(x)v(x)=1$ тенглик ўринли бўлади. Бу тенгликда $x=\alpha$ бўлса, у ҳолда $g(\alpha)u(\alpha)+$ $+p(\alpha)v(\alpha)=1$ бўлиб, бунда $p(\alpha)=0$ эканлиги эътиборга олинса, $g(\alpha)u(\alpha)=1$ тенгликка эга бўламиз. Бундан $g(\alpha)=\frac{1}{u(\alpha)}$ бўлгани учун

$$\frac{f(\alpha)}{g(\alpha)}=\frac{f(\alpha)}{\frac{1}{u(\alpha)}}=f(\alpha)\,u(\alpha),$$

яъни

$$\frac{f(\alpha)}{g(\alpha)}=f(\alpha)\,u(\alpha)$$

тенгликни ҳосил қиламиз. Сўнгра

$$f(\alpha)\,u(\alpha)\in\mathscr{P}[\alpha]\ \text{ёки}\ \frac{f(\alpha)}{g(\alpha)}\in\mathscr{P}[\alpha]$$

бўлгани сабабли ва у $p(\alpha)$ нинг ихтиёрий элементи бўлгани учун

$$\mathscr{P}(\alpha)\subset\mathscr{P}[\alpha] \tag{4}$$

муносабат ўринли.

(2) ва (4) муносабатлардан эса $\mathscr{P}(\alpha)=\mathscr{P}[\alpha]$ тенглик келиб чиқади.

Таъриф. $\mathscr{F}$ майдон $\mathscr{P}$ майдоннинг қисм майдони бўлиб, $\alpha\in F$ бўлса, у ҳолда $\mathscr{P}$ майдонни ва α элементни ўз ичига олган $\mathscr{P}$ майдоннинг энг кичик қисм майдони α элемент орқали ҳосил қилинган $\mathscr{P}$ майдоннинг *оддий кенгайтмаси*, агар α алгебраик элемент бўлса, у ҳолда $\mathscr{P}$ майдоннинг энг кичик қисм майдоннинг *оддий алгебраик кенгайтмаси* дейилади.

Рационал сонлар майдони Q га даражаси иккига тенг бўлган $\sqrt{2}$ алгебраик сонни киритамиз ва уни $Q[\sqrt{2}]$

каби белгилайлик. $Q[\sqrt{2}]$ тўплам майдон ташкил қилади. $Q[\sqrt{2}]$ майдон Q майдоннинг оддий алгебраик кенгайтмаси бўлади.

2-теорема. *α элемент $\mathscr{P}$ майдон устида мусбат даражали алгебраик элемент бўлса, у ҳолда $\mathscr{P}(\alpha)$ майдондаги ихтиёрий элемент коэффициентлари $\mathscr{P}$ дан олинган n та $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ элементларнинг чизиқли комбинацияси бўлади.*

Исботи. β элемент $\mathscr{P}(\alpha)$ майдоннинг ихтиёрий элементи бўлсин. 1-теоремага кўра $\mathscr{P}(\alpha)=\mathscr{P}[\alpha]$ эди. Демак, $\mathscr{P}[x]$ да шундай $f(x)$ кўпҳад топиладики, натижа $x=\alpha$ бўлганда

$$\beta=f(\alpha) \tag{5}$$

бўлади. $\mathscr{P}$ майдон устида α учун минимал кўпҳад $g(x)$ бўлсин. Теорема шартига кўра унинг даражаси n га тенг. Қолдиқли бўлиш теоремасига кўра $\mathscr{P}[x]$ ҳалқада шундай $h(x)$ ва $r(x)$ кўпҳадлар топиладики, натижада $f(x)=g(x)h(x)+r(x)$ тенглик ўринли бўлиб, бунда $r=0$ ёки дар $r(x)<$ дар $g(x)=n$, яъни

$$r(x)=c_0+c_1x+\ldots+c_{n-}x^{n-1}(c_i\in\mathscr{P}) \tag{6}$$

бўлади. (2) да $x=\alpha$ деб олиб, (5) тенгликдан

$$\beta=c_0+c_1\alpha+\ldots+c_{n-1}\alpha^{n-1} \tag{7}$$

тенгликка эга бўламиз.

Энди β элемент $1, \alpha, \ldots, \alpha^{n-1}$ элементларнинг бир қийматли чизиқли комбинацияси эканини кўрсатайлик.

Фараз қилайлик, β нинг (7) дан бошқа

$$\beta=d_0+d_1\alpha+\ldots+d_{n-1}\alpha^{n-1}(d_i\in\mathscr{P}) \tag{8}$$

ифодаси бўлсин. Ушбу

$$\varphi(x)=(c_0-d_0)+(c_1-d_1)x+\ldots(c_{n-1}-d_{n-1})x^{n-1}$$

кўпҳадни текширамиз.

(7) ва (8) га асосан $\varphi(\alpha)=0$ бўлгани учун $\varphi(x)$ нинг даражаси n дан кичик бўлмайди. $\varphi(x)$ нинг даражаси эса $g(x)$ нинг даражасидан кичик. Бу ҳоллар фақат $\varphi(x)=0$ бўлгандагина бажарилади, яъни $(c_0-d_0)+(c_1-d_1)x+\ldots+(c_{n-1}-d_{n-1})x^{n-1}=0$ бўла-

ди. Бундан $c_0 = d_0$, $c_1 = d_1$, ..., $c_{n-1} = d_{n-1}$ келиб чиқади. Демак, β элемент $1, \alpha, \dots \alpha^{n-1}$ элементларнинг чизиқли комбинацияси кўринишида бир қийматли ифодаланар экан.

77-§. Майдоннинг чекли кенгайтмаси

$\mathcal{F}$ майдоннинг қисм майдони $\mathcal{P}$ бўлсин. У ҳолда $\mathcal{F}$ ни $\mathcal{P}$ майдон устида вектор фазо деб қараш мумкин.

1-**таъриф.** Агар $\mathcal{F}$ майдон $\mathcal{P}$ майдон устида вектар фазо сифатида чекли ўлчамга эга бўлса, у ҳолда $\mathcal{F}$ майдон $\mathcal{P}$ майдоннинг *чекли кенгайтмаси* дейилади.

$\mathcal{F}$ нинг $\mathcal{P}$ майдон устидаги чекли ўлчами $[\mathcal{F} : \mathcal{P}]$ каби белгиланади.

1-**теорема.** *Агар α элемент $\mathcal{P}$ майдон устида n-даражали алгебраик элемент бўлса, у ҳолда $[\mathcal{P}(\alpha) : \mathcal{P}] = n$ бўлади.*

Исботи. Бу теорема майдоннинг оддий алгебраик кенгайтмасини қуриш мавзусидаги 2- теоремадан бевосита келиб чиқади.

2-**таъриф.** Агар $\mathcal{F}$ майдоннинг ҳар бир элементи $\mathcal{P}$ майдон устида алгебраик бўлса, у ҳолда $\mathcal{F}$ майдон $\mathcal{P}$ майдоннинг *алгебраик кенгайтмаси* дейилади.

2-**теорема.** *$\mathcal{P}$ майдоннинг ихтиёрий чекли кенгайтмаси бўлган $\mathcal{F}$ майдон $\mathcal{P}$ майдон устида алгебраик кенгайтма бўлади.*

Исботи. $\mathcal{P}$ устида $\mathcal{F}$ майдон n ўлчовли бўлсин. Агар $n=0$ бўлса, у ҳолда теорема ўринли бўлади. $n>0$ бўлсин. У ҳолда $\mathcal{P}$ устида $\mathcal{F}$ дан олинган ихтиёрий $n+1$ та элемент чизиқли боғланган бўлади. Хусусий ҳолда $1, \alpha, \dots, \alpha^n$ элементлар системаси чизиқли боғланган, яъни $\mathcal{P}$ да камида биттаси ноль бўлмаган $c_0, c_1, \dots, c_n$ элементлар топиладики, натижада $c_0 \cdot 1 + c_1\alpha + \dots + c_n\alpha^n = 0$ тенглик ўринли бўлади. Демак, α элемент $\mathcal{P}$ майдон устида алгебраик экан.

78-§. Майдоннинг мураккаб алгебраик кенгайтмаси

1-**таъриф.** Агар $\mathcal{F}$ майдоннинг $L_i (i = \overline{0, k})$ қисм майдонларининг ўсувчи занжири мавжуд бўлса, яъни

$$\mathcal{P} = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_k = \mathcal{F} \quad (k > 1)$$

муносабат ўринли бўлса, у ҳолда $\mathcal{F}$ майдон $\mathcal{P}$ майдоннинг *мураккаб кенгайтмаси* дейилади.

1-теорема. *$\mathcal{F}$ майдон L майдоннинг чекли кенгайтмаси бўлиб, L майдон $\mathcal{P}$ майдоннинг чекли кенгайтмаси бўлса, у ҳолда $\mathcal{F}$ майдон $\mathcal{P}$ майдоннинг чекли кенгайтмаси бўлади ва*

$$[\mathcal{F}:\mathcal{P}]=[\mathcal{F}:L]\cdot[L:\mathcal{P}] \tag{1}$$

муносабат ўринли бўлади.

Исботи. Ушбу

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_m \tag{2}$$

лар $\mathcal{P}$ устида L майдоннинг базиси бўлсин ва

$$\beta_1,\ \beta_2,\ \ldots,\ \beta_n \tag{3}$$

эса L устида $\mathcal{F}$ майдоннинг базиси бўлсин.

$\mathcal{F}$ даги ихтиёрий a элементни (3) базис орқали қуйидагича чизиқли ифодалаш мумкин:

$$a=e_1\beta_1+e_2\beta_2+\ldots+e_n\beta_n\ \ (e_n\in L). \tag{4}$$

e_k коэффициентларни эса (2) базис орқали қуйидагича чизиқли ифодалаймиз:

$$e_k=p_{1k}\alpha_1+p_{2k}\alpha_2+\ldots+p_{mk}\alpha_k\ \ (p_{ik}\in\mathcal{P}). \tag{5}$$

(5) даги e_k нинг қийматларини (4) га қўямиз, яъни

$$a=(p_{11}\alpha_1+p_{21}\alpha_2+\ldots+p_{m1}\alpha_m)\beta_1+(a_{12}\alpha_1+$$
$$+p_{22}\alpha_2+\ldots+p_{m2}\alpha_m)\beta_2+\ldots+(p_{1n}\alpha_1+p_{2n}\alpha_2+$$
$$+\ldots+p_{mn}\alpha_m)\beta_n=\sum_{i=1}^{n}\Big(\sum_{i=1}^{m}p_{ik}\alpha_i\Big)\beta_k,$$

$$a=\sum_{k=1}^{n}\Big(\sum_{i=1}^{m}p_{ik}\alpha_i\Big)\beta_k$$

бўлади.

Демак, $\mathcal{F}$ майдоннинг ҳар бир элементи $B=\{\alpha_i\beta_k/i=\overline{1,\ m};\ k=\overline{1,\ n}\}$ тўплам элементларининг чизиқли комбинацияси кўринишида ифодаланади.

B тўплам $\mathcal{P}$ майдон устида $\mathcal{F}$ нинг базиси, яъни B тўплам элементлари чизиқли боғланмаган эканини кўрсатамиз. Ушбу

$$\sum_{i,\ k}c_{ik}\alpha_i\beta_k=0\quad(c_{ik}\in\mathcal{P}) \tag{6}$$

тенглик берилган бўлсин.

(3) система базис бўлгани учун чизиқли боғланмаган. Шунинг учун (6) тенгликдан

$$c_{1k}\alpha_1 + c_{2k}\alpha_2 + \ldots + c_{mk}\alpha_m = 0 \quad (k = \overline{1, n}) \qquad (7)$$

тенгликлар ҳосил бўлади.

(2) система ҳам чизиқли бўлмагани учун (7) тенгликдан $c_{1k} = 0, c_{2k} = 0, \ldots, c_{mk} = 0$ $(k = \overline{1, n})$ тенгликлар келиб чиқади.

Демак, (6) нинг барча коэффициентлари нолга тенг экан. Бундан B система элементлари чизиқли боғланмаган ва $\mathcal{F}$ устида $\mathcal{P}$ нинг базиси экан. Натижада $[\mathcal{F} : \mathcal{P}] = nm = [\mathcal{F} : L] \cdot [L : \mathcal{P}]$ бўлиб, $\mathcal{F}$ майдон $\mathcal{P}$ майдон устида чекли кенгайтма бўлади.

2-таъриф. Агар $\mathcal{F}$ майдон L_i қисм майдонларининг ўсувчи занжири

$$\mathcal{P} = L_0 \subset L_1 \subset L_2 \subset \ldots \subset L_k = \mathcal{F} \quad (k > 1) \qquad (8)$$

мавжуд бўлса ва $i=1$ дан k гача ўзгарганда L_i майдон L_{i-1} майдоннинг оддий алгебраик кенгайтмаси бўлса, $\mathcal{F}$ майдон $\mathcal{P}$ майдоннинг *мураккаб алгебраик кенгайтмаси* дейилади. k сон эса (8) *занжир узунлиги* дейилади.

1-натижа. $\mathcal{P}$ майдоннинг $\mathcal{F}$ мураккаб алгебраик кенгайтмаси $\mathcal{P}$ майдоннинг чекли кенгайтмаси ҳам бўлади.

Исботи. $k = 1$ бўлсин. У ҳолда $\mathcal{F}$ майдон $\mathcal{P}$ майдоннинг оддий алгебраик кенгайтмаси бўлади. Майдоннинг оддий алгебраик кенгайтмасини қуришга асосан, $\mathcal{F}$ майдон $\mathcal{P}$ майдоннинг чекли кенгайтмаси ҳам бўлади.

k дан кичик сонлар учун 1-натижа ўринли бўлсин. k сон учун 1-натижанинг ўринли эканини кўрсатамиз.

$k-1$ учун фаразга асосан L_{k-1} майдон $\mathcal{P}$ майдоннинг чекли кенгайтмаси бўлади.

L_k майдон L_{k-1} нинг оддий алгебраик кенгайтмаси бўлгани учун L_k майдон L_{k-1} нинг ва $\mathcal{P}$ нинг ҳам чекли кенгайтмаси бўлади.

2-теорема. *$\mathcal{F}$ майдоннинг майдон $\mathcal{P}$ устида алгебраик элементлари $\alpha_1, \alpha_2, \ldots, \alpha_k$ бўлса, у ҳолда $\mathcal{P}(\alpha_1, \alpha_2, \ldots, \alpha_k)$ майдон $\mathcal{F}$ майдоннинг чекли кенгайтмаси бўлади.*

Исботи. $L_0 = \mathcal{P}$, $L_1 = \mathcal{P}[\alpha_1]$, $L_2 = \mathcal{P}[\alpha_1, \alpha_2], \ldots,$ $L_k = \mathcal{P}[\alpha_1, \alpha_2, \ldots, \alpha_k]$ белгилашларни киритамиз.

У ҳолда $L_1 = \mathscr{P}[\alpha_1]$ майдон L_0 майдоннинг оддий алгебраик кенгайтмаси бўлади. L_2 майдон эса L_1 нинг оддий алгебраик кенгайтмаси бўлади.
Ҳақиқатан,

$$L_2 = \mathscr{P}[\alpha_1, \alpha_2] = (\mathscr{P}[\alpha_1])[\alpha_2] = L_1[\alpha_2] = L_1(\alpha_1)$$

ва ҳоказо. Демак,

$$\mathscr{P} = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_k = \mathscr{F}$$
$$(L_i = L_{i-1})\alpha_i, (i = 1, k) \qquad (9)$$

бўлиб, занжирнинг ҳар бир ҳади ўзидан олдинги ҳаднинг оддий алгебраик кенгайтмаси бўлади.

$\mathscr{F}$ майдон $\mathscr{P}$ майдоннинг мураккаб алгебраик кенгайтмаси бўлади. 1-натижага кўра эса $\mathscr{F}$ майдон $\mathscr{P}$ майдоннинг чекли кенгайтмаси ҳам бўлади,

2-натижа. Майдоннинг мураккаб алгебраик кенгайтмаси ўша майдоннинг алгебраик кенгайтмаси бўлади.

79-§. Алгебраик сонлар майдони ва унинг алгебраик ёпиқлиги

1-теорема. *Барча алгебраик сонлар тўплами* $\mathscr{A}$ *комплекс сонлар ҳалқаси* $\mathscr{C}$ *да ёпиқ бўлиб, алгебраик сонлар тўплами ҳосил қилган* $\mathscr{A}$ *алгебра комплекс сонлар майдонининг қисм майдони бўлади.*

Исботи. a ва b элементлар A тўпламнинг ихтиёрий элементлари бўлсин. Q майдоннинг $Q(a; b)$ мураккаб алгебраик кенгайтмаси майдоннинг мураккаб алгебраик кенгайтмаси мавзусидаги 2-натижага (75-§) асосан $Q(a. b)$ майдон Q майдоннинг алгебраик кенгайтмаси бўлади. Шунинг учун $a+b$, $a \cdot b$, $-a$, 1 сонлар алгебраик, яъни A тўпламга тегишли бўлади.

A тўплам C даги қўшиш, кўпайтириш каби асосий амалларга нисбатан ёпиқ. Демак, $\mathscr{A}$ алгебра $\mathscr{C}$ ҳалқанинг қисм ҳалқаси бўлганидан $\mathscr{A}$ ҳам ҳалқа бўлади. Агар a элемент A тўпламнинг нолмас элементи бўлса, у ҳолда $a^{-1} \in Q(a; b)$ ва $a^{-1} \in A$ бўлади. Шунинг учун $\mathscr{A}$ алгебра майдон бўлади ва $\mathscr{C}$ майдоннинг қисм майдони бўлади.

2-теорема. *Алгебраик сонлар майдони алгебраик ёпиқ*

Исботи. $\mathscr{A}$ алгебраик сонлар майдони устида $\mathscr{A}[x]$ кўпҳадлар ҳалқаси берилган бўлсин. Ушбу

$$f(x) = a_0 + a_1x + \dots + a_nx^n \quad (a_i \in A)$$

кўпҳад $\mathcal{A}[x]$ даги ихтиёрий мусбат даражали кўпҳад бўлсин. Теоремани исботлаш учун $f(x)$ кўпҳаднинг A тўпламда илдизга эга эканлигини кўрсатиш етарли. $f(x) \in \mathcal{C}[x]$ ва $\mathcal{C}$ майдон алгебраик ёпиқ бўлгани учун $f(x)$ кўпҳад $\mathcal{C}$ да илдизга эга бўлади. У илдизни c дейлик. У ҳолда $f(c)=0$ бўлади. $L = Q(a_0, a_1, \ldots, a_n)$ ва c элемент орқали L майдоннинг оддий алгебраик кенгайтмаси $L(c)$ бўлсин. Натижада $Q \subset L \subset L(c)$ занжирдаги $L(c)$ майдон L майдоннинг чекли алгебраик кенгайтмаси бўлади. Майдоннинг мураккаб кенгайтмасидаги 2-теоремага асосан L майдон Q майдоннинг чекли кенгайтмаси, майдоннинг мураккаб кенгайтмасидаги 1-теоремага асосан эса $L(c)$ майдон Q майдоннинг чекли алгебраик кенгайтмаси бўлади. Чекли кенгайтмадаги 2-теоремага асосан $L(c)$ майдон Q майдоннинг алгебраик кенгайтмаси бўлади ва $c \in A$.

Демак, $\mathcal{A}[x]$ дан олинган мусбат даражали ихтиёрий кўпҳад A тўпламда илдизга эга, яъни $\mathcal{A}$ майдон алгебраик ёпиқ.

80-§. Тенгламаларнинг радикалларда ечилиши тушунчаси

1-таъриф. Агар $\mathcal{F} = \mathcal{G}(\alpha)$ $(\alpha \overline{\in} \mathcal{P}, \ \alpha^2 \in \mathcal{P})$ муносабатни қаноатлантирувчи α элемент мавжуд бўлса, у ҳолда $\mathcal{F}$ майдон $\mathcal{T}$ майдоннинг *квадратик кенгайтмаси* дейилади.

Мисоллар. 1. $Q[\sqrt{2}]$ майдон Q майдоннинг квадратик кенгайтмаси бўлади.

2. $Q(\sqrt[3]{3})$ майдон Q майдоннинг квадратик кенгайтмаси эмас.

3. $Q(i)$ майдон Q майдоннинг квадратик кенгайтмаси бўлади.

2-таъриф. Агар

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n (a_i \in Q) \qquad (1)$$

тенгламанинг илдизларини қуйидаги икки ҳадли квадратик тенгламалар занжирларининг илдизлари орқали рационал (яъни қўшиш, айириш, кўпайтириш, бўлиш амаллари ёрдамида) ифодалаш мумкин бўлса, у ҳолда $f(x)$ кўпҳад *квадрат радикалда ечилади* дейилади:

$$x^2 - \alpha_0 = 0, \quad \alpha_0 \in Q = \mathcal{G}_0;$$

$$x^2 - \alpha_1 = 0, \quad \alpha_1 \in \mathcal{P}_1 = \mathcal{G}_0(\sqrt{\alpha_0});$$

$$x^2 - \alpha_2 = 0, \quad \alpha_2 \in \mathcal{F}_2 = \mathcal{F}_1(\sqrt{\alpha_1});$$

. . . .

$$x^2 - \alpha_{k-1} = 0, \quad \alpha_{k-1} \in \mathcal{F}_{k-1} = \mathcal{F}_{k-2}(\sqrt{\alpha_{k-2}}).$$

Шундай қилиб, (1) тенгламанинг барча илдизлари $\sqrt{\alpha_0}$, $\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_{k-1}}$ сонлар орқали рационал ифодаланади ва $\mathcal{F}_k = \mathcal{F}_{k-1}(\sqrt{\alpha_{k-1}})$ майдонга тегишли бўлади. Бошқача айтганда,

$$Q = \mathcal{F}_0 \subset \mathcal{F}_1 \subset \cdots \subset \mathcal{F}_{k-1} \in \mathcal{F}_k$$

ўсувчи сонли майдонлар занжири мавжуд бўлиб, бу занжирдаги ҳар бир $\mathcal{F}$ майдон ўзидан олдинги $\mathcal{F}_{i-1}$ майдоннинг квадратик кенгайтмаси бўлса ва $\mathcal{F}_k$ майдон (1) тенгламанинг барча илдизларини ўз ичига олса, у ҳолда (1) тенглама *квадрат радикалда ечиладиган тенглама* дейилади.

3-таъриф. Агар (1) тенглама илдизлари қуйидаги икки ҳадли тенгламалар занжирларининг илдизлари орқали ифодаланса, (1) *тенглама радикалда ечилади* дейилади:

$$x^{n_0} - \alpha_0 = 0, \quad \alpha \in Q = {}_0;$$

$$x^{n_1} - \alpha_1 = 0, \quad \sigma_1 \in \mathcal{F}_1 = \mathcal{F}_0(\sqrt[n_0]{\alpha_0});$$

$$x^{n_2} - \alpha_2 = 0, \quad \alpha_2 \in \mathcal{F} = \mathcal{F}_1(\sqrt[n_1]{\alpha_2});$$

. . . .

$$x^{n_{k-1}} - \alpha_{k-1} = 0, \quad \alpha_{k-1} \in \mathcal{F}_{k-1} = \mathcal{F}_{k-2}(\sqrt[n_{k-2}]{\alpha_{n_{k-2}}}).$$

Шундай қилиб (1) тенгламанинг барча илдизлари $\sqrt[n_0]{\alpha_0}, \sqrt[n_1]{\alpha_1}, \ldots, \sqrt[n_{k-1}]{\alpha_{k-1}}$ сонлар орқали рационал ифодаланади ва $\mathcal{F}_k = \mathcal{F}_{k-1}\left(\sqrt[n_{k-1}]{\alpha_{k-1}}\right)$ майдонга тегишли бўлади.

Даражаси тўртдан кичик бўлмаган тенгламаларни квадрат радикалларда ечилиш шарти билан шуғулланайлик. Фараз қилайлик, $f(x)$ кўпҳад бирор $\mathcal{R}$ сонлар майдони устида берилган бўлсин.

4-таъриф. Агар

$$f(x)=0 \qquad (2)$$

тенгламанинг илдизлари

$$f_i(x)=0 \quad (i=\overline{1,k}) \qquad (3)$$

тенгламаларнинг илдизлари орқали рационал ифодаланса, у ҳолда (2) тенгламани ҳар бирининг даражаси иккидан юқори бўлмаган *тенгламалар занжирига келтирилади* дейилади.

(3) даги ҳар бир $f_i(x)$ кўпҳад учун қуйидаги иккита ҳол юз бериши мумкин:

а) Ихтиёрий $f_i(x)$ лар биринчи даражали кўпҳад;

б) $f_i(x)$ берилган $\mathscr{F}$ майдон устидаги келтирилмайдиган иккинчи даражали кўпҳаддир.

Агар $f_1(x)$ нинг бирор илдизини α десак, $f_2(x)$ кўпҳад $\mathscr{F}(\alpha)$ да келтирилмайдиган иккинчи даражали кўпҳад, $f_3(x)$ эса $\mathscr{F}(\alpha)$ га $f_2(x)$ нинг бирор β илдизини киритишдан ҳосил бўладиган $\mathscr{F}(\alpha;\ \beta)$ келтирилмайдиган иккинчи даражали кўпҳаддир ва ҳоказо.

5-таъриф. Агар $f(x)$ кўпҳад $\mathscr{F}$ нинг бирор кенгайтмасида чизиқли кўпайтувчилар кўпайтмаси шаклида ёзилса, у ҳолда *Q нормал майдон* дейилади.

1-теорема. *Коэффициентлари $\mathscr{F}$ майдонга тегишли $f(x)$ кўпҳад учун Q кенгайтма нормал кенгайтма бўлса, у холда $f(x)=0$ тенглама квадрат радикалларда ечилиши учун $(Q:\mathscr{F})=2^m$ бўлиши зарур ва етарлидир.*

Исботи. 1. Зарурийлик шарти. Фараз қилайлик, (1) тенглама (2) каби тенгламалар занжирига келтирилган бўлсин. У ҳолда юқоридаги каби икки ҳол бўлиши мумкин

а) $f_i(x)$ ларнинг барчаси биринчи даражали. Бундай ҳолда биринчи даражали тенгламаларнинг илдизларини $\mathscr{F}$ га киритиш билан бу майдон ўзгармайди, яъни бу ҳолда $(Q:\mathscr{F})=2^0=1$ бўлгани учун $Q=\mathscr{F}$ бўлади.

б) $f_i(x)$ лар орасида даражаси иккидан кичик бўлмаган кўпҳад мавжуд бўлса, у ҳолда $\mathscr{F}$ нинг шу $\mathscr{F}$ га нисбатан 2^n даражали кенгайтмаси ҳисобланган $\mathscr{F}_1$ кенгайтма мавжуд бўлади. У ҳолда $(Q:\mathscr{F})$ даражага $(\mathscr{F}_1:\mathscr{F})$ даража бўлинади. Бундан $(Q:\mathscr{F})=2^m$ эканлиги келиб чиқади.

2. Етарлилик шарти. Энди $(Q:\mathscr{F})=2^m$ деб олиб, $f(x)=0$ ни $f_i(x)=0$ каби тенгламалар занжирига келишини кўрсатамиз.

Бунда қуйидаги уч ҳол бўлади:

1) $m=0$. Бунда $(Q:\mathscr{P})=1$ бўлгани учун $f_i(x)$ кўпҳадларнинг барчаси биринчи даражали бўлади. Ўз-ўзидан маълумки, бундай ҳолда $f_i(x)=0$ тенгламаларнинг илдизлари $\mathscr{P}$ майдонга тегишлидир.

2) $m=1$ бўлганда $(Q:\mathscr{P})=2$ бўлиб, $f(x)$ нинг нормаси, яъни Q майдон $\mathscr{P}$ га коэффициентлари шу $\mathscr{P}$ майдонга тегишли бўлган квадрат тенгламанинг илдизини киритишдан ҳосил бўлади. Бундай ҳолда $f_i(x)=0$ занжирдаги ҳар бир тенгламанинг даражаси албатта иккидан юқори бўлмайди.

3) $m>1$ бўлсин. У ҳолда $(Q:\mathscr{P})=2^m$ бўлиб, $\mathscr{G}$ нинг шу $\mathscr{P}$ га нисбатан иккинчи даражали $\mathscr{P}_1$ кенгайтмаси мавжуд бўлади. Бу кенгайтма учун $(Q:\mathscr{P}_1)=2^{m-1}$ бўлади.

Энди $\mathscr{P}$ ўрнига $\mathscr{P}_1$ ни олайлик. Унда $\mathscr{P}_1$ ва Q орасида шундай $\mathscr{P}_2$ кенгайтма мавжудки, унинг учун $(Q:\mathscr{P}_2)=2^{m-2}$ бажарилади, яъни $\mathscr{P}_2$ кенгайтма $\mathscr{P}_1$ га нисбатан иккинчи даражали бўлади. Бу жараённи давом эттириб, ҳар бир кейингиси олдингиси учун иккинчи даражали бўлган

$$\mathscr{P}\subset\mathscr{P}_1\subset\mathscr{P}_2\subset\cdots\subset\mathscr{P}_m=Q$$

чекли кенгайтмалар кетма-кетлигига эришамиз. Натижада $f(x)=0$ тенгламанинг ҳар бири иккинчи даражали бўлган тенгламалар занжирига келтирилганига ишонч ҳосил қиламиз.

81-§. Учинчи даражали тенгламанинг квадрат радикалларда ечилиш шарти

Теорема. *Ушбу*

$$x^3+ax\;+{}^{h}x+c=0 \qquad (1)$$

рационал коэффициентли учинчи даражали тенглама квадрат радикалда ечилиши учун унинг камида битта илдизи рационал сон бўлиши зарур ва етарли.

Исботи. 1. Етарлилик шарти. $f(x)=x^3+ax^2+bx+c$ кўпҳад d рационал илдизга эга бўлсин. У ҳолда уни қуйидагича ёзамиз: $f(x)=(x-d)(x^2+mx+n)$, бунда $m,\ n\in Q$.

$$1)\ x^2-d^2=0,\ d\in Q=\mathscr{P}_0;$$

$$2)\ \left(x+\frac{m}{2}\right)^2+\left(n-\frac{m^2}{4}\right)=0 \text{ ёки } y^2-\alpha_1=0,\ \alpha_1=\frac{m^2}{4}-n$$

муносабатлар ўринли бўлгани учун (1) тенглама квадрат радикалда ечилади.

2. Зарурийлик шарти. (1) тенглама квадрат радикалда ечилсин ва унинг рационал илдизи йўқ деб фараз қилайлик. Шундай

$$Q=\mathscr{F}_0\subset\mathscr{F}_1\subset\mathscr{F}_2\subset\ldots\subset\mathscr{F}_{k-1}\subset\mathscr{F}_k, \tag{2}$$

квадрат кенгайтмалар занжири мавжудки, у ҳолда (1) тенгламанинг x_1, x_2, x_3 илдизларидан камида биттаси $\mathscr{F}_k/\mathscr{F}_{k-1}$ га тегишли бўлади. Масалан,

$$x_1\in\mathscr{F}_k/\mathscr{F}_{k-1} \tag{3}$$

ва x_1, x_2, x_3 илдизлардан ҳеч бири $\mathscr{F}_{k-1}$ га тегишли эмас, яъни

$$\{x_1,\ x_2,\ x_3\}\cap\mathscr{F}_{k-1}=\varnothing \tag{4}$$

бўлсин деб фараз қилайлик.

$\mathscr{F}_k$ майдон $\mathscr{F}_{k-1}$ майдоннинг квадратик кенгайтмаси бўлгани учун шундай $\alpha\in\mathscr{F}_k/\mathscr{F}_{k-1}$ элемент мавжудки, натижада

$$\mathscr{F}_k=\mathscr{F}_{k-1}(\alpha),\ \alpha\notin\mathscr{F}_{k-1},\ \alpha^2\in\mathscr{F}_{k-1} \tag{5}$$

муносабат бажарилади. (3) ва (5) га асосан,

$$x_1=p+q\alpha,\ (p,\ q\in\mathscr{F}_{k-1},\ q\neq 0) \tag{6}$$

бўлади.

Энди $p-q\alpha$ ифода $f(x)$ кўпҳаднинг илдизи эканини исботлаймиз. Ҳақиқатан,

$$f(p+q\alpha)=(p+q\alpha)^3+a(p+q\alpha)^2+b(p+ \\ +q\alpha)+c=A+B\alpha, \tag{7}$$

бунда

$$\begin{cases} A=f(p)+3pq^2\alpha^2+aq^2\alpha^2, \\ B=3p^2q+q^3\alpha^2+2apq+bq. \end{cases} \tag{8}$$

A, $B\in\mathscr{F}_{k-1}$ ва $\alpha\notin\mathscr{F}_{k-1}$ бўлгани сабабли

$$f(p+q\alpha)=A+B\alpha=0 \tag{9}$$

тенгликдан

$$A=B=0 \tag{10}$$

келиб чиқади. (7), (8), (9) ва $A=B=0$ га кўра $f(p-q\alpha)=A-B\alpha$ тенглик келиб чиқади. Демак, $p-q\alpha$ ҳам $f(x)$ нинг илдизи экан. $x_2=p-q\alpha$ бўлсин. (6) муносабатга асосан $x_1-x_2=2q\alpha\neq 0$ бўлгани учун $x_1\neq x_2$.

Виет формуласига асосан $x_4+x_2+x_8=-a$. (6) га асосан $x_1+x_2=2p\in\mathcal{F}_{k-1}$, $x_3=-a-2p\in\mathcal{F}_{k-1}$. Бу эса (4) фаразга қарама-қарши. Демак, $f(x)$ кўпҳад рационал илдизга эга экан.

82-§. Тенгламасини квадрат радикалларда ечиб бўлмайдиган геометрик масалалар

Баъзи бир геометрик ясашларни бажаришда кўпинча циркуль ва чизғичдан фойдаланилади.

Қуйидаги учта масалани гарчи бошқа ясаш қуроллари ёрдамида бажариш мумкин бўлса-да, лекин фақат чизғич ва циркуль ёрдамида ҳал этиш мумкин эмаслиги масаласи диққатга сазовордир. У масалалар қуйидагилардан иборат:

1. Кубни иккилаш.
2. Бурчакни тенг уч бўлакка бўлиш.
3. Мунтазам еттибурчакни чизиш.

Масалалар. 1. *Ҳажми x га тенг бўлган кубни иккилаш.* Бу масала

$$x^3-2=0 \tag{1}$$

тенгламани квадрат радикалларда ечиш деган сўздир.

(1) тенглама квадрат радикалларда ечилиши учун 77-§ га асосан у даражаси иккидан юқори бўлмаган тенгламалар занжирига келтирилади.

Аввало (1) тенглама рационал сонлар майдони, яъни Q да илдизга эга эмаслигини кўрсатайлик.

Биз бу масаланинг тескарисини фараз қилиб, (1) тенглама Q га тегишли илдизга эга дейлик. У ҳолда x^3-2 кўпҳад Q да иккита кўпайтувчи кўпайтмасига ёйилиб, улардан бири a. $b\in Q$ бўлганда албатта $ax+b$ кўринишга эга бўлар эди. Лекин бундай бўлиши мумкин эмас, чунки x^3-2 кўпҳад рационал сонлар майдони устида келтирилмайдиган кўпҳаддир.

$\mathcal{P}$ майдон сифатида рационал сонлар майдонини олиб, $x^3-2=0$ тенгламага „кенгайтмалар“ мавзусидаги натижани қўллаймиз. Бу натижага кўра $(\mathbf{Q}:Q)$ даража $(Q(\alpha):Q)$ даражага бўлинади. Лекин $(Q(\alpha):Q)=3$. $(\mathbf{Q}:Q)=2^m$ бўлганидан у 3 га бўлинмайди. Демак, кубни иккилаш масаласи квадрат радикалларда ечилмайди ёки бошқача айтганда, кубни фақат циркуль ва чизғич ёрдамида иккита кубга бўлиш мумкин эмас.

2. *Бурчакни учта (тенг) конгруэнт бўлакларга бўлиш.* Бу масаланинг моҳияти шундан иборатки, бурчакни фақат чизғич ва циркуль ёрдамида учта конгруэнт бўлакка бўлиб бўлмайди.

Бу деганимиз ҳар қандай бурчакни ҳам учта конгруэнт бўлакка бўлиш мумкин эмас деган сўз эмас. Шундай бурчаклар борки (масалан 90°, 180°), буларни циркуль ва чизғич ёрдамида учта конгруэнт бўлакка осонгина бўлиш мумкин. Лекин исталган бурчакни учта конгруэнт бўлакка бўлишнинг қатъий усули мавжуд эмас. Ҳозир шу тасдиқни исботлаш билан шуғулланамиз. Бунинг учун қаралаётган масалани алгебраик моҳияти нуқтаи назаридан текширамиз.

Фараз қилайлик, бирор θ бурчакнинг косинуси берилган бўлсин, яъни $\cos\theta=t$ бўлсин. Унда масала $x=\cos\frac{\theta}{3}$ миқдорни ўлчашга келтирилади. Ушбу

$$\cos\theta=4\cos^3\frac{\theta}{3}-3\cos\frac{\theta}{3}$$

тенглама $\cos\theta=t$ берилгани учун

$$4x^3-3x-t=0 \tag{2}$$

кўринишни олади. Қўйилган масалани $\theta=60°$ бурчак учун қараймиз. $\theta=60°$ да (2)

$$8x^3-6x=1 \tag{3}$$

кўринишга эга бўлади.

Мақсадимиз, (3) тенгламанинг бирорта ҳам рационал илдизга эга эмаслигини кўрсатишдан иборатдир. Бу тасдиқнинг тўғрилигини кўрсатиш учун $v=2x$ алмаштириш киритиб, (3) ни

$$v^3-3v=1 \tag{4}$$

шаклга келтириб оламиз.

Фараз қилайлик, $(r;\, s)=1$ бўлганда (4) тенглама $v=\frac{r}{s}$ илдизга эга бўлсин. $v=\frac{r}{s}$ ни (4) га қўйиб,

$$r^3-3s^2r=s^3 \tag{5}$$

га эга бўлар эдик. (5) нинг чап томони r га бўлинади. Иккинчидан, $s^3+3s^2r=r^3$ бўлгани учун $r^3=s^2(s+3r)$

сон s^2 га бўлинади. $(s; r)=1$ бўлгани учун юқоридаги шартлар фақатгина $s=r=\pm 1$ бўлгандагина бажарилади. Демак, $v=\pm 1$ экан. Лекин $v=+1$ ҳам, $v=-1$ ҳам (4) ни қаноатлантирмайди, яъни қарама-қаршиликка учрадик.

Демак, (4) тенгламанинг бирорта илдизи ҳам рационал сонлар майдонига тегишли эмас экан, яъни қўйилган масалани фақатгина циркуль ва чизғич ёрдамида ечиш мумкин эмас экан

3. *Мунтазам еттибурчакни ясаш.* Фараз қилайлик, мунтазам еттибурчак бирлик доира ичида чизилган бўлиб, унинг бир томони узунлиги x бўлсин.

Агар бу етгибурчак учларининг координаталарини $(x; y)$ десак, бу координаталар

$$z^n-1=0 \tag{6}$$

тенгламанинг илдизларидан иборат бўлади. (6) да $z=x+iy$ дир. Биз қараётган ҳол учун $n=7$ бўлади.Демак, (6) тенглама

$$z^7-1=0 \tag{7}$$

кўринишни олади. (7) тенгламанинг битта илдизи $z=1$ бўлгани учун уни

$$\frac{z^7-1}{z-1}=z^6+z^5+z^4+z^3+z^2+z+1 \tag{8}$$

кўринишда ёзиб оламиз. (8) нинг иккала томонини z^3 га бўлиб,

$$z^3+\frac{1}{z^3}+z^2+z+\frac{1}{z}+z=0 \tag{9}$$

ни ҳосил қиламиз. (9) нинг чап томони z ва $\frac{1}{z}$ нинг симметрик функциясидир. Шунинг учун уни асосий симметрик кўпҳадлар, яъни $z+\frac{1}{z}$ ҳамда $z\cdot\frac{1}{z}=1$ лар орқали ифодалай оламиз. У ҳолда ушбу тенглик ҳосил бўлади:

$$\left(z+\frac{1}{z}\right)^3+\left(z+\frac{1}{z}\right)^2-2\left(z+\frac{1}{z}\right)-1=0. \tag{10}$$

Агар (10) тенгликда $1+\frac{1}{z}=y$ десак, у ҳолда (10) дан

$$y^3+y^2-2y-1=0 \tag{11}$$

тенгликни ҳосил қиламиз. Сўнгра

$$z=\cos\varphi+i\sin\varphi \quad \text{ва} \quad \frac{1}{z}=\bar{z}=\cos\varphi-i\sin\varphi$$

лар ўзаро қўшма комплекс сонлардир. Уларни қўшиб,

$$y=z+\frac{1}{z}=2\cos\varphi \qquad (12)$$

ифодани ҳосил қиламиз. Энди, биз y ифодани циркуль ва чизғич билан қура олсак, (12) га асосланиб, $\cos\varphi$ ифодани ҳам қура оламиз ва аксинча. Лекин y ифодани қуриш масаласи (11) тengламанинг бирорта рационал илдизга эга бўлиши масаласи билан боғлиқлигини биз биламиз. Шунинг учун (11) тенгламанинг рационал илдизлари йўқлигини кўрсата олсак кифоя.

Тескарисини фараз қилайлик, яъни шундай r ва s бутун сонлар мавжудки, қисқармайдиган $\frac{r}{s}$ каср (11) нинг илдизи бўлсин. Унда (11) тенглама

$$r^3+r^2s-2rs^2-s^3=0 \qquad (13)$$

кўринишни олади. (13) тенгликни $r^3=s(r^2-2rs-s^2)$ ва $s^3=r(r^2+rs-2s^2)$ каби ёзиб, r^3 нинг s га ва, аксинча, s^3 нинг r га бўлинишига эришамиз. Бундай ҳолат $(r;\ s)=1$ бўлгани учун фақатгина $r=s=\pm1$ бўлганда юз беради. Демак, $y=\frac{r}{s}=\pm1$, $y=\pm1$ сон (11) нинг илдизи экан. Лекин $y=\pm1$ сони (11) нинг илдизи эмаслигини бевосита текшириб билиш мумкин. Бундан эса қилган фаразимизнинг нотўғри эканлиги келиб чиқади, яъни (11) рационал илдизга эга эмас. Демак, мунтазам еттибурчакни фақатгина чизғич ва циркуль ёрдамида чизиш мумкин эмас.

Илова

ИНДЕКСЛАР ЖАДВАЛИ

Туб сон 3

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

Туб сон 5

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

Туб сон 7

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

Туб сон 11

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

Туб сон 13

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

Туб сон 17

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

Туб сон 19

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

Туб сон 23

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

Туб сон 29

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

Туб сон 31

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	9	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

Туб сон 37

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	8	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

Туб сон 41

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	4	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Туб сон 43

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

Туб сон 47

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	9	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

Туб сон 53

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

Туб сон 59

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	39		

Туб сон 61

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	4	19	38	15	30
3	60	59	57	53	45	29	58	65	49	37
4	13	26	52	43	25	50	9	17	34	7
5	14	28	56	51	41	21	42	23	46	31

Туб сон 67

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	4	22	11	58
4	18	53	63	9	61	27	28	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	2	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

Туб сон 71

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	43	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

Туб сон 73

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	15	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

Туб сон 79

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

Туб сон 83

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	6	32	64	45	7	4
1	28	56	29	58	3	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	8	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

Туб сон 89

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	17	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	85	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

Туб сон 97

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	13	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	5	81	17
9	85	37	88	52	66	39				

АДАБИЕТ

Бухштаб А. А. Теория чисел. М., «Просвещение», 1966.

Ван дер Варден Б. Л. Алгебра. М., «Наука», 1979

Виноградов И. М. Основы теории чисел. М., «Наука», 1974.

Виноградов И. М. Сонлар назарияси асослари. Т., «Ўқувпеддавнашр», 1959.

Искандаров Р. И., Назаров Р. Алгебра ва сонлар назарияси, I қисм, Т., «Ўқитувчи», 1977.

Искандаров Р. И., Назаров Р. Алгебра ва сонлар назарияси, II қисм, Т., «Ўқитувчи», 1979.

Қалужнин Л. А. Введение о общую алгебру. М., «Наука», 1973.

Қоган Л. А., Тошпўлатов Б. Т., Файзиев С. Р. Представление чисел квадратными формами. Т., «Фан», 1980.

Қоган Л. А., Тошпўлатов Б. Т., Дусумбетов А. Д. Представление чисел квадратными формами. Т., «Фан», 1989.

Қострикин А. И. Введение в алгебру. М., «Наука», 1977.

Қострикин А. И., Манин Ю. И. Линейная алгебра и геометрия. Изд. МГУ, 1980.

Қуликов Л. Я. Алгебра и теория чисел. М., «Высшая школа», 1979.

Қурош А. Г. Олий алгебра курси. Т., «Ўқитувчиси». 1976.

Ляпин Е. С., Евсеев А. Е. Алгебра и теория чисел. М., «Просвещение», ч. II, 1978.

Мальцев А. И. Основы линейной алгебры. М., «Наука», 1970.

Нечаев В. И. Числовые системы. М., «Просвещение», 1975.

Окунев Л. Я. Высшая алгебра. Изд. 2 М., «Просвещение», 1966.

Постников М. М. Теория Галуа. М., «Физматгиз», 1963.

Прахар Қ. Распределение простых чисел, М., «Мир», 1967.

Проскуряков И. В. Сборник задач по линейной алгебре. М., «Наука», 1974.

Скорняков Л. А. Элементы алгебры. М., «Наука», 1980.

Фаддеев Д. Қ. Лекции по алгебре. М., «Наука», 1984.

Фаддеев Д. Қ., Соминиский И. С. Сборник задач по высшей алгебре. М., «Наука», 1977.

Феферман С. Ф., Числовые системы. М., «Наука», 1971.

Шнеперман Л. Б. Қурс алгебры и теории чисел в задачах и упражнениях. Минск, «Вышейшая школа», ч. I, 1986.

МУНДАРИЖА

I боб. Бутун сонлар ҳалқасида бўлиниш назарияси

II боб. Таққосламалар назариясининг арифметикага татбиқи

Назаров Расул,
Тошпӯлатов Баҳодир Тошпӯлатович,
Дусумбетов Абдулла

АЛГЕБРА ВА СОНЛАР НАЗАРИЯСИ

II ҚИСМ

Педагогика институтлари ва университетларининг
математика факультетлари талабалари учун
ӯқув қӯлланма

Тошкент «Ӯқитувчи» 1995

Таҳририят мудири **М. Пӯлатов**
Муҳаррирлар: **У. Ҳусанов, Н. Ғоипов**
Расмлар муҳаррири **Т. Қаноатов**
Тех. муҳаррирлар **Н. Винникова, Т. Золотилова**
Мусаҳҳиҳа **М. Иброҳимова**

ИБ № 6432

Теришга берилди 26.04.94. Босишга рухсат этилди. 20.06.95. Бичими 84×108/32. Литературная гарнитураси. Юқори босма усулида босилди. Шартли б. т. 14,28. Нашр т. 12,98. Шартли кр.-отт. 14,49. Нусхаси 7000. Буюртма 980.

«Ӯқитувчи» нашриёти. 700129 Тошкент, Навоий кӯчаси, 30. Шартнома 09-34-93.

Область газеталарининг М. В. Морозов номидаги босмахонаси ва бирлашган нашриёти. Самарқанд, У. Турсунов кӯчаси, 82. 1995.

Н 12

Назаров Р. ва бошқ.

Алгебра ва сонлар назарияси: Пед. ин-ти ва ун-тлар учун дарслик. II қ. Р. Назаров, Б. Тошпўлатов, А. Дусумбетов.—Т.: Ўқитувчи, 1995.—272 б.

1. 1,2 Автордош.

22.132Я73.

Ҳурматли муаллимлар!
Азиз ўқувчилар!

«Ўқитувчи» нашриёти 1995 йилда Сизга атаб қуйидаги дарслик ва ўқув қўлланмаларни чоп этади

Математика:

1. А. Абдуқодиров ва б. Информатика ва ҳисоблаш техникаси асослари.
   9- синф учун дарслик.
2. Н. Дадахўжаева. Математика.
   Заиф эшитувчи мактабларининг 2- синфи учун дарслик.
3. Б. Омонов. Юз билан юзма-юз.
   Кичик ёшдаги мактаб ўқувчилари учун қўлланма.
4. А. Сатторов ва б. Информатика ва ҳисоблаш техникаси асослари.
   Педагогика институтлари талабалари учун қўлланма.
5. Т. Шарипова ва б. Математик анализдан мисол ва масалалар.
   Педагогика институтлари ва университетлари талабалари учун қўлланма.
6. Р. Иброҳимов ва б. Математикадан масалалар тўплами.
   Юқори синф ўқувчилари учун қўлланма.
7. А. Раҳимқориев. Трансцендент тенгсизликларни график усулда ечиш..
   Ўқитувчилар учун қўлланма
8. А. Ҳикматов. Модулли ифодалар.
   Ўқитувчилар учун қўлланма.
9. А. Тоҳиров ва б. Математикадан олимпиада масалалари.
   Битирувчи синфлари ўқувчилари ва олий ўқув юртларига кирувчилар учун қўлланма.

Физика:

1. А. Бойдадаев. Табиат кучлари.
   Ўқувчилар ва талабалар учун қўлланма.
2. А. Юсупов ва б. Физикадан масалалар тўплами.
   Ҳунар техника билим юртлари талабалари учун қўлланма.
3. Ҳ. Абдувоҳидов ва б. Амалий физика.
   Педагогика институтлари талабалари учун қўлланма.

4. С. Турсунов ва б. Умумий физика курси.

Педагогика институтлари талабалари учун қўлланма.

5. М. Раҳматуллаев. Умумий физика курси. Механика.

Педагогика институтлари ва университетлари талабалари учун қўлланма.

6. М. Ўлмасова ва б. Физикадан практикум.

Педагогика институтлари талабалари учун қўлланма.

7. Т. Азимов ва б. Электромагнитизм ҳақида таълимот.

Педагогика институтлари ва университетлари талабалари учун қўлланма.

8. Ҳ. Хошимов ва б. Квант механикаси асослари.

Педагогика институтлари ва университетлари талабалари учун қўлланма.

9. А. Юсупов. Физикадан синфдан ташқари машғулотлар.

7—9-синф ўқувчилари учун қўлланма.

10. Т. Сафаева. Физикадан табақалаштирилган фронтал лаборатория ишлари.

7—9-синф ўқувчилари учун қўлланма.

11. Хайрутдинов ва б. Гелиотехника элементлари.

Ўқувчилар учун қўлланма.

12. Ч. Бердиев. Физика ўқитиш.

Ўқитувчилар учун қўлланма.

13. А. Аҳмедов ва б. Физикадан масалалар тўплами.

Олий ўқув юртларига кирувчилар учун қўлланма.

14. Р. Бекжонов. Ядро физикаси ва зарралар.

Педагогика институтлари ва университетлари талабалари учун қўлланма.