



تنگرهار ساينس پوهنځی

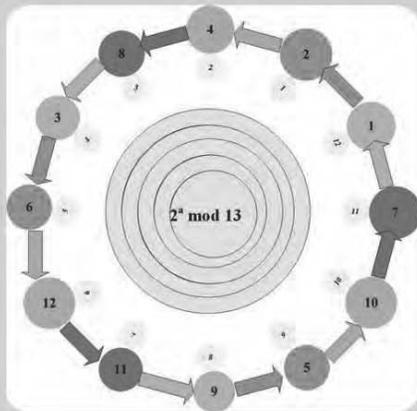


Nangarhar Science Faculty

Afghan

الجبر او د عددونو تيوري

دوهمه برخه



الجبر او د عددونو تيوري - دوهمه برخه

Algebra & Theory of Numbers Part II

Sultan Ahmad Niazman

Algebra & Theory of Numbers Part II



Funded by



Konrad Adenauer Stiftung

ISBN 978-9936-620-50-6



9 789936 620506



سلطان احمد نيازمن
۱۳۹۶

سلطان احمد نيازمن

۱۳۹۶

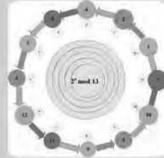
د کونراډ اډناور

Not for Sale

2017

الجبر او د عددونو تيوري دوهمه برخه

افغانیک
Afghanic



Pashto PDF
2017

سلطان احمد نيازمن



مېرکېلېو سولنډر فونډ
مركز فار انجمنين او علمي

Funded by
Konrad Adenauer Stiftung (KAS)

Algebra & Theory of Numbers Part II

Sultan Ahmad Niazman

Download:
www.ecampus-afghanistan.org

بسم الله الرحمن الرحيم

الجبر او د عددونو تيوري دوهمه برخه

سلطان احمد نيازم

نومې چاپ

دغه کتاب په پي ډي ايف فارمټ کې په مله سي ډي کې هم لوستلی شئ:



| | |
|------------|--------------------------------------|
| د کتاب نوم | الجبر او د عددونو تیوري (دوهمه برخه) |
| لیکوال | سلطان احمد نیازمن |
| خپرنډوی | ننګرهار پوهنتون، ساینس پوهنځی |
| وېب پاڼه | www.nu.edu.af |
| د چاپ کال | ۱۳۹۶، لومړی چاپ |
| چاپ شمېر | ۱۰۰۰ |
| مسلسل نمبر | ۲۵۶ |
| ډاونلوډ | www.ecampus-afghanistan.org |
| چاپ ځای | سهر مطبعه، کابل، افغانستان |



دا کتاب د کانراډ ادناور (KAS) لخوا تمویل شوی دی. اداري او تخنیکي چارې یې په آلمان کې د افغانیک لخوا ترسره شوي دي. د کتاب د محتوا او لیکنې مسؤلیت د کتاب په لیکوال او اړونده پوهنځي پورې اړه لري. مرسته کوونکي او تطبیق کوونکي ټولني په دې اړه مسؤلیت نه لري.

د تدریسي کتابونو د چاپولو لپاره له مور سره اړیکه ونیسئ:
ډاکتر یحیی وردک، د لوړو زده کړو وزارت، کابل
تېلیفون ۰۷۵۶۰۱۴۶۴۰
ایمېل textbooks@afghanic.de

د چاپ ټول حقوق له مؤلف سره خوندي دي.

ای اس بی ان ۶-۵۰-۶۲۰-۹۹۳۶-۹۷۸

د لوړو زده کړو وزارت پیغام



د بشر د تاریخ په مختلفو دورو کې کتاب د علم او پوهې په لاسته راوړلو، ساتلو او خپرولو کې ډیر مهم رول لوبولی دی. درسي کتاب د نصاب اساسي برخه جوړوي چې د زده کړې د کیفیت په لوړولو کې مهم ارزښت لري. له همدې امله د نړیوالو پیژندل شویو معیارونو، د وخت د غوښتنو او د ټولني د اړتیاوو په نظر کې نیولو سره باید نوي درسي مواد او کتابونه د محصلینو لپاره برابر او چاپ شي.

له ښاغلو استادانو او لیکوالانو څخه د زړه له کومي مننه کوم چې دوامداره زیار یې ایستلی او د کلونو په اوږدو کې یې په خپلو اړوندو څانگو کې درسي کتابونه تألیف او ژباړلي دي، خپل ملي پور یې اداء کړی دی او د پوهې موتور یې په حرکت راوستی دی. له نورو ښاغلو استادانو او پوهانو څخه هم په درنښت غوښتنه کوم تر څو په خپلو اړوندو برخو کې نوي درسي کتابونه او درسي مواد برابر او چاپ کړي، چې له چاپ وروسته د گرانو محصلینو په واک کې ورکړل شي او د زده کړو د کیفیت په لوړولو او د علمي پروسې په پرمختگ کې یې ښکې گام اخیستی وي.

د لوړو زده کړو وزارت دا خپله دنده بولي چې د گرانو محصلینو د علمي سطحې د لوړولو لپاره د علومو په مختلفو رشتو کې معیاري او نوي درسي مواد برابر او چاپ کړي. په پای کې له کانراډ ادناور بیسټ (KAS) او زموږ همکار ډاکتر یحیی وردک څخه مننه کوم چې د دی کتاب د خپرولو لپاره یې زمینه برابره کړې ده.

هیله منده یم چې نوموړې گټوره پروسه دوام وکړي او پراختیا ومومي تر څو په نږدې راتلونکې کې د هر درسي مضمون لپاره لږ تر لږه یو معیاري درسي کتاب ولرو.

په درنښت

پوهنمل دوکتور نجیب الله خواجه عمری

د لوړو زده کړو وزیر

کابل، ۱۳۹۶

د درسي کتابونو چاپول

قدرمنو استادانو او گرانو محصلينو!

د افغانستان په پوهنتونونو کې د درسي کتابونو کموالی او نشتوالی له لویو ستونزو څخه گڼل کېږي. یو زیات شمیر استادان او محصلین نویو معلوماتو ته لاس رسی نه لري، په زاړه میتود تدریس کوي او له هغو کتابونو او چپترونو څخه گټه اخلي چې زاړه دي او په بازار کې په ټیټ کیفیت فوتوکاپي کېږي.

تر اوسه پورې موږ د ننگرهار، خوست، کندهار، هرات، بلخ، البیروني، کابل، کابل طبي پوهنتون او کابل پولي تخنیک پوهنتون لپاره ۲۵۸ عنوانه مختلف درسي کتابونه د طب، وترینری، فارمسی، روانشناسی، ساینس، انجنیري، اقتصاد، ژورنالیزم او زراعت پوهنځیو (۹۶ طبي د آلمان د علمي همکاریو ټولني DAAD، ۱۴۰ طبي او غیر طبي د افغان ماشومانو لپاره د جرمني کمپني Kinderhilfe-Afghanistan، ۷ کتابونه د آلماني او افغاني پوهنتونونو ټولني DAUC، ۲ کتابونه په مزار شریف کې د آلمان فدرال جمهوري جنرال کنسولگری، ۲ کتابونه د Afghanistan-Schulen، ۱ د صافی بنسټ لخوا، ۱ د سلواک اېډ او ۸ نور کتابونه د کانراډ اډناور بنسټ) په مالي مرسته چاپ کړي دي.

د یادونې وړ ده، چې نوموړي چاپ شوي کتابونه د هېواد ټولو اړونده پوهنتونونو او یو زیات شمېر ادارو او مؤسساتو ته په وړیا توگه وپشل شوي دي. ټول چاپ شوي کتابونه له www.afghanistan-ecampus.org ویب پاڼې څخه ډاډولود کولای شئ.

دا کړنې په داسې حال کې تر سره کېږي چې د افغانستان د لوړو زده کړو وزارت د (۲۰۱۰-۲۰۱۴) کلونو په ملي ستراتیژیک پلان کې راغلي دي چې:

"د لوړو زده کړو او د ښوونې د ښه کیفیت او زده کوونکو ته د نویو، کره او علمي معلوماتو د برابرولو لپاره اړینه ده چې په دري او پښتو ژبو د درسي کتابونو د لیکلو فرصت برابر شي د تعلیمي نصاب د ریفورم لپاره له انگریزي ژبې څخه دري او پښتو ژبو ته د کتابونو او درسي موادو ژباړل اړین دي، له دې امکاناتو څخه پرته د پوهنتونونو محصلین او استادان نشي کولای عصري، نویو، تازه او کره معلوماتو ته لاس رسی پیدا کړي."

مونږ غواړو چې د درسي کتابونو په برابرولو سره د هیواد له پوهنتونونو سره مرسته وکړو او د چپتر او لکچر نوټ دوران ته د پای ټکی کېږدو. د دې لپاره دا اړینه ده چې د لوړو زده کړو د موسساتو لپاره هر کال څه نا څه ۱۰۰ عنوانه درسي کتابونه چاپ شي.

له ټولو محترموا استادانو څخه هيله کوو، چې په خپلو مسلکي برخو کې نوي کتابونه وليکي، وژباړي او يا هم خپل پخواني ليکل شوي کتابونه، لکچر نوټونه او چپټرونه ايډېټ او د چاپ لپاره تيار کړي، زموږ په واک کې يې راکړي چې په نښه کيفيت چاپ او وروسته يې د اړوند پوهنځيو، استادانو او محصلينو په واک کې ورکړو. همدارنگه د ياد شويو ټکو په اړوند خپل وړاندیزونه او نظريات له مونږ سره شريک کړي، تر څو په گډه پدې برخه کې اغيزمن گامونه پورته کړو.

د مؤلفينو او خپروونکو له خوا پوره زيار ايستل شوی دی، ترڅو د کتابونو محتويات د نړيوالو علمي معيارونو په اساس برابر شي، خو بيا هم کيدای شي د کتاب په محتوی کې ځينې تيروتنې او ستونزې وليدل شي، نو له درنو لوستونکو څخه هيله مند يو تر څو خپل نظريات او نيوکې مؤلف او يا مونږ ته په ليکلې بڼه راوليږي، تر څو په راتلونکي چاپ کې اصلاح شي.

له کانراډ ادناور بنسټ (KAS) څخه ډېره مننه کوو چې د دغه کتاب د چاپ لگښت يې ورکړی دی، دوی تر دې مهاله ۸ عنوانه درسي کتابونو د چاپ لگښت پر غاړه اخيستی دی.

په ځانگړې توگه د جي آی زيت (GIZ) له دفتر او CIM (Center for International Migration & Development) څخه، چې زما لپاره يې له ۲۰۱۰ نه تر ۲۰۱۶ پورې په افغانستان کې د کار امکانات برابر کړي وو، هم د زړه له کومې مننه کوم.

د لوړو زده کړو له وزير پوهنمل دوکتور نجيب الله خواجه عمری، علمي معين پوهنمل ديپلوم انجنير عبدالتواب بالاكرزی، مالي او اداري معين ډاکتر احمد سير مهجور، مالي او اداري رئيس احمد طارق صديقي، په لوړو زده کړو وزارت کې سلاکار ډاکتر گل رحيم صافي، د پوهنتونونو رئيسانو، د پوهنځيو رييسانو او استادانو څخه مننه کوم چې د کتابونو د چاپ لړۍ يې هڅولې او مرسته يې ورسره کړې ده. د دغه کتاب له مؤلف څخه ډېر منندوی يم او ستاينه يې کوم، چې خپل د کلونو-کلونو زيار يې په وړيا توگه گرانو محصلينو ته وړاندې کړ.

همدارنگه د دفتر له همکارانو هر يو حکمت الله عزيز، فهيم حبيبي او ډاکتر نيسم خوگياڼی څخه هم مننه کوم چې د کتابونو د چاپ په برخه کې يې نه ستړې کيدونکې هلې ځلې کړې دي.

ډاکتر يحيی وردک، د لوړو زده کړو وزارت سلاکار

کابل، دسمبر ۲۰۱۷

د دفتر ټيليفون: ۰۷۵۶۰۱۴۶۴۰

ايميل: textbooks@afghanic.de

فهرست

| | |
|----|------------------------------------------------------------------------------------------|
| i | فهرست |
| iv | سریزه |
| 6 | تقریظ |
| 1 | لمری فصل |
| 1 | گروپ (Group) |
| 1 | I§ د گروپ (Group) بیل بیل تعریفونه |
| 7 | |
| 9 | II§ سبگروپ - دورانی (خرخنده) گروپونه |
| 13 | III§ دگروپو تجزیه په سبگروپونو - د لاگرانژ قضیه |
| 17 | IV§ د گروپ نارمل وپشونکي او د گروپ تجزیه (Factor Group) |
| 19 | V§ د گروپو ورته والي هومومورفیزم Homomorphism |
| 23 | دوهم فصل |
| 23 | رینگ (کری) |
| 23 | I§ رینگ - سب رینگ |
| 25 | II§ د رینگ ساده خاصیتونه |
| 28 | III§ آیديال رینگ او پر هغه باندی عملی |
| 29 | IV§ د رینگ تجزیه (Factor Ring) |
| 31 | V§ د رینگو ورته والي (هومومورفیزم Homomorphism) |
| 34 | دریم فصل |
| 34 | د تامو عددو په رینگ (کری) کی د وپش د ورتوب تیوری |
| 34 | I§ د وپش د ورتوب اریکه او دهغه ساده خاصیتونه |
| 37 | II§ نیمگری وپش (نا مکمل وپش) |
| 39 | III§ لوی ترین مشترک وپشونکی (قاسم) او د هغه خاصیتونه - د اقلیدس الگوریتم |
| 44 | VI§ نسبت یو او بل ته اولیه (متباین) عددونه (Relatively Primes) او دهغوی خاصیتونه ... |
| 47 | V§ کوچنی ترین مشترک مضرب او د هغه ارتباط د لوی ترین مشترک وپشونکی سره |
| 49 | VI§ اولیه عددونه او دهغوی ترتیب د طبیعی عددو په لاری - د ایراتوستینس غلییل |
| 52 | VII§ د اولیه عددو د حاصل ضرب په شکل د مرکبو عددو تجزیه |
| 55 | VIII§ د شمېرنی سیستمونه ، د g پر قاعده باندی د شمېرنی په سیستم کی د طبیعی عددونو ارائه |

| | | |
|-------|-------------------------------------------------------------------------------|-----|
| IX§ | د عددو په سیستماتیکه ارائه کی حسابی عملی | 59 |
| X§ | د عددو اړول دشمبرني د یوه سیستم څخه دشمبرني و بل سیستم ته | 62 |
| | څلرم فصل | 66 |
| | د مقایساتو (پرتلی) تیوری | 66 |
| I§ | د کانگروینسی اړیکه د تامو عددو په رینگ کی او د هغه ساده خاصیتونه | 66 |
| II§ | د تامو عددو دوپش د ورتوب عمومی معیارونه | 69 |
| III§ | د باقیمانده وو د تولگیو رینگ - د باقیمانده وو کامل سیستم | 72 |
| V§ | د اویلر تابع - د اویلر او فرما قضیې | 76 |
| VI§ | یو مجهوله لمړی درجه کانگروینسی - د هغوی د حل موجودیت او تعداد | 80 |
| VII§ | د لمړی درجی کانگروینسی د حل طریقې | 83 |
| VIII§ | د راکره سوی مودول پر اساس د عدد او د باقیمانده و د تولگی ترتیب - مؤلد جذرونه | 85 |
| IX§ | د اولیه مودول پر اساس اندکسونه او د هغوی خاصیتونه | 88 |
| X§ | د عام کسر اړول په اعشاریه کسر باندی او په اعشاریه کسر کی د تکراری رقمو تعینول | 91 |
| XI§ | د عددونو د تیوری عملی بیلگی | 94 |
| | پنځم فصل | 98 |
| | یو متحوله پولینوم | 98 |
| I§ | د عددونو پر فیلا باندی د یو متحوله پولینومو رینگ | 98 |
| II§ | د پولینومو څېړنه د تابع په څېر | 102 |
| III§ | د پولینومو نامکمل وېش | 106 |
| IV§ | د پولینومو وېش د $g(x)=x-a$ پر باینوم (دوه حدیزه) باندی | 110 |
| V§ | د پولینومو دوپش ورتوب | 113 |
| VI§ | د پولینومو لوی ترین مشترک وېشونکی او د اقلیدس الگوریتم | 114 |
| VII§ | د پولینومو د لوی ترین مشترک وېشونکی خطی ارائه (خطی څرگندونه) | 118 |
| VIII§ | نسبت یو اویل ته اولیه (متبائن) پولینومونه | 120 |
| IX§ | د پولینومو کوچنی ترین مشترک مضرب | 122 |
| X§ | نه تجزیه کیدونکی پولینومونه Irreducible polynoms او د هغوی خاصیتونه | 123 |
| XI§ | د پولینومو تجزیه په نه تجزیه کیدونکو ضربی عاملو باندی | 125 |
| XII§ | د پولینومو مشتق او دهغه خاصیتونه | 127 |
| XIII§ | د پولینوم جذرونه | 130 |
| XIV§ | د پولینوم مضاعف ضربی عاملونه | 133 |
| VX§ | یو متحوله پولینومونه پر اختیاری فیلا باندی - د پولینوم د تجزیې فیلا | 138 |

| | |
|-----|------------------------------------------------------------------------------------|
| 141 | شپږم فصل..... |
| 141 | څو متحولې پولینومونه..... |
| 141 | I§. پر عددی فیله باندي د n متحولې پولینومو رینګ..... |
| 147 | II§. د n متحولې پولینوم د حدونو قاموسی (الفبایي Lexicographic) ترتیب..... |
| 149 | III§. د n متحولې پولینومو دوېش ورتوب..... |
| 150 | IV§. متناظر پولینومونه او د هغوی خاصیتونه..... |
| 153 | V§. د متناظرو پولینومو د تیوری اساسی قضیه..... |
| 156 | اووم فصل..... |
| 156 | د مختلطو او حقیقی عددو پر فیله باندي پولینومونه..... |
| 156 | I§. د مختلطو عددو پر فیله باندي یو متحولې پولینومونه او د مطلقه قیمت خاصیتونه..... |
| 159 | II§. د پولینومو د الجبر اساسی قضیه..... |
| 164 | III§. د پولینومو تجزیه په خطی ضربی عاملو باندي – د وینا قضیه..... |
| 167 | IV§. د حقیقی عددو د ضربیو سره د پولینومو د مختلطو جذرو خاصیتونه..... |
| 169 | V§. د دریمی درجې معادلو حل..... |
| 174 | VI§. د څلرمې درجې معادلو حل..... |
| 178 | VII§. د حقیقی ضربیو سره د پولینومو د حقیقی جذرو سرحد..... |
| 181 | VIII§. د شتورم (Charles-Francois Sturm) په طریقې د پولینوم د جذرو تعینول..... |
| 187 | اتم فصل..... |
| 187 | د نسبتي عددو پر فیله باندي پولینومونه - الجبری عددونه..... |
| 187 | I§. د تامو عددو د ضربیو سره د پولینوموتام او نسبتي جذرونه..... |
| 191 | II§. دپولینومودنه تجزیه کېدو معیار(د آیزنشتاین معیار)..... |
| 195 | III§. الجبری او ترانسندنټ عددونه..... |
| 198 | IV§. د فیله ساده الجبری توسعه(پراختیا) او دهغه د جوړښت طریقې..... |
| 201 | اندکس..... |
| 204 | ماخذ..... |

سریزه

د الجبر او د عددونو تیوری د کتاب دوهمه برخه د ننګرهار د پوهنتون د طبیعی علومو د پوهنځي د محصلینو دپاره پېشنهاد سویده ، چي محتوی یې د تدریس د دریم څخه تر پنځم سمستر ضرورت پوره کوی.

دغه کتاب د الجبر او عددونو تیوری د لمړی برخي په ادامه لیکل سوی دی او اته فصله لری. په لمړیو دوو فصلونو کی د الجبری ساختمانو اساسی مفهومیونه لکه گروپ، اورینگ چي په لمړی برخه کی یې لنډه یادونه سوی وه، په تفصیل سره څېړل سوی دی. دریم او څلرم فصلونه تامو عددو ته وقف سویدی . پدی فصلو کی د تامو عددو د ویش د ورتوب ، د عددو تجزیه په اولیه ضریبی عاملو باندی او د طبیعی عددو دپاره د شمېرني مختلف سیستمونه په جزئیاتو سره څېړل سوی دی . په څلرم فصل کی د تامو عددو د کانگروینسی تیوری په تفصیل سره څېړل سویده. د فصل په پای کی په اوسنی ژوند کی د عددونو د تیوری عملی بېلګی لکه د لس ځانیزه ISBN نمری شمېرل چي د کتابو د په نښه کولو بین المللی معیار دی او د معلوماتو د قفلولو ساده بېلګه راوړه سوی ده ، څو محصلین ریاضی ته په عمومی ډول او الجبرته په خاص ډول نه د یوه وچ د فورمولونو د مجموعی په صفت بلکه په عملی ژوند کی د عملی پرابلمو د حل دپاره د ضروری وسیلی په حیث وگوری.

وروستی څلور فصلونه د پولینومونو و تیوری ته وقف سوی دی . هغه هم پداسی ډول چي په پنځم فصل کی پر اختیاری فیله باندی د یو متحوله پولینومونو عمومی تیوری راوړه سوی ده. پدی فصل کی پولینومونه د تامو عددو د رینگ په اړوند تشریح سویدی او تامو عددو ته ورته د پولینومونو خاصیتونه توضیح سوی دی. په شپږم فصل څو متحوله پولینومونه مطالعه سوی او د متناظرو پولینومو د تیوری اساسی قضیه ثابتته سوی ده.

وروستی دوه فصله د پنځم فصل موضوع گانې پر مشخصو عددی ، لکه د مختلطو، حقیقی او نسبتي عددو پر فیله باندی په مشخص ډول مطالعه کوی. د پولینومو د تیوری اساسی قضیه په اووم فصل کی ثبوت او د هغه نتیجی تشریح سوی دی. علاوه پردی پر عددی فیله باندی په مختلفو درجو باندی د پولینومو د جذرو مسنالی ته په کافی اندازه پاملرنه سوی ده. الجبري او ترانسندنت عددو د مفهومیو په تشریح باندی کتاب پای ته رسیری.

په کتاب کی د تجربی په شکل ځنی اصطلاحات په دوو مختلفو کلمو افاده سوی دی ، د بېلګی په توگه د عددو لار او ترادف او یا د عددی فیله وسعت او عددی فیله پراختیا په عین مفهوم سره استعمال سوی دی، دلته موخه داده چي لوستونکی د زده کولو پر ځای و فکر کولو ته و هڅول سی.

هڅه می کړیده چي د تېروتنو مخه ونیسیم ، خو بیا هم چي گران لوستونکی کوم تکی ته څیر سی ، هیله ده چي خپل وړاندیز زما ددغی موخی دپاره د الکترونیکی لیک پر پته math@niazman.de راولیری. د غلطیو نیولیک به زما په وېبپاڼه www.niazman.de کی خپره سی.

د کتاب د چاپولو په برخه کی دیناغلی ډاکتر صاحب یحیی وردگ هلی ځلی د ستاینی وړ او وړ څخه پیره مننه کوم . زما د زړه له کومی او خاصه مننه او درناوی ډاکتر صاحب ایروز Dr. Erös او دهغه خیریه ټولنی ته ، نه یوازی پدی خاطر چي ددی کتاب د چاپولو لگښت یې پر غاړه اخیستی دی ، بلکه هغه خدمتونه چي دوی د جنگ په کلو او تر هغه وروسته د افغانستان د ځوان نسل دپاره کړیدی ، وړاندی کوم .

سلطان احمد نیازمن

اکتوبر ۲۰۱۷

لمری فصل گروپ (Group)

I§. د گروپ (Group) بیل بیل تعریفونه.

د گروپ د تعریف سره د لمړی ځل د پاره د الجبر او عددونو د نظریې د لمړی برخې ، د دوهم فصل په §III کی مخامخ سو. هلته مو د گروپ څو بیلگی راوړی. و مو وپل چې د مختلطو عددو سیټ نظر د جمعی و عملیې ته گروپ دی، همدا ډول د یوه عدد π - ام درجه جذرو سیټ نظر د ضرب و عملیې ته گروپ دی، د وکتوری فضاء د ټولو وکتورو سټ نظر د وکتورو د جمعی و عملیې ته ، د ټولو n - مرتبه ئی ماترکسو سټ د نظر د ماترکسو د جمعی د عملیې او د ټولو غیرسنگولار non-singular ماترکسو سټ نظر د ماترکسو د ضرب و عملیې ته ، گروپ تشکیلوی.

د گروپونو نور بیلگی غیر له ریاضی څخه په کیمیا، فزیک ، کرسټالوگرافی او نورو علومو کی هم موندلای سو.

د گروپ تیوری چې بنسټ یی د نولسمی پیری په ۳۰ کلوکی د فرانسوی ریاضی پوه گالوا Galios په ذریعه ایښودل سویدی ، نن ورځ د الجبر د کلاسیکو نظریو په قطار کی شمېرل کیږی.

پدی فصل کی کی به د گروپونو د نظریې اساسی مفهومونه او دهغوی ساده خاصیتونه ، چې د هغه پیژندنی ته د ریاضی هر ښونکی اړ دی، مطالعه کړو. د نوموړو خاصیتو څخه به ددی کتاب په نورو فصلو کی هم کار واخلو.

د گروپ په هکله د دی کتاب د لمړی برخې لندونه دلته راوړو:

تعریف ۱ - د G سیټ چې خالی نه وی، او پر هغه باندی د "*" عملیه ، یعنی

$\langle G, * \rangle$ د گروپ به نامه یادیږی، که لاندنی شرطونه صدق وکی:

$$1. (\forall x, y, z \in G)((x * y) * z = x * (y * z))$$

یعنی د "*" عملیه د G پر سیټ اتحادی خاصیت لری.

$$2. (\exists e \in G)(\forall a \in G)(a * e = e * a = a)$$

یعنی د G په سیټ کی بی اغیزی Neutral عنصر وجود لری.

$$3. (\forall x \in G)(\exists y \in G)(x * y = y * x = e)$$

یعنی د G د سیټ د هر عنصر $x \in G$ دپاره د G په سیټ کی متضاد عنصر $y \in G$ وجود لری.

که په گروپ کی راکړه سوی عملیه د جمعی عملیه "+" وی ، نو گروپ د جمعی او که د ضرب عملیه " ." وی ، نو گروپ د ضربی گروپ په نامه یادیږی.

مخکی مو ثابتہ کړه چې په گروپ کی یوازنی بی اغیزی عنصر وجود لری. په جمعی گروپ کی بی اغیزی عنصر صفر دی چې په 0 سره ښیو، او په ضربی گروپ کی بی اغیزی عنصر یو دی چې په 1 سره یی ښیو. بر سیره پردی ثابتہ موکړه چې د G په سیټ کی د هر عنصر دپاره یوازنی متضاد عنصر وجود لری. په جمعی گروپ کی د g د عنصر متضاد عنصر په $-g$ سره ښیو چې د g د عنصر په متضاد سره نوموو. په ضربی گروپ کی د g د عنصر متضاد عنصر په g^{-1} سره ښیو چې د g د عنصر په معکوس سره یی نوموو.

که د "*" عملیه د G پر سیټ تبدیلی خاصیت هم ولری ، یعنی :

$$(\forall x, y \in G)(x * y = y * x)$$

نو د G گروپ د تبدیلی گروپ یا د آبل $Abel$ ¹ د گروپ په نامه یادېږي.

د تامو عددو \mathbb{Z} جمعې گروپ، د ناطقو عددو \mathbb{Q} ضربې گروپ، د یوه د عدد n - ام جذر ضربې گروپ (د لمړي ټوک د دوهم فصل پای وگورئ)، د مختلطو عددو پر ډگر باندې د n - ام ترتیب مربعي ماترکسو جمعې گروپ د تبدیلی گروپو بیلگې دي. په آسانی سره آزمویل کېدای سې چې د $A = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ سیټ نظر د \oplus عمليې ته چې د کیلي (لمړي ټوک، دوهم فصل، $I\&$ وگورئ) د لاندني جدول په ذریعه راکړه سوی وی، هم تبدیلی گروپ دی.

| | | | | |
|-----------|-----------|-----------|-----------|-----------|
| \oplus | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

د G گروپ د متناهی (غیرمتناهی) په نامه یادېږي، که د G سیټ متناهی (غیر متناهی) وي. د G د سیټ د عنصر و شمېر د G د گروپ په ترتیب سره یادېږي.

د بیلگې په توگه زموږ پاسني گروپ $A = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ متناهی دی او ترتیب یې ۴ دی. د یوه عدد د مربع جذر $G = \{-1, 1\}$ یو ضربې گروپ او ترتیب یې هم ۲ دی؛ خو د تامو عددو \mathbb{Z} جمعې گروپ غیرمتناهی گروپ دی.

اکثراً قبول سویدی چې د گروپ په تیوري کې د ضرب د عمليې څخه د دوه نيزی عمليې په صفت کار اخلي. په راتلونکي کې به موږ هم ددغه تړون پیروي کوو.

په ریاضی کې ډیر مفهومونه دی چې په بیلا بیلو ډولونو سره معادلو څیرو تعریف سویدی، دبیلگې په توگه که د بنونځي د ریاضی کتابونه وگورو، نو په هغه کې به د ناصف الزاویې لاندني تعریفونه وموندو:

- ناصف الزاویه عبارت دی له هغه مستقیمې کرني څخه چې د زاویې د رأس څخه تېرېږي او زاویه پر دوه مساوی برخو وېشي.

- ناصف الزاویه د یوې زاویې د تناظر د محور څخه عبارت دی.

- ناصف الزاویه په مستوی کې د هغو هندسي نقطو د ځای څخه عبارت دی چې د زاویې د ضلعو څخه مساوی فاصله ولري.

د یوه مفهوم د بیلا بیلو معادلو تعریفو څخه مو موخه داده چې د مختلفو مسئلو په څېرلو کې د کار د آسانی دپاره د مختلفو تعریفو څخه کار واخیستلای سو. د گروپ مفهوم هم په بیلا بیلو توگه تعریفولای سو.

تعریف ۲- د G غیر خالی سیټ او پر هغه باندې د ضرب ددوه نيزی عمليې سره د گروپ په نامه یادېږي، که:

۱- د G پر سیټ راکړه سوی دوه نيزه عمليه اتحادی خاصیت ولري.

۲- د G په سیټ کې د $ax=b$ او $ya=b$ په شکل معادلی د G د سیټ د هر a او b د عنصر دپاره په همدغه سیټ کې یوازنی حل ولري.

¹: آبل نارویژي ریاضی پوه ؤ چې په ۱۸۰۲ عیسوی زیږیدلی او په ۱۸۲۹ عیسوی کې مړ سو.

کله چې د یوه مفهوم دپاره بیلا بیل تعریفونه راوړو، نو لازمه ده چې ددغو تعریفو معادل والی په ثبوت ورسوو.

قضیه ۱- د گروپ لمړی او دوهم تعریف سره معادل دی.

ثبوت - فرضوو چې د G په سیټ کې د ضرب راکړه سوی عملیه د لمړی تعریف شرطونه پرځای کوی. نو دوهم تعریف دوهم شرط باید ثبوت کړو، ځکه چې لمړی شرط په دواړو تعریفو کې راوړل سویدی. د لمړی تعریف د شرطو څخه په استفاده سره د دوهم تعریف دوهم شرط ثابتوو.

د G د سیټ دوه کیفی عنصرونه a او b رااخلو $a, b \in G$ او د $ax=b$ معادله تر څېړنی لاندی نیسو.

د گروپ د لمړی تعریف له مخی د G په گروپ کې د a^{-1} عنصر وجود لری. ځکه نو:

$$a^{-1}(ax)=a^{-1}b$$

$$(a^{-1}a)x=a^{-1}b$$

$a^{-1}a$ د G په سیټ کې بی اغیزی عنصر دی (د لمړی تعریف دریم شرط وگوری)، ځکه نو: $x=a^{-1}b$

پدی معنی چې د G په سیټ کې د $ax=b$ معادله حل لری. همدا ډول ثابتیدلای سی چې $ya=b$ معادله هم د G په سیټ کې حل لری او هغه عبارت دی له: $y=ba^{-1}$

پدی ډول مو ثابتہ کړه چې د G په سیټ کې زموږ د نظر معادلی حل لری، خو ثبوت لا پوره ندی، ځکه چې ځانگړیتوب او یا د حل یوازنی والی باید هم ثبوت کړو. ددی موخی دپاره معمولاً فرضوو چې یوه معادله دوه حل لری. زموږ په حالت کې فرضوو چې د $ax=b$ معادله د x_1 او x_2 دوه حل لری. یعنی: $ax_1=b$ او $ax_2=b$ سره کیږی پدی حساب $ax_1=ax_2$ سره کیږی. اوس که د وروستی معادلی دواړی خواوی د کینی خوا څخه په a^{-1} کی ضرب کړو، په نتیجه کی به:

$a^{-1}(ax_1)=a^{-1}(ax_2)$ او یا $(a^{-1}a)x_1=(a^{-1}a)x_2$ لاسته راسی. په نتیجه کی $x_1=x_2$ سره کیږی، یعنی معادله د یوازنی حل درلودونکی ده. په همدی ډول ثابتولای سو چې د $ya=b$ معادله هم یوازنی حل لری.

د پورتنیو دلایلو په نتیجه کی ادعا کولای سو چې د G په سیټ کې د ضرب عملیه دوهم تعریف شرطونه پر ځای کوی.

برعکس، فرضوو چې د ضرب عملیه د G په سیټ کې د دوهم تعریف شرطونه پر ځای کوی. دلته باید د لمړی تعریف دوهم او دریم شرط په ثبوت ورسوو (ولی؟ دللمری شرط په هکله څه ویلای سو؟).

د $a \in G$ دپاره د $ax=a$ معادله څېړو. دوهم تعریف دوهم شرط له مخی نوموړی معادله یوازنی حل لری او هغه په e' سره ښیو. فرض کړو چې $b \in G$ وی او y_0 د $ya=b$ د معادلی حل وی، یعنی $y_0a=b$ سره وی. ددی ځایه $be'=(y_0a)e'=y_0(ae')=ya=b$ سره کیږی. وروستی اړیکه ښیی چې:

$$(\forall b \in G)(be' = b)$$

همدا ډول ښودلای سو چې د $ya=a$ د معادلی دحل دپاره چې په e'' به یی وښیو:

$$(\forall b \in G)(e''b = b)$$

صدق کوی. په نتیجه کی $e' = e'e'' = e'' = e'$ یعنی $e' = e'' = e$ د G په سیټ کې نظر د ضرب و عملیې ته چې د G پر سیټ تعریف سویده، بی اغیزی عنصر دی چې په e سره یی ښیو.

اوس به نو وښیو چې د $a \in G$ هر عنصر دپاره متضاد عنصر وجود لری.

دوهم تعریف دوهم شرط پر بنسټ د $ax=c$ او د $ya=c$ معادلی د G په سیټ کې د یوازنی حل $x=a_1$ او $y=a_2$ درلودونکی دی. یعنی $a_2a=e$ او $aa_1=e$ سره کیږی. ددی ځایه:

$$a_1 = e a_1 = (a_2 a) a_1 = a_2 (a a_2) = a_2 e = a_2$$

فلهذا : $aa_1 = a_1 a = e$ ، پدی معنی چي a_1 د a د عنصر متضاد عنصر دی. پدی ډول مو ثابتہ کره چي د لمري تعريف ټوله شرطونه صدق کوي . پدی معنی چي د گروپ لمري او دوهم تعريف سره معادل دی. نتیجه د G په هر گروپ کی دینی او کین لوری څخه د لنډون (اختصار) عملیه سرته رسولای سو. یعنی:

$$(\forall a, b_1, b_2 \in G)(ab_1 = ab_2 \rightarrow b_1 = b_2) \wedge (b_1 a = b_2 a \rightarrow b_1 = b_2)$$

پاسنی نتیجه د G په گروپ کی د $ax=b$ او $ya=b$ د معادلو د یوازنی حل څخه استنباط کیری.

د G د گروپ a_1, a_2, \dots, a_k عنصرونه تر څیرنی لاندی نیسو. بیله دی چي ددی عنصر و تسلسل ته تغییر ورکرو د دوه نیزی عملی د سرته رسولو دپاره کولای سو چي په اختیاری بڼه قوسونه ځای پر ځای کړو. د بیلگی په توگه که د a_1, a_2, a_3 دري عنصره را کره سوی وی ، نو د $a_1(a_2 a_3)$ او $(a_1 a_2)a_3$ امکانات وجود لری. داتحادی خاصیت له مخی په دواړو حالتو کی و یوی نتیجی ته رسیرو ، یعنی یو عنصر لاسته راځی.

قضیه ۲- د G د گروپ پر عنصر a_1, a_2, \dots, a_k په پر له پسې ډول د عملی د سرته رسولو نتیجه ، په هغه ترتیب چي د قوسو پذیرعه بنودل سوی وی، د عنصر په منځ کی د قوسو په ځای پر ځای کولو پوری اړه نلری .

ثبوت - فرضوو چي a_1, a_2, \dots, a_k د G د گروپ اختیاری عنصرونه دی او $g = (\dots(a_1 a_2) a_3) \dots a_{k-1} a_k$ دی. د قضیې ثبوت نظر د ضربی عاملو (فاکتورو) و شمېر ته یعنی k د ریاضی د استقراء په طریقہ سرته رسوو.

که $k=3$ وی ، نو $g = (a_1 a_2) a_3 = a_1 (a_2 a_3)$ مساوات د گروپ د تعريف له مخی صدق کوی.

اوس به نو فرض کړو ، چي د $k=n-1$ عنصر و دپاره د قوسو ځای پر ځای کول د عملی د عملي کولو په نتیجه کی کوم رول نه لوبوی ، یعنی د اتحادی خاصیت پیروي کوی. پدی مانا چي د G د گروپ د b_{n-1}, \dots, b_2, b_1 اختیاری عنصر و د پاره صدق کوی چي:

$$g = (\dots(b_1 b_2) b_3) \dots b_{n-2} b_{n-1} = b_1 (\dots(b_2 b_3) \dots b_{n-1}) = (b_1 (b_2 (b_3 (\dots (b_{n-2} b_{n-1})))) \dots)$$

فرضوو چي $k=n$ سره دی او د a_1, a_2, \dots, a_k په لار کی قوسونه په لاندی ډول سره ځای پر ځای سوبیدی :

$$g_1 = [(\dots(a_1 a_2) \dots a_s)] [(a_{s+1} a_{s+2}) \dots a_n]$$

پداسی ډول چي $1 \leq s \leq n-1$ وی. د استقراء د فرضیې پر بنسټ دراکره سوی گروپ عملیه د a_s, \dots, a_2, a_1 او a_n, \dots, a_{s+1} پر لارونود قوسونو ځای پر ځای کول د عملی د عملی کیدو په نتیجه کی کوم تغییر نه راولی . پدی معنی چي:

$$b = (\dots a_1 a_2) \dots a_s , c = a_{s+1} (a_{s+2} \dots (a_{n-1} a_n) \dots)$$

او $g_1 = bc$ سره اوډلای سو . ځکه نو:

$$g_1 = bc = b [a_{s+1} (a_{s+2} \dots (a_{n-1} a_n) \dots)] = (b \cdot a_{s-1}) (a_{s-2} (a_{s+3} \dots (a_{n-1} a_n) \dots))$$

په پورتنی اړیکه کی د b, a_{s+1} او $a_{s+2} (a_{s+3} \dots (a_{n-1} a_n) \dots)$ پر عنصر و اتحادی قانون تطبیقوو او وروسته له $n-s$ ورته قدمو څخه لاندنی نتیجه لاسته راځی:

$$g_1 = (\dots (b a_{s+1}) a_{s+2}) \dots a_{n-1} a_n = (\dots (a_1 a_2) a_3 \dots a_{n-1}) a_n = g$$

پدی ډول مو ثابتہ کره چي د قوسو د اختیاری خای پر خای کیدو په نتیجه کی بیاهم د عملی د عملی کیدو نتیجه مساوی په g سره کیری. پدی معنی چي قضیه د $k=n$ دپاره هم صدق کوی . اوس نو ویلای سو چي قضیه د G د گروپ د اختیاری لار دپاره چي تر درو عنصرو زیاد هم ولری ، صدق کوی.

د پورتنی ثابتی سوی قضیې څخه ځنی مهمی نتیجی استنباط کیدای سی .

نتیجه ۱- د گروپ د عملی د عملی کیدو نتیجه د G د گروپ د n مساوی عنصرو پر لار د قوسو د خای پر خای کیدو تابع نده.

د پورتنی واقعیت د په نظر کی نیولو سره اوس نو اجازه لرو چي د G د گروپ د عنصرو د طبیعی طاقت مفهوم تعریف کرو.

د G د گروپ د a عنصر ، یعنی $a \in G$ ، n ام طاقت عبارت دی د گروپ د عملی د عملی کیدو د نتیجی څخه ددغه گروپ د عنصرو پر هغه لار باندی چي په هغه کی د a عنصر n ځله نغبتی وی (یا په ځان کی ولری). د a د عنصر n - ام طاقت په a^n سره بنیو.

$$a^n \stackrel{\text{df}}{=} \underbrace{(a \cdot a \cdot a \dots a)}_{n\text{-}\text{ځله}}$$

اکثراً د پورتنی اړیکی په بنی خوا کی د قوسو څخه صرف نظر کوو.

نتیجه ۲- د G د گروپ د هر عنصر a او د m او n اختیاری طبیعی عددو دپاره لاندنی مساواتونه صدق کوی:

$$a^n \cdot a^m = a^{m+n} \quad \text{او} \quad (a^n)^m = a^{mn}$$

پورتنی اړیکی د دوهمی قضیې او د طبیعی طاقت د تعریف څخه مستقیماً استنباط کیری.

قضیه ۳- د G د گروپ د a_1, a_2, \dots, a_k کیفی عنصرو دپاره لاندنی مساوات صدق کوی:

$$(a_1 \cdot a_2 \cdot \dots \cdot a_k)^{-1} = a_k^{-1} \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1}$$

ثبوت: د هغه ځایه چي :

$$\begin{aligned} (a_1 \cdot a_2 \cdot \dots \cdot a_k)(a_k^{-1} \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1}) &= a_1 \cdot a_2 \cdot \dots \cdot (a_k a_k^{-1}) \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1} = \\ &= a_1 \cdot a_2 \cdot \dots \cdot (a_{k-1} a_{k-1}^{-1}) \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1} = \\ &= a_1 (a_2 a_2^{-1}) a_1^{-1} = a_1 a_1^{-1} = e \end{aligned}$$

کیری ، نو د $a_1^{-1} \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1}$ عنصر د a_1, a_2, \dots, a_k دپاره معکوس عنصر دی.

دمعکوس عنصر د تعریف او ددریمی قضیې پر بنسټ لاندنی قضیه ثابتدلای سی :

قضیه ۴- د G د گروپ د هر عنصر a دپاره لاندنی مساواتونه صدق کوی:

$$(a^{-1})^{-1} = a \quad \text{او} \quad (a^n)^{-1} = (a^{-1})^n$$

² د df سمبول د تعریف پر اساس by definition د بیانولو په مفهوم دی.

تعریف ۳- د G غیر خالی سیټ او پر هغه باندی راکړه سوی دوه نېزه عملیه د گروپ په نامه یادیری که:

۱- دوه نېزه عملیه اتحادی خاصیت لری.

۲- د G د سیټ د هرو a او b عنصرو دپاره د $ax=b$ او $ya=b$ معادلی حل لری.

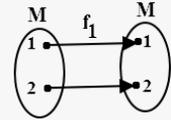
د دوهم تعریف پر خلاف دلته د حل د یوازی والی څخه صرف نظر سویدی.

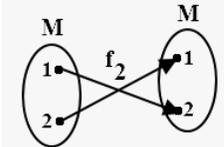
په لمړی قضیه کی مو د لمړی او دوهم تعریف معادل والی په ثبوت ورساوه. دوهم تعریف نظر و دریم تعریف ته قوی دی، ځکه چي په دوهم شرط کی د معادلو د حل دیوازی والی غوښتنه کوی. ددغه اسیته دوهم تعریف څخه دریم تعریف اسانه ثابتلائی سی. د دریم تعریف څخه دوهم تعریف د ثبوت دپاره کافی ده چي په تعریف کی د معادلو د حل یوازی والی په ثبوت ورسیری.

بیلگه ۱- پر n عنصر لرونکی سیټ M باندی مو د تعویض مفهوم د M د سیټ څخه د M پر سیټ باندی د بایجکتیف مپینگ په صفت تعریف کړی. (د لمړی برخي، څلرم فصل، $V\S$ ، ۱۷۵ صفحه وگوری)

لمړی به د M د سیټ څخه د M پر سیټ باندی د ټولو بایجکتیف مپینگو په سیټ کی د ترکیب عملیه تشریح کړو. وروسته به وگورو چي د مپینگو دغه ډول سیټ (یعنی د n -درجه ئی تعویضو سیټ) نظر د ترکیب و عملی ته گروپ دی. څرنگه چي تعویض په خپل ذات کی یو مپینگ دی او مپینگ د دوه نیزواریکو د توکو (انواعو) څخه دی، ځکه نو ترکیب یی د لمړی برخي، د لمړی فصل، $V\S$ ، د څلرم تعریف پر بنسټ صورت نیسي.

د بیلگي په توگه که د $M = \{1, 2\}$ دوه عنصره سیټ راکړه سوی وی، نو پر نوموړی سیټ د بایجکتیف مپینگونه (تعویضونه) عبارت دی له:

$f_1(1) = 1$ یا $\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$ یا 

$f_2(1) = 2$ یا $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ یا 

اوس نو د M د سیټ د هر عنصر دپاره $f_1 \circ f_2$ جلا جلا موندو، یعنی:

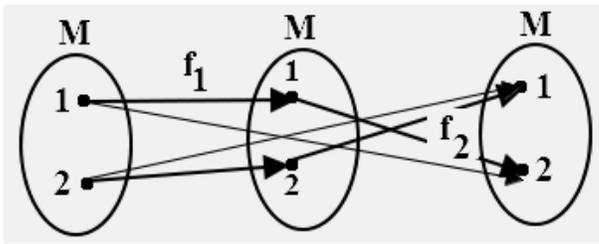
$$f_1 \circ f_2(1) = f_1(f_2(1)) = f_1(2) = 2$$

$$f_1 \circ f_2(2) = f_1(f_2(2)) = f_1(1) = 1$$

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

یا

او یاداسی یی هم انځورولای سو:



اوس به نو د دري عنصره سيټ $M = \{1, 2, 3\}$ د تعويضونوسيت در مطالعي لاندی ونيسو. د هغه سيټ عنصرونه عبارت دی له :

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

په اسانی سره امتحانيدلای سی چې د $P_M = \{f_0, f_1, f_2, f_3, f_4, f_5\}$ په سيټ کی د ترکیب عملیه د لاندني جدول په ذریعه تعینيدای سی (د کورنی وظیفې په شکل یې و آزمویي!).

جدول ۲

| | | | | | | |
|---------|-------|-------|-------|-------|-------|-------|
| \circ | f_0 | f_1 | f_2 | f_3 | f_4 | f_5 |
| f_0 | f_0 | f_1 | f_2 | f_3 | f_4 | f_5 |
| f_1 | f_1 | f_0 | f_5 | f_4 | f_3 | f_2 |
| f_2 | f_2 | f_3 | f_4 | f_5 | f_0 | f_1 |
| f_3 | f_3 | f_2 | f_1 | f_0 | f_5 | f_4 |
| f_4 | f_4 | f_5 | f_0 | f_1 | f_2 | f_3 |
| f_5 | f_5 | f_4 | f_3 | f_2 | f_1 | f_0 |

د P_M سيټ نظر د تعويضو و ترکیب « \circ » ته گروپ دی ، یعنی $\langle P_M, \circ \rangle$ گروپ دی. د گروپ د لمړي تعريف له مخي د « \circ » د عمليي اتحادی خاصیت آزمویو ، پدی معنی چې دري کيفي عنصرونه د P_M د سيټ څخه ، د بيلگي په توگه f_5, f_4, f_2 ، ټاکو او ثابتوو چې:

$$f_2 \circ (f_3 \circ f_4) = (f_2 \circ f_3) \circ f_4 \quad \dots(I)$$

د پورتنی مساوات (I) د ثبوت دپاره به لمړی د کين طرف د قوس په منځ کی قیمت پيدا کړو، یعنی:

$$f_5 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_1$$

$$f_2 \circ (f_3 \circ f_4) = f_2 \circ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_3 \quad \dots(i)$$

اوس به نو د مساوات (I) په بنی خوا کی د قوسوپه منځ کی قیمت محاسبه کړو:

$$f_2 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_1$$

$$(f_2 \circ f_3) \circ f_4 = f_1 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_3 \quad \dots(ii)$$

لیدل کیری چی د (i) او (ii) مساواتو بنی خواوی سره مساوی دی ، ځکه نو کینی خواوی یی هم سره مساوی دی. پدی معنی چی اتحادی خاصیت صدق کوی. د پورتنیو عملیو نتیجی د جدول سره پرتله کړی! په آسانی سره ازمویل کیدای سی چی f_0 د خنثی یا بی تأثیره عنصر وظیفه لری، یعنی د P_M د سیټ د هر عنصر دپاره ؛ دبیلگی په توگه د f_4 دپاره لاندنی اړیکه صدق کوی:

$$f_0 \circ f_4 = f_4 \circ f_0 = f_4 \quad \dots(iii)$$

$$f_0 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_4$$

$$f_4 \circ f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_4$$

پورتنی مساواتونه د (iii) اړیکي حقیقت تصد بقوی. په آخر کی باید ثابتہ کړو چی د P_M په سیټ کی نظر د ترکیب « \circ » عملی ته د هر عنصر دپاره متضاد عنصر وجود لری. دبیلگی په توگه د f_5 دپاره متضاد عنصر موندو.

فرضوو چی د f_5 متضاد عنصر $f = \begin{pmatrix} 1 & 2 & 3 \\ x & y & z \end{pmatrix}$ دی. ځکه نو باید $f \circ f_5 = f_0$ سره وی. د f_5, f_0 او

قیمتونه د 1, 2 او 3 په عددو کی د تابعگانو د قیمتو په شکل په لاندی ډول ارائه کوو:

$$f_5(1)=1 \quad f(1)=x \quad f_0(1)=1$$

$$f_5(2)=3 \quad f(2)=y \quad f_0(2)=2$$

$$f_5(3)=2 \quad f(3)=z \quad f_0(3)=3$$

$$f \circ f_5(1) = f_0(1)$$

$$f(f_5(1)) = f_0(1) = 1$$

$$f(1) = x = f_0(1) = 1 \quad \rightarrow \quad x = 1$$

$$f \circ f_5(2) = f_0(2)$$

$$f(f_5(2)) = f_0(2) = 2$$

$$f(3) = z = f_0(2) = 2 \quad \rightarrow \quad z = 2$$

$$f \circ f_5(3) = f_0(3)$$

$$f(f_5(3)) = f_0(3) = 3$$

$$f(2) = y = f_0(3) = 3 \quad \rightarrow \quad y = 3$$

په نتیجہ کی $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ او په حقیقت کی پخپله f_5 دی.

پدی معنی چی د f_5 متضاد عنصر پخپله f_5 دی. په پورتنی ډول او یا د جدول څخه په استفادی سره د P_M د سیټ دنورو عنصرو دپاره نظر د ترکیب و عملی ته متضاد عنصر موندلای سو.

بیلگه ۲- د $G = \{\epsilon_1, \epsilon_2, \epsilon_3\}$ سیټ نظر د ضرب و عملی ته چی د لاندی جدول پذیرعه راکړه سوی

وی، $\langle G, \cdot \rangle$ گروپ دی ، پداسی حال کی چی $\epsilon_3 = 1$ ، $\epsilon_2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ ، $\epsilon_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ وی.

جدول ۳

| | | | |
|--------------|--------------|--------------|--------------|
| . | ϵ_1 | ϵ_2 | ϵ_3 |
| ϵ_1 | ϵ_2 | ϵ_3 | ϵ_1 |
| ϵ_2 | ϵ_3 | ϵ_1 | ϵ_2 |
| ϵ_3 | ϵ_1 | ϵ_2 | ϵ_3 |

په رشتیا هم:

$$\varepsilon_1.(\varepsilon_2.\varepsilon_3) = (\varepsilon_1.\varepsilon_2).\varepsilon_3 \quad \dots(1)$$

$$\varepsilon_1.(\varepsilon_2.\varepsilon_3) = \varepsilon_1.\varepsilon_2 = \varepsilon_3 \quad \dots(a)$$

$$(\varepsilon_1.\varepsilon_2).\varepsilon_3 = \varepsilon_3.\varepsilon_3 = \varepsilon_3 \quad \dots(b)$$

د (a) او (b) د مساواتو د مقایسې په نتیجه کې د (1) مساوات لاسته راځي. پدې معنی چې د ضرب عملیه د G پر سیټ باندې د اشتراکي خاصیت درلودونکې ده. په جدول کې بنسټه لیدل کېږي چې ε_3 د خنثی عنصر رول لوبوي. د ε_1 او ε_2 عنصرونه یوډبله سره متضاد دي. ددې اسیتنه ویلای سو چې د G سیټ او پر هغه باندې د جدول پذیریه راکړه سوی د ضرب عملیه، گروپ تشکیلوي.

II§. سبگروپ - دورانی (څرخنده) گروپونه.

کله چې یو انسان ته یو نوي شئ په لاس ورسې نو لمړی د هغه شئ ظاهري بڼه گوری او په غور سره یې څېری. وروسته یې د کنجکاوی له مخې کرار کرار توتیه توتیه کړی خو د هغه د پرزو د تجزیې او تحلیل له مخې د هغه شئ په اصلیت او ماهیت ښه پوه سی. مور هم اوس همدابول کړنه کوو. د گروپ ډول ډول تعریفونه مو راوړه، د هغوی ترمنځ اړیکې مو وڅېرلي، نو اوس به د گروپ نور خاصیتونه تر مطالعې لاندې ونیسو.

تعریف ۱- د G د گروپ سبسیټ H د G د گروپ د سبگروپ په نامه یادېږي، که H نظر و هغی دوه نېزی عملیې ته چې په G کې راکړه سویده، گروپ وی.

بیلگه ۱- څرگنده ده چې هر د G گروپ دوه ساده Trivial سبگروپونه لری، چې هغه عبارت دی پخپله د G د گروپ څخه او د یو عنصره سبگروپ $H = \{e\}$ ، چې یوازی یو عنصر لری.

بیلگه ۲- د ټولو جفتو تامو عددو جمعې گروپ H د ټولو تامو عددو د جمعې گروپ \mathbb{Z} ، سبگروپ دی.

بیلگه ۳- د نسبي عددو (ناطقو عددو) چې د صفر څخه خلاف وی، ضربې گروپ $H = \mathbb{Q} \setminus \{0\}$ د حقیقي عددو چې د صفر څخه خلاف وی $G = \mathbb{R} \setminus \{0\}$ ضربې گروپ، سبگروپ دی.

بیلگه ۴- د $H = \{1, -1\}$ ضربې گروپ د نسبي عددو چې د صفر څخه خلاف وی $G = \mathbb{Q} \setminus \{0\}$ نظر د ضرب و عملیې ته سبگروپ دی.

دلاندنئ قضیې په مرسته د راکړه سوی گروپ، سبگروپ والي آزمویلای سو.

قضیه ۱- د G د گروپ غیر خالی سب سیټ H ، د G د گروپ سبگروپ دی، یوازی او یوازی هغه وخت چې لاندني شرطونه پر ځای سوی وی.

$$(\forall a, b \in H)(a.b \in H) \quad \dots(1)$$

$$(\forall a \in H)(a^{-1} \in H) \quad \dots(2)$$

ثبوت - که H د G سبگروپ وی، نو H نظر و دوه نېزی عملیې ته چې پر G تعریف سویده، گروپ دی. یعنی (1) او (2) شرطونه صدق کوی. پدې معنی چې H په سیټ کې د a او b کیفی عنصر سره د هغوي د ضرب حاصل، یعنی $a.b$ هم شامل دی. په همدا ډول د هر a عنصر سره چې د H د سیټ وی، a^{-1} هم د H په سیټ کې شامل دی.

اوس به نو فرض کړو چې د G غیر خالی سبسیټ $H \neq \emptyset$ د قضیې (1) او (2) شرطونه پر ځای کوی. باید ثابت کړو چې د H د دوه نېزی عملیې سره گروپ دی. د لمړی شرط پر بنسټ هغه عملیه چې د G پر سیټ راکړه سوی ده، د H د سیټ پر عنصر هم عملی کېږي. څرنگه چې دغه عملیه د G په سیټ کې اشتراکي خاصیت لری او $H \subseteq G$ دی، ځکه نو دغه عملیه د H پر سیټ هم د اشتراکي خاصیت درلودونکې ده.

څرنگه چې $H \neq \emptyset$ دی، نو د H په سیټ کې لږ تر لږه یو عنصر $a \in H$ وجود لری، د قضیې دوهم شرط له مخې د همدې عنصر معکوس عنصر هم په H کې موجود دی، یعنی $a^{-1} \in H$. بر سیره پر دی

د $a.a^{-1} \in H$ اړیکه هم حقیقت لری، خو $a.a^{-1}=c$ یعنی $c \in H$ دی. ددغه اسیته د $I \S$ د لمړی تعریف له مخی H د راکړه سوی دوه نېزی عملیې سره گروپ دی.

بیلگه ۵ - د لمړی قضیې څخه په استفاده سره ثابتوو چي د دری عنصره سیټ د ټولو تعویضو د سیټ سبسیت $H = \{f_0, f_2, f_4\}$ نظر د ترکیب و عملیې ته د دری عنصره سیټ د ټولو تعویضو د گروپ، سبگروپ جوړوی (د $I \S$ ، لمړی بیلگه وگوری).

که د $I \S$ دوهم جدول ته څیر سی، $f_0 \circ f_0 = f_0, f_2 \circ f_2 = f_4, f_4 \circ f_4 = f_2, f_2 \circ f_0 = f_2, f_4 \circ f_0 = f_4$ دی.

پدی معنی چي د H د سیټ د دوو کیفی عنصر و ترکیب بیا هم د H په سیټ کی داخل دی او د قضیې لمړی شرط صدق کوی.

د نوموړی جدول څخه بیا هم په استفاده سره د f_0 متضاد عنصر بیا هم f_0 دی، f_2 او f_4 بود بل په مقابل کی متضاد عنصرونه دی، یعنی د f_2 متضاد عنصر f_4 او برعکس د f_4 متضاد عنصر f_2 دی. په نتیجه کی ویلای سو چي د H په هکله د قضیې دوهم شرط هم صدق کوی. بالاخره دغه ادعا چي د H دری عنصره د ټولو تعویضو د گروپ سبگروپ دی، حقیقت لری.

فرض کړو چي H او F د G د گروپ سبگروپونه دی. طبعاً سوال مطرح کیږی چي آیا $H \cap F$ او $H \cup F$ د G د گروپ سبگروپونه دی او که نه؟ د $H \cup F$ په اړه جواب منفی دی. ددی دپاره چي خپله ادعا مو په ثبوت رسولی وی، کافی ده چي یوه بیلگه پیدا کړو چي دهغه دپاره زموږ ادعا صدق ونه کړی.

که $H = \{2k/k \in \mathbb{Z}\}$ او $F = \{3n/n \in \mathbb{Z}\}$ د تامو عددو د جمعی گروپو سبگروپونه وی، نو $2 \in H \cup F$ او $3 \in H \cup F$ ؛ خو $3+2=5 \notin H \cup F$ ، یعنی د قضیې لمړی شرط نقضوی. د $H \cap F$ په هکله لاندنی قضیه جواب ورکوی.

قضیه ۲- که H او F د G د گروپ سبگروپونه وی، پس $H \cap F$ هم د G د گروپ سبگروپ دی.

ثبوت - فرضوو چي $a, b \in H \cap F$ دی، د مشترکي برخی د تعریف له مخی په عین وخت کی $a, b \in H$ او $a, b \in F$ دی، څرنگه چي H او F سبگروپونه دی، نو پدی لحاظ $a.b \in F$ او $a.b \in H$ دی، یعنی $a.b \in H \cap F$.

همداول استدلال کولای سو که $a^{-1} \in H$ او $a^{-1} \in F$ وی، نو $a^{-1} \in H \cap F$ دی. د لمړی قضیې پر بنسټ ویلای سو چي $H \cap F$ د G د گروپ سبگروپ دی.

فرض کړو چي G گروپ، $a \in G$ او $e \in G$ په گروپ کی خنثی عنصر وی.

د $a^0 = e$ او $a^{-k} = (a^{-1})^k$ مساواتونه د حقیقت په صفت قبلوو. د (a) د نښي څخه مو هدف د

$$(a) = \{a^n/n \in \mathbb{Z}\} \text{، یعنی: } \{a^n/n \in \mathbb{Z}\}.$$

په آسانی بی آزمویلای سو چي (a) ، چي د G سب سیټ دی، د G سبگروپ دی. په رشتیا هم:

$$a^m \in (a) \wedge a^l \in (a) \rightarrow a^m \cdot a^l = a^{l+m} \in (a)$$

$$a^m \in (a) \rightarrow a^{-m} \in (a)$$

د لمړی قضیې پر بنسټ (a) سبگروپ دی.

تعریف ۲ - د (a) سبگروپ چي د G د گروپ د عنصر $a \in G$ د ټولو طاقتو څخه تشکیل سویدی ، د G د گروپ د دوراني (څرخنده) Cyclic Subgroup سبگروپ په نامه یادېږي، چي د $a \in G$ د عنصر په ذریعه تولید سویدی.

د $a \in G$ عنصر د (a) سبگروپ زیږونکی (مولد) Generator دی.

اوس به وگورو چي د څرخنده سبگروپ جوړول ډیر ساده دی.

کیدای سی چي د G د گروپ د a د عنصر ټوله طاقتونه یو دبله سره مختلف وی. په هغه صورت کی وایو چي د a د عنصر ترتیب لایتناهي دی؛ د بیلگي په توگه د ټولو تامو (نسبتي) مثبتو عدو \mathbb{Q} په گروپ کی د 2 د عدد ترتیب لایتناهي دی ، ځکه چي د $(2) = \{2n/n \in \mathbb{Z}\}$ د سیټ ټول عنصرونه یو دبله سره مختلف دی.

کیدای سی چي د G د گروپ د a د عنصر یو د طاقتو څخه د a د عنصر د یوه طاقت سره مساوی وی، پدی معنی چي $a^l = a^s$ وی ، پداسی حال کی چي $s > l$ وی. په منتهای گروپو کی دغه ډول حالت نل بیښیږي ، خو کله کله په غیر منتهای گروپو کی هم منځ ته راځي.

ددغه ډول څرخنده گروپونو د جوړولو طریقه به په لاندی ډول د جزئیاتو سره وڅېړو.

په هغه صورت کی چي $s > l$ وی ، څرگنده ده چي $s - l > 0$ وی او $a^{s-l} = e$ سره کیږي. پدی معنی چي د a د عنصر داسی مثبت طاقت وجود لری چي د a عنصر په هغه طاقت باندی مساوی په خنثی عنصر سره کیږي. فرضوو چي n د a د عنصر دغه ډول د کوچنی ترینو طاقتو څخه دی، دغه ډول طاقت ، د کوچنی ترین عدد د پرنسیب له مخي؛ لمری برخه، دوهم فصل ، § II ، ۷۰، ایم مخ ، قضیه ۲، وگوری؛ وجود لری، چي $a^n = e$ کیږي. ځکه نو وایو چي د G د گروپ د a د عنصر ترتیب n دی.

قضیه ۳- که د G د گروپ د a د عنصر ترتیب n وی. نو هغه څرخنده گروپ چي د a عنصر یی زیږونکی دی ، یعنی (a) د لاندني عنصرو درلودونکی دی:

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

ثبوت - لمری خو به وگورو چي آیا د $e, a, a^2, \dots, a^{n-1}$ په منځ کی خو دوه مساوی عنصرونه نسته ، یعنی ټول عنصرونه باید یو دبله مختلف وی.

په رشتیا هم که د $0 \leq l < s \leq n$ دپاره $a^l = a^s$ وی ، نو $a^{s-l} = e$ سره کیږي. پدی معنی چي د a د عنصر ترتیب $s - l < n$ دی. مگر موږ خو د قضیې په فرضیه کی ویلي دی چي د a د عنصر ترتیب n دی.

ددغه اسیته دغه حالت ناممکنه دی. ځکه نو ټوله راکړه سوی عنصرونه په خپل منځ کی مختلف دی.

اوس نو که $k > n$ یو تام عدد وی ، یعنی $k \in \mathbb{Z}$ ، او د k عدد پر n ووېشو ، نو $k = n \cdot q + r$ به لاسته راسی پداسی حال کی چي $0 \leq r < n$ وی.

ځکه نو: $a^k = a^{n \cdot q + r} = (a^n)^q \cdot a^r = c \cdot a^r = a^r$ سره کیږي. په نتیجه کی $(a) \subset \{c, a, a^2, \dots, a^{n-2}, a^{n-1}\}$ او قضیه په ثبوت ورسیده. (qed)

لاندني حقیقتونه د ثابتی سوی قضیې نتیجی دی.

که د G د گروپ د a د عنصر ترتیب n وی، نو د هغه څرخنده سبگروپ چي د a عنصر یی مولد دی ، یعنی (a) ، فقط n عنصره لری پدی معنی چي د سبگروپ ترتیب n دی.

تعريف ۳- د G گروپ د څرخنده (دورانې) گروپ Cyclic Group په نامه يادېږي ، که G د خپلو سيکروپو څخه (a) د يوه سيکروپ سره منطبق وي. پدغه حالت کې د G د گروپ د a عنصر، د $G=(a)$ د گروپ د زيرونکي (مولد) عنصر په نامه يادېږي.

په آساني سره ليدل کيږي چې هر څرخنده گروپ تبديلي گروپ (آبل گروپ) دی په رشتيا سره :

$$a^m \cdot a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m$$

بيلگه ۶- د تامو عددو جمعې گروپ $\langle \mathbb{Z}; + \rangle$ لايتناهي څرخنده گروپ دی، چې د هغه زيرونکي عنصر د يوه عدد دی.

بيلگه ۷- د مربع د ټولو څرخيدو سيټ دهغه پر مرکز باندې $G = \{R_0^0, R_0^{90}, R_0^{180}, R_0^{270}\}$ د څرخيدو د ترکيب د عمليې سره د څارم ترتيب څرخنده گروپ دی چې زيرونکي عنصر يې (R_0^{90}) دی.

په رياضي کې په عمومي ډول د رياضي ساختمانو د پرتلي دپاره (چې آيا دوه د رياضي ساختمانونه مساوي دي او که مختلف؟) او په خاص ډول د گروپونو د پرتلي دپاره د ايزومورفيزم Isomorphism د مفهوم څخه کار اخيستل کيږي (لمرې برخه، دوهم فصل ، $\forall \xi$ وگوري). دلته يې بيا هم يادونه کوو، چې د G_1 او G_2 دوه گروپونه هغه وخت ايزومورف (هم شکله) دي که د G_1 څخه پر G_2 باندې داسې بايجکتيف مپينگ $f: G_1 \rightarrow G_2$ وجود ولري چې:

$$(\forall x, y \in G_1)(f(x \cdot y) = f(x) \cdot f(y))$$

قضيه ۴- هره څرخنده لايتناهي گروپ د تامو عددو د جمعې گروپ سره ايزومورف دی. هر څرخنده د n -ام ترتيب لرونکي گروپ د مختلطو عددو د يوه دعدد د n - ام جذر د ضربې گروپ سره ايزومورف دی.

ثبوت - فرضوو چې څرخنده گروپ $G=(a)$ لايتناهي ترتيب لري. د G د گروپ څخه د تامو عددو پر سيټ باندې مپينگ $f: G \rightarrow \mathbb{Z}$ د $f(a^n) = n$ د فارمول پذريعه تعريفوو.

څرگنده ده چې د f مپينگ بايجکتيف دی. سر بيره پر دی:

$$f(a^n \cdot a^m) = f(a^{n+m}) = n+m = f(a^n) + f(a^m)$$

پدې معنی چې G د \mathbb{Z} سره ايزومورف دی.

اوس به نو فرض کړو چې $G=(a) = \{e, a, a^2, \dots, a^{n-1}\}$ د n -ام ترتيب لرونکي څرخنده گروپ دی چې a د هغه زيرونکي عنصر دی. د مختلطو عددو د يوه عدد د n - ام جذر ضربې گروپ

$H = \{1, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{n-1}\}$ پداسې حال کې څپرو چې $\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$ ، $k \in \{0, 1, 2, \dots, n-1\}$ دی.

د مؤاور (DeMoivre) د فارمول له مخې چې د لمړي برخې په دوهم فصل ، $\forall \xi$ کې ثبوت کړی ، لاندې اړيکه لاسته راځي.

$$\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} = \left(\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \right)^k = \varepsilon_1^k$$

ځکه نو : $H = \{1, \varepsilon_1, \varepsilon_1^2, \dots, \varepsilon_1^{n-1}\} = \langle \varepsilon_1 \rangle$

وروستي اړیکه ددی حقیقت څرگندوی ده ، چې H څرخنده گروپ دی او د هغه زېږونکي عنصر ε_1 دی.

اوس که د ټول k دپاره ، $0 \leq k \leq n-1$ د $f:G \rightarrow H$ مپینګ د $f(a^k) = \varepsilon_1^k$ اړیکي پذیرعه تعریف کړو ، نو څرگنده ده چې د f مپینګ بایجکتیف دی ، علا وه پر دی د $x=a^m$ او $y=a^s$ اختیاری عنصر و دپاره صدق کوی :

$$f(x, y) = f(a^m, a^s) = \begin{cases} f(a^{m+s}) & ; \quad m+s < n \\ f(a^{m+s-n}) & ; \quad m+s \geq n \end{cases}$$

په لمړي حالت کی ، چې $m+s < n$ وی :

$$f(a^{m+s}) = \varepsilon_1^{m+s} = \varepsilon_1^m \cdot \varepsilon_1^s = f(a^m) \cdot f(a^s) = f(x) \cdot f(y)$$

په دوهم حالت کی ، چې $m+s \geq n$ وی:

$$f(a^{m+s-n}) = \varepsilon_1^{m+s-n} = \varepsilon_1^m \cdot \varepsilon_1^s \cdot \varepsilon_1^{-n} = f(a^m) \cdot f(a^s) \cdot (\varepsilon_1^n)^{-1} = f(a^m) \cdot f(a^s) = f(x) \cdot f(y)$$

په نتیجه کی ویلای سو چې د f مپینګ آیزومورفیزم دی او د G او H گروپونه آیزومورف دی. پدی ترتیب د څلرمي قضیې څخه استنباط کیری چې د تامو عددو جمعی گروپ او د مختلط واحد عدد n - مو جذرو ضربی گروپ د ټولو څرخنده گروپو نماینده گي کوی.

§ III. دگروپو تجزیه په سبگروپونو - د لاگرانژ قضیه

فرضوو چې G گروپ ، N او M دهغه غیر خالی سبسیټونه دی.

تعریف ۱- د M او N د سبسیټونو ضرب عبارت دی د MN د سبیت څخه چې عنصرونه یې د M د سبیت د عنصر وټوله ممکنه د ضرب حاصل د N د سبیت په عنصر و کی تشکیلوی . یعنی:

$$MN \stackrel{\text{df}}{=} \{xy/x \in M \wedge y \in N\}$$

په آسانی سره امتحانیدلای سی ، چې د G د گروپ د سبسیټو د ضرب عملیه اشتراکی خاصیت لری .

$$(MN)P = M(NP)$$

یعنی:

غیر له دی څخه ، که M د G د گروپ سبگروپ وی ، نو لاندنی مساوات هم صدق کوی:

$$MM = M$$

په راتلونکي کی به نوموړی عملیه په هغه حالت کی تر څېړنی لاندی نیسو چې زموږ تر نظر لاندی سبسیټو څخه یو سبسیټ یې یوازی یو عنصر ولری او دوهم سبسیټ یې سبگروپ وی.

فرضوو چې G گروپ ، $g \in G$ او H د G د گروپ ، سبگروپ دی.

تعریف ۲- د G د گروپ کپنه فرعی ټولگی د H د سبگروپ پر بنسټ د g د عنصر په نمائنده گي سره ، عبارت دی له H . $\{g\}$ څخه . نوموړي ټولگی به په راتلونکي کی په gH سره بنیوو .

د G_L^H په سمبول سره د G د گروپ ټولی هغه کینی فرعی ټولگیانی ښیو، چې د سبگروپ H پر بنسټ جوړي سوی وی، یعنی: $G_L^H = \{gH / g \in G\}$ (دلته L د کین په مفهوم دی). اوس به نو د G د گروپ د سبگروپ H پر بنسټ د G د گروپ د کینو فرعی ټولگیو د عنصر و ځنی خاصیتونه تر مطالعی لاندی ونیسو.

خاصیت ۱- د G د گروپ د سبگروپ H پر بنسټ د G د گروپ د ټولو کینو فرعی ټولگیو اتحاد د G په گروپ سره مساوی کیږی، یعنی: $G = \bigcup_{g \in G} \{gH / g \in G\}$

په رشتیا هم، د G د گروپ هر عنصر $a \in G$ په کینی فرعی ټولگی پوری اړه لری، ځکه چې H د G د سبگروپ په صفت بی تاثیر عنصر په ځان کی لری، یعنی: $(\forall a \in G)(a = a.c \in aH)$

پدی معنی چې: $G \subset G_L^H$

برعکس که $a \in G_L^H$ وی، پدی معنی چې a د کینو فرعی ټولگیو د یوی ټولگی عنصر دی، پدی معنی چې د $g \in G$ داسی وجود لری چې $a \in gH$. د کینی فرعی ټولگی او د سبگروپ د تعریف له مخی $a = g.h$ سره کیږی، یعنی: $(g \in G \wedge h \in H \wedge H \subset G) \Rightarrow (g.h = a \in G)$

خاصیت ۲- د G د گروپ د هرو دوو کینو فرعی ټولگیو دپاره یعنی g_1H او g_2H چې د G د سبگروپ H پر بنسټ جوړی سوی وی، یو د لاندنیو حالتو څخه صدق کوی.

$$1. \quad g_1H = g_2H \quad \text{او یا} \quad 2. \quad g_1H \cap g_2H = \emptyset$$

ثبوت - فرضوو چې g_1H او g_2H یو مشترک عنصر g لری، یعنی: $g \in g_1H \cap g_2H$. ثابتوو چې دواړه راکړه سوی ټولگی سره مساوی دی.

$$g \in g_1H \cap g_2H \Rightarrow g \in g_1H \quad \wedge \quad g \in g_2H$$

پدی معنی چې د H په سبگروپ کی د h_1 او h_2 داسی عنصرونه وجود لری چې:

$$g = g_1h_1 \quad \wedge \quad g = g_2h_2$$

$$g_1h_1 = g_2h_2 \quad \wedge \quad g_1 = g_2h_2h_1^{-1} \quad \text{ددی ځایه:}$$

ددی دپاره چې د g_1H او g_2H د ټولگیو مساوی والی $g_1H = g_2H$ په ثبوت ورسوو، نو باید لاندنی دوی اړیکې په ثبوت ورسوو:

$$a) \quad g_1H \subset g_2H \quad \wedge \quad b) \quad g_2H \subset g_1H$$

د لمری اړیکې د ثبوت دپاره د x یو اختیاری عنصر د g_1H څخه را اخلو، یعنی فرضوو چې $x \in g_1H$ دی. ځکه نو:

$$x = g_1.h = (g_2h_2h_1^{-1}).h = g_2.(h_2h_1^{-1}.h)$$

څرنګه چې $h_2h_1^{-1}.h \in H$ ، نو ددی اسیته د x اختیاری عنصر د g_2H په ټولگی هم شامل دی، یعنی $x \in g_2H$. په نتیجه کی مو ثابتته کړه چې $g_1H \subset g_2H$. همدا ډول ثابتیدلای سی چې $g_2H \subset g_1H$ دی. ځکه نو د $g_1H = g_2H$ مساوی والی په ثبوت ورسیدی.

د پورتنی لمړی او دوهم خاصیت څخه مستقیماً دغه نتیجه اخیستل کیږي، چې د G د ګروپ د سبګروپ H پر بنسټ د ټولو فرعي کینو ټولګیو سیټ، یعنی G_R^{II} د G د ګروپ تجزیه ده.

تعریف ۳- د G د سبګروپ H پر اساس د G د ګروپ تجزیه په فرعي کینو ټولګیو G_L^H باندې، د G د ګروپ د سبګروپ H پر بنسټ د G د ګروپ د کیني تجزيي څخه عبارت ده.

بیلګه ۱- د تامو عددو د جمعي ګروپ کینه تجزیه د د ټولو تامو جفتو عددو H پر بنسټ یوازی دوی ټولګي لري، هغه هم عبارت دی له:

H - د ټولو تامو جفتو عددو ټولګي او $I+H$ د تامو طاقو عددو ټولګي، یعنی:

$$\mathbb{Z}_R^{II} = \{II, I+II\}$$

همدارنگه د Hg سیټ د G د ګروپ د سبګروپ H پر بنسټ د G د ګروپ د فرعي بڼي ټولګي په نامه یادېږي. ثابتیدلای سې چې د G د ګروپ د ټولو فرعي بڼي ټولګیو سیټ G_R^{II} د هغه د سبګروپ H پر بنسټ هم د G د ګروپ تجزیه ده، چې د G د ګروپ د سبګروپ H پر بنسټ د G د ګروپ د بڼي تجزيي په نامه یادېږي.

د پاسنیو واقعیتو فارمولې او د هغوی د حقانیت ثبوت د تمرین په څیر وړاندیزوو.

خاصیت ۳- د G د ګروپ د سبګروپ II پر بنسټ د هرو دوو فرعي کینو ټولګیو ترمنځ بایجکټیف مپینګ (یو په یو اړیکه) وجود لري.

ثبوت - که g_1H او g_2H د G د ګروپ د سبګروپ H پر بنسټ کیني فرعي ټولګي وی، نو د $f: g_1H \rightarrow g_2H$ مپینګ چې د ټولو $h \in H$ دپاره د $f(g_1h) = g_2h$ فارمول په ذریعه راکړه سوېدي، زموږ د غوښتنې سره برابر مپینګ دی.

څرګنده ده چې د f مپینګ د g_1H د سیټ څخه د g_2H پر سیټ باندې دی. که فرض کړو چې $g_1h_1 = g_1h_2$ دی، نو $h_1 = h_2$ سره وی. یعنی د f مپینګ یو په یوه اړیکه ده. په نتیجه کې f د g_1H څخه پر g_2H باندې بایجکشن دی.

پاسنی خاصیتونه د G د ګروپ د سبګروپ H پر بنسټ د بڼو فرعي ټولګیو دپاره هم صدق کوي.

د دریم خاصیت څخه داسې نتیجه اخیستل کیږي چې:

په هغه صورت کې چې د H سبګروپ متناهي وی، نو د G د ګروپ ټوله فرعي بڼي او کیني ټولګي د نوموړي سبګروپ پر بنسټ متناهي دی، او د هغوی د عنصر و شمېر د H د عنصر و شمېر سره مساوی دی. دغه نتیجه موږ ته اجازه راکوي څو لاندني قضیه، چې د لاګرانژ د قضیې په نامه یادېږي، په آسانی سره ثبوت کړو.

د لاګرانژ Lagrange قضیه - په هر متناهي ګروپ کې د هغه د هر سبګروپ ترتیب د ګروپ د ترتیب وېشونکي (قاسم) دی.

دغه قضیه داسې ادعا کوي چې په متناهي ګروپ کې د هغه د سبګروپ ترتیب د نوموړي ګروپ ترتیب وېشي.

ثبوت - فرضوو چي د G گروپ متناهي او دهغه ترتيب په n سره مساوی کيږي او H د همدغه گروپ د سبگروپو څخه دی چي ترتيب يې مساوی په k سره دی. د G د گروپ د سبگروپ H پر بنسټ د ټولو کينو فرعي ټولگيو سيټ يعنی G_L^{II} تر څېړني لاندی نيسو. فرض کړو چي د G_L^{II} د کينو فرعي ټولگيو شمېر s وی. تر هغه ځايه چي د هرې کينې ټولگي د عنصرو شمېر k دی، ځکه چي د G سبگروپ H د عنصرو شمېر k دی او G_L^H د G د گروپ تجزيه ده، نو $n=k.s$ سره پدی معنی چي د n عدد د k پر عدد دوېش وړ دی.

نتیجه ۱- د متناهي گروپ G د هر عنصر g ترتيب د نوموړی گروپ د ترتيب وېشونکی (قاسم) دی. په رشتيا هم، د $g \in G$ ترتيب په واقعيت کی د G د گروپ دهغه څرخنده سبگروپ (g) د ترتيب سره مساوی کيږي چي د g پذريعه جوړ سوی وی.

د لاگرانژ قضيه تر ډيره حده زموږ دپاره د متناهي گروپو د جوړښت لاره آسانه کوی. د بيلگي په ډول هغه گروپ چي ترتيب يې په 5 سره مساوی کيږي، يوازی دوه ساده سبگروپونه درلودلای سی، چي د هغوی ترتيب يواو پنځه دی. (ولی؟)

بيلگه ۱- د I د لمړی بيلگي او د II د پنځمی بيلگي څخه په استفاده سره د $P_M = \{f_0, f_1, f_2, f_3, f_4, f_5\}$ گروپ د ټولو کينو ټولگيو سيټ نظر د $H = \{f_0, f_2, f_4\}$ و سبگروپ ته شمېرو:

$$\begin{aligned} \{f_0\}H &= f_0H = \{f_0 \cdot f_0, f_0 \cdot f_2, f_0 \cdot f_4\} = \{f_0, f_2, f_4\} \\ \{f_1\}H &= f_1H = \{f_1 \cdot f_0, f_1 \cdot f_2, f_1 \cdot f_4\} = \{f_1, f_3, f_5\} \\ \{f_2\}H &= f_2H = \{f_2 \cdot f_0, f_2 \cdot f_2, f_2 \cdot f_4\} = \{f_2, f_4, f_0\} \\ \{f_3\}H &= f_3H = \{f_3 \cdot f_0, f_3 \cdot f_2, f_3 \cdot f_4\} = \{f_3, f_1, f_5\} \\ \{f_4\}H &= f_4H = \{f_4 \cdot f_0, f_4 \cdot f_2, f_4 \cdot f_4\} = \{f_4, f_0, f_2\} \\ \{f_5\}H &= f_5H = \{f_5 \cdot f_0, f_5 \cdot f_2, f_5 \cdot f_4\} = \{f_5, f_3, f_1\} \end{aligned}$$

نظر و لمړی خاصيت ته :

$$f_0H \cup f_1H \cup f_2H \cup f_3H \cup f_4H \cup f_5H = \{f_0, f_1, f_2, f_3, f_4, f_5\} = P_M$$

$$P_M^H = \{f_0H, f_1H\} \quad \text{همداډول:}$$

که دوهم خاصيت په نظر کی ونيسو، نو: $f_0H \cap f_1H = \emptyset$ ، $f_0H = f_2H = f_4H$ ، او $f_1H = f_3H = f_5H$.

پدی معنی چي P_M^H په رشتيا هم د P_M د گروپ کينه تجزيه ده.

د P_M پر گروپ د لاگرانژ قضيه تطبیقوو او بنیو چي په رشتيا هم نوموړی گروپ يوازی او يوازی د لمړی، دوهم، دريم او شپږم ترتيب سبگروپو درلودونکی دی او هغه عبارت دی له:

$$H_1 = \{f_0\}$$

$$H_2 = \{f_1, f_0\}$$

$$H_3 = \{f_0, f_2, f_4\}$$

$$H_4 = \{f_0, f_1, f_2, f_3, f_4, f_5\}$$

په پورتنۍ بیلگې کې مو ولیدل چې د سبگروپ H د عنصر و شمېر او ددغه سبگروپ پر بنسټ فرعي کینو ټولگيو د عنصر و شمېر سره مساوی دی.

§IV. د گروپ نارمل وېشونکي او د گروپ تجزيه (Factor Group).

که د سبگروپ پر بنسټ د بوه گروپ د بڼې او کيڼې فرعي ټولگيو تجزيه په ډيرو بيلگو باندې مطالعه کړو ، نو وبه گورو چې هغوی په خپل منځ کې سره مساوی دی . خو دغه واقعیت تل صدق نه کوی . ځکه نو هغه گروپونه چې د هغوی په هکله دغه واقعیت صدق کوی ، د گروپ په تيوري کې خاص رول لوبوی.

تعريف ۱- د G د گروپ سبگروپ H د نوموړی گروپ د نارمل وېشونکي په نامه يادېږی ، که د سبگروپ H پر بنسټ د G د گروپ کيڼه او بڼي تجزيه يو دبله سره مساوی وی.

که $G_R^H = G_L^H$ وی ، نو د هر $g \in G$ دپاره داسی $g_1 \in G$ وجود لری چې $gH = Hg_1$ سره کيږی. تر هغه ځايه چې $g \in gH$ ده ، نو $g \in Hg_1$ ؛ خو په عين حال کې $g \in Hg$ هم دی ، ځکه نو $gH = Hg$ سره کيږی.

د پاسنی مشاهدی له مخی د گروپ د نارمل وېشونکي دپاره بل تعريف هم طرح کولای سو .

تعريف ۲- د G د گروپ سبگروپ II د نوموړی گروپ د نارمل وېشونکي په نامه يادېږی ، که

$$(1) \dots (\forall g \in G)(gII = IIg) \text{ صدق وکړی.}$$

بيلگه ۱- د تبدیلی گروپ (آبل گروپ) G هر سبگروپ H د هغه نارمل وېشونکي دی. ځکه چې د دوهم تعريف شرط (1) صدق کوی.

بيلگه ۲- په هر گروپ G د هغه ساده سبگروپونه ، يعنی $\{e\}$ او په خپله G د G د گروپ نارمل وېشونکي دی ، ځکه چې : $(\forall g \in G)(g\{e\} = \{e\} = \{e\}g)$ او $(\forall g \in G)(gG = G = Gg)$ صدق کوی.

بيلگه ۳- که P_M د $\S III$ د لمړی بیلگې گروپ وی ، نو د هغه سبگروپ $H = \{f_0, f_2, f_4\}$ د نوموړی گروپ نارمل سبگروپ دی. ځکه چې :

$$P_{M, H}^H = \{II, \{f_1, f_2, f_3\}\} = P_{M, H}^H$$

وروستي بيلگه بڼي چې د غير تبدیلی گروپونو نارمل وېشونکي امکان لری چې غير ساده سبگروپونه هم وی.

قضيه ۱- د G د گروپ سبگروپ H یوازی او یوازی هغه وخت د G د گروپ نارمل وېشونکي دی ،

$$(2) \dots (\forall g \in G)(h \in H \rightarrow g^{-1}hg \in H) \text{ که:}$$

ثبوت - فرضوو چې د G د گروپ سبگروپ H د نوموړی گروپ نارمل وېشونکي وی ، نودوهم تعريف د لمړی شرط له مخی د هر $g \in G$ او $h \in H$ داسی عنصر وجود لری چې $gh_1 = hg$ سره کيږی. ددی ځايه :

$$h_1 = g^{-1}hg \rightarrow g^{-1}hg \in H$$

برعکس، فرضوو چې د G د گروپ سبگروپ H (2) شرط پر ځای کوی. پدی معنی چې:

$$(\forall g \in G)(g^{-1}Hg \subset H) \text{ وی.}$$

اوس نو که د $g \in G$ د عنصر په عوض کی $g^{-1} \in G$ و ټاکو (آیا ددغه ټاکنی اجازه لرو؟)، نو وروستي

$$gHg^{-1} \subset H \text{ يا } (g^{-1})^{-1}Hg^{-1} \subset H$$

خو : $g^{-1}Hg \subset H \rightarrow g(g^{-1}Hg) \subset gH \rightarrow (gg^{-1})Hg \subset gH \rightarrow Hg \subset gH$

په همدا ډول : $gHg^{-1} \subset H \rightarrow (gHg^{-1})g \subset Hg \rightarrow gH \subset Hg$

د پورتنیو دوو کرښو په نتیجه کی $(\forall g \in G)(gH = Hg)$ سره کیږی.

د دوهم تعریف پر بنسټ د H سبگروپ د G ډگروپ نارمل وېشونکی دی. ثابته سوی قضیه مورته د لاندني واقعیت د فورمولبندی اجازه راکوی.

د G ډگروپ د نارمل وېشونکو مشترکه برخه بیا هم د G ډگروپ نارمل وېشونکی دی.

فرضوو چې H د G ډگروپ کیفی نارمل وېشونکی دی، پدی صورت کی $G_R^H = G_L^H$ د G ډگروپ د تجزیې څخه عبارت ده. څرنگه چې څرگنده ده (د لمړی برخی، د لمړی فصل §VI وگوری) چې د G پر سیټ باندی د معادل والی یوه اړیکه ε د نوموړی تجزیې جواب ورکونکی ده، پداسی ډول چې د G/ε فاکتور سیټ یا د G د سیټ تجزیه د G_L^H د تجزیې سره منطبقه ده. تر هغه ځایه چې د ε اړیکه د نارمل وېشونکی په ذریعه تعریف کیږی، نو د G ډگروپ د تجزیو سیټ په $G/H = G_R^H = G_L^H$ سره ښیو.

د G د سیټ د تجزیو پر سیټ، یعنی G/H باندی د فرعی ټولگیو د ضرب عملیه « \cdot » په لاندی ډول سره تعریفوو:

$$(\forall g_1, g_2 \in G)(g_1H \cdot g_2H = (g_1g_2)H) \quad \dots (3)$$

دلته باید یادونه وسی چې پورتنی اړیکه (3) د فرعی ټولگیو د نمایندده د ټاکلو تابع نده، پدی معنی چې که $g_1H = \bar{g}_1H$ او $g_2H = \bar{g}_2H$ وی، نو :

$$\begin{aligned} g_1H \cdot g_2H &= (g_1g_2)H = g_1(g_2H) = g_1(\bar{g}_2H) = g_1(H\bar{g}_2) = (g_1H)\bar{g}_2 = (\bar{g}_1H)\bar{g}_2 \\ &= \bar{g}_1(H\bar{g}_2) = \bar{g}_1(\bar{g}_2H) = (\bar{g}_1\bar{g}_2)H = \bar{g}_1H \cdot \bar{g}_2H \end{aligned}$$

پاس مو د سبسیتو د ضرب د عملیې د اتحادی خاصیت او نارمل وېشونکی د دوهم تعریف څخه استفاده کړیده.

قضیه ۲ - د G ډگروپ د سبگروپ H پر بنسټ د ټولو فرعی ټولگیو سیټ، یعنی G/H ، نظر د ټولگیو د ضرب و عملیې ته « \cdot » گروپ دی.

ثبوت - فرضاً $g_1, g_2, g_3 \in G$ وی، نو :

$$\begin{aligned} (g_1H \cdot g_2H) \cdot g_3H &= (g_1g_2)H \cdot g_3H = ((g_1g_2)g_3)H = (g_1(g_2g_3))H = \\ &= g_1H \cdot (g_2g_3)H = g_1H \cdot (g_2H \cdot g_3H) \end{aligned}$$

پدی معنی چې د « \cdot » عملیه اتحادی خاصیت لری.

د $H = eH$ فرعی ټولگی د بی تأثیره یا خنثی عنصر رول لوبوی، ځکه چې :

$$H \cdot gH = gH = gH \cdot H$$

د gH هرې ټولګې دپاره نظر د « \cdot » عملي ته معکوس عنصر وجود لري او هغه هم عبارت دی د $g^{-1}H$ د ټولګې څخه.

$$gH \cdot g^{-1}H = H = g^{-1}H \cdot gH \quad \text{په رشتيا هم :}$$

په نتيجه کې ويلای سو چې د G د تجزيې سيټ G/H نظر د ټولګيو د ضرب و عملي « \cdot » ته گروپ دی.

نومورئ گروپ ، يعنی G/H ، د نارمل وېشونکي H پر بنسټ د G د گروپ د تجزيې د گروپ په نامه يادوو.

§V. د گروپو ورته والي هومومورفيزم Homomorphism .

په عمومي ډول د الجبري ساختمانو او په خاص ډول د گروپونو د تطابق يا مختلف والي په هکله د قضاوت معيار د ايزومورفيزم مفهوم دی (§III وگورئ). د هغه مفهوم له مخې د G او G_1 گروپونه يودبله ايزومورف دی که د G د گروپ څخه د G_1 پر گروپ د بايجکشن $f: G \rightarrow G_1$ داسې مپينګ وجود ولري چې:

$$(\forall x, y \in G)(f(xy) = f(x) \cdot f(y))$$

پدې معنی چې د G او G_1 د گروپونو بعدونه مساوی او پر هغوی باندې علمي يو بل ته ورته خاصيتونه لري.

د بنوونځي د رياضي څخه پوهيږي چې همدارنگه معيارونه د بيلګې په توګه په هندسه کې هم سته. کله چې دوه هندسي شکلونه سره مقابسه کوو ، نو وايو چې هغوی مطابقت لري او يا يې نلري ، د بلي خوا د تشابه يا ورته والي مفهوم هم پيژني ، دغه مفهوم نظر د تطابق و مفهوم ته عمومي دی او په هندسه کې ډير مهم رول لوبوي.

په الجبر کې هم دغه ډول عمومي مفهوم وجود لري ، چې هغه عبارت له ورته والي يا هومومورفيزم Homomorphism څخه دی. دغه مفهوم بر سيره پر دی د نارمل وېشونکي د مفهوم سره ، چې په تېر پاراګراف کې مو وڅپري ، نژدې اړيکه لري.

تعريف ۱- د G د گروپ څخه د G_1 په گروپ کې هومومورفيزم عبارت دی له هغه مپينګ $f: G \rightarrow G_1$ څخه چې:

$$(\forall x, y \in G)(f(xy) = f(x) \cdot f(y))$$

په بله ژبه ويلای سو چې په هومومورفيزم کې گروپونه يودبل څخه مختلف بعدونه لري ، خو پر هغوی باندې عملي يواو بل ته ورته خاصيتونه لري.

څرګنده ده چې د G او G_1 د گروپو په منځ کې هر ايزومورفيزم په عين حال کې ددوی په منځ کې هومومورفيزم هم دی ، خو وروسته به وگورو چې ددغې ادعا عکس صدق نه کوي ، پدې معنی چې هر هومومورفيزم د گروپونو په منځ کې ايزومورفيزم ندی.

که $f: G \rightarrow G_1$ د G د سيټ څخه د G_1 پر سيټ باندې هومومورفيزم وی (يعنی د f مپينګ سرچکشن وی) ، نو په هغه صورت کې وايو چې د G د سيټ څخه د G_1 پر سيټ باندې هومومورفيزم دی او يا د G_1 سيټ د G د سيټ هومومورف (ورته) تصوير دی ، چې په $G \sim G_1$ سره ښيو.

بيلګه ۱- فرضاً د G او G_1 ځيني ضربی گروپونه وی او e_1 په G_1 په گروپ کې د عينيت عنصر وی. که د هر $x \in G$ دپاره د $f: G \rightarrow G_1$ مپينګ د $f(x) = e_1$ مساوات پذريعه تعريف کړو ، نو دغه مپينګ

د G د گروپ څخه د G_1 په گروپ کې هومومورفیزم دی، ځکه چې د هر $x, y \in G$ دپاره لاندې اړیکه صدق کوی:

$$f(xy) = e_1 = e_1 \cdot e_1 = f(x) \cdot f(y)$$

دلته مو د G د گروپ ټوله عنصرونه د G_1 د عینیت په عنصر e_1 کې انځور کړیدی.

بیلگه ۲- فرض کړو چې G گروپ او H د نوموړی گروپ کیفی نارمل وېشونکی وی، د G د گروپ څخه د هغه د تجزیې په گروپ کې G/H د ε مپینگ داسې څپړو چې:

$$(\forall x \in G)(\varepsilon(x) = xH)$$

د G/H د تجزیې په گروپ کې د « \cdot » د عملیې د تعریف څخه استنباط کیری چې د G د گروپ د ټولو عنصر و $x, y \in G$ دپاره صدق کوی چې:

$$\varepsilon(xy) = (xy)H = xH \cdot yH = \varepsilon(x) \cdot \varepsilon(y)$$

همدا ډول څرگنده ده چې د ε مپینگ د G د گروپ څخه د G/H پر گروپ باندې دی. نوموړی هومومورفیزم د G د گروپ څخه د هغه د تجزیې پر گروپ G/H باندې د اساسی او یا ستندرد (معیاری) هومومورفیزم په نامه یادېږی.

په پورتنی بیلگه کې مو وښودل چې د G د گروپ هر نارمل وېشونکی دهغه د معیاری هومومورفیزم جواب ورکونکی دی.

ددې دپاره چې معکوسه اړیکه مو هم ټینګه کړی وی، نو ځینی قضیې چې د گروپود هومومورفیزم خصوصیات بیانوی، دلته ثابتوو.

قضیه ۱- که f د G د گروپ څخه د G_1 په گروپ کې هومومورفیزم وی، نو د G د گروپ د عینیت د عنصر e انځور د G_1 په گروپ کې د G_1 د عینیت عنصر یعنی e_1 دی.

ثبوت - د $c \cdot c = c$ څخه $f(c) \cdot f(c) = f(c)$ استنباط کیری، بر سیره پر دی $c_1 \cdot f(c) = f(c)$ سره کیری. ځکه نو $f(e) \cdot f(e) = e_1 \cdot f(e)$ دی. د $f(e)$ د لڼډولو څخه وروسته $\{I\}$ ، د لمړی قضیې نتیجه وگورئ) به $f(e) = e_1$ لاسته راسی. qed

قضیه ۲- که f د G د گروپ څخه د G_1 په گروپ کې هومومورفیزم وی، نو:

$$(\forall x \in G)(f(x^{-1}) = f(x)^{-1})$$

ثبوت - فرضوو چې $f(x^{-1}) = g_1 \in G_1$ دی، نو پدی حالت کې:

$$e_1 = f(e) = f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1}) = f(x) \cdot g_1$$

$$e_1 = f(e) = f(x^{-1} \cdot x) = f(x^{-1}) \cdot f(x) = g_1 \cdot f(x)$$

د پورتنیو دوو مساواتو څخه استنباط کیری چې g_1 د $f(x)$ معکوس عنصر دی، یعنی $g_1 = (f(x))^{-1}$ دی. په نتیجه کې $f(x^{-1}) = f(x)^{-1}$.

قضیه ۳- که f د G د گروپ څخه د G_1 په گروپ کې هومومورفیزم وی، نو $f(G)$ د G_1 سبگروپ دی.

ثبوت - فرض کړو چې $g_1, g_2 \in f(G)$ وی، نو د ځینو $x, y \in G$ دپاره $g_1 = f(x)$ او $g_2 = f(y)$ سره کیری. او

$$g_1 \cdot g_2 = f(x) \cdot f(y) = f(x \cdot y) \in G$$

$$g_1^{-1} = (f(x))^{-1} = f(x^{-1}) \in G$$

پدی معنی چي $f(G)$ د G_1 سبگروپ دی.

اوس به نو د هومومورفیزم د هستی مفهوم تعریف کړو. فرض کړو f د G د گروپ څخه د G_1 په گروپ کی هومومورفیزم دی .

تعریف ۲- د هومومورفیزم f هسته عبارت ده د G د گروپ د ټولو هغو عنصر و د سیټ څخه ، چي د هغوی انځور د G_1 په سیټ کی د عینیت عنصر ، یعنی e_1 وی .

د هومومورفیزم f هسته په $\text{Ker } f$ سره بنیو. (د $\text{Ker } f$ مخفف د Kernel د کلیمی چي د هستی په معنی دی اخیستل سوی دی.)

قضیه ۴- د G د گروپ د هومومورفیزم f هسته ، یعنی $\text{Ker } f$ د G د گروپ نارمل وپشونکی دی.

ثبوت - لمړی باید ثابتته کړو چي $\text{Ker } f$ د G د گروپ سبگروپ دی.

فرض کړو چي $x, y \in \text{Ker } f$ وی، نو $f(x) = f(y) = e_1$ او $f(x \cdot y) = f(x) \cdot f(y) = e_1 \cdot e_1 = e_1$ سره کیری، پدی معنی چي $x \cdot y \in \text{Ker } f$ دی. علاوه پر دی $f(x^{-1}) = (f(x))^{-1} = e_1^{-1} = e_1$ دی.

یعنی $x^{-1} \in \text{Ker } f$. په نتیجه کی ویلای سو چي $\text{Ker } f$ د G د گروپ سبگروپ دی.

فرض کړو چي $x \in \text{Ker } f$ او $g \in G$ وی، نو :

$$f(g^{-1}xg) = f(g^{-1}) \cdot f(x) \cdot f(g) = f(g^{-1}) \cdot e_1 \cdot f(g) = (f(g))^{-1} \cdot f(g) = e_1$$

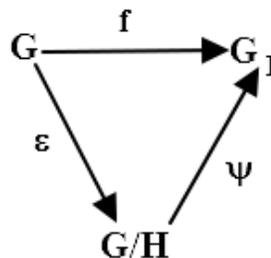
د §VI د لمړی قضیې څخه نتیجه اخیستل کیری چي $\text{Ker } f$ د G د گروپ نارمل وپشونکی دی.

ثابته سوی قضیه مور ته بنی چي د گروپ نارمل وپشونکی د هومومورفیزم پداسی ډول جواب ورکونکی دی چي هر معیاری هومومورفیزم $\varepsilon: G \rightarrow G/H$ د سبگروپ H سره منطبق کیری.

قضیه ۵ - (د گروپو د هومومورفیزم په هکله)

که f د G د گروپ هومومورفیزم او $H = \text{Ker } f$ وی، نو د G_1 د گروپ څخه د G/H پر گروپ یوازنی ایزومورفیزم ψ داسی وجود لری چي $f = \psi \circ \varepsilon$ ، پداسی حال کی چي ε د G څخه پر G/H باندی معیاری هومومورفیزم دی.

پاسنی حقیقت په لاندی ډول سره بنکاره کوو:



ویل کیری چي پورتنی ډیاگرام تبدیلی دی، یعنی: $f = \psi \circ \varepsilon$

ثبوت - فرض کړو چې $G \div xH$ د گروپ د سبگروپ $H = \text{Ker } f$ پر بنسټ اختیاری فرعی ټولګی ، x د هغه نماینده او $f(x) = g_1$ سره وی .

اوس نو که $y \in xH$ وی ، نو د H د کم عنصر $h \in H$ دپاره $y = xh$ سره کیږی. او:

$$f(y) = f(xh) = f(x) \cdot f(h) = f(x) \cdot c_1 = f(x)$$

سره کیږی. ددی ځایه استنباط کیدای سی چې د $\psi(xH) = f(x)$ مساوات د G/H د تجزیې گروپ میپینګ د G_1 په گروپ کی ، یعنی $\psi: G/H \rightarrow G_1$ ، ارائه کوی.

څرنګه چې f سرچکشن ده ، نو د ψ میپینګ هم سرچکشن دی ، بر سیره پر دی د $\psi(xH) = \psi(yH)$ استنباط کیږی چې: $f(x) = f(y)$ او $f(x) \cdot f(y^{-1}) = f(y) \cdot (f(y))^{-1} = e_1$ ، یعنی $x \cdot y^{-1} \in H$ دی.

پدی ترتیب $x \in Hy = yH$ او $xH = yH$ سره. پدی معنی چې د ψ میپینګ بایچکشن دی.

سر بیره پر دی د ټولو $xH, yH \in G/H$ دپاره لاندنی اړیکه صدق کوی:

$$\psi(xH \cdot yH) = \psi((xy)H) = f(xy) = f(x) \cdot f(y) = \psi(xH) \cdot \psi(yH)$$

یعنی ψ د G/H د گروپ څخه د G_1 پر گروپ آیزومورفیزم دی.

څرنګه چې د هر $g \in G$ څخه $\varepsilon(g) = gH$ سره دی ، نو :

$$\psi \circ \varepsilon(g) = \psi(\varepsilon(g)) = \psi(gH) = f(g) \quad \wedge \quad f = \psi \circ \varepsilon$$

په نتیجه کی قضیه په ثبوت ورسیده.

ثابته سوی قضیه بنیې چې د G د گروپ ټول هومومورفیزمونه دهغه د تجزیې د گروپ د معیاری هومومورفیزم پذیرعه محاسبه کیدای سی . پدی معنی چې د یوه گروپ د هومومورفیزم شمېر دهغه د نارمل وېشونکی د شمېر سره مساوی دی.

دوهم فصل رينگ (کری)

I§. رينگ - سب رينگ.

دلته به درينگ (کری) د مفهوم ، چي د لمړی برخي د دوهم فصل په I§III کی مو تعريف کی ، بياهم يادونه وکړو.

د K سيټ ، چي پر هغه باندی د جمع (+) او ضرب (.) دوه نيزی عمليي تعريف سوی وی ، د رينگ Ring (کری) په نامه يادپیری ، که لاندني شرطونه پر خای کی:

۱- د K سيټ نظر د جمع و عمليي ته گروپ دی.

۲- د جمع عمليه د K په سيټ کی تبديلی خاصيت لری.

۳- د ضرب عمليه د K په سيټ کی اتحادي خاصيت لری.

۴- د ضرب عمليه نظر د جمع و عمليي ته توزيعی خاصيت لری.

د رينگ بنی بيلگي د تامو عددو سيټ \mathbb{Z} نظر د جمع او ضرب و عمليي ته ، يعنی $\langle \mathbb{Z}, +, \cdot \rangle$ ، د ټولو نسبي (ناطقو) عددو سيټ \mathbb{Q} او د ټولو حقيقي عددو سيټ \mathbb{R} دی . په راتلونکی کی به درينگ دنورو بيلگو سره هم مخامخ سو. پاته دی نه وی چي د مختلطو عددو سيټ (لمړی برخه ، دوهم فصل ، VI§) او د حقيقي عددو پر فيلد $M_n(\mathbb{R})$ د n -ام ترتيب د ماترکسو سيټ (لمړی برخه ، څلرم فصل ، I§) هم درينگ ساختمان لری.

د ابل د گروپ د تعريف په نظر کی نيولو سره (لمړی فصل ، I§) کولای سو چي رينگ داسی هم تعريف کړو:

د K سيټ او په هغه کی د جمع او ضرب د تعريف سوی عمليو سره ، يعنی $\langle K, +, \cdot \rangle$ ، په هغه صورت کی کری ده چي لاندني شرطونه صدق وکی:

۱- د K سيټ نظر د جمع و عمليي ته د ابل گروپ دی.

۲- د K په سيټ کی د ضرب عمليه اتحادي خاصيت لری.

۳- د K په سيټ کی د ضرب عمليه نظر د جمع و عمليي ته توزيعی خاصيت لری.

که د K په سيټ کی پر پورتنیو خاصیتو برسیره د ضرب عمليه هم تبديلی خاصيت ولری ، نو نوموړی رينگ د تبديلی رينگ په نامه يادوو.

څرگنده ده چي د \mathbb{Z} ، \mathbb{Q} ، \mathbb{R} او \mathbb{C} رينگ ، تبديلی رينگ دی ، خو د $M_n(\mathbb{R})$ رينگ ، تبديلی رينگ ندی.

د K رينگ د واحد عنصر درلودونکی رينگ په نامه يادپیری که د K په سيټ کی نظر د ضرب و عمليي ته خنثی عنصر وجود ولری. په ياد يي ولری چي په مخکنی ټولو بيلگو کی د واحد عنصر درلودونکی رينگ سره په تماس کی ؤ . د \mathbb{Z} ، \mathbb{Q} ، \mathbb{R} او \mathbb{C} په رينگ کی واحد عنصر يو او د $M_n(\mathbb{R})$ په رينگ کی واحد عنصر د n -ام ترتيب واحد ماترکس ، يعنی E_n دی. په عين حال کی \mathbb{Z}_2 د

ټولو جفتو تامو عددو رينگ د بي واحدو عنصر د رينگ بڼه بيلگه ده. پدي معنی چي د ټولو جفتو تامو عددو رينگ واحد عنصر نلري.

د کتاب په لمړي فصل کي مو وليدل چي د گروپ د مفهوم تر څنگه د سبگروپ مفهوم د گروپ د تيوري په جوړولو او د هغه په بڼه درک کي ، ډير مهم رول درلودی. د رينگ په تيوري کي همداراز د سبرينگ Subring مفهوم ډير مهم رول لوبوي. دلته د سب کلمه چي د انگریزي څخه د لاندی په معنی ده ، په مشکله د پښتو د مفهوم کړی سره يو ځای کيدای سي ، تر کړی لاندی يا لاندی کړی بي خونده بنکاري ، خو په عين حال کي د فرعي رينگ د مفهوم سره چي پخوا په درسي کتابو کي په کاريدل هم موافق نه يم، ځکه چي د فرعي کلمه اصلي هدف نه اړانه کوي ، ځکه نو دلته د سب رينگ مفهوم بهتره بولم. په عين حال کي وروسته به د کړی پر ځای به هم د انگلیسي کلمه رينگ استعمالوم.

تعريف ۱- د K د رينگ غير خالی سب سيټ M د سبرينگ په نامه يادېږي، که د M سيټ نظر و هغه جمع او ضرب عمليو ته چي د K په رينگ کي راکړه سوی وي ، رينگ وي.

بيلگه ۱- د K هر رينگ د خپل ځان سبرينگ دی. د K د رينگ سبسيټ $M = \{0\}$ هم د K سب رينگ دی. نوموړي سبرينگونه د راکړه سوی رينگ د ابتدائي يا ساده (trivial) سبرينگ په نامه يادېږي.

بيلگه ۲- د تامو عددو رينگ \mathbb{Z} د نسبي عددو د رينگ \mathbb{Q} ، سبرينگ دی.

بيلگه ۳- د حقيقي عددو رينگ \mathbb{R} د مختلطو عددو د رينگ \mathbb{C} ، سب رينگ دی.

بيلگه ۴- د تامو عددو \mathbb{Q} پر رينگ د ټولو n ام ترتيب ماترکسو رينگ $M_n(\mathbb{Q})$ د حقيقي عددو پر رينگ د ټولو n ام ترتيب ماترکسو $M_n(\mathbb{R})$ د رينگ ، سب رينگ دی.

قضيه - د K د رينگ غير خالی سب سيټ $M \neq \emptyset$ يوازی او يوازی هغه وخت سب رينگ دی چي د هرو $a, b \in M$ دپاره $a+b$, $a-b$ او $a \cdot b$ هم د M په سيټ کي شامل وي.

ثبوت - که د M سبسيټ د K د رينگ سب رينگ وي ، نو د M سيټ نظر د جمع او ضرب و عمليي ته چي د K په رينگ کي تعريف سوی دی، ترلی دی علاوه پردی د هرو $a, b \in M$ د $b+x=a$ معادلی حل هم د M په سيټ کي شامل دی. په نتيجه کي $a-b \in M$ لاسته راځي.

معکوساً ، فرضوو چي د K د رينگ غير خالی سبسيټ يعنی د M سيټ د قضیي شرطونه پر ځای کوي. ځکه نو $0 \in M$ ، $a \in M$ کيږي . ددی ځايه د هر $a \in M$ ، $0-a = -a \in M$ دی. پدي معنی چي M د K سب گروپ دی. څرنگه چي د جمع د عمليي تبديلی خاصيت ، د ضرب د عمليي اتحادی خاصيت او د ضرب د عمليي توزیعی خاصيت نظر د جمع و عمليي ته د K د سيټ د ټولو عنصر و دپاره صدق کوي ، نو نوموړی خاصيتونه د M د سيټ د عنصر و دپاره هم صدق کوي. ځکه نو ادعا کولای سو چي M نظر د جمع او ضرب و عمليو ته چي د K په سيټ کي تعريف سوی دی ، سب رينگ دی.

د پورتنی قضیي په ذريعه کولای سو چي د K د رينگ غير خالی سب سيټ M امتحان کړو چي آیا د K د رينگ سب رينگ دی او که نه.

تعريف ۲- د مختلطو عددو هر سب رينگ د عددی رينگ په نامه يادوو.

د پورتنی قضیي څخه استنباط کيږي چي د S عددی سيټ يوازی او يوازی هغه وخت رينگ دی چي د S سيټ د دوو اختیاری عددو د جمع ، تفریق او د ضرب حاصل د S په سيټ کي شامل وي.

په یاد یې ولری ، پداسی حالت کی چي د K رینگ د عینیت (واحد) عنصر e ولری ، نو حتمی نده چي د هغه سب رینگ دی هم واحد عنصر e ولری . لکه دمخه چي مو هم یادونه وکړه چي د ټولو تامو عددو رینگ \mathbb{Z} واحد عنصر (1) لری، خو د جفتو تامو عددو رینگ \mathbb{Z}_2 واحد عنصر نلری.

بیلگه ۵- ثابتہ به یې کړو چي د $\mathbb{Z}[\sqrt{2}]$ سیټ ، د هغو عددو سیټ دی چي د $a+b\sqrt{2}$ شکل ولری ، پداسی حال کی چي $a, b \in \mathbb{Z}$ وی. یعنی د $\mathbb{Z}[\sqrt{2}] = \{x / x = a + b\sqrt{2} \wedge a, b \in \mathbb{Z}\}$ سیټ ، رینگ دی.

د پورتنی قضیې پر اساس کافی ده چي ثابتہ یې کړو چي د هرو دوو عددو چي د $a+b\sqrt{2}$ شکل ولری ، د هغوی د جمع ، ضرب او تفریق نتیجہ بیا هم د $a+b\sqrt{2}$ په بڼه وی. د لاندنیو مساواتو د څېړني په نتیجہ کی زموږ هدف استنباط کیری:

$$(a+b\sqrt{2}) \pm (c+d\sqrt{2}) = (a \pm c) + (b \pm d)\sqrt{2}$$

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$$

پداسی حال کی چي $a, b, c, d \in \mathbb{Z}$ دی.

بیلگه ۶- پر تام عددو باندی د n ام ترتیب ماترکسو رینگ ، پر حقیقی عددو باندی د n ام ترتیب ماترکسو د رینگ ، سب رینگ دی.

د پنځمی بیلگي په شان د ثابتوی سوی قضیې څخه په استفادہ سره ثابتیدلای سی. یعنی پر تام عددو د دوو ماترکسو جمع ، ضرب او تفریق ، بیرته پر تام عددو ماترکس راکوی.

بیلگه ۷- که $\mathbb{Z}[x]$ د ټولو هغو پولینومو سیټ وی چي ضریبونه یې تام عددونه وی او $\mathbb{R}[x]$ د ټولو هغو پولینومو سیټ وی چي ضریبونه یې حقیقی عددونه وی ، نو $\mathbb{Z}[x]$ د $\mathbb{R}[x]$ سب رینگ دی.

تر اوسه موږ رینگ بیلگي وړاندی کړی. لاندنی بیلگه مورته بڼی چي هر سیټ او پر هغه باندی عملیې رینگ کیدای نسی.

بیلگه ۸- د K د سیټ عنصرونه د $a+b\sqrt[3]{2}$ په شکل دی ، پداسی حال کی چي $a, b \in \mathbb{Z}$ دی.

د K سیټ د جمع ، ضرب او تفریق د عملیو سره چي د تامو عددو پر سیټ تعریف سوی دی ، رینگ ندی . ځکه چي :

$$\sqrt[3]{2} = 0 + 1 \cdot \sqrt[3]{2} \in K$$

خو:

$$\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4} \notin K$$

§ II . د رینگ ساده خاصیتونه.

پدی څپرکی کی به د رینگ ځنی مهم خاصیتونه تر مطالعی لاندی ونیسو.

د رینگ د تعریف له مخی د K هر رینگ نظر د جمع و عملیې ته په خپل ذات کی د آبل گروپ دی او دغه گروپ د K د رینگ د جمعی گروپ په نامه یادوو. که د لمړی فصل ، §I بیا وگوری ، نو د رینگ د عنصر په هکله لاندنی قضیې استنباط کیدای سی:

۱- په رینگ کی نظر د جمع و عملی ته دهغه صفری عنصر یوازنی بی تأثیره عنصر دی.

۲- نظر د جمع عملی ته د هر $a \in K$ عنصر دپاره د K په سیټ کی یوازنی متضاد عنصر $-a$ وجود لری .

۳- که $a+b=a+c$ وی، نو $b=c$ سره کیږی.

۴- د K د رینگ د عنصر د هر لار (ترادف) a_1, a_2, \dots, a_k دپاره د هغوی د جمع حاصل چي د $a_1+a_2+\dots+a_k$ د افادی په شکل تعریف سوی ده ، یوازنی دی.

که $a \in K$ او $n \in \mathbb{N}$ وی ، نو د a ، n ځله د جمع حاصل چي هر جزء یی د a عنصر وی په na سره

$$na = \underbrace{a+a+\dots+a}_n$$

ن - ځله

بښیو

پاملرته وکی چي پورتنی افاده د n او د a د ضرب د حاصل په صفت نسو قبلولای ، ځکه چي د K رینگ تل د تامو عددو رینگ په ځان کی نلری .

قضیه ۱- د K په هر رینگ کی ، د هغه د عنصر و $a, b \in K$ او د تامو عددو $m, n \in \mathbb{Z}$ دپاره لاندني مساواتونه صدق کوی:

- 1) $a - (-b) = a + b$
- 2) $-(a + b) = -a - b$
- 3) $ma + na = (m + n)a$
- 4) $ma + mb = m(a + b)$

ثبوت -

څرنگه چي $(-b) = b$ سره کیږی ، نو :

$$a - (-b) = a + [-(-b)] = a + b$$

همدا ډول :

$$a + b + (-a - b) = a + b + ((-a) + (-b)) = (a + (-a)) + (b + (-b)) = 0$$

په نتیجه کی $a + b - (a + b) = 0$ سره کیږی. یعنی دوهم مساوات حقیقت لری.

پاته خاصیتونه په §I کی د گروپ د خاصیتو څخه استنباط کیږی.

قضیه ۲- د K د رینگ د اختیاری عنصر و $a, b, c \in K$ دپاره لاندني مساواتونه صدق کوی:

- 1) $a \cdot 0 = 0 \cdot a = 0$
- 2) $a \cdot (-b) = -ab$
- 3) $(-a)b = -ab$
- 4) $(-a)(-b) = ab$
- 5) $a(b - c) = ab - ac \wedge (b - c)a = ba - ca$

ثبوت - څرنگه چي $a \cdot b + a \cdot 0 = a(b + 0) = ab$ سره کیږی ، نو $a \cdot 0 = ab - ab = 0$ سره دی.

همدا ډول $ab + a(-b) = a(b - b) = a \cdot 0 = 0$ سره دی ، پدی معنی چي د $a(-b)$ عنصر د $a \cdot b$ د

عنصر متضاد عنصر دی ، یعنی $a(-b) = -ab$ سره. په همدی شکل (3) او (4) مساواتونه ازمویلای

سو.

اوس به نو د وروستی مساوات لمړی برخه وگورو:

$$a(b-c)=a(b+(-c))=ab+a(-c)=ab-ac$$

همداهول د وروستي مساوات دوهمه برخه ازمويلای سو.

پنځم مساوات په خپل ذات کی ادعاکوی چي د ضرب عملیه نظر د تفریق و عملیې ته توزیعی خاصیت لری.

د K په رینگ کی د ضرب د عملیې د اتحادی خاصیت څخه په استفاده سره، په اسانې لاندنی خاصیتونه استنباط کیدای سی.

$$a^m \cdot a^n = a^{m+n} \quad \text{او} \quad (a^m)^n = a^{m \cdot n}$$

د پورتنی مساواتو دثبوت سره باید د بنوونځي په الجبر کی مخامخ سوی یاست. که د K رینگ تبدیلی رینگ وی، نو لاندنی مساوات هم صدق کوی:

$$(a \cdot b)^n = a^n \cdot b^n$$

که د K رینگ، تبدیلی رینگ وی او واحد عنصر ولری، پدغه رینگ کی د وپش د ورتوب داریکی عمومی بڼه تعریفولای سو.

تعریف ۱- د K د رینگ د a عنصر د همدی رینگ د $b \neq 0$ پر عنصر د وپش وړدی، که د K په رینگ د c داسی عنصر وجود ولری چي $a = b \cdot c$ سره سی.

پورتنی تعریف په ریاضی کی په سمبولیکه بڼه $a:b$ لیکو.

معلومه ده چي د وپش د ورتوب ":" د اړیکي عمومی شکل د تامو عددو د وپش ورتوب (په راتلونکی فصل کی به په مشرحه توگه وڅپړل سی) ته ورته خاصیتونه لری.

د K په رینگ کی د خارج قسمت د عنصر په هکله څه نسو ویلای؛ د بیلگی په توگه د $M_2(\mathbb{R})$ په رینگ کی لاندنی مساواتونه صدق کوی:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 5 & 0 \end{pmatrix}$$

پدی معنی چي د $a = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ او $b = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ د عنصر و دپاره دوه عنصره د $c_1 = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}$

او $c_2 = \begin{pmatrix} 0 & 0 \\ 5 & 0 \end{pmatrix}$ داسی وجود لری چي: $a = b \cdot c_1$ او $a = b \cdot c_2$

ددی دپاره چي د K په رینگ کی د خارج قسمت په هکله څه ویلای سو، نو باید د رینگ مخصوصی ټولگی تعریف کړو.

تعریف ۲- د K په تبدیلی رینگ کی چي واحد عنصر ولری، د $a \neq 0$ عنصر د K په رینگ کی د صفر د وپشونکی (قاسم) په نامه یادیری که د K په رینگ کی د $b \neq 0$ داسی عنصر وجود ولری چي $a \cdot b = 0$ سره سی.

تعريف ۳- د K تبديلي رينگ د واحد عنصر سره د انټيگرال دومين Integral Domain په نامه يادېږي ، که په نوموړي رينگ کې د صفر وپشونکي وجود ونلري.

عددي رينگونه ، انټيگرال دومين دی . ځکه چې د دوو غير صفری عددو د ضرب حاصل صفر کېدای نسي. علاوه پردې که K انټيگرال دومين وي ، نو د a د عنصر دوپش د وړتيا په صورت کې پر $b \neq 0$ باندې ، په K کې يوازنی د q عنصر وجود لري چې $a=b \cdot q$ سره کېږي. ځکه چې د $bq_1=bq_2$ استنباط کېږي چې $b(q_1-q_2)=0$ سره کېږي . څرنگه چې $b \neq 0$ دی ، نو $q_1-q_2=0$ سره کېږي ، يعنی $q_1=q_2$ دی.

په پورتنۍ حالت کې د q عنصر د $b \neq 0$ پر عنصر باندې د a د تقسيم د خارج قسمت په نامه يادېږي.

کله کله انټيگرال دومين د واحد عنصر سره د هغه تبديلي رينگ په صفت تعريفوی چې په هغه کې داخصار قانون Cancellation law صدق وکي، يعنی که $c \neq 0$ وي او $ca=cb$ سره وي، نو $a=b$ سره کېږي.

تردی وروسته به يوازی انټيگرال دومين زموږ د څېړنې موضوع وي.

§ III. آيديال رينگ او پر هغه باندې عمليي .

که لږ څه شاته د گروپ تيوري ته نظر واچوو ، نو د راکړه سوی گروپ د ټولو سبگروپو په منځ کې د گروپ نارمل وپشونکي (لمړی فصل ، § IV) ډير مهم رول لوباوه. د رينگ په تيوري کې هم دغه ډول الجبري ساختمان وجود لري چې د آيديال رينگ په نامه يادېږي.

تعريف ۱- د K د رينگ غير خالی سبسيټ $I \neq \emptyset$ د K په رينگ کې د K د رينگ د آيديال په نامه يادېږي ، که لاندې شرطونه صدق وکي:

$$1- (\forall a, b \in I)(a-b \in I)$$

يعنی د I سبټ د خپلو دوو اختياري عنصر و تفاضل يا دتفریق حاصل هم په ځان کې لري.

$$2- (\forall a \in I)(\forall b \in K)(a \cdot b \in I \wedge b \cdot a \in I)$$

په اسانۍ سره ليدل کېږي چې د K د رينگ هر آيديال رينگ I د K د رينگ، سب رينگ دی. ځکه چې د $I \neq \emptyset$ ځخه استنباط کېږي چې د $a \in K$ کوم عنصر دپاره ، $a \in I$ دی.

د لمړي شرط له مخې د هر $a \in I$ دپاره $a-a=0 \in I$ او $-a=0-a \in I$ دی. ددی خپه که $a, b \in I$ وي ، نو $a+b=a-(-b) \in I$ دی. په نتیجه کې د I و قضیې پر اساس قضاوت کولای سو چې د K د رينگ سبسيټ I ، د K د رينگ سب رينگ دی.

بيلگه ۱- د K رينگ د خپل ځان آيديال رينگ دی. څرنگه ده چې د $I = \{0\}$ هم د K د رينگ ، آيديال رينگ دی.

بيلگه ۲- د ټولو جفتو تامو عددو سبټ $I = \mathbb{Z}_2$ د تامو عددو \mathbb{Z} په رينگ کې ، آيديال دی.

بيلگه ۳- فرضوو چې K تبديلي رينگ او $a \in K$ دی. د $I = \{a \cdot x / x \in K\}$ سبټ د K په رينگ کې آيديال دی. په رشتيا هم د K د رينگ د ټولو $x, y, x_1, x_2 \in K$ دپاره صدق کوي چې:

$$ax_1 - ax_2 = a(x_1 - x_2) \in I \quad \text{او} \quad (ax)y = a(xy) \in I$$

تعریف ۲ - K په تبدیلی رینگ کی $I = \{a.x / x \in K\}$ په رینگ کی a د عنصر پذیرعه تشکیل سوی اساسی آیديال $I = (a)$ په نامه یادیری او په $I = (a)$ سره یې بنیو.

په اسانی سره لیدل کیږی چې د تامو عددو \mathbb{Z} په رینگ کی د \mathbb{Z}_2 آیديال اساسی آیديال دی چې د 2 د عدد پذیرعه تشکیل سوی دی ، یعنی $\mathbb{Z}_2 = (2)$.

بیلگه ۴ - د پولینومو په هغه رینگ کی چې ضربونه یې تام عددونه وی $\mathbb{Z}[x]$ ، د ټولو هغو پولینومو سیټ I چې ثابت حد یې د صفر سره مساوی وی ، اساسی آیديال دی چې په $I = (x)$ سره یې بنیو.
(د کورنی کار په شکل یې امتحان کړی!)

قضیه ۱- د K د رینگ I_1 او I_2 آیديالو مشترکه برخه $I_1 \cap I_2$ د K د رینگ آیديال دی.

ثبوت - څرنگه چې $0 \in I_1$ او $0 \in I_2$ دی ، نو $0 \in I_1 \cap I_2$ دی. یعنی $I_1 \cap I_2 \neq \emptyset$ خالی ندی. فرضوو چې $a, b \in I_1 \cap I_2$ وی ، نو په عین حال کی $a, b \in I_1$ او $a, b \in I_2$ دی . د آیديال د تعریف د لمړی شرط پر اساس په عین حال کی $(a-b) \in I_1$ او $(a-b) \in I_2$ دی ، پدی معنی چې $(a-b) \in I_1 \cap I_2$ دی. همدا ډول ، فرضوو چې $a \in I_1 \cap I_2$ او $b \in K$ وی. څرنگه چې په عین حال کی $a \in I_1$ او $a \in I_2$ دی . د بلی خوا I_1 او I_2 د K د رینگ آیديالونه دی ، نو د لمړی تعریف دوهم شرط پر اساس $b.a, a.b \in I_1$ او $b.a, a.b \in I_2$ دی ، پدی معنی چې $b.a, a.b \in I_1 \cap I_2$ دی . پدی ترتیب د $I_1 \cap I_2$ سب سیټ خالی ندی او د لمړی تعریف شرطونه پر ځای کوی. پدی معنی چې $I_1 \cap I_2$ د K د رینگ آیديال دی.

د ثابتی سوی قضیې پر اساس کولای سوچي زموږ ادعا ته د K د رینگ پرمتناهی تعداد اختیاری آیديالو ته عمومیت ورکړو . خو په عین حال کی باید دی ټکی ته متوجه اوسو چې د K د رینگ د آیديالو اتحاد حتمی نده چې د نوموړی رینگ آیديال دی وی. ددی ادعا د ثبوت دپاره کافی ده چې د تامو عددو \mathbb{Z} په رینگ کی د (2) او (5) آیديالونه په نظر کی ونیسو . د $I = (2) \cup (5)$ آیديال یوازی هغه عددونه احتوا کوی چې هغوی پر 2 او یا پر 5 دوپشور وی ، ځکه نو $2 \in I$ او $5 \in I$ دی ، خو $3 \notin I$ ، یعنی د رینگ د آیديال د تعریف لمړی شرطونه پر ځای کوی.

د رینگ پر آیديالو باندی نوری عملیې هم تعریفولای سو . په خاص ډول د K د رینگ I_1 او I_2 آیديالو د جمع حاصل یعنی $I_1 + I_2$ عبارت دی د ټولو هغو عنصر د سیټ څخه چې د $a+b$ په شکل وی ، پداسی حال کی چې $a \in I_1$ او $b \in I_2$ وی.

په اسانی سره لاندنی قضیه ثابتولای سو

قضیه ۲- د K د رینگ I_1 او I_2 آیديالو د جمع حاصل یعنی $I_1 + I_2$ ، د K د رینگ آیديال دی.

د پورتنی قضیې د حقانیت ثبوت لوستونکو ته د تمرین په شکل وړاندیزوو.

§IV. د رینگ تجزیه (Factor Ring).

که I د K په رینگ کی آیديال وی، نو د I جمعی سب گروپ د K د رینگ د جمعی گروپ نارمل وېشونکی دی. I د نارمل وېشونکی په صفت د K/I د گروپ تجزیه تعینوی (لمړی فصل ، §IV وگورئ) . د سب گروپ I پر بنسټ د K د گروپ فرعي ټولگی د I د آیديال پر بنسټ د K د رینگ د باقیمانده و د ټولگیو په نامه یادوو . د گروپ په تیوری کی مو مطالعه کړه چې د I د آیديال پر بنسټ د K د رینگ د باقیمانده و ټولگی چې د هغه نماینده $a \in K$ وی ، د $a+I$ شکل لری. د آیديالی جمع عملیه \oplus د K/I د گروپ په تجزیه کی د لاندنی اړیکی په ذریعه راکړه سوی ده:

$$(a+I) \oplus (b+I) = (a+b)+I$$

دلته باید یوه واقعیت ته څیر سو ، هغه دا چې دلته دوی مختلفې د جمع عملیې لرو . د \oplus په ذریعه دوی مختلفې د تجزیې ټولګې سره جمع کوو او د $+$ په ذریعه د K د رینګ د a عنصر د I د عنصر و سره جمع کوو.

د K/I په سیټ کې د ایډیالو ترمنځ د ضرب عملیه په لاندې ډول سره تعریفوو:

$$(a+I) \otimes (b+I) = a \cdot b + I \quad \dots(1)$$

د پورتنۍ تعریف درست والی باید ثابت کړو ، پدې معنی چې پورتنۍ اړیکه پرته له دې چې د نکر سوو ټولګیو د نماینده گانو خصوصیتونه په نظر کې ونیسو ، صدق کوی.

په رشتیا هم همداسی ده . فرضوو چې $a_1 \in a+I$ او $b_1 \in b+I$ یعنی a_1 او b_1 د راکړه سوو ټولګیو دوه نور نماینده گان دی. نو د $i_1, i_2 \in I$ دپاره $a_1 = a + i_1$ او $b_1 = b + i_2$ دی. اوس به نو a_1 او b_1 د ضرب حاصل وگورو:

$$a_1 \cdot b_1 = (a+i_1)(b+i_2) = a \cdot b + a \cdot i_2 + b \cdot i_1 + i_1 \cdot i_2$$

څرنگه چې $a \cdot i_2 \in I$, $b \cdot i_1 \in I$ او $i_1 \cdot i_2 \in I$ دی ، نو $a_1 \cdot b_1 \in a \cdot b + I$ دی. په نتیجه کې ویلای سو چې $a_1 \cdot b_1 + I = a \cdot b + I$ کیری. پدې معنی چې د ایډیالو ضرب $(a+I) \otimes (b+I)$ د $a+I$ او $b+I$ په ټولګیو کې د هغود نماینده گانو د انتخاب تابع ندی.

قضیه - د K د رینګ د ایډیال پر اساس I د K/I د باقیمانده و د ټولګیو سیټ ، نظر د ایډیالو د جمع \oplus او د ایډیالو د ضرب \otimes و عملیو ته رینګ دی.

ثبوت - څرگنده ده چې K/I نظر د جمع \oplus و عملیې ته گروپ دی (لمړی فصل، § IV وگوری) همدابول :

$$(a+I) \oplus (b+I) = (a+b)+I = (b+a)+I = (b+I) \oplus (a+I)$$

پدې معنی چې K/I د ابل گروپ دی. علاوه پر دې:

$$[(a+I) \otimes (b+I)] \otimes (c+I) = (ab+I) \otimes (c+I) = (ab)c+I = a(bc)+I =$$

$$= (a+I) \otimes (bc+I) = (a+I) \otimes [(b+I) \otimes (c+I)]$$

یعنی د ضرب عملیه \otimes اتحادی خاصیت لری.

اوس به نو د ایډیالو د ضرب د عملیې توزیعی خاصیت نظر د ایډیالو د جمع و خاصیت ته و آزمویو:

$$(a+I) \otimes [(b+I) \oplus (c+I)] = (a+I) \otimes [(b+c)+I] = a(b+c)+I = (ab+ac)+I =$$

$$= (ab+I) \oplus (ac+I) = (a+I) \otimes (b+I) \oplus (a+I) \otimes (c+I)$$

په عین ډول لاندنۍ مساوات امتحانولای سو:

$$[(b+I) \oplus (c+I)] \otimes (a+I) = (b+I) \otimes (a+I) \oplus (c+I) \otimes (a+I)$$

په مجموع کې نتیجه اخیستلای سو چې د K/I د ټولګیو سیټ نظر د جمع \oplus او ضرب \otimes و عملیو ته رینګ دی.

تعريف - د K/I رينگ د I د آيدپال پر اساس د K د رينگ د تجزيې (Factor Ring) په نامه يادېږي. موږ به يې تردې وروسته K/I د فاکتور رينگ په نامه يادوو. پدې معنی چې د K/I څخه به مو مقصد د I د آيدپال پر اساس د K د رينگ تجزيه وي.

بيلگه ۱- د K/K فاکتور رينگ يوازې يو عنصر لري ، يعنی صفری رينگ دی.

بيلگه ۲- د $K/\{0\}$ فاکتور رينگ عنصرونه د ټولو عنصر $a \in K$ دپاره د $a+0=a$ شکل لري. د $K/\{0\}$ فاکتور رينگ د K د رينگ سره آيزومورف دی. نوموړی آيزومورفيزم د لاندني مساوات پذريعه ارائه کيدای سي:

د ټولو $a \in K$ دپاره $f(a) = \{a\}$ دی.

بيلگه ۳- د $Z/(2)$ فاکتور رينگ يوازې دوه عنصره د (2) او $(2)+1$ لري.

د فاکتور رينگ د نورو مثالو سره به په راتلونکي مطالعاتو کې هم مخامخ سو.

§۷. د رينگو ورته والي (هومومورفيزم Homomorphism)

دلمری فصل په V کې مو د گروپو د ورته والی يا هومومورفيزم مفهوم طرح او د هغه اړيکه مو د گروپ د نارمل وېشونکي او د هومومورفيزم ترمنځ ځای پر ځای کړه. همدا ډول د هومومورفيزم مفهوم په رينگ کې هم طرح کولای سو.

بنکاره ده چې د رينگ د آيدپال او د رينگ د هومومورفيزم تر منځ اړيکه د گروپ د نارمل وېشونکي او د گروپ د هومومورفيزم و مفهوم ته ورته ده.

فرض کړو چې د K او K_1 رينگونه راکړه سوی دی.

تعريف ۱- د K د رينگ څخه د K_1 په رينگ کې مپينگ $f: K \rightarrow K_1$ ، د هومومورفيزم په نامه يادېږي که لاندی شرطونه صدق وکي:

- 1) $(\forall a, b \in K)(f(a+b) = f(a) + f(b));$
- 2) $(\forall a, b \in K)(f(a.b) = f(a).f(b)).$

که د f مپينگ سرچکشن وي ، نو وايو چې هومومورفيزم د K د رينگ څخه د K_1 پر رينگ باندی راکړه سوی دی. پدغه حالت کې وايو چې د K_1 رينگ د K د رينگ هومومورف انځور (تصوير) دی.

بيلگه ۱- د هر رينگ K په اختياری رينگ K_1 کې ساده هومومورفيزم وجود لري. نوموړی هومومورفيزم د هر $x \in K$ دپاره د $f(x) = 0$ سره تعريفولای سو. ځکه چې د هر $a, b \in K$ دپاره لاندی مساواتونه صدق کوي:

$$f(a+b) = 0 = 0 + 0 = f(a) + f(b)$$

$$f(a.b) = 0 = 0.0 = f(a).f(b)$$

بيلگه ۲- د ټولو پولينو مو رينگ چې ضريبونه يې تام عددونه وي يعنی $\mathbb{Z}[x]$ او د تامو عددود رينگ \mathbb{Z} ترمنځ د f مپينگ داسی تعريفوو چې د هر پولينوم $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ په مقابل کې د

هغه پولینوم ثابت جز یعنی a_0 ایردو . دغه ډول تعریف سوی میپینگ د $\mathbb{Z}[x]$ څخه پر \mathbb{Z} باندی هومومورفیزم دی . ځکه چي :

$$\begin{aligned} f((a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) + (b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0)) &= \\ f((a_n + b_n) x^n + (a_{n-1} + b_{n-1}) x^{n-1} + \dots + (a_1 + b_1) x + (a_0 + b_0)) &= a_0 + b_0 = \\ f(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) + f(b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0) & \end{aligned}$$

او

$$\begin{aligned} f((a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) \cdot (b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0)) &= \\ f(a_n b_n x^{2n} + \dots + (a_1 b_0 + b_1 a_0) x + a_0 b_0) &= a_0 b_0 = \\ = f(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) \cdot f(b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0). & \end{aligned}$$

څرگنده ده چي د f میپینگ سرچکشن دی.

قضیه ۱- د K درینگ د هر آیديال I دپاره د K درینگ څخه د هغه پر فاکتور رینگ K/I باندی د $\varepsilon: K \rightarrow K/I$ هومومورفیزم وجود لری.

ثبوت - زموږ د نظر میپینگ ε د هر $x \in K$ د پاره د $\varepsilon(x) = x + I$ په ذریعه ارانه کوو. څرنگه چي هر د x عنصر د I آیديال پر اساس په یوه باقیمانده ټولگی پوری اړه لری او په بله اصطلاح هر د x عنصر د I آیديال پر اساس یوی باقیمانده ټولگی ته منسوب دی ، نو د ε میپینگ سرچکشن دی ، علاوه پر دی:

$$\varepsilon(x+y) = x+y+I = (x+I) \oplus (y+I) = \varepsilon(x) \oplus \varepsilon(y)$$

$$\varepsilon(x \cdot y) = xy+I = (x+I) \otimes (y+I) = \varepsilon(x) \otimes \varepsilon(y)$$

د ε هومومورفیزم د معیاری یا ستندرد هومومورفیزم په نامه یادوو.

قضیه ۲- که f د K درینگ څخه د K/I په رینگ کی هومومورفیزم وی ، نو :

$$1) f(0) = 0$$

$$2) (\forall a \in K)(f(-a) = -f(a))$$

$$3) f(K) \text{ د } K \text{ سبرینگ دی.}$$

د قضیې ثبوت د لمړی فصل د $\S 7$ لمړی ، دوهمی او دریمي قضیې ته ورته دی.

تعریف ۲ - که $f: K \rightarrow K_1$ د K هومومورفیزم د K_1 په رینگ وی ، نو د $\text{Ker } f$ سیټ د ټولو هغو عنصر و سیټ چي تصویر یی د K_1 په رینگ کی د صفر عنصر وی د هومومورفیزم د هستی په نامه یادیری.

په لمړی بیلگه کی د هومومورفیزم هسته د K مکمل رینگ تشکیلوی. په دوهمه بیلگه کی د هومومورفیزم هسته د ټولو هغو پولینومو سیټ دی چي ضریبونه یی تام عددونه وی او ثابت جزء یی مساوی په صفر سره وی.

قضیه ۳- د K درینگ د هومومورفیزم f هسته $\text{Ker } f$ د K درینگ آیديال دی.

ثبوت - فرض کرو چي $a, b \in \text{Ker } f$ وی ، نو $f(a) = f(b) = 0$ دی ، او :

$$f(a-b)=f(a+(-b))=f(a)+f(-b)=f(a)-f(b)=0-0=0$$

پدی معنی چي $a-b \in \text{Ker} f$ دی.

که $x \in \text{Ker} f$ وی ، نو :

$$f(a.x)=f(a).f(x)=0.f(x)=0$$

$$f(xa)=f(x).f(a)=f(x).0=0$$

پدی معنی چي $ax \in \text{Ker} f$ او $xa \in \text{Ker} f$ دی.

همدا ډول د قضیې عکس هم حقیقت لری.

قضیه ۴ - د K د رینگ هر آیديال I د هغه رینگ د هومومورفیزمو څخه د یوه هومومورفیزم هسته ده.

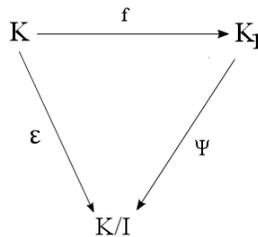
ثبوت - معیاری یا ستندرد هومومورفیزم $\varepsilon: K \rightarrow K/I$ څېرو. څرنگه چي $\varepsilon(0)=0+I=I$ سره دی. نو I په فاکتور رینگ K/I کی صفر دی. ځکه چي یوازی او یوازی د I آیديال د عنصر و تصویر د ε په هومومورفیزم کی د K/I په رینگ کی ، صفر دی. ځکه نو $\text{Ker} \varepsilon = I$ سره کیږی.

د ثابتی سوږو قضیو څخه په استفاده سره کولای سو چي د رینگو د هومومورفیزم په هکله قضیه فورمولبندی کرو.

قضیه ۵ - (د رینگو د هومومورفیزم په هکله قضیه)

که f د K د رینگ هومومورفیزم د K_1 پر رینگ باندی او $I = \text{Ker} f$ وی ، نو د K_1 او K/I یوازنی آیزومورفیزم Ψ داسی وجود لری چي $\varepsilon \circ \Psi = f$ دی، پداسی حال کی چي ε د K د رینگ څخه پر K/I پر رینگ باندی معیاری (ستندرد) هومومورفیزم دی.

پورتنی قضیه د ډیاگرام پذیرعه داسی بنودلای سو:



په قضیه کی غواړو چي وښیو ، چي پورتنی ډیاگرام تبدیلی دی، یعنی $f = \Psi \circ \varepsilon$.

د پنځمی قضیې ثبوت د گروپ د هومومورفیزم د قضیې په ډول دی او ثبوت یې لوستونکو ته د تمرین په شکل پریردو.

دریم فصل

د تامو عددو په رینگ (کری) کی د وپش د ورتوب تیوری

§.1 د وپش د ورتوب اړیکه او دهغه ساده خاصیتونه.

په بنوونځیو کی د تامو عددو و تدریس ته ډیر ځای ورکړه سوی دی، ځکه نو د بنوونځی د بنوونکو دپاره لازمه ده چي د تامو عددو په اړوند یې ټوله نظری بنسټیزې په ژوره توگه درک کړی وی. پدی معنی چي بنوونکی باید د تامو عددو په سیټ او د هغه په خاصیتو کی په کافی اندازه وارد وی.

دلته به یو ځل بیا پر هغه مفهومو چي ددی کتاب په لمړئ برخه کی موزده کړل (الجبر او د عددونو تیوری لمړی برخه، دوهم فصل وگوری)، حواله درکړم. هلته مو وویل چي د تامو عددو سیټ \mathbb{Z} نظر د ضرب او جمع عملیې ته، $\langle \mathbb{Z}, +, \cdot \rangle$ ، د الجبری عمومی ساختمان چي د تبدیلی کړی (رینگ) په نامه یادېږی، بیلگه ده. پدی معنی چي د جمع او ضرب عملیې د تامو عددو په سیټ \mathbb{Z} کی تبدیلی او اتحادی خاصیت لری، د ضرب عملیې نظر د جمعی و عملیې ته توزیعی ده. د تامو عددو په سیټ کی د تفریق عملیې هم اجراء کولای سو، پدی معنی چي د دوو تامو عددو د تفریق حاصل او یا لاسته راوړنه بیا هم تام عدد دی، یعنی د تامو عددو سیټ نظر د تفریق عملیې ته تړلی دی. په بله اصطلاح د تامو عددو سیټ \mathbb{Z} نظر د جمع او ضرب و عملیو ته تبدیلی رینگ دی. زمور په مخ کی د څېړنو دپاره فرضوو چي لوستونکی د مطلقه قیمت د مفهوم او د هغه د خاصیتو سره آشنا دی.

اوس به یې نو د تامو عددو د وپش د ورتوب د خاصیتو د مطالعی څخه را شروع کړو.

تعریف - د a یو تام عدد پر یو بل تام عدد b ، پداسی حال کی چي $b \neq 0$ وی، د وپش وړ دی (قابل تقسیم دی) چي داسی تام عدد q وجود ولری چي $a = b \cdot q$ سره وی.

پدغه حالت کی د a عدد د مقسوم، د b عدد د مقسوم علیه او د q عدد د خارج قسمت په نامه یادېږی. که a پر b بانندی د وپش وړ وی، نو لیکو: $a:b$.

په سمبولیک شکل پورتنی تعریف په لاندی ډول سره فارمولبندی کولای سو.

$$(\forall a, b \in \mathbb{Z}, b \neq 0)(a:b) \Leftrightarrow (\exists q \in \mathbb{Z})(a = b \cdot q)$$

د بیلگی په توگه 42 پر 7 د وپش وړ دی $(42:7)$ ، ځکه چي $42 = 7 \cdot 6$ سره. دلته د q تام عدد مساوی کیری په 6 سره. همدا ډول $3:-27$ دی، ځکه چي $(-9) \cdot (-3) = 27$ سره. بله په زړه پوری بیلگه $0:3$ ده، ځکه چي $0 = 3 \cdot 0$ سره کیری.

د وپش د ورتوب اړیکه $a:b$ ، د تامو عددو \mathbb{Z} په سیټ کی یوه دوه نېزه اړیکه ده. د نوموړی دوه نېزی اړیکی ځینی خاصیتونه په لاندی ډول تر مطالعی لاندی نیسو.

۱- د صفر عدد پر هر تام عدد $a \neq 0$ چي د صفر څخه خلاف وی، د وپش وړ دی.

$$(\forall a \in \mathbb{Z})(a \neq 0 \rightarrow 0:a)$$

ځکه چي $0 = a \cdot 0$ سره کیری. دلته د q تام عدد مساوی کیری په 0 سره.

۲- هر تام عدد a پر 1 او -1 د وپش وړ دی.

$$(\forall a \in \mathbb{Z})(a:1 \wedge a:(-1))$$

$$a=(-1).(-a) \wedge a=1.a$$

خُکِه چي:

۳- د صفر خُکِه خلاف د $a \neq 0$ هر تام عدد پر a او $-a$ دوپش وړ دی. یعنی:

$$(\forall a \in \mathbb{Z})(a \neq 0 \rightarrow a:a \wedge a:(-a))$$

خُکِه چي: $a=(-a)(-1) \wedge a=1.a$ سره کيږي.

نتیجه - د طبیعي عددو په سیټ او د نامو عددو، چي د صفر خُکِه خلاف وی، په سیټ کی دوپش د ورتوب اړیکه انعکاسی خاصیت لری.

د نتیجی ثبوت دوپش د ورتوب ددریم خاصیت او د غیرکونی اړیکی د انعکاسی والی د تعریف خُکِه استنباط کيږي. خُکِه چي:

$$(\forall a \in \mathbb{N})(a:a) \wedge (\forall a \in \mathbb{Z} / \{0\})(a:a)$$

۴- دوپش د ورتوب اړیکه انتقالی خاصیت لری، پدی معنی چي:

$$(\forall a, b, c \in \mathbb{Z})(a:b \wedge b:c \rightarrow a:c)$$

ثبوت - خرنګه چي $a:b$ (په a پر b دوپش وړدی)، نو b باید د صفر خُکِه خلاف وی، یعنی $b \neq 0$ او داسی تام عدد q وجود لری چي $a=bq$ سره کيږي. همدا ډول د $b:c$ خُکِه استنباط کيږي چي $c \neq 0$ او د q_1 داسی تام عدد وجود لری، چي $b=cq_1$ سره کيږي. خُکِه نو:

$$a=bq=(cq_1)q=c(q_1q)$$

خرنګه چي q_1q تام عدد دی، نو $a:c$.

۵- د مقسوم او مقسوم علیه د علامو د تغییر ورکولو په نتیجه کی دوپش د ورتوب په اړیکه کی تغییر نه راخی (په بله اصطلاح دوپش د ورتوب اړیکه ساتل کيږي)، یعنی:

$$(\forall a, b \in \mathbb{Z}, b \neq 0)(a:b \rightarrow a:(-b) \wedge (-a):b \wedge (-a):(-b))$$

ثبوت - که $a:b$ وی، نو د q داسی تام عدد به وجود ولری چي $a=bq$ سره کيږي. خُکِه نو:

$$a=(-b)(-q) \wedge -a=b(-q)=-bq$$

۶- که د a او b تام عددونه د c پر تام عدد دوپش وړ وی، نو دهغوی د جمع حاصل او د تفریق حاصل هم د c پر عدد دوپش وړ دی، یعنی:

$$(\forall a, b, c \in \mathbb{Z})(a:c \wedge b:c \rightarrow (a+b):c \wedge (a-b):c)$$

ثبوت - د $a:c$ او $b:c$ دوپش د ورتوب د تعریف خُکِه استنباط کيږي چي د q او q_1 داسی تام عددونه وجود لری چي $a=cq$ او $b=cq_1$ سره کيږي، خُکِه نو:

$$a+b=cq+cq_1=c(q+q_1)$$

$$a-b=cq-cq_1=c(q-q_1)$$

یعنی: $(a+b):c$ او $(a-b):c$.

۷- که د a او b د تامو عددو د حاصل ضرب $a \cdot b$ د ضربی عاملو څخه یو عامل د c پر تام عدد دوپش وړ وی ، نو هغوی د ضرب حاصل هم د c پر عدد دوپش وړ دی، یعنی :

$$(\forall a, b, c \in \mathbb{Z})(a:c \vee b:c \rightarrow a \cdot b:c)$$

ثبوت - فرضوو چې $a:c$ دی. پدی معنی چې د q تام عدد داسی وجود لری چې $a = c \cdot q$ سره کیږی . که د وروستي مساوات دواړی خواوی د b په عدد کی ضرب کړو نو $a \cdot b = c \cdot b \cdot q$ لاسته راځی. پدی معنی چې $a \cdot b:c$ دی.

۸- که $a_1:c, a_2:c, \dots, a_n:c$ وی ، نو د b_1, b_2, \dots, b_n اختیاری تامو عددو د پاره لاندنی اړیکه صدق کوی: $(a_1 b_1 + a_2 b_2 + \dots + a_n b_n):c$

پورتنی خاصیت مخامخ د ۶م او ۷م خاصیت څخه استنباط کیږی.

۹- که $a:b$ او $a \neq 0$ وی ، نو $|a| \geq |b|$ دی.

ثبوت - د $a:b$ د فرضیې څخه $a = b \cdot q$ لاسته راځی ، ځکه نو :

$$|a| = |b \cdot q| = |b| \cdot |q| \geq |b|$$

نتیجه ۱- که $1:a$ وی ، نو $a=1$ او یا $a=-1$ سره کیږی.

ثبوت - د $1:a$ د فرضیې او نهم خاصیت څخه استنباط کیږی چې $1 \geq |a|$.

د بلی خوا د هر تام عدد a دپاره چې د صفر څخه خلاف وی $|a| \geq 1$ دی . پدی معنی چې : $|a| = 1$ سره کیږی او یا په بله اصطلاح $a=1$ او یا $a=-1$ سره کیږی.

نتیجه ۲- که $a:b$ او $b:a$ وی ، نو یو د مساواتو څخه یا $a=b$ او یا $a=-b$ حقیقت لری.

ثبوت - د $a:b$ د اړیکې په نتیجه کی $|a| \geq |b|$ لاسته راځی او د $b:a$ د اړیکې په نتیجه کی $|a| \leq |b|$ لاسته راځی . ځکه نو باید $|a| = |b|$ سره وی . پدی معنی چې یا باید $a=b$ او یا $a=-b$ سره وی.

دلته باید یادونه وکړو چې د a او b د تامو عددو دوپش د وړتوب په اړیکه کی ضروری چې $b \neq 0$ وی . د $b \neq 0$ فرضیه په لاندی حقیقت پوری تړلی ده:

د هر عدد $a \neq 0$ دپاره داسی عدد وجود نلری چې $a = 0 \cdot q$ سره سی. که $a=0$ سره وی ، نو د هر تام عدد q دپاره د $0 = 0 \cdot q$ اړیکه صدق کوی ، ځکه نو قبول سویده چې پر صفر باندی وپش ممکن ندی.

بیلگه ۱ - د کومو طبیعی عددو n د پاره لاندنی اړیکه صدق کوی :

$$(n^3 + 9n^2 + 14):(n^2 + 2)$$

حل - که $n=1$ وی ، نو لیدل کیږی چې پورتنی اړیکه صدق کوی .

په آسانی سره ثابتیدلای سی چې:

$$(\forall a, b, c \in \mathbb{Z})((a+b:c \wedge a:c) \rightarrow b:c)$$

(د تمرین په شکل بی ثابت کړی) ، ځکه نو :

$$\begin{aligned} n^3+9n^2+14 &= n^3+2n-2n+7n^2+2n^2+14= \\ &= n(n^2+2)+7(n^2+2)-2n+2n^2= \\ &= (n^2+2)(n+7)+(2n^2-2n) \end{aligned}$$

څرنګه چې د n^3+9n^2+14 درې غړيز (درې حده) د دوو توپو (اجزاؤ) $(n^2+2)(n+7)$ او $(2n^2-2n)$ څخه تشکیل سوی دی او n^3+9n^2+14 باید د هر طبیعي عدد دپاره پر n^2+2 باندې دوپش وړ وی. $(n^2+2)(n+7)$ پر n^2+2 دوپش وړ دی، نو د تېر خاصیت پر بنسټ باید $2n^2-2n$ هم پر n^2+2 دوپش وړ وی. په هغه صورت کې چې n^3+9n^2+14 پر n^2+2 دوپش وړ وی.

پدې ډول، څرنګه چې n^3+9n^2+14 او $(n^2+2)(n+7)$ پر n^2+2 دوپش وړ دی، نو د ذکر سوی خاصیت له مخې $(2n^2-2n)$ هم باید پر n^2+2 دوپش وړ وی.

د بلې خوا، څرنګه چې $(n^2+2):(n^2+2)-2n-4=(2n^2-2n-4)-2n-4=2n^2-2n=2n^2+4-4-2n$ صدق کوی، نو په همدې ډول استدلال سره $2n^2-2n$ هغه وخت پر n^2+2 دوپشور دی چې $(-2n-4)$ پر n^2+2 دوپش وړ وی، یعنی $(n^2+2):(-2n-4)$ وی، خو وروستی اړیکه د هیڅ طبیعي عدد $n > 1$ صدق نه کوی. ځکه نو زموږ اولني اړیکه یوازې او یوازې د $n=1$ د پاره حقیقت لری.

بیلګه ۲ - لاندني اړیکه د کومو تامو عددو د پاره صدق کوی؟

$$(n^4+4):(n^2-2n+2)$$

حل - څرنګه چې $(n^2+2n+2)(n^2-2n+2)=n^4+4$ دی، نو نوموړی اړیکه د هر تام عدد دپاره صدق کوی.

§II. نیمګړي وپش (نامکمل وپش)

په بنونځیو کې دوپش د ورتوب څخه پرته نامکمله وپش هم تدریس کیږی.

تعریف - د a د تام عدد نامکله وپش د b پر تام عدد چې د صفر څخه خلاف وی ($b \neq 0$) عبارت دی د q او r داسی تامو عددو د موندلو څخه چې:

$$a = b \cdot q + r \quad 0 \leq r < |b| \quad \text{وی.} \quad 1$$

دلته د q تام عدد د خارج قسمت او د r تام عدد د باقی په نامه یادیږی.

د بیلګې په توګه د 30 د عدد پر 7 باندې دنامکمل تقسیم په نتیجه کې به $30=7 \cdot 4+2$ ولرو. دلته د نامکمل وپش خارج قسمت 4 او باقی یې 2 کیږی.

قضیه - که د a او $b \neq 0$ اختیاری تام عددونه راکړه سوی وی، نو تام عدد a پر تام عدد b تل نامکمل داسی وپشلای سو چې لاسته راغلي خارج قسمت او باقی بی ساري ($unique$) دی.

ثبوت - باید ثبوت په دوو پړاوو کې سرته ورسیري. لمړی باید د نامکمل وپش د موجودیت امکان باید په ثبوت ورسیري او دوهم باید د خارج قسمت او باقی بی ساریتوب په ثبوت ورسیري.

لمړی د a د عدد د نامکمل وپش امکان د $b \neq 0$ پر عدد ثابتوو.

لمری - فرضوو چي $a \geq 0$ او $b > 0$ دی. د $M = \{bk/k \in \mathbb{Z}\}$ سیټ په نظر کی نیسو. د M په سیټ کی د طبیعی عددو داسی یو سب سیټ جلا کوو چي د b د عدد هغه مضربونه په بر کی ونیسی چي د a تر عدد لوی وی. په نوموړی سب سیټ کی (د کوچنی ترین عدد دپرنسیب له مخی) کوچنی ترین عدد وجود لری، چي هغه په $b(q+1)$ سره بنیو. ځکه نو:

$$bq < a < b(q+1)$$

ددی ځایه:

$$0 \leq a - bq < b$$

$a - bq$ په r سره بنیو، یعنی $a - bq = r$ ، ددی ځایه $a = bq + r$ او $0 \leq r < b = |b|$ لاسته راځی. څرنګه چي $b > 0$ دی، نو $b = |b|$ سره کیږی. پدی معنی چي پدغه حالت کی نامکمل وپش ممکن دی.

دوهم - فرضوو چي $a < 0$ او $b > 0$ دی. ددی ځایه $-a > 0$ کیږی او د $-a$ او b دپاره مو د نامکمل وپش موجودیت په ثبوت ورساوه. یعنی د q_1 او r_1 داسی عددونه وجود لری چي $-a = bq_1 + r_1$ سره کیږی او د $0 \leq r_1 < b$ اړیکه صدق کوی. ددی ځایه:

$$a = -bq_1 - r_1 = -bq_1 - b + b - r_1 = b(-q_1 - 1) + (b - r_1)$$

څرنګه چي $0 < b - r_1 < b$ کیږی، نو $-q_1 - 1 = q_2$ او $-r_1 = r_2$ سره ایږدو. په نتیجه کی $a = bq_2 + r_2$ داسی لاسته راځی چي $0 < r_2 < b$. پدی معنی چي د a د عدد نامکمل وپش د b پر عدد باندی ممکن دی.

دریم - فرضوو چي $a \in \mathbb{Z}$ او $b < 0$ وی، نو $-b > 0$ وی. د لمړی او دوهم حالت له مخی د a د عدد نامکمل وپش د $-b$ پر عدد ممکن دی. پدی معنی چي د q او r عددونه داسی وجود لری چي $a = (-b)q + r$ او $0 \leq r < -b$ دی. بالاخره لیکلای سو چي $a = (-b)q + r$ او $0 \leq r < |b|$ حقیقت لری.

پدی معنی چي په هر حالت کی د a د عدد نامکمل وپش د b پر عدد باندی ممکن دی.

اوس به نو راسو د ثبوت و دوهم پړاو ته، هغه داچي د خارج قسمت او باقی بی ساریتوب باید په ثبوت ورسپیږی.

فرضوو چي د a د عدد د b پر عدد د نلمکمل وپش په نتیجه کی دوه خارج قسمتونه د q_1 او q_2 او دوه باقی د r_1 او r_2 لاسته راځی، پدی صورت کی:

$$a = bq_1 + r_1 \quad ; \quad 0 \leq r_1 < |b|$$

$$a = bq_2 + r_2 \quad ; \quad 0 \leq r_2 < |b|$$

$$b(q_1 - q_2) = r_2 - r_1 \quad \dots (*) \quad \text{ځکه نو:} \quad bq_1 + r_1 = bq_2 + r_2 \quad \text{او یا}$$

څرنګه چي $0 \leq r_1 < |b|$ او $0 \leq r_2 < |b|$ دی، نو $|r_2 - r_1| < |b|$ کیږی. خو پدی حالت کی د (*) مساوات هغه وخت صدق کولای سی چي $r_2 - r_1 = 0$ وی. ځکه نو $r_2 = r_1$ او $q_1 - q_2 = 0$ یعنی $q_1 = q_2$ سره کیږی.

بیلګه - د نامکمل وپش عملیه د 528 پر 23 عملی کوو.

$$\begin{array}{r|l} 528 & 23 \\ 46 & 22 \\ \hline 68 & \\ 46 & \\ \hline 22 & \end{array}$$

پدی معنی چي : $528=23 \cdot 22+22$

اوس نو که د تبری قضیې د دوهم حالت پر اساس مخ ته ولاړ سو ، لیند کیری چي :

$$-528=(-23) \cdot 23+1$$

پدی حالت کی د نامکمل تقسیم خارج قسمت مساوی په 23 او باقی 1 دی.

§III. لوی ترین مشترک وپشونکی (قاسم) او د هغه خاصیتونه - د اقلیدس الگوریتم

د تامو عددو وپش د ورتوب د پنځم خاصیت پر بنسټ د $a:b$ استنباط کیری چي $(\pm b):(\pm a)$ ، ځکه نو د تامو عددو د ورتوب د ورتوب د څېړلو په وخت کی خپل مطالعات یوازی د طبیعي عددو په سیټ باندی محدود کولای سو. په راتلونکی کی بیله دی چي د عددو سیټ ذکر کرو ، د وپش د ورتوب په هکله به مو هدف د طبیعي عددو سیټ وی. په عین حال کی لاسته راغلی نتبجي د پنځم خاصیت له مخی د تامو عددو په سیټ کی قبلوو.

تعریف ۱- د δ طبیعي عدد د a او b طبیعي عددو د مشترک وپشونکی په نامه یادیری، که $a:\delta$ او $b:\delta$ وی .

د a او b د عددو تر ټولو لوی مشترک وپشونکی د هغوی د لوی ترین مشترک وپشونکی په نامه یادیری او په (a,b) سره یې بنیو.

د لوی ترین مشترک وپشونکی ، چي په لنډه توگه $G.C.D$ (Greatest Common Divisor) سره بنودل کیری، د پیدا کیدو طریقه د لرغونی یونان د ریاضی پوه اقلیدس له خوا طرح سوی ده او د اقلیدس د الگوریتم په نامه یادیری . د الگوریتم کلمه مور ته د عربی تکره ریاضی پوه محمد ابن موسی الخوارزمی څخه را پاته ده. الخوارزمی په نهمه عیسوی پیری کی د اوسنی افغانستان د ختیځ او د هند په لویدیځو برخو کی مروجه ریاضی و عربیو ته ورنقل کړه او هلته یې خپل مشهور کتاب د الجبر و المقابله تر عنوان لاندی ولیکی . د الخوارزمی د الجبر په کتاب کی د یو درجه ای او دوه درجه ای یو مجهوله معادلو د حل طریقی تشریح سوی دی . ځکه نو تر اوسه د یو پرابلم د حل د طریقی د پاره د هغه د نامه ، یعنی الگوریتم، څخه کار اخیستل کیری. دواړه کلیمی ، الجبر او الگوریتم ، مور ته د الخوارزمی څخه په میراث پاته سویدی ، چي څو سوه کاله وروسته بیا اروپا ته نقل سوی ده. د الگوریتم کلمه نه یوازی په ریاضی کی ، بلکه په کمپیوټری علومو کی ډیره مروجه ده.

دمخه تردی چي د اقلیدس پر الگوریتم بحث وکو، ضرور دی چي ځني کومکی دعوی وی (Lemma) په ثبوت وروسوو.

لیما ۱- که $a:b$ وی ، نو $(a,b)=b$ سره دی.

ثبوت - د $a:b$ د فرضیې څخه استدلال کولای سو چې د کوم تام عدد q دپاره به $a=b \cdot q$ وی. اوس به نو د a او b د مشترکو وېشونکو سیټ، چې په M_1 سره یې بنیو، په نظر کې ونیسو. د a او b هر مشترک وېشونکی د b د عدد وېشونکی هم دی. علاوه پر دې د b د عدد هر وېشونکی δ د a د عدد هم وېشې، پدې معنی چې د هغوی مشترک وېشونکی دی. پدې حساب د a او b د مشترکو وېشونکو سیټ M_1 د b د عدد د ټولو وېشونکو د سیټ M_2 سره مساوی دی. د M_2 په سیټ کې د b د عدد لوی ترین دی، ځکه نو $(a,b)=b$ سره کیږی.

بیلگه ۱ - د ۱۸ او ۶ عددونه په نظر کې ونیسو. $(18,6)=6$ دی.

$M_1=\{1,2,3,6\}$ د ۱۸ او ۶ د مشترکو وېشونکو سیټ او $M_2=\{1,2,3,6\}$ د ۶ د وېشونکو سیټ دی. په دواړو سیټو کې لوی ترین عدد ۶ دی، ځکه نو د هغوی لوی ترین مشترک وېشونکی ۶ دی.

لیما ۲ - که $a=b \cdot q+r$ سره وی، پداسی حال کې چې b, a او r د صفر څخه خلاف عددونه وی. نو د $(a,b)=(b,r)$ د اړیکې حقانیت ثابتوو.

ثبوت - فرضوو چې M_1 د a او b د عددو د ټولو مشترکو وېشونکو سیټ او M_2 د b او r د عددو د ټولو مشترکو وېشونکو سیټ دی. د لیما د ثبوت دپاره کافی ده چې د M_1 او M_2 د سیټو مساوی والی په ثبوت ورسوو. یعنی باید ثابتته کړو چې $M_2 = M_1$ سره کیږی.

که $\delta \in M_1$ وی، نو $a:\delta$ او $b:\delta$ ، پدې معنی چې د q_1 او q_2 تام عددونه داسی وجود لری چې:

$$a = \delta \cdot q_1$$

$$b = \delta \cdot q_2$$

ددی ځایه $\delta \cdot q_1 = \delta \cdot q_2 + r$ او $r = \delta(q_1 - q_2)$ کیږی، پدې معنی چې $r:\delta$ دی. یعنی $M_1 \subset M_2$ دی.

همدا ډول که $\delta_1 \in M_2$ وی، نو $b:\delta_1$ او $r:\delta_1$ دی، په نتیجه کې $a:\delta_1$ دی. یعنی $\delta_1 \in M_1$ او

$M_2 \subset M_1$ دی، په نتیجه کې $M_2 = M_1$ سره کیږی. بالاخره ثابتته سوه چې $(a,b)=(b,r)$ دی. ■

اوس به نو د اقلیدس الگوریتم د دوو طبیعی عددو د لوی ترین مشترک وېشونکی د موندلو دپاره دلته طرح کړو:

فرضو چې a او b دوه طبیعی عددونه او یو پر بل دوېش وړ نه وی. د a د عدد د نامکمل وېش څخه د b پر عدد باندی لاندی مساوات لاسته راځی:

$$a = bq_1 + r_1 ; 0 < r_1 < b$$

په هغه صورت کې چې b پر r_1 دوېش وړ نه وی، نو بیا هم b پر r_1 باندی نامکمل وېشو، په نتیجه کې

$$b = r_1q_2 + r_2 ; 0 < r_2 < r_1$$

لاسته راځی. همدا ډول که r_1 پر r_2 دوېش وړ نه وی، نو بیا هم r_1 پر r_2 باندی نامکمل وېشو چې

$$r_1 = r_2q_3 + r_3 ; 0 < r_3 < r_2$$

به يې نتیجه وی. څرنګه چې $0 < r_3 < r_2 < r_1$ دی، نو نوموړی د نا مکمل وېش پروسه لایتناهی نده، بلکه چې ډیر وی $b-1$ ځلی د نا مکمل وېش عملیه اجرا کولای سو. د بیلګې په توګه که وروسته له $n-1$ ام قدم څخه r_{n-1} پر r_n دوېش وړ وی، نو د خطی معادلو لاندنی سیستم به لاسته راسی:

$$\begin{cases} a = bq_1 + r_1 & ; 0 \leq r_1 < b \\ b = r_1q_2 + r_2 & ; 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3 & ; 0 \leq r_3 < r_2 \\ \vdots & \\ r_{n-2} = r_{n-1}q_n + r_n & ; 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_nq_{n+1} & \end{cases} \quad \dots(1)$$

د مساواتو سیستم (1) د اقلیدس د الګوریتم په نامه یادېږی.

قضیه ۱- فرضوو چې د a او b دوه عدده داسی راکړه سوی وی چې a پر b دوېش وړ نه وی. د a او b د عددو لوی ترین مشترک وېشونکی عبارت دی، د a او b د اقلیدس په الګوریتم کی، له وروستني باقی څخه چې د صفر څخه خلاف وی.

ثبوت - فرضوو چې د a او b د عددو دپاره د مساواتو (1) سیستم صدق کوی. نو د دوهمی لیما پر بنسټ لیکلای سو چې:

$$(a,b) = (b,r_1) = (r_1,r_2) = \dots = (r_{n-2},r_{n-1}) = (r_{n-1}, r_n)$$

څرنګه چې $r_n : r_{n-1}$ دی، ځکه نو د لمړی لیما پر بنسټ $(r_{n-1}, r_n) = r_n$ سره کیږی. په نتیجه کی د a او b د عددو لوی ترین مشترک وېشونکی په r_n سره مساوی کیږی.

بیلګه ۲ - غواړو چې $(2530, 7975)$ پیدا کړو.

حل -

$$\begin{array}{r|l} 7975 & 2530 \\ 7590 & 3 \\ \hline & 385 = r_1 \end{array} \quad \begin{array}{r|l} 2530 & 385 \\ 2310 & 6 \\ \hline & 220 = r_2 \end{array} \quad \begin{array}{r|l} 385 & 220 \\ 220 & 1 \\ \hline & 165 = r_3 \end{array}$$

$$\begin{array}{r|l} 220 & 165 \\ 165 & 1 \\ \hline & 55 = r_4 \end{array} \quad \begin{array}{r|l} 165 & 55 \\ 165 & 3 \\ \hline & 0 = r_5 \end{array}$$

$$\begin{cases} 7975 = 2530 \cdot 3 + 385 \\ 2530 = 385 \cdot 6 + 220 \\ 385 = 220 \cdot 1 + 165 \\ 220 = 165 \cdot 1 + 55 \\ 165 = 55 \cdot 3 + 0 \end{cases} \quad \dots(*) \quad \text{پا:}$$

څرنگه چې د نامکمله وېش په پروسه کې ورستی د صفر څخه خلاف باقی په 55 سره مساوی کېږي ، نو د راکړه سوو عددو لوی ترین مشترک وېشونکی 55 دی ، یعنی: $(2530,7975)=55$ دی.

نتیجه - که M_1 د a او b د عددو د ټولو مشترکو وېشونکو سیټ او M_2 د a او b د عددو د ټولو لوی ترینو مشترکو وېشونکو سیټ وي ، نو پدې صورت کې $M_1=M_2$ سره کېږي .

ثبوت - ددی نتیجې ثبوت د اقلیدس د الگوریتم د مساواتو او وېش د وړتیا د خاصیتو څخه استنباط کېږي.

د پورتنۍ نتیجې څخه په استفاده باندې کولای سو چې د a او b د عددو د لوی ترین مشترک وېشونکی تعریف داسې هم فارمولېندی کړو:

تعریف ۲ - د a او b طبیعي عددولوی ترین مشترک وېشونکی عبارت دی د داسې طبیعي عدد d څخه چې د a او b د عددو پر هر وېشونکي δ وېش ور وي.

د دوو عددو لوی ترین مشترک وېشونکی لاندې خاصیتونه لری:

خاصیت ۱ - که د a او b د عددو څخه هر یو په طبیعي عدد $k \neq 0$ کې ضرب کړو ، نو د هغوی لوی ترین مشترک وېشونکی هم د k په عدد کې ضربېږي.

ثبوت - که د (1) سیسټم هر مساوات د k په عدد کې ضرب کړو ، نو لاندنۍ سیسټم به لاسته راسی:

$$\left\{ \begin{array}{l} a \cdot k = b \cdot kq_1 + r_1 \cdot k \quad ; \quad 0 \leq r_1 \cdot k < b \cdot k \\ b \cdot k = r_1 \cdot kq_2 + r_2 \cdot k \quad ; \quad 0 \leq r_2 \cdot k < r_1 \cdot k \\ r_1 \cdot k = r_2 \cdot kq_3 + r_3 \cdot k \quad ; \quad 0 \leq r_3 \cdot k < r_2 \cdot k \\ \vdots \\ r_{n-2} \cdot k = r_{n-1} \cdot kq_n + r_n \cdot k \quad ; \quad 0 \leq r_n \cdot k < r_{n-1} \cdot k \\ r_{n-1} \cdot k = r_n \cdot kq_{n+1} \end{array} \right.$$

ددې ځایه نتیجه اخیستل کېږي چې $(a \cdot k, b \cdot k) = r_n \cdot k = (a, b) \cdot k$.

خاصیت ۲ - که د a او b د عددو څخه هر یو د هغوی پر مشترک وېشونکي δ وېشو ، نو د هغوی لوی

ترین مشترک وېشونکي به مو هم پر δ وېشلی وي. یعنی :

$$\left(\frac{a}{\delta}, \frac{b}{\delta} \right) = \frac{(a, b)}{\delta}$$

ددې خاصیت ثبوت هم د لمړي خاصیت د ثبوت په ډول دی، دغه ثبوت لوستونکو ته د تمرین په شکل پریږدم.

خاصیت ۳ - که د d او a او b د عددولوی ترین مشترک وېشونکي وي، نو د x او y داسې تام عددونه وجود لری چې :

$$ax+by=d \quad \dots(2)$$

سره کېږي.

ثبوت - ددریم خاصیت د ثبوت دپاره هم د اقلیدس د الگوریتم څخه کار اخلو. د لمړي مساوات څخه

$$r_1 = a - bq_1$$

لاسته راخی.

په همدی ډول ددو هم مساوات څخه r_2 پیدا کوو او د r_1 قیمت په هغه کی وضع کوو، یعنی:

$$r_2 = b - r_1 q_2 = b - (a - bq_1) q_2 = (-q_2)a + (1 + q_1 q_2)b$$

همدارنگه:

$$r_3 = r_1 - r_2 q_3 = a - bq_1 - [(-q_2)a + (1 + q_1 q_2)b] q_3 = a(1 + q_2 q_3) + b(-q_1 - q_3 - q_1 q_2 q_3)$$

که پورتنی پروسه ته ادامه ورکړو، نو په آخر کی به د $r_n = ax + by$ مساوات داسی لاسته راسی چي د x او y پر ځای به تام عددونه وی. پدی ترتیب: $d = ax + by$ سره کیږی.

دوهم مساوات د a او b د عددود لوی ترین مشترک وپشونکی د خطی ترکیب شکل دی.

بیلگه ۳- د دوهمی بیلگي د لوی ترین مشترک وپشونکی د خطی ترکیب شکل پیدا کوو، پدی معنی چي

$$d = 55 = x \cdot 7975 + y \cdot 2530$$

دوهمی بیلگي د (*) په سیستم کی قیمتونه د لاندی څخه و لور ته وضع کوو.

$$55 = 220 - 165 \cdot 1 = 220 - 165$$

$$55 = 220 - (385 - 220 \cdot 1) = 220 - 385 + 220 = 2 \cdot 220 - 385$$

$$55 = 2 \cdot (2530 - 385 \cdot 6) - 385 = (-13) \cdot 385 + 2 \cdot 2530$$

$$55 = (-13) \cdot (7975 - 2530 \cdot 3) + 2 \cdot 2530$$

$$55 = (-13) \cdot 7975 + 39 \cdot 2530 + 2 \cdot 2530 = (-13) \cdot 7975 + 41 \cdot 2530$$

$$55 = 7975 \cdot (-13) + 2530 \cdot 41 \quad \dots (**)$$

پدی حساب $x = -13$ او $y = 41$ سره دی او د (***) مساوات د 7975 او 2530 د لوی ترین مشترک وپشونکی د خطی ترکیب شکل دی.

په پای کی ددی حقیقت یادونه ضرور ده چي د دوو عددو د لوی ترین مشترک وپشونکی تعریف په دواړو شکلو سره، یعنی په لمړی تعریف او دوهم تعریف سره درست دی. د a او b د عددود لوی ترین مشترک وپشونکی، پداسی حال کی چي یو عدد یی د صفر څخه خلاف وی، تل وجود لری او هغه هم حتی د تامو عددو په سیټ کی په $(a, b) = (|a|, |b|)$ سره مساوی کیږی.

که $a = b = 0$ وی، نو د هغوی لوی ترین مشترک وپشونکی وجود نلری.

د لوی ترین مشترک وپشونکی مفهوم تر دوو اضافه عددو پر سیټ $\{a_1, a_2, \dots, a_n\}$ باندی عمومیت ورکولای سو. د طبیعی عددو د متناهی سیټ لوی ترین مشترک وپشونکی په (a_1, a_2, \dots, a_n) سره بنیو.

قضیه ۲- که $(a_1, a_2, \dots, a_{n-1}) = \delta$ او $(\delta, a_n) = d$ وی، نو $(a_1, a_2, \dots, a_n) = d$ سره دی.

د قضیې ثبوت د تمرین په شکل پیشنهادوم.

VI§. نسبت یو او بل ته اولیه (متباین) عددونه (Relatively Primes) او دهغوی خاصیتونه

د طبیعی عددو په سیټ کی اکثرآ د داسی عددو د جوړو سره مخامخ کیږو چې د هغوی لوی ترین مشترک وېشونکی یوازی یو دی. ددغه ډول جوړو خاصیتونه زموږ سره دوپش د ورتوب د قضیو په ثبوت کی ډیره مرسته کوی او دهغو قضیو د ثبوت پروسه راته اسانه کوی.

تعریف - د a او b دوه عددونه د متباین یا نسبت یو او بل ته اولیه relatively primes عددو په نامه یادیری، که $(a,b)=1$ وی.

دغه ډول عددونه کله کله یو ډبل سره په وپش کی بیگانه عددو په نامه هم یادیری. د بیلگی په ډول $(35,33)=1$ دی.

د متباین کلمه چې د عربی څخه اخیستل سویده او معمولاً د مشابه په معنی استعمالیری، زما په نظر اصلی مفهوم نه ارائه کوی. تر هغه په وپش کی بیگانه عددونه، اصلی مفهوم ښه ارائه کوی. د تعریف څخه معلومیږی چې دوه عدده مشترک وېشونکی نلری یعنی په وپش کی سره بیگانه دی.

اوس به نو نسبت یو او بل ته اولیه عددو خاصیتونه وڅیږو:

قضیه ۱- د a او b دوه عددونه یوازی او یوازی نسبت یو او بل ته هغه وخت اولیه دی، چې د x او y دوه تام عددونه داسی وجود ولری چې د $ax+by=1$ اړیکه حقیقت ولری.

ثبوت - د قضیې لازمی شرط په III§ کی د لوی ترین مشترک وېشونکی د خاصیت څخه استنباط کیږی.

فرضوو چې د x او y ځینو تامو عددو دپاره د $ax+by=1$ مساوات صدق کوی. که $(a,b)=d$ وی، نو $d:1$ وی. په نتیجه کی باید $d=1$ وی.

قضیه ۲- د a او b د عددو خارج قسمتونه د هغوی پر لوی ترین مشترک وېشونکی (a,b) ، نسبت یو او

بل ته اولیه عددونه دی. یعنی: که $(a,b)=d$ وی، نو $\left(\frac{a}{d}, \frac{b}{d}\right)=1$ سره کیږی.

ثبوت - فرضوو چې $(a,b)=d$ دی. نو د x او y دوه تام عددونه داسی وجود ولری چې د $ax+by=d$ کیږی. ددی ځایه:

$$\frac{a}{d}x + \frac{b}{d}y = 1$$

پدی معنی چې $\left(\frac{a}{d}, \frac{b}{d}\right)=1$ سره کیږی.

قضیه ۳- که د a او b دوو عددو ضرب حاصل د c پر عدد دوپش وړ وی او د a او c عددونه نسبت یو او بل ته اولیه عددونه وی، نو د b عدد د c پر عدد دوپش وړ دی.

ثبوت - څرنگه چې $(a,c)=1$ دی، نو:

$$(\exists x, y \in \mathbb{Z})(ax+cy=1)$$

که د پورتنی مساوات دواړه خواوی په b کی ضرب کړو، نو :

$$abx + cby = b$$

سره کیږی . څرنگه چې $ab:c$ دی ، نو $b:c$ وی .

قضیه ۴- د a او b عددونه نسبت یو او بل ته اولیه عددونه وی ، نو د c عدد یوازې او یوازې هغه وخت پر $a \cdot b$ دوپش وړ دی چې c پر a او b دوپش وړ وی .

ثبوت - که $c:a \cdot b$ وی ، څرنگه چې $a \cdot b:a$ او $a \cdot b:b$ دی ، نو دوپش دور توب د انتقالی خاصیت له مخی $c:a$ او $c:b$ دی .

برعکس ، که $c:a$ او $c:b$ وی ، نو $c=aq$ سره او $aq:b$ دی . څرنگه چې $(a,b)=1$ ، نو $q:b$ دی . یعنی $q=bq_1$ سره . ددی خایه $c=aq=abq_1$ ، پدی معنی چې $c:ab$ دی .

د وروستی خاصیت څخه د مرکبو عددو دوپش د ورتوب په معیار کی کار اخیستل کیږی . د بیلگی په توگه ، ددی دپاره چې m عدد پر 6 دوپش وړ وی لازمه او کافی ده چې m په عین وخت کی پر 2 او 3 دوپش وړ وی . دغه حقیقت د ثابتته سوی قضیې څخه استنباط کیږی . ځکه چې $6=2 \cdot 3$ او $(2,3)=1$ سره کیږی .

قضیه ۵- که د a او b دوه عددونه د دریم عدد c سره نسبت یو او بل ته اولیه وی ، نو د هغوی د ضرب حاصل هم د c د عدد سره نسبت یو او بل ته اولیه دی .

ثبوت - فرضوو چې $(b,c)=1$ ، $(a,c)=1$ او $(ab,c)=d$ وی . یعنی $c=dq$ سره کیږی . څرنگه چې د ځینو تامو عددو x او y دپاره د $ax+cy=1$ اړیکه صدق کوی ، نو $ax+d(qy)=1$ او $(a,d)=1$ دی . ځکه نو د $ab:d$ او $(a,d)=1$ څخه د دریمی قضیې پر بنسټ $b:d$ لاسته راځی . ځکه نو د $(b,c)=1:d$ څخه $d=1$ لاسته راځی ، یعنی $(ab,c)=1$ دی .

نتیجه - که $(a,b)=1$ وی ، نو د هر طبیعی عدد n دپاره $(a^n, b^n)=1$ دی .

ثبوت - د $(a,b)=1$ او $(a,b)=1$ په نتیجه کی $(a^2, b^2)=1$ لاسته راځی . همدا ډول د $(a^2, b)=1$ او $(a^2, b)=1$ څخه $(a^2, b^2)=1$ استنباط کیږی . په همدی ترتیب پورتنی پروسه ته ادامه ورکوی . وروسته له n نامی مرحلی څخه $(a^n, b^n)=1$ لاسته راځی .

د پورتنی نتیجی پر بنسټ ثابتولای سو چې د یوه ساده کسر (پدی معنی هغه کسر چې د لنډیدو نه وی ، یعنی د اختصار وړ نه وی) په طبیعی طاقت لور هم کړو بیا هم ساده کسر پاته کیږی .

بیلگه ۱- غواړو چې د $\sqrt[3]{5}$ غیر نسبتی والی په ثبوت ورسو .

فرضوو چې $\sqrt[3]{5}$ یو نسبتی عدد دی ، پدی معنی چې $\sqrt[3]{5} = \frac{p}{q}$ سره ، پداسی حال کی چې $(p,q)=1$

دی . څرنگه چې د $\sqrt[3]{5} = \frac{p}{q}$ د $5 = \frac{p^3}{q^3}$ مساوات او بلاخره د $p^3 = 5q^3$ مساوات لاسته راځی او د

$(p,q)=1$ څخه د پورتنی نتیجی پر بنسټ $(p^3, q^3)=1$ کیږی . نو د $p^3 = 5q^3$ او $(p^3, q^3)=1$ مساواتو موجودیت ناممکنه دی ، ځکه نو د $\sqrt[3]{5}$ عدد غیر نسبتی عدد دی .

بیلگه ۲ - ثابتو چي د n او $n+1$ عددونه نسبت یو او بل ته اولیه دی . یعنی : $(n,n+1)=1$.

حل - فرضوو چي هغوی نسبت یو او بل ته اولیه نه وی ، یعنی $(n,n+1)=d > 1$ وی . پدی معنی چي باید $n:d$ او $(n+1):d$ وی .

دوېش د ورتوب د خاصیتو څخه په استفاده سره (د $I\&$ لمړی بیلگه وگوری) د $1:d$ اړیکه استنباط کیری . خو دغه حالت یوازی هغه وخت ممکن دی چي $d=1$ سره وی . ځکه نو د $d > 1$ په فرضیه کی و ناممکنی نتیجی ته ورسیدو ، یعنی د مسئلې اصل چي د $(n,n+1)=1$ عبارت دی ، حقیقت لری .

بیلگه ۳ - د خطی معادلو لاندنی سیستم د طبیعی عددو په سیټ کی حلوو .

$$\begin{cases} x + y = 168 \\ (x, y) = 24 \end{cases}$$

حل - د راکړه سوی معادلو په سیستم کی دوهمه معادله مورته وایی چي د x او y هغو نامعلومو عددو چي مور یی په لټه کی یو ، لویترین مشترک وېشونکی 24 دی . پدی معنی چي $x:24$ او $y:24$ دی . دوېش د ورتوب د تعریف پر بنسټ د q_1 او q_2 داسی تام عددونه وجود لری چي :

$$x = 24 q_1 , y = 24 q_2 \text{ او } (q_1, q_2) = 1$$

سره دی . که د x او y قیمتونه په لمړی معادله کی وضع کړو ، نو

$$24 q_1 + 24 q_2 = 24(q_1 + q_2) = 168$$

$$q_1 + q_2 = \frac{168}{24} = 7$$

$$q_1 + q_2 = 7$$

لاسته راخی .

اوس نو پداسی دوو عددو پسی گړځو چي نسبت یو او بل ته اولیه او دجمع حاصل یی 7 وی . پدی حالت کی لاندنی امکانات وجود لری :

$$q_1 = 1 \quad \wedge \quad q_2 = 6$$

$$q_1 = 2 \quad \wedge \quad q_2 = 5$$

$$q_1 = 3 \quad \wedge \quad q_2 = 4$$

او برعکس ، پدی معنی چي د q_1 او q_2 قیمتونه سره تبدیل کړو . د هر حالت په نتیجه کی د x او y قیمتونه پیدا کوو :

$$x_1 = 24 \quad \wedge \quad y_1 = 144$$

$$x_2 = 48 \quad \wedge \quad y_2 = 120$$

$$x_3 = 72 \quad \wedge \quad y_3 = 96$$

او برعکس د q_1 او q_2 د قیمتو د تبد یولو په نتیجه کی د x_i او y_i ($i=1,2,3$) قیمتونه په خپل منځ کی اوری.

V§. کوچنی ترین مشترک مضرب او د هغه ارتباط د لوی ترین مشترک وپشونکی سره
دوېشدرتوب په تیوری کی د لوی ترین مشترک وپشونکی په څنگ کوچنی ترین مشترک مضرب هم مهم رول لوبوی. نوموړی مفهوم هم د طبیعی عددو دپاره تعریفوو.

تعریف ۱- د a او b طبیعی عددو مشترک مضرب عبارت دی د هر تام عدد څخه چې هم د a پر عدد او هم د b پر عدد دوېشور وی.

بیلگه ۱- د 3 او 8 مشترک مضربونه عبارت دی له : $24, 48, 96, 192, \dots$ او داسی نورو څخه.

تعریف ۲- د a او b د عددو په ټولو مثبتو مشترکو مضربو کی کوچنی ترین مضرب د نوموړو عددو د کوچنی ترین مضرب په نامه یادیری او په $[a, b]$ سره یې بنیو.

د a او b د مشترکو مضربو په سیټ کی د کوچنی ترین عدد د پرنسیب پر بنسټ تل کوچنی ترین عدد وجود لری. پدی معنی چې د a او b دپاره تل کوچنی ترین مضرب $[a, b]$ وجود لری او بی ساری دی.

د کوچنی ترین مضرب د محاسبی د طریقو څخه یوه طریقه د لاندنی قضیې په ریهه ارائه کیږی.

قضیه ۱- د a او b اختیاری طبیعی عددو دپاره لاندنی مساوات صدق کوی:

$$[a, b] = \frac{a \cdot b}{(a, b)}$$

ثبوت - ددعوی د ثبوت دپاره $M = \frac{a \cdot b}{(a, b)}$ او $(a, b) = d$ سره ایږدو. لمړی به ثبوت کړو چې M د a او b د عددو مشترک مضرب دی.

څرنکه چې $a = d \cdot n$ او $b = d \cdot k$ ، پداسی حال کی چې $(k, n) = 1$ ، دی ، نو :

$$M = \frac{a \cdot b}{d} = \frac{d \cdot n \cdot b}{d} = b \cdot n$$

$$M = \frac{a \cdot b}{d} = \frac{a \cdot d \cdot k}{d} = a \cdot k$$

یعنی د M عدد د a او b د عددو مشترک مضرب دی.

اوس به نو فرض کړو چې M_1 د a او b د عددویو بل مشترک مضرب دی ، یعنی $M_1 : a$ او $M_1 : b$ ، ځکه نو د m او l داسی طبیعی عددونه وجود لری چې : $M_1 = a \cdot m$ او $M_1 = b \cdot l$ دی.

ددی ځایه $(dn)m = (dk)l$ او $n \cdot m = k \cdot l$ دی. څرنکه چې $(k, n) = 1$ دی ، نو د $V§$ ددریمی قضیې پر بنسټ $m : k$ دی. ځکه نو داسی طبیعی عدد q وجود لری چې $m = k \cdot q$ سره کیږی. که د m قیمت د $M_1 = a \cdot m$ په مساوات کی کښیږدو ، نو په نتیجه کی به

$$M_1 = a \cdot m = a \cdot k \cdot q = aq \cdot \frac{b}{d} = \frac{a \cdot b}{d} \cdot q = M \cdot q$$

لاسته راسی پدی ترتیب $M_1:M$ دی او $M_1 \geq M$ دی، یعنی M د a او b د عددو مشترک مضرب دی.

$$[a, b] = M = \frac{a \cdot b}{(a, b)} \quad \text{په نتیجه کی :}$$

نتیجه - د a او b د عددو هر مشترک مضرب M_1 د نوموړو عددو پر کوچنی ترین مشترک مضرب یعنی $[a, b]$ دویش وړ دی.

په رشتیا هم که M_1 طبیعی عدد وی ، نو پورتنی نتیجه د اولی قضیې د ثبوت څخه استنباط کیږی. او که $M_1 < 0$ وی ، نو $|M_1| > 0$ او $|M_1| : [a, b]$ دی ، پدی صورت کی بیا هم $M_1 : [a, b]$ سره کیږی.

د لمړی قضیې استنباط کیږی چې a او b د عددو د کوچنی ترین مشترک مضرب د موندلو د پاره باید لمړی د هغوی لوی ترین مشترک وېشونکی پیدا کړو او وروسته بیا د a او b د عددو د ضرب حاصل پر هغه ووېشو څو به نتیجه کی $[a, b]$ لاسته راسی .

بیلگه ۲ - غواړو چې $[267, 36]$ پیدا کړو.

حل - لمړی $(267, 36)$ پیدا کړو:

$$\begin{array}{r|l} 267 & 36 \\ \hline 252 & 7 \\ \hline 15 & \end{array} \quad \begin{array}{r|l} 36 & 15 \\ \hline 30 & 2 \\ \hline 6 & \end{array} \quad \begin{array}{r|l} 15 & 6 \\ \hline 12 & 2 \\ \hline 3 & \end{array} \quad \begin{array}{r|l} 6 & 3 \\ \hline 6 & 2 \\ \hline 0 & \end{array}$$

وینو چې $(267, 36) = 3$ سره کیږی . نو د لمړی قضیې له مخی

$$[267, 36] = \frac{267 \cdot 36}{3} = 267 \cdot 12 = 3204$$

قضیه ۲ - که د a او b د عددو څخه هر یو د k په یوه طبیعی عدد کی ضرب کړو ، نو دهغوی کوچنی ترین مشترک مضرب هم په هغه عدد کی ضربیږی.

ثبوت -

$$[a \cdot k, b \cdot k] = \frac{a \cdot k \cdot b \cdot k}{(a \cdot k, b \cdot k)} = \frac{a \cdot k \cdot b \cdot k}{(a, b) \cdot k} = \frac{a \cdot b}{(a, b)} \cdot k = [a, b] \cdot k$$

د a او b تامو عددو دپاره چې د صفر څخه خلاف وی ، د کوچنی ترین مشترک مضرب تعریف د طبیعی عددو د تعریف سره مطابق دی ، خو محاسبه یې د لاندنی فارمول پذیریه کیږی:

$$[a, b] = \frac{|a \cdot b|}{(a, b)}$$

د کوچنی ترین مشترک مضرب مفهوم د څو عددو a_1, a_2, \dots, a_n دپاره عمومیت ورکولای سو او په لاندی ډول یې تعریفوو

تعريف ۳ - د a_n, \dots, a_2, a_1 د صفر څخه خلاف تامو عددو کوچنی ترین مشترک مضرب عبارت دی د هغه کوچنی ترین طبیعی عدد څخه چې پر هر یو د a_n, \dots, a_2, a_1 عددو باندی د وېش وړ وی. د نوموړو عددو کوچنی ترین مشترک مضرب په $[a_1, a_2, \dots, a_n]$ سره بڼیو .

قضیه ۳ - که $[a_1, a_2, \dots, a_{n-1}] = p$ سره وی او $[p, a_n] = m$ وی ، نو $[a_1, a_2, \dots, a_n] = m$ سره دی. ثبوت - څرنگه چې $m:p$ او p پر هر یو ه د عددو a_{n-1}, \dots, a_2, a_1 د وېش وړ دی ، نو m پر هر یو ه د راکړه سوو عددو د وېش وړ دی ، یعنی m د ټولو عددو a_n, \dots, a_2, a_1 مشترک مضرب دی .

فرضوو چې M د a_n, \dots, a_2, a_1 عددو یو بل مشترک مضرب وی ، نو M د a_{n-1}, \dots, a_2, a_1 د عددو مشترک مضرب او $M:p$ دی. پدی معنی چې M د p او a_n د عددو مشترک مضرب دی . څرنگه چې $[p, a_n] = m$ سره دی ، نو $M \geq m$ دی . بدی ترتیب د m عدد د مشترکو مضربو څخه هغه کوچنی ترین دی.

د پورتنی قضیې حقانیت مور ته د څو عددو د کوچنی ترین مشترک مضرب د شمېرلو طریقه رابڼی . نتیجه -

$$[a_1, a_2, a_3] = [[a_1, a_2], a_3]$$

$$[a_1, a_2, a_3, a_4] = [[a_1, a_2, a_3], a_4]$$

VI§. اولیه عددونه او دهغوی ترتیب د طبیعی عددو په لار کی - د ایراتوستینس غلبیل

که طبیعی عددونه د هغوی د وېشونکی د سیټ له مخی مطالعه کړو ، نو په زړه پوری او په معاصر ژوند کی ډیرو مفیدو واقعیتوته به متوجه سو. د بیلگي په توگه 13 یوازی دوه وېشونکی لری چې هغه عبارت دی له 1 او 13 څخه، خو 12 بیا شپږ وېشونکی لری چې هغه عبارت دی له : 1, 2, 3, 4, 6 او 12 څخه. د یوه عدد د وېشونکو سیټ باید د هغه عدد په اړوند وڅېړل سی. خو په زړه پوری د عددو سیټ هغه سیټ دی چې عنصرونه یی یوازی پر یوه او پر خپل ځان د وېش وړ وی. ددغه ډول عددو سیټ نه یوازی د عددونو د تیوری په تاریخ کی بلکه د معاصر ژوند په تکنالوجی ډیر مهم رول لوبوی.

تعريف ۱ - د p طبیعی عدد د اولیه عدد Prime Number په نامه یادیری ، که $p > 1$ وی او غیر له 1 او p څخه بل هیڅ وېشونکی ونلری.

که طبیعی عددونه په یوه لار کی واوډل سی ، نو لمړنی اولیه عددونه عبارت دی له:

2, 3, 5, 7, 11, 13, 17, 19, 23, ... څخه. وگوری چې د هغوی د جملی څخه یوازی د 2 عدد جفت او نور یی طاق عددونه دی.

تعريف ۲ - طبیعی عدد n د مرکب عدد Composite Number په نامه یادیری ، که علاوه پر 1 او n نور وېشونکی هم ولری.

د مرکبو عددو لمړی دسته د طبیعی عددو په لار کی عبارت ده له: 4, 6, 8, 9, 10, 12, 14, 15, 16, ... او نورو څخه . لیدل کیږی چې په مرکبو عددو کی هم جفت عددونه او هم طاق عددونه شامل دی. په یاد یی ولری چې 1 نه مرکب عدد دی اونه اولیه عدد دی.

اوس به نو د اوليه عددو ځني خاصيتونه وڅېړو.

خاصيت ۱ - که اوليه عدد p پر کم طبيعي عدد $n > 1$ دوېش وړ وي ، نو $p = n$ سره کيږي.

ثبوت - که $p \neq n$ وي ، نو د p د اوليه عدد وېشونکي به $p, 1$ او n وي، پدې معنی چي p اوليه عدد ندی، ځکه نو $p = n$ سره دی.

خاصيت ۲ - که p_1 او p_2 دوه مختلف اوليه عددونه وي ، نو نه p_1 پر p_2 دوېش وړ دی او نه p_2 پر p_1 دوېش وړ دی.

دغه حقيقت د اوليه عددو د تعريف څخه مستقيماً استنباط کيږي .

خاصيت ۳ - که n طبيعي عدد او p اوليه عدد وي ، نو يا $n:p$ او يا $(n,p)=1$ دی.

ثبوت - فرضوو چي $(n,p)=d > 1$ دی ، نو $p:d$ او $p=d$ سره دی، ځکه چي p اوليه عدد دی. ددی په نتيجه کی $n:p$ کيږي.

خاصيت ۴ - هر طبيعي عدد $n > 1$ لږ تر لږه پر يوه اوليه عدد دوېش وړ دی.

ثبوت - دغه خاصيت د رياضي د اسقراء به طريقه ثابتوو.

قضيه د $n=2$ د پاره صدق کوي .

فرضوو چي زموږ قضيه د هر طبيعي عدد چي تر طبيعي عدد k کوچنی وي ، صدق کوي. که k په خپله اوليه عدد نه وي ، نو k مرکب عدد دی ، پدې معنی چي $k = n_1 \cdot n_2$ سره کيږي. پداسی ډول چي $n_1 < k$ او $n_2 < k$ دی . د استقراء د فرضيې پر بنسټ n_1 او n_2 پر کم اوليه عدد p_1 او p_2 دوېش وړ دی. ځکه نو دهغوی د ضرب حاصل k هم پر p_1 او p_2 دوېش وړ دی . يعنی $k:p_1$ او $k:p_2$ دی . د استقراء د پرنسيب پر بنسټ قضيه د هر طبيعي عدد $n > 1$ د پاره صدق کوي.

خاصيت ۵ - که د څو طبيعي عددو د ضرب حاصل پر اوليه عدد p دوېش وړ وي ، نو لږ تر لږه يو دهغو طبيعي عددو څخه پر p دوېش وړ دی .

ثبوت - فرضوو چي $a = (n_1 \cdot n_2 \cdot \dots \cdot n_k):p$ دی . که $(n_i, p) = 1$ وي ، نو $(n_1, p):p$. که $(n_i, p) = 1$ وي ، نو $(n_1, p):p$ دی. همدی پروسې ته په همدا ډول ادامه ورکوو ، څو داسی يو عدد n_i پيدا کړو چي د p پر عدد دوېش وړ وي. په هغه صورت کی چي داسی عدد وجود ونلری، نو د هر i دپاره n_i/p ($1 \leq i \leq k$) دی او يا $(n_i, p) = 1$ دی، نو د IV د پنځمی قضیې له مخی د $(n_1, n_2, \dots, n_k, p) = 1$ استنباط کيږي . ولی د III د اولی لیما او د فرضیې پر بنسټ $(n_1, n_2, \dots, n_k, p) = p$ سره کيږي. پدې معنی چي وروستی لاسته راغلی نتیجی يو ډبل سره مغایرت لری.

خاصيت ۶ - د مرکب عدد n کوچنی ترین اوليه وېشونکی تر \sqrt{n} لوی ندی.

ثبوت - فرضوو چي n مرکب عدد دی او p دهغه کوچنی ترین اوليه وېشونکی وي . نو $n = p \cdot n_1$ سره کيږي . څرنگه چي $p \leq n_1$ دی ، نو $p^2 \leq p \cdot n_1 = n$. په نتيجه کی $p \leq \sqrt{n}$ لاسته راځی.

د ميلاد څخه مخکی په دريمه پيړی کی يونانی رياضیپوه ایراتوستينيس Eratosthenes د طبيعي عددو پر اختیاری قطعہ خط باندي ، يا په بله اصطلاح د طبيعي عددو د لار په اختیاری توته کی، د اوليه

عددو د جلا کولو طریقه کشف کړه . پدی طریقه کی لمړی د 1 پر عدد خط کشوی ، بیا پر ټولو هغو عددو چي د 2 مضرب وی (یعنی هغه عددونه چي په 2 کی ضرب سوی وی) خط کشوی، بیا پر ټولو هغو عددو چي 3 یی مضرب وی او په همدی ډول مخ ته ځی پر ټولو هغو عددو چي د اولیه عدد مضرب وی ، خط کشوی. پر ټولو مضربو باندی د خط کشولو د پروسه لمن د $p \leq \sqrt{n}$ پذیریه را محدودیری.

نوموړی طریقه د ایراتوستینیس د غلبیل sieve of Eratosthenes په نامه یادیری.

د پورتنی طرح پر بنسټ که وغواړو چي ، دبیلگی په ډول ، تر 100 پوری اولیه عددونه پیدا کړو ، نو باید تر $\sqrt{100} = 10$ پوری د ټولو اولیه عددو پر مضربو خط کش کړو. تر لسو پوری اولیه عددونه 2,3,5,7 دی ، پدی معنی چي د نوموړو څلورو عددو پر مضربو تر 100 پوری باید خط کش کړوڅو تر 100 پوری ټوله اولیه عددونه لاسته راسی.

~~1~~ ~~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

په پورتنی جدول کی د خط کشولو په پروسه داسی خاص نظم نه لیدل کیږی ، هرڅونه چي مخ ته ځو ، هغونه د اولیه عددو شمېر لږیږی ، حتی مور کولای سو چي د طبیعی عددو د لار یوه ټوټه داسی غوره کړو چي په هغه کی هیڅ اولیه عدد وجود ونلری. خو پر هغه سر بیره لاندنی قضیه د لایتناهی اولیه عددو موجودیت ثابتوی.

د اقلیدیس قضیه - د اولیه عددو سیټ لایتناهی دی.

ثبوت - فرضوو چي د اولیه عددو سیټ متناهی دی او هغه په $M = \{2, 3, 5, 7, \dots, p_k\}$ سره نښو. پداسی حال کی چي p_k لوی ترین اولیه عدد دی. د M د سیټ د ټولو اولیه عددو د ضرب حاصل ، یعنی د $a + 1 = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p_k + 1$ تر مطالعی لاندی نیسو. څرنگه چي $p_k < a + 1 = 2 \cdot 3 \cdot 5 \cdot \dots \cdot p_k + 1$ ، نو $a + 1$ مرکب عدد دی او پر کم یوه اولیه عدد باندی دپش وړ دی. د a عدد پر اولیه عدد باندی دپش وړ دی، نو 1 هم باید پر اولیه عدد باندی دپش وړ وی . خو 1 پر هیڅ اولیه عدد باندی دپش وړ ندی . ځکه نو د قضیې اصلی ادعا حقیقت لری.

قضیه - د طبیعی عددو په لار کی په اختیاری اوږدوالی سره ټوټه (انتروال) وجود لری ، چي په هغه کی هیڅ اولیه عدد وجود نلری.

ثبوت - فرضوو چي طبیعی عدد n تر یوه لوی ، یعنی $n > 1$ دی. د

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \dots, (n+1)!+(n+1)$$

عددونه څېړو. پورتنی ټوله عددونه مرکب عددونه دی او د هغوی په منځ کی هیڅ اولیه عدد وجود نلری. پدی ډول قضیه په ثبوت ورسیده .

ددی دپاره چي په موضوع ښه پوه سی ، نو د $n=4$ سره د څلورو عددو توتیه پیداوو چي په هغه کی هیڅ اولیه عدد وجود نلری . د پورتنی فارمول له مخی هغه عبارت دی له 126,125,124,123,122 څخه.

وروستی دوی قضیې په طبیعی عددو کی د اولیه عددو د مشخصاتو مغلق والی نائیدوی. خو په عین حال کی په نننی تکنالوجی ډیر مفید رول لوبوی . ډیره ښه بیلگه یی په کریپتوگرافی کی د RSA(Rivest, Shamir, Adleman) طریقہ ده چي د هغه پذیرعه دانترنټ د لاری د قلف سوی معلوماتو په راکړه ورکړه او د عامه کلیبو په جوړولو کی د کار اخیستل دی.

§VII. د اولیه عددو د حاصل ضرب په شکل د مرکبو عددو تجزیه.

د اولیه عددو او د مرکبو عددو په منځ کی د ارتباط قضیه نه یوازی د وپشد وړ توب په تیوری کی بلکه د عددو په تیوری خاص رول لوبوی. نوموړی قضیه د عددو د تیوری د اساسی قضیې په نامه یادیری. قضیه ۱ (د عددو د تیوری اساسی قضیه) -

هر طبیعی عدد ، چي تر یوه لوی وی ، $n > 1$ یا اولیه عدد دی او یا د اولیه عددو د حاصل ضرب په شکل (بیله دی چي د ضربی عاملو ترتیب په نظر کی ونیسو) په بی ساری شکل ارائه کیدای سی.

ثبوت - لمړی د مرکبو عددو د تجزیې موجودیت په اولیه عددو باندی ثابتوو یعنی د قضیې دوهمه برخه ثابتوو.

د ریاضی د استقراء د متود څخه په استفاده سره $n=2$ اولیه عدد دی او د نوموړی عدد دپاره د قضیې ادعا صدق کوی. فرضوو چي هر طبیعی عدد $m < n$ ($n > 1$) یا اولیه عدد دی او یا د اولیه عدد د ضرب د حاصل په شکل ارائه کیدلای سی. اوس نو د n عدد څپرو:

که n اولیه عدد وی ، نو قضیه حقیقت لری.

که n اولیه عدد نه وی، نو n مرکب عدد دی ، چي د $n = n_1 \cdot n_2$ په شکل لیکل کیدای سی. دلته $n_1 < n$ او $n_2 < n$ دی. د استقراء د فرضیې له مخی $n_1 = p_1 \cdot p_2 \cdot \dots \cdot p_i$ او $n_2 = p_{i+1} \cdot p_{i+2} \cdot \dots \cdot p_k$ سره کیری ، پداسی حال کی چي p_1, p_2, \dots, p_k اولیه عددونه دی. په نتیجه کی :

$$n = (p_1 \cdot p_2 \cdot \dots \cdot p_i) \cdot (p_{i+1} \cdot p_{i+2} \cdot \dots \cdot p_k)$$

یعنی قضیه د طبیعی عدد n دپاره هم صدق کوی. ددی ځایه د استقراء د قضیې د پرنسیب له مخی د قضیې دعوا د هر طبیعی عدد n د پاره حقیقت لری.

اوس به نو بیله دی چي د ضربی عاملو(مضربو) ترتیب په نظر کی ونیسو د ارائی د شکل بی ساری توب په ثبوت ورسوو.

فرضو چي راکړه سوی طبیعی عدد n په دوو مختلفو شکلو سره ارائه کرای سو. یعنی :

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k \quad \text{او} \quad n = q_1 \cdot q_2 \cdot \dots \cdot q_s$$

پداسی ډول چي $k \geq s$ دی. ځکه نو :

$$p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_s \quad \dots(1)$$

څرنگه چې د پورتنی مساوات چپه خوا پر p_1 دوپش وړ ده ، نو راسته خوابی هم پر p_1 دوپش وړ ده. د اولیه عددو د پنځم خاصیت له مخی د q_1, q_2, \dots, q_s د ضربی عاملو څخه یو پر p_1 دوپش وړ دی. فرضوو چې $p_1 : q_1$ دی. څرنگه چې دواړه اولیه عددونه دی ، نو د لمړی خاصیت له مخی $p_1 = q_1$ سره کیږی. د (1) مساوات دواړی خواوی پر p_1 وپشو چې په نتیجه کی یی $q_1 \cdot \dots \cdot q_s = p_1 \cdot \dots \cdot p_k$ لاسته راځی. په همدغه ډول خپل استدلال ته ادامه ورکوو چې په نتیجه کی یی $p_{s+1} \cdot p_{s-2} \cdot \dots \cdot p_k = 1$ لاسته راځی. د ذکر سوی مساوات څخه استنباط کیږی چې $k=s$ دی ، یعنی :

$$p_1 = q_1, p_2 = q_2, \dots, p_s = q_s$$

په نتیجه کی قضیه په ثبوت ورسیده ، پدی معنی چې مرکب طبیعی عدد n په بی ساری ډول د اولیه عددو د حاصل ضرب په شکل ارائه کولای سو.

تعریف ۱- د مرکب طبیعی عدد n ارائه $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$ د p_1, p_2, \dots, p_k اولیه عددو د حاصل ضرب په شکل ، په اولیه ضربی عاملو (اولیه مضربو) باندی د مرکب عدد تجزیی په نامه یادیږی.

د عددو دثیوری اساسی قضیه مور ته بننی چې طبیعی عددونه د ضرب د عملی څخه په استفاده سره د اولیه عددو څخه لاسته راوړای سو.

بیلگه ۱ - 600 به د اولیه عددو په ضربی عاملو تجزیه کرو .

$$600 = 25 \cdot 24 = 5 \cdot 5 \cdot 3 \cdot 2 \cdot 2 \cdot 2$$

فرضوو چې $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$ د مرکب طبیعی عدد n تجزیه د اولیه عددو په ضربی عاملو سره ده. لکه په پورتنی بیلگه کی داسی پینیری چې د p_1, p_2, \dots, p_k عددو په منځ کی ځنی دهغوی په خپل منځ کی مساوی وی ، زموږ په بیلگه کی د 5 او 2 عددونه په ترتیب سره دوه ځله او دری ځله تکرار سوی دی. پدغه ډول حالتو کی د طاقت څخه په استفاده سره د $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$ تجزیه ساده کولای سو.

فرضوو چې $p_1, p_2, \dots, p_m, m \leq k$ مختلف اولیه عددونه دی. پداسی حال کی چې

$$\{ p_{m+1}, \dots, p_k \} \subset \{ p_1, p_2, \dots, p_m \}$$

وی. نو د n د عدد تجزیه د اولیه عددو په ضربی عاملو باندی په لاندی ډول لیکلای سو :

$$n = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_m^{s_m} \quad \dots (2)$$

تعریف ۲- طبیعی مرکب عدد n ارائه د (2) مساوات په شکل د اولیه عددو په ضربی عاملو باندی د n د عدد د ستندرد یا معیاری تجزیی په نامه یادیږی.

$$600 = 5^2 \cdot 3 \cdot 2^3$$

زموږ پورتنی بیلگه داسی هم لیکلای سو :

د عددو د تیوری د اساسی قضیې څخه استنباط کیږی ، چې د n د عدد ستندرد یا معیاری تجزیه د اولیه عددو په ضربی عاملو باندی (بیله دی چې ترتیب یی په نظر کی ونیسو) بی ساری او ځانگری ده.

قضیه ۲- که $n = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_m^{s_m}$ د n د عدد ستندرد تجزیه وی ، نو د n د عدد ټول وپشونکی د

$$d = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m} \quad \dots (3)$$

شکل لری ، پداسی ډول چې $0 \leq \alpha_1 \leq s_1, 0 \leq \alpha_2 \leq s_2, \dots, 0 \leq \alpha_m \leq s_m$ سره دی.

ثبوت - څرگنده ده ، هر د d عدد چي د (3) شکل ولری د n د عدد وپشونکی دی. برعکس ، فرضوو چي $n:d$ وی ، نو $n=d \cdot q$ سره کیری، پدی معنی چي د d په معیاری تجزیه کی یوازی د p_1, p_2, \dots, p_m ، اولیه عددونه وجود درلودلای سی ، پداسی ډول چي د هغوی طاقتونه تر s_1, s_2, \dots, s_m زیاد ندی. ځکه نو د d د عدد معیاری تجزیه (3) شکل لری.

فرضوو چي د p_1, p_2, \dots, p_t مختلف اولیه عددونه وی ، پداسی ډول چي هر یو د هغوی څخه لږ تر لږه یو ځل په اولیه ضربی عاملو باندی د a او b د عددو په معیاری تجزیه کی داخل وی. د بیلگي په توگه که $a=5^3 \cdot 3 \cdot 2^7$ او $b=5 \cdot 7^2 \cdot 3^3$ وی ، نو دغه ډول اولیه عددونه عبارت دی له $7, 5, 3, 2$ څخه. ځکه نو د a او b عددونه په لاندنی بڼه سره ارائه کولای سو.

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_t^{\alpha_t} \quad \text{او} \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_t^{\beta_t} \quad \dots(4)$$

که p_i د a او b د عددو په معیاری تجزیه کی داخل نه وی ، نو هر یو د α_i او β_i ($1 \leq i \leq t$) د طاقتو څخه مساوی په صفر سره کیدای سی، د بیلگي په ډول $a=7^0 \cdot 5^3 \cdot 3^1 \cdot 2^7$ او $b=7^2 \cdot 5^1 \cdot 3^3 \cdot 2^0$ دی.

نتیجه ۱ - که د a او b طبیعی عددونه د (4) اړیکي په بڼه راکړه سوی وی ، نو دهغوی لوی ترین مشترک وپشونکی عبارت دی له :

$$(a,b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \dots \cdot p_t^{\gamma_t}$$

پداسی ډول چي د هر عدد i دپاره $\gamma_i = \min\{\alpha_i, \beta_i\}$, $1 \leq i \leq t$ دی.

پدی معنی چي د a او b طبیعی عددو د لوی ترین مشترک وپشونکی د محاسبی دپاره ددواړو عددو په تجزیه کی هغه اولیه عددونه چي کوچنی ترین طاقتونه ولری ، راوخله او سره ضرب یی کړه .

نتیجه ۲ - که د a او b طبیعی عددونه د (4) اړیکي په بڼه راکړه سوی وی ، نو دهغوی کوچنی ترین مشترک مضرب عبارت دی له :

$$[a,b] = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_t^{\delta_t}$$

پداسی ډول چي د هر عدد i دپاره $\delta_i = \max\{\alpha_i, \beta_i\}$, $1 \leq i \leq t$ دی.

پدی معنی چي د a او b طبیعی عددو د کوچنی ترین مشترک مضرب د محاسبی دپاره ددواړو عددو په تجزیه کی هغه اولیه عددونه چي لوی ترین طاقتونه ولری ، راوخله او سره ضرب یی کړه .

اوله او دوهمه نتیجه مستقیماً د دوهمی قضیې ، د لوی ترین مشترک وپشونکی او کوچنی ترین مشترک مضرب د تعریفو څخه استنباط کیری. پورتنی نتیجی د بنوونځیو په ریاضیاتو کی د لوی ترین مشترک وپشونکی او کوچنی ترین مشترک مضرب د محاسبی د طریقو اساس تشکیلوی.

د بیلگي په توگه د $a=7^0 \cdot 5^3 \cdot 3^1 \cdot 2^7$ او $b=7^2 \cdot 5^1 \cdot 3^3 \cdot 2^0$ د عددو لوی ترین مشترک وپشونکی او کوچنی ترین مشترک مضرب پیدا کوو:

$$(a,b) = 7^0 \cdot 5 \cdot 3 \cdot 2^0 = 15$$

$$[a,b] = 7^2 \cdot 5^3 \cdot 3^3 \cdot 2^7 = 21168000$$

په ضربی عاملو باندی د طبیعی عدد د معیاری تجزیې څخه په استفاده سره کولای سو چي د طبیعی عدد د وپشونکو تعداد تعیین کړو. د n طبیعی عدد د وپشونکو تعداد په $\tau(n)$ سره نښو .

قضیه ۳- که $n = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_m^{s_m}$ د عدد ستندرد تجزیه وی ، نو

$$\tau(n) = (s_1+1)(s_2+1)\dots(s_m+1)$$

ثبوت - ددوهمی قضیې پر اساس د طبیعی عدد n ټول وېشونکی d د $d = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m}$

شکل لری ، پداسی ډول چې $0 \leq \alpha_1 \leq s_1, 0 \leq \alpha_2 \leq s_2, \dots, 0 \leq \alpha_m \leq s_m$ سره دی.

پدی معنی چې α_1 پوره s_1+1 قیمتونه ځانته اخیستلای سی، α_2 پوره s_2+1 ، ...، او بلاخره α_m پوره s_m+1 قیمتونه ځانته اخیستلای سی. په بله اصطلاح د $(\alpha_1, \alpha_2, \dots, \alpha_m)$ په مرتبه m نښه کی د وېشونکی d اختیاری طاقتونه چې لمړی جزء یې s_1+1 قیمتونه، دوهم جزء یې s_2+1 او بلاخره آخری او یا m -ام جزء یې s_m+1 قیمتونه ځانته اخیستلای سی. په نتیجه کی $(s_1+1)(s_2+1)\dots(s_m+1)$ مختلفي m نښي وجود لری. په نتیجه کی

$$\tau(n) = (s_1+1)(s_2+1)\dots(s_m+1)$$

سره کیری ■

بیلگه ۲ - $\tau(8) = 4$ کیری ، ځکه چې $8 = 2^3$ دی . دلته یوازی s_1 لرو چې هغه هم په 3 سره مساوی کیری ، ددی اسبته $s_1+1 = 4$ کیری . او په رشتیا هم د 8 څلور وېشونکی لری چې هغه هم عبارت دی له 1, 2, 4 او پخپله 8 څخه. که د طبیعی عدد a د ټولو وېشونکو سیټ په $D(a)$ سره وښیو ، نو

$$D(8) = \{1, 2, 4, 8\}$$

$\tau(600) = 24$ کیری ، ځکه چې $600 = 2^3 \cdot 3 \cdot 5^2$ دی او د 600 عدد د وېشونکی سیټ د عنصر و تعداد $D(600) = (3+1)(1+1)(2+1) = 24$ پیداکری.

§ VIII. د شمېرني سیستمونه ، د g پر قاعده باندی د شمېرني په سیستم کی د طبیعی عددونو ارانه

په نړی کی مختلف ملیتونه وجود لری او که تاریخ ته وگورو ، نو د تکامل په معینه سطح کی په هر ملیت کی د طبیعی عددو مفهوم په یو ډول فورمولبندی سویدی چې په ځینو ملیتو کی د لرغونو تاریخي دلایلو پر اساس محدود مشخصات لری . په واقعیت کی د طبیعی عددو نوم ایښودنه او د هغوی ارانه په مختلفو ملیتو کی مختلف دی . دغه اختلافات د ملیتو په منځ کی د وخت په تېریدو سره د اقتصادی او کلتوری اړیکو په نتیجه لږ سوی دی .

اوس به د طبیعی عددو د ارانی مختلفي طریقې په جزئیاتو سره طرح کړو. خو لمړی به د شمېرني سیستم تعریف کړو.

تعریف ۱ - د طبیعی عددو د نوم ایښودلو و طریقې او ارانی ته د شمېرني سیستم وایو.

د شمېرني په هر سیستم کی عددونه د معینو سمبولو یا نښو په ذریعه لیکل کیری چې دغه نښو ته په اوسنی عصر کی رقم $digit$ وایو . د بیلگی په توگه د لسو پر قاعده باندی د شمېرني سیستم لس مختلف رقمه لری چې هغه عبارت دی له 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 څخه.

د شمېرني سيستم د غير ځايي (غير موضعي اويا غير قيمت مقامی) non positional په نامه يادېږي که په هغه سيستم کې د هر رقم قيمت د عدد په اړانه کې د هغه رقم په ځای او يا مقام پورې اړه ونلري. که د رقم قيمت يا ارزش د عدد په اړانه کې د هغه په ځای او مقام پورې اړه ولري ، نو دغه ډول د شمېرني سيستم ته د ځايي (موضعي يا قيمت مقامی) positional سيستم وايو. څرگنده چې زموږ مروج د لسو پر قاعده سيستم ځايي (موضعي يا قيمت مقامی) سيستم دی. د بيلگې په توگه د 1111 د عدد په څرگندونه يا اړانه کې د 1 رقم مختلف قيمتونه لري چې هر قيمت يې په دغه عدد کې د هغه په ځای پورې تړلی دی.

د شمېرني ځنې غير ځايي سيستمونه تراوسه هم ساتل سوی دی ، د بيلگې په ډول د روميانو د شمېرني سيستم دی . په لرغوني روم کې دطبيعي عددو د څرگندونې يا اړانې د پاره د لاندنيو سمبولو يا نښو څخه کار اخيستل کيدی:

I- يو ، V- پنځه ، X- لس ، L- پنځوس ، C- سل ، D- پنځه سوه او M- زر . د يوه د پاره نښه د يوې گوتې I نښه ده،دوه او درې يې هم د گوتو پر نښه (II, III) اړانه کولی، د پنځو دپاره يې خلاص لاس V او د لسو دپاره يې د دواړو لاسو څخه سر پر سر X کار اخيستی. د سلو او زرو دپاره يې د لاتيني کليمو د سر حروف (يعنی Centum او Mille) قبول کړی وه. د روم د شمېرني په سيستم کې د عددو د ليکلو طريقه په لاندې ډول وه:

(a) که يوه نښه يا سمبول چې لږتره عدد اړانه کوی ، نو بايد د هغه نښې چې لوی تره عدد اړانه کوی و راسته لاسته وليکل سي. د آخری عدد د څرگندونې دپاره د جمع عمليه اجراء کيږي. يا په بله اصطلاح د کوچنی عدد نښه د لوی عدد د نښې و نښې لاس ته ليکل کيږي، د بيلگې په ډول XII د $10+2=12$ عدد دی. همدا ډول XV د $10+5=15$ عدد نښی .

(b) که هغه نښه چې کوچنی عدد څرگندوی او د لوی عدد د نښې و کيښي خواته وليکل سي ، نو د تفریق عمليه اجراء کيږي. د بيلگې په ډول IV د $5-1=4$ عدد څرگندوی. XD د $500-10=490$ عدد څرگندوی.

د (a) او (b) د اصولو د ترکيب په نتيجه کې ويلاى سو چې د LMV څخه يې هدف د $1000-50+5=955$ او د MMXVI څخه يې هدف د 2016 عدد دی.

په لرغوني يونان کې د شمېرني سيستم د غير ځايي د شمېرني د سيستم يوه بله بيلگه ده. په نوموړی سيستم کې د 1,2,3,4,5,6,7,8,9 عددو څرگندولو دپاره يې د يوناني الفبا د لمړی نه حروفو څخه کار اخيستی ، د 10,20,30,40,50,60,70,80 او 90 دپاره تر هغه ورسته نه حروف ټاکلی وه او بالاخره 100,200,300,400,500,600,700,800,900 دپاره يې د ورستې شپږو حروفو او درې مخصوصو نښو څخه کار اخيستی . د عربو د شمېرني سيستم تر اسلام دمخه ابجد و چې د يونانيانو په څير يې عددونه د الفبا د تورو په مرسته اړانه کوله. د يادولو وړ ده چې د بالتیک د بحيرې په شمال او په پخواني روسيه کې هم د يونانيانو په شان د غير ځايي د شمېرني د سيستم څخه کار اخيستل کيدی.

د شمېرني په ټولو سيستمو کې چې پاس ټکر سول صفر وجود نلري ، دوی د صفر سره حساب نسواى کولای او د شمېرني سيستمونه يې غير ځايي دی . د لويو عددو څرگندونه مشکله وه. د چينايانو د شمېر د سيستم نژدی والی د شمېر و ځايي سيستم ته په دی کې و چې هغوی د عدد دځای (موضع) په څنگ کې يو حرف ورسره يو ځای کاوه پدی معنی چې 3T څخه به يې درې زره ، د 9H څخه به يې نه سوه مقصد و.

په اوومه عيسوی پيړی کی او تر هغه دمخه یوازنی ملیتونه چي لسيز د شمېرنی سیستم یې اختراع کړی ؤ او د هغه څخه یې کار اخیستی په هند او افغانستان کی میشته ولسونه وه . د شمېرنی د پاره د 1,2,3,4,5,6,7,8,9 نښی چي نن ورځ د عربی ارقامو په نامه مشهور دی په اصل کی په اتمه عیسوی پيړی کی د هند او افغانستان څخه و عربو ته او په دولسمه عیسوی پيړی کی د عربو څخه و اروپا ته نقل سوی دی . ددوی د شمېرنی په سیستم کی ددی دپاره چي د 42 او 402 فرق وکړی ، نو د 4 او 2 تر منځ به یې د ۰ نښه ایښودله (2۰4) . دغی نښی ته یې "sunya" ، چي د خالی او یا «سوره» په معنی دی ، ویله . پدی معنی چي دوی د صفر سره عادت وه او پر هغه باندی یې حساب کاوه .

د هند او افغان ولس د علومو ، په عام ډول د کلتور په تاریخ کی د لویو لاسته راوړنو څخه د لسيز ځایي شمېرنی د سیستم اختراع وه [6],[11],[12] او [16] وگوری.

اوس به نو راسو د g پر قاعده به د شمېرنی سیستم مطالعه کړو.

تعریف ۲ - د طبیعی عدد m سیستماتیکه لیکنه د g پر قاعده باندی ، عبارت دی د لاندنی افادی د حاصل جمع په شکل د نوموړی عدد د څرگندونی څخه:

$$m = a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0 \quad \dots (1)$$

پداسی حال کی چي $a_n \neq 0$ او a_n, a_{n-1}, \dots, a_0 د $0, 1, \dots, g-1$ او $g-1$ قیمتونه اخیستلای سی. پدی معنی چي $(a_n \neq 0)$ او $(0 \leq a_i \leq g-1)$ ($\forall i, 0 \leq i \leq n$) دی.

که د m طبیعی عدد د (1) داریکی په ذریعه اړانه سی، نو وایو چي د m طبیعی عدد د g د شمېرنی په سیستم کی راکړه سوی دی . لکه مخکی چي مو اشاره ورته وکړه لسيز د شمېرنی ځایي سیستم د الخوارزمی پذیرعه د هند او افغانستان څخه د عربو ته او په دولسمه عیسوی پيړی کی د عربو څخه و اروپا ته را نقل سو او تر نن ورځی پوری یې داسی سیال پیدا نکړی چي دهغه ځای دی ونیسی. یوازی په کمپیوتر کی د دوئیز (Binary) او شپاړسيز Hexadccimal د شمېرنی د سیستمو څخه کار اخیستل کیزی. د شمېرنی دوئیز سیستم یو د ډیرو پخوانیو د شمېرنی سیستمو څخه دی چي په پخوانی مصر کی پنځه زره کاله دمخه کار ځنی اخیستل کیدی. په پخوانی بابیلون کی (دوه تر دری زره کاله مخ کی) بیا برعکس د 60 پر قاعده د شمېرنی سیستم مروج ؤ ، چي تر نن ورځی پوری په ځینو مقیاساتو کی کار ځنی اخیستل کیدی . د بیلگی په توگه یو ساعت پر 60 دقیقو او یوه دقیقه پر 60 ثانیو وېشل سویدی .

په انگلستان او د هغه په مستعمرو کی مروج د شمېرنی سیستم د 12 پر قاعده دی. اکثرأ شیان په درجن (درزن) څرخیزی ، د بیلگی په توگه د گیلسو سیټ دولس گیلسونه لری .

په افغانستان کی تر اوسه د شمېرنی سیستم د څلورو پر قاعده هم مروج دی . د بیلگی په ډول یو سیر څلور چهاریکه ، یو چهاریک ، څلور پاوه او یو پاو څلور خورده کیزی.

په کندهار او هرات کی عوام خلک تر اوسه هم د شمېرنی سیستم د شلو پر قاعده استعمالوی.

د g پر قاعده د شمېرنی په سیستم کی د $0, 1, 2, \dots, g-1$ عددو د څرگندولو دپاره د g په تعداد نښو (سمبولو) ته ضرورت لرو چي د ارقامو په نامه یادیزی. که $g < 10$ وی ، نو د شمېرنی د سیستم د لسو پر قاعده د ارقامو څخه کار اخلو (څرگنده ده چي په هغه صورت کی د ټولو رقمو څخه کار نسو اخیستلای) د بیلگی په ډول د دوو پر قاعده د شمېرنی په سیستم کی یوازی د 0 او 1 څخه استفاده کوو.

که $g > 10$ وی ، نو تر نهو پوری د لسيز سیستم د ارقامو څخه کار اخلو او تر هغه اضافه بیا مجبوره یو چي د نورو نښو (سمبولو) څخه کار واخلو . ښه ترینه بیلگه د 16 پر قاعده د شمېرنی سیستم دی

چي په هغه کی د لسو څخه بیا تر شپاړسو پوری ، یعنی د 10,11,12,13,14 او 15 دپاره، د لاتینی الفبا د حروفو E,D,C,B,A او F څخه کار اخلو.

پدی هکله لاندني قضیه صدق کوی.

قضیه ۱ - هر طبیعي عدد m یوازی په یوه ډول په سیستماتیک شکل چي د (1) اړیکي په ذریعه افاده سوی دی پر اختیاری قاعده $g > 1$ ارائه کولای سو.

ثبوت - لمړی د طبیعي عدد m د اړائي موجودیت د (1) اړیکي په ذریعه د شمېرني په سیستم کی د g پر قاعده ، د ریاضی د استقراء پذیرعه ثابتوو.

که $m=1$ وی ، نو د نوموړی عدد سیستماتیکه څرگندونه پر اختیاری قاعده باندی $g > 1$; $m=1 \cdot g^0$ دی.

فرضوو چي د هر طبیعي عدد $1 \leq m < s$ دپاره د g پر قاعده باندی سیستماتیکه څرگندونه وجود لری. اوس نو د s عدد د $1, g, g^2, \dots, g^{n-1}, g^n$ د عددو په منځ کی مطالعه کوو. د M سیټ د هغو عددو

$$M = \{g^l / g^l > s\}$$

سیټ چي تر s لوی وی ټاکو. پدی معنی چي

د کوچنی ترین عدد د پرنسیب پر اساس د M په سیټ کی کوچنی ترین عدد وجود لری. فرضوو چي g^{n+1} کوچنی ترین عددوی چي تر s لوی دی (پداسی حال کی چي $n > 0$ دی). ځکه نو :

$$g^n \leq s < g^{n+1}$$

که $n=0$ وی ، نو $1 \leq s < g$ سره کیږی چي پدی حالت کی د شمېرني په سیستم کی د g بر قاعده باندی s یو د ارقامو څخه دی. یعنی $s=a_0$ دی.

که $n > 0$ وی ، نو د s عدد پر g^n باندی وېشو. په نتیجه کی

$$s = g^n \cdot a + r \quad \dots (*)$$

داسی لاسته راخی چي $0 \leq r < g^n \leq s$ او $0 < a < g$ وی (که $a > g$ وی ، نو $a > g^n > g^{n-1}$ ، یعنی $s > g^{n-1}$ سوی وی ، خو دا حالت ناممکنه دی)

د ریاضی د استقراء د فرضیې له مخی د r دپاره سیستماتیکه ارائه وجود لری، یعنی :

$$r = a_k g^k + \dots + a_1 g + a_0 ; \quad k < n$$

که پاس د (*) په اړیکه کی $a = a_n$ سره کیږیږدو ، نو زموږ د غوښتنې مساوات به لاسته راسی:

$$s = a_n \cdot g^n + a_k g^k + \dots + a_1 g + a_0 = a_n \cdot g^n + 0 \cdot g^{n-1} + \dots + 0 \cdot g^{k+1} + a_k g^k + \dots + a_1 g + a_0$$

یعنی د s دپاره سیستماتیکه ارائه وجود لری (پداسی حال کی چي $n > 0$ دی).

پدی ترتیب د استقراء د پرنسیب پر بنسټ د (1) سیستماتیکه ارائه د هر طبیعي عدد m دپاره وجود لری.

اوس به د (1) د اړیکي بی ساری توب په ثبوت ورسو . که $1 \leq m < g$ وی ، نو څرگنده ده چي $m = a_0$ سره ، بی ساری او یا پکړی دی.

که د $n > 0$ کم قیمت دپاره ، $g^n \leq m < g^{n+1}$ حقیقت ولری ، نو پر g^n باندی د m د عدد دوېش په نتیجه کی $a_n \neq 0$ (د نامکمله خارج قسمت) او باقیمانده r په بی ساری توگه یا پکړ تعین کیږی.

د r د عدد د وېش عمليه پر g^{n-1} باندې سرته رسوو. په نتيجه کې يې د a_{n-1} رقم د نوموړی وېش د باقیمانده په څېر لاسته راځي. دغه پروسه ته په همدا ډول ادامه ورکوو، چې په نتيجه کې يې د $g > 1$ پر قاعده د m د عدد د سيستماتيکي اړاني ټوله ارقام په بيساري توگه لاسته راځي. پدې ډول قضيه په ثبوت ورسېده.

په راتلونکې کې د $m = a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0$ اوږده شکل په عوض کې معمولاً د ليکلو د لنډ شکل $m = (a_n \dots a_1 a_0)_g$ او يا $m = a_n \dots a_1 a_0 g$ څخه کار اخلو. ددې دپاره چې د ارقامو او د

$a_0 a_1 \dots a_{n-1}$ د عددو د حاصل ضرب په منځ کې سوء تفاهم رانسې، نو يا يې پر سر يو خط کښو او يا ټوله په قوس کې لیکو او د قوس په آخر کې د سيستماتيکي اړاني قاعده لیکو. د لسو پر قاعده ($g=10$) د شمېر د سيستم د قاعدې د ليکلو څخه صرف نظر کوو. د بيلگي په ډول د 1301 طبيعي عدد د 7 پر قاعده د شمېرنې په سيستم کې داسې اړانه کوو:

$$m = 1301 = 3 \cdot 7^3 + 5 \cdot 7^2 + 3 \cdot 7 + 6$$

ددې ځايه $m = (3536)_7$ دی.

تر اوسه مو يوازې د طبيعي عددو د سيستماتيکي اړاني په هکله بحث وکړی. همدا ډول کولای سو چې د منفي طاقتو څخه په استفاده سره د g پر قاعده د نسبتې عددو دپاره د سيستماتيکي څرگندونې ته عمومي شکل ورکړو. د نسبتې عددو د لنډې اړاني د پاره غيرله ارقامو څخه وکامې «،» ته هم ضرورت لرو، خو تر يو ويز يعنی a_0 وروسته ارقام جدا کړای سو.

د بيلگي په ډول اعشاري عدد $23,561$ (د لسو پر قاعده) داسې اړانه کولای سو:

$$23,561 = 2 \cdot 10 + 3 \cdot 10^0 + 5 \cdot 10^{-1} + 6 \cdot 10^{-2} + 1 \cdot 10^{-3}$$

په زړه پورې ده چې يو نسبتې عدد د شمېرنې په يوه سيستم کې محدود کسر، خو د شمېرنې په بل سيستم کې تکراری (متوالی) کسر دی. د بيلگي په توگه د $\frac{1}{5}$ کسر د لسو پر قاعده $0,2$ دی، خو د دولسو پر قاعده $0,2497 \overline{2497}$ دی.

IX§. د عددو په سيستماتيکه اړانه کې حسابي عمليي

د مکتب په ریاضی کې د لسو پر قاعده د شمېرنې په سيستم کې د جمع، تفریق، ضرب او تقسیم عمليي مو په اسانۍ سره عملی کولی. په جمع، تفریق او ضرب کې مو عددونه به يوه ستون کې يو تر بل

لاندې ليکل او د تقسیم په عمليه کې مو عددونه د زاويي په شيمه (يعنی $\begin{array}{r} b \\ a \end{array}$) ليکل او بيا مو عمليه اجراء کول په مشابه ډول په اختیاری قاعده کې، يعنی $g > 1$ ، د شمېرنې په سيستم کې عددونه يو دبله سره جمع، تفریق، ضرب او تقسیمولای سو. ددې طریقي په استخراج کې د جمع د عمليي د تبدیلی او اتحادی خاصیتو او نظر د جمع و عمليي ته د ضرب د عمليي د توزیعی خاصیت څخه استفاده کوو.

فرضوو چې $m_1 = a_k a_{k-1} \dots a_1 a_0 g$ او $m_2 = b_s b_{s-1} \dots b_1 b_0 g$ د g پر قاعده د دوو عددو سيستماتيکه څرگندونه وی. بيله دی چې عمومیت مو نقض کړی وی، فرضوو چې $k > s$ دی. د نوموړو عددو د جمع حاصل $m_1 + m_2$ مطالعه کوو.

$$\begin{aligned}
m_1 + m_2 &= \overline{a_k a_{k-1} \dots a_1 a_0}_g + \overline{b_s b_{s-1} \dots b_1 b_0}_g = \\
&= (a_k g^k + a_{k-1} g^{k-1} + \dots + a_s g^s + \dots + a_1 g + a_0) + (b_s g^s + \dots + b_1 g + b_0) \\
&= a_k g^k + a_{k-1} g^{k-1} + \dots + a_{s+1} g^{s+1} + (a_s + b_s) g^s + \dots + (a_1 + b_1) g + (a_0 + b_0)
\end{aligned}$$

امکان لری چي وروستي اړیکه د g پر قاعده باندی د m_1+m_2 سیستماتیکه اړانه نه وی ، ځکه چي ځنی عددونه د $a_s+b_s, \dots, a_1+b_1, a_0+b_0$ د جملی څخه تر g لوی او یا د g سره مساوی وی .

که $a_0+b_0 \geq g$ وی ، نو $a_0+b_0 = g+c_0$ سره کیږی. ځکه نو :

$$\begin{aligned}
m_1+m_2 &= a_k g^k + \dots + (a_s+b_s) g^s + \dots + (a_1+b_1) g + g + c_0 = \\
&= a_k g^k + \dots + (a_s+b_s) g^s + \dots + (a_1+b_1+1) g + c_0
\end{aligned}$$

اوس نو که $a_1+b_1+1 \geq g$ وی ، نو $a_1+b_1+1 = g+c_1$ سره ، پداسی ډول چي $0 < c_1 < g$ دی.

ځکه نو :

$$\begin{aligned}
m_1+m_2 &= a_k g^k + \dots + (a_s+b_s) g^s + \dots + (a_2+b_2) g^2 + (g+c_1) g + c_0 = \\
&= a_k g^k + \dots + (a_s+b_s) g^s + \dots + (a_2+b_2+1) g^2 + c_1 g + c_0
\end{aligned}$$

په همدی ترتیب د استدلال پروسه ته (که ضرور وی د پورته په شان د تعویض عملیه عملی کوو) د g^2, g^3, \dots, g^k د ضریبو په هکله ادامه ورکوو ، څو په نتیجه کی د g پر قاعده د m_1+m_2 د جمع حاصل لاسته راسی. یعنی :

$$m_1+m_2 = c_n g^n + c_{n-1} g^{n-1} + \dots + c_1 g + c_0$$

پداسی ډول چي n مساوی په k او یا مساوی په $k+1$ سره دی.

پدی ترتیب که دوه عدده د g پر قاعده د شمېرنی په سیستم کی یو د بل سره جمع کوو ، نو باید لاندی ټکی په نظر کی ونیسو:

- (1) د نوموړی سیستم د یو رقمی عددو د جمع جدول باید راته معلوم وی . د جمع کونکو عددو ارقام باید داسی یو تر بل لاندی ولیکل سی چي د یوی مرتبی رقمونه یو تر بل لاندی وی.
- (2) د بنی لاس څخه آخری رقمونه یو د بل سره جمع کوو. که د جمع حاصل یی د g سره مساوی او یا تر هغی لوی وی ، نو د a_1+b_1 سره د یو عدد چي د مخکنی مرتبی په تعقیب سره راځی ، جمع کوو.
- (3) د مشخص حالت د په نظر کی نیولو سره a_1+b_1 یا a_1+b_1+1 پیدا کوو او پروسه ته په همدی ډول تر هغه وخته ادامه ورکو څو د آخری مرتبی رقمونه جمع کړی وی . د کار د آسانی دپاره راکړه سوی عددونه په یوه ستون کی یو تر بل لاندی لیکو ، څو وکولای سو چي په عین مرتبه کی ارقام یو د بل سره جمع کړو.

د بیلگي په توگه د څلور پر قاعده باندی د عددو جمع مطالعه کوو.

لمړی د څلورو پر قاعده د یو رقمی عددو د جمع جدول جوړوو:

جدول (4)

| | | | | |
|---|---|----|----|----|
| + | 0 | 1 | 2 | 3 |
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 10 |
| 2 | 2 | 3 | 10 | 11 |
| 3 | 3 | 10 | 11 | 12 |

د پورتنی جدول ددوهمی کړنښی او دوهم ستون څخه شروع (د کیني خوا څخه) په حجرو کی د څلورو پر قاعده د یو رقمه عددو د جمع حاصل دی ، پداسی ډول چي یو رقم یی په لمړی ستون او دوهم رقم یی د مربوطي حجری په اول کړنښه کی ځای پر ځای سوی دی. د بیلگي په ډول $3_4 + 3_4 = 12_4$ دی.

بیلگه ۱- غواړو چي 322103_4 او 1312_4 عددونه جمع کړو.

حل -

$$\begin{array}{r} 322103_4 \\ + 1312_4 \\ \hline 330021_4 \end{array}$$

په پورتنی بیلگه کی مو ولیدل چي د څلورو پر قاعده د عددو د جمع عملیه د لسو پر قاعده د جمع عملیې ته ورته دی . دلته د $11_4, 10_4$ او 12_4 زموږ د لسيز سیستم په مفهوم لس ، یولس او دولس نه بلکه یو او صفر ، یو او یو او یو او یو ده دی.

په اسانی سره امتحانیدلای سی چي پر اختیاری قاعده باندی د عددو ضرب د لسيز پر قاعده باندی د عددو و ضرب ته ورته دی، پدی معنی چي لمړی باید د یو رقمه عددو د ضرب جدول جوړ کړو (په لسيز سیستم کی تر 9 پوری ضرب زباني زده کوی). بیا هم د څلورو پر قاعده د ضرب عملیه مطالعه کوو.

د څلورو پر قاعده باندی د ضرب جدول په لاندی ډول دی:

جدول (5)

| | | | | |
|---|---|---|----|----|
| × | 0 | 1 | 2 | 3 |
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 10 | 12 |
| 3 | 0 | 3 | 12 | 21 |

بیلگه ۲ - غواړو چي د 3021_4 او 132_4 د عددو د ضرب حاصل پیدا کړو.

حل - څرنګه چي پدغه او راتلونکي بیلگه کی ټوله عملیې د څلورو پر قاعده د شمېرنی په سیستم کی صورت نیسی ، نو د قاعدی د تذکر څخه صرف نظر کوو.

$$\begin{array}{r}
3021 \\
\times 132 \\
\hline
12102 \\
21123 \\
\hline
3021 \\
\hline
1132032
\end{array}$$

بیلگه ۳- د 2112 او 12 د تقسیم حاصل لټوو.

$$\begin{array}{r}
2112:12=121 \\
-12 \\
\hline
31 \\
-30 \\
\hline
12 \\
-12 \\
\hline
0
\end{array}$$

څرگنده ده چې دشمېرني د هر سیستم دپاره باید د جمع او ضرب خانگري جدولونه جوړ کړو ، خو په هغه سیستم کی د جمع ، تفریق ، ضرب او تقسیم عمليي سرته ورسو. خو دا کار هم ډیر پرکتس غواړی .

X§. د عددو اړول دشمېرني د یوه سیستم څخه د شمېرني و بل سیستم ته.

د m هر طبیعی عدد کولای سو چې په اختیاری قاعده $g > 1$ د شمېرني په سیستم کی ارائه کړو. د ریاضی د ځینو مسئلو د حل په وخت کی نظر د شمېرني یوه سیستم ته په بل سیستم کی محاسبه اسانه صورت نیسی. ددغه اسیته ضرورت پیداکیږی چې عین عدد د شمېرني په مختلفو سیستمو کی ولرو. ډیره ساده بیلگه یی کمپیوټری سیستم دی چې عددونه او یا ځینی خصوصیات په دوئیز او یا شپاړسیز سیستم کی غواړی. ځکه نو په اوسنی ژوند کی لږ ترلږه د لسيز سیستم په څنگ کی د دوئیز او شپاړسیز سیستم سره بلد یت حتمی دی. که څه هم اوس پروگرامونه وجود لری چې د نوموړو سیستمو اړونه په چټکی او بیله کومی ستونځی سرته رسوی، خو تاسو باید دموضوع په اساس پوه سی.

فرضوو چې د m طبیعی عدد د p پر قاعده د شمېرني په سیستم کی ارائه سوی دی . غواړو چې نوموړی عدد د g پر قاعده د شمېرني په سیستم کی په لاندی ډول ارائه کړو:

$$m = a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0 \quad \dots(1)$$

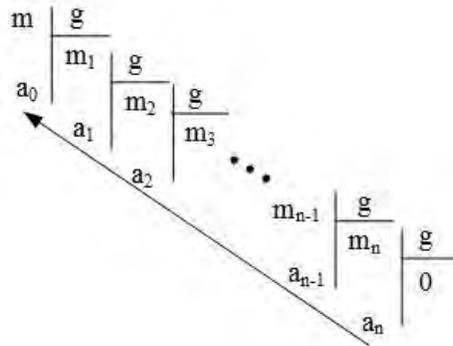
په (1) اړیکه کی د جمع او ضرب عملی د p پر قاعده د شمېرني په سیستم کی صورت نیسی. تر هغه ځایه چې د (1) اړیکه وجود درلودلای سی ، نو :

$$m = (a_n g^{n-1} + a_{n-1} g^{n-2} + \dots + a_1) g + a_0 = m_1 g + a_0$$

دلته a_0 عبارت دی پر g باندی د m د عدد دتقسیم په نتیجه پاته سوی باقی څخه . همدا ډول :

$$m_1 = a_n g^{n-1} + a_{n-1} g^{n-2} + \dots + a_2 g + a_0 = (a_n g^{n-2} + a_{n-1} g^{n-3} + \dots + a_2) g + a_1 = m_2 g + a_1$$

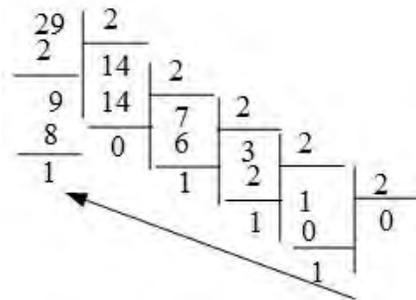
پدی معنی چي د a_1 رقم پر g باندی د m_1 د عدد د تقسیم په نتیجه د پاته سوی باقی په صفت لاسته راغلی دی. همدا ډول m_2 پر g تقسیمو او a_2 د باقی په حیث لاسته راځی. د تقسیم و عملیې پروسې ته تر هغه وخته ادامه ورکوو ترڅو خارج قسمت مساوی په صفر سره سی. پدی ترتیب مو د g پر قاعده د شمېر په سیستم کی د m د عدد د ټوله ارقام $a_n, a_{n-1}, \dots, a_1, a_0$ لاسته راوړه. د پورتنی پروسې شیما په لنډ ډول داسی انځورولای سو.



په شیما کی د وکتور مسیر د آخری باقی څخه د اول باقی و خواته چي د g پر عدد باندی د m د عدد دوېش نتیجه ده ، بنکاره کوی. پدی صورت کی $m = a_n a_{n-1} \dots a_1 a_0$ لاسته راځی.

په یاد یی ولری ، په هغه صورت کی چي $g < p$ وی نو د a_n, a_{n-1}, \dots, a_0 ټول ارقام هم تر p کوچنی دی. پدی حالت کی په نوی سیستم کی عدد مستقیماً د همدغه ارقامو څخه لاسته راځی. خو که $g > p$ وی نو دهغو ارقامو دپاره چي تر p اضافه وی ، مجبوره یو چي د نورو سمبولو په مرسته یی ارائه کړو. بیلگه ۱ - 29_{10} د دوو پر قاعده د شمېرنی په سیستم کی ارائه کوو.

حل - د لسو پر قاعده د شمېرنی په سیستم کی 29 پر 2 د پورتنی شیما پر اساس وپشو.



په نتیجه کی $29_{10} = 11101_2$ سره لاسته راځی.

کله چي د m طبیعی عدد د p پر قاعده د شمېرنی د سیستم څخه د g پر قاعده د شمېرنی سیستم ته اړوو، نو د pa_0 او g په سیستمو کی باید په کافی اندازه پر څلورگونو عملیو باندی تسلط ولرو. که د شمېرنی سیستم د لسو پر قاعده وی ، یعنی $p=10$ سره وی ، لکه پورته چي مو ولیدل ، نو د هغه اړونه د شمېرنی و سیستم ته د g پر قاعده ساده دی.

اوس به نو د شمېرنی د یوه سیستم څخه بل سیستم ته د تبدیلولو بله طریقه طرح کړو.

فرضوو چي د $m = b_k p^k + \dots + b_1 p + b_0$ افاده ، د p پر قاعده د m د عدد سیستماتیکه ارائه وی. د b_k, b_{k-1}, \dots, b_0 ارقام او د p عدد د g پر قاعده د شمېرنی په سیستم کی ارائه کوو. وروسته له دی چي د

ضرب او جمع ټوله عمليې مو د g پر قاعده د شمېرني په سيستم کې اجراء کړي ، نو راکړه سوی عدد m د g پر قاعده د شمېرني په سيستم کې ارائه سوی دی. يعنې:

$$m = a_n g^n + \dots + a_1 g + a_0$$

بيلگه ۲ - غواړو چې د 323_4 عدد د 2 پر قاعده د شمېرني په سيستم کې ارائه کړو.

$$\begin{aligned} 323_4 &= 3 \cdot 4^2 + 2 \cdot 4 + 3 \cdot 4^0 = 11_2(100_2)^2 + 10_2(100_2) + 11_2 = \\ &= 110000_2 + 1000_2 + 11_2 = 111011_2 \end{aligned}$$

پورتني طريقه هم د g پر قاعده باندې د شمېرني په سيستم کې پر څلورگونو عمليو باندې په کافي اندازه تسلط غواړي. خو که $g=10$ وي ، نو کوم مشکل ندی.

اوس نو پورتني ذکر سوی طريقي ترکیبوو. يعنې لمړی د p پر قاعده د شمېرني په سيستم کې راکړه سوی عدد و لسيز سيستم ته اړوو او بيا د لسيز سيستم څخه د g پر قاعده د شمېرني و سيستم ته اړوو. که څه هم دا طريقه اوږده ده ، خو څلورگونی عمليې يوازی د لسو پر قاعده د شمېرني په سيستم کې صورت نیسي. ددی اسپته دغه طريقه اسانه ده.

بيلگه ۳ - د 32014_5 عدد د 8 پر قاعده د شمېرني په سيستم کې ارائه کوو.

حل - راکړه سوی عدد لسيز سيستم ته را اړوو پدې معنی چې:

$$32014_5 = 3 \cdot 5^4 + 2 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5 + 4 \cdot 5^0 = 2134_{10}$$

اوس نو د 2134 عدد د 8 پر قاعده د شمېرني په سيستم کې ارائه کوو.

| | | | | |
|------|-----|----|---|---|
| 2134 | 8 | | | |
| 16 | 266 | 8 | | |
| 53 | 24 | 33 | 8 | |
| 48 | 26 | 32 | 4 | 8 |
| 54 | 24 | 1 | 4 | 0 |
| 48 | 24 | | | |
| 6 | 2 | | | |

په نتیجه کې $32014_5 = 4126_8$ لاسته راځي.

پورتني شيما چې د دوو طريقو د ترکیب په نتیجه لاست راغلی ده ، د ورځني ژوند د بيلگي سره پوره مطابقت کوي. پدې معنی که و غواړي چې يو لغت د چينائي څخه و انگليسي ته و ژباړي ، نو په هغه صورت کې چې پر دواړو ژبو تسلط ولري ، کم مشکل ندی ، خو که يوازی په چينائي او پښتو پوهیږي ، نو لمړی لغت د چينائي څخه په پښتو او بيا يې د پښتو څخه په انگليسي باند ژباړي. بله بيلگه يې د ننگرهار څخه مزار شريف ته د مخکې د لاری مستقيماً سفر کولای سي ، څرگنده ده چې زياد وخت به په بر کې و نیسي. خو دغه سفر د ننگرهار څخه کابل او د کابل څخه مزار شريف ته ژر او په آسانی سره کيدای سي.

په هغه صورت کې چې د شمېرني سيستمونه د p او g پر قاعده داسی راکړه سوی وي چې د کم طبيعي عدد k دپاره $g=p^k$ سره وي ، نو د p پر قاعده راکړه سوی عدد په آسانی سره د g پر قاعده د شمېرني و سيستم تبديلولای سو. د بيلگي په توگه ، که $p=2$ او $g=8=2^3$ وي ، د شمېرني د سيستم د اړولو پروسه تر مطالعی لاندې نیسو.

فرضوو چي $m = a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \dots + a_1 \cdot 2 + a_0$ راکړه سوی وی.

په پورتنی اړیکه کی د بڼې څخه و کین لوری ته دری دری غړی د قوسو پذیریه جلا کوو او $2_{10}^3, 2_{10}^6, 2_{10}^9, \dots$ د قوس څخه دباندی نیسو. امکان لری چي آخری قوس تر دری غړو لږ احتواء کری ، نو په هغه صورت کی فرضوو چي یو غړی عبارت دی له $0 \cdot 2_{10}^{n-1}$ او یا دوه غړی عبارت دی له $0 \cdot 2_{10}^{n+2}$ او $0 \cdot 2_{10}^{n+1}$ څخه. بلاخره پورتنی اړیکه داسی لیکلای سو:

$$m = (a_n \cdot 2^2 + a_{n-1} \cdot 2 + a_{n-2}) 2^{3k} + \dots + (a_5 \cdot 2^2 + a_4 \cdot 2 + a_3) \cdot 2^3 + (a_2 \cdot 2^2 + a_1 \cdot 2 + a_0) = \\ = (a_n \cdot 2^2 + a_{n-1} \cdot 2 + a_{n-2}) 8^k + \dots + (a_5 \cdot 2^2 + a_4 \cdot 2 + a_3) \cdot 8 + (a_2 \cdot 2^2 + a_1 \cdot 2 + a_0)$$

په قوسو کی دننه افادی د اتو پر قاعده باندی د شمېرنی په سیستم کی د m د عدد ارقام دی.

ددی طریقې معکوسه پروسه څرگنده ده پدی معنی چي د اتو پر قاعده د شمېرنی په سیستم کی د m د عدد رقم ددوو پر قاعده باندی ارائه کوو او په نتیجه کی د دوو پر قاعده د عدد څرگندونه لاسته راخی.

د کار د آسانی دپاره د $0, 1, 2, 3, 4, 5, 6, 7$ د ارقامو جدول د دوو پر قاعده د شمېرنی په سیستم کی ترتیبوو:

| | | | | | | | | |
|--------------|-----|-----|-----|-----|-----|-----|-----|-----|
| $g = 8_{10}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| $g = 2_{10}$ | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |

بیلگه ۴- غواړو چي د 42503_8 عدد د دوو پر قاعده د شمېرنی په سیستم کی ارائه کړو.

حل - د جدول څخه په استفاده سره $42503_8 = 10001010100011_2$ کیږی.

بیلگه ۵ - غواړو چي د 11001101110_2 عدد د اتو پر قاعده باندی د شمېرنی په سیستم کی ارائه کړو.

حل - راکړه سوی عدد د راستی څخه د چپي خواته په دری رقمی گروپو وېشو ، یعنی :

$$11\ 001\ 101\ 110_2$$

اوس نو د جدول څخه په استفاده سره : $11001101110_2 = 3156_8$ کیږی.

ددی فصل په پای کی یوه مهم حقیقت ته ستاسو پاملرنه را اړوم ، هغه داچي د عددو دغه ډول څرگندونه - بی تفاوته ده چي په کمه قاعده باندی وی - څونه د صفر د موجودیت د برکته ممکن دی . یوازی د صفر په مرسته کولای سو چي نور ارقام پر هغه ځای باندی ځای پر ځای کړو چي د قاعدی د طاقت جواب ورکونکی وی. لکه مخکی چي مو اشاره ورته وکړه (د VIII § شروع وگورې) د نن ورځی مروج لسيز سیستم د هند په لویدیځو او د افغانستان په ختیځو برخو کی میشت ولسونو د 300 قبل المیلاد او 600 میلادی کلو په منځ کی اختراع او تکامل ورکړی. [12]

ځلرم فصل

د مقایساتو (پرتلی) تیوری

1.8. د کانگروینسی اړیکه د تامو عددو په رینګ کې او د هغه ساده خاصیتونه

فرضوو چې m ، تر یوه لوی، اختیاری طبیعي عدد دی. د تامو عددو په رینګ \mathbb{Z} کې د کانگروینسی Congruency اړیکه د m د مودول Modulo پر اساس په لاندې ډول تعریفوو.

تعریف ۱. a او b تام عددونه د m د مودول پر اساس یو ډبل سره کانگروینت دی که پر m باندې د a او b د عددو دوپش په نتیجه کې عین باقی پاته سی. پدې معنی چې:

$$a = mq_1 + r \wedge b = mq_2 + r \wedge 0 \leq r < m$$

که د a او b تام عددونه د m د مودول پر اساس کانگروینت وی، نو لنډ لیکو: $a \equiv b \pmod{m}$.
پورتني څرګندونه د کانگروینسی د اړیکې په نامه یادوو.

بیلګه ۱. که $m=2$ وی، نو د 2 د مودول پر اساس ټوله جفت عددونه په خپل منځ کې کانگروینت دی. ځکه چې هر جفت عدد پر 2 دوپشور دی او دهغه باقیمانده پر 2 باندې دوپش په نتیجه کې مساوی په صفر سره دی. همدا ډول دوه اختیاری طاق عددونه هم د 2 د مودول پر اساس کانگروینت دی. ځکه چې د هر طاق عدد پر 2 باندې دوپش په نتیجه کې باقیمانده مساوی په 1 سره دی.

بیلګه ۲. که $m=7$ سره وی، نو $1 \equiv 8 \pmod{7}$, $8 \equiv 15 \pmod{7}$, $22 \equiv -13 \pmod{7}$ او داسې نور.

قضیه - د a او b تام عددونه د $m > 1$ د مودول پر اساس یو ډبل سره یوازې او یوازې هغه وخت کانگروینت دی، چې د هغوی د تفریق حاصل، یعنی $a-b$ پر m دوپشور وی.

ثبوت - فرضوو چې د a او b تام عددونه د $m > 1$ د مودول پر اساس یو ډبل سره کانگروینت دی، نو د لمړي تعريف له مخې $a = mq_1 + r$, $b = mq_2 + r$ او $0 \leq r < m$ دی. ددې ځایه

$$a - b = (mq_1 + r) - (mq_2 + r) = mq_1 - mq_2 = m(q_1 - q_2)$$

پدې معنی چې $(a-b):m$ دی.

برعکس، فرضوو چې $(a-b):m$ دی، نو د کم تام عدد q دپاره به $a-b=mq$ سره وی. اوس نو که $a = mq_1 + r$ او $0 \leq r < m$ وی، نو $b = a - mq = mq_1 + r - mq = m(q_1 - q) + r$ دی.

په نتیجه کې د m پر عدد باندې د a او b د عددو دوپش په نتیجه کې د هغوی باقیمانده په خپل منځ کې سره مساوی دی.

نتیجه - د a او b تام عددونه د $m > 1$ د مودول پر اساس کانگروینت دی، که د t داسې تام عدد وجود ولری، چې $a = b + mt$ سره وی.

د ثابتې سوی قضیې پر بنسټ د m د مودول پر اساس د a او b د تامو عددو د کانگروینسی بل تعريف هم فورمولبندي کولای سو:

تعریف ۲. د a او b تام عددونه د m د مودول پر اساس یو ډبل سره کانگروینت دی، که د هغوی د تفریق حاصل د m پر عدد دوپشور وی.

په تامو عددو کی دکانگروینسی اړیکه ډیر په زړه پوری خاصیتونه لری چې ځنی د هغوی څخه به اوس تر مطالعی لاندی ونیسو.

اول - په تامو عددو کی د کانگروینسی اړیکه د معادلیت اړیکه ده .

ثبوت - د هر تام عدد $a \in \mathbb{Z}$ دپاره $a \equiv a \pmod{m}$ دی، یعنی د کانگروینسی اړیکه انعکاسی خاصیت لری. همدا ډول د $a \equiv b \pmod{m}$ څخه استنباط کیری چې $b \equiv a \pmod{m}$ دی ، پدی معنی چې د کانگروینسی اړیکه تناظری خاصیت لری. بلاخره که $a \equiv b \pmod{m}$ او $b \equiv c \pmod{m}$ وی ، نو $a \equiv c \pmod{m}$ سره کیری. پدی معنی چې د کانگروینسی اړیکه د انتقالی خاصیت درلو دونکی ده. څرنکه چې د کانگروینسی اړیکه د ټولو درو خاصیتو ، یعنی انعکاسی ، تناظری او انتقالی خاصیتو درلو دونکی ده ، نو ویلای سو چې نوموړی اړیکه د معادلیت اړیکه ده.

دوهم - که $a \equiv b \pmod{m}$ او $c \equiv d \pmod{m}$ وی ، نو $(a+c) \equiv (b+d) \pmod{m}$ او $(a-c) \equiv (b-d) \pmod{m}$ سره کیری.

په بله اصطلاح د m د مودول پر اساس د کانگروینسی پر اړیکه د جمع او تفریق عملی اجراء کولای سو.

ثبوت - د $a \equiv b \pmod{m}$ او $c \equiv d \pmod{m}$ استنباط کیری چې:

$$a = b + mt_1$$

$$c = d + mt_2$$

ځکه نو $a+c = (b+d) + m(t_1+t_2)$ او $a-c = (b-d) + m(t_1-t_2)$ سره کیری . پدی معنی چې $a+c \equiv (b+d) \pmod{m}$ او $a-c \equiv (b-d) \pmod{m}$ لاسته راغلل.

نتیجه ۱ - د کانگروینسی د اړیکی په دواړو خواو کی عین تام عدد اضافه کولای سو.

نتیجه ۲ - د کانگروینسی د اړیکی اجزاء د کانگروینسی د اړیکی د یوی خوا څخه بلی خواته د علامی په تغیر سره اړولای سو.

نتیجه ۳ - د کانگروینسی د اړیکی په هره خواکی یو عدد چې د m پر عدد دوش وړ وی ، جمع یا تفریق کولای سو.

دریم - که $a \equiv b \pmod{m}$ او $c \equiv d \pmod{m}$ وی ، نو $(a \cdot c) \equiv (b \cdot d) \pmod{m}$ سره کیری.

ثبوت - که $a \equiv b \pmod{m}$ او $c \equiv d \pmod{m}$ وی ، نو $a = b + mt_1$ او $c = d + mt_2$ سره کیری ، ددی ځایه :

$$\begin{aligned} ac &= (b + mt_1)(d + mt_2) = bd + bmt_2 + dmt_1 + m^2t_1t_2 = \\ &= bd + m \underbrace{(bt_2 + dt_1 + mt_1t_2)} = bd + mt \end{aligned}$$

ځکه نو $(a \cdot c) \equiv (b \cdot d) \pmod{m}$ لاسته راځی.

نتیجه ۱ - د کانگروینسی د اړیکی دواړی خواوی د طبیعی عدد په اختیاری طاقت سره لوړلای سو،

$$a \equiv b \pmod{m} \rightarrow (\forall n \in \mathbb{N})(a^n \equiv b^n \pmod{m}) \quad \text{یعنی:}$$

نتیجه ۲ - د کانگروینسی د اریکی دواړی خواوی په عین تام عدد کی ضربولای سو.

څلرم - د کانگروینسی د اریکی $a \equiv b \pmod{m}$ دواړی خواوی د a او b پر مشترک وېشونکی چي نسبت د m و عدد ته اولیه وی ، وېشلای سو.

ثبوت - فرضوو چي $a \equiv b \pmod{m}$, $a = a_1k$, $b = b_1k$ او $(k, m) = 1$ یعنی د k او m عددونه نسبت یو او بل ته اولیه دی، ځکه نو $a = b + mt$ او $a_1k = b_1k + mt$ دی. ددی ځایه $(a_1 - b_1)k = mt$ سره کیږی . نسبت یو او بل ته د اولیه عددو د دریم خاصیت پر اساس استدلال کولای سو چي $m : (a_1 - b_1)$ کیږی. په نتیجه کی د کانگروینسی د دوهم تعریف له مخی $a_1 \equiv b_1 \pmod{m}$ دی.

پنځم - که د $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ پولینوم ضریبونه تام عددونه وی او $a \equiv b \pmod{m}$ وی ، نو $f(a) \equiv f(b) \pmod{m}$ دی.

ثبوت - د $a \equiv b \pmod{m}$ د شرط پر اساس

$$a^n \equiv b^n \pmod{m}, a^{n-1} \equiv b^{n-1} \pmod{m}, \dots, a^2 \equiv b^2 \pmod{m}$$

د پورتنیو کانگروینسی دواړی خواوی نظر د هغوی و طاقت ته د $a_n, a_{n-1}, \dots, a_2, a_1$ په تامو عددو کی ضربوو :

$$a_1 a \equiv a_1 b \pmod{m}$$

$$a_2 a^2 \equiv a_2 b^2 \pmod{m}$$

:

$$a_{n-1} a^{n-1} \equiv a_{n-1} b^{n-1} \pmod{m}$$

$$a_n a^n \equiv a_n b^n \pmod{m}$$

پورتنی کانگروینسی خوا په خوا یو د بل سره جمع کوو:

$$a_n a^n + a_{n-1} a^{n-1} + \dots + a_1 a \equiv a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b \pmod{m}$$

اوس به نو د پورتنی کانگروینسی دواړو خواو سره a_0 جمع کرو چي په نتیجه کی یی

$$f(a) \equiv f(b) \pmod{m}$$

لاسته راځی.

تراوسه چي مو دکانگروینسی خاصیتونه مطالعه کړه په هغوی کی مودول m تغیر نه کاوه. په ځینو حالتو کی کیدای سی چي د کانگروینسی مودول ته هم تغیر ورکرو.

شپږم - د کانگروینسی دواړی خواوی د هغه د مودول په شمول په طبیعی عدد n کی ضربولای سو، یعنی:

$$a \equiv b \pmod{m} \rightarrow (\forall n \in \mathbb{N})(an \equiv bn \pmod{mn})$$

ثبوت - د $a \equiv b \pmod{m}$ څخه استنباط کیږی چي $a = b + mt$ او $na = nb + nmt$. پدی معنی چي $an \equiv bn \pmod{mn}$ سره کیږی.

اووم - د کانګروینسی دواړی خواى د هغه د مودول په شمول د هغوى پر لوى ترين مشترک وېشونکي ، وېشلای سو .

پاسنئ خاصیت هم د نورو خاصیتو په شان ثابتولای سو .

دلته باید یادونه وسى چي د کانګروینسی پورتنی خاصیتوته په اختیاری رینگ کی عمومیت ورکولای سو .

§ II. د تامو عددو دوېش د ورتوب عمومی معیارونه .

فرضوو چي د a او b طبیعي عددونه راکړه سوی دی . د b پر عدد باندی د a د عدد دوېش د ورتوب مسئله دوېش د شپما پذیرعه حل کولای سو ، خو کله کله ضرور وی ، بيله دی چي یو عدد پر بل عدد ووېشو ، پدی پوه سو چي آیا راکړه سوی عدد پر بل راکړه سوی عدد دوېش وړ دی او که نه. اول خو به د یوه اختیاری طبیعي عدد دوېش د ورتوب معیار پر بل اختیاری طبیعي عدد باندی تعریف کرو .

تعریف ۱- د یوه اختیاری طبیعي عدد a دوېش د ورتوب معیار پر بل اختیاری طبیعي عدد m باندی عبارت دی له هغه معیار څخه چي د a د عدد دوېش د ورتوب کافی او لازمی شرط د m پر عدد باندی ارائه کوی .

دلته باید د اختیاری عدد m دوېش د ورتوب د عمومی معیار او د هغه عمومی معیار تر منځ چي د m د ځینو قیمتو دپاره صدق کوی ، فرق قابل سو .

دوېش د ورتوب یو د عمومی معیارو څخه د فرانسوی ریاضی پوه بلیز پاسکال Blaise Pascal له خوا کشف سوی دی .

قضیه ۱ (د پاسکال دوېش د ورتوب عمومی معیار) -

د a عدد چي د g پر اختیاری قاعده د شمېرنی په سیستم کی په لاندی ډول ارائه سوی وی ، په نظر کی نیسو :

$$a = a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0$$

د a عدد یوازی او یوازی هغه وخت د m پر عدد دوېش وړ دی چي د

$$b = a_n r_n + a_{n-1} r_{n-1} + \dots + a_1 r_1 + a_0$$

عدد پر m دوېش وړ وی ، پداسی حال کی چي د هر $1 \leq i \leq n$ ، $g^i \equiv r_i \pmod{m}$ وی او r_i په مطلقه قیمت کی کوچنی ترین عدد وی .

ثبوت - فرضو چي:

$$g \equiv r_1 \pmod{m}$$

$$g^2 \equiv r_2 \pmod{m}$$

⋮

$$g^{n-1} \equiv r_{n-1} \pmod{m}$$

$$g^n \equiv r_n \pmod{m}$$

د کانگروینسی د دریم خاصیت دوهمی نتیجی پر اساس لاندنی کانگروینسی لاسته راخی:

$$a_1g \equiv a_1r_1 \pmod{m}$$

$$a_2g^2 \equiv a_2r_2 \pmod{m}$$

⋮

$$a_{n-1}g^{n-1} \equiv a_{n-1}r_{n-1} \pmod{m}$$

$$a_n g^n \equiv a_n r_n \pmod{m}$$

که پورتنی کانگروینسی خوا په خوا سره جمع کرو، نو لاندنی کانگروینسی به لاسته راسی:

$$(a_n g^n + a_{n-1} g^{n-1} + \dots + a_2 g^2 + a_1 g) \equiv (a_n r_n + a_{n-1} r_{n-1} + \dots + a_1 r_1) \pmod{m}$$

او بیا دواړو خواوو سره a_0 جمع کوو:

$$(a_n g^n + a_{n-1} g^{n-1} + \dots + a_2 g^2 + a_1 g + a_0) \equiv (a_n r_n + a_{n-1} r_{n-1} + \dots + a_1 r_1 + a_0) \pmod{m}$$

پدی ترتیب $a \equiv b \pmod{m}$ ، یعنی $a = b + mt$ لاسته راخی.

د وروستی مساوات څخه استنباط کیری چې $a:m$ دی په هغه صورت کی چې $b:m$ وی.

د پاسکال دوپش د ورتوب د عمومی معیار څخه د یوه مشخص عدد دپاره دوپش د ورتوب معیار لاسته راوړلای سو چې د هغو څخه ځنی بی په لاندی ډول مطالعه کوو.

نتیجه ۱- د a عدد چې د لسو پر قاعده د شمېر په سیستم کی ارائه سوی وی، یوازی او یوازی هغه وخت پر دوو 2 او پنځو 5 دوپش وړ دی چې د هغه عدد اخری رقم (پروویز) بی پر دوو او پنځو دوپش وړ وی.

ثبوت - د a عدد د لسيز (د لسو پر قاعده) د شمېر په سیستم کی په لاندی ډول ارائه کولای سو.

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_2 10^2 + a_1 10 + a_0$$

څرنګه چې د هر i $1 \leq i \leq n$ دپاره $10^i \equiv 0 \pmod{2}$ او $10^i \equiv 0 \pmod{5}$ دی، نو $b = a_0$ سره کیری ددی ځایه استنباط کیری چې:

$$a:2 \leftrightarrow a_0:2$$

$$a:5 \leftrightarrow a_0:5$$

بیلګه ۱- د 10236 عدد پر 2 دوپش وړ دی. ځکه چې 6:2 دی، ولی نوموړی عدد پر 5 دوپش وړ ندی، ځکه چې 6 پر 5 دوپش وړ ندی.

نتیجه ۲- د a عدد چې د لسو پر قاعده د شمېر په سیستم کی ارائه سوی وی، یوازی او یوازی هغه وخت پر درو 3 او نهو 9 دوپش وړ دی چې دهغوی د ارقامو د جمع حاصل پر 3 یا 9 دوپش وړ وی.

ثبوت - بیا هم د a عدد د لسيز (د لسو پر قاعده) د شمېر په سیستم کی ارائه کوو:

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_2 10^2 + a_1 10 + a_0$$

څرنگه چې د هر $1 \leq i \leq n$; $10^i \equiv 1 \pmod{3}$ او $10^i \equiv 1 \pmod{9}$ دی، نو

$$b = a_n + a_{n-1} + \dots + a_0$$

دی. پدی معنی چې د b عدد په اصل کې د a د عدد د ارقامو د جمع حاصل دی. د پاسکال د قضیې پر اساس زموږ ادعا په ثبوت رسیری.

بیلگه ۲- د 51447 عدد پر 3 دوېش وړ دی، ځکه چې د ارقامو د جمع حاصل یې 21 کیږي او $21:3$ دی، خو پر 9 دوېش وړ ندی، ځکه نو نوموړی عدد هم پر 9 دوېش وړ ندی.

نتیجه ۳- د a عدد چې د لسو پر قاعده د شمېر په سیستم کې ارائه سوی وی، یوازی او یوازی هغه وخت پر 11 دوېش وړ دی که د هغه عدد د جفتو طاقتو د ارقامو د مجموعی د تفریق حاصل د طاقتو طاقتو د ارقامو د مجموعی څخه، پر 11 دوېش وړ وی.

ثبوت - د هر $k \geq 0$; $10^{2k} \equiv 1 \pmod{11}$ او $10^{2k+1} \equiv -1 \pmod{11}$ دی، ځکه نو $r_4=1, r_3=-1, r_2=1, r_1=-1$ ددی ځایه:

$$b = a_0 - a_1 + a_2 - a_3 + a_4 - \dots = (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + \dots)$$

د پاسکال د قضیې پر اساس نتیجه په ثبوت رسیری.

بیلگه ۳- د 41437 عدد پر 11 دوېش وړ دی، ځکه چې $b = (7+4+4) - (3+1) = 11$ عدد پر 11 دوېش وړ دی.

دوېش د ورتوب معیار یوازی او یوازی هغه وخت عملی او د استفادی وړ دی چې ساده او په آسانی ورڅخه کار واخیستل سی. دوېش د ورتوب ډیر معیارونه دی چې د پاسکال د عمومی معیار څخه لاسته راوړل کیږي، خو په آسانی سره نسبی عملی کیدای؛ د مثال په ډول پر 7 او 13 دوېش د ورتوب معیارونه نظر و هغو معیاروته چې مخکې مو و څېړل، مغلق دی. په عین حال کې، بیله دی چې د پاسکال د عمومی معیار څخه کار واخلو، د نوموړو عددو دوېش د ورتوب نور معیارونه سته چې په آسانی سره کار ورڅخه اخیستلای سو.

قضیه ۲- د a عدد چې د لسو پر قاعده د شمېر په سیستم کې ارائه سوی وی، یوازی او یوازی هغه وخت پر 7 یا 11 یا 13 دوېش وړ دی چې هغه عدد چې دوروستیو درو رقمو (یعنی یویز، لسيز او سليز) څخه لاسته راځي او هغه عدد چې د نوموړی عدد د پاته رقمو څخه لاسته راځي، دهغوی د تفریق نتیجه پر 7 یا 11 یا 13 دوېش وړ وی.

ثبوت - د $a = a_n 10^n + \dots + a_1 10 + a_0$ عدد په لاندی ډول سره ارائه کولای سو:

$$\begin{aligned} a &= (a_n 10^n + \dots + a_3 10^3) + a_2 10^2 + a_1 10 + a_0 = \\ &= 1000(a_n 10^{n-3} + \dots + a_3) + \overline{a_2 a_1 a_0} = \\ &= 1000 \overline{a_n \dots a_3} + \overline{a_2 a_1 a_0} \end{aligned}$$

په یاد یې ولری چې $7.11.13 = 1001$ سره کیږي. د a عدد په لاندی ډول ارائه کوو:

$$a = 1001 \overline{a_n a_{n-1} \dots a_3} + (\overline{a_2 a_1 a_0} - \overline{a_n a_{n-1} \dots a_3})$$

ددی ځایه:

$$a:7 \leftrightarrow (\overline{a_2 a_1 a_0} - \overline{a_n a_{n-1} \dots a_3}):7$$

$$a:11 \leftrightarrow (\overline{a_2 a_1 a_0} - \overline{a_n a_{n-1} \dots a_3}):11$$

$$a:13 \leftrightarrow (\overline{a_2 a_1 a_0} - \overline{a_n a_{n-1} \dots a_3}):13$$

بیلگه ۴-د 454111 عدد پر کم یو دعدد و 13,11,7 دوپش وړ دی.

حل - د تبری قضیې له مخې د راکړه سوی عدد د څخه د رقمو له مخې دوه عدده یعنی 111 او 454 جوړوو او دهغوی د تفریق حاصل، یعنی $454-111=343$ مشاهده کوو. د 343 عدد پر 7 دوپش وړ دی، خو نوموړی عدد پر 11 او 13 دوپش وړ ندی، ځکه نو اصلی راکړه سوی عدد هم یوازی پر 7 دوپش وړ خو پر 11 او 13 دوپش وړ ندی.

§III. د باقیمانده وو د ټولگیو رینگ - د باقیمانده وو کامل سیستم.

فرضوو چې $m \in \mathbb{N}$ او $m > 1$ دی. په \mathbb{I} کې مو ولیدل چې د تامو عددو په رینگ کې د m د مودول پر اساس د کانګروینسی اړیکه د معادلیت یوه اړیکه ده. ددی اړیکې څرګندونکی د تامو عددو د تجزئې سیت دی چې په \mathbb{Z} / m سره یې بنیو. معادله ټولګې چې د a عنصر یې استازئ (نماینده) وی په K_a^m (کله کله په \bar{a}) سره بنیو.

اوس به نو ددی ډول ټولګې، یعنی د K_a^m د جوړولو طریقه تشریح کړو.

فرضوو چې $b \in K_a^m$ دی. پدی معنی چې د a او b عددونه د m د مودول پر اساس کانګروینت دی. یعنی که دواړه عددونه پر m ووېشو، نو باقی به یې مساوی وی. د \mathbb{I} د دوهم تعریف له مخې د $b-a$ عدد پر m دوپش وړ دی. پدی معنی چې د t تام عدد داسی وجود لری چې $b-a=mt$ سره کیږی. خو د ټولو تامو عددو سیت چې د m په عدد کې ضرب سوی وی، د تامو عددو په رینگ \mathbb{Z} کې اساسی آیدیل جوړوی چې هغه په (m) سره بنیو. ځکه نو $b-a \in (m)$ او $b \in a+(m)$ دی. ددی استدلال په نتیجه کې $K_a^m \subset a+(m)$ کیږی.

اوس نو که $d \in a+(m)$ وی، نو $d=a+mt_1$ او $(d-a):m$ کیږی. ځکه نو $d \equiv a \pmod{m}$ او $d \in K_a^m$ دی. ددی په نتیجه کې $a+(m) \subset K_a^m$ دی او $K_a^m = a+(m)$ لاسته راځی.

پدی ډول مو وښودله چې د \mathbb{Z} / m فاکتور سیت او د $\mathbb{Z} / (m)$ فاکتور رینگ یو دبله سره منطبق دی. په دغه سیت کې د جمع \oplus او ضرب \odot عملیې په لاندی ډول سره تعریفوو:

$$K_a^m \oplus K_b^m = K_{a+b}^m$$

$$K_a^m \odot K_b^m = K_{a \cdot b}^m$$

تعریف ۱-د \mathbb{Z} / m د رینگ هر عنصر د m د مودول پر بنسټ د باقیمانده وو د ټولګې په نامه یادېږی. د \mathbb{Z} / m رینگ د m د مودول پر اساس د باقیمانده وو د ټولگیو د رینگ په نامه یادېږی. د K_a^m د ټولګې عنصر د m د مودول پر اساس د راکړه سوی ټولګې د باقیمانده په نامه یادېږی.

د ذکر وړ ده چې د 4 د مودول پر بنسټ د باقیمانده وو د ټولګیو رینګ عبارت دی له $M = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ څخه. دغه بیلګه مو د الجبر او عددونو د تیورۍ د لمړۍ برخې، د دوهم فصل په § III کې وڅېړله. قضیه ۱-د m د مودول پر اساس د باقیمانده وو د ټولګیو رینګ یعنی \mathbb{Z}/m فقط m عنصرونه لری. ثبوت - د هر تام عدد a پر m باندې د نامکمل وېش په نتیجه کې د $0, 1, 2, \dots, m-1$ د عددو څخه یوازې یو عدد باقی پاته کیږی، پدې معنی چې:

$$a = mq + r ; 0 \leq r < m$$

څرنگه چې $a \equiv r \pmod{m}$ دی، نو هر تام عدد د $K_0^m, K_1^m, K_2^m, \dots, K_{m-1}^m$ د ټولګیو څخه په یوه ټولګي اړه لری، علاوه پر دې ذکر سوي ټولګي په خپل منځ کې مختلفې دی. ځکه نو:

$$\mathbb{Z}/m = \{K_0^m, K_1^m, K_2^m, \dots, K_{m-1}^m\}$$

قضیه ۲ - که m یو مرکب عدد وی، نو \mathbb{Z}/m داسې یو تبدیلی رینګ دی چې د عینیت عنصر او د صفر وېشونکی لری. که m اولیه عدد وی، نو \mathbb{Z}/m فیلډ دی.

ثبوت - څرنگه چې د تامو عددو رینګ تبدیلی خاصیت لری، نو د ایډیالی ضرب \odot د تعریف څخه استنباط کیږی، چې د \mathbb{Z}/m رینګ هم تبدیلی خاصیت لری. د عینیت د عنصر وظیفه د K_1^m ټولګي سرته رسوی. اوس نو که $m = p \cdot q$ او $1 < p < m$ ، $1 < q < m$ وی، نو $K_p^m \neq K_0^m$ او $K_q^m \neq K_0^m$ دی.

په عین حال کې $K_p^m \odot K_q^m = K_{pq}^m = K_m^m = K_0^m$ صدق کوی. پدې معنی چې K_p^m او K_q^m صفری وېشونکی دی.

فرضوو چې m اولیه عدد دی. اوس به نو ثابتې کړو چې د \mathbb{Z}/m په رینګ کې د هر عنصر $K_a^m \neq K_0^m$ دپاره متضاد عنصر وجود لری.

په رشتیا هم که د a او m عددونه متبائن (نظر یو او بل ته اولیه یا په وېش کې بیګانه)، یعنی $(a, m) = 1$ وی، نو دوهم فصل، § IV، اولی قضیې پر اساس د x او y داسې تام عددونه وجود لری چې $ax + my = 1$ سره کیږی. ددې ځایه $ax = 1 - my$ او $ax \equiv 1 \pmod{m}$ کیږی. ځکه نو $K_a^m \cdot K_x^m = K_{ax}^m = K_1^m$ سره دی. پدې معنی چې د K_x^m ټولګي د K_a^m د ټولګي متضاد عنصر دی. په نتیجه کې ویلای سو چې \mathbb{Z}/m فیلډ دی.

بیلګه ۱ - فرضوو چې $m = 4$ سره دی. څرنگه چې 4 مرکب عدد دی، نو په حقیقت کې $\mathbb{Z}/4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ نظر د جمع او ضرب عملیو ته چې په لاندنی جدولو کې راګرځه سوی دی، تبدیلی رینګ دی. (د تمرین په شکل یې امتحان کړی!)

| | | | | |
|-----------|-----------|-----------|-----------|-----------|
| \odot | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

جدول ۸

| | | | | |
|-----------|-----------|-----------|-----------|-----------|
| \oplus | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

جدول ۷

لیدل کیری چي د عینیت عنصر یې $\bar{1}$ او د $\bar{2}$ دپاره $\bar{2} \odot \bar{2} = \bar{0}$ کیری. پدی معنی چي صفری ویشونکی لری.

بیلگه ۲ - فرسووچي $m=5$ سره دی. څرنګه چي 5 اولیه عدد دی ، نو په رشتیا هم $\mathbb{Z}/5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ نظر د جمع \oplus او ضرب \odot و عملیو ته چي د لاندنیو جدولو پذیرعه راکره سوی دی ، فیلا دی.

| | | | | | |
|-----------|-----------|-----------|-----------|-----------|-----------|
| \odot | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{1}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

جدول ۱۰

| | | | | | |
|-----------|-----------|-----------|-----------|-----------|-----------|
| \oplus | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |

جدول ۹

په آسانی سره امتحانیدای سی چي $\langle \mathbb{Z}/5, \oplus \rangle$ او $\langle \mathbb{Z}/5, \odot \rangle$ تبدیلی گروپونه دی. علاوه پر دی د ضرب عملیه \odot نظر د جمع \oplus و عملیو ته توزیعی خاصیت لری ، په نتیجه کی وپلائی سو چي $\mathbb{Z}/5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ فیلا دی.

د کار د آسانی دپاره به $\mathbb{Z}/4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ و څیرو. د $\bar{0}$ یوه ټولګی ده چي عنصرونه $4, 8, 12, \dots$ او داسی نور دی. د $\bar{1}$ په ټولګی کی $5, 9, 13, \dots$ او داسی نور شامل دی. همداسی د $\bar{2}$ او $\bar{3}$ د ټولګیو عنصرونه قطارولای سو. اوس نو که د هری ټولګی څخه په نمایندګی یو یو عنصر راواخلو نو د باقیمانده وو کامل سیستم به لاسته راسی.

تعریف ۲ - د m د مودول پر اساس د باقیمانده وو کامل سیستم عبارت دی له هغه سبت څخه چي د m عنصر و څخه داسی تشکیل سوی وی چي د m د مودول پر بنسټ د باقیمانده وو د هری ټولګی څخه یو عدد ټاکل سوی وی.

بیلګی:

۱- د $\{0, 1, 2, 3\}$ سبت د $m=4$ د مودول پر اساس د باقیمانده وو کامل سیستم دی.

۲- د $\{-1, 0, 1, 7, 8\}$ سبت د $m=5$ د مودول پر بنسټ د باقیمانده وو کامل سیستم دی.

د m د مودول پر اساس د باقیمانده وو د کامل سیستم ټولګی په لاندی ډول وپشل کیری:

۱- هغه کامل سیستمونه چي د کوچنی ترین غیر منفی باقیمانده څخه تشکیل سوی وی. پدی ډول سیستمو کی د باقیمانده وو د هری ټولګی څخه کوچنی ترین غیر منفی عدد ټاکل سوی دی.

۲- هغه کامل سیستمونه چي د کوچنی ترین مطلقه قیمت څخه تشکیل سوی دی. پدی ډول سیستمو کی د باقیمانده وو د هری تولگی څخه نظر و مطلقه قیمت ته کوچنی ترین عدد ټاکل سوی دی .

بیلگه - د 6 د مودول پر اساس $\{0,1,2,3,4,5\}$ د کوچنی ترین غیر منفی باقیمانده وو کامل سیستم دی، خو $\{-2,-1,0,1,2,3\}$ او $\{-3,-2,-1,0,1,2\}$ د کوچنی ترین مطلقه قیمت پر اساس تشکیل سوی د باقیمانده وو کامل سیستمونه دی.

قضیه ۳- که $b,(a,m)=1$ اختیاری نام عدد او x_m, \dots, x_2, x_1 د مودول پر اساس د باقیمانده وو کامل سیستم وی ، نو د $ax_m+b, \dots, ax_2+b, ax_1+b$ عددونه هم د m د مودول پر اساس د باقیمانده وو کامل سیستم جوړوی.

ثبوت - د $\{ax_1+b, ax_2+b, \dots, ax_m+b\}$ په سیټ کی m مختلف عددونه دی. که فرض کړو چي د ax_1+b او ax_2+b عددونه د m د مودول پر اساس د باقیمانده وو په یوه تولگی کی وی ، نو

$$ax_1+b \equiv ax_2+b \pmod{m}$$

$$ax_1 \equiv ax_2 \pmod{m}$$

څرنګه چي $(a,m)=1$ دی، نو $x_1 \equiv x_2 \pmod{m}$ سره کپړی. پدی معنی چي د x_1 او x_2 عددونه د باقیمانده وو په یوه تولگی کی شامل دی ، خو دغه نتیجه زموږ د فرضیې سره مغایرت لری ، ځکه چي موږ ویلی وه چي دوی مختلف دی. ځکه نو د ax_1+b او ax_2+b عددونه د m د مودول پر اساس د باقیمانده وو په یوه تولگی کی نسې شاملیدای. همداسی نتیجه د نوموړو عددو د اختیاری جوړو دپاره لاسته راوړای سو. پدی معنی چي هغوی د m د مودول پر اساس د باقیمانده وو د مختلفو تولگیو څخه انتخاب سوی او د باقیمانده وو کامل سیستم جوړوی.

IV§ د هغو باقیمانده وو د سیستم څېړنه او خاصیتونه چي د خپل مودول سره متبائن دی

د \mathbb{Z}/m د رینگ اختیاری تولگی K_a^m څېړو.

قضیه ۱- د K_a^m د تولگی هر باقیمانده د m سره عین لویترین مشترک وپشونکی لری.

ثبوت - فرضوو چي $(a,m)=d$ دی . د K_a^m د تولگی اختیاری عنصر x په نظر کی نیسو. $x \in K_a^m$ پدی معنی دی چي $x \equiv a \pmod{m}$ دی او $x-a=mt$ کپړی، پداسی حال کی چي $t \in \mathbb{Z}$ دی. د لوی ترین مشترک وپشونکی د تعریف او وروستی مساوات په نتیجه کی $(x,m)=d$ لاسته راځي.

تعریف ۱- د m د مودول او $x \in K_a^m$ لوی ترین مشترک وپشونکی د m د عدد او K_a^m د تولگی د لوی ترین مشترک وپشونکی په نامه یادپیری.

بیلگه - د K_6^8 لوی ترین مشترک وپشونکی د $m=8$ د مودول سره 2 دی.

تعریف ۲- د باقیمانده وو تولگی K_a^m د m د مودول سره د متبائن یا نسبت یو اوبل ته د اولیه په نامه یادپیری ، که د نوموړی تولگی لوی ترین مشترک وپشونکی د m د مودول سره مساوی په یوه وی.

بیلگه - فرضوو چي $m=8$ سره دی. د K_5^8 د باقیمانده وو ټولگي نسبت د 8 و مودول ته اوليه (متبائنه) ده ، ځکه چي $(5,8)=1$ دی. د یادوني وړ ده چي د K_1^8, K_3^8 او K_7^8 ټولگي هم د 8 د مودول سره (په وېش کی بیگانه) متبائن دی.

که د m د مودول سره د متبائنو ټولگيو څخه ، د هری ټولگي څخه یو عدد د اسی و ټاکوچي په نتیجه کی یي د باقیمانده وو کامل سیستم لاسته راسی ، بیانو دغه ډول سیستم د m د مودول سره د متبائن سیستم په نامه سره یادوو.

تعریف ۳ - د m د مودول پر اساس د باقیمانده وو هغه سیټ چي د m د مودول سره د هری متبائني ټولگي څخه یو عدد ټاکل سو وی ، د m د مودول سره د متبائن سیستم په نامه یادیری.

پورتني تعریف د m د مودول سره د متبائن سیستم د جوړیدو طریقو رابښي. پدی معنی چي اول باید د m د مودول پر اساس د باقیمانده وو کامل سیستم پیدا کرو او بیا د نوموړی سیستم څخه ټولی هغی ټولگي چي د m د مودول سره متبائن نه وی جدا کرو ، پاته عددونه د m د مودول سره متبائن سیستم جوړوی.

په هغه صورت کی چي د باقیمانده وو کامل سیستمونه مو د کوچنیترین غیر منفي باقیمانده او یا کوچنیترین باقیمانده د مطلقه قیمت له مخی ټاکلی وی ، نو په نتیجه کی یي د m د مودول سره متبائن سیستم د کوچنیترین غیر منفي باقیمانده او یا کوچنیترین باقیمانده د مطلقه قیمت له مخی لاسته راخی.

د بیلگي په ډول که $m=6$ وی ، نو د $\{1,5\}$ سیستم د 6 د مودول سره متبائن سیستم د کوچنیترین غیر منفي باقیمانده پر اساس جوړ سو سیستم دی. همدا ډول د $\{-1,1\}$ سیستم د 6 د مودول سره متبائن سیستم د مطلقه قیمت له مخی د کوچنیترینو باقیمانده څخه جوړ سو دی.

قضیه ۲ - که $(a,m)=1$ وی او $\{x_1, x_2, \dots, x_k\}$ د m د مودول سره متبائن سیستم وی، نو د $\{ax_1, ax_2, \dots, ax_k\}$ سیستم هم د m د مودول سره متبائن سیستم دی.

ثبوت - څرنگه چي $\{x_1, x_2, \dots, x_k\}$ د m د مودول سره متبائن سیستم دی، نو د m د مودول سره k متبائني ټولگي وجودلری. د بلی خوا $(a,m)=1$ دی او $(x_1, m)=1, (x_2, m)=1, \dots, (x_k, m)=1$ دی. ځکه نو $(ax_1, m)=1, (ax_2, m)=1, \dots, (ax_k, m)=1$ دی.

همدا ډول که $i \neq j$ د پاره $ax_i \equiv ax_j$ وی ، نو $x_i \equiv x_j \pmod{m}$ لاسته راخی. پدی معنی چي د $i \neq j$ د پاره د ax_i او ax_j باقیمانده په مختلفو ټولگيو اړه لری. په مجموع کی د ax_1, ax_2, \dots, ax_k باقیمانده په مختلفو ټولگيو اړه لری ، ځکه نو د $\{ax_1, ax_2, \dots, ax_k\}$ سیستم د m د مودول سره متبائن دی.

V§. د اویلر تابع - د اویلر او فرما قضیې

د کانگروینسی د تیوري عملی اړخ په خپله د عددونو په تیوري کی لټولای سو. د عددونو په تیوري کی کله کله د داسی عددی تابع گانو څخه کار اخلوچي د تعریف ساحه یي د طبیعی عددو سیټ وی. د هغو تابع گانو څخه یوه هم د اویلر تابع (Euler function) ده چي په ϕ سره یي ښیو.

تعریف - د $\phi: \mathbb{N} \rightarrow \mathbb{N}$ تابع د اویلر د تابع په نامه یادیری که د هر $m \in \mathbb{N}$ دپاره د $\phi(m)$ قیمت د هغو طبیعی عددو په تعداد سره مساوی وی چي تر m کوچنی او د m سره متبائن وی.

د بیلگي په توگه $\phi(1)=1, \phi(2)=2, \phi(3)=2, \phi(4)=2, \phi(5)=4, \phi(6)=2, \phi(7)=6$ کیږی. څرنگه چي د بیلگي په توگه یوازی 6 د 1 او 5 سره متبائن دی ، ځکه نو $\phi(6)=2$ کیږی.

قضيه ۱ - که د m او n طبيعي عددونه يودبله سره متبائن وي، نو $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ سره کيزي.

ثبوت - په لاندني جدول کې د $m \cdot n$ د مودول پر اساس د باقيمانده وو کامل سيستم څپرو:

| | | | | | |
|------------|------------|---------|------------|---------|------|
| 1 | 2 | \dots | r | \dots | m |
| $m+1$ | $m+2$ | \dots | $m+r$ | \dots | $2m$ |
| $2m+1$ | $2m+2$ | \dots | $2m+r$ | \dots | $3m$ |
| \vdots | | | | | |
| $(n-1)m+1$ | $(n-1)m+2$ | \dots | $(n-1)m+r$ | \dots | nr |

څرنگه چې $(m, n) = 1$ دی، یعنی هغوی يودبل سره متبائن دی، نو د a عدد د $m \cdot n$ د عدد سره يوازی او يوازی هغه وخت متبائن دی، چې هغه دهر يوه m او n سره متبائن وي (دغه حقيقت د متبائنو عددو د خاصيتو څخه په ثبوت رسيدلای سي). ځکه نو د پاسني جدول څخه لمری هغه عددونه ټاکو چې د m د عدد سره متبائن وي، وروسته بيا د ټاکلو عددو په منځ کې هغه عددونه ټاکو چې د n د عدد سره متبائن وي.

په لمری کرښه کې د m سره $\varphi(m)$ متبائن عددونه وجود لري. هغوی د m د مودول پر اساس متبائن سيستم جوړوي. ادعا کوو چې که د بيلگي په توگه $(r, m) = 1$ وي، نو تر r لاندی په ټوله ستون کې عددونه هم د m سره متبائن دي.

په رشتيا هم، که $(km+r, m) = d$ وي، نو $(r, m) = d$ سره کيزي. پدی معنی چې په جدول کې د m سره $\varphi(m) \cdot n$ متبائن عددونه موجود دي. ځکه چې د r په شمول تر r لاندی په ستون کې پوره n عددو وجود لري چې د m سره متبائن دي. ځکه نو د ټولو $\varphi(m)$ عددو دپاره د m سره د $\varphi(m) \cdot n$ متبائنو عددو موجوديت حقيقت لري.

اوس به نو د r په ستون کې ټوله عنصرونه وڅپرو:

$$r, m+r, 2m+r, \dots, (n-1)m+r \quad \dots(1)$$

ذکر سوي عددونه د $mx+r$ د اړيکي څخه پداسی حال کې چې x د مودول پر اساس د باقيمانده وو کامل سيستم عنصر دی، هم لاسته راتلای سي. پدی معنی چې په هغه صورت کې چې x په ترتيب سره په $0, 1, 2, \dots, (n-1)$ وي، نو د $mx+r$ د اړيکي پذيرعه د (1) سيستم عددونه لاسته راځي. د § III د دريمي قضیې پر اساس دی نتيجي ته رسيرو چې د (1) د عددو سيستم د n د مودول پر اساس د باقيمانده وو کامل سيستم تشکيلوي. د (1) د سيستم په عددو کې د n سره $\varphi(n)$ متبائن عددونه وجود لري. پدی لحاظ په ټولو $\varphi(m)$ ستونو کې د n عدد سره $\varphi(m) \cdot \varphi(n)$ متبائن عددونه وجود لري. پدی معنی چې:

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

بيلگه - د پورتنی ثبوت طريقه به د $\varphi(3 \cdot 4) = \varphi(3) \cdot \varphi(4)$ په بيلگه کې مشاهده کړو.

د 3 او 4 عددونه يودبل سره متبائن دي، پدی معنی چې $(3, 4) = 1$ او $12 = 3 \cdot 4$ سره کيزي. اوس نو بايد پورتنی اړيکه په ثبوت ورسوو.

د قضیې د ثبوت په څیر تر 12 عددونه په لاندې ډول اودو.

| | | | |
|---|----|----|----|
| 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 |

د 4 سره ټوله متبائن عددونه د کین لاس څخه په لمړی او دریم ستون کی ځای پر ځای سویدی ، یعنی $\varphi(4)=2$ دی . پدی معنی چي د $3 \cdot 4 = 12$ سره د متبائنو عددو سیټ باید په دغه دوو ستونو کی د عددو سب سیټ وی. څرنگه چي 1,5,9 د 3 د مودول پر اساس د 1,2,0 سره کانگروینت دی او 11,7,3 د 3 د مودول پر اساس د 2,1,0 سره کانگروینت دی ، نو په دواړو ستونو کی د 3 سره پوره $\varphi(3)=2$ متبائن عددونه وجود لری. په نتیجه کی د 12 سره پوره $\varphi(3) \cdot \varphi(4)$ متبائن عددونه وجود لری. څرنگه چي د $\varphi(12)$ د تعریف له مخي د 12 سره څلور متبائن عددونه وجود لری ، ځکه نو $\varphi(3 \cdot 4) = \varphi(3) \cdot \varphi(4)$ سره کیږی.

د ثابتی سوی قضیې څخه په استفاده سره د اویلر د تابع د قیمت د محاسبی فورمول طرح کولای سو.

قضیه ۲ - که $m = p^k$ وی ، پداسی حال کی چي p اولیه عدد دی، نو :

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

ثبوت - د p اولیه عدد په نظر کی نیسو ، هغه یوازی پر خپل ځان یعنی p او پر یوه دوپش وردی ، ځکه د ټولو هغو عددو شمېر چي تر p کوچنی او د p سره متبائن یا په وپش کی بیگانه دی $\varphi(p) = p - 1$ سره کیږی.

د $m = p^k$ د عدد وپشونکی یوازی د اولیه عدد p د غیر منفي طاقتو څخه دی ، ځکه نو د $1 \leq a \leq p^k$ عدد د p^k د عدد سره یوازی هغه وخت دیوه څخه خلاف مشترک وپشونکی لری چي $a:p$ وی. خو د $m = p^k$ د مودول پر اساس د باقیمانده ژ په کامل سیستم $1, 2, 3, \dots, p, \dots, p^k$ کی یوازی د $p^k, \dots, 2p, p$ عددونه چي تر p^k کوچنی او پر p دوپش وړ دی. د نوموړو عددو تعداد p^{k-1} دی. نور ټول عددونه یعنی $p^k - p^{k-1}$ د p^k سره متبائن دی ، یعنی $\varphi(p^k) = p^{k-1}(p-1)$ دی.

په اسانی سره لیدل کیږی چي د اویلر د تابع قیمت د $\varphi(p^k) = p^k (1 - \frac{1}{p})$ په بڼه هم لیکلای سو.

قضیه ۳ - که د m د عدد سټنډرډ (معیاری) تجزیه $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_s^{k_s}$ وی ، نو :

$$\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_s})$$

کیږی.

ثبوت - د پاسنی فارمول د لاسته راوړلو د پاره په ترتیب سره دلمړي او دوهمی قضیې څخه کار اخلو .

$$\begin{aligned}
\varphi(m) &= \varphi(p_1^{k_1} \cdot p_2^{k_2} \dots p_s^{k_s}) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \dots \varphi(p_s^{k_s}) \\
&= p_1^{k_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{k_2} \left(1 - \frac{1}{p_2}\right) \dots p_s^{k_s} \left(1 - \frac{1}{p_s}\right) = \\
&= \underbrace{p_1^{k_1} \cdot p_2^{k_2} \dots p_s^{k_s}}_m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right) = \\
&= m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right)
\end{aligned}$$

بیلگه - غوارو چي $\varphi(120)$ وشمېرو.

څرنګه چي $120=2^3 \cdot 3 \cdot 5$ سره کیری ، ځکه نو :

$$\varphi(120) = 120 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = \frac{120 \cdot 1 \cdot 2 \cdot 4}{2 \cdot 3 \cdot 5} = 32$$

د یادولو وړ ده چي د m د مودول سره هر متبائن سیستم پوره $\varphi(m)$ عنصرونه لری. دغه حقیقت د مودول د متبائنو سیستمو د تعریف (§IV وګورئ) او د اویلر د تابع څخه استنباط کیری.

قضیه ۴ (د اویلر قضیه) - که m تر یوه لوی طبیعی عدد وی او $(a, m) = 1$ وی ، نو

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

دی.

ثبوت - فرضوو چي د $x_1, x_2, \dots, x_{\varphi(m)}$ عددونه د m د مودول سره متبائن سیستم دی او د m د مودول پر اساس د کوچنیترینو غیر منفي باقیمانده و څخه تشکیل سوی دی. د §IV نظر و دوهمی قضیې ته د $ax_1, ax_2, \dots, ax_{\varphi(m)}$ عددونه هم د m د مودول پر اساس تشکیل سوی سیستم سره متبائن یا په وېش کی بیګانه دی. د ذکر سوی عددو څخه هر یو داویله سیستم د یوه عدد سره معادل دی. فرضوو چي :

$$\begin{aligned}
ax_1 &\equiv x_1^1 \pmod{m} \\
ax_2 &\equiv x_2^1 \pmod{m} \\
&\vdots \\
ax_{\varphi(m)} &\equiv x_{\varphi(m)}^1 \pmod{m}
\end{aligned} \quad \dots(2)$$

او $\{x_1, x_2, \dots, x_{\varphi(m)}\} = \{x_1^1, x_2^1, \dots, x_{\varphi(m)}^1\}$ دی.

که د دوهمی اړیکې عنصرونه ، یعنی (2) طرف په طرف سره ضرب کړو ، نو لاندنی اړیکه به لاسته راسی:

$$a^{\varphi(m)} x_1 \cdot x_2 \dots x_{\varphi(m)} \equiv x_1^1 \cdot x_2^1 \dots x_{\varphi(m)}^1 \pmod{m} \quad \dots(3)$$

څرنګه چي د $x_1^1, x_2^1, \dots, x_{\varphi(m)}^1$ عدد د $x_1 \cdot x_2 \dots x_{\varphi(m)}$ د عدد سره مساوی او د m د عدد سره متبائن دی ، نو د (3) اړیکې دواړی خواوی پر $x_1 \cdot x_2 \dots x_{\varphi(m)}$ وېشو څو په نتیجه کی :

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

لاسته راخي.

قضيه ۵ (د فرما Fermat کوچني قضيه) - که p اوليه عدد او $(a,p)=1$ وی، نو $a^{p-1} \equiv 1 \pmod{p}$ دی.

ثبوت - د فرما قضيه د اويلر د قضيه مستقيمه نتيجه ده. د اويلر د قضيه په ثبوت کې مو وليدل چي که p اوليه عدد وی، نو $\varphi(p)=p-1$ دی. ځکه نو $a^{p-1} \equiv 1 \pmod{p}$ سره کيږي.

نتيجه - که p اوليه عدد وی، نو د هر عدد دپاره:

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

صدق کوي.

په رشتيا هم، که $(a,p)=1$ وی، نو د فرما د قضيه پر بنسټ $a^{p-1} \equiv 1 \pmod{p}$ او $a^p \equiv a \pmod{p}$ دی.

که $d > 1$ ، $(a,p)=d$ وی، نو $a:p$ کيږي، ځکه نو د کانگروينسي د تعريف له مخي $a^p \equiv a \pmod{p}$ دی.

د اويلر او فرما قضيه د عددونو د تيوري د ډيرو مسئلو د پاره د حل لاره هواروي.

بيلگه ۱ - د 5 عدد يو اوليه عدد دی، پدې حساب د هر عدد a دپاره $a^5 \equiv a \pmod{5}$ دی، يعنی د هر عدد پنځم طاقت د 5 د مودول پر اساس باندې د خپل عدد سره معادل دی. ځکه نو $(1396)^5 \equiv 1396 \pmod{5}$ سره دی.

بيلگه ۲ - د 36^{97} عدد راکړه سوی دی، غواړو چي پوه سو چي که نوموړی عدد پر 17 وېشو، نو څو به باقي پاته سي.

حل - څرنگه چي د 36 او 17 عددونه په وېش کې بيگانه (متبائن) دی، يعنی $(36,17)=1$ دی، نو $36^{\varphi(17)} \equiv 1 \pmod{17}$ دی، ځکه نو $36^{16} \equiv 1 \pmod{17}$ کيږي. که د وروستۍ اړيکي دواړی خواوی د 6 په طاقت لور کړو، نو $36^{96} \equiv 1 \pmod{17}$ به لاسته راسي. ځکه نو:

$$36^{97} \equiv 36^{96} \cdot 36 \equiv 36 \pmod{17} \equiv 2 \pmod{17}$$

کيږي. پدې معنی چي پر 17 د 36^{97} د عدد دوېش په نتيجه کې 2 باقي پاته کيږي.

§VI. يو مجهوله لمړی درجه کانگروينسي - د هغوی د حل موجوديت او تعداد

تعريف ۱ - د m د مودول پر اساس يو مجهوله کانگروينسي عبارت ده له:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{m} \quad \dots(1)$$

پداسی حال کې چي د (1) اړيکي په چپه خوا کې داسی پولینوم ځای پر ځای سوی دی چي ضريبونه يي تام عددونه دی. که $a_n \not\equiv 0 \pmod{m}$ وی، نو وايو چي د (1) کانگروينسي n مه درجه لری. که $a_n \equiv 0 \pmod{m}$ وی، نو د $a_n x^n$ څخه صرف نظر کولای سو.

تعريف ۲- د (1) کانگروینسي حل عبارت دی د m د مودول پر اساس دهغه باقیمانده و د ټولگی څخه چې دهغه هر عضو په راکړه سوی کانگروینسي کی صدق وکي.

څرنګه چې د m د مودول پر اساس د باقیمانده و د ټولګيو شمېر m دی ، نو کانگروینسي په هره درجه چې وی تر m اضافه حلونه نسي درلودلای. د (1) کانگروینسي د حل د موندلو دپاره کافی ده چې د x د مجهول په عوض کی د m د مودول پر اساس د باقیمانده و کامل سیستم وضع کړو.

بیلګه - غواړو چې لاندني کانگروینسي حل کړو.

$$(2x^3+3x^2-1)\equiv 0(\text{mod } 5)$$

حل - د 5 د مودول پر اساس د باقیمانده و کامل سیستم عبارت دی د 4,3,2,1,0 د عددو څخه . که نوموړي عددونه یو په بل پسې د x په عوض کی وضع کړو ، نو لاندني نتیجې به لاسته راسي:

$$-1 \not\equiv 0(\text{mod } 5)$$

$$4 \not\equiv 0(\text{mod } 5)$$

$$27 \not\equiv 0(\text{mod } 5)$$

$$80 \equiv 0(\text{mod } 5)$$

$$175 \equiv 0(\text{mod } 5)$$

پدی ترتیب پورتنی کانگروینسي دوه حله لری چې هغه عبارت دی له K_3^5 او K_1^5 څخه.

د معادلي کانگروینسي د مفهوم څخه په استفادی سره نوموړی کانگروینسي و ساده تری کانگروینسي ته اړولای او حلولای سو.

تعريف ۲- دوی یو مجهوله کانگروینسي یو دبله سره د معادل په نامه یادوو که د هغوی د حل سبتونه یو دبل سره مساوی وی .

د بیلګی په ډول د $2x-3\equiv 0(\text{mod } 5)$ او $4x-1\equiv 0(\text{mod } 5)$ کانگروینسي یو د بل سره معادل دی، ځکه چې دهغوی دواړو د حل سبت د K_4^5 د باقیمانده و سبت دی.

د راکړه سوی کانگروینسي سره د معادلي کانگروینسي جوړول په کانگروینسي کی د هغو تبدیلاتو راوستل دی چې د کانگروینسي پر خاصیتو استوار دی (§I وګورئ). په اسانی سره امتحانیدلای سی چې په راکړه سوی کانگروینسي کی د لاندنيو تبدیلاتو په راوستلو سره د راکړه سوی کانگروینسي سره معادله کانگروینسي لاسته راځی.

(a) د کانگروینسي دواړو خواوته د $g(x)$ اختیاری پولینوم، چې ضریبونه یې تام عددونه وی، اضافه کولای سو.

(b) د کانگروینسي د یوی خوا سره داسی پولینوم اضافه کولای سو چې د هغه ضریبونه د راکړه سوی مودول مضرب وی.

(c) د کانگروینسي دواړی خواوی په داسی عدد کی ضربولای سو چې د راکړه سوی مودول مضربی عامل وی.

(d) د کانگروینسي دواړی خواوی او د هغه مودول په عین مثبت عدد کی ضربولای سو.

وروستی څېړنې به یوازې د کانګروینسي د لمړي درجي معادلوته وقف کړو.

لمړي درجه کانګروینسي د $a_1x+a_0 \equiv 0 \pmod{m}$ بڼه لري.

د کار د آسانی د پاره د پورتنی معادلی بڼه داسې اړوو چې د هغه ثابت حد د کانګروینسي د اړیکې و
بڼې خواته را اړوو او د ضریبو علامو ته یې تغیر ورکړو. په نتیجه کې اصلي کانګروینسي داسې بڼه
اخلې:

$$ax \equiv b \pmod{m} \quad \dots (2)$$

لاندي قضیه د (2) کانګروینسي د حل د موجودیت او دهغه د تعداد شرطونه طرح کوي.

قضیه ۱ - که $(a,m)=1$ وي ، نو (2) کانګروینسي یوازنی حل لري.

ثبوت - فرضوو چې x_1, x_2, \dots, x_m د مودول پر اساس د باقیمانده و کامل سیستم دی. د § III د
دریمي قضیې پر اساس د ax_1, ax_2, \dots, ax_m عددونه هم د m د مودول پر اساس د باقیمانده و کامل
سیستم جوړوي. ځکه نو ویلای سو چې د b عدد د ذکر سوو عددو د باقیمانده و په یوه ټولګې کې شامل
دی. فرض کړو چې د $1 \leq i \leq m$ دپاره $ax_i \equiv b \pmod{m}$ وي. ددی ځایه استنباط کيږي چې د K_x^m د
باقیمانده و ټولګې د (2) کانګروینسي حل دی .

د m د مودول پر اساس د ax_1, ax_2, \dots, ax_m د باقیمانده و د سیستم د عددو د یوازې والی څخه د
کانګروینسي د حل یوازې والی استنباط کيږي.

قضیه ۲ - که $(a,m)=d > 1$ وي ، او د b عدد پر d دوپش وړ نه وي ، نو (2) کانګروینسي حل
نلري.

ثبوت - د قضیې حقانیت په غیر مستقیمه توګه په ثبوت رسوو. فرضوو چې د (2) کانګروینسي حل لري
او x_0 د هغه حل دی ، پدی معنی چې $ax_0 \equiv b \pmod{m}$ د (2) کانګروینسي حل دی. ددی ځایه
استدلال کولای سو چې د یوه تام عدد t دپاره $ax_0 = b + mt$ مساوات صدق کوي. څرنگه چې $a:d$ او
 $m:d$ دی ، نو دوپش د ورتوب د اړیکې د خاصیتو په نتیجه کې $b:d$ لاسته راځي ، پدی معنی چې د b
عدد د d پر عدد دوپش وړ دی. خو دا حالت زموږ د قضیې د فرضي پر خلاف دی. ځکه نو د (2)
کانګروینسي د حل موجودیت حقیقت نلري.

قضیه ۳ - که $(a,m)=d > 1$ وي ، او د b عدد پر d دوپش وړ وي ، نو (2) کانګروینسي د حل
شمېر d دی.

ثبوت - فرضوو چې $a=a_1d$, $b=b_1d$ او $m=m_1d$ سره دی. پدی صورت کې د (2) کانګروینسي
ځانته داسې شکل اخلې:

$$a_1dx \equiv b_1d \pmod{m_1d} \quad \dots (3)$$

پداسی حال کې چې $(a_1, m_1)=1$ دی.

د $a_1dx \equiv b_1d \pmod{m_1d}$ کانګروینسي د (3) - می کانګروینسي سره معادله ده . نوموړی
کانګروینسي د لمړي قضیې پر اساس د یوازني حل درلودونکي ده.

فرضو ڇي د باقیمانده وټولگي K_i^m د هغه حل وی، نو د $i+(d-1)m, \dots, i+2m, i+m, i$ عددونه د m_1 د مودول پراساس کاتگروینت دی، خود m د مودول پراساس کاتگروینت ندی (ولی ۹).

د ذکر سوو عددو څخه هر یو د (2) کاتگروینسي دی. پدی معنی ڇي د (2) کاتگروینسي د حل شمېر d دی او هغه عبارت دی له $K_{i+(d-1)m}^m, \dots, K_{i+m}^m, K_i^m$.

ثابته سوی قضیه د کاتگروینسي د معادلی د حل موجودیت ته جواب ورکوی، خو هغه د موندلو دپاره عملی لار نه طرح کوی. د بیلگي په ډول ددوهمی قضیې پر بنسټ بی درنگه قضاوت کولای سو ڇي د $2x \equiv 5 \pmod{6}$ د کاتگروینسي معادله حل نلری. په عین حال کی د دریمي قضیې څخه استنباط کیری ڇي د $16x \equiv 28 \pmod{124}$ د کاتگروینسي معادله 4 حلونه لری، خو د نوموړو قضیو پراساس هغه حلونه نسو پیدا کولای. راتلونکی برخه به موږ ته پدی هکله د حل لارې راوبنځی.

VIII. د لمړي درجي کاتگروینسي د حل طریقې

د تبری برخی د لمړي تعریف له مخی د $a_1x + a_0 \equiv 0 \pmod{m}$ کاتگروینسي د لمړي درجي یو مجهوله کاتگروینسي ده. اوس به نو د $ax \equiv b \pmod{m} \dots (1)$ کاتگروینسي د حل طریقې په داسی حال کی وڅیړو ڇي $m > 1$ او $a \not\equiv 0 \pmod{m}$ وی. د نوموړی کاتگروینسي د حل د پاره لمړی باید د هغه د حل د موجودیت او دهغه د حلونو د شمېر په هکله سوالونه جواب ورکړو. پدی موخه لمړی د a او m لوی ترین مشترک وپشونکي $(a, m) = d$ محاسبه کوو.

که (1) کاتگروینسي حل ولری، نو د هغه د لاسته راوړلو د پاره د لاندنیو طریقو څخه کار اخلو:

لمړی طریقہ - د m د مودول پراساس د باقیمانده وټولگي په کامل سیستم هر عنصر په (1) کاتگروینسي کی وضع کوو.

ددی طریقې څخه هغه وخت کار اخیستلای سو ڇي $(a, m) = 1$ وی او د m عدد ډیر لوی نه وی. که د m عدد لوی وی، نو ددی طریقې څخه د نورو طریقو په وروستیو قدمو کی کار اخلو.

بیلگه - د $5x \equiv 3 \pmod{7}$ کاتگروینسي به حل کړو.

حل - څرنگه ڇي $(5, 7) = 1$ دی، نو راکړه سوی کاتگروینسي یو حل لری. اوس به نو د 7 د باقیمانده وټولگي په نظر کی ونیسو، هغه عبارت دی له 0, 1, 2, 3, 4, 5, 6 څخه. د باقیمانده وټولگي په کامل سیستم عنصرونه یو په یو په راکړه سوی کاتگروینسي کی وضع کوو:

$$x = 0 \rightarrow 0 \not\equiv 3 \pmod{7}$$

$$x = 1 \rightarrow 5 \not\equiv 3 \pmod{7}$$

$$x = 2 \rightarrow 10 \equiv 3 \pmod{7}$$

څرنگه ڇي پوهیږو ڇي راکړه سوی کاتگروینسي یو حل لری او هغه مو پیدا کړی، ځکه نو ضرور ندی ڇي د باقیمانده وټولگي په سیستم نور عددونه په کاتگروینسي کی د آزموینی دپاره وضع کړو. پدی معنی ڇي د

راکړه سوی کاتگروینسي حل $x=2$ سره دی. په نتیجه کی ویلای سو ڇي د باقیمانده وټولگي K_7 د

راکړه سوی کاتگروینسي حل دی. څه فکر کوی د K_7 په ټولگی کی کوم عناصر شامل دی؟

دوهمه طریقہ - راکړه سوی لمړی درجه کاتگروینسي دهغی سره په معادله کاتگروینسي داسی اړو ڇي x ضریب یی مساوی په یوه سره وی.

پدی طریقه کی پر راکړه سوی کانګرونیسی باندی لمړنې اړونې چې په §VI کی مو طرحه کړی ، عملی کوو .

دغه طریقه به پر مخکنئ بیلګه باندی عملی کړو. د کانګرونیسی دواړی خواوی که د 3 په عدد کی ضرب کړو: $15x \equiv 9 \pmod{7}$ به لاسته راسی. د $g(x) = -14x$ پولینوم د راکړه سوی پولینوم سره کانګروینت دی (ولی؟) ، نوموړی پولینوم د وروستی کانګرونیسی د کینی برخی سره جمع کوو . په نتیجه کی

$$x \equiv 9 \pmod{7}$$

لاسته راخی. اوس نو د وروستی کانګرونیسی د راستی خوا سره د $h(x) = -7$ کانګروینت پولینوم جمع کوو. په نتیجه کی $x \equiv 2 \pmod{7}$ لاسته راخی.

پدی معنی چې د K_2^7 د باقیمانده و ټولګی د راکړه سوی لمړی درجی کانګرونیسی حل دی.

دریمه (د اویلر) طریقه - د (1) کانګرونیسی د حل د طریقې اساس چې و اویلر ته منسوب سویده ، لاندنی قضیه ده.

قضیه ۱ - که $(a, m) = 1$ وی ، نو د $x = a^{\varphi(m)-1} \cdot b$ عدد د (1) کانګرونیسی حل دی.

ثبوت - د قضیې د شرط څخه استنباط کیری چې د (1) کانګرونیسی یوازنی حل لری. د $x = a^{\varphi(m)-1} \cdot b$ عدد د (1) په کانګرونیسی کی وضع کوو:

$$a \cdot (a^{\varphi(m)-1} \cdot b) = a^{\varphi(m)} \cdot b \equiv b \pmod{m}$$

په حقیقت کی د اویلر د قضیې پر بنسټ $a^{\varphi(m)} \equiv 1 \pmod{m}$ دی ، ځکه نو $a^{\varphi(m)} \cdot b \equiv b \pmod{m}$ دی . پدی معنی چې د $K_{a^{\varphi(m)-1}, b}^m$ باقیمانده و ټولګی د (1) کانګرونیسی حل دی.

بیلګه - لاندنی کانګرونیسی حلوو:

$$12x \equiv 5 \pmod{13}$$

څرنګه چې $(12, 13) = 1$ دی ، نو راکړه سوی کانګرونیسی یوازنی حل لری. د فورمول څخه په استفادی سره د x قیمت پیدا کوو ، هغه عبارت دی له: $x = 12^{\varphi(13)-1} \cdot 5 = 12^{11} \cdot 5$. پدی معنی چې د $K_{12^{11}, 5}^{13}$ د باقیمانده و ټولګی د راکړه سوی کانګرونیسی حل دی. داوسنی تخنیک څخه په استفادی سره

د $12^{11} \cdot 5$ عدد محاسبه کولای سو او هغه 3715041853440 دی. اوس نو که دغه عدد په 12 کی ضرب (44580502241280) او بیای پر 13 ووېشو ، نو 5 به باقی پاته سی (امتحان یی کی!). خو تر اوسه لا هم پدی نه پوهیرو چې د $K_0^{13}, K_1^{13}, \dots, K_{11}^{13}, K_{12}^{13}$ د باقیمانده و ټولګیو څخه کومه ټولګی د راکړه سوی کانګرونیسی حل دی.

دغه بیلګه مورته دابنې چې د اویلر طریقه ستومانه کیدونکی ده . معلومه ده چې ددوهمې طریقې له لاری په اسانی سره مطلوبی نتیجی ته رسیدای سو.

په رشتیا هم ، که د راکړه سوی کانګرونیسی د کینی خوا سره $13x - 1$ اضافه کړو ، نو

$$-x \equiv 5 \pmod{13}$$

به لاسته راسی. ددی خایه $x \equiv -5 \pmod{13}$ او یا $x \equiv 8 \pmod{13}$ دی. په نتیجه کی

$$K_{12,5}^{13} = K_8^{13} \text{ سره کیری.}$$

د لمړی درجی کانگروینسی د حل نوری طریقې هم وجود لری ، خو د هغو څېړنه ددی کتاب د درسی چوکاټ څخه وزی. په اصطلاح خطی کانگروینسی د عددونو د تیوری یوه ډیره په زړه پوری برخه تشکیلی .

دلمری درجی کانگروینسی حل ځکه هم د اهمیت وړ دی چي د هغوی د حل په نتیجه کی د دیوفانتوس Diophantus لمړی درجی معادلی حلولای سو. نوموړی معادلی د $(2) \dots ax+by=c$ ، پداسی حال کی چي $a, b, c \in \mathbb{Z}$ دی، بڼه لری.

قضیه ۲- که $(a, b) = 1$ وی ، نو د تامو عددو جوړه (x_0, y_0) یوازی او یوازی هغه وخت د (2) معادلی حل دی چي $K_{x_0}^b$ د $ax \equiv c \pmod{b}$ کانگروینسی حل وی.

ثبوت- فرضوو چي $(a, b) = 1$ دی. پدی صورت کی که $ax_0 + by_0 = c$ سره وی ، نو $ax_0 = c - by_0$ او $ax_0 \equiv c \pmod{b}$ دی.

برعکس ، فرض کړو چي x_0 د $ax \equiv c \pmod{b}$ کانگروینسی حل دی. ددی خایه $ax_0 \equiv c \pmod{b}$ کیری. په نتیجه کی د t تام عدد $t \in \mathbb{Z}$ داسی وجود لری چي دهغه دپاره د $ax_0 = c + bt$ مساوات صدق کوی ، پدی معنی چي $ax_0 - bt = c$ او (x_0, y_0) د $y_0 = t$ سره ددوهمی معادلی تام حل دی.

بیلگه- د لاندني معادلی قسمي حل (یعنی د ممکنه حلونو څخه یو حل) د تامو عددو په سیټ پیدا کوو.

$$10x + 11y = 19$$

حل- دلته $a=10$ ، $b=11$ او $c=19$ دی. د تېری قضیې د مخي د $10x \equiv 19 \pmod{11}$ کانگروینسی زموږ د معادلی جواب ورکونکی ده. د 10 او 11 عددونه یوډبله سره په وېش کی بیگانه یا متبائن دی $(10, 11) = 1$. که د راکړه سوی کانگروینسی د چپي خوا سره د $g(x) = -11x$ کانگروینت پولینوم جمع کړو ، نو د $-x \equiv 19 \pmod{11}$ کانگروینسی به لاسته راسی. د K_3^{11} د باقیمانده و ټولگی دراکړه سوی کانگروینسی حل دی ، یعنی $10 \cdot 3 \equiv 19 \pmod{11}$ دی. ددی خایه $t=1$ او $x_0=3, y_0=-1$ د تامو عددوپه سیټ کی دراکړه سوی معادلي قسمي حل دی.

د یادوني وړ دی ، کله چي د (2) معادلی قسمي حل ولرو ، نو نور حلونه یي په اسانې سره پیدا کولای سو.

§ VIII. د راکړه سوی مودول پر اساس د عدد او د باقیمانده و ټولگی ترتیب - مؤلده جزونه

فرضوو چي $m \in \mathbb{N}$ او $m > 1$ دی. د طبیعی عدد a د ټولو طاقتو سیټ ، یعنی $(1) \dots a, a^2, a^3, \dots, a^n$ د کانگروینسی د نظره د یوه د عدد (1) سره څېړو.

که $(a, m) = d > 1$ وی، نو د نومولو عددو څخه هیڅ یو هم د یوه سره د m مودول پر اساس کانگروینت ندی.

په رشتیا هم ، د $a^m \equiv 1 \pmod{m}$ د کانګروینسي څخه استنباط کيږي چې $a^n = 1 + mt$ او $1:d$ دی ، خو $1:d$ امکان نلري.

فرضو چې $(a,m)=1$ دی ، نو د اویلر د قضیې پر اساس $a^{\varphi(m)} \equiv 1 \pmod{m}$ دی.

ددی ځایه د ټولو طبیعي عددو $k \in \mathbb{N}$ دپاره $a^{k\varphi(m)} \equiv 1 \pmod{m}$ کيږي. پدی ترتیب د (1) د عددو په سیټ کی د m د مودول پر اساس لایتناهی ډیر عددونه چې د یوه سره کانګروینت دی ، وجود لري. د کوچنیترین عدد ډیرنسب پر اساس د هغو په منځ کی کوچنی ترین عدد وجود لري.

تعریف ۱- کوچنی ترین طبیعي عدد δ چې د هغه دپاره $a^\delta \equiv 1 \pmod{m}$ صدق کوی ، د m د مودول پر اساس د a د عدد د ترتیب په نامه یاديږي. که $\delta = \varphi(m)$ وی ، نو د m د مودول پر اساس د مؤلّد جذر په نامه یاديږي.

بیلگه ۱- د $a=3$ عدد د $m=4$ د مودول پر اساس مؤلّد جذر دی.

په رشتیا هم ، $\varphi(4)=2$ ، $3 \not\equiv 1 \pmod{4}$ او $3^2 \equiv 1 \pmod{4}$ کيږي. همدا ډول 3^3 او 3^4 وڅپړي.

بیلگه ۲- د $a=3$ د عدد ترتیب که څه هم د $m=8$ د مودول پر اساس دوه دی ، خو د ذکرسوی مودول پر اساس دهغه مؤلّد جذر ندی.

په رشتیا هم ، $3 \not\equiv 1 \pmod{8}$ ، $3^2 \equiv 1 \pmod{8}$ ، خو په عین حال کی $\varphi(8)=4$ دی.

قضیه ۱- که $(a,m)=1$ او $a_1 \equiv a_2 \pmod{m}$ وی ، نو د a_1 او a_2 عددونه د ذکرسوی مودول پر اساس د مساوی ترتیب خاوندان دی.

ثبوت- فرضوو چې $(a_1,m)=1$ دی او د m د مودول پر اساس د a_1 د عدد ترتیب δ_1 دی. د $a_1 \equiv a_2 \pmod{m}$ د کانګروینسي څخه استنباط کيږي چې $(a_2,m)=1$ دی. فرض کړو چې د m د مودول پر اساس د a_2 د عدد ترتیب δ_2 دی.

څرنګه چې $a_1^{\delta_1} \equiv 1 \pmod{m}$ او $a_1^{\delta_2} \equiv a_2^{\delta_2} \pmod{m}$ دی ، نو ددغه واقعیتو څخه استنباط کيږي چې $a_2^{\delta_2} \equiv 1 \pmod{m}$ دی. پدی معنی چې $\delta_2 \leq \delta_1$ دی.

همدا ډول د $a_1^{\delta_1} \equiv a_2^{\delta_1} \pmod{m}$ او $a_2^{\delta_2} \equiv 1 \pmod{m}$ استنباط کيږي چې $a_1^{\delta_1} \equiv 1 \pmod{m}$ دی، پدی معنی چې $\delta_1 \leq \delta_2$ دی ، ځکه نو $\delta_1 = \delta_2$ سره کيږي. پدی معنی چې د m د مودول پر اساس د a_1 او a_2 عددو ترتیب سره مساوی دی.

د ثابتی سوی قضیې څخه استنباط کيږي چې د K_n^m د باقیمانده و د ټولګي ټول عددونه د m د مودول پر اساس ، په هغه صورت کی چې $(a,m)=1$ وی، د عین ترتیب δ خاوندان دی. ځکه نو δ د m د مودول پر اساس د ټولو باقیمانده و د ټولګي K_n^m د ترتیب په نامه یاديږي.

علاوه پر دی د m د مودول پر اساس د عددو د ترتیب د څېړني په وخت کی کفایت کوی چې د m د مودول سره د باقیمانده و متبائن سیستم په نظر کی ونیسو.

قضیه ۲ - که $(a, m) = 1$ وی او د a د عدد ترتیب د m د مودول پر اساس δ وی. نو د $a^0 = 1, a, a^2, \dots, a^{\delta-1}$ عددو په منځ کی داسی د عددو جوړه وجود نلری چې د m د مودول پر اساس په خپل منځ کی کانگروینت وی.

ثبوت - فرضو چې د عددو داسی جوړه وجود لری. پدی معنی چې د k او l عددونه داسی وجود لری چې $0 \leq k < l < \delta$ وی او $a^k \equiv a^l \pmod{m}$ دی. پدی معنی چې $a^{l-k} \equiv 1 \pmod{m}$ دی (څرنګه چې $(a^k, m) = 1$ دی ، نو د کانگروینسی دواړی خواوی پر a^k وپشلاوی سو).

ددی ځایه استنباط کیری چې $l - k < \delta$ دی . دغه واقعیت د قضیې شرط چې δ د a د عدد ترتیب دی ، نقض کوی .

نتیجه ۱ - که د m د مودول پر اساس د باقیمانده و د ټولګی K_m^m ترتیب δ وی ، نو د باقیمانده و ټوله ټولګی $K_1^m, K_4^m, K_{p-1}^m, \dots, K_{p-2}^m, K_{p-1}^m$ په خپل منځ کی دوه په دوه مختلفی دی.

نتیجه ۲ - که د m د مودول پر اساس د a عدد مؤلذ جذر وی ، نو د $1 = a^0, a, a^2, \dots, a^{q(m)-1}$ د عددو سیستم د m د مودول سره متبائن دی.

پاسنی دواړه واقعیتونه د دوهمی قضیې او د تعریفو څخه مستقیماً استنباط کیری.

قضیه ۳ - که د m د مودول پر اساس د a د عدد ترتیب مساوی په δ وی، نو $a_1^{k_1} \equiv a_2^{k_2} \pmod{m}$ یوازی او یوازی هغه وخت صدق کوی چې $k_1 \equiv k_2 \pmod{\delta}$ وی.

ثبوت - فرضوو چې $k_1 \equiv k_2 \pmod{\delta}$ صدق کوی ، ددی ځایه $k_1 = k_2 + \delta t$ او $a^{k_1} = a^{k_2 + \delta t} = a^{k_2} \cdot a^{\delta t}$. یعنی $a^{\delta t} \equiv 1 \pmod{m}$ دی، نو $a^{k_1} \equiv a^{k_2} \pmod{m}$ او $a^{\delta t} \equiv 1 \pmod{m}$ کیری.

برعکس ، که $a^{k_1} \equiv a^{k_2} \pmod{m}$ وی ، نو د δ پر عدد باندی د k_1 او k_2 عددو د نامکمل وپش په نتیجه کی به لاندی اړیکه لاسته راسی.

$$a^{\delta q_1 - r_1} \equiv a^{\delta q_2 - r_2} \pmod{m} \text{ پداسی حال کی چې } 0 \leq r_1 < \delta \text{ او } 0 \leq r_2 < \delta \text{ دی.}$$

څرنګه چې $a^{\delta} \equiv 1 \pmod{m}$ دی ، نو باید $a^{r_1} \equiv a^{r_2} \pmod{m}$ وی . وروستی کانگروینسی یوازی هغه وخت امکان لری چې $r_1 = r_2$ سره وی، پدی معنی چې $k_1 \equiv k_2 \pmod{\delta}$ دی.

د m د مودول پر اساس د عددو او باقیمانده و ټولګیو د ترتیب د خاصیتو ثبوتونه نور زموږ ددرسی چوکاټ څخه وزی، ځکه نو لاندنی مهمه قضیه بیله ثبوته دلته فورمولبندی کوو:

قضیه ۴ - داختیاری اولیه مودول پر اساس p لااقل یو مؤلذ جذر وجود لری.

د یادونی وړ ده چې پورتنی قضیه امکان لری چې د مرکب مودول دپاره صدق ونکری. د بیلګی په ډول آزمویل کیدای سی چې د $m = 15$ مودول پر اساس مؤلذ جذر وجود نلری. په واقعیت کی $\varphi(15) = 8$ سره کیری ، په عین وخت کی د یوه ترتیب 1 ، د 4, 11, 14 ترتیب 2 ، د 2, 7, 8, 13 ترتیب 4 دی او د 3, 5, 6, 10, 12 عددونه د $m = 15$ د مودول سره متبائن ندی.

§ IX. د اوليه مودول پر اساس اندکسونه او د هغوی خاصیتونه

فرضوو چې p اوليه عدد دی، د p د مودول سره هغه متبائن سیستم چې د p د مودول پر اساس د کوچنی ترینو غیر منفي باقیمانده و څخه تشکیل سوی وی، لاندی بڼه لری:

$$1, 2, 3, \dots, (p-1) \dots (1)$$

فرضوو چې q د p د مودول پر اساس د مؤلديو جذر څخه یو جذر وی (دغه ډول جذر د تېر پاراگراف د څلرمی قضیې پر اساس وجود لری). پدی معنی چې د q د عدد ترتیب نظر د p و مودول ته په $\delta = \varphi(p) = p-1$ سره مساوی کیری. ځکه نو نظر و دوهمی قضیې، § VIII ته د

$$q^0 = 1, q, q^2, \dots, q^{p-2} \dots (2)$$

عددونه د p د مودول پر اساس دوه په دوه غیر کانگروینت دی. په بله اصطلاح د (2) عددونه په خپل منځ کی یوډبله سره کانگروینت ندی. پدی معنی چې هغوی د p د مودول پر اساس متبائن سیستم جوړوی.

د (1) د باقیمانده و د متبائن سیستم هر عدد د p د مودول پر اساس د (2) سیستم د یوه عدد سره کانگروینت دی. په بل عبارت د هر a ، $1 \leq a < p-1$ ، $0 \leq \gamma < p-2$ عدد داسی وجود لری چې $q^\gamma \equiv a \pmod{p}$ دی.

تعریف - a د عدد اندکس نظر د p و مودول (یا K_p^p ټولگی) ته د q پر قاعده باندی عبارت دی د غیر منفي تام عدد څخه پداسی ډول چې:

$$q^\gamma \equiv a \pmod{p}$$

که د اندکس تعریف ته ښه څیر سو، نو د لوگاریتم د تعریف سره یې ورته والی لیدل کیری. مور به اندکس په $\gamma = \text{ind}_q a$ سره وینیو (دغه ډول په ښه کول د $x = \log_b a$ سره پرتله کړی). د اندکس د خاصیتو د مطالعی په برخه کی دغه ډول ورته والی لیدل کیری. په خاص ډول د صفر دپاره هم (همدا ډول د K_0^p د ټولگی د ټولو عددو دپاره) د اندکس مفهوم نه تعریفوو. په عین ترتیب په هره قاعده باندی صفر د عدد لوگاریتم هم نه سو تعریفولای.

همدا ډول لکه د لوگاریتم جدول چې ترتیبوو، د p د مودول پر اساس د هر مؤلديو جذر q دپاره د اندکسو جدول هم جوړولای سو.

بیلگه ۱ - فرضوو چې $p=7$ سره کیری. د 7 د مودول پر اساس 3 مؤلديو جذر دی.

په رشتیا هم:

$$3^1 \equiv 3 \pmod{7}$$

$$3^2 \equiv 2 \pmod{7}$$

$$3^3 \equiv 6 \pmod{7}$$

$$3^4 \equiv 4 \pmod{7}$$

$$3^5 \equiv 5 \pmod{7}$$

$$3^6 \equiv 1 \pmod{7} \wedge 3^0 \equiv 1 \pmod{7}$$

پدی ډول د 7 د مودول پر اساس د $q=3$ پر قاعده د اندکسو جدول لاسته راغی.

| | | | | | | |
|--------------------|---|---|---|---|---|---|
| a | 1 | 2 | 3 | 4 | 5 | 6 |
| ind ₃ a | 0 | 2 | 1 | 4 | 5 | 3 |

جدول ۱۱

دغه ډول جدولونه معمولاً د عددونو د تیوری د مسائلو د کتاب سره ضمیمه وی.

د اولیه عدد p د مودول پر اساس اندکس لاندی خاصیتونه لری.

خاصیت ۱ - د $\gamma' \geq 0$ عدد یوازی او یوازی هغه وخت نظر د p و مودول ته د q پر قاعده د a د عدد اندکس دی ، که $(\gamma' \equiv \gamma \pmod{p-1})$ وی. پداسی حال کي چي $\gamma = \text{ind}_q a$ نظر د p مودول ته دی.

ثبوت - فرضوو چي نظر د p و مودول ته $\gamma = \text{ind}_q a$ او $\gamma' = \text{ind}_q a$ دی. ددی خایه $q^{\gamma'} \equiv a \pmod{p}$ او $q^{\gamma} \equiv a \pmod{p}$ لاسته راځي. څرنگه چي د q د عدد طاقت $\varphi(p) = p-1$ دی ، نو د § VIII ددریمی قضیې پر اساس $(\gamma' \equiv \gamma \pmod{p-1})$ کیری.

برعکس ، که $(\gamma' \equiv \gamma \pmod{p-1})$ او $p-1$ نظر د p و مودول ته د q د عدد طاقت وی ، نو بیا هم د ذکرسوی قضیې (§ VIII ، دریمه قضیه) پر اساس $q^{\gamma'} \equiv q^{\gamma} \pmod{p} \equiv 1 \pmod{p}$ کیری. پدی معنی چي γ' هم نظر د p و مودول ته د q پر قاعده د عدد اندکس دی.

خاصیت ۲ - د $a \equiv b \pmod{p}$ کانگروینسی یوازی او یوازی هغه وخت حقیقت لری چي $\text{ind}_q a \equiv \text{ind}_q b \pmod{p-1}$ وی.

دنوموری خاصیت ثبوت د لمړی خاصیت و ثبوت ته ورته دی. ځکه نو ثبوت یې د تمرین په شکل لوستونکو ته پریردم.

خاصیت ۳ - $\text{ind}_q 1 \equiv 0 \pmod{p-1}$

په رشتیا هم : $q^0 = 1 \equiv 1 \pmod{p}$ دی ، یعنی $\text{ind}_q 1 = 0$ دی.

اوس نو که $\text{ind}_q 1 = \gamma'$ وی ، نو نظر و لمړی خاصیت ته $(\text{ind}_q 1 \equiv 0 \pmod{p-1})$ او یا په بله اصطلاح $(\gamma' \equiv 0 \pmod{p-1})$ دی.

خاصیت ۴ - $\text{ind}_q q \equiv 1 \pmod{p-1}$ دی.

دغه خاصیت هم د دریم خاصیت په څېر ثابتیدلای سي.

خاصیت ۵ - د $p-1$ د مودول پر اساس د دوو عددو د حاصل ضرب اندکس د د مضربو د حاصل جمع د اندکسو سره کانگروینت دی، پدی معنی چي :

$$\text{ind}_q(a \cdot b) \equiv \text{ind}_q a + \text{ind}_q b \pmod{p-1}$$

په بله ژبه د دوو عددو د ضرب د نتیجی اندکس د هریوه عدد د اندکسو د جمع د نتیجی سره کانگروینت دی.

ثبوت - فرضوو چي $\gamma = \text{ind}_q(a \cdot b)$ ، $\gamma_1 = \text{ind}_q a$ او $\gamma_2 = \text{ind}_q b$ ، ددی خایه $q^{\gamma} \equiv a \cdot b \pmod{p}$ ،

$q^{\gamma_1} \equiv a \pmod{p}$ او $q^{\gamma_2} \equiv b \pmod{p}$ کيږي. که وروستی دوی کانگروینسي خوا په خوا سره ضرب کړو، نو $q^{\gamma_1+\gamma_2} \equiv a \cdot b \pmod{p}$ به لاسته راسي. ددی ځایه:

$$q^{\gamma} \equiv q^{\gamma_1+\gamma_2} \pmod{p}$$

د VIII §، ددریمی قضیې پر اساس :

$$\gamma \equiv \gamma_1 + \gamma_2 \pmod{p-1}$$

کيږي، پدی معنی چي $\text{ind}_q(a \cdot b) \equiv \text{ind}_q a + \text{ind}_q b \pmod{p-1}$ دی.

خاصیت ۶ -

$$\text{ind}_q a^n \equiv n \cdot \text{ind}_q a \pmod{p-1}$$

خاصیت ۷ - که $a:b$ وی، نو $\text{ind}_q a/b \equiv \text{ind}_q a - \text{ind}_q b \pmod{p-1}$ دی.

شیرم او اووم خاصیتونه مستقیماً د پنځم خاصیت څخه استنباط کيږي.

د اندکس د مفهوم څخه د لاندني کانگروینسي د حل د پاره هم استفاده کولای سو:

$$a x^n \equiv b \pmod{P}$$

پداسي حال کي چي $(a,p)=1$ او $n \in \mathbb{N}$ دی.

په رشتیا هم، که q د p د مودول پر اساس مؤلد جذر وی، نو راکره سوی کانگروینسي د لاندني لمړی درجی کانگروینسي سره معادله ده:

$$\text{ind}_q a + n \cdot \text{ind}_q x \equiv \text{ind}_q b \pmod{p-1}$$

وروستی لاسته راغلی کانگروینسي په اسانی سره حلولای سو.

بیلگه ۲ - د $3x^3 \equiv 4 \pmod{7}$ کانگروینسي حلوو.

نظر د 7 و مودول ته د 3 پر قاعده اندکس تعینوو:

$$\text{ind}_3 3 + 3 \cdot \text{ind}_3 x \equiv \text{ind}_3 4 \pmod{6}$$

د لمړی بیلگي د جدول له مخي د اندکس قیمتونه عوضوو.

$$1 + 3 \text{ind}_3 x \equiv 4 \pmod{6}$$

ددی ځایه $3 \text{ind}_3 x \equiv 3 \pmod{6}$ یا $\text{ind}_3 x \equiv 1 \pmod{6}$ کيږي.

ځکه نو: $\text{ind}_3 x \equiv 1 \pmod{6}$, $\text{ind}_3 x \equiv 3 \pmod{6}$ او $\text{ind}_3 x \equiv 5 \pmod{6}$ لاسته راځي. په نتیجه کی راکره سوی کانگروینسي دری حلونه لری چي د اندکسو د جدول له مخی یې موندلای سو، هغوی عبارت دی له: $x \equiv 5 \pmod{7}$, $x \equiv 6 \pmod{7}$ او $x \equiv 3 \pmod{7}$.

X§. د عام کسر اړول په اعشاریه کسر باندې او په اعشاریه کسر کې د تکراری رقمو تعینول

فرضوو چې a او b متبائن طبیعي عددونه دی. د $\frac{a}{b}$ عام کسر اړول په اعشاری کسر باندې د لاندنیو قضیو پذیرعه څپرو.

قضیه ۱. د $\frac{a}{b}$ عام کسر د اړولو په وخت به اعشاریه کسر باندې یوازی هغه وخت محدود اعشاری کسر لاسته راځی چې د مخرج د عدد ستندرده تجزیه د $2^\alpha \cdot 5^\beta$ شکل ولری.

ثبوت. فرضوو چې $2^\alpha \cdot 5^\beta$ دی. که $\alpha = \beta$ سره وی، نو $\frac{a}{b} = \frac{a}{2^\alpha \cdot 5^\alpha} = \frac{a}{10^\alpha}$ یو محدود اعشاریه عدد دی.

که $\alpha < \beta$ وی، نو د $\frac{a}{b} = \frac{a}{2^\alpha \cdot 5^\beta} \cdot \frac{2^{\beta-\alpha}}{2^{\beta-\alpha}} = \frac{a \cdot 2^{\beta-\alpha}}{10^\beta}$ کیری او د $\frac{a \cdot 2^{\beta-\alpha}}{10^\beta}$ عدد بیا هم یو محدود اعشاریه عدد دی.

همدا ډول که $\beta < \alpha$ وی، نو د $\frac{a}{b} = \frac{a}{2^\alpha \cdot 5^\beta} \cdot \frac{5^{\alpha-\beta}}{5^{\alpha-\beta}} = \frac{a \cdot 5^{\alpha-\beta}}{10^\alpha}$ عدد بیا هم محدود اعشاریه عدد دی.

فرضوو چې $b = c \cdot 2^\alpha \cdot 5^\beta$ دی، پداسی ډول چې $(c, 2) = 1$ او $(c, 5) = 1$ دی. فرضوو چې

$$\frac{a}{b} = \frac{a}{c \cdot 2^\alpha \cdot 5^\beta} = \frac{d}{10^m} \quad \text{حقیقت لری، ځکه نو } a \cdot 10^m = d \cdot c \cdot 2^\alpha \cdot 5^\beta \text{ سره کیری او } a \cdot 10^m : c \text{ دی. خو}$$

دغه حالت زموږ فرضیې خلاف دی. پدی معنی چې د $\frac{a}{b}$ کسر په اعشاریه محدود کسر نسو اړولای.

قضیه ۲. که د $\frac{a}{b}$ د کسر چې نورنسی لنډیدلای، د صورت معیاری (ستندرده) تجزیه د 2 او 5

مضربونه په ځان کې ونلری، نو نوموړی کسر په خالص اعشاریه متوالی کسر اړول کیدای سی. پدی حالت کې په پوه دوره کې د رقمو تعداد د b د مودول پر اساس د 10 د عدد په ترتیب δ سره مساوی کیری.

ثبوت. فرضوو چې $a < b$ دی. د a د عدد د اعشاریه کسر دوپش پروسه د b پر عدد باندې د لاندنیو شیما (طرح) په شکل تصور کولای سو:

$$\begin{array}{r}
a \cdot 10 \left| \frac{b}{0, q_1 q_2 \dots q_m q_{m+1} \dots} \right. \\
\underline{- b \cdot q_1} \\
r_1 \cdot 10 \\
\underline{- b \cdot q_2} \\
r_2 \\
\vdots \\
r_m \cdot 10 \\
\underline{b \cdot q_{m+1}} \\
r_{m+1} \\
\vdots
\end{array}$$

پورتنی پروسه د مساوات په څېر په لاندی ډول سره ارائه کولای سو:

$$\begin{array}{l}
10 a = b q_1 + r_1, \quad 0 < r_1 < b \\
10 r_1 = b q_2 + r_2, \quad 0 < r_2 < b \\
\vdots \\
10 r_m = b q_{m+1} + r_{m+1}, \quad 0 < r_{m+1} < b \\
\vdots
\end{array} \quad \dots(1)$$

څرگنده ده چې د ټولو $i \geq 1$ د پاره $0 \leq q_i < 10$ دی.

څرنګه چې $(a, b) = 1$ او $(10, b) = 1$ دی، نو د متبائنو عددو د خاصیتو پر بنسټ استدلال کولای سو چې $(10a, b) = 1$ دی. ددی ځایه څخه نتیجه اخیستل کیږی چې $(b, r_1) = 1$ دی. په همدی ډول خپل استدلال ته ادامه ورکوو، $(b, r_2) = 1$ لاسته راځی او په آخر کې

$$(b, a) = (b, r_1) = (b, r_2) = \dots = (b, r_{m+1}) = \dots = 1$$

حاصلیږی.

په نتیجه کې د $a, r_1, r_2, \dots, r_{m+1}$ عددونه د b د مودول پر اساس د کوچنیترینو مثبتو باقیمانده و سیستم جوړوی. څرنګه چې د b د مودول سره متبائن سیستم $\varphi(b)$ یعنی کوچنیترین مثبت باقیمانده احتوا کوی، نو باقیمانده تکرار پیری.

فرضوو چې د b د مودول پر اساس د 10 ترتیب δ دی. ځکه نو:

$$10^\delta \equiv 1 \pmod{b} \quad \text{او} \quad 10^\delta \cdot a \equiv a \pmod{b} \text{ دی.}$$

وروستی لاسته راغلی کانګروینسی مورته بنسټی چې د a باقیمانده د لمړی ځل د پاره وروسته له δ حده (ځله) څخه تکرار پیری. دا ځکه چې:

$$10^\delta \cdot a \equiv 10^{\delta-1} \cdot (10a) \equiv 10^{\delta-1} r_1 \equiv 10^{\delta-2} r_2 \equiv \dots \equiv r_\delta \equiv a \pmod{b}$$

دی. د (1) مساوات څخه په نتیجه کې $r_{\delta+1}=r_1$, $r_{\delta+2}=r_2$ لاسته راځي. پدی معنی چې :

$$\frac{a}{b} = 0, q_1 q_2 \dots q_\delta$$

پدی ترتیب زموږ قضیه ثابتې سوه.

د یادولو وړ ده چې د $10^\delta \equiv 1 \pmod{b}$ کانګروینسی د $10^\delta - 1 \equiv 0 \pmod{b}$ یا $\underbrace{999\dots 9}_{\delta\text{-digit}} \equiv 0 \pmod{b}$ د کانګروینسی سره معادله ده. په بله اصطلاح ویلای سو چې د نهو شمېر دلته

$\underbrace{999\dots 9}_{\delta\text{-digit}}$ تر ټولو کوچنی ترین عدد دی چې یوازی د 9 د رقم پذیرعه داسی لیکل سوی دی چې د b پر

عدد دوېش وړ دی. ددی واقعیت څخه په استفادی سره کولای سو چې د اختیاری عدد b د پاره δ محاسبه کړو.

بیلگه - اوس به وښیو چې د $\frac{9}{37}$ کسر په متوالی (تکراری) خالص اعشاریه کسر اړولای سو.

څرنګه چې $9 \div 37$, $99 \div 37$ او $999 \div 37$ دی . پدی حساب د نوموړی کسر د تکراری رقمو شمېر

دری دی. پدی معنی چې $\frac{9}{37} = 0,234$ دی.

قضیه ۳ - که د $\frac{a}{b}$ د کسر د مخراج معیاری (سټنډرډ) تجزیه د $b=2^\alpha \cdot 5^\beta \cdot c$ بڼه ولری، پداسی حال کې

چې $(c, 10) = 1$ دی، نو نوموړی کسر په غیر خالص متوالی اعشاریه کسر اوښتلاى سی. پداسی ډول چید رقمو شمېر تر تکراری دوری پوری د a او b څخه په لوی ترین سره مساوی کیری او د رقمو شمېر په یوه دوره کې د c د مودول پر اساس د 10 په ترتیب سره مساوی کیری.

ثبوت - د $\frac{a}{b} = \frac{a}{2^\alpha \cdot 5^\beta \cdot c}$ کسر په 10^γ کې داسی ضربوو چې $\gamma = \max\{\alpha, \beta\}$ دی.

$$\frac{10^\gamma \cdot a}{b} = \frac{a \cdot 2^{\gamma-\alpha} \cdot 5^{\gamma-\beta}}{c} = \frac{a_1}{c}$$

څرنګه چې $(a, c) = 1$ دی، نو د دوهمی قضیې پر اساس د $\frac{a_1}{c}$ کسر په خالص متوالی اعشاریه کسر

داسی تبدیلیدای سی چې په یوه دوره کې د رقمو شمېر یې د c د مودول پر اساس د 10 په ترتیب سره

مساوی دی. خو $\frac{a}{b} = \frac{a_1}{c} 10^{-\gamma}$ کیری ، پدی معنی چې د $\frac{a_1}{c}$ په کسر کې لازمه ده چې د γ تر عدد

وروسته و کینی خواته د اعشاریې علامه کښیښودل سی. په نتیجه کې غیر خالص متوالی اعشاریه کسر داسی لاسته راځی چې تر یوه دوران پوری یې د رقمو شمېر د γ د په اندازه دی.

بیلگه - د $\frac{9}{47}$ کسر په غیر خالص متوالي تر دوران پوری یو رقم او په یوه دوران کی دری رقمه ،

$$\frac{9}{47} = 0,1216\overline{216} \quad \text{یعنی:}$$

تراوسه مو د عددونو د تیوری عملی اړخ په ریاضی کی وڅیړي. خو د عددونو تیوری نه یوازې په ریاضی بلکه په معاصر ژوند خصوصاً په معاصر تخنیک کی ډیر مهم عملی رول لوبوی . په راتلونکی برخه کی به یې دوی بیلگې راوړم.

XI § د عددونو د تیوری عملی بیلگې

I - په عددو باندې د کتابو د په نېټه کولو بین المللی سندرد (ISBN)

ISBN (International Standard Book Number) د لمړی ځل د پاره د احصایې د پروفیسر گوردون فوستر Gordon Foster له خوا په ۱۹۶۶ع کال کی اختراع سو چي هرنوی کتاب باید تر چاپیدو وروسته د یوه نهه رقمی عدد پذیرعه په نېټه سوی وای. په ۱۹۷۰ کی د معیاری کیدلو د بین المللی سازمان ISO له خوا د هر کتاب دپاره لس رقمی عدد و ټاکل سو او هغه کتابونه چي د ۲۰۰۷ کال د جنوری تر لمړی نیټې وروسته چاپ سوی دی په دیارلس رقمی عدد په نېټه سوی دی. مور په دلته د لس رقمی سیستم په څېر نه اکتفاء وکړو.

په هند کی چاپ سوی کتاب چي د IT Infrastructure Management په نامه یادیری داسی په نېټه سوی دی: ISBN 9-38-002740-0

پورتني نېټه پر څلورو گروپو وېشل سوی ده. د کیني خوا څخه لمړی رقم یعنی 9 د ژبني یا منطقوی گروپ نمبر ده. دوهم گروپ د خپروونکي مؤسسی نمبر ده، دریم گروپ په خپروونکي مؤسسه کی د کتاب نمبر ده. مهم او په زړه پوری یې په څلورم گروپ کی یوازنی عدد دی چي د امتحانی رقم په نامه یادیری. دغه عدد په لاندی ډول سره تعینیری:

$$10 \cdot 9 + 9 \cdot 3 + 8 \cdot 8 + 7 \cdot 0 + 6 \cdot 0 + 5 \cdot 2 + 4 \cdot 7 + 3 \cdot 4 + 2 \cdot 0 = 231$$

لاسته راغلي عدد داسی تکمیلوو چي پر یولسو دوېش وړ وی. څرنګه چي 231 په خپله پر 11 وېشل کیدای سی، نو یوازې صفر د هغه سره جمع کوو، پدی معنی چي امتحانی رقم یې صفر دی. لکه چي وینوی دنوموړی کتاب د آی ایس بی ان د عدد وروستی رقم صفر دی.

دغه حقیقت به اوس د عددونو د تیوری په ژبه ولیکو:

$$(10 \cdot a + 9 \cdot b + 8 \cdot c + 7 \cdot d + 6 \cdot e + 5 \cdot f + 4 \cdot g + 3 \cdot h + 2 \cdot i + p) \equiv 0 \pmod{11} \quad \dots (1)$$

دلته د $p \in \{0, 1, 2, \dots, 10\}$ عدد امتحانی رقم دی چي د پورتني کانګروینسی د دواړو خواو سره د $a + 2b + 3c + 4d + 5e + 6f + 7g + 8h + 9i$ د جمع کیدو په نتیجه لاسته راځي، یعنی:

$$p \equiv (a + 2 \cdot b + 3 \cdot c + 4 \cdot d + 5 \cdot e + 6 \cdot f + 7 \cdot g + 8 \cdot h + 9 \cdot i) \pmod{11}$$

د امتحانی رقم په هکله لاندني دوی قضیې ثابتیدلای سی.

قضیه ۱ - په آی اس بی ان کی د یوه رقم غلطی د امتحانی رقم پذیرعه په ډاګه کیدلای سی.

قضیه ۲ - په آی اس بی ان کی د دو عددو اړول د امتحانی رقم پذیرعه په ډاګه کیدلای سی.

بیلگه - په جرمنی کی د IT-Strategie تر عنوان لاندی د چاپ سوی کتاب د آی اس بی ان نمره :

ISBN 3-658-02048-2

ده. دلته 3 د جرمنی ژبو مملکتو نمره ده پدی معنی چي اتریش او سویس هم پکینی شامل دی.

658 په جرمنی کی د Springer Vieweg د خپرونکی مؤسسی کود(نمره) دی. نوموړی کتاب په دغه مؤسسه کی 2048 عنوان دی چي هغوی چاپ کړیدی.

$$10\cdot3+9\cdot6+8\cdot5+7\cdot8+6\cdot0+5\cdot2+4\cdot0+3\cdot4+2\cdot8=218$$

$$218 \equiv 9 \pmod{11}$$

$$218+2 \equiv 0 \pmod{11}$$

پدی معنی چي 2 یی په رشتیا هم امتحانی رقم دی.

که په پورتنی آی اس بی ان نمره کی د بیلگی په ډول د 3 پر خای 1 ولیکو ، یعنی:

ISBN 1-658-02048-2

نو امتحانی رقم به یی 2 نه بلکه 0 به وی.

اوس نو که په راکړه سوی آی اس بی ان کی سهواً دوه رقمه سره واړو ، د بیلگی په توگه

ISBN 3-658-02084-2

ولیکو بیا به هم د هغه امتحانی رقم 2 نه بلکه (خو؟) به وی.

II- د خبرونو قفلول(شفرول) Cryptology

په لرغونی یونان او پخوانی مصر کی د جگړو په وخت کی د خبرونو لیرل د شفر پذیرعه یوه عامه نظامی طریقه وه. په اوسنی عصر کی د الکترونیکی خبرونو د لیرلو او رالیرلو په برخه کی یا د بانک پذیرعه د پیسو د لیرلو ، د بیمی او سفر د محاسبی د سیستمو په برخه کی د ارقامو او معلوماتو قفلول (شفرول) ډیر ضروری او مهمه کړنلاره ده. مور دلته د درو طریقو څخه لنډه یادونه کوو.

a) د الفباء یوويز تعویض

په دغه طریقه کی د خبر د اصلی حروفو پر خای تر هر حرف وروسته د بیلگی په ډول دریم حرف په دورانی بڼه خای پر خای کوی . دغه طریقه په لرغونی یونان کی د قیصر له خوا څخه په کار اچول سوی وه.

بیلگه:

ABC...XYZ

اصلی الفباء

DEF...ABC

قلف سوی الفباء

نو د حروفو پر خای په ترتیب سره د 0 څخه تر 25 عددو څخه کار واخلو نو د C حرف به د لاندی کانگروینسی په ذریعه قلف کرای سو

$$C(x) \equiv x+3 \pmod{26} ; 0 \leq C(x) < 26$$

هر خبر چي قلف سی ، نو د هغه د خلاصولو (دی شفرولو) دپاره کلي ته ضرورت دی . د D د حرف د خلاصولو کلي

$$D(y) \equiv y+23 \pmod{26} ; 0 \leq D(y) < 26$$

ده. ځکه چي په جمعی رینگ کی 23 د 26 د مودول پر اساس د 3 معکوس دی.

پدی حالت کی د قفلولو یوازی 25 امکانه لرو ، ځکه چي $C_{1,m}(x) \equiv x+m \pmod{26}$ دی ، پداسی حال کی چي $m \in \{1,2,3,\dots,25\}$ دی . دا طریقہ ډیره غیر مصونه ده .

که د جمع پر ځای د ضرب د عملیې څخه کار واخلو ، یعنی که $C_n(x) \equiv n \cdot x \pmod{26}$ وی ، پداسی حال کی چي $0 \leq C_n(x) < 26$ دی او پدی طریقہ خبر قلف کړو ، نو ډیر ژر به ځیر سو چي د $n \in \{1,2,3,\dots,25\}$ د ټولو عددو څخه کار نسو اخیستلای ، ځکه چي د بیلگي په توگه د $n=2$ د پاره د $C_2(x) \equiv 2 \cdot x \pmod{26}$ کانگروینسی د 0 او 13 دپاره عین قیمت لاسته راځی . یعنی :

$$2 \cdot 0 \equiv 0 \pmod{26}$$

$$2 \cdot 13 \equiv 0 \pmod{26}$$

عملاً A او N دواړه د A جواب ورکونکي دی . دا ځکه چي د 2 او 26 لوی ترین مشترک وپشونکی وجودلری او هغه 2 دی ، پدی معنی چي $(2,26)=2$ کیږی. ددی دپاره چي یوازي نتیجه لاسته راسی ، باید $(n,26)=1$ وی. پدی حالت کی د قفلولو امکانات نور هم لږیږی او د قفلولو طریقہ نوره هم غیر مصونه کیږی.

(b) د الفباء ځونېز تعویض

پدی طریقہ کی د الفباء یو حرف د څو حروفو په سلسله سره تعویض کیږی . د بیلگي په ډول کولای سو چي A په $CEXL$ باندی تعویض کړو. دلته که څه هم د قفلولو امکانات ډیر یږی ، خو د ډیرو خبرو د خلاصولو په هڅه کی د یو ډول نظم حدس وهل کیدای سی. یعنی کلي یې په اسانه لاسته راتلای سی.

(c) د قفلولو (شفرولو) سیستم - د ډیفی - هیلمن د کلیو تبادله

تورپیکی او ریډی غواړی چي خپل مسیجونه مصنون ، بیله دی چي نور یې ولولی ، سره تبادله کړی. څرنګه چي دواړه په لوړو ریاضیاتو پوهیږی ، نو فیصله یې وکړه چي هر حرف به ، د بیلگي په توگه لکه په ابجد کی ، په عدد سره شفر کړی . پدی معنی چي ددی شفر به یو مثبت تام عدد وی. په عمل کی معمولاً ډیر لوی عدد وی ، خو زه دلته د مسئلې د څرګندولو دپاره فرضوم چي مسیج ټوټه ټوټه سوی دی او زه دلته یوازی یو کلمه د شفر څخه خلاصوم.

زموږ شفر سوی کلمه "پوهه" ده ، په ابجد کی "پ" نسته ، خو زه "پ" په 11 سره بنییم، د "و" قیمت په ابجد کی 6 او د "ه" قیمت 5 دی ، که ټوله سره جمع کړو نو 27 لاسته راځی. یعنی زموږ مسیج $m=27$ دی. اوس نو باید د k یوه کلي وټاکي څو د هغه پذیرعه تورپیکی د m مسج په شفر کی قلف او ریډی یې وروسته د k په کلي خلاص کړی.

هغوی دری رقمیزه اولیه عدد ، د بیلگي په توگه $p=113$ ، او یوه کلي $k=34$ سره وټاکل.

تورپيکي و ريدي ته د 14 عدد وروليزي ($k \cdot m = 34 \cdot 27 \equiv 14 \pmod{113}$). ريدي پوهيږي چي د هغوي کلي 34 او اوليه عدد يا د مودول اساس يي 113 ټاکلي و. څرنگه چي $m < p$ دی ، نو ريدي پدي پوهيږي چي د $k^{-1}(km) = (k^{-1}k)m \equiv m \pmod{p}$ د فورمول پر اساس د اصلي مسيح قيمت پيدا کولای سي. خو ددي موخي دپاره بايد لمري د k^{-1} قيمت پيدا کړي. هغه پوهيږي چي په §V د فرما د قضیې پر اساس :

$$k^{p-1} \equiv 1 \pmod{p}$$

کيري او $k^{-1} \cdot k \equiv 1 \pmod{p}$ دی . هغه وروستي دوی کانگروينسي سره پرتله کړي او دی نتيجي ته ورسیدی چي $k^{-1} \equiv k^{p-2} \pmod{p}$ سره . يعنی $k^{-1} \equiv 34^{111} \pmod{113}$ سره د وروستي کانگروينسي قيمت به وروسته پيدا کړو.

$$k^{-1} \equiv 10 \pmod{113} \wedge 10 \cdot 14 = 140 \equiv 27 \pmod{113}$$

پدي معنی چي اصلي مسيح 27 و.

اوس به نو وگورو چي هغه $k^{-1} \equiv 34^{111} \pmod{113}$ څنگه وشمېرل.

$$111 = 64 + 32 + 8 + 4 + 2 + 1$$

$$k^{-1} \equiv 34^{111} \pmod{113} = 34^{64} \cdot 34^{32} \cdot 34^8 \cdot 34^4 \cdot 34^2 \cdot 34 \pmod{113}$$

$$34^2 \equiv 26 \pmod{113}$$

$$34^4 \equiv 26^2 \pmod{113} \equiv 111 \pmod{113}$$

$$34^8 \equiv 111^2 \pmod{113} \equiv 4 \pmod{113}$$

$$34^{16} \equiv 4^2 \pmod{113} \equiv 16 \pmod{113}$$

$$34^{32} \equiv 16^2 \pmod{113} \equiv 30 \pmod{113}$$

$$34^{64} \equiv 30^2 \pmod{113} \equiv 109 \pmod{113}$$

ددي ځايه:

$$k^{-1} \equiv 34^{111} \pmod{113} = 34^{64} \cdot 34^{32} \cdot 34^8 \cdot 34^4 \cdot 34^2 \cdot 34 \pmod{113}$$

$$k^{-1} \equiv 34^{111} \pmod{113} = 109 \cdot 30 \cdot 4 \cdot 111 \cdot 26 \cdot 34 \pmod{113} \equiv 10 \pmod{113}$$

د ډيفي - هيلمن د کلي د تبادلې طريقه تر نن ورځي پوري د بيلگي په ډول د کمپيوټري جال د ssh په پروتوکول کي په کار اچول کيږي.

پنجم فصل يو متحوله پولينوم

1.8. د عددونو پر فيلډ باندې د يو متحوله پولينومو رينگ

د پولينوم مفهوم دريځي د اساسي مفهومو څخه شمېرل کيږي. ددغه مفهوم څخه په الجبر ، اناليز ، دار قامو دپه شفرولو (Data encoding) او د رياضي په نورو برخو کې استفاده ځنې کيږي. پولينوم په دوو طريقو سره تعريفيدای سي . يو تعريف يې د تابع په شکل دی او بل تعريف يې الجبري دی . په لمړي حالت کې پولينوم د مخصوصي تابع په شکل څېرل کيږي او په دوهم حالت کې د الجبري افادې په څير تعبير کيږي. مور به يې دلته دوهم شکل وڅېرو .

د پولينوم د تعريف د پاره فرضور چې P د عددونو فيلډ دی .

تعريف 1- د P پر فيلډ باندې يو مجهوله پولينوم عبارت دی له لاندني افادې څخه :

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \dots(1)$$

پداسي حال کې چې n غير منفي تام عدد $a_n, a_{n-1}, \dots, a_1, a_0 \in P$ او x^0, \dots, x^{n-1}, x^n سمبولونه دی . x د متحول د k درجې په نامه يادېږي ، a_k د (1) پولينوم د k ام ضريب او يا د x^k ($k=1,2,\dots,n$) د ضريب په نامه يادېږي.

پولينوم چې متحول يې x وي په $f(x), g(x), h(x), f_1(x), f_2(x), \dots$ او داسي نور ، سره بڼيو. د P پر فيلډ باندې د x د متحول سره د ټولو پولينومو سيټ په $P[x]$ سره بڼيو. څرگنده ده چې $P \subset P[x]$ دی.

تعريف 2- د $a_k x^k$ افاده ، پداسي حال کې چې $k=1,2,\dots,n$ دی، د (1) پولينوم د k -ام حد (غړي) په نامه يادېږي. د a_0 عدد د نوموړي پولينوم د ثابت حد په نامه يادېږي. په ياد يې ولری چې دواړه a_0 او $a_0 x^0$ سره يو دی. که په (1) پولينوم کې $a_k = 0$ وي ، نو وايو چې د پولينوم k -ام حد مساوی په صفر سره دی.

$$f(x) = 5x^3 + (-\sqrt{2})x^2 + x + (-3) \quad \text{بيلگه 1 -}$$

په پورتنی پولينوم کې -3 يې ثابت حد ، $x=1$ يې لمړی حد ، $-\sqrt{2}x^2$ يې دوهم حد او $5x^3$ يې دريم حد دی. نوموړی پولينوم نور حدونه (غړي) نه لری . څرگنده ده چې د

$$s(x) = 0 \cdot x^5 + 0 \cdot x^4 + 5x^3 + (-\sqrt{2})x^2 + x + (-3)$$

پولينوم د $f(x)$ د پولينوم سره عين حدونه لری ، پدې معنی چې د $s(x)$ پولينوم د $f(x)$ د پولينوم سره مساوی دی. له دې وروسته به د پولينومو د صفری حدو د ليکلو څخه ډډه کوو.

بيلگه 2- د $g(x) = ix^4 + (2-3i)x + (1-\sqrt{2})$ په پولينوم کې $1-\sqrt{2}$ يې ثابت حد ، $(2-3i)x$ يې لمړی حد او ix^4 څلرم حد دی . نور حدونه يې مساوی په صفر سره دی .

تعريف 3- د $f(x)$ په پولينوم کې هغه حد چې صفر نه وي اود غير صفری حدو په منځ کې لوړترين طاقت نما ولری د پولينوم د لوی ترين حد په نامه يادوو. د لوی ترين حد ضريب د لوی ترين ضريب او

د لوی ترین حد طاقت د د نوموړي پولینوم د طاقت په نامه یادوو. د $f(x)$ د پولینوم طاقت په $\deg f(x)$ یا dcgf سره ښیو. په پورتنی بیلگو کی $\text{dcgf}=3$ او $\text{dcgg}=4$ دی، د لمړی پولینوم لوی ترین حد $5x^3$ او د دوهم پولینوم لوی ترین حد ix^4 دی.

تعریف ۴- هغه پولینوم چي ټوله حدونه یې مساوی په صفر سره وی د صفری پولینوم په نامه یادیری. صفر پولینوم په $0(x)=0$ سره ښیو. د صفری پولینوم د ښودلو دپاره د دریم تعریف څخه استفاده نسو کولای، پدی معنی چي صفری پولینوم ته هیڅ ډول طاقت نه قائلیریو. همدا ډول کله کله د کار د اسانولو دپاره کله چي د n درجه ای پولینومو سیټ تر مطالعی لاندی نیسو، ښه دی چي صفری پولینوم هم د هغه سیټ د غړی په صفت قبول کړو.

تعریف ۵- د $f(x)$ د صفر څخه خلاف پولینوم ښودنه د $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ په شکل، په داسی حال کی چي $a_n \neq 0$ وی، د نوموړي پولینوم د ستندرد (معیاری) شکل په نامه یادیری.

$0(x)=0$ د صفری پولینوم ستندرد (معیاری) شکل دی.

فرضوو چي د $f(x)$ او $g(x)$ دوه پولینومه په ستندرد شکل د P پر فیله باندی راکړه سوی دی، یعنی:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \dots(2)$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0 \quad \dots(3)$$

تعریف ۶- د (2) او (3) پولینومونه یو ډبل سره مساوی دی، که د هغوی ستندرد شکلونه یو ډبل سره مساوی وی. مساوی پولینومونه په $f(x)=g(x)$ سره ښیو. پورتنی تعریف په سمبولیکه بڼه داسی لیکلای سو:

$$f(x) = g(x) \stackrel{\text{def}}{\iff} n = m \wedge (\forall k, 0 \leq k \leq n)(a_k = b_k)$$

بیلگه ۳- لاندنی پولینومونه یوډبله سره مساوی دی:

$$f(x) = (\sin^2 \alpha + \cos^2 \alpha)x^2 + i^2 x + \log_2 4$$

او

$$g(x) = x^2 + (-1)x + 2$$

ځکه چي $\sin^2 \alpha + \cos^2 \alpha = 1$ ، $i^2 = -1$ او $\log_2 4 = 2$ دی.

اوس به نو پر پولینومو د جمع او ضرب عملی تعریف کړو.

تعریف ۷- که د (2) او (3) د $f(x)$ او $g(x)$ ستندرد شکل وی او د $n \geq m \geq 0$ غیر مساوات صدق وکړی، نو د $f(x)$ او $g(x)$ د پولینومو د جمع حاصل عبارت دی له:

$$s(x) = a_n x^n + \dots + a_{m+1} x^{m+1} + (a_m + b_m)x^m + \dots + (a_1 + b_1)x + (a_0 + b_0) \quad \dots(4)$$

د $f(x)$ او $g(x)$ د پولینومو د ضرب حاصل عبارت دی له:

$$h(x) = c_{n+m}x^{n+m} + \dots + c_1x + c_0 \quad \dots (5)$$

پداسی حال کی چي :

$$c_{n+m} = a_n b_m, \dots, c_2 = a_2 b_2 + a_1 b_1 + a_2 b_0, c_1 = a_1 b_1 + a_1 b_0, c_0 = a_0 b_0$$

دی. د $f(x)$ او $g(x)$ د پولینوم حاصل جمع $s(x)$ او د هغوی د ضرب حاصل $h(x)$ په یوازنی ډول تعریف سوی دی او په لاندی ډول سره یې ښیو:

$$h(x) = f(x) \cdot g(x) \quad \text{او} \quad s(x) = f(x) + g(x)$$

څرگنده ده چي $s(x)$ او $h(x)$ د P پر فیله باندی پولینومونه دی. پدی معنی چي $s(x) \in P[x]$ او $h(x) \in P[x]$ دی. که $f(x)$ او $g(x)$ عددونه وی، نو $s(x)$ او $h(x)$ د P پر فیله باندی د نوموړو عددو د جمع او ضرب حاصل دی.

په اسانی سره لیدل کیږی چي اووم تعریف د پولینومو د جمع او ضرب عمومی قوانین دی چي د ښوونکی د وختو څخه ورسره آشنا یاست.

د اووم تعریف څخه مستقیماً استنباط کیږی چي:

1- د دوو پولینومو د جمع د حاصل طاقت د دواړو پولینومو تر لوی ترین طاقت لوړ ندی.

2- که د $f(x)$ او $g(x)$ پولینومونه د صفر څخه خلاف وی، نو د هغوی د ضرب د حاصل طاقت ښوونکی (طاقت نما) مساوی دی د دواړو پولینومو د طاقتو د جمع په حاصل سره.

په رشتیا هم، که $n=m$ او $a_n = -b_m$ وی، نو $a_n + b_m = 0$ کیږی او $\deg s(x) < n$ دی. همدا ډول که $a_n \neq 0$ او $b_m \neq 0$ وی، نو $a_n \cdot b_m \neq 0$ کیږی او $\deg h = n+m = \deg f + \deg g$ سره کیږی.

قضیه - د P پر فیله باندی د ټولو پولینومو سیټ $P[x]$ د پولینومو د جمع او ضرب د عملیو سره تبدیلی رینگ دی.

ثبوت - د $f(x)$ او $g(x)$ د پولینومو د جمع او ضرب تبدیلی خاصیتونه پر عددو باندی د جمع او ضرب د عملیو د تبدیلی خاصیتو څخه استنباط کیږی. پدی معنی چي:

$$(\forall k, 0 \leq k \leq m)(a_k + b_k = b_k + a_k) \wedge \left(\sum_{i+j=k} a_i b_j = \sum_{j+i=k} b_j a_i \right)$$

همدا ډول د پولینومو د جمع د عملیو اتحادی خاصیت مستقیماً د عددو د جمع د عملیو د اتحادی خاصیت څخه استنباط کیږی.

د $P[x]$ په سیټ کی صفری پولینوم، یعنی $0(x)$ ، د صفر د عنصر وظیفه سرته رسوی. په رشتیا هم د هر اختیاری پولینوم $f(x)$ دپاره $f(x) + 0(x) = f(x)$ سره کیږی. د هر اختیاری پولینوم $f(x)$ دپاره د هغه متضاد عنصر عبارت دی له:

$$f_1(x) = (-a_n)x^n + (-a_{n-1})x^{n-1} + \dots + (-a_1)x + (-a_0)$$

په رشتیا هم: $f(x) + f_1(x) = 0(x) = f_1(x) + f(x)$ دی.

د اتحادی خاصیت د ثبوت دپاره باید لاندنی حقیقت ته متوجه اوسو:

د ټولو $0 \leq k \leq n+m$ دپاره $c_k = \sum_{i+j=k} a_i b_j$ دی. پدی حالت کی د $[f(x).g(x)].p(x)$ د پولینوم د r -ام

طاقة ضریب پداسی حال کی چي $p(x) = d_1 x^1 + d_{l-1} x^{l-1} + \dots + d_1 x + d_0$ په وی ، په

$$\sum_{k+s=r} c_k d_s = \sum_{k+s=r} \left(\sum_{i+j=k} a_i b_j \right) d_s = \sum_{i+j+s=r} (a_i b_j) d_s$$

مساوی کیری.

که د $f(x)[g(x).p(x)]$ د پولینوم د r -ام طاقه ضریب وشمېرو ، نو لاندنی فارمول به لاسته راسی.

$$\sum_{i+t=r} a_i \left(\sum_{j+s=t} b_j d_s \right) = \sum_{i+j+s=r} a_i (b_j d_s)$$

څرنګه چي $\sum_{i+j+s=r} (a_i b_j) d_s = \sum_{i+j+s=r} a_i (b_j d_s)$ دی، نو ددواړو پولینومود r -ام طاقه ضریبونه یوډبله

سره مساوی دی. ځکه نو :

$$[f(x).g(x)].p(x) = f(x)[g(x).p(x)]$$

توزیعی قانون $[f(x)+g(x)].p(x) = f(x).p(x) + g(x).p(x)$ د لاندنی مساوات څخه په څرګند ډول استنباط کیری:

$$\sum_{i+j=k} (a_i + b_i) d_j = \sum_{i+j=k} a_i d_j + \sum_{i+j=k} b_i d_j$$

پدی ترتیب قضیه پوره ثابته سوه.

په نتیجه کی ویلای سو چي د پولینومو د جمع او ضرب د عملیو خاصیتونه ، هغو خاصیتو ته چي په یوه اختیاری رینګ کی صدق کوی ، ورته دی.

د پولینومو د جمع او ضرب دپاره د عینی نښو څخه " + " ، " - " کار اخلولګه د عددو د پاره . آلبته ددی کار په نتیجه کی سؤتفاهم منځ ته نه راځی.

څرنګه چي د P فیلډ کی د یو عدد وجود لری ، نو د پولینومو په سیټ $P[x]$ کی هم د یو عدد

$p(x)=1$ وجود لری. پدی معنی چي د هر طبیعی عدد د پاره

$$x^k = \underbrace{p(x).p(x).\dots.p(x)}_k \in P[x].$$

د $a_k x^k$ په څېر هره افاده د $P[x]$ په رینګ کی د پولینومو د حاصل ضرب په صفت مطالعه کولای

سو. د (1) افاده د مشابه پولینومو د هر حد د ضریبو د جمع د حاصل په صفت څپرل کیدای سی. علاوه پر دی د $P[x]$ د پولینومو په رینګ کی ددو پولینومو د تفریق حاصل هم څپر لای سو.

$$f(x) - g(x) = a_n x^n + \dots + a_{m+1} x^{m+1} + (a_m - b_m) x^m + \dots + (a_1 - b_1) x + (a_0 - b_0)$$

II§. د پولینومو څېړنه د تابع په څېر

په تېره برخه کې مو پولینومونه پر عددی فیلډ باندې د الجبري افادې په صفت تر مطالعې لاندې ونيول، خو داډول تعريف د انالایز دپاره مفید نه تمامیری. ځکه نو اوس به د پولینومو تابعي شکل په جزئیاتو سره مطالعه او د الجبري او انالیتیکي تعريفو د معادل والی مسئله به تر څېړنې لاندې ونیسو.

فرضوو چې P عددی فیلډ دی او $a_0, a_1, \dots, a_n \in P$ دی. اوس نو په P کې لاندې تعريف بیانوو:

تعريف ۱- د $f: P \rightarrow P$ مېپنگ چې د هر $x \in P$ دپاره د لاندني فارمول پذیرعه راگره سوی وی

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

د P پر فیلډ باندې د a_n, \dots, a_1, a_0 د ضریبو سره د x ديو مجهوله پولینوم په نامه یادیری.

که $a_n \neq 0$ وی، نو د $f(x)$ د پولینوم درجه n ده.

بیلگه ۱- $f(x) = 3x^4 + \sqrt{5}x + -1$ د حقیقي عددو \mathbb{R} پر فیلډ باندې پولینوم دی چې درجه ای څلور ده.

بیلگه ۲- $g(x) = ix^3 + (2 + 3i)x + (i - \sqrt{2})$ د مختلطو عددو \mathbb{C} پر فیلډ باندې پولینوم دی چې درجه ای درې ده.

پدې ډول پولینوم ته د یوې خاصی عددی تابع په سترگه گورو.

د حقیقي عددو \mathbb{R} پر فیلډ باندې د پولینومو ساده ترین شکل په خاص ډول خطي تابع یعنی

$$f(x) = ax + b \text{ او دوهمه درجه تابع یعنی } f(x) = ax^2 + bx + c \text{ دی چې په ښوونځي کې د هغوی د}$$

جزئیاتو سره آشنا سوی یاست. څرگنده ده چې د $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ پولینوم د الجبري

افادې په صفت د $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ پولینومی تابع جواب ورکونکی ده او برعکس پورتنی پولینومی تابع د ذکر سوی الجبري افادې جواب ورکونکی ده. ځکه نو د عددی تابع گانو دپاره هم د مساوی او د تابع گانو د حاصل جمع او حاصل ضرب مفهومونه تعريف کیدای سی چې دلته یې یادونه کوو.

عددی تابع گانې $g, f: P \rightarrow P$ یوازې او یوازې هغه وخت سره مساوی دی چې د ذکر سوی تابع گانو قیمتونه د تعريف د ساحې P د هر عنصر دپاره سره مساوی وی. د ریاضی په سمبولیکه ژبه یې داسی

$$f(x) = g(x) \Leftrightarrow (\forall \alpha \in P) (f(\alpha) = g(\alpha)) \text{ لیکو:}$$

د P پر فیلډ باندې د f او g د تابع گانو د جمع (ضرب) حاصل عبارت دی د $[t(x)] h(x)$ د تابع څخه پداسی ډول چې:

$$[(\forall \alpha \in P) (t(\alpha) = g(\alpha) \cdot f(\alpha))] ((\forall \alpha \in P) (h(\alpha) = g(\alpha) + f(\alpha)))$$

په حقیقت کې د تابع گانو د مساوات، جمع او ضرب پورتنی نوی تعريفونه یوازې او یوازې هغه وخت د مخکنیو تعريفو سره معادل دی که موږ د ذکر سوو تعريفو معادل والی د پولینومو د مساوات، جمع او ضرب د تعريفو سره چې په I§ ذکر سوو، ثابت کړای سوو.

فرضوو چي $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ او $b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ د P پر فيلډ باندی پولینومونه او $n \geq m$ دی. ذکر سوی پولینومونه په ترتیب سره د پولینومی تابع گانو

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \text{ او } g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

جواب ورکونکی دی. د $I \S$ څخه پوهیږو چي د ذکر سوو پولینومو د جمع حاصل د

$$a_n x^n + \dots + a_{m+1} x^{m+1} + (a_m + b_m) x^m + \dots + (a_1 + b_1) x + (a_0 + b_0)$$

پولینوم دی چي دهغه جواب ورکونکی پولینومی تابع

$$(\forall \alpha \in P) h(\alpha) = a_n \alpha^n + \dots + a_{m+1} \alpha^{m+1} + (a_m + b_m) \alpha^m + \dots + (a_1 + b_1) \alpha + (a_0 + b_0)$$

ده. خو د هر $\alpha \in P$ دپاره

$$h(\alpha) = (a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0) + (b_m \alpha^m + b_{m-1} \alpha^{m-1} + \dots + b_1 \alpha + b_0) = f(\alpha) + g(\alpha)$$

دی. پدی ترتیب $h(x) = f(x) + g(x)$ کیری، یعنی د پولینومو او د تابع گانو د جمع د حاصل مفهومونه سره مطابق دی. همدا ډول د راکړه سوی پولینومو د ضرب حاصل

$$\begin{aligned} (a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0) \cdot (b_m \alpha^m + b_{m-1} \alpha^{m-1} + \dots + b_1 \alpha + b_0) = \\ = a_n b_m x^{n+m} + \dots + (a_1 b_m + b_1 a_n) x + a_0 b_0 \end{aligned}$$

د $t(x) = f(x) \cdot g(x)$ د تابع جواب ورکونکی دی. پدی معنی چي دواړه مفهومونه بیا هم مطابقت سره لری. همدا ډول څرگنده ده چي که دوه پولینومونه یو ډبل سره مساوی وی، یعنی $n=m$ او $a_n = b_n, \dots, a_0 = b_0$ وی، نو د هغوی جواب ورکونکی تابع گانی $f(x)$ او $g(x)$ یو ډبل سره مطابق دی.

دپولینومو د مساوی والی مسأله پداسی حال کی چي د هغوی پولینومی تابع گانی $f(x)$ او $g(x)$ یوډبله سره مساوی وی، مغلط تره ده.

قضیه - که پولینومی عددی تابع گانی $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ او

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

د P د فیلیډ څخه د $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n, \alpha_{n+1} = 0$ ، مختلف قیمتونه داسی واخلی چي هغوی په

خپل منځ کی سره مساوی وی، نو هغه پولینومونه چي د پولینومی تابع گانو جواب ورکونکی دی،

یعنی $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ او $b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ هم په خپل منځ

کی سره مساوی دی، یعنی: $a_n = b_n, \dots, a_1 = b_1, a_0 = b_0, n = m$ دی.

په بله اصطلاح:

$$(\deg f(x), \deg g(x) \leq n) \wedge (\forall i, j / 1 \leq i, j \leq n+1) (\alpha_i \neq \alpha_j) \wedge$$

$$(\forall i / 1 \leq i \leq n \wedge \alpha_{n+1} = 0) (f(\alpha_i) = g(\alpha_i)) \rightarrow$$

$$(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) = (b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0)$$

ثبوت - فرضوو چي $\alpha_{n+1} = 0, \alpha_n, \dots, \alpha_3, \alpha_2, \alpha_1$ د فيلډ مختلف عددونه دي او د هر $1 \leq i \leq n+1$ دپاره $f(\alpha_i) = g(\alpha_i)$ دی.

د $f(0) = g(0)$ د مساوات څخه $a_0 = b_0$ استنباط کيږي. اوس به نو پاته n مساواتونه تر مطالعي لاندې ونيسو:

$$\begin{aligned} a_n \alpha_1^n + a_{n-1} \alpha_1^{n-1} + \dots + a_1 \alpha_1 + a_n &= b_m \alpha_1^m + b_{m-1} \alpha_1^{m-1} + \dots + b_1 \alpha_1 + b_n \\ a_n \alpha_2^n + a_{n-1} \alpha_2^{n-1} + \dots + a_1 \alpha_2 + a_n &= b_m \alpha_2^m + b_{m-1} \alpha_2^{m-1} + \dots + b_1 \alpha_2 + b_n \\ &\vdots \\ a_n \alpha_n^n + a_{n-1} \alpha_n^{n-1} + \dots + a_1 \alpha_n + a_n &= b_m \alpha_n^m + b_{m-1} \alpha_n^{m-1} + \dots + b_1 \alpha_n + b_n \end{aligned}$$

که د پورتنی مساوات ټوله اجزای د مساوات کيږي لاس ته راوړوو ، نو

$$\begin{aligned} a_n \alpha_1^n + \dots + (a_m - b_m) \alpha_1^m + \dots + (a_1 - b_1) \alpha_1 &= 0 \\ a_n \alpha_2^n + \dots + (a_m - b_m) \alpha_2^m + \dots + (a_1 - b_1) \alpha_2 &= 0 \\ &\vdots \\ a_n \alpha_n^n + \dots + (a_m - b_m) \alpha_n^m + \dots + (a_1 - b_1) \alpha_n &= 0 \end{aligned}$$

معادلي به لاسته راسی. په ترتیب سره لمړی معادله پر α_1 ، دوهمه معادله پر α_2 او همدا ډول تر n -مې معادلي پوري مخته ځو او n -مې معادله پر α_n باندې وپشو، څو لاندني معادلي لاسته راسی:

$$\begin{aligned} a_n \alpha_1^{n-1} + \dots + (a_m - b_m) \alpha_1^{m-1} + \dots + (a_2 - b_2) \alpha_1 + (a_1 - b_1) &= 0 \\ a_n \alpha_2^{n-1} + \dots + (a_m - b_m) \alpha_2^{m-1} + \dots + (a_2 - b_2) \alpha_2 + (a_1 - b_1) &= 0 \\ &\vdots \\ a_n \alpha_n^{n-1} + \dots + (a_m - b_m) \alpha_n^{m-1} + \dots + (a_2 - b_2) \alpha_n + (a_1 - b_1) &= 0 \end{aligned}$$

پورتنی معادلي بڼي چي د $a_1 - b_1, (a_2 - b_2), \dots, (a_m - b_m), \dots, a_n$ عددونه دلاندني n مجهوله n خطي معادلو د متجانس سيستم حل دی.

$$\begin{cases} y_1 \alpha_1^{n-1} + \dots + y_m \alpha_1^{m-1} + \dots + y_{n-1} \alpha_1 + y_n = 0 \\ y_1 \alpha_2^{n-1} + \dots + y_m \alpha_2^{m-1} + \dots + y_{n-1} \alpha_2 + y_n = 0 \\ \vdots \\ y_1 \alpha_n^{n-1} + \dots + y_m \alpha_n^{m-1} + \dots + y_{n-1} \alpha_n + y_n = 0 \end{cases} \quad \dots(1)$$

د پورتنی سيستم د اصلي ماترکس ديترمنانت به لاندني شکل ولری:

$$\begin{vmatrix} \alpha_1^{n-1} & \dots & \alpha_1 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_2^{n-1} & \dots & \alpha_2 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_n^{n-1} & \dots & \alpha_n & 1 \end{vmatrix}$$

پورتنی دیترمنانت د واندروموند Vandermond د دیترمنانت په نامه یادیری چې $\Delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$

فارمول پذیرعه شمېرل کیږی. (پورتنی فارمول د استقراء په متود ثابتیدلای سی، چې د تمرین په شکل یی توصیه کوم.)

څرنگه چې د $\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n$ قیمتونه مختلف دی، نو $\Delta \neq 0$ ده. ځکه نو د کرامر د فارمول له مخی (لمری برخه، څلرم فصل، § XII وگوری) پورتنی (1) سیستم یوازی د صفری حل خاوند دی، پدی معنی چې $a_1 - b_1 = 0, a_2 - b_2 = 0, \dots, a_m - b_m = 0$ او $a_n = 0$ دی. پدی ترتیب قضیه په ثبوت ورسیده.

نتیجه ۱- که د $f(x)$ او $g(x)$ پولینومی تابع گانی د اختیاری درجی سره یو دبله سره مساوی وی، نو هغه پولینومونه چې په ترتیب سره د هغوی جوابگوی دی هم یو دبل سره منطبق دی. پورتنی نتیجه د ثابتی سوی قضیې او لاندنی حقیقت د موجودیت څخه استنباط کیږی.

هر عددی فیلد د لاینهای عنصرونه لری!

پدی ترتیب پر اختیاری عددی فیلد P باندی د پولینومو دواړه تعریفونه (الجبری او انالیتیکی) سره معادل دی. ځکه نو اجازه لرو چې ددواړو تعریفو څخه کار واخلو، پاته دی نه وی چې که P عددی فیلد نه وی نو دغه معادلیت صدق نه کوی.

کله کله د مسئلو د حل په ترڅ کی د داسی تابع گانو مخامخ کیږو چې د جدول په ذریعه راکړه سوی وی. په حقیقت کی که څوک ددغه ډول مسئلې سره مخامخ سی، نو غواړی چې د جدول پذیرعه راکړه سوی تابع د فارمول په واسطه ارائه کړی. د ثبوت سوی قضیې څخه یوه بله نتیجه هم استنباط کیدای سی چې نوموړی پر ابلم حلوی.

نتیجه ۲- د هر طبیعی عدد n دپاره یوازنی د $f(x)$ پولینوم وجود لری چې د هغه درجه به تر n اضافه نه وی او د $\beta_1, \beta_2, \dots, \beta_{n+1}$ د مخکی له مخکی راکړه سوو قیمتونه د x د مجهول په عوض کی د راکړه سوی قیمتو $\alpha_1, \alpha_2, \dots, \alpha_{n+1}$ د وضع کیدو په نتیجه کی اخلی.

کله چې د پولینوم د موجودیت په هکله رغیږو، نو باید هغه ډول پولینوم ترتیب کړو. په حقیقت کی زموږ پر شرطو برابر پولینوم لاندی شکل لری:

$$f(x) = \beta_1 \frac{(x - \alpha_2)(x - \alpha_3) \dots (x - \alpha_{n+1})}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \dots (\alpha_1 - \alpha_{n+1})} + \beta_2 \frac{(x - \alpha_1)(x - \alpha_3) \dots (x - \alpha_{n+1})}{(\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3) \dots (\alpha_2 - \alpha_{n+1})} + \dots + \beta_{n+1} \frac{(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)}{(\alpha_{n+1} - \alpha_1)(\alpha_{n+1} - \alpha_2) \dots (\alpha_{n+1} - \alpha_n)}$$

دلته $f(\alpha_{n+1}) = \beta_{n+1}, \dots, f(\alpha_2) = \beta_2, f(\alpha_1) = \beta_1$ سره کیری او د پولینوم درجه هم تر n اضافه نده. پورتنی پولینوم د لاگرانژ د انترپولیشن Lagrange Interpolation په نامه یادیری. د پولینوم یکر توب د ثابتی سوی قضیې څخه استنباط کیری.

§III. د پولینومو نامکمل وپش

ددی کتاب په دوهم فصل کی مو د تامو عددو رینگ په جزئیاتو سره وڅیری. د P پر فیله باندی د x د متحول سره د ټولو پولینومو رینگ $P[x]$ د تامو عددو رینگ ته ورته خاصیتونه لری. لمړی به هغه خاصیتونه مطالعه کړو چي پر اختیاری فیله باندی د پولینومو د رینگو دپاره مشترک دی. فرضوو چي $f(x)$ او $g(x)$ د $P[x]$ د رینگ پولینومونه دی. پداسی ډول چي $g(x)$ د صفری پولینوم څخه خلاف وی.

تعریف - د $f(x)$ پولینوم د $g(x)$ پر پولینوم باندی نامکمل وپشل کیری که د $P[x]$ په رینگ کی د $s(x)$ او $r(x)$ پولینومونه داسی وجود ولری چي :

1. $f(x) = g(x) \cdot s(x) + r(x)$
2. $\deg r < \deg g \quad \vee \quad r(x) = 0$

پدی حالت کی د $f(x)$ پولینوم د مقسوم، د $g(x)$ پولینوم د مقسوم علیه، د $s(x)$ پولینوم د خارج قسمت او د $r(x)$ پولینوم د باقی په نامه یادیری.

بیلگه ۱ - فرضوو چي $f(x) = x^3 - 3x + 1$ او $g(x) = x^2 + 1$ دی.

د $x^3 - 3x + 1 = (x^2 + 1)x + (-4x + 1)$ د مساوات څخه څرگندیږی، چي د $f(x)$ پولینوم د $g(x)$ پر پولینوم نامکمل وپشل سوی دی. پدی وپش کی یی خارج قسمت د $s(x) = x$ او باقی یی د $r(x) = -4x + 1$ پولینوم دی.

بیلگه ۲ - که د $f(x) = x^3 - 8$ پولینوم د $g(x) = x - 2$ پر پولینوم نامکمل ووپشو، نو $f(x) = g(x)(x^2 + 2x + 4)$ به وی. پدی حالت کی د وپش د عملیې خارج قسمت $s(x) = x^2 + 2x + 4$ او باقی یی $r(x) = 0$ دی.

د دوهم فصل په §II کی مو ولیدل چي هر نام عدد پر یو بل اختیاری نام عدد چي د صفر څخه خلاف وی، په نامکمل ډول وپشلای سو. اوس به وښیو چي د $P[x]$ په رینگ کی ورته (مشابه) خاصیت صدق کوی.

قضیه - د $P[x]$ د رینگ هر پولینوم $f(x)$ د نوموړی رینگ پر اختیاری پولینوم چي د صفر څخه خلاف وی ، نامکمل وپشلاى سو ، پداسی ډول چي د نامکمل وپش په نتیجه کی لاسته راغلی خارج قسمت او باقی د $P[x]$ په رینگ کی یکر (بی ساری) دی.

ثبوت - فرضوو چي د

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

پولینومونه په معیاری بڼه راکړه سوی وی، یعنی $a_n \neq 0$ او $b_m \neq 0$ دی او $n \geq m$ دی.

د $f(x)$ د پولینوم نامکمل وپش د $g(x)$ پر پولینوم باندی نظر د $f(x)$ و درجی، یعنی n ، ته د ریاضی د استقراء د متود څخه په استفادی سره په ثبوت رسوو. په لمړی گام کی د $n=0$ سره شروع کوو.

که $n=0$ وی ، نو $m=0$ دی ، $f(x)=a_0$ او $g(x)=b_0 \neq 0$ ، ځکه نو $s(x) = \frac{a_0}{b_0}$ او $r(x)=0$ دی. پدی

معنی چي د نامکمل وپش عملیه ممکنه ده.

اوس نو فرضوو چي زموږ قضیه د ټولو پولینومو دپاره چي درجه ای تر n کښته وی ، صدق کوی. لاندنی پولینوم به وڅېرو:

$$\begin{aligned} p(x) &= f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = \\ &= a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 - a_n x^n - \frac{a_n b_{m-1}}{b_m} x^{n-1} - \dots - \frac{a_n b_1}{b_m} x - \frac{a_n b_0}{b_m} = \\ &= \left(a_{n-1} - \frac{a_n b_{m-1}}{b_m} \right) x^{n-1} + \dots + \left(a_1 - \frac{a_n b_1}{b_m} \right) x + \left(a_0 - \frac{a_n b_0}{b_m} \right) \end{aligned}$$

څرنگه چي د $\deg p < n$ ده، د استقراء د فرضیې پر اساس د $p(x)$ پولینوم د $g(x)$ پر پولینوم نامکمل وپشل کیدای سی. پدی معنی چي د $s_1(x)$ او $r_1(x)$ پولینومونه داسی وجود لری چي $p(x) = g(x) \cdot s_1(x) + r_1(x)$ کیزی، پداسی ډول چي $r_1(x) = 0$ یا $\deg r_1(x) < \deg g(x)$ ده.

ددی ځایه :

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = g(x) s_1(x) + r_1(x)$$

او

$$f(x) = \left(\frac{a_n}{b_m} x^{n-m} + s_1(x) \right) g(x) + r_1(x)$$

ځکه نو :

پداسی ډول چي یا $r_1(x) = 0$ یا $\deg r_1(x) < \deg g(x)$ ده. په نتیجه کی د استقراء د پرنسیب له مخی

زموږ قضيه د ټولو پولينومو دپاره چې درجه ای n او د f(x) او g(x) پولينومو دپاره چې
 $\deg f(x) \geq \deg g(x)$ وی . حقيقت لری .

که $f(x)=0$ او $g(x) \neq 0$ وی ، نو $s(x)=r(x)=0$ کیری .

که $\deg f(x) < \deg g(x)$ وی ، نو $f(x)=g(x) \cdot 0 + f(x)$ کیری ، يعنی $s(x)=0$ او $r(x)=f(x)$ دی .

پدی ډول مو د f(x) د پولينوم نامکمل وېش د عمليې د اجراء امکان د $g(x) \neq 0$ پر پولينوم په ثبوت ورساوه . اوس به نو د s(x) او r(x) يکر توب په ثبوت ورسوو .

ددی موخي د لاسته راوړو دپاره فرضوو چې د نامکمل وېش په نتیجه کې دوه خارج قسمته او دوه باقی لاسته راځی ، يعنی :

$$f(x) = g(x) \cdot s_1(x) + r_1(x) \quad ; \quad \deg r_1(x) < \deg g(x)$$

$$f(x) = g(x) \cdot s_2(x) + r_2(x) \quad ; \quad \deg r_2(x) < \deg g(x)$$

$$g(x) \cdot s_1(x) + r_1(x) = g(x) \cdot s_2(x) + r_2(x)$$

$$g(x)(s_1(x) - s_2(x)) = r_2(x) - r_1(x)$$

د وروستي مساوات د بني خوا درجه د g(x) تر درجې لږ ده په عين حال کې ، په هغه صورت کې چې $s_1(x) - s_2(x) \neq 0$ وی ، بايد د کينی خوا د پولينوم درجه د g(x) تر درجې لوړه وی ، ځکه نو بايد د

$$s_1(x) - s_2(x) = 0$$
 مساوات صدق وکړی . پدی معنی چې $s_1(x) = s_2(x)$ بايد حقيقت ولری . ددی

$$\text{حقيقت پر بنسټ } r_2(x) - r_1(x) = 0 \text{ دی او } r_2(x) = r_1(x) \text{ دی .}$$

پدی ډول مو ثابتته کړه چې که د نامکمل وېش په نتیجه کې دوه خارج قسمته او دوه باقی لاسته راځی ، نو هغوی به په خپل منځ کې مساوی وی .

د f(x) او g(x) د پولينومو د نامکمل وېش د خارج قسمت s(x) او د باقی r(x) شمېرنه په مختلفو طريقو باندی صورت نیسی . د هغو طريقو څخه ديوې طريقه مفکوره د تېری قضیې په ثبوت کې نغښتی ده چې په لاندی ډول به یې تشریح کړو :

لمړی بايد د $p(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$ پولينوم پداسی ډول اعمار کړو چې $\deg p < \deg g$ وی .

پدی صورت کې $s(x) = \frac{a_n}{b_m} x^{n-m}$ او $r(x) = p(x)$ دی . که $\deg p \geq \deg g$ وی ، نو د p(x) او g(x) د

پولينومو دپاره د $p_1(x) = p(x) - \frac{c_k}{b_m} x^{k-m} g(x)$ پولينوم داسی شمېرو چې c_k د $p_1(x)$ د پولينوم

لوی ترين ضريب دی . که $\deg p_1 < \deg p$ وی ، نو

$$f(x) = \left(\frac{a_n}{b_m} x^{n-m} + \frac{c_k}{b_m} x^{k-m} \right) g(x) + p_1(x)$$

$$s(x) = \frac{a_n}{b_m} x^{n-m} + \frac{c_k}{b_m} x^{k-m} \text{ او } r(x) = p_1(x) \text{ کیری .}$$

که $dcgp_1 \geq dcgp$ وی ، نو پورتنی پروسه بیا تکرارؤ .

بنه به داوی چي دغه پروسه دلاندنی شیمایه بنه مشاهده کرو: ³

$$\begin{array}{r}
 f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \\
 \frac{a_n}{b_m} x^{n-m} g(x) = a_n x^n + \frac{a_n b_{m-1}}{b_m} x^{n-1} + \dots + \frac{a_n b_0}{b_m} x^{m-n} \\
 \hline
 p(x) = c_k x^k + \dots + c_1 x + c_0 \\
 \frac{c_k}{b_m} x^{k-m} g(x) = c_k x^k + \dots + \frac{c_k b_0}{b_m} x^{k-m} \\
 \hline
 p_1(x) = \dots \\
 \vdots \\
 \hline
 r(x)
 \end{array}
 \quad \left| \quad \begin{array}{l}
 g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0 \\
 \frac{a_n}{b_m} x^{n-m} + \frac{c_k}{b_m} x^{k-m} + \dots = s(x)
 \end{array}
 \right.$$

پورتنی طریقہ به پر مشخصه بیلگه باندی عملی کرو. فرضوو چي $f(x) = 4x^4 + 3x^3 - 2x + 1$ او $g(x) = x^2 + 2$ دی ، نو د قائمی زاویي دوپششیمایه داسی بنکاری:

$$\begin{array}{r}
 4x^4 + 3x^3 - 2x + 1 \\
 \underline{-4x^4 \pm 8x^2} \\
 3x^3 - 8x^2 - 2x + 1 \\
 \underline{-3x^3 \pm 6x} \\
 -8x^2 - 2x + 1 \\
 \underline{\mp 8x^2 \mp 16} \\
 -8x + 17
 \end{array}
 \quad \left| \quad \begin{array}{l}
 x^2 + 2 \\
 \hline
 4x^2 + 3x - 8
 \end{array}
 \right.$$

پدی ترتیب د $f(x)$ د پولینوم د نا مکمل وپش په نتیجه کی د $g(x)$ پر پولینوم باندی د $s(x) = 4x^2 + 3x - 8$ خارج قسمت او $r(x) = -8x + 17$ باقی لاسته راغلل.

همدا راز د خارج قسمت او باقی محاسبه د نا معینو ضربوو د طریقہ څخه په استفادہ سره لاسته راوړلای سو. پر پورتنی بیلگي باندی به دا طریقہ واضح کرو.

د ثابت سوی قضیي څخه پوهیرو چي د $s(x)$ او $r(x)$ داسی پولینومونه وجود لری چي

$$4x^4 + 3x^3 - 2x + 1 = (x^2 + 2)s(x) + r(x)$$

³ ذکر سوی شیمایه کله د قائمی زاویي په شکل د وپش په نامه یادیری

کیری . دلته لیدل کیری چي $\text{deg } s(x) \leq 2$ او $\text{deg } r(x) < 2$ باید وی ، یعنی :

په $P \mid a_2, a_1, a_0, b_1, b_0$ چي پداسی حال کي دی . $r(x) = b_1x + b_0$ او $s(x) = a_2x^2 + a_1x + a_0$ فیله کی نامعلومه عددونه دی. خکه نو :

$$4x^4 + 3x^3 - 2x + 1 = (x^2 + 2)(a_2x^2 + a_1x + a_0) + (b_1x + b_0)$$

$$4x^4 + 3x^3 - 2x + 1 = a_2x^4 + a_1x^3 + (a_0 + 2a_2)x^2 + (2a_1 + b_1)x + (a_0 + b_0)$$

د پولینومو د مساوات د تعریف (§I وگوری) پر اساس په وروستی مساوات کی باید په دواړو خواوکی د طاقتو ضریبونه یو دبل په مخامخ کی سره مساوی وی ، پدی معنی چي د معادلانو لاندنی سیستم لاسته راخی:

$$\begin{cases} a_2 = 4 \\ a_1 = 3 \\ a_0 + 2a_2 = 0 \\ 2a_1 + b_1 = -2 \\ 2a_0 + b_0 = 1 \end{cases} \rightarrow \begin{cases} a_2 = 4 \\ a_1 = 3 \\ a_0 = -8 \\ b_1 = -8 \\ b_0 = 17 \end{cases}$$

پدی ترتیب $s(x) = 4x^2 + 3x - 8$ او $r(x) = -8x + 17$ دی.

دواړی طریقې خپل مثبت او منفی اړخونه لری. د طریقې گتورتوب په مشخصی بیلگی پوری تړلی دی.

IV§. د پولینومو وپش د $g(x) = x - a$ پر باینوم (دوه حدیزه) باندی

کله کله د ځینو مسئلو د حل په وخت کی ضرورت پیدا کیری چي راگره سوی پولینوم پر یوه $g(x) = x - a$ دوه حدیزه یا باینوم باندی وپشو. څرگنده ده چي دغه عملیه لکه چي په §III کی تشریح سوه ، سرته ورسوو، خو ددی مسئلی د حل دپاره یوه اسانه طریقه هم وجود لری چي پدی برخه کی به یې طرح کړو.

فرضوو چي $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ او $g(x) = x - a$ وی ، نو هغه خارج قسمت $s(x)$ چي د $f(x)$ د وپش په نتیجه کی پر $g(x)$ باندی لاسته راخی باید داسی پولینوم وی چي درجه یې $n-1$ او باقی یې $r(x)$ باید یا صفری پولینوم وی او یا درجه یې مساوی په صفر وی. پدی معنی چي د P د فیله عدد دی او په r سره یې بنیو.

د $s(x)$ او r د شمېرنی د پاره د نامعینو ضریبو د طریقې څخه کار اخلو.

$$a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - a)(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \dots + b_1x + b_0) + r$$

یا

$$a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = b_{r-}x^n + (b_{n-2} - ab_{n-1})x^{n-1} + (b_{r-3} - ab_{n-2})x^{n-2} + \dots + (b_0 - ab_1)x + (r - ab_0)$$

د پولینومو د مساوی والی د تعریف پر اساس لاندنی سیستم لاسته راځی:

$$\begin{cases} a_n = b_{n-1} \\ a_{n-1} = b_{n-2} - ab_{n-1} \\ a_{n-2} = b_{n-3} - ab_{n-2} \\ \vdots \\ a_1 = b_0 - ab_1 \\ a_0 = r - ab_0 \end{cases}$$

خکه نو:

$$\begin{cases} b_{n-1} = a_n \\ b_{n-2} = a_{n-1} + ab_{n-1} \\ b_{n-3} = a_{n-2} + ab_{n-2} \\ \vdots \\ b_0 = a_1 + ab_1 \\ r = a_0 + ab_0 \end{cases}$$

وروستی سیستم د خارج قسمت $s(x)$ باقی r د شمېرنی د پاره په آسانی سره په لاندنی جدول کی ایږدو.

| | | | | | | |
|-----|-----------|----------------------|----------------------|---------|--------------|--------------|
| | a_n | a_{n-1} | a_{n-2} | \dots | a_1 | a_0 |
| a | a_n | $ab_{n-1} + a_{n-1}$ | $ab_{n-2} + a_{n-2}$ | \dots | $ab_1 + a_1$ | $ab_0 + a_0$ |
| | b_{n-1} | b_{n-2} | b_{n-3} | | b_0 | r |

جدول ۱۲

پورتنی جدول د هورنر Horner د شیما په نامه یادیری . ددی شیما په لمړی کرښه کی د $f(x)$ د پولینوم ضریبونه ځای پر ځای سوی دی او په دوهمه کرښه کی د a عدد ، د $s(x)$ د ضریبوشمېرنه او د r عدد ځای پر ځای سوی دی.

دپورتنی شیما پر اساس د خارج قسمت هر ضریب b_{k-1} (د b_{n-2} څخه شروع) او باقی r او a د b_k د حاصل ضرب او د a_k د حاصل جمع (یعنی $ab_k + a_k$) په نتیجه کی لاسته راځی.

بیلگه ۱- د $f(x) = x^4 - 2x^3 + 6x^2 - x + 1$ پولینوم د $g(x) = x - 1$ پر باینوم باندی د هورنر د شیما پر اساس ویشو.

جدول ۱۳

| | | | | | |
|---|---|----|---|----|---|
| | 1 | -2 | 6 | -1 | 1 |
| 1 | 1 | -1 | 5 | 4 | 5 |

د پورتنی جدول له مخی $s(x) = x^3 - x^2 + 5x + 4$ او $r=5$ دی. د هورنر شیمما هغه وخت ډیره کتوره تمامیری چي دلاسته راوړی خارج قسمت وېش بیا هم پر باینوم باندی په نظر کی وی . پدغه حالت کی د ضربیو و لیکلو ته حاجت نسته ، ځکه چي دپوش د لمړی پروسه په پای ته رسیدو سره دپوش دوهمه پروسه شروع کیږی. پدغه ډول د $f(x)$ د پولینوم تجزیه د $x-a$ په طاقتو باندی په انالایز او الجبر کی حلیری.

تعریف - د n درجه ای پولینوم $f(x)$ اړانه د

$$f(x) = c_n(x-a)^n + c_{n-1}(x-a)^{n-1} + \dots + c_2(x-a)^2 + c_1(x-a) + c_0$$

په شکل د $f(x)$ د پولینوم تجزیه د $x-a$ په طاقتو باندی یادیری.

ددی دپاره چي د $f(x)$ پولینوم د $x-a$ په طاقتو باندی تجزیه کړو ، باید د $c_n, c_{n-1}, \dots, c_2, c_1, c_0$ ضریبونه پیدا کړو.

$$f(x) = (x-a)[c_n(x-a)^{n-1} + c_{n-1}(x-a)^{n-2} + \dots + c_2(x-a) + c_1] + c_0$$

پدی معنی چي c_0 عبارت دی له هغه باقی څخه چي د $f(x)$ د پولینوم دپوش په نتیجه کی د $g(x) = x-a$ پر پولینوم باندی لاسته راځي. c_1 عبارت دی د لاسته راغلي خارج قسمت دپوش څخه د $g(x) = x-a$ پر پولینوم باندی ، یعنی:

$$s(x) = c_n(x-a)^{n-1} + c_{n-1}(x-a)^{n-2} + \dots + c_2(x-a) + c_1$$

په همدا ډول د c_n, \dots, c_3, c_2 ضریبونه محاسبه کولای سو.

بیلگه ۲ - د $x+1$ په درجو باندی د $f(x) = x^5 - 3x^3 + x^2 - 2x + 1$ د پولینوم تجزیه پیدا کړو.

حل - زمور د غوښتنی ضریبونه د هورنر د شیمما څخه به استفادی سره پیدا کړو.

| | | | | | | |
|----|---|----|----|---|----|---|
| | 1 | 0 | -3 | 1 | -2 | 1 |
| -1 | 1 | -1 | -2 | 3 | -5 | 6 |
| -1 | 1 | -2 | 0 | 3 | -8 | |
| -1 | 1 | -3 | 3 | 0 | | |
| -1 | 1 | -4 | 7 | | | |
| -1 | 1 | -5 | | | | |
| -1 | 1 | | | | | |

پدی ترتیب لاسته راغلی تجزیه لاندنی شکل لری.

$$f(x) = (x+1)^5 - 5(x+1)^4 + 7(x+1)^3 - 8(x+1) + 6$$

§۷. د پولینومو د وپش ورتوب

څه ډول چې د تامو عددو په څېړنه کې د عددو د وپش د ورتوب اړیکه مهم رول لوبوی همدی ته ورته د پولینومو په مطالعه کې هم د وپش د ورتوب اړیکه مهم رول لوبوی .

فرضوو چې $f(x), g(x) \in P[x]$ ، P د عددی فیلیډو څخه یو فیلیډ او د $g(x)$ پولینوم خلاف د صفر دی.

تعریف ۱- د $P[x]$ په رینګ کې د $f(x)$ پولینوم د $g(x)$ پر پولینوم په هغه صورت کې د وپش وړ دی چې د $s(x) \in P[x]$ پولینوم داسی وجود ولری چې $f(x) = g(x) \cdot s(x)$ وی.

بیلګه ۱- د $f(x) = (x^2+1)(x-3)$ پولینوم د $g(x) = x^2+1$ پر پولینوم د وپش وړ دی ، ځکه چې $s(x) = x-3$ دی.

بیلګه ۲- د $f(x) = x^2+2x+1$ پولینوم د $g(x) = x+1$ پر پولینوم د وپش وړ دی ، ځکه چې $s(x) = x+1$ دی.

د $f(x)$ د وپش ورتوب د $g(x)$ پر پولینوم باندی ، لکه د عددونو په تیوری کې ، د $f(x):g(x)$ په ذریعه بڼیو . پدی معنی چې د پولینومو د وپش اړیکه هم " : " پذیرعه بڼیو . د $f(x):g(x)$ په حالت کې وایو چې د $g(x)$ پولینوم د $f(x)$ پولینوم وپشی . څرګنده ده چې د $s(x)$ پولینوم هم د $f(x)$ پولینوم وپشی .

د وپش د ورتوب اړیکه داسی هم تعریفولای سو:

تعریف ۲- د $P[x]$ په رینګ کې د $f(x)$ پولینوم د $g(x)$ پر پولینوم په هغه صورت کې د وپش وړ دی ، که پر $g(x)$ باندی د $f(x)$ د پولینوم د وپش په نتیجه کې باقی یی صفر وی.

په § III کې مو د پولینومو د وپش طریقې تشریح کړی . د نوموړی طریقې څخه پر یوه پولینوم باندی د بل پولینوم د وپش د ورتوب په موندلو کې هم کار اخیستلای سو .

د پولینومو د وپش د ورتوب اړیکه لاندنی خاصیتونه لری چې هغوی زموږ په وروسته څېړنه کې د پولینومو په هکله ډیر مهم رول لوبوی.

۱- د وپش د ورتوب اړیکه انتقالی خاصیت لری پدی معنی که د $f(x)$ پولینوم د $g(x)$ پر پولینوم د وپش وړ وی او د $g(x)$ پولینوم د $h(x)$ پر پولینوم د وپش وړ وی ، نو د $f(x)$ پولینوم د $h(x)$ پر پولینوم د وپش وړ دی.

په رشتیا هم ، د راکره سوی شرط پر اساس $f(x) = g(x) \cdot s(x)$ او $g(x) = h(x) \cdot t(x)$ کیری ، ځکه نو $f(x) = h(x) [t(x) \cdot s(x)]$ دی.

په همدی ډول لاندنی خاصیتونه آزمویلای سو:

۲- که د $f(x)$ او $h(x)$ پولینومونه د $g(x)$ پر پولینوم دوش وړ وی ، نو د هغوی حاصل جمع $f(x)+h(x)$ او د هغوی د حاصل تفریق $f(x)-h(x)$ هم پر $g(x)$ دوش وړدی.

۳- که د $f(x)$ پولینوم د $g(x)$ پر پولینوم دوش وړ وی، نو د $f(x)$ د پولینوم د ضرب حاصل د یوه اختیاری پولینوم $h(x)$ سره هم د $g(x)$ پر پولینوم دوش وړدی.

۴- که هر یو د $f_1(x), f_2(x), \dots, f_k(x)$ پولینومو څخه د $g(x)$ پر پولینوم دوش وړ وی ، نو د $s_1(x), s_2(x), \dots, s_k(x)$ اختیاری پولینومو دپاره د

$$f_k(x) \cdot s_k(x) + \dots + f_2(x) \cdot s_2(x) + f_1(x) \cdot s_1(x)$$

پولینوم هم د $g(x)$ پر پولینوم دوش وړدی.

۵- د $f(x)$ هر پولینوم پر اختیاری پولینوم باندی چي درجه یې صفر وی ، دوش وړ دی.

په رشتیا هم ، که $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ او c د صفر څخه خلاف اختیاری عدد وی ، یعنی د صفر درجی پولینوم وی ، نو $f(x) = c \left(\frac{a_n}{c} x^n + \frac{a_{n-1}}{c} x^{n-1} + \dots + \frac{a_1}{c} x + \frac{a_0}{c} \right)$ دی.

۶- که د $f(x)$ پولینوم د $g(x)$ پر پولینوم دوش وړ وی ، نو د اختیاری عدد $c \in P$ ، چي خلاف د صفر وی ، دپاره د $f(x)$ پولینوم د $cg(x)$ پر پولینوم دوش وړدی.

په رشتیا هم د $f(x) = g(x) \cdot s(x)$ مساوات د $f(x) = [c \cdot g(x)] \cdot \left[\frac{1}{c} s(x) \right]$ د مساوات سره معادل دی.

۷- که $f(x):g(x)$ وی او $g(x):f(x)$ وی ، نو د صفر څخه خلاف د c عدد داسی وجود لری چي $f(x) = c \cdot g(x)$ سره دی.

د $f(x):g(x)$ استنباط کیری چي $f(x) = g(x) \cdot s(x)$ او $\deg g(x) \leq \deg f(x)$ دی. همدا ډول د $g(x):f(x)$ استنباط کیری چي $\deg f(x) \leq \deg g(x)$ دی. پدی معنی چي $\deg g(x) = \deg f(x)$ او $\deg s(x) = 0$ دی. یعنی $s(x) = c \in P$ او $c \neq 0$ دی. پدی ترتیب $f(x) = c \cdot g(x)$ دی.

§VI. د پولینومو لوی ترین مشترک وېشونکی او د اقلیدس الگوریتم

لکه څنگه چي ددوهم فصل په §III کی مو ولیدل ، د عددو لوی ترین مشترک وېشونکی مو په دوو طریقو تعریف کی.

۱- د (a,b) عدد د a او b د عددو د لوی ترین مشترک وېشونکی په نامه یادیږی ، که (a,b) عدد د مطلقه قیمت له مخی د a او b د عددو تر ټولو مشترکو طبیعی وېشونکو لوی وی.

۲- د (a,b) عدد د a او b د عددو د لوی ترین مشترک وېشونکی په نامه یادیږی ، که د (a,b) عدد د a او b د عددو مشترک طبیعی وېشونکی وی او د نوموړو عددو پر هر مشترک وېشونکی δ دوش وړ وی.

په لمړۍ تعريف كې د مشترك وېشونكې د مفهوم څخه د كميتو د پرتلې په اړه كار اخيستل سوي دي ، خو په دوهم تعريف كې يوازي د دوېش د وړ توب دارېكي څخه كار اخيستل سوي دي.

تام عددونه په هر اختياري عددي فيلډ P كې شامل دي. پدې معنی چي $\mathbb{Z} \subset P[x]$ دی ، يا په بله اصطلاح هر تام عدد يو پولينوم دی. څرگنده ده چي د پولينومو د لوی ترين مشترك وېشونكې تعريف بايد د عددو په اړه د هغوی د تعريف سره معادل وي ، خو پولينومونه د هغوی د طاقت نما په ارتباط مقایسه كولاى سو او عددونه هغه پولينومونه دي چي د هغوی طاقت نما مساوی په صفر سره ده. ځكه نو ښه به وي چي د پولينومو د لوی ترين مشترك وېشونكې مفهوم د پولينومو د پرتلې څخه پرته فورمولبندي كړو.

فرضوو چي $f(x), g(x)$ او $d(x) \mid P$ پر عددي فيلډ باندې پولينومونه دي.

تعريف - د $d(x)$ پولينوم د $f(x)$ او $g(x)$ د پولينومو د لوی ترين مشترك وېشونكې په نامه يادېږي ، كه لاندني شرطونه صدق وكړي.

1- $f(x):d(x)$ او $g(x):d(x)$ وي ، يعنی د $d(x)$ پولينوم د $f(x)$ او $g(x)$ د پولينومو مشترك وېشونكې وي.

2- د $d(x)$ پولينوم د $f(x)$ او $g(x)$ د پولينومو پر هر مشترك وېشونكې باندې دوېش وړ وي.

د پولينومو د لوی ترين مشترك وېشونكې د څرگندولو دپاره د عين سمبول څخه لكه د عددو دپاره كار اخلو ، پدې معنی چي د $f(x)$ او $g(x)$ د پولينومولوی ترين مشترك وېشونكې په $(f(x), g(x))$ سره ښيو.

پورتنۍ تعريف د $f(x)$ او $g(x)$ اختياري پولينومو د لوی ترين كډ وېشونكې د موجوديت سوال ته جواب نه وايي ، همدا ډول د پولينومو دوېش د وړتوب د خاصيتو پر اساس ($V \& \S$ وگورئ) كه لوی ترين مشترك وېشونكې (كه موجود هم وي!) ، نو په پكړه توگه نسي تعيندلای. په حقيقت كې كه $d(x) = (f(x), g(x))$ وي ، نو د هر $c \neq 0 \in P$ دپاره $c \cdot d(x)$ هم د $f(x)$ او $g(x)$ د پولينومولوی ترين مشترك وېشونكې دي. ځكه نو د $d(x)$ د پكړ والي په خاطر فرضوو چي د $d(x)$ لوی ترين ضريب مساوی په يوه سره دي.

د طبيعي عددو لوی ترين مشترك وېشونكې مو د اقليدس د الكورېتم څخه په استفاده سره لاسته راوړي. اوس به يې وښيو چي دپولينومو د لوی ترين مشترك وېشونكې د پيداكيډو دپاره هم هغې طريقې ته ورته طريقه په كار اچولای سو. د پولينومو دپاره د اقليدس الكورېتم په لاندې ډول دي.

د $f(x)$ او $g(x)$ د پولينومو نامكمل وېش د لاندني شېما پر اساس صورت نيسي:

$$\begin{aligned} f(x) &= g(x).s_1(x) + r_1(x) \\ g(x) &= r_1(x).s_2(x) + r_2(x) \\ r_1(x) &= r_2(x).s_3(x) + r_3(x) \\ &\vdots \\ r_{k-2}(x) &= r_{k-1}(x).s_k(x) + r_k(x) \\ r_{k-1}(x) &= r_k(x).s_{k+1}(x) \end{aligned} \quad \dots(1)$$

څرنګه چې د $I_1(x), I_2(x), I_3(x), \dots$ طاقتونه په ترتیب سره کوچني کيږي ، نو د نامکمل وېش د عملي په سلسله کې و داسې نقطې ته رسېږو چې هېڅ باقی پاته نسي او پروسه پای ته ورسېږي.

قضیه - د P پر عددي فيلډ باندې د $P[x]$ په رينګ کې د $f(x)$ او $g(x)$ دوو اختياري پولینومو لوی ترين مشترک وېشونکي وجود لري او د $f(x)$ او $g(x)$ د اقليدس په الګوريتم کې په وروستي باقی کې د صفر څخه خلاف وی مساوی کيږي.

ثبوت - فرضوو چې $f(x)$ او $g(x)$ د $P[x]$ په رينګ کې خلاف د صفر څخه پولینومونه دي. د (1) شيما څخه په استفادې سره د اقليدس الګوريتم عملي کوو. د نوموړي شيما وروستي معادله بنښي چې $I_k(x)$ د $I_{k-1}(x)$ د وېشونکي رول لوبوي. ددی ځايه استدلال کولای سو چې د وروستي مساوات څخه مخ کې د مساوات دواړه ټوټې پر $I_k(x)$ دوېش وړ دي، ځکه نو $I_k(x)$ د $I_{k-2}(x)$ وېشونکي هم دي. په عين ډول که خپل استدلال ته د لاندې څخه و لور ته ادامه ورکړو و دی نتېجې ته به ورسېږو چې:

$I_1(x):I_k(x), I_2(x):I_k(x), \dots, I_{k-3}(x):I_k(x)$ د (1) شيما د دوهم مساوات څخه $g(x):I_k(x)$ لاسته راځي او دلمړي مساوات څخه يې $f(x):I_k(x)$ حاصلېږي. پدې ترتيب $I_k(x)$ د $f(x)$ او $g(x)$ مشترک وېشونکي دي.

اوس نو د $f(x)$ او $g(x)$ د پولینومو يو مشترک وېشونکي $\delta(x)$ څېړو. څرنګه چې د (1) شيما د لمړي مساوات کينه خوا او د راسته خوا لمړي ټوټه پر $\delta(x)$ دوېش وړ دي ، نو $r_1(x):\delta(x)$ په عين ترتيب د دوهم مساوات ... بلاخره د وروستي مساوات څخه لاندې اړيکې لاسته راځي:

$I_2(x):\delta(x), I_3(x):\delta(x), \dots, I_k(x):\delta(x)$. په نتيجه کې $I_k(x)$ د $f(x)$ او $g(x)$ د پولینومو لوی ترين مشترک وېشونکي دي. همدا ډول په ياد يې ولري چې د پولینومو د نامکمل وېش د تعريف پر اساس $r_1(x), r_2(x), \dots, r_k(x) \in P[x]$ دي.

ثابته سوي قضیې د دوو پولینومو د لوی ترين مشترک وېشونکي د موجوديت سوال ته جواب ووايه او په عين حال کې يې د هغه د موندلو عملي طريقه طرح کړه.

لکه مخکې چې مو ياداوري وکړه د دوو پولینومو لوی ترين مشترک وېشونکي د ثابت پولینوم په دقت سره په پکړه بڼه محاسبه کېدای سي. پدې معنی چې که بل پولینوم هم دراکړه سوو دوو پولینومو لوی ترين مشترک وېشونکي وی نو د لاسته راغلي پولینوم څخه به د ثابت پولینوم په اندازه فرق ولري. ځکه نو د کار د آساني دپاره مقسوم يا مقسوم عليه په اختياري عدد کې چې د صفر څخه خلاف وی ، ضربوو . ددی دپاره چې نه يوازي اختياري مساوات په دغه عدد کې ضرب سي ، بلکه د الګوريتم په پروسه کې تر هغه وروسته ټوله مساواتونه په نوموړي عدد کې ضرب سي. څرګنده ده چې دغه کار (يعنی د خلاف صفر عدد ضربول) خارج قسمت تحريفوی (تغيير ورکوي) خو د اقليدس د الګوريتم په پروسه کې باقی مورته دلچسپه دي او هغوی په ترتيب سره په هغه د صفر څخه خلاف عدد کې ضربېږي.

بيلګه - د $f(x) = 6x^4 + 9x^3 - 2x^2 - x + 3$ او $g(x) = 2x^3 + 3x^2 - 6x - 9$ د پولینومو لوی ترين مشترک وېشونکي محاسبه کوو.

حل - د $f(x)$ پولینوم د $g(x)$ پر پولینوم باندې په نامکمل ډول وېشو.

$$\begin{array}{r} 6x^4 + 9x^3 - 2x^2 - x + 3 \\ -6x^4 \pm 9x^3 \mp 18x^2 \mp 27x \\ \hline \end{array} \left| \begin{array}{r} 2x^3 + 3x^2 - 6x - 9 \\ 3x \end{array} \right.$$

$$16x^2 + 26x + 3 = r_1(x)$$

$$f(x) = g(x)s_1(x) + r_1(x)$$

اوس نو $g(x)$ پر $r_1(x)$ داسی وپشوچي د $g(x)$ پولينوم د 8 په عدد کی ضربوو:

$$8 * / \quad 2x^3 + 3x^2 - 6x - 9$$

$$\begin{array}{r} 16x^3 + 24x^2 - 48x - 72 \\ -16x^3 \pm 26x^2 \pm 3x \\ \hline \end{array} \left| \begin{array}{r} 16x^2 + 26x + 3 \\ x + 1 \end{array} \right.$$

$$-8 * / \quad -2x^2 - 51x - 72$$

$$16x^2 + 408x + 576$$

$$-16x^2 \pm 26x \pm 3$$

$$\div 191 / \quad 382x + 573$$

وروستی باقی چي پر 191 وپشو ، نو $2x + 3 = r_2(x)$ لاسته راځي. اوس نو $r_1(x)$ پر $r_2(x)$ باندي وپشو.

$$2x + 3 = r_2(x)$$

$$\begin{array}{r} 16x^2 + 26x + 3 \\ -16x^2 \pm 24x \\ \hline \end{array} \left| \begin{array}{r} 2x + 3 \\ 8x + 1 \end{array} \right.$$

$$2x + 3$$

$$-2x \pm 3$$

$$0$$

پدی ترتیب د راکره سوو پولينومو لوی ترین مشترک وپشونکی $2x+3$ دی. په نتیجه کی ویلای سو

$$\text{چي } (f(x), g(x)) = x + \frac{3}{2} \text{ دی.}$$

په هغه صورت کی چي د $f_1(x), f_2(x), \dots, f_m(x)$ څو اختیاری پولينومه راکره سوی وی ، نو د هغوی د لوی ترین مشترک وپشونکی مفهوم د دوو پولينومو د مشترک وپشونکی پر تعریف باندي ولاړ دی. د هغوی د لوی ترین مشترک وپشونکی د لاندنیو افادو پذیرعه پیدا کولای سو.

لمری $d_1(x) = (f_1(x), f_2(x))$ شمېرو ، وروسته $d_2(x) = (d_1(x), f_3(x))$ لاسته راوړو او بیا

$d_{m-1}(x) = (d_{m-2}(x), f_m(x))$ بلاخره . محاسبه کوو .

چي د $f_1(x), f_2(x), \dots, f_m(x)$ د پولينومو لوی ترین مشترک وپشونکی دی ، لاسته راځي.

VIII. د پولینومو د لوی ترین مشترک وپشونکی خطی ارائه (خطی څرگندونه)

د پولینومو د لوی ترین مشترک وپشونکی د مهمترینو خاصیتو څخه یو خاصیت د لاندني قضیې پذریعه ارائه کیږی.

قضیه - که $d(x)$ د $f(x)$ او $g(x)$ د پولینومو لوی ترین مشترک وپشونکی وی ، نو د $u(x)$ او $v(x)$ پولینومونه داسی پیدا کولای سو چي :

$$f(x) \cdot u(x) + g(x) \cdot v(x) = d(x) \quad \dots (1)$$

دی.

په هغه حالت کی چي د $f(x)$ او $g(x)$ د پولینومو درجه تر صفر اضافه وی ، نو د $u(x)$ درجه د $g(x)$ تر درجی او د $v(x)$ درجه د $f(x)$ تر درجی کښته ده.

ثبوت - د اقلیدس الگوریتم د $f(x)$ او $g(x)$ پر پولینومو عملی کوو.

$$f(x) = g(x) \cdot s_1(x) + r_1(x)$$

$$g(x) = r_1(x) \cdot s_2(x) + r_2(x)$$

$$r_1(x) = r_2(x) \cdot s_3(x) + r_3(x)$$

⋮

... (2)

$$r_{k-3}(x) = r_{k-2}(x) \cdot s_{k-1}(x) + r_{k-1}(x)$$

$$r_{k-2}(x) = r_{k-1}(x) \cdot s_k(x) + r_k(x)$$

$$r_{k-1}(x) = r_k(x) \cdot s_k(x) + l(x)$$

د قضیې د شرط پر اساس $d(x) = r_k(x)$ سره دی. د آخری مساوات تر مخه مساوات څخه لاندني مساوات لاسته راځی :

$$d(x) = r_{k-2}(x) - r_{k-1}(x) \cdot s_k(x) \quad \dots (3)$$

اوس نو په (3) اړیکه کی د $r_{k-1}(x)$ افاده د $r_{k-3}(x)$ او $r_{k-2}(x)$ له جنسه ارائه کوو چي په نتیجه کی لاندني اړیکه لاسته راځي:

$$\begin{aligned} d(x) &= r_{k-2}(x) - (r_{k-3}(x) - r_{k-2}(x) \cdot s_{k-1}(x)) \cdot s_k(x) = \\ &= -r_{k-3}(x) \cdot s_k(x) + (1 + s_{k-1}(x) \cdot s_k(x)) \cdot r_{k-2}(x) \end{aligned} \quad \dots (4)$$

په (2) اړیکه کی د پورتنی تعویض پروسه ته د لوری خواته ادامه ورکوو، پدی معنی چي په (4) اړیکه کی د $r_{k-2}(x)$ قیمت د $r_{k-3}(x)$ او $r_{k-4}(x)$ له جنسه تعویضوو. تر هغه وخته ودی پروسه ته ادامه ورکوو څو د (1) اړیکه لاسته راسی. پدی ترتیب مو د $u(x)$ او $v(x)$ د پولینومو موجودیت په ثبوت ورساوه.

د قضیې د دوهمې برخې د ثبوت دپاره فرضوو چې $u(x)$ او $v(x)$ پولینومونه داسې وجود لری چې
 $f(x) \cdot u(x) + g(x) \cdot v(x) = d(x)$ او $\deg u(x) \geq \deg g(x)$ دی . اوس نو د $u(x)$ پولینوم د $g(x)$ پر
 پولینوم وپشو.

$$u(x) = g(x) \cdot s(x) + r(x)$$

دلته $\deg r(x) < \deg g(x)$ دی ، ځکه نو

$$d(x) = f(x) \cdot r(x) + g(x) \cdot (v(x) + f(x) \cdot s(x)) \quad \dots(5)$$

د $v(x) + f(x) \cdot s(x)$ د پولینوم درجه د $f(x)$ تر پولینوم لږ ده . په حقیقت کی وینو چې

$\deg(v(x) + f(x) \cdot s(x)) \geq \deg f(x)$ حقیقت لری ، نو په (5) مساوات کی دوهم جزء درجه تر
 $f(x) \cdot g(x)$ لږ نده ، ځکه چې $\deg(f(x), r(x)) < \deg(f(x), g(x))$ دی. بالاخره دی نتیجی ته رسیرو
 چې د لوی ترین مشترک وپشونکی درجه د $f(x)$ او $g(x)$ د پولینومو تر درجی زیاته ده ، خو دداسی
 حالت موجودیت ناممکنه دی. پدی ډول قضیه ثبوت سوه.

تعریف - د (1) مساوات د $f(x)$ او $g(x)$ د پولینومو د لوی ترین مشترک وپشونکی د خطی اړای
 (څرگندونی) په نامه یادیری.

د تبری قضیې ثبوت په عین حال کی د $u(x)$ او $v(x)$ د پولینومو د محاسبی کرنلاره طرح کوی. مور
 به یی په لاندنی بیلگه کی عملاً وگورو.

بیلگه - د لاندنیو پولینومو د لوی ترین مشترک وپشونکی خطی اړانه پیداکوو.

$$f(x) = 4x^4 - 2x^3 - 16x^2 + 5x + 9$$

$$g(x) = 2x^3 - x^2 - 5x + 4$$

حل - پر راکره سوو پولینومو د اقلیدس الگوریتم عملی کوو ، منتهی پدی حالت کی د نامکمل وپش په
 پروسه کی خارج قسمتونه نادیده نسو نیولای . ځکه چې د خارج قسمتو څخه د $u(x)$ او $v(x)$ د پولینومو
 په محاسبه کی کار اخیستل کیږی.

$$\begin{array}{r|l} 4x^4 - 2x^3 - 16x^2 + 5x + 9 & 2x^3 - x^2 - 5x + 4 \\ \hline -4x^4 \mp 2x^3 \mp 10x^2 \pm 8x & \end{array} \quad \begin{array}{l} 2x = s_1(x) \\ \hline \end{array}$$

$$r_1(x) = -6x^2 - 3x + 9$$

$$f(x) = g(x) \cdot s_1(x) + r_1(x)$$

$$\begin{array}{r|l} 2x^3 - x^2 - 5x + 4 & -6x^2 - 3x + 9 \\ \hline -2x^3 \pm x^2 \mp 3x & \end{array} \quad \begin{array}{l} -\frac{1}{3}x + \frac{1}{3} = s_2(x) \\ \hline \end{array}$$

$$-2x^2 - 2x + 4$$

$$\mp 2x^2 \mp x \pm 3$$

$$r_2(x) = -x + 1$$

$$g(x) = r_1(x) \cdot s_2(x) + r_2(x)$$

$$\begin{array}{r|l} -6x^2 - 3x + 9 & -x + 1 \\ \hline \mp 6x^2 \pm 6x & 6x + 9 = s_3(x) \\ \hline -9x + 9 & \\ \hline \mp 9x \pm 9 & \\ \hline 0 & \end{array}$$

$$r_1(x) = r_2(x) \cdot s_3(x)$$

پدی معنی چي $d(x) = r_2(x) = -x + 1$ دی ، ځکه نو :

$$\begin{aligned} d(x) &= g(x) - r_1(x) \cdot s_2(x) = g(x) - (f(x) - g(x) \cdot s_1(x)) \cdot s_2(x) = \\ &= g(x)(1 + s_1(x) \cdot s_2(x)) + f(x) \cdot (-s_2(x)) \end{aligned}$$

$$u(x) = -s_2(x) = \frac{1}{3}x - \frac{1}{3} \quad \text{ددی ځایه}$$

$$v(x) = 1 + s_1(x) \cdot s_2(x) = 1 + (2x) \cdot \left(-\frac{1}{3}x + \frac{1}{3}\right) = -\frac{2}{3}x^2 + \frac{2}{3}x + 1 \quad \text{او}$$

د ټولو شمېرنو په نتجه کی

$$d(x) = -x + 1 = f(x) \cdot \left(\frac{1}{3}x - \frac{1}{3}\right) + g(x) \cdot \left(-\frac{2}{3}x^2 + \frac{2}{3}x + 1\right)$$

لاسته راځی.

VIII §. نسبت یو او بل ته اولیه (په وپش کی بیگانه یا متبائن) پولینومونه

په ریاضیاتو کی د تامو عددو د خاصیتو په څېر د هغو پولینومو مطالعه چي د هغوی لوی ترین مشترک وېشونکی مساوی په یوه سره وی ، مهم رول بازی کوی.

تعریف - د عددی فیادوڅخه پر اختیاری فیلد P باندی د $f(x)$ او $g(x)$ پولینومونه د متبائن یا نسبت یو او بل ته اولیه پولینومو په نامه یادېږی ، که $(f(x), g(x)) = 1$ وی.

په تېر پاراگراف کی د ثابتی سوی قضیې څخه استنباط کیری چي:

قضیه ۱- د $f(x)$ او $g(x)$ پولینومونه یوازی او یوازی هغه وخت متبائن دی ، که د $u(x)$ او $v(x)$ پولینومونه داسی وجود ولری چي $(1) \dots f(x) \cdot u(x) + g(x) \cdot v(x) = 1$ وی.

په رشتیا هم ، که $(f(x), g(x)) = 1$ وی ، نو د VII § د قضیې پر اساس (1) اړیکه صدق کوی.

برعکس، که (1) اریکه صدق وکی ، نو د $f(x)$ او $g(x)$ پولینومونه یوازی یو مشترک وپشونکی لری چي هغه هم یو دی ، یعنی د P د فیله یو عدد دی.

د پورتنی نتیجی پر اساس کولای سو چي خنی قضیې چي د متبائنو پولینوموساده او مهم خاصیتونه مشخصوی ، په ثبوت ورسوو.

قضیه ۲ - که د $f(x)$ پولینوم د $g(x)$ او $h(x)$ د هریوه پولینوم سره متبائن وی ، نو د $f(x)$ پولینوم دهغوی د ضرب د حاصل سره هم متبائن دی.

ثبوت - فرضوو چي $(f(x),g(x))=1$ دی ، ددی خایه د $u(x)$ او $v(x)$ پولینومونه داسی وجود ولری چي $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$ کیږی.

د $h(x)$ په پولینوم کی د پورتنی اریکی د ضرب څخه وروسته لاندنی مساوات لاسته راخی:

$$f(x) \cdot (u(x) \cdot h(x)) + (g(x) \cdot h(x)) \cdot v(x) = h(x)$$

که $f(x)$ او $g(x) \cdot h(x)$ د $\delta(x)$ مشترک وپشونکی ولری ، نو $\delta(x) : h(x)$ دی . ددی خایه استنباط کیږی چي :

$$(f(x),h(x)) : \delta(x)$$

په عین حال کی د قضیې د شرط پر اساس $(f(x),h(x))=1$ هم حقیقت لری ، ځکه نو $\delta(x) \in P$ او $(f(x),g(x) \cdot h(x))=1$ هم حقیقت لری.

قضیه ۳ - که د $f(x)$ او $g(x)$ پولینومونه یوډبل سره متبائن وی او $f(x) \cdot h(x)$ د $g(x)$ پر پولینوم دپوش وړ وی ، نو د $h(x)$ پولینوم د $g(x)$ پر پولینوم دپوش وړ دی.

ثبوت - د $(f(x),g(x))=1$ د فرضیې څخه استنباط کیږی چي $f(x) \cdot u(x) + g(x) \cdot v(x) = 1$ دی.

د آخری مساوات دواړی خواوی په $h(x)$ کی ضربوو:

$$f(x) \cdot u(x) \cdot h(x) + g(x) \cdot v(x) \cdot h(x) = h(x)$$

څرنګه چي $f(x) \cdot h(x) = g(x) \cdot s(x)$ دی ، نو

$$h(x) = g(x) \cdot s(x) \cdot u(x) + g(x) \cdot v(x) \cdot h(x)$$

ځکه نو $h(x) : g(x)$ دی.

قضیه ۴ - که د $f(x)$ پولینوم پر هریوه په خپل منځ کی متبائن پولینومو $g(x)$ او $h(x)$ باندی دپوش وړ وی ، نو $f(x)$ د هغوی پر حاصل ضرب یعنی $g(x) \cdot h(x)$ باندی دپوش وړ دی.

ثبوت - فرضوو چي $f(x) = g(x) \cdot s(x)$ او $(g(x),h(x))=1$ وی . د دریمی قضیې پر اساس $s(x) : h(x)$

دی ، پدی معنی چي $s(x) = h(x) \cdot s_1(x)$ دی ، په نتیجه کی $f(x) = g(x) \cdot h(x) \cdot s_1(x)$ لاسته راخی . ددی خایه $f(x) : g(x) \cdot h(x)$ دی .

قضیه ۵ - که $d(x)$ د $f(x)$ او $g(x)$ د پولینومو لوی ترین مشترک وپشونکی وی ، نو

$$\left(\frac{f(x)}{d(x)}, \frac{g(x)}{d(x)} \right) = 1$$

ثبوت - د VII § د قضیې پر اساس $f(x) \cdot u(x) + g(x) \cdot v(x) = d(x)$ که ددی مساوات دواړی خواوی پر $d(x)$ ووېشو ، نو $\frac{f(x)}{d(x)} \cdot u(x) + \frac{g(x)}{d(x)} \cdot v(x) = 1$ به لاسته راسی. اوس نو د لمړی قضیې پر اساس دی نتیجې ته رسیرو چې د $\frac{f(x)}{d(x)}$ او $\frac{g(x)}{d(x)}$ پولینومونه یوډبله سره متبائن دی.

IX §. د پولینومو کوچنی ترین مشترک مضرب

فرضوو چې د P پر عددی فیله باندی د $f(x)$ او $g(x)$ پولینومونه راگره سوی دی .

تعریف - د $h(x)$ پولینوم د $f(x)$ او $g(x)$ د پولینومو د کوچنیترین مشترک مضرب په نامه یادیری ، په هغه صورن کی چې لاندنی شرطونه پر خای کی:

1- $h(x):f(x)$ او $h(x):g(x)$ وی. یعنی $h(x)$ د دواړو مشترک مضرب وی.

2- د $f(x)$ او $g(x)$ د پولینومو هر مشترک مضرب د $h(x)$ پر پولینوم دپوش وړ دی.

که د $h(x)$ پولینوم د $f(x)$ او $g(x)$ د پولینومو کوچنیترین مشترک مضرب وی ، نو دپوش د ورتوب د خاصیتو څخه استنباط کیږی چې هر د صفر څخه خلاف هر عدد $c \in P$ دپاره د $ch(x)$ پولینوم هم د هغوی کوچنیترین مشترک مضرب دی. د $f(x)$ او $g(x)$ د پولینومو کوچنیترین مشترک مضرب په $[f(x), g(x)]$ سره بنیواو فرضوو چې د هغه د لوی ترین حد ضریب د یوه سره مساوی دی.

بیلگه - که $f(x) = x - 1$ او $g(x) = x + 1$ سره وی ، نو

$$[f(x), g(x)] = x^2 - 1$$

دی. په رشتیا هم $f(x): (x^2 - 1)$ او $g(x): (x^2 - 1)$. علاوه پر دی د $f(x)$ او $g(x)$ د پولینومو هر مشترک مضرب $m(x)$ باید پر $x^2 - 1$ دپوش وړ وی. څرنگه چې د $f(x)$ او $g(x)$ پولینومونه متبائن دی ، ځکه نو $m(x): (x^2 - 1)$ دی.

لاندنی قضیه مورته د کوچنیترین مشترک مضرب د محاسبی طریقه رابینی .

قضیه - پر عددی فیله P باندی د $f(x)$ او $g(x)$ د صفر څخه خلاف اختیاری پولینومو مشترک مضرب

وجود لری او هغه مساوی په $\frac{f(x) \cdot g(x)}{(f(x), g(x))}$ دی.

ثبوت - د $h(x) = \frac{f(x) \cdot g(x)}{(f(x), g(x))}$ پولینوم تر مطالعی لاندی نیسو.

څرنگه چې $h(x) = \frac{f(x)}{(f(x), g(x))} \cdot g(x) = \frac{g(x)}{(f(x), g(x))} \cdot f(x)$ دی ، نو $h(x)$ د $f(x)$ او $g(x)$

د پولینومو مشترک مضرب دی.

فرضوو چي $m(x) = f(x) \cdot s(x)$ او $g(x)$ د پولینومو یو بل مضرب وی، نو $m(x) = f(x) \cdot s(x)$ او $m(x) = g(x) \cdot t(x)$ سره .

غیر له دی څخه $f(x) = f_1(x) \cdot (f(x), g(x))$ او $g(x) = g_1(x) \cdot (f(x), g(x))$ دی. د VIII § د پنځمی قضیې پر اساس د $f_1(x)$ او $g_1(x)$ پولینومونه متبائن دی. ځکه نو

$$f_1(x) \cdot (f(x), g(x)) \cdot s(x) = g_1(x) \cdot (f(x), g(x)) \cdot t(x)$$

$$f_1(x) \cdot s(x) = g_1(x) \cdot t(x) \quad \text{یا}$$

د متبائنو پولینومو خاصیت پر اساس (VIII § ، دریمه قضیه وگورئ) دی نتیجی ته رسیرو چي $s(x) : g_1(x)$ دی ، یعنی $s(x) = g_1(x) \cdot s_1(x)$ دی. پدی ترتیب

$$\begin{aligned} m(x) = f(x) \cdot s(x) &= f(x) \cdot g_1(x) \cdot s_1(x) = f(x) \cdot \frac{g(x)}{(f(x), g(x))} \cdot s_1(x) \\ &= \frac{f(x) \cdot g(x)}{(f(x), g(x))} \cdot s_1(x) = h(x) \cdot s_1(x) \end{aligned}$$

لاسته راځي. وروستي اړیکه مورته بنځي چي $m(x) : h(x)$ دی ، یعنی د $h(x)$ پولینوم د $f(x)$ او $g(x)$ د پولینومو کوچنیترین مشترک مضرب دی.

مور کولای سو چي د کوچنیترین مشترک مضرب مفهوم د درو او یا اضافه تر درو پولینومو دپاره هم مطالعه کرو. په راتلونکي برخه کی به د لوی ترین مشترک وپشونکی او کوچنیترین مشترک مضرب د شمېرنی بله طریقه هم مطالعه کرو.

X§. نه تجزیه کیدونکي پولینومونه Irreducible polynoms او د هغوی خاصیتونه

طبیعی عددونه مو د هغوی د وپشونکو په اړوند پر درو ټولگیو وپشل (دریم فصل ، VI §) ، په لمړی ټولگی کی د یوه عدد شامل ؤ ، په دوهمه ټولگی کی ټوله اولیه عددونه شامل وه او په دریمه ټولگی کی ټوله مرکب عددونه شامل وه. دغه ټول تصنیف د طبیعی عددو د په زړه پوری خاصیتو څېړنه په خاص ټول د اریتمتیک د اساسی قضیې ثبوت ساده کاوه . دغه ټول تصنیف د P پر عددی فیلد باندی د پولینومو په هر رینگ $P[x]$ کی مشاهده کولای سو ، پداسی حال کی چي د یوه د عدد وظیفه د P د عددی فیلد ټول عددونه اجراء کوی، د اولیه عددو وظیفه د P پر فیلد باندی نه تجزیه کیدونکي پولینومونه او د مرکبو عدد وظیفه د P پر فیلد باندی د تجزئی وړ پولینومونه اجراء کوی.

تعریف ۱- د $P[x]$ د رینگ څخه د $f(x)$ پولینوم د P پر فیلد باندی د نه تجزیه کیدونکي پولینوم په نامه یادیری که:

$$1 - \deg f(x) \geq 1 ,$$

۲- د $f(x) = g(x) \cdot s(x)$ په $P[x]$ په رینگ کی ، په ضریبی عاملو باندی په اختیاری تجزیه کی د $g(x)$ یا $s(x)$ دپولینومو څخه د یوه پولینوم درجه مساوی په صفر ده ، یعنی یو د هغو څخه د P د فیلد د عدد و څخه یو عدد دی.

تعريف ۲ - د $P[x]$ د رينگ څخه د $f(x)$ پولينوم د P پر فيلډ باندې د تجزيه كيدونكې (د تجزيې وړ) پولينوم په نامه يادېږي ، كه :

$$1 - \deg f(x) \geq 1 \text{ وى،}$$

۲- د $P[x]$ په رينگ كې د $g(x)$ او $s(x)$ پولينومونه داسې وجود ولري چې د هغوى درجې مساوى په صفر نه وى او $f(x) = g(x) \cdot s(x)$ وى.

د پولينومو د غير تجزيه كيدو او يا د تجزيې وړتوب د هغوى د تعريف په فيلډ پورې مستقيماً اړه لري. لكه څنگه چې په لاندني بېلگه كې په څرگند ډول ليدل كېږي.

بېلگه - د $f(x) = x^2 + 1$ پولينوم د \mathbb{R}, \mathbb{Q} او \mathbb{C} پر عددې فيلډو باندې مشاهده كوو. څرگنده ده چې نوموړى پولينوم د ناطقو او حقيقي، يعنې \mathbb{R}, \mathbb{Q} عددو پر فيلډ د تجزيې وړ ندى. خو د مختلطو عددو \mathbb{C} پر فيلډ باندې د تجزيې وړ دى ، ځكه چې د مختلطو عددو پر فيلډ باندې $f(x) = (x+i)(x-i)$ دى. د P پر فيلډ باندې د نه تجزيه كيدونكو پولينومو اساسى خاصيتونه مطالعه كوو.

لمړئ خاصيت - د P پر فيلډ باندې هر پولينوم چې درجه يې د يوه سره مساوى وى ، د تجزيې وړ ندى.

ثبوت - فرضوو چې د $f(x) = ax + b$ پولينوم ، داسې حال كې چې $a \neq 0$ وى، د تجزيې وړ دى . د تعريف له مخې بايد د $g(x)$ او $s(x)$ پولينومونه داسې وجود ولري چې د هغوى درجې مساوى په صفر نه وى او $f(x) = g(x) \cdot s(x)$ وى. د وروستۍ مساوات پر اساس $\deg f(x) = \deg g(x) + \deg s(x) \geq 2$ دى . په عين حال كې د قضيې د شرط له مخې $\deg f(x) = 1$ دى. لكه چې ليدل كېږي وروستې دوى ادعاوى يو ډبل ضد دى ، پدې معنى چې د $f(x)$ پولينوم د P پر فيلډ باندې نه تجزيه كيدونكئ دى.

دوهم خاصيت - كه د P پر فيلډ باندې د $f(x)$ پولينوم نه تجزيه كيدونكئ (د تجزيې وړ نه وى) ، نو د P پر فيلډ باندې د صفر څخه خلاف هر عدد c دپاره $cf(x)$ پولينوم هم نه تجزيه كيدونكئ دى.

ثبوت - فرضو چې د P پر فيلډ باندې د $f(x)$ پولينوم نه تجزيه كيدونكئ او c د P په فيلډ كې د صفر څخه خلاف عدد دى. اوس نو د $f_1(x) = c \cdot f(x)$ پولينوم مطالعه كوو.

كه د $P[x]$ په رينگ كې د $f_1(x)$ پولينوم د P پر فيلډ باندې د تجزيې وړ وى ، نو بايد د $g(x)$ او $s(x)$ پولينومونه داسې وجود ولري چې $\deg g(x) \geq 1, \deg s(x) \geq 1$ او $f_1(x) = g(x) \cdot s(x)$ دى، ځكه نو

$$c \cdot f(x) = g(x) \cdot s(x) \text{ او } f(x) = \left[\frac{1}{c} g(x)\right] \cdot s(x) \text{ دى. پدې معنى چې د } f(x) \text{ پولينوم د } P \text{ پر فيلډ باندې}$$

د تجزيې وړ دى ، خو دغه حالت زموږ د فرضيې خلاف دى ، ځكه نو د P پر فيلډ باندې د $f_1(x)$ پولينوم نه تجزيه كيدونكئ دى.

دريم خاصيت - كه $f(x) \in P$ پر فيلډ باندې اختياري پولينوم وى او د $p(x)$ پولينوم د P پر فيلډ باندې نه تجزيه كيدونكئ وى ، نو د لاندنيو شرطو څخه يو شرط صدق كوي:

$$1 - f(x) : p(x) \text{ ، يا}$$

$$2 - f(x) \text{ او } p(x) \text{ پولينومونه متباين دى.}$$

ثبوت - فرضوو چې $f(x), p(x) \in P[x]$ او د $p(x)$ د P پر فيلډ باندې نه تجزيه كيدونكئ وى. همدا ډول فرضوو چې $d(x)$ د $f(x)$ او $p(x)$ د پولينومو لوى ترين مشترك وېشونكئ وى. څرنگه چې $d(x)$ د

$p(x)$ وېشونکې دی ، نو یا $\deg d(x)=0$ او یا $d(x) \mid c \cdot p(x)$ ($c \neq 0$) په شکل ارائه کېدای سی. په لمړی حالت کې د $f(x)$ او $p(x)$ پولینومونه متبائن دی او په دوهم حالت کې د $f(x)=d(x) \cdot s(x)$ څخه استنباط کېږی چې $f(x)=c \cdot p(x) \cdot s(x)$ دی ، یعنی $f(x):p(x)$ دی.

څلرم خاصیت - که د $P[x]$ د رینگ د $f(x)$ او $g(x)$ دپولینومود ضرب حاصل پر نه تجزیه کېدونکې پولینوم $p(x)$ د P پر فیله باندی دوش وړ وی ، نو لږ تر لږه د نوموړو پولینومو څخه یو د $p(x)$ پر پولینوم دوش وړ دی.

ثبوت - که د $f(x)$ پولینوم د $p(x)$ پر پولینوم دوش وړ نه وی ، نو ددریم خاصیت پر اساس هغوی یو د بله سره متبائن دی، یعنی $(f(x), p(x))=1$ دی . پدی لحاظ د § VIII دریمې قضیې پر اساس $g(x):p(x)$ دی .

په هغه صورت کې چې څو پولینومه راگره سوی وی ، نو د څلرم خاصیت عمومی شکل په آسانی سره ثابتولای سو.

XI§ . د پولینوموتجزیه په نه تجزیه کېدونکو ضربی عاملو باندی

د نه تجزیه کېدونکې پولینوم د مفهوم څخه په استفادی سره د اریتمتیک و اساسی قضیې (دریم فصل ، § VII) ته ورته قضیه ثابتولای سو.

قضیه - د P پر فیله باندی هر پولینوم چې درجه یې د صفر څخه خلاف وی د

$$f(x) = p_1(x) \cdot p_2(x) \cdot \dots \cdot p_k(x) \quad \dots (1)$$

په شکل ارائه کولای سو. پداسی ډول چې د $p_i(x)$ ، $1 \leq i \leq k$ ټول پولینومونه د P پر فیله باندی نه تجزیه کېدونکې دی. د (1) افاده د ثابت ضربی عامل او دضربی عاملو تر ترتیب پرته ، پکره ده.

ثبوت - که د $f(x)$ پولینوم د P پر فیله باندی نه تجزیه کېدونکې وی ، نو د (1) افاده یوازی یو ضربی عامل لری ، پدی حالت کې $f(x)=p_1(x)$ دی .

که د $f(x)$ پولینوم د P پر فیله باندی د تجزیې وړ وی، نو د $g(x)$ او $s(x)$ پولینومونه داسی وجود لری چې د هغوی درجه د صفر څخه خلاف او $f(x)=g(x) \cdot s(x)$ وی.

که د P پر فیله باندی یو د $g(x)$ او $s(x)$ د پولینوموڅخه د تجزیې وړ وی ، نو هغه بیا هم په ضربی عاملو تجزیه کوو . دغی پروسې ته ادامه ورکوو. څرنگه چې د ضربی عاملو د طاقتو د جمع حاصل باید د راگره سوی پولینوم د طاقت ، یعنی $\deg f(x)=n$ ، سره مساوی سی، ځکه نو د ضربی عاملو تعداد چې درجه ای د صفر څخه خلاف وی ، تر n نه اضافه کېږی. پدی معنی چې د پولینوم د تجزیې پروسه ورسته له k ($k \leq n$) قدم څخه متوقف کېږی او (1) اړیکه لاسته راځی.

اوس به نو د قضیې دوهمه برخه په ثبوت ورسوو. فرضوو چې د P پر فیله باندی د $f(x)$ د پولینوم دپاره دوی څرگندونې د (1) په شکل وجود ولری، پدی معنی چې :

$$f(x) = p_1(x) \cdot p_2(x) \cdot \dots \cdot p_k(x) = t_1(x) \cdot t_2(x) \cdot \dots \cdot t_s(x) \quad \dots (2)$$

پداسی حال کی چي $k \leq s$ دی. څرنگه چي د P پر فيلډ باندی نه تجزیه کیدونکی پولینوم $t_1(x)$ د $f(x)$ د پولینوم وېشونکی دی، نو د نه تجزیه کیدونکو پولینومو د څلرم خاصیت ($X \S$ وگوری) پر اساس لږ تر لږه د $p_1(x) \cdot p_2(x) \cdot \dots \cdot p_k(x)$ د پولینومو څخه یو پولینوم د $t_1(x)$ پر پولینوم وېش ور دی. د بیلگي په ډول فرضوو چي $t_1(x) : p_1(x)$ دی. ولی د P پر فيلډ باندی د $p_1(x)$ هم نه تجزیه کیدونکی دی. ځکه نو د $c_1 \in P$ عدد داسی وجود لری چي $p_1(x) = c_1 t_1(x)$ دی. اوس نو که دغه افاده په (2) اړیکه کی وضع کړو، د دواړو طرفو د اختصار څخه وروسته به لاندی اړیکه لاسته راسی:

$$c_1 \cdot p_2(x) \cdot p_3(x) \cdot \dots \cdot p_k(x) = t_2(x) \cdot t_3(x) \cdot \dots \cdot t_s(x) \quad \dots (3)$$

په همدی ډول د $t_2(x) \cdot t_3(x) \cdot \dots \cdot t_k(x)$ د پولینومو په هکله استدلال کوو څو وروسته له k قدمو څخه $c_1 \cdot c_2 \cdot c_3 \cdot \dots \cdot c_k = t_{k+1}(x) \cdot \dots \cdot t_s(x)$ ددی ځایه استنباط کیری چي د $t_s(x) \cdot \dots \cdot t_{k+1}(x)$ د پولینومو درجی باید مساوی په صفر سره وی. ولی دغه حالت زموږ د فرضیې سره مغایرت لری، ځکه نو باید $k=s$ وی، او د هر $1 \leq j \leq k$ دپاره $p_j(x) = c_j \cdot t_j(x)$ مساوات صدق کوی. پدی معنی چي په رشتیا هم د (1) اړیکه پرته د ثابت ضربی عامل او د ضربی عاملو د ترتیب څخه پکړه ده.

نتیجه - د P پر فيلډ باندی هر د $f(x)$ پولینوم چي درجه ای د صفر څخه خلاف وی د

$$f(x) = [p_1(x)]^{k_1} \cdot [p_2(x)]^{k_2} \cdot \dots \cdot [p_m(x)]^{k_m} \quad \dots (4)$$

په شکل ارائه کولای سو. پداسی حال کی چي $p_1(x) \cdot \dots \cdot p_m(x)$ د P پر فيلډ باندی مختلف نه تجزیه کیدونکی پولینومونه دی. (4) څرگندونه پرته له ثابت ضربی عامل څخه پکړه ده.

په حقیقت کی که په (1) څرگندونه کی هغه ضربی عاملونه چي مساوی وی سره یوځای کړو، نو د (4) څرگندونه به لاسته راسی.

تعریف - د (4) څرگندونه د P پر فيلډ باندی د $f(x)$ د پولینوم د ستندرد یا معیاری تجزیې په نامه یادیری.

بیا هم د یادولو وړ ده چي د $f(x)$ د پولینوم ستندرد یا معیاری تجزیه پدی اړه لری چي نوموړی پولینوم پر کم فيلډ باندی په نظر کی لرو

بیلگه - فرضوو چي $f(x) = x^4 - 4x^2 + 4$ وی. د $f(x)$ معیاری ارائه د ناطقو عددو \mathbb{Q} پر فيلډ باندی $f(x) = (x^2 - 2)^2$ ده، خو د حقیقی عددو \mathbb{R} پر فيلډ باندی عبارت ده له:

$$f(x) = (x - \sqrt{2})^2 \cdot (x + \sqrt{2})^2$$

قضیه ۲ - که د P پر فيلډ باندی د $f(x)$ او $g(x)$ د پولینومو ستندرد تجزیه په نه تجزیه کیدونکو پولینومو راکړه سوی وی، نو د نوموړو پولینومو لوی ترین مشترک وېشونکی $d(x)$ د هغو عاملو په حاصل ضرب سره مساوی کیری چي دواړو پولینومو په تجزیه کی شامل او د کوچنیترین طاقت نما

درلودونکی وی. که په سټنډرډ تجزیه کې مشترک ضربی عاملونه وجود ونلری ، نو د $f(x)$ او $g(x)$ پولینومونه متبائن دی.

ثبوت - فرضوو چې د P پر فیله باندی د $f(x)$ او $g(x)$ د پولینومو سټنډرډ تجزیه په لاندی ډول راکړه سوی ده :

$$f(x) = [p_1(x)]^{k_1} \cdot [p_2(x)]^{k_2} \cdot \dots \cdot [p_r(x)]^{k_r} \cdot \dots \cdot [p_s(x)]^{k_s}$$

$$g(x) = [p_1(x)]^{l_1} \cdot [p_2(x)]^{l_2} \cdot \dots \cdot [p_r(x)]^{l_r} \cdot [t_{r+1}(x)]^{l_{r+1}} \cdot \dots \cdot [t_m(x)]^{l_m}$$

پداسی حال کې چې د $p_1(x), \dots, p_2(x), p_r(x)$ پولینومونه نه تجزیه کیدونکی او دواړو پولینومو په تجزیه کې مشترک ضربی عاملونه دی. د

$$d(x) = [p_1(x)]^{\alpha_1} \cdot [p_2(x)]^{\alpha_2} \cdot \dots \cdot [p_r(x)]^{\alpha_r}$$

پولینوم داسی مشاهده کوو چې $\alpha_1 = \min[k_1, l_1], \alpha_2 = \min[k_2, l_2], \dots, \alpha_r = \min[k_r, l_r]$ دی.

واضح ده چې $d(x)$ د $f(x)$ او $g(x)$ د پولینومو مشترک وېشونکی دی. علاوه پردی د $f(x)$ او $g(x)$ د پولینومو اختیاری مشترک وېشونکی $\delta(x)$ په سټنډرډ تجزیه کې یوازی د $p_1(x), \dots, p_2(x), p_r(x)$ نه تجزیه کیدونکی پولینومونه شاملیدای سی. ځکه نو $d(x) : \delta(x)$ دی. پدی معنی چې $d(x)$ د $f(x)$ او $g(x)$ د پولینومولوی ترین مشترک وېشونکی دی.

که د $f(x)$ او $g(x)$ د پولینومو په سټنډرډ تجزیه کې مشترک ضربی عاملونه وجود ونلری ، نو هغوی په وېش کې بیگانه (متبائن) دی.

په حقیقت کې د $(f(x), g(x)) = d(x)$ د مساوات څخه په هغه صورت کې چې $\deg d(x) \geq 1$ وی استنباط کیری چې د $f(x)$ او $g(x)$ د پولینومونه لږ تر لږه یو مشترک نه تجزیه کیدونکی ضربی عامل لری. خو دغه نتیجه زموږ د شرط سره مغایرت لری .

ثابته سوی قضیې ته د متعددو پولینومو په اړوند انکشاف ورکولای سو. همدا ډول د همدی قضیې ثبوت موږ ته د پولینومو د لوی ترین مشترک وېشونکی د پیداکیډو عملی لار رابښی . منتهی په هغه صورت کې چې د پولینومو سټنډرډ اړانه راکړه سوی وی. لمړی قضیه موږ ته د پولینوم تجزیه په سټنډرډ و پولینومو باندی نه رابښی ، که څه هم د اریتمتیک د اساسی قضیې په ثبوت کې د طبیعی عدد د تجزیې طریقې نغښتی وه. څرنگه چې د نه تجزیه کیدونکو پولینومو شمېر چې درجه یی د یوه سره مساوی وی د P پر فیله باندی بی نهایت ډېر دی ، ځکه نو د هغو تصنیف مشکل دی. خو د طبیعی عددو په هکله پوهیږو چې تر راکړه سوی عدد لاندی په متناهی تعداد اولیه عددونه وجودلری ، ځکه نو د هغو تصنیف هم اسانه دی.

XII§ د پولینومو مشتق او دهغه خاصیتونه

پدی هیله چې لوستونکی د ریاضی د انالیز څخه د مشتق د مفهوم سره پوره بلایت لری ، غواړم چې د پولینومو د نورو خاصیتو د څېړنی د پاره د مشتق د مفهوم څخه کار واخلم. علاوه پردی د پولینومو د الجبر د اساسی قضیې په ثبوت کې چې د اوم فصل په §II کې به مطالعه سی ، څه ناڅه د پولینومو د مشتق او متمادیت د مفهومو څخه کار اخیستل کیری. د ریاضی په انالیز کې د حقیقی متحول لرونکو تابع گانو مشتق د لیمیت د مفهوم په مرسته تعریف سوی دی. دپولینومو په الجبر کې پر اختیاری عددی

فیلد (زمور) د مطالعی ساحه به د مختلطو عددو فیلد وی) بیله لیمیت د مفهوم څخه څېړل کیږی. ځکه نو ضرور دی چې پر اختیاری عددی فیلد باندی دپولینومو د مشتق مفهوم په الجبری بڼه تعریف سی. البته الجبری تعریف باید په خصوصی حالت کی (یعنی د حقیقی عددو پر فیلد \mathbb{R} باندی) د ریاضی د اناالیز د تعریف سره معادل وی.

فرضوو چې P د عددی فیلد باندی $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ n -درجه ای پولینوم دی.

تعریف - د $f(x)$ د پولینوم مشتق ، په هغه صورت کی چې درجه ای د صفر څخه خلاف وی، عبارت دی د

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1} x^{n-2} + \dots + 2a_2 x + a_1 \dots (1)$$

د پولینوم څخه . د صفری پولینوم مشتق او دهغه پولینوم مشتق چې درجه یی مساوی په صفر سره وی ، په صفر سره قبلوو .

د پورتنی تعریف څخه استنباط کیږی چې P پر عددی فیلد باندی د $f(x)$ د پولینوم مشتق بیا هم P پر عددی فیلد باندی پولینوم دی. پداسی حال کی چې $\deg f'(x) = \deg f(x) - 1$ دی. پدی شرط چې $\deg f(x) \geq 1$ وی.

په حقیقت کی د (1) فورمول څخه نتیجه اخیستلای سو چې د $f(x)$ د پولینوم د مشتق $f'(x)$ ضریبونه به داسی شکل ولری.

$$na_n = \underbrace{a_n + a_n + \dots + a_n}_{n\text{-ځلې}}$$

$$(n-1)a_{n-1} = \underbrace{a_{n-1} + a_{n-1} + \dots + a_{n-1}}_{(n-1)\text{-ځلې}}$$

:

$$2a_2 = a_2 + a_2$$

پدی معنی چې د راځړه سوی پولینوم د مشتق ضریبونه د P د فیلد د عنصر و د جمع حاصل دی، علاوه پر دی $na_n \neq 0$ دی. په هغه صورت کی چې $\deg f(x) \geq 1$ وی ، $\deg f'(x) = \deg f(x) - 1$ کیږی.

بیلگه - د $f(x) = 2ix^3 - 3x^2 + (1-2i)x + 2-i$ د پولینوم مشتق په

$$f'(x) = 6ix^2 - 6x + (1-2i)$$

سره مساوی کیږی.

د ریاضی د انالیز و مشتق ته مشابه ، د $f'(x)$ د پولینوم لمړی مشتق د $f(x)$ د پولینوم د دوهم مشتق په نامه یادیری او په $f''(x)$ سره یې بنیو. په اسانې سره امتحانولای سو چې $f^{(n)}(x) = n!a_n$ کیری.

په نتیجه کی د n درجه ای پولینوم $(n+1)$ م مشتق مساوی په صفر سره دی.

دریاضی په انالیزکی د تابع گانو د مشتق جمع او ضرب د فورمولو سره بلد یاست ، هغوی ته ورته فورمولونه د اختیاری پولینومو دپاره هم صدق کوی.

قضیه - د P پر عددی فیلد باندی د $f(x)$ او $g(x)$ د اختیاری پولینومو دپاره لاندنی فورمولونه صدق کوی:

$$(f(x) \pm g(x))' = f'(x) \pm g'(x) \quad \dots (2)$$

$$(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x) \quad \dots (3)$$

ثبوت - فرضوو چې :

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

فرضوو چې $n \geq m$ دی ، نو

$$f(x) + g(x) = a_n x^n + \dots + (a_m + b_m) x^m + \dots + (a_1 + b_1) x + (a_0 + b_0)$$

اوس نود مشتق د تعریف له مخی لاندنی افاده لاسته راخی:

$$\begin{aligned} (f(x) + g(x))' &= n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + m(a_m + b_m) x^{m-1} + \dots + (a_1 + b_1) \\ &= (n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + m a_m x^{m-1} + \dots + 2 a_2 x + a_1) + \\ &\quad + (m b_m x^{m-1} + \dots + 2 b_2 x + b_1) = f'(x) + g'(x) \end{aligned}$$

د (2) فورمول پاته برخه او (3) فورمول لوستونکو ته د تمرین په شکل پریزدو.

نتیجه ۱- د ټولو $c \in P$ دپاره صدق کوی چې $(c \cdot f(x))' = c \cdot f'(x)$ دی.

په رشتیا هم :

$$(c \cdot f(x))' = c' \cdot f(x) + c \cdot f'(x) = 0 \cdot f(x) + c \cdot f'(x) = c \cdot f'(x)$$

نتیجه ۲- د هر $k \in \mathbb{N}$ دپاره د $([f(x)]^k)' = k[f(x)]^{k-1} \cdot f'(x)$ حقیقت لری.

په رشتیا هم ،

$$\begin{aligned}
([f(x)]^k)' &= \underbrace{(f(x) \cdot f(x) \cdot \dots \cdot f(x))}'_{k\text{-حلي}} = \\
&= f'(x) \cdot \underbrace{(f(x) \cdot \dots \cdot f(x))}_{(k-1)\text{-حلي}} + f(x) \cdot \underbrace{(f(x) \cdot \dots \cdot f(x))}'_{(k-1)\text{-حلي}} = \\
&= f'(x) \cdot [f(x)]^{k-1} + f(x) \cdot [f'(x) \cdot \underbrace{(f(x) \cdot \dots \cdot f(x))}_{(k-2)\text{-حلي}} + \\
&\quad + f(x) \cdot \underbrace{(f(x) \cdot \dots \cdot f(x))}'_{(k-2)\text{-حلي}}] \\
&= 2f'(x) \cdot [f(x)]^{k-1} + [f(x)]^2 \cdot \underbrace{(f(x) \cdot \dots \cdot f(x))}'_{(k-2)\text{-حلي}} = \dots = \\
&= kf'(x) \cdot [f(x)]^{k-1}
\end{aligned}$$

پدی ترتیب په راتلونکي کی د مشتق د جمع ، ضرب او طاقت فورمولونه چي په انالایز کی ورسره بلد سوی یاست ، د P پر اختیاری فیله باندی پر پولینومو په آزادانه توگه عملی کولای سو.

§ XIII. د پولینوم جذرونه

فرضوو چي $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ د P پر عددی فیله n -ام درجه پولینوم راکړه سوی وی. نوموړی پولینوم د $f: P \rightarrow P$ په صفت تر څېړني لاندی نیسو. څرنگه چي د $a \in P$ هر عدد دپاره $f(a)$ عبارت دی د تابع د قیمت څخه او یا د $x=a$ دپاره د $f(x)$ د پولینوم د قیمت څخه .

دپولینومو په تیوري کی د $a \in P$ هغه عددونه چي د هغه دپاره $f(a)=0$ وی په خاص ډول په زړه پوری دی.

تعریف ۱- د $a \in P$ عدد د $f(x) \in P[x]$ د پولینوم د جذر په نامه یادېږی ، که $f(a)=0$ وی.

بیلگه - د 2 عدد د \mathbb{Q} پر فیله باندی د $f(x)=x^2-4$ د پولینوم جذر دی. په عین حال کی د $f(x)=x^2+1$ پولینوم د حقیقی عددو \mathbb{R} په فیله کی جذر نلری.

پورتنی بیلگه مورته ښی چي د $f(x)$ پولینوم امکان لری چي د P پر راکړه سوی فیله باندی جذر ولری او یا امکان لری چي جذر ونلری.

د راکړه سوی پولینوم د جذر د موجودیت او د هغه د شمېرني مسأله د پولینومو د تیوري د بنسټیزو مسئلو څخه شمېرل کیږی. ددی په اړوند د $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$ د معادلی حل عبارت دی د معادلی په چپه لاس کی د پولینومو د ټولو جذرو د محاسبی څخه.

د پولینومو د جذر پورتنی تعریف تابعی خصوصیت لری . مور کولای سو چي د پولینوم د جذر مفهوم په الجبری بڼه هم تعریف کړو.

تعريف ۲- د $a \in P$ عدد د P پر راکړه سوی فيلډ باندی د $f(x) \in P[x]$ د پولینوم د جذر په نامه یادیری ، که $f(x)$ پر $x-a$ دوپش وړ وی.

د پولینومو د جذر دوهم تعريف د پولینومو دوپش د ورتوب په مرسته طرح سوی دی ، ځکه نو الجبری کرکتر لری.

قضیه ۱- د P پر فيلډ باندی د $f(x)$ د پولینوم د جذرتایبعی او الجبری تعريفونه یوډبل سره معادل دی. په بله اصطلاح مخکنی لمړی او دوهم تعريفونه سره معادل دی.

ثبوت- فرضوو چي $f(a)=0$ دی، یعنی د a عدد د لمړی تعريف پر اساس د پولینوم جذر دی. پر $x-a$ باندی د $f(x)$ پولینوم د نامکمل وپش په نتیجه کی $f(x)=(x-a) \cdot s(x)+r$ پداسی ډول لاسته راځی چي $r \in P$ دی. ددی ځایه $f(a)=(a-a) \cdot s(a)+r$ لاسته راځی.

د فرضیې پر اساس $f(a)=0$ دی ، ددی ځایه $r=0$ کیږی. پدی معنی چي $f(x):(x-a)$ دی.

برعکس ، فرضوو چي د a عدد دوهم تعريف له مخي د $f(x)$ د پولینوم جذر دی، پدی معنی چي $f(x):(x-a)$ دی. ددی ځایه استنباط کیږی چي د P پر فيلډ باندی د $s(x)$ پولینوم داسی وجود لری چي $f(x)=(x-a) \cdot s(x)$ دی. ددی ځایه $f(a)=(a-a) \cdot s(a)=0$ سره کیږی ، یعنی د a عدد د لمړی تعريف له مخي د $f(x)$ د پولینوم جذر دی.

د ثابتی سوی قضیې پر اساس د پولینوم د جذر ددوارو تعريفو څخه کار اخیستلای سو، خو دوهم تعريف یې نظر و لمړی تعريف ته پدی لحاظ ښه دی چي د هغه پر بنسټ د پولینوم د جذر عمومی تعريف په اصطلاح مضاعف جذر تعريفولای سو .

تعريف ۳- د $a \in P$ عدد د صفر څخه خلاف پولینوم $f(x)$ د k -ام جذر په نامه یادیری ، که $f(x):(x-a)^k$ او $f(x):(x-a)^{k+1}$ وی.

په بله اصطلاح د $f(x)$ د پولینوم د a د جذر مضاعف والی عبارت دی له هغه لوی ترین طبیعی عدد m څخه چي د $P[x]$ په رینګ کی $(x-a)^m$ د $f(x)$ د پولینوم وپشونکی وی. ددی ځایه استنباط کیږی چي د $a \in P$ عدد یوازی او یوازی هغه وخت د $f(x)$ د پولینوم k -ام مضاعف جذر دی چي :

$$f(x) = (x-a)^k \cdot g(x) \quad \dots(I)$$

پداسی حال کی چي $g(x)$ پر $x-a$ باندی دوپش وړ نه وی.

د صفری پولینوم دپاره د مضاعف جذر مفهوم نه تعريف کیږی، ځکه چي صفری پولینوم د $(x-a)^m$ هر پولینوم باندی دوپش وړ دی.

د $f(x)$ د پولینوم دپاره د a د عدد د جذر مضاعف والی د هورنر د شیمای پزریعه ټاکلای سو. پدی معنی چي د $f(x)$ د پولینوم دوپش پروسه پر $x-a$ تر هغه وخته عملی کوو چي د صفر څخه خلاف باقیمانده لاسته راسی.

بیلگه- د $x=2$ د جذر مضاعف والی د $f(x) = x^5 - 8x^4 + 25x^3 - 38x^2 + 28x - 8$ د پولینوم دپاره تعینوو.

حل - د هورنر د شپما څخه په استفاده سره د $f(x)$ پولینوم پر $x-2$ باندی وپشو.

| | | | | | | |
|---|---|----|----|-----|----|----|
| | 1 | -8 | 25 | -38 | 28 | -8 |
| 2 | 1 | -6 | 13 | -12 | 4 | 0 |
| 2 | 1 | -4 | 5 | -2 | 0 | |
| 2 | 1 | -2 | 1 | 0 | | |
| 2 | 1 | 0 | 1 | | | |

جدول 15

په نتیجه کی $f(x)=(x-2)^3(x^2-2x+1)$ دی. پدی معنی چي د 2 عدد د نوموړی پولینوم دریمه درجه مضاعف (دری ځلی) جذر دی.

قضیه ۲ - P د $f(x)$ د فیله باندی د $f(x)$ د صفر څخه خلاف پولینوم د ټولو ممکنو جذرو شمېر د پولینوم تر درجی نسی اضافه کیدای. پداسی حال کی چي هر جذر د هغه د تضاعف درجی سره په نظر کی ونیسو.

ثبوت - فرضوو چي a_1, a_2, \dots, a_m د n -ام درجه ای $f(x)$ پولینوم ($n \geq 1$) په ترتیب سره د k_1, k_2, \dots, k_m د تضاعف د درجی سره ټول جذرونه وی. نو د (1) اړیکي پر اساس لیکلای سو چي:

$$f(x) = (x - a_1)^{k_1} \cdot g_1(x)$$

پداسی حال کی چي $g_1(x)$ د $(x - a_1)$ همدادول د $f(x) : (x - a_1)^{k_1}$ د اړیکي او د $(x - a_1)$ د متبائن والی څخه

$$f(x) = (x - a_1)^{k_1} \cdot (x - a_2)^{k_2} \cdot g_2(x)$$

لاسته راخی پداسی حال کی چي a_1 او a_2 د $g_2(x)$ د پولینوم جذرونه ندی. په همدی ډول خپل استدلال ته د a_1, a_2, \dots, a_m ټولو جذرو په هکله ادامه ورکوو، څو په نتیجه کی

$$f(x) = (x - a_1)^{k_1} \cdot (x - a_2)^{k_2} \cdot \dots \cdot (x - a_m)^{k_m} \cdot g_m(x)$$

پداسی ډول لاسته راسی چي د $g_m(x)$ پولینوم د P فیله کی جذر ونلری. ددی خایه

$$\deg f(x) = k_1 + k_2 + \dots + k_m + \deg g_m(x)$$

پدی معنی چي $k_1 + k_2 + \dots + k_m \leq \deg f(x) = n$ دی.

هغه غیر صفری پولینوم چي درجه یی د صفر سره مساوی وی، جذر نلری.

ثابته سوی قضیه د P په فیله کی د $f(x)$ د پولینوم د جذرو شمېر د لوړی خوا څخه محدودوی. په عین حال کی مو ولیدل چي د $f(x)=x^2+1$ د پولینوم د جذرو شمېر د تعریف په فیله پوری تړلی دی. پدی معنی چي نوموړی پولینوم د \mathbb{Q} او \mathbb{R} په فیله کی جذر نلری، خو د \mathbb{C} په فیله کی دوه جذره لری چي هغه هم عبارت دی له i او $-i$ څخه.

XIV§. د پولینوم مضاعف ضربی عاملونه

فرضوو چې د P پر عددی فیله باندی

$$f(x) = [p_1(x)]^{k_1} \cdot [p_2(x)]^{k_2} \cdots [p_m(x)]^{k_m} \cdots (1)$$

د $f(x)$ د پولینوم ستنډرډ تجزیه وی.

تعریف - که د P پر فیله باندی د $f(x)$ د پولینوم په ستنډرډ تجزیه کی د $p_i(x)$ ($1 \leq i \leq m$) پولینوم د k_i په طاقت وی ، نو د $p_i(x)$ پولینوم د راکره سوی پولینوم د k_i په مرتبه مضاعف ضربی عامل په نامه یادیری.

د راکره سوی تعریف څخه دا نتیجه اخیستلای سو چې:

$p_1(x)$ - د راکره سوی پولینوم $f(x)$ د k_1 (خلی) (په مرتبه مضاعف) ضربی عامل ،

$p_2(x)$ - د راکره سوی پولینوم $f(x)$ د k_2 (خلی) (په مرتبه مضاعف) ضربی عامل ، ... ،

$p_m(x)$ - د راکره سوی پولینوم $f(x)$ د k_m (خلی) (په مرتبه مضاعف) ضربی عامل دی.

په آسانی سره یی آزمویلای سو چې د $p(x)$ نه تجزیه کیدونکی پولینوم یوازی او یوازی هغه وخت د $f(x)$ د پولینوم د k په مرتبه مضاعف ضربی عامل دی که د $f(x)$ پولینوم پر $[p(x)]^k$ دوپش وړوی ، خو پر $[p(x)]^{k+1}$ دوپش وړ نه وی.

قضیه ۱ - که د P پر فیله باندی د $p(x)$ نه تجزیه کیدونکی پولینوم د $f(x)$ د پولینوم د k مرتبه یی $k \geq 2$ مضاعف ضربی عامل وی ، نو $p(x)$ د $f'(x)$ د پولینوم $k-1$ مرتبه یی ضربی عامل دی.

که $p(x)$ د $f(x)$ د پولینوم یو خلی ضربی عامل وی ، نو د $p(x)$ پولینوم د P په فیله کی په ضربی عاملونو د $f'(x)$ په ستنډرډ تجزیه کی شامل ندی.

ثبوت - فرضوو چې د P پر فیله باندی د $p(x)$ نه تجزیه کیدونکی پولینوم د $f(x)$ د پولینوم k -خلی $k \geq 2$ ضربی عامل وی ، نو $f(x) = [p(x)]^k \cdot s(x)$ دی. څرنگه چې $p(x) \nmid s(x)$ دی ، نو $s(x)$ او $p(x)$ یوډبل سره متبائن دی. د $f(x)$ د پولینوم مشتق یعنی $f'(x)$ محاسبه کوو. د مشتق نیولو د قوانینو (د ضرب او طاقت قوانین) له مخی

$$\begin{aligned} f'(x) &= \{[p(x)]^k \cdot s(x)\}' = \{[p(x)]^k\}' \cdot s(x) + [p(x)]^k \cdot s'(x) = \\ &= k[p(x)]^{k-1} p'(x) \cdot s(x) + [p(x)]^k \cdot s'(x) = \\ &= [p(x)]^{k-1} \cdot [k \cdot p'(x) \cdot s(x) + p(x) \cdot s'(x)] \end{aligned}$$

دی. پدی معنی چی $f'(x) : [p(x)]^{k-1}$ دی.

د $g(x) = k \cdot p'(x) \cdot s(x) + p(x) \cdot s'(x)$ پولینوم به وڅیرو.

که $g(x):p(x)$ وای ، نو د وېش د ورتوب د خاصیتو پر اساس باید $k \cdot p'(x) \cdot s(x):p(x)$ وی. څرنګه چې $s(x)$ او $p(x)$ یوډبل سره متبائن دی ، نو باید $p'(x):p(x)$ وی ، خو دا امکان نلری ځکه چې د پولینوم د مشتق طاقت تر اصلی پولینوم تر طاقت زیات نه وی. ځکه نو د $g(x)$ پولینوم د $p(x)$ پر پولینوم د وېش وړ ندی. په نتیجه کی استدلال کولای سو چې د $f'(x)$ پولینوم د $[p(x)]^k$ پر پولینوم د وېش وړ ندی. پدی معنی چې د $p(x)$ پولینوم د $f'(x)$ د پولینوم $(k-1)$ -ځلی ضربی عامل دی.

که د ضربی عامل $p(x)$ د تضاعف مرتبه د یوه سره مساوی وی ، نو

$$f'(x) = p'(x) \cdot s(x) + p(x) \cdot s'(x)$$

کیرلی. د پاس په شان استدلال کولای سو چې د $f'(x)$ پولینوم د $p(x)$ پر پولینوم د وېش وړ ندی. پدی معنی چې د $p(x)$ پولینوم د P پر فیله باندی د $f'(x)$ د پولینوم په معیاری تجزیه کی شامل ندی.

نتیجه - د $f(x)$ پولینوم یوازی او یوازی هغه وخت د مضاعف ضربی عاملو درلودونکی ندی چې د $f(x)$ او $f'(x)$ پولینومونه په خپل منځ کی سره متبائن وی.

ثبوت - که د $f(x)$ د پولینوم د ټولو ضربی عاملو د تضاعف ترتیب د یوه سره مساوی وی ، نو هغوی ټوله د $f'(x)$ په ستندرد تجزیه کی شامل ندی . ځکه نو د $\S XI$ د دوهمی قضیې پر اساس د $f(x)$ او $f'(x)$ پولینومونه یوډبل سره متبائن دی. که د $f(x)$ پولینوم لږ تر لږه د $p(x)$ یو مضاعف ضربی عامل ولری، نو د $f(x)$ او $f'(x)$ د پولینومو لوی ترین مشترک وېشونکی د $p(x)$ پر پولینوم د وېش وړ دی. پدی معنی چې د $f(x)$ او $f'(x)$ پولینومونه یوډبل سره متبائن ندی.

د ثابتی قضیې څخه په استفاده د پولینومو د تضاعف جذر لازمی او کافی شرط طرح کولای سو . د مضاعف جذر د تعریفو څخه نتیجه اخیستلای سو چې $a \in P$ د $f(x) \in P[x]$ د پولینوم یوازی او یوازی هغه وخت k -مه مرتبه مضاعف جذر دی ، چې $x-a$ د $f(x)$ د پولینوم k -مه مرتبه مضاعف ضربی عامل وی.

قضیه ۲ - ددی دپاره چې د $a \in P$ عدد د $f(x) \in P[x]$ د پولینوم k -مه مرتبه مضاعف جذر وی ، لازمه او کافی ده چې :

$$f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0 \quad \text{او} \quad f^{(k)}(a) \neq 0 \quad \dots (2)$$

ثبوت - فرضوو چې a د $f(x)$ د پولینوم k -مه مرتبه مضاعف جذر دی. ځکه نو $f(x) = (x-a)^k \cdot s(x)$ دی ، پداسی حال کی چې $s(x)$ او $x-a$ یوډبل سره متبائن دی. د لمړی قضیې پر اساس

$$f'(x) = (x-a)^{k-1} \cdot s_1(x), f''(x) = (x-a)^{k-2} \cdot s_2(x), \dots, f^{(k-1)}(x) = (x-a) \cdot s_{k-1}(x)$$

او $f^{(k)}(x) = s_k(x)$ دی . په نتیجه کی :

$$f(a)=f'(a)=\dots=f^{(k-1)}(a)=0 \text{ او } f^{(k)}(a)=s_k(a) \neq 0 \text{ دی.}$$

برعکس ، که فرض کرو چي د قضیې (2) شرط صدق کوی ، نو د a عدد د $f(x)$ د پولینوم مضاعف جذر دی چي د هغه ترتیب په m سره ښیو.

$$f(a)=f'(a)=\dots=f^{(m-1)}(a)=0 \text{ او } f^{(m)}(a) \neq 0 \text{ دی.}$$

که $m < k$ وی ، نو $m \leq k-1$ سره کیږی ، په نتیجه کی $f^{(m)}(a)=0$ دی. خو دغه حالت د قضیې د شرط سره مغایرت لری .

په همدی ډول استدلال کولای سو چي که $m > k$ وی ، نو $m-1 \geq k$ او $f^{(k)}(a)=0$ سره کیږی ، خو دغه حالت هم د قضیې د شرط سره مغایرت لری ، ځکه نو باید $k=m$ وی.

موږ کولای سو چي د ثابتی سوی قضیې څخه کار واخلو او د پولینوم د راکړه سوی جذر تضاعف په اسانۍ سره وټاکو. کله داسی هم پېښیږی چي د پولینوم د جذر محاسبه یوازې د هغه دیوه په تضاعف سره ختمه سی.

فرضوو چي د $f(x)$ پولینوم د مضاعف ضربی عاملو درلودونکی وی ، یعنی د $f(x)$ او $f'(x)$ پولینومونه یوډبل سره متبائن نه وی او د (1) اړیکه د P پر فیلډ باندی دهغوی ستندرد تجزیه وی. که د ټولو هغو نه تجزیه کیدونکو ضربی عاملو دضرب حاصل چي د تضاعف درجه یی په یوه سره مساوی وی په h_1 سره وښیو، د ټولو هغو نه تجزیه کیدونکو ضربی عاملو دضرب حاصل چي د تضاعف درجه یی په دوه سره مساوی وی په h_2 سره وښیو، ... ، نو د (1) ستندرد تجزیه به ځانته لاندی ښه واخلی:

$$f(x) = h_1(x) \cdot [h_2(x)]^2 \cdot [h_3(x)]^3 \cdots [h_r(x)]^r$$

$$f = h_1 \cdot h_2^2 \cdot h_3^3 \cdots h_r^r \quad \dots(3) \quad \text{یا په لنډ ډول یی داسی هم لیکلای سو:}$$

که د (1) په تجزیه کی د k ام ترتیب مضاعف ضربی عاملونه وجود ونلری ، نو $h_k=1$ سره اېږدو. همدا ډول د یادونی وردی که په (1) تجزیه کی مضاعف ضربی عاملونه وجود ونلری ، نو $f(x) = h_1(x)$ سره کیږی.

تعریف ۲ - د $f(x)$ د پولینوم د څرگندونې مسئله د (3) په شکل د مضاعفو ضربی عاملو د تفکیک (بیلول) Isolation په نامه یادېږی.

قضیه ۳ - د P پر فیلډ باندی د هر پولینوم $f(x)$ مضاعف ضربی عاملونه د $P[x]$ د رینګ پر ځینو پولینومو باندی د متناهی الجبری عملیو څخه د استفادی په نتیجه کی ، تفکیک کولای سو.

ثبوت - فرضوو چي د $f(x)$ د پولینوم مضاعف ضربی عاملونه بیل سوی دی، پدی معنی چي (3)مه

$$f = h_1 \cdot h_2^2 \cdot h_3^3 \cdots h_r^r \quad \text{اړیکه صدق کوی .}$$

د $h_1, h_2, h_3, \dots, h_r$ د پولینومو د موندلو طریقه د $f(x)$ د پولینوم پر اساس طرح کووږ.

د $f(x)$ د پولینوم مشتق یعنی f' څېرو. د دوهمی قضیې پر اساس f' پر h_1 د وېش وړ ندی خو په عین حال کی h_2 بوخل (یعنی د تضاعف ترتیب یې یو دی)، h_3 دوه ځلې (یعنی د تضاعف ترتیب یې دوه دی)، ...، په همدی ترتیب h_r ، $r-1$ ځلې د f' په سنډرډ یا معیاری تجزیه کی دخپل دی. ددی اسیته لیکلای سو چي:

$$f' = h_2 \cdot h_3^2 \cdots h_r^{r-1} \cdot s_1(x)$$

پداسی حال کی چي د $s_1(x)$ پولینوم پر هیڅ یو د $h_1, h_2, h_3, \dots, h_r$ د وېش وړ ندی. ځکه نو د $f(x)$ او $f'(x)$ د پولینومو لوی ترین مشترک وېشونکی (د XIS د دوهمی قضیې پر اساس)

دی. اوس نو د d_1 مشتق یعنی d_1' لاسته راوړو او د $d_1(x)$ او $d_1'(x)$ لوی

ترین مشترک وېشونکی یعنی $d_2(x)$ پیدا کوو. هغه به عبارت وی له: $d_2 = h_3 \cdot h_4^2 \cdots h_r^{r-2}$

که په همدی ډول خپلی شمېرنی ته ادامه ورکړو نو د مساواتو لاندنی سیستم به لاسته راسی:

$$d_3 = h_4 \cdot h_5^2 \cdots h_r^{r-3}$$

:

$$d_{r-2} = h_{r-1} \cdot h_r^2 \quad \dots(4)$$

$$d_{r-1} = h_r$$

$$d_r = 1$$

اوس به نو د $\frac{f}{d_1} = g_1, \frac{d_1}{d_2} = g_2, \dots, \frac{d_{r-2}}{d_{r-1}} = g_{r-1}$ او $\frac{d_{r-1}}{d_r} = g_r$ لاسته راوړو. د پورتنیو فارمولو (4) پر اساس g_1, g_2, \dots, g_r شمېرو:

$$g_1 = \frac{f}{d_1} = h_1 \cdot h_2 \cdots h_r$$

$$g_2 = \frac{d_1}{d_2} = h_2 \cdot h_3 \cdots h_r$$

:

...(5)

$$g_{r-1} = \frac{d_{r-2}}{d_{r-1}} = h_{r-1} \cdot h_r$$

$$g_r = \frac{d_{r-1}}{d_r} = h_r$$

بلاخره د مساواتو د (5) سیستم څخه $\dots(6) \quad h_1 = \frac{g_1}{g_2}, h_2 = \frac{g_2}{g_3}, \dots, h_{r-1} = \frac{g_{r-1}}{g_r}, h_r = g_r$

لاسته راځی.

څرنګه چي د d_1, d_2, \dots, d_r او د g_1, g_2, \dots, g_r پولینومونه د الجبری عملیو څخه په استفاده سره د $f(x)$ د پولینوم څخه لاسته راغلي دی، ځکه نو د (6) فارمولونه مطلوبه نتیجه ورکوی.

بیلگه - د $f(x) = x^4 - x^3 - 3x^2 + 5x - 2$ د پولینوم مضاعف ضربی عاملونه به تفکیک کرو.

حل - لمړی به د $f(x)$ د پولینوم مشتق پیدا کړو.

$$f'(x) = 4x^3 - 3x^2 - 6x + 5$$

د $d_1(x)$ د لاسته راوړلو دپاره د اقلیدس د الگوریتم څخه کار اخلو:

$$\begin{array}{r} 4x^4 - 4x^3 - 12x^2 + 20x - 8 \\ \underline{-4x^4 + 3x^3 + 6x^2 + 5x} \\ 7x^3 - 18x^2 + 25x - 8 \\ \underline{-7x^3 + 21x^2 - 49x + 8} \\ 43x^2 - 24x \\ \underline{-43x^2 + 172x - 172} \\ 148x - 172 \\ \underline{-148x + 172} \\ 0 \end{array}$$

$$\begin{array}{r} 4x^3 - 3x^2 - 6x + 5 \\ \underline{-4x^3 + 8x^2 + 4x} \\ 11x^2 - 10x + 5 \\ \underline{-11x^2 + 10x + 5} \\ 0 \end{array}$$

پدی معنی چې $d_1(x) = x^2 - 2x + 1$ دی. ددی ځایه $d_1'(x) = 2x - 2$ کیری او

$d_2(x) = x - 1$ دی. ځکه نو $d_2'(x) = 1$ او $d_3(x) = 1$ دی.

اوس به نو د $g_1(x), g_2(x)$ او $g_3(x)$ پولینومونه پیدا کړو.

$$g_1(x) = \frac{f(x)}{d_1(x)} = \frac{x^4 - x^3 - 3x^2 + 5x - 2}{x^2 - 2x + 1} = x^2 + x - 2$$

$$g_2(x) = \frac{d_1(x)}{d_2(x)} = \frac{x^2 - 2x + 1}{x - 1} = x - 1$$

$$g_3(x) = \frac{d_2(x)}{d_3(x)} = x - 1$$

ځکه نو $h_3(x) = g_3(x) = x - 1$ او $h_2(x) = \frac{g_2(x)}{g_3(x)} = 1$, $h_1(x) = \frac{g_1(x)}{g_2(x)} = x + 2$

په نتیجه کی $f(x) = (x+2)(x-1)^3$ دی.

په پورتنی بیلگه کی لیدل کیږی چې د مضاعفو ضربی عاملو د تفکیک د مسألې د حل په نتیجه کی د راکړه سوی پولینوم سټنډرډه تجزیه په اولیه ضربی عاملو لاسته راځی. پدی معنی چي د بوی مسألې د حل په نتیجه کی دوو هدفو ته رسیږو. دغه ډول امکان تل نه میسر کیږی. خو د پولینوم د اولیه ضربی عاملو تفکیک په ډیرو حالتو کی د راکړه سوی پولینوم تحلیل او د جزو محاسبه اسانه کوی.

VX§. یو متحوله پولینومونه پر اختیاری فیلډ باندی - د پولینوم د تجزیې فیلډ

ددی فصل په تېرو برخو کی مو یو متحوله پولینومونه پر عددی فیلډو باندی وڅېړل ، د پولینوم مفهوم له دوو اړخو څخه تر کتنې لاندی ونیوی . یو د پولینوم الجبری اړخ (I§) او بل هم د پولینوم تابعی اړخ (II§) ، وروسته مو ددی دواړو اړخو معادلیت په ثبوت ورساوه. پوښتنه کیږی چي آیا د پولینوم د مفهوم تعریف ته د P پر اختیاری فیلډ باندی عمومیت ورکولای سو که نه ؟ څرگنده ده چي د پولینوم مفهوم د لید د دواړه پلوه یعنی الجبری او تابعی د P پر اختیاری فیلډ باندی مطالعه کولای سو. خو په متناهی فیلډو کی د پولینومو د الجبری او تابعی تعریفو معادلیت نه ساتل کیږی.

په رشتیا هم ، که د Z_2 د مودول پر اساس د باقیمانده و فیلډ $P=Z_2=\{0,1\}$ په نظر کی ونیسو (څلرم فصل ، §III وگورئ)، نو د پولینومو مساوی والی د الجری تعریف د نظره نه پر ځای کیږی. د بیلگی په توگه د $f(x)=x+1$ او $g(x)=x^2+1$ پولینومونه چي ضریبونه یې د Z_2 د فیلډ څخه وی د الجبری تعریف له مخی سره مساوی ندی، خو په عین حال کی دواړه پولینومونه د تابع په څېر سره مساوی دی ، ځکه چي $f(0)=g(0)=1$ او $f(1)=g(1)=0$ دی. پدی معنی چي د $f(x)$ او $g(x)$ دواړه پولینومونه د X د یوه متحوله تابع گانو په څېر چي یوازی او یوازی د Z_2 د فیلډ څخه قیمتونه واخلی ، یو د بله سره مساوی دی.

پدی ترتیب د P پر اختیاری فیلډ باندی د پولینومو په تیوری کی ، په هغه صورت کی چي د پام لرنی وړ مغلق والی غوښتونکی ونه اوسو ، د پولینومو څېړنه د تابع په صفت ناممکنه ده. ځکه نو پدی پاراگراف کی به پولینومونه پر اختیاری فیلډ باندی د الجبری نقطه نظره تر مطالعی لاندی ونیسو.

په اسانی سره یې ازمویلای سو چي په I§ کی که د "عددی فیلډ" د کلمی پر ځای د "اختیاری فیلډ" کلمه په تعریف او قضیو کی راوړو ، په هغوی کی به کوم تغیر رانسی . پدی معنی چي د P پر اختیاری فیلډ باندی د X یو متحوله پولینومو سیټ یعنی $P[x]$ تبدیلی رینگ دی او مور کولای سو چي د هغه د خاصیتو څخه و عددی فیلډ P ته ورته کار واخلو.

لاندی خصوصیتونه پر اختیاری فیلډ P باندی د پولینومو په رینگ $P[x]$ کی صدق کوی:

- د پولینومو د وپش دورتوب تیوری ،

- د لوی ترین مشترک و بشونکی تعریفونه او ټول خصوصیتونه ، د اقلیدس الگوریتم ، د لوی ترین مشترک و بشونکی خطی ارائه (VII§) او یوډبل سره متبائنو پولینومو خاصیتونه،

د پولینومو د جزو مفهوم او د مضاعفو جزو اساسی خاصیتونه .

په § VIII کی موثباته کره چي د پولینومو د جذرو شمېر دهغه تر درجی نه اضافه کیری (دوهمه قضیه). په عین حال کی د صفر څخه خلاف پولینوم په هکله د لیرتزره یوه جذر د موجودیت مسئله لاینحله پاته سوه.

ومولیدل چي د $f(x)=x^2-2$ پولینوم د ناطقو عددو \mathbb{Q} په فیلد کی جذر نلری، د $g(x)=x^2+1$ پولینوم د حقیقی عددو \mathbb{R} په فیلد کی جذر نلری، خو دواړه پولینومونه د مختلطو عددو \mathbb{C} په فیلد کی، چي د نوموړو فیلدو وسعت ورکړه سوی فیلدونه دی، جذر لری. پوښتنه کیری چي آیا پاسنی بیلگی پر اختیاری فیلد باندی د پولینومو په هکله د یوډول عمومی نظم ښکارندوی ندی؟

قضیه ۱ (کرونکر Kronecker) - که د P پر اختیاری فیلد باندی د $f(x)$ پولینوم د تجزیې وړ نه وی، نو د نوموړی فیلد توسعه K داسی وجود لری چي د $f(x)$ د پولینوم جذر احتواء کوی.

ثبوت - فرضوو چي $(f(x))$ د $P[x]$ د رینگ اساسی آیدبال دی چي د P پر فیلد باندی د نه تجزیه کیدونکی پولینوم $f(x)$ په ذریعه تشکیل سوی دی. د $P[x]/f(x)$ فاکتور رینگ به مطالعه کړو. د نوموړی رینگ عنصرونه د $P[x]$ د پولینومو هغه ټولگی دی چي د $f(x)$ پر پولینوم باندی دوپش په نتیجه کی د عین باقیمانده خاوند وی. پدی معنی که د $h(x)$ او $g(x)$ پولینومو نه په یوه ټولگی اړه ولری، نو د هغوی د تفریق حاصل د $f(x)$ پر پولینوم دوپش وړ دی.

څرنگه چي د $P[x]$ رینگ تبدیلی دی، نو دهغه فاکتور رینگ $P[x]/f(x)$ هم تبدیلی رینگ دی. علاوه پردی فرضوو چي $A \in P[x]/f(x)$ او $A \neq 0$ وی. که $g(x) \in A$ د $g(x)$ پولینوم د A په ټولگی پوری اړه ولری، نو د $g(x)$ پولینوم د $f(x)$ پر پولینوم پوره نسی وپشل کیدای. څرنگه چي د $f(x)$ پولینوم د P پر فیلد نه تجزیه کیدونکی دی، نو د $f(x)$ او $g(x)$ پولینومونه یوډبل سره متبائن دی. ځکه نو د $P[x]$ په رینگ کی د $u(x)$ او $v(x)$ پولینومونه داسی وجود لری چي $g(x).u(x)+f(x).v(x)=1$ دی.

$$g(x).u(x)=1-f(x).v(x) \quad \text{ددی خایه:}$$

که د وروستی اړیکی راسته خوا پر $f(x)$ وپشو، نو د یوه عدد باقی پاته کیری، یعنی د E په ټولگی پوری اړه لری. که دهغه پولینومو ټولگی چي د $u(x)$ پولینوم احتواء کوی په B سره وښیو، نو لاندنی مساوات ښیي چي $A \cdot B = E$ دی.

ورستی اړیکه ښیي چي د $P[x]/f(x)$ په رینگ کی د هر غیر صفری عنصر دپاره معکوس عنصر وجود لری، پدی معنی چي $P[x]/f(x)$ فیلد دی. که نوموړی فیلد په K سره وښیو، نو دهر عنصر $a \in P$ جواب ورکونکی د \bar{a} د پولینومو هغه ټولگی ده چي پر $f(x)$ باندی دوپش په نتیجه کی a باقی پاته کیری. څرگنده ده چي $a \in \bar{a}$ ده. ټوله هغه ټولگی چي دغه ډول ښه ولری د K د فیلد داسی سب فیلد تشکیلوی چي د P د فیلد سره ایزومورف دی. په حقیقت کی زموږ د نظر ایزومورف د $\varphi(a) = \bar{a}$ د مساوات په ذریعه تعریف کیدای سی. ددی اسیته په راتلونکو څېړنو کی د P د فیلد عنصرونه د هغوی د جواب ورکونکی ټولگی سره منطبق کوو.

د هغو پولینومو ټولگی چي د $f(x)$ د پولینوم دوپش په نتیجه کی x باقی پاته سی په \bar{x} سره ښیو. همدا ډول فرضوو چي $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ دی. اوس نو د K په فیلد کی لاندنی ټولگی شمېرو:

$$\bar{a}_n \bar{x}^n + \bar{a}_{n-1} \bar{x}^{n-1} + \dots + \bar{a}_1 \bar{x} + \bar{a}_0 = C$$

د K په فیلډ کې (یعنی د $P[x]/f(x)$ په فاکتور رینګ کې) د جمع او ضرب د تعریفو څخه لاندې اړیکه لاسته راځی:

$$C = \overline{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0} = \overline{(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0)} = \overline{f(x)}$$

پدې معنی چې د C ټولګې یوازې د $f(x)$ پولینوم احتواء کوی. ددې ځایه استنباط کېږی چې $C = (f(x)) = 0$ کېږی، یعنې د C ټولګې، صفری ټولګې ده. د هر $0 \leq i \leq n$ دپاره د $\bar{a}_i = a_i$ د مطابقت څخه $a_n \bar{x}^n + a_{n-1} \bar{x}^{n-1} + \dots + a_1 \bar{x} + a_0 = 0$ لاسته راځی. پدې معنی چې د \bar{x} ټولګې د $f(x)$ د پولینوم جذر دی.

تعریف - د L په فیلډ کې چې د $f(x)$ پولینوم په خطی ضربی عاملو باندې تجزیه کېږی، د نوموړی پولینوم د تجزیې د فیلډ په نامه یادېږی.

لاندې مهمه قضیه د کروئکر د قضیې نتیجه ده.

قضیه ۲ - د هر $f(x) \in P[x]$ پولینوم دپاره چې درجه یې تره یوه لویه او یا مساوی وی یعنې $(\deg f(x) \geq 1)$ وی، د L د تجزیې فیلډ وجود لری.

ثبوت - فرضوو چې د $f(x)$ پولینوم د P پر فیلډ باندې د تجزیې وړ نه وی، نو د لمړی قضیې پر اساس د P د فیلډ توسعه K_1 داسی وجود لری چې د $f(x)$ پولینوم د α_1 جذر درلودونکی دی، پدې معنی چې

$$f(x) = (x - \alpha_1) f_1(x); f_1(x) \in K_1[x]$$

که $\deg f_1(x) \geq 1$ وی، نو د $f_1(x)$ د پولینوم په هکله د لمړی قضیې د تطبیق په نتیجه کې چې دهغه درجه د $f(x)$ تر درجې کوچنی $(\deg f(x) = \deg f_1(x) + 1)$ ده، د K_1 د فیلډ توسعه K_2 لاسته راځی. پداسی حال کې چې د K_2 په فیلډ کې د $f_1(x)$ جذر α_2 پروت دی. څرګنده ده چې α_2 د $f(x)$ د پولینوم جذر او K_2 د P د فیلډ توسعه ده $f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot f_2(x)$.

که پورتنی پروسې ته د $f(x)$ د پولینوم ددرجې په تعداد $(\deg f(x))$ ادامه ورکړو د $K_{\deg f}$ توسعه داسی لاسته راځی چې د $f(x)$ پولینوم په هغه کې تجزیه کېږی.

پدې برخه کې د ثابتی سوی قضیو څخه په اووم فصل کې د مختلطو عددو پر فیلډ باندې د پولینومو د مطالعې په وخت کې کار واخلو.

په اسانۍ سره لیدل کېږی چې د $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ د پولینوم وسعت موندلی فیلډ \mathbb{R} او د $f(x) = x^2 + 1 \in \mathbb{R}[x]$ د پولینوم وسعت موندلی فیلډ \mathbb{C} دی.

شپږم فصل څو متحوله پولینومونه

I§. پر عددی فیله باندی د n متحوله پولینومو رینگ

د P پر اختیاری عددی فیله باندی د یو متحوله پولینومو ډیر خصوصیتونه مو په تېر فصل کی وڅېړل ، خو ټوله پولینومونه مو مطالعه نه کړل . په ښونځی کی کله کله د داسی پولینومو سره مصروف و چې هغوی څو متحوله درلوده ، د بیلگی په ډول $x^2+2xy+y^2, x^3-y^3, x^3+y^3, (x-y)^2$... او داسی نور. ددغه اسیته باید ددغه ډول پولینومو عمومی خاصیتونه په تفصیل سره وڅېړل سی.

فرضوو چې n دطبیعی عددو څخه یو عدد او P عددی فیله دی. په x_1, x_2, \dots, x_n باندی د P پر فیله باندی متحولونه ښیو، همدا ډول فرضوو چې $a, b, c, \dots \in P$ دی .

تعریف ۱- د P پر عددی فیله باندی د x_1, x_2, \dots, x_n د متحولو سره n متحوله پولینوم عبارت دی د

$$ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} + bx_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} + \dots + cx_1^{\gamma_1} \cdot x_2^{\gamma_2} \cdot \dots \cdot x_n^{\gamma_n} \quad \dots(1)$$

افادی څخه چې د $ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$ ، $bx_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n}$ ، ... ، $cx_1^{\gamma_1} \cdot x_2^{\gamma_2} \cdot \dots \cdot x_n^{\gamma_n}$ متناهی حدونه احتوا کوی او د $\alpha_1, \beta_1, \gamma_1, \dots, \alpha_n, \beta_n, \gamma_n$ ($1 \leq i \leq n$) ټوله عددونه غیر منفی تام عددونه دی.

پدغه حالت کی $a, b, c, \dots \in P$ د ذکر سوږو حدونو د ضریبو په نامه او $\alpha_1, \beta_1, \gamma_1, \dots, \alpha_n, \beta_n, \gamma_n$ د متحول د طاقت په نامه یادیری.

د n متحوله پولینومو د ښودلو دپاره د یو متحوله پولینومو په شان د تابع گانو د سمبولو څخه کار اخلو. پدی معنی چې $f(x_1, x_2, \dots, x_n), g(x_1, x_2, \dots, x_n), h(x_1, x_2, \dots, x_n), \dots$ لیکو.

بیلگی -

$$f_1(x_1, x_2) = x_1^2 + 5x_1x_2 + 3x_2^2$$

$$f_2(x_1, x_2, x_3) = \sqrt{3}x_1x_2x_3 + 5x_1x_2x_3^2 + 4x_1x_2x_3$$

په هغه صورت کی چې د متحولو شمېر ډیر نه وی ، کولای سو چې هغوی هر یو د الفبی په جلا حروفو سره وښیو. د بیلگی په ډول د $f_1(x_1, x_2)$ پولینوم داسی هم لیکلای سو :

$$f(x, y) = x^2 + 5xy + 3y^2$$

فرضوو چې :

$$f(x_1, x_2, \dots, x_n) = ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} + bx_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} + \dots + cx_1^{\gamma_1} \cdot x_2^{\gamma_2} \cdot \dots \cdot x_n^{\gamma_n} \quad \dots(2)$$

د P پر فیله باندی n متحوله پولینوم دی.

وايو چي د نوموړی پولینوم د $dx_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot \dots \cdot x_n^{\sigma_n}$ او $cx_1^{\delta_1} \cdot x_2^{\delta_2} \cdot \dots \cdot x_n^{\delta_n}$ حدونه یو اوبل ته ورته (یوډبله سره مشابه) دی، که $\delta_n = \sigma_n, \dots, \delta_2 = \sigma_2, \delta_1 = \sigma_1$ وی.

په پورتنۍ بیلگه کې د $f_1(x_1, x_2)$ پولینوم ورته حدونه نلری، خو د $f_2(x_1, x_2, x_3)$ په پولینوم کې د $\sqrt{3}x_1x_2x_3$ او $4x_1x_2x_3$ حدونه سره ورته دی.

وايو چي د $f(x_1, x_2, \dots, x_n)$ پولینوم په سینټرډ يا معیاری شکل راکړه سوی دی که په هغه کې ورته او صفری حدونه وجود ونلری.

د بیلگې په ډول لاندني پولینومونه په معیاری شکل بنودل سوی دی:

$$g(x_1, x_2) = -2x_1^3x_2^2 + \sqrt{3}x_1x_2 + 0,5x_2^5$$

$$h(x_1, x_2, x_3) = x_1x_2x_3 + 5x_1^2x_3 + 6x_2^5x_3$$

د یادولو وړ ده چي د کار د آسانی دپاره د $1 \cdot x_1 \cdot x_2 \cdot x_3$ پر ځای $x_1x_2x_3$ او د $6x_1^0x_2^5x_3, 5x_1^2x_2^0x_3, 0,5x_1^0x_2^5x_3^0$ پر ځای په ترتیب سره $6x_1^5x_3, 5x_1^2x_3, 0,5x_1^0x_2^5x_3^0$ لیکو. په راتلونکي کې د ذکر سو لنډونو (اختصاراتو) څخه کار اخلو. پدی معنی چي په دواړو پولینومو کې د x_1^0 د لیکلو څخه صرف نظر کوو.

د $f(x_1, x_2, \dots, x_n)$ په پولینوم کې مو د $dx_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot \dots \cdot x_n^{\sigma_n}$ او $ex_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot \dots \cdot x_n^{\sigma_n}$ د ورته حدونو د یوځای کیدو څخه مو هدف هغه عملیه ده چي د هغه په نتیجه کې د $(d+e)x_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot \dots \cdot x_n^{\sigma_n}$ یو حد لاسته راځی.

د ورته حدونو د یوځای کیدو او د هغه حدونو چي ضریب یې صفر دی، د منځه وړلو په نتیجه کې نوموړی پولینوم په معیاری شکل ارائه کیږی. هر پولینوم چي په معیاری شکل دراکړه سوی پولینوم څخه لاسته راسی، د راکړه سوی پولینوم سره مساوی دی.

$$f_1(x_1, x_2) = 2x_1^2 + 3x_1x_2 + 5x_2^2 + (-4)x_1x_2 = 2x_1^2 + (-1)x_1x_2 + 5x_2^2 \quad \text{بیلگه ۱ -}$$

د $f(x_1, x_2, \dots, x_n)$ او $g(x_1, x_2, \dots, x_n)$ دوه پولینومه چي په معیاری شکل راکړه سوی دی، یو ډبله سره هغه وخت مساوی دی که د هغوی حدونه په خپل منځ کې ورته او د ورته حدونو ضریبونه سره مساوی وی.

بیلگه ۲-

$$g(x_1, x_2) = i^4x_1^2 + 2(\sin^2 \frac{\pi}{3} + \cos^2 \frac{\pi}{3})x_1x_2 + \text{tg} \frac{\pi}{4} x_2^2 \quad \text{او} \quad f(x_1, x_2) = x_1^2 + 2x_1x_2 + x_2^2$$

پولینومونه یو ډبل سره مساوی دی، ځکه چي $2(\sin^2 \frac{\pi}{3} + \cos^2 \frac{\pi}{3}) = 2, i^4 = 1$ او $\text{tg} \frac{\pi}{4} = 1$ دی.

په آسانی سره لیدل کیږی چي د P پر فیله باندی د $f(x_1, x_2, \dots, x_n)$ هر پولینوم دپاره معیاری ارائه وجودلری او هغه هم په یوازنی شکل تعینیری.

که د $f(x_1, x_2, \dots, x_n)$ پولینوم د P پر فیله باندی راکړه سوی وی ، نو دهغه درجه د x_i ($i=1, 2, \dots, n$) د متحول په اړوند عبارت دی د x_i د لوی ترین طاقت څخه چې په نوموړی پولینوم کی وجود لری . امکان لری چې دغه درجه د صفر سره مساوی وی . پدی معنی که څه هم د $f(x_1, x_2, \dots, x_n)$ پولینوم د x_1, x_2, \dots, x_n متحوله پولینوم دی ، خو د x_i متحول په هغه کی شامل ندی .

د $f(x_1, x_2, \dots, x_n)$ د پولینوم درجه $\alpha_1 x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$ عبارت ده د $\alpha_1 + \alpha_2 + \dots + \alpha_n$ د عدد څخه ، پدی معنی چې عبارت ده په یوه حد کی د ټولو متحولو د طاقتو د جمع د حاصل څخه .

د $f(x_1, x_2, \dots, x_n)$ په پولینوم کی د هر حد درجه چې تر ټولو حدونو لوړه وی ، هغه د نوموړی پولینوم د درجی په نامه یادوو او په $\deg f$ سره یې بنیو . په خاص حالت کی یو متحوله پولینوم ته ورته هغه پولینوم چې درجه یې د صفر سره مساوی وی د P د فیله د صفر څخه خلاف عدد باندی قبلیو . د 0 عدد یوازنی n متحوله پولینوم دی چې د هغه درجه نه تعریف کیږی . د یادولو وړ دی چې یو څو متحوله پولینوم کیدای سی چې د لوړترینی درجی څو حدونه ولری . ځکه نو دیو متحوله پولینومو په څېر د پولینوم د لوړترین حد په هکله نسو برغیدلای ، د بیلگی په ډول د $f(x_1, x_2) = 4x_1^2 + 5x_1x_2 + 4x_1 + 3$ پولینوم دوه حده لری چې د هغوی درجه د 2 سره مساوی کیږی ، یو حد لری چې دهغه درجه مساوی په یوه سره کیږی او د یوه حد درجه یې صفر ده . ځکه نو دراکړه سوی پولینوم درجه مساوی په دوه یعنی $\deg f = 2$ ده .

د P پر فیله باندی د ټولو n متحوله پولینومو سیټ په $P[x_1, x_2, \dots, x_n]$ سره بنیو . د $P[x_1, x_2, \dots, x_n]$ په سیټ کی د جمع او ضرب عملی په لاندی ډول سره تعریفوو :

فرضوو چې د $f(x_1, x_2, \dots, x_n)$ او $g(x_1, x_2, \dots, x_n)$ پولینومونه د P پر فیله باندی په معیاری شکل ارائه سوی دی . پدی صورت کی :

$$f(x_1, x_2, \dots, x_n) = ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} + bx_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} + \dots + cx_1^{\gamma_1} \cdot x_2^{\gamma_2} \cdot \dots \cdot x_n^{\gamma_n}$$

$$g(x_1, x_2, \dots, x_n) = \bar{a}x_1^{\delta_1} \cdot x_2^{\delta_2} \cdot \dots \cdot x_n^{\delta_n} + \bar{b}x_1^{\epsilon_1} \cdot x_2^{\epsilon_2} \cdot \dots \cdot x_n^{\epsilon_n} + \dots + \bar{c}x_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot \dots \cdot x_n^{\sigma_n}$$

دی .

تعریف ۲ - د $f(x_1, x_2, \dots, x_n)$ او $g(x_1, x_2, \dots, x_n)$ د پولینومو د جمع حاصل عبارت دی د $S(x_1, x_2, \dots, x_n)$ د پولینوم څخه پداسی ډول چې :

$$s(x_1, x_2, \dots, x_n) = ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} + bx_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} + \dots + cx_1^{\gamma_1} \cdot x_2^{\gamma_2} \cdot \dots \cdot x_n^{\gamma_n} + \bar{a}x_1^{\delta_1} \cdot x_2^{\delta_2} \cdot \dots \cdot x_n^{\delta_n} + \bar{b}x_1^{\epsilon_1} \cdot x_2^{\epsilon_2} \cdot \dots \cdot x_n^{\epsilon_n} + \dots + \bar{c}x_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot \dots \cdot x_n^{\sigma_n} \quad ..(3)$$

په بله اصطلاح د $S(x_1, x_2, \dots, x_n)$ د پولینوم د محاسبی دپاره د $f(x_1, x_2, \dots, x_n)$ دپولینوم ټول حدونه د $g(x_1, x_2, \dots, x_n)$ د پولینوم د حدونوسره یو ځای لیکو او ورته حدونه یې سره جمع کوو .

بیلگه - فرضوو چې $f(x_1, x_2) = x_1^3 + 3x_1x_2^2$ او $g(x_1, x_2) = -3x_1x_2^2 + x_2^2$ دی . ددوی د جمع حاصل $s(x_1, x_2) = x_1^3 + 3x_1x_2^2 + (-3)x_1x_2^2 + x_2^2 = x_1^3 + x_2^2$ دی .

څرگنده ده چې د دوو پولینومو د جمع حاصل په یکره بڼه لاسته راوړلای سوږد $P[x_1, x_2, \dots, x_n]$ په سیت کی د دوه نیزی عملی عملی کول پداسی ډول چې د $f(x_1, x_2, \dots, x_n)$ او $g(x_1, x_2, \dots, x_n)$ د پولینومو په مقابل د هغوی د جمع حاصل $s(x_1, x_2, \dots, x_n)$ اېږدی، د پولینومو د جمع په نامه یادېږی او په "+" سره ښودل کیږی، یعنی :

$$s(x_1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n) + g(x_1, x_2, \dots, x_n)$$

قضیه ۱- د دوو پولینومو د جمع د حاصل درجه د دواړو را کره سوو پولینومو تر لوړ ترینې درجی اضافه کیدای نسی. پدی معنی چې $\deg s \leq \max\{\deg f, \deg g\}$ دی .

د قضیې رشتیاوالی مستقیماً د پولینومو د جمع د او د پولینومو د درجی د تعریفو څخه استنباط کیږی .

تعریف ۳- د $f(x_1, x_2, \dots, x_n)$ او $g(x_1, x_2, \dots, x_n)$ د پولینومو د ضرب حاصل عبارت دی د

$$p(x_1, x_2, \dots, x_n) = (a\bar{a})x_1^{\alpha_1 + \delta_1} x_2^{\alpha_2 + \delta_2} \dots x_n^{\alpha_n + \delta_n} + \dots + (a\bar{c})x_1^{\alpha_1 + \sigma_1} x_2^{\alpha_2 + \sigma_2} \dots x_n^{\alpha_n + \sigma_n} + \dots + \dots (4)$$

$$+ (c\bar{a})x_1^{\gamma_1 + \delta} x_2^{\gamma_2 + \delta_2} \dots x_n^{\gamma_n + \delta_n} + \dots + (c\bar{c})x_1^{\gamma_1 + \sigma_1} x_2^{\gamma_2 + \sigma_2} \dots x_n^{\gamma_n + \sigma_n}$$

د پولینوم څخه.

په بله اصطلاح ویلای سو چې د $f(x_1, x_2, \dots, x_n)$ او $g(x_1, x_2, \dots, x_n)$ د پولینومو د ضرب حاصل د لمړی پولینوم د ټولو حدونو د ضرب نتیجه د دوهم پولینوم په هر حد کی ده ، پداسی ډول چې مشابه حدونه یوډبل سره جمع کیږی.

بیلگه - فرضوو چې د $f(x, y) = 5x^2y + 3y^3$ او $g(x, y) = 3x + 4y$ پولینومونه را کره سوی دی، نو د هغوی د ضرب حاصل به

$$p(x, y) = (5x^2y + 3y^3)(3x + 4y) = 15x^3y + 20x^2y^2 + 9y^3x + 12y^4$$

وی.

په اسانی سره لیدلای سو چې د دوو پولینومو د ضرب حاصل په یکره بڼه ټاکل کیدای سی.

د $P[x_1, x_2, \dots, x_n]$ په سیت کی د دوه نیزی عملی عملی کول پداسی ډول چې د $f(x_1, x_2, \dots, x_n)$ او $g(x_1, x_2, \dots, x_n)$ د پولینومو په مقابل د هغوی د ضرب حاصل $p(x_1, x_2, \dots, x_n)$ اېږدی، د پولینومو د ضرب په نامه یادېږی او په "•" سره ښودل کیږی، یعنی :

$$p(x_1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n) \cdot g(x_1, x_2, \dots, x_n)$$

قضیه ۲- پر عددی فیلد باندی د ټولو پولینومو سیت $P[x_1, x_2, \dots, x_n]$ نظرد پولینومو د جمع او ضرب و تعریف سوو عملیو ته داسی تبدیلی رینگ دی چې د عینیت عنصر لری او صفری وپشونکی نلری.

ثبوت - د پولینومو د جمع او ضرب د عملیو تبدیلی او اتحادی خاصیتونه او د ضرب د عملیو توزیعی خاصیت نظر د جمع و عملیو ته نېغ په عددی سیتو کی د ذکر سوو خاصیتو د تطبیق او د هغوی د تعریفو څخه استنباط کیدای سی. په حقیقت کی د بیلگي په ډول که :

$$f(x_1, x_2, \dots, x_n) \cdot g(x_1, x_2, \dots, x_n) = (a\bar{a})x_1^{\alpha_1+\delta_1}x_2^{\alpha_2+\delta_2}\dots x_n^{\alpha_n+\delta_n} + \dots + \\ (a\bar{c})x_1^{\alpha_1+\sigma_1}x_2^{\alpha_2+\sigma_2}\dots x_n^{\alpha_n+\sigma_n} + \dots + (c\bar{a})x_1^{\gamma_1-\delta_1}x_2^{\gamma_2-\delta_2}\dots x_n^{\gamma_n-\delta_n} \\ + \dots + (c\bar{c})x_1^{\gamma_1-\sigma_1}x_2^{\gamma_2-\sigma_2}\dots x_n^{\gamma_n-\sigma_n}$$

وی، نو ترهغه ځایه چې $\alpha_1 + \delta_1 = \delta_1 + \alpha_1, \dots, \alpha_n + \delta_n = \delta_n + \alpha_n$ دی او $a\bar{a} = \bar{a}a$ سره کیری ، ځکه نو د پاسني پولینوم او د $p(x_1, x_2, \dots, x_n)$ د پولینوم لمړی حدونه یو دبل سره مساوی دی.

په همدی ډول بی امتحانولای سو چې د ذکر سوی د ضرب د حاصل هر حد د $p(x_1, x_2, \dots, x_n)$ د پولینوم د یوه حد سره مساوی دی او برعکس . همدا ډول نظر د جمع و عملی ته بی تاثیر یا خنثی عنصر عبارت دی له صفری پولینوم څخه . یعنی

$$f(x_1, x_2, \dots, x_n) + 0 = f(x_1, x_2, \dots, x_n)$$

د $f(x_1, x_2, \dots, x_n)$ و پولینوم ته متضاد عنصر عبارت دی له:

$$\Psi(x_1, x_2, \dots, x_n) = (-a)x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} + (-b)x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} + \dots + (-c)x_1^{\gamma_1} \cdot x_2^{\gamma_2} \cdot \dots \cdot x_n^{\gamma_n}$$

څخه . په رشتیا هم : $f(x_1, x_2, \dots, x_n) + \Psi(x_1, x_2, \dots, x_n) = 0$ سره کیری .

د $P[x_1, x_2, \dots, x_n]$ په رینګ کی هغه پولینوم چې درجه یی صفر وی ، یعنی (د یوه عدد) د عینیت د عنصر وظیفه پر غاړه لری. په حقیقت کی $f(x_1, \dots, x_n) \cdot 1 = f(x_1, \dots, x_n)$ سره کیری.

فرضوو چې $f(x_1, x_2, \dots, x_n)$ او $g(x_1, x_2, \dots, x_n)$ د صفر څخه خلاف پولینومونه دی ، $\bar{a} \neq 0$ او $a \neq 0$ دی. ځکه نو د هغوی د ضرب په نتیجه کی د $p(x_1, x_2, \dots, x_n)$ د پولینوم د $a\bar{a}$ ضریب هم د صفر څخه خلاف دی . پدی معنی چې $p(x_1, x_2, \dots, x_n) \neq 0$ دی . ددی ځایه استدلال کولای سو چې د $P[x_1, x_2, \dots, x_n]$ په رینګ کی د صفر وپشونکی وجود نلری.

پدی ترتیب قضیه په بشپړ توګه په ثبوت ورسیده.

د یادلو وړ ده چې د $P[x_1, x_2, \dots, x_n]$ رینګ د P پر عددی فیلډ باندی د یو متحوله پولینومو $P[x_1]$ د رینګ څخه د استقرار د طریقې څخه په استفادی سره جوړولای سو. پدی صورت کی لازمه ده چې د یو متحوله پولینومو د رینګ په جوړښت پر اٹیګرال دومین ، یعنی پر داسی تبدیلی رینګ چې د عینیت عنصر ولری خو د صفر وپشونکی ونلری ، پوه سو.

پدی ترتیب د پولینومو د جمع او ضرب د عملیو په هکله ، هر هغه څه چې په اختیاری رینګ کی حقیقت لری ، صدق کوی.

د $f(x_1, \dots, x_n)$ پولینوم د متجانس پولینوم په نامه یادوو که د هغه د ټولو حدونو درجه سره مساوی وی. د بېلګې په ډول $f(x, y) = 9x^4 + x^3y + x^2y^2$ یو متجانس پولینوم دی چې درجه یې مساوی په څلور سره ده.

موږ کولای سو چې هر n متحوله پولینوم د متناهی شمېر متجانسو پولینومو د جمع په شکل ارائه کړو. د بېلګې په ډول د $f(x, y, z) = x^5 + xy^4 + 3x^2y^2 + 4xyz^2 + 9z$ پولینوم د لاند نیو متجانسو پولینومو جمع ده:

$$g_1(x, y, z) = x^5 + xy^4$$

$$g_2(x, y, z) = 3x^2y^2 + 4xyz^2$$

$$g_3(x, y, z) = 9z$$

قضیه ۳- د دوو پولینومو ، چې دصفر څخه خلاف وی ، د ضرب د حاصل درجه د هغوی د درجو د جمع په حاصل سره مساوی کیږی. پدی معنی چې :

$$\text{deg}(f \cdot g) = \text{deg } f + \text{deg } g \quad \text{که } f \neq 0 \text{ او } g \neq 0 \text{ وی ، نو}$$

ثبوت - که د $f(x_1, \dots, x_n)$ او $g(x_1, \dots, x_n)$ پولینومونه متجانس ، $\text{deg } f = k$ او $\text{deg } g = m$ وی . نو دهغوی د ضرب حاصل ، یعنی د $p(x_1, \dots, x_n)$ پولینوم هم متجانس دی او

$$\text{deg } p = k + m = \text{deg } f + \text{deg } g$$

دی.

فرضوو چې د $f(x_1, \dots, x_n)$ او $g(x_1, \dots, x_n)$ پولینومونه د متجانسو پولینومو د جمع په شکل ارائه سوی دی. پدی معنی چې :

$$f(x_1, \dots, x_n) = h_1(x_1, \dots, x_n) + \dots + h_s(x_1, \dots, x_n)$$

$$g(x_1, \dots, x_n) = \varphi_{m_1}(x_1, \dots, x_n) + \dots + \varphi_{m_r}(x_1, \dots, x_n)$$

پداسی حال کی چې $\text{deg } h_i = l_i$ ($1 \leq i \leq s$) او $\text{deg } \varphi_{m_j} = m_j$ ($1 \leq j \leq r$)، دی . څرګنده ده چې

$$\text{deg } f = \max\{l_1, l_2, \dots, l_s\} \quad \text{او} \quad \text{deg } g = \max\{m_1, m_2, \dots, m_r\}$$

مو نقض کړی وی ، فرضوو چې $\text{deg } f = l_1$ او $\text{deg } g = m_1$ دی . اوس به نو د $f(x_1, \dots, x_n)$ او $g(x_1, \dots, x_n)$ پولینومونه سره ضرب کړو:

$$f(x_1, \dots, x_n) \cdot g(x_1, \dots, x_n) = h_1(x_1, \dots, x_n) \cdot \varphi_{m_1}(x_1, \dots, x_n) + \dots +$$

$$h_s(x_1, \dots, x_n) \cdot \varphi_{m_r}(x_1, \dots, x_n)$$

څرنګه چې د $h_i(x_1, \dots, x_n) \cdot \varphi_{m_j}(x_1, \dots, x_n)$ ټوله پولینومونه متجانس دی او د هغوی درجه په

ترتیب سره $l_i + m_j$ ده ، نو څرګنده ده چې $l_1 + m_1 = \text{deg } p = \text{deg } f + \text{deg } g$ سره کیږی.

په پای کی بیا هم د یادولو وړ ده چې د (1) افاده مو د سمبولیکي څرګندونی په صفت قبول کړی وه . همداراز په (4) افاده کی د n متحوله پولینومو د جمع او ضرب د تعریفونو په نظر کی نیولوسره د جمع

"+" د عملیې څخه مو هدف د پولینومو د دوو حدو جمع کول او هریو د $ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$ څخه مو هدف د a او $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$ د پولینومو ضرب دی.

مور کولای سو چي د n متحوله پولینوم مفهوم د تابع په بڼه هم تعريف کړو.

د P پر فیلډ باندی د x_n, \dots, x_2, x_1 ، n متحوله پولینوم عبارت دی د $f: P^n \rightarrow P$ مپینګ څخه چي (2) مساوات پذیریه ارائه سوی دی.

د یو متحوله پولینومو تیوری ته ورته ثابتولای سو چي د P پر عددی فیلډ باندی د n متحوله پولینومو الجبری او تابعی تعریفونه سره معادل دی.

II§. د n متحوله پولینوم د حدونو قاموسی (الفبایی⁴ Lexicographic) ترتیب

فرضوو چي د P پر عددی فیلډ باندی د

$$f(x_1, x_2, \dots, x_n) = ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} + bx_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} + \dots + cx_1^{\gamma_1} \cdot x_2^{\gamma_2} \cdot \dots \cdot x_n^{\gamma_n} \dots (1)$$

n متحوله پولینوم په معیاری بڼه (ستندرد شکل) راکړه سوی دی، پدی معنی چي دهغه د حدونو په منځ کی مشابه حدونه وجود نلری. د یو متحوله پولینوم په هکله هدف مو د معیاری بڼی څخه داوو چي پولینوم د هغه د متحول د طاقت له مخی په نزولی شکل تنظیم سوی وی (د پنځم فصل ، I§ وگوری) ، خو په n متحوله پولینوم کی امکان لری چي ځنی (یا ټوله) حدونه د طاقت له مخی سره مساوی وی. طبعاً سوال پیدا کیری چي څه ډول کولای سو چي د n متحوله پولینوم (1) حدونه ترتیب کړو؟ د $f(x_1, \dots, x_n)$ د پولینوم د حدونو د ترتیب یوه ساده طریقہ قاموسی Lexicographic ترتیب دی. پدی حالت کی د لمړی ، دوهم ، دریم ، حرف رول x_n, \dots, x_2, x_1 لوبوی او د قاموسی اوډنی پرنسیب پر i - یم حرف باندی د نوموړی متحول x_i پر طاقت باندی عملی کیری.

د (1) پولینوم دوه اختیاری حدونه $T_1 = dx_1^{\delta_1} \cdot x_2^{\delta_2} \cdot \dots \cdot x_n^{\delta_n}$ او $T_2 = lx_1^{\sigma_1} \cdot x_2^{\sigma_2} \cdot \dots \cdot x_n^{\sigma_n}$ څپرو. څرنګه چي د $f(x_1, \dots, x_n)$ د پولینوم په (1) بڼودنه کی ورته حدونه وجود نلری ، نو د σ_i او δ_i ټوله طاقتونه په خپل منځ کی سره مساوی ندی، پدی معنی چي داسی j ($1 \leq j \leq n$) وجود لری چي $\delta_{j-1} = \sigma_{j-1}, \dots, \delta_2 = \sigma_2, \delta_1 = \sigma_1$ او $\delta_j \neq \sigma_j$ دی.

تعریف ۱- د T_1 حد د T_2 تر حد لوړ دی که $\delta_1 = \sigma_1, \delta_2 = \sigma_2, \dots, \delta_{j-1} = \sigma_{j-1}$ او $\delta_j > \sigma_j$ وی. همدا ډول که $\delta_1 = \sigma_1, \delta_2 = \sigma_2, \dots, \delta_{j-1} = \sigma_{j-1}$ او $\delta_j < \sigma_j$ وی ، نو وایو چي د T_2 حد د T_1 تر حد لوړ دی. څرګنده ده چي د $f(x_1, \dots, x_n)$ د پولینوم د دوو حدو څخه یو تر بل لوړ دی.

قضیه ۱- د $f(x_1, \dots, x_n)$ د پولینوم د ټولو حدونو پر سیټ باندی د حدونو د لوړوالی دوه نېزه اړیکه د ترتیب دقیقه خطی اړیکه ده .

⁴ د Lexicographic کلمه د لاتینی اصطلاح Lexicon چي د قاموس په معنی ده اخیستل سوی ده . لکه څنګه چي معلومه ده ، په قاموس کی لغاتونه د الفبی پر اساس اوډل سوی دی . یعنی په هغه صورت کی چي دوه مختلف لغتونه راکړه سوی وی ، نو د هغوی لمړی حرفونه سره پرتله کو و او که د هغوی لمړی حرفونه سره یو وی بیا نو د هغوی دوهم حرف سره مقایسه کوو

ثبوت - د لمړی تعريف څخه نتیجه اخیستل کيږی چې د $f(x_1, \dots, x_n)$ د پولینوم هېڅ حد تر خپل ځان لور ندی. پدی معنی چي دغه اړیکه ضد انعکاسی ده. همدا ډول که د T_1 حد د T_2 تر حد لوروی ، نو د T_2 حد د T_1 تر حد نسې لوریدای. پدی معنی چي د لوړوالی اړیکه ضد تناظری ده . علاوه پردی د « د T_1 حد د T_2 تر حد لوردی» او « د T_2 حد د T_3 تر حد لوردی» د ادعاؤ څخه استنباط کيږی چې « د T_1 حد د T_3 تر حد لوردی». پدی معنی چي د «لوړوالی» اړیکه انتقالی ده. بلاخره ، لکه مخ کی چي مو وویل د پولینوم ددو حدو څخه تل یو تر بل لور دی ، پدی معنی چي د «لوړوالی» اړیکه د خطی ترتیب اړیکه ده.

د ثابتی سوی قضیې څخه استنباط کيږی چې د $f(x_1, \dots, x_n)$ د پولینوم حدونه د (1) په سټنډرډ بنودنه کی پر یوه کرښه داسی اوډل سوی دی چې د $f(x_1, \dots, x_n)$ په پولینوم کی لوړترینه حدونه تر کښته ترینو حدو تر مخه ځای پر ځای سوی دی. دغه ډول ترتیب یا د $f(x_1, \dots, x_n)$ د پولینوم د حدونو اوډنه د قاموسی ترتیب په نامه یاديږی.

بیلگه - د $f(x_1, x_2, x_3) = x_1^4 x_2^2 x_3^3 - 2x_1^3 + 3x_1 x_2^3 x_3^4 - x_2 x_3 + 4x_3$ د پولینوم د قاموس په شکل ترتیب سوی دی. یا په بله اصطلاح نوموړی پولینوم په قاموسی شکل راکړه سوی دی.

د پولینوم د حدونو په قاموسی ترتیب کی کله چي یو حد تر نورو حدونو لوړ وی ، نو هغه د لوړترین حد په نامه یادوو. په پورتنی بیلگه کی د $x_1^4 x_2^2 x_3^3$ حد د نوموړی پولینوم لوړ ترین حد دی.

قضیه ۲- (د لوړترین حد په هکله)

د دوو n متحوله پولینومو د ضرب د حاصل لوړترین حد ددواړو پولینومو د لوړترینو حدو د ضرب په حاصل سره مساوی کيږی.

ثبوت - فرضوو چې د $f(x_1, \dots, x_n)$ او $g(x_1, \dots, x_n)$ پولینومونه چي په قاموسی بڼه ترتیب سوی دی ، د $f(x_1, \dots, x_n)$ د پولینوم د (1) په شکل او د $g(x_1, \dots, x_n)$ د پولینوم په لاندی شکل راکړه سوی دی.

$$g(x_1, x_2, \dots, x_n) = mx_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_n^{k_n} + nx_1^{l_1} \cdot x_2^{l_2} \cdot \dots \cdot x_n^{l_n} + \dots + px_1^{t_1} \cdot x_2^{t_2} \cdot \dots \cdot x_n^{t_n}$$

فرضوو چي پورتنی پولینومونه یوډبل سره ضرب سوی دی . د یادونی وړ ده چي د

$T = dx_1^{\delta_1} \cdot x_2^{\delta_2} \cdot \dots \cdot x_n^{\delta_n}$ په حد کی د $f(x_1, \dots, x_n)$ د پولینوم د ضرب په نتیجه کی د پولینوم قاموسی ترتیب ساتل کيږی .

د $f(x_1, \dots, x_n) \cdot g(x_1, \dots, x_n)$ د ضرب عملیه داسی سرته رسوو چي د $f(x_1, \dots, x_n)$ هر حد د $g(x_1, \dots, x_n)$ د پولینوم په لمړی حد (یعنی لوړترین حد) کی ضربوو ، وروسته بیا په دوهم ، دریم ... او داسی نور ، کی ضربوو څو لاندنی نتیجه لاسته راسی:

$$\begin{aligned} f(x_1, \dots, x_n) \cdot g(x_1, x_2, \dots, x_n) &= f(x_1, \dots, x_n) mx_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_n^{k_n} + \\ & f(x_1, \dots, x_n) nx_1^{l_1} \cdot x_2^{l_2} \cdot \dots \cdot x_n^{l_n} + \dots + \\ & f(x_1, \dots, x_n) px_1^{t_1} \cdot x_2^{t_2} \cdot \dots \cdot x_n^{t_n} \end{aligned}$$

د مخکنې یادونې د اسیتنه د $f(x_1, \dots, x_n)nx_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_n^{k_n}$ ، $f(x_1, \dots, x_n)nx_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_n^{k_n}$ ، $f(x_1, \dots, x_n)px_1^{l_1} \cdot x_2^{l_2} \cdot \dots \cdot x_n^{l_n}$ د حدونو په هر ګروپ کې قاموسی ترتیب تغیر نه کوی. ځکه

نو لوړترین حد یې د حدونو په ګروپ کې د لوړترینو حدونو د ضرب حاصل دی. پدې معنی چې لوړترین حد به د لاندنیو حدونو په منځ کې وی .

$$a \cdot mx_1^{\alpha_1 - k_1} \cdot x_2^{\alpha_2 + k_2} \cdot \dots \cdot x_n^{\alpha_n + k_n}, a \cdot nx_1^{\alpha_1 - l_1} \cdot x_2^{\alpha_2 - l_2} \cdot \dots \cdot x_n^{\alpha_n - l_n}, \dots, a \cdot px_1^{\alpha_1 + l_1} \cdot x_2^{\alpha_2 + l_2} \cdot \dots \cdot x_n^{\alpha_n + l_n}$$

خو پورتنی حدونه داسې اوډل سوی دی چې ګواکې د $g(x_1, \dots, x_n)$ پولینوم چې په قاموسی بڼه ترتیب سوی دی د $ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$ په حد کې ضرب سوی وی. ځکه نو لوړترین حد یې عبارت دی له $a \cdot mx_1^{\alpha_1 + k_1} \cdot x_2^{\alpha_2 + k_2} \cdot \dots \cdot x_n^{\alpha_n + k_n}$ څخه ، چې د دواړو پولینومو د لوړترینو حدو د ضرب په نتیجه کې لاسته راغلی دی.

د ثابتې سوی قضیې څخه وروسته د متناظرو پولینومو په څېرته کې کار اخلو. نوموړی قضیه د لوړترین حد د لیمای په نامه هم یادېږی.

د n متحوله پولینومو حدونه غیر له قاموسی ترتیب څخه اکثراً په بله بڼه چې هغه عبارت د یوه متحول د طاقت پر اساس د حدود اوډلو څخه. پدې حالت کې د P پر فیله باندې د $f(x_1, \dots, x_n)$ پولینوم په لاندې ډول سره اړانه کولای سو.

$$f(x_1, \dots, x_n) = g_s(x_1, \dots, x_{p-1}, x_{p+1}, \dots, x_n)x_p^s + g_{s-1}(x_1, \dots, x_{p-1}, x_{p+1}, \dots, x_n)x_p^{s-1} + \dots + g_0(x_1, \dots, x_{p-1}, x_{p+1}, \dots, x_n)$$

پداسې حال کې چې د $g_i(x_1, \dots, x_{p-1}, x_{p+1}, \dots, x_n)$ ، $0 \leq i \leq s$ ضریبونه د $x_1, \dots, x_{p-1}, x_{p+1}, \dots, x_n$ متحوله پولینومونه دی.

د بیلګې په توګه د مخکنې بیلګې پولینوم د x_3 د متحول د طاقت پر اساس په لاندې ډول اوډلای سو:

$$f(x_1, x_2, x_3) = 3x_1x_2^3x_3^4 + x_1^4x_2^2x_3^3 + (4 - x_2)x_3 + 2x_1^3$$

III. د n متحوله پولینومو دوپش ورتوب

د پولینومو دوپش ورتوب ډیر مسائل د P پر فیله باندې د n متحوله پولینومو په تیوری کې خائته عمومی بڼه غوره کوی. په خاص ډول هغه مفهومونه لکه دوپش ورتوب ، وپشونکې ، دوپش د ورتوب عمومی خاصیتونه او د نه تجزیه کیدونکې پولینوم مفهوم او دهغه خاصیتونه کولای سو د n متحوله پولینومو دپاره بیله کوم تغیر څخه تعریف کړو. ذکر سوی تعریفونه او خصوصیات بیله ثبوت او تبصری څخه دلته راوړو.

تعریف ۱- فرضوو چې $f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in P[x_1, \dots, x_n]$ وی. وایو چې د $f(x_1, \dots, x_n)$ پولینوم د صفر څخه خلاف پولینوم $g(x_1, \dots, x_n)$ باندې دوپش ورتوب دی که د P پر فیله باندې د $s(x_1, \dots, x_n)$ پولینوم داسې وجود ولری چې $f(x_1, \dots, x_n) = g(x_1, \dots, x_n) \cdot s(x_1, \dots, x_n)$ وی.

دغه حقيقت چي د $f(x_1, \dots, x_n)$ پولينوم د صفر څخه خلاف پولينوم $g(x_1, \dots, x_n)$ باندی د وېش وړ دی ، په ساده شکل $f: g$ باندی نښو. په لمړی تعريف کی د $g(x_1, \dots, x_n)$ پولينوم د $f(x_1, \dots, x_n)$ د پولينوم د وېشونکی په نامه يادوو.

د n متحوله پولينومو د وېش د وړتوب اړیکه لاندنی خاصیتونه لری:

1. $(\forall f, g, h \in P[x_1, \dots, x_n])(f: g \wedge g: h \rightarrow f: h)$.
2. $(\forall f, g, h \in P[x_1, \dots, x_n])(f: g \wedge g: h \rightarrow (f + g): h \wedge (f - g): h)$.
3. $(\forall f, h \in P[x_1, \dots, x_n])(f: h \rightarrow (\forall g \in P[x_1, \dots, x_n])(f \cdot g: h)$.
4. $(\forall h, f_1, f_2 \in P[x_1, \dots, x_n])(f_1: h \wedge f_2: h \rightarrow (\forall g_1, g_2 \in P[x_1, \dots, x_n])(f_1 g_1 + f_2 g_2: h))$.
5. $(\forall f \in P[x_1, \dots, x_n])(\forall c \in P / \{0\})(f: c)$.
6. $(\forall f, g \in P[x_1, \dots, x_n])(\forall c \in P / \{0\})(f: g \rightarrow f: cg)$.

تعريف ۲ - د P پر فيلډ باندی د $f(x_1, \dots, x_n)$ پولينوم د نه تجزیه کيدونکی پولينوم په نامه يادوو ، که :

1. $\text{dcg} f(x_1, \dots, x_n) \geq 1$
2. $(\forall u, v \in P[x_1, \dots, x_n])(f = u \cdot v \rightarrow \text{dcg} u = 0 \vee \text{dcg} v = 0)$

تعريف ۳ - د P پر فيلډ باندی د $f(x_1, \dots, x_n)$ پولينوم د تجزیه کيدونکی پولينوم په نامه يادوو ، که :

1. $\text{deg} f(x_1, \dots, x_n) \geq 1$
2. $(\exists u, v \in P[x_1, \dots, x_n])(f = u \cdot v \rightarrow \text{deg} u \geq 1 \wedge \text{deg} v \geq 1)$

د P پر فيلډ باندی نه تجزیه کيدونکی پولينومونه لاندنی خاصیتونه لری:

1- د P پر فيلډ باندی د $f(x_1, \dots, x_n)$ هر پولينوم چي درجه يی مساوی په يوه سره وی ، نه تجزیه کيدونکی دی.

2- که د P پر فيلډ باندی د $f(x_1, \dots, x_n)$ پولينوم نه تجزیه کيدونکی وی او $c \in P / \{0\}$ وی ، نو د $c \cdot f(x_1, \dots, x_n)$ هم د P پر فيلډ باندی نه تجزیه کيدونکی دی.

3- که د P پر فيلډ باندی د $f(x_1, \dots, x_n), p(x_1, \dots, x_n) \in P[x_1, \dots, x_n]$ نه تجزیه کيدونکی پولينومونه وی، نو يا $f: p$ دی او يا د هغوی مشترک وېشونکی د P د فيلډ څخه يو عدد دی.

ثابتولای سو چي د $P[x_1, \dots, x_n]$ په رينگ کی هر n متحوله پولينوم په يوازنی شکل د نه تجزیه کيدونکو پولينومو د ضرب په حاصل باندی تجزیه کولای سو. د ذکر سوی واقعیت ثبوت د $P[x_1, \dots, x_n]$ په رينگ کی په کافی اندازه پېچلی دی ، ځکه چي د $P[x_1, \dots, x_n]$ په رينگ کی چي $n \geq 2$ وی ، د اقلیدس د الگوريتم او د هغه د نتېجو څخه کار نسو اخیستلای.

IV§. متناظر پولينومونه او د هغوی خاصیتونه

متناظر پولينومونه چي په دغه او راتلونکی پاراگراف کی تر مطالعی لاندی نښو ، د n متحوله پولينومو په منځ کی ډير مهم رول لوبوی.

تعريف ۱-د P پر فيلډ باندې د $f(x_1, \dots, x_n)$ پولينوم د متناظر پولينوم په نامه يادېږي ، که دهغه د متحولو د اختياري تعويض په نتيجه کې په پولينوم کې کوم تغيير رانسې.

بيلگې - ۱- د $f_1(x_1, x_2) = x_1^3 + x_2^3$ پولينوم متناظر دی ، ځکه چې :

$$f_1(x_1, x_2) = f_1(x_2, x_1)$$

۲- د $f_2(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - 2x_1x_2x_3$ پولينوم متناظر دی . ځکه چې :

$$\begin{aligned} f_2(x_1, x_2, x_3) &= f_2(x_3, x_1, x_2) = f_2(x_2, x_3, x_1) = f_2(x_1, x_3, x_2) \\ &= f_2(x_3, x_2, x_1) = f_2(x_2, x_1, x_3) \end{aligned}$$

۳- د $f_3(x_1, x_2) = x_1 + 2x_1x_2$ پولينوم متناظر پولينوم ندي ، يا په بله اصطلاح نوموړی پولينوم غير متناظر دی. ځکه چې : $f_3(x_2, x_1) = x_2 + 2x_2x_1$ دی او $f_3(x_1, x_2) \neq f_3(x_2, x_1)$ دی.

متناظر n متحوله پولينومونه لاندني خاصيتونه لري :

لمړی خاصيت - د P پر فيلډ باندې د n متحوله متناظرو پولينومو د جمع ، تفريق او ضرب حاصل متناظر پولينوم دی.

په رشتيا هم ، که د $f(x_1, \dots, x_n)$ او $g(x_1, \dots, x_n)$ پولينومونه د P پر فيلډ باندې متناظر وي ، نو د :

$$s(x_1, \dots, x_n) = f(x_1, \dots, x_n) + g(x_1, \dots, x_n),$$

$$h(x_1, \dots, x_n) = f(x_1, \dots, x_n) - g(x_1, \dots, x_n),$$

$$p(x_1, \dots, x_n) = f(x_1, \dots, x_n) \cdot g(x_1, \dots, x_n).$$

په پولينومو کې د x_n, \dots, x_2, x_1 د متحولو د اختياري اوښتونو په نتيجه کې کوم تغيير نه راځي. پدې معنی چې د $h(x_1, \dots, x_n), s(x_1, \dots, x_n)$ او $p(x_1, \dots, x_n)$ پولينومونه هم متناظر دي.

نتيجه - د P پر فيلډ باندې د n متحوله متناظرو پولينومو سيټ د $P[x_1, \dots, x_n]$ د رينگ سپرينگ جوړوي.

پورتنی نتېجه د لمړی خاصيت او د (درېم فصل ، IS) د قضیې څخه استنباط کېږي . څرگنده ده چې نوموړی سپرينگ د عينيت عنصر $f(x_1, \dots, x_n) \equiv 1$ په ځان کې لري او د صفر وېشونکي ندي پکښې نغښتي .

دوهم خاصيت - که د $f(x_1, \dots, x_n)$ متناظر پولينوم د (1) $\dots \cdot x_n^{\alpha_n} \cdot \dots \cdot x_j^{\alpha_j} \cdot \dots \cdot x_i^{\alpha_i} \cdot \dots \cdot x_2^{\alpha_2} \cdot \dots \cdot x_1^{\alpha_1}$ په څېر يو حد ولري ، نو نوموړی پولينوم هر حد چې د (1) څخه د $\alpha_1, \alpha_2, \dots$ د طاقتو د اوښتنو (تعويض) په نتيجه کې لاسته راځي ، په ځان کې لري.

ثبوت - څرگنده ده (لمړی برخه ، څلورم فصل ، §V وگورئ) چې د $\alpha_1, \alpha_2, \dots, \alpha_n$ تعويض د متناهي ترانسپوزيشنو په نتيجه کې يعنی د مخکنی تعويض په پرته ، بل تعويض د دوو عددو د ځايو د اليشولو په نتيجه کې لاسته راځي . ځکه نو کافي ده چې په ثبوت يې ورسوو چې د $\alpha_1, \alpha_2, \dots, \alpha_n$ په حد کې د دوو اختياري طاقتو د ترانسپوزيشن په نتيجه کې

بیا هم د $f(x_1, \dots, x_n)$ د پولینوم یو حد لاسته راځی . د بیلګې په توګه د α_j او α_i د ځایو د تبدیلولو په نتیجه کې لاندنی حد لاسته راځی:

$$ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_{i-1}^{\alpha_{i-1}} \cdot x_j^{\alpha_j} \cdot x_{i+1}^{\alpha_{i+1}} \cdot \dots \cdot x_{j-1}^{\alpha_{j-1}} \cdot x_i^{\alpha_i} \cdot x_{j+1}^{\alpha_{j+1}} \cdot \dots \cdot x_n^{\alpha_n} \dots (2)$$

د متناظر پولینوم د تعریف پر اساس

$$f(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = f(x_1, \dots, x_{i-1}, x_j, x_{i+1}, \dots, x_{j-1}, x_i, x_{j+1}, \dots, x_n)$$

دی. د مساوات په نښې خوا کې پولینوم (2) حد په ځان کې لری. څرنګه چې نوموړی حد د (1) څخه د x_i او x_j د ځایو د ایشولو په نتیجه کې لاسته راغلی دی. څرنګه چې د پولینوم سټنډرډ اړانه یوازنی شکل لری نو راکړه سوی پولینوم د (2) حد هم په ځان کې لری.

نتیجه - که (3) $ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_i^{\alpha_i} \cdot x_{i+1}^{\alpha_{i+1}} \cdot \dots \cdot x_n^{\alpha_n} \dots$ د $f(x_1, \dots, x_n)$ متناظر پولینوم لوړترین حد وی ، نو $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$ دی.

په رشتیا هم که فرض کړو چې i داسی وجود لری چې $\alpha_i < \alpha_{i+1}$ دی. نظر و دوهم خاصیت ته باید ذکر سوی پولینوم د (4) $ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_{i+1}^{\alpha_{i+1}} \cdot x_i^{\alpha_i} \cdot \dots \cdot x_n^{\alpha_n} \dots$ حد هم ولری. خو نظر د $\alpha_i < \alpha_{i+1}$ د شرط له مخې (4) حد تر (3) حد لوړ دی. خو (3) د $f(x_1, \dots, x_n)$ د پولینوم لوړترین حد دی. ددی حالت په نتیجه کې د ټولو $1 \leq i \leq n-1$ دپاره $\alpha_i \geq \alpha_{i+1}$ دی .

د متناظرو پولینومو په منځ کې ابتدائی متناظر پولینومونه اساسی رول لوبوی.

تعریف ۲- د

$$\sigma_1(x_1, x_2, \dots, x_n) = x_1 + x_2 + \dots + x_n$$

$$\sigma_2(x_1, x_2, \dots, x_n) = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n$$

⋮

$$\sigma_n(x_1, x_2, \dots, x_n) = x_1 \cdot x_2 \cdot \dots \cdot x_n$$

پولینومونه د n متحوله ابتدائی متناظر پولینومو په نامه یادیری.

په هغه صورت کې چې د موضوع د متن څخه څرګنده وی ، په آینده کې به د څو متحوله پولینومو په هکله برغیرو. ابتدائی متناظر پولینومونه به په مختصر ډول په $\sigma_n, \dots, \sigma_2, \sigma_1$ سره وښیو.

د ابتدائی متناظر پولینومو سره د ښونځي په وخت د وینا د فارمول په شکل مخامخ سوی یاست . په حقیقت کې مو د دوهمی درجی دمعادلی $x^2 + px + q = 0$ د x_1 او x_2 د جذرو دپاره لاندنی مساواتونه صدق کوی:

$$x_1 + x_2 = -p$$

$$x_1 x_2 = q$$

پدی معنی چې $\sigma_1(x_1, x_2) = -p$ او $\sigma_2(x_1, x_2) = q$ دی.

د لمړی خاصیت څخه استنباط کيږی چې هر ابتدائي متناظر پولینوم چې په مثبت طاقت لور سی ، بیا هم ابتدائي متناظر پولینوم دی . نوموړی حقیقت د اختیاری تعداد ابتدائي متناظر پولینومو د جمع او ضرب په هکله هم صدق کوی . په بله اصطلاح هر پولینوم چې د $\sigma_1, \sigma_2, \dots, \sigma_n$ ابتدائي متناظر پولینومو څخه چې ضریبونه یې د P د فیلډ څخه وی ، لاسته راسی د x_1, x_2, \dots, x_n متحوله پولینوم په څیر څیرل کيږی ، چې هغه هم متناظر پولینوم دی .

ددغی قضیې برعکس ثبوت عملی اهمیت لری چې په راتلونکی پاراگراف کی به یې وڅېړو .

V§. د متناظرو پولینومو د تیوری اساسی قضیه

فرضو چې د P پر عددی فیلډ باندی لاندنی متناظر پولینوم راکړه سوی دی:

$$f(x_1, x_2, \dots, x_n) = ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} + bx_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} + \dots + cx_1^{\gamma_1} \cdot x_2^{\gamma_2} \cdot \dots \cdot x_n^{\gamma_n} \dots (1)$$

د (1) پولینوم د متجانس پولینوم په نامه یادووکه دهغه ټول حدونه مساوی طاقت ولری . د بیلگی په ډول:

$$f(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 + 3x_1x_2x_3$$

متجانس پولینوم دی ، ځکه چې هر حد یې د درو په طاقت دی .

په اسانی سره لیدل کيږی چې هر (1) پولینوم د متناظرو متجانسو پولینومو د جمع په شکل ارائه کولای سو . پدغه ډول جمع کی د اجزاوو تعداد د راکړه سوی پولینوم تر طاقت اضافه نه وی .

په حقیقت کی لمړی باید ټوله هغه حدونه سره جمع کړو چې طاقت مساوی په یوه سره وی ، بیا هغه حدونه سره جمع کړو چې طاقت مساوی په دوه ، ... او داسی نور ، وی . دبیلگی په ډول که :

$$f(x_1, x_2) = x_1^5 + x_2^5 + 2x_1^2x_2 + 2x_1x_2^2 + x_1 + x_2$$

وی ، نو :

$$f_1(x_1, x_2) = x_1 + x_2$$

$$f_2(x_1, x_2) = 2x_1^2x_2 + 2x_1x_2^2$$

$$f_3(x_1, x_2) = x_1^5 + x_2^5$$

متجانس پولینومونه دی . پداسی ډول چې :

$$f(x_1, x_2) = f_3(x_1, x_2) + f_2(x_1, x_2) + f_1(x_1, x_2)$$

همدا ډول دیادونی وړ ده چې د (1) په پولینوم کی د ټولو حدو شمېر چې درجه یې ثابت نه وی ، متناهی دی . لکه په مخکنی بیلگه کی چې مو ولیدل د $f(x_1, x_2)$ پولینوم دوه حده لری چې درجه یې یوه ده او دوه دوه حده لری چې درجه یې دری او پنځه ده . نور حدونه چې درجه یې د ذکر سویو درجو څخه خلاف وی په نوموړی پولینوم کی وجود نلری .

تحلیل سوی موضوع مورته د اساسی قضیې ثبوت اسانه کوی .

قضیه ۱-۱ د P پر عددی فیلد باندی هر n متحولہ متناظر پولینوم $f(x_1, \dots, x_n)$ د ابتدائی متناظرو پولینومو $\sigma_n, \dots, \sigma_2, \sigma_1$ پذیرعه داسی ارانه کیدای سی چي ضریبونه یی د P په فیلد کی دی.

ثبوت - بیله دی چي عمومیت مو نقض کری وی فرضوو چي راکړه سوی متناظر پولینوم

$$f(x_1, x_2, \dots, x_n) = ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} + bx_1^{\beta_1} \cdot x_2^{\beta_2} \cdot \dots \cdot x_n^{\beta_n} + \dots + cx_1^{\gamma_1} \cdot x_2^{\gamma_2} \cdot \dots \cdot x_n^{\gamma_n}$$

متجانس دی او $ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$ لوړ ترین حد دی. د

$$g(x_1, x_2, \dots, x_n) = a\sigma_1^{\alpha_1 - \alpha_2} \cdot \sigma_2^{\alpha_2 - \alpha_3} \cdot \dots \cdot \sigma_{n-1}^{\alpha_{n-1} - \alpha_n} \cdot \sigma_n^{\alpha_n}$$

پولینوم څپرو. نوموړی پولینوم متناظر او متجانس دی ، ځکه چي د $\sigma_n, \dots, \sigma_2, \sigma_1$ د پولینومو څخه هر یو متناظر او متجانس دی . د $g(x_1, \dots, x_n)$ پولینوم لوړترین حد عبارت دی د $a\sigma_1^{\alpha_1 - \alpha_2}$ ، $\sigma_2^{\alpha_2 - \alpha_3}$ ، ... ،

$\sigma_{n-1}^{\alpha_{n-1} - \alpha_n}$ او $\sigma_n^{\alpha_n}$ د پولینومو د لوړترینو حدو د ضرب د حاصل څخه . څرنگه چي د $\sigma_n, \dots, \sigma_2, \sigma_1$

لوړترین حدونه په ترتیب سره $x_1 \cdot x_2 \cdot \dots \cdot x_n$ او $x_1 \cdot x_2 \cdot \dots \cdot x_{n-1} \cdot x_n$ ، نو د

$g(x_1, \dots, x_n)$ د پولینوم لوړترین حد په

$$ax_1^{\alpha_1 - \alpha_2} \cdot (x_1 x_2)^{\alpha_2 - \alpha_3} \cdot \dots \cdot (x_1 \cdot x_2 \cdot \dots \cdot x_{n-1})^{\alpha_{n-1} - \alpha_n} \cdot (x_1 \cdot x_2 \cdot \dots \cdot x_n)^{\alpha_n} = ax_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$$

سره مساوی کیری. پدی معنی چي د $f(x_1, \dots, x_n)$ او $g(x_1, \dots, x_n)$ د پولینومو لوړ ترین حدونه سره مساوی دی. ددی ځایه استنباط کیری چي د $f(x_1, \dots, x_n)$ او $g(x_1, \dots, x_n)$ د پولینومو د تفریق په نتیجه

کی دهغوی لوړترین حد له منځه ځي ، پدی معنی چي د $f_1(x_1, \dots, x_n)$

$$f_1(x_1, \dots, x_n) = f(x_1, \dots, x_n) - g(x_1, \dots, x_n) \quad \dots(2)$$

پولینوم د طاقت له مخی د $f(x_1, \dots, x_n)$ تر پولینوم کبنته دی. په عین شکل د $f_1(x_1, \dots, x_n)$ د پولینوم په هکله استدلال کولای سو د.

$$f_2(x_1, \dots, x_n) = f_1(x_1, \dots, x_n) - g_1(x_1, \dots, x_n) \quad \dots(3)$$

پولینوم داسی لاسته راغلی دی چي دهغه لوړترین حد د $f_1(x_1, \dots, x_n)$ تر پولینوم کبنته دی. البته د $g_1(x_1, \dots, x_n)$ پولینوم مو د $g(x_1, \dots, x_n)$ د پولینوم په ډول جوړکی.

څرنگه چي د پولینوم طاقت متناهی دی ، نو ترمتناهی قدمو وروسته (د بیلگی په ډول وروسته له k قدمو) څخه راکړه سوی پولینوم د ابتدائی متناظرو پولینومو پذیرعه ارانه کیری. ځکه چي $\alpha_1 + \alpha_2 + \dots + \alpha_n$ متناهی دی . پدی ډول په $(k+1)$ - قدم کی لاندنی پولینوم لاسته راځي:

$$0 = f_{k-1}(x_1, \dots, x_n) - g_{k-1}(x_1, \dots, x_n) \dots(k+1)$$

اوس نو که د (1) ، (2) ، (3) ، ... ، $(k+1)$ مساواتونه طرف په طرف جمع کرو :

$$f_1 + f_2 + \dots + f_{k-1} = (f - g) + (f_1 - g_1) + \dots + (f_{k-1} - g_{k-1})$$

ددی ځایه $f = g + g_1 + \dots + g_{k-1}$ لاسته راځي .

څرنګه چې د وروستي مساوات د بني خوا ټوله پولينومونه د ابتدائي متناظرو پولينومو $\sigma_n, \dots, \sigma_2, \sigma_1$ پذيريه اړانه سوي دي ، نو د $f(x_1, \dots, x_n)$ پولينوم هم د ابتدائي متناظرو پولينومو $\sigma_n, \dots, \sigma_2, \sigma_1$ پذيريه اړانه سو ، پدې معني چې $f(x_1, \dots, x_n) = h(\sigma_1, \sigma_2, \dots, \sigma_n)$ دي. د $h(\sigma_1, \sigma_2, \dots, \sigma_n)$ د پولينوم ضريبونه د $f(x_1, \dots, x_n)$ د پولينوم د ضريبو څخه د جمع او تفريق د عمليو په نتيجه كې لاسته راغلي دي، پدې معني چې د لاسته راغلي پولينوم ضريبونه بيا هم د P د فيلډ څخه دي. لاندني قضيه هم په ثبوت رسولاى سو.

قضيه ۲ - هر متناظر پولينوم د ابتدائي متناظرو پولينومود افادې په شكل په يوازني ډول اړانه كولاى سو.⁵

په واقعيت كې د اساسي قضيه ثبوت مورته د ابتدائي متناظرو پولينومو پذيريه د متناظر پولينوم د اړاني عملي طريقه راښيي . بيلګه - د

$$f(x_1, x_2, x_3) = 4(x_1^2 + x_2^2 + x_3^2) + 5x_1x_2x_3$$

د متناظرو ابتدائي پولينومو پذيريه اړانه كوو.

څرنګه چې $\sigma_3 = x_1x_2x_3$ دي ، نو بايد زموږ بيلګه يوازي د $f_1(x_1, x_2, x_3) = 4x_1^2 + 4x_2^2 + 4x_3^2$ د پاره حل كړو.

څرنګه چې د $f_1(x_1, x_2, x_3)$ لوړترين حد عبارت دي له $4x_1^2$ څخه ، نو

$$g_1(x_1, x_2, x_3) = 4\sigma_1^{2-0} \cdot \sigma_2^{0-0} \cdot \sigma_3^0 = 4\sigma_1^2$$

دي. د $f_2(x_1, x_2, x_3) = f_1(x_1, x_2, x_3) - g_1(x_1, x_2, x_3)$ په پولينوم كې يې لوړترين حد تر $4x_1^2$ كېښته دي. پدې معني چې طاقتونه يې يوازي $1, 1, 0$ كيداى سي ، پداسې حال كې چې مخكې $2, 0, 0$ و. ځكه نو $g_2(x_1, x_2, x_3) = a\sigma_1^{1-1} \cdot \sigma_2^{1-0} \cdot \sigma_3^0 = a\sigma_2$ دي . پداسې حال كې چې دلته د a ضريب نامعلوم دي . ځكه نو $f_1(x_1, x_2, x_3) = g_1(x_1, x_2, x_3) + g_2(x_1, x_2, x_3) = 4\sigma_1^2 + a\sigma_2$ لاسته راځي.

د a د محاسبې دپاره كافي ده چې د x_1 ، x_2 او x_3 متحولته قيمت كېښودو. د مثال په توګه كه $x_1 = x_2 = x_3 = 1$ سره كېښودو ، نو $12 = 36 + 3a$ وي ، يعنې $a = -8$ او

$$f_1(x_1, x_2, x_3) = 4\sigma_1^2 - 8\sigma_2$$

دي . ځكه نو زموږ راکړه سوي پولينوم به د ابتدائي متناظرو پولينومو پذيريه داسې اړانه سي:

$$f(x_1, x_2, x_3) = 4\sigma_1^2 - 8\sigma_2 + 5\sigma_3$$

⁵ د قضيه ثبوت د پاره د [7] كتاب كې 11 فصل ، § 52 وګورئ

د یادولو ورده چي د نامعینو ضریبو د شمېرني دپاره به ښه وی چي د جدول څخه کار واخلو. زمور د بیلگی دپاره چي مخکی مو حل کړی ، د نامعلوم ضریب د شمېرني جدول به په لاندی ډول وی

| x_1 | x_2 | x_3 | $f_1(x_1, x_2, x_3)$ | σ_1 | σ_2 | σ_3 | $f_1 = 4\sigma_1^2 + a\sigma_2$ |
|-------|-------|-------|----------------------|------------|------------|------------|---------------------------------|
| 1 | 1 | 1 | 12 | 3 | 3 | 1 | $12=36+3a$ |

د متناظرو پولینومو څخه د الجبر په نورو برخو کی ډیر کار اخیستل کیږی. د متناظرو پولینومو د اساسی قضیې څخه په استفادی سره د پولینومو د تیوری اساسی قضیه (اووم فصل، §II) ثابتولای سو. دنوموړی قضیې څخه د معادلو د سیستم په حل کی ، د کسری افادو په مخرج کی د غیر نسبتی افادو د له منځه وړلو دپاره او همدا ډول د الجبری معادلاتو د حل په تیوری کی تر جذر لاندی افادو (رادیکالو) دپاره کار ورڅخه اخیستل کیږی.

اووم فصل

د مختلطو او حقیقی عددو پر فیلد باندی پولینومونه

§I. د مختلطو عددو پر فیلد باندی یو متحوله پولینومونه او د مطلقه قیمت خاصیتونه

ددی کتاب په مخکنیو دوو فصلو کی موپه عمومی ډول د یو متحوله او څو متحوله پولینومو عمومی خاصیتونه پر داسی فیلد باندی چي عددی نه وه ، وڅېړل. پر مشخصو عددی فیلدو ($\mathbb{C}, \mathbb{R}, \mathbb{Q}$) باندی پولینومونه ډیر ځانگړی خاصیتونه لری چي هغوی ته مو ددی کتاب وروستی دوه فصله وقف کړیدی.

فرضوو چي د $f(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$ دپولینوم ضریبو نه a_n, \dots, a_1, a_0 او متحول z مختلط عددونه دی.

قضیه ۱. که د صفر څخه خلاف پولینوم $f(z)$ درجه د صفر څخه خلاف وی ، یعنی $\deg f(z) \geq 1$ وی، نو د M اختیاری مثبت عدد دپاره داسی $N > 0$ موندلای سو چي د $|z| > N$ د غیر مساوات څخه $|f(z)| > M$ استنباط کیږی .

ثبوت. د مختلطو عددو د مطلقه قیمت د خاصیتو سره بلد یو (لمری برخه ، دوهم فصل ، §X وگوری) ، دلته یی لنډه یادونه کوو:

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|; \left| \frac{z_1}{z_2} \right| = \frac{|z_1|}{|z_2|}; |z_1 + z_2| \leq |z_1| + |z_2|; |z_1 + z_2| \geq |z_1| - |z_2|$$

د پورتنیو خاصیتو څخه په استفادی سره لیکلای سو :

$$|f(z)| = |a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0| \geq |a_n z^n| - |a_{n-1} z^{n-1} + \dots + a_1 z + a_0| = \dots(1)$$

$$|a_n| |z|^n - |a_{n-1} z^{n-1} + \dots + a_1 z + a_0|$$

که د $|a_{n-1}|, \dots, |a_1|, |a_0|$ ضریبو د مطلقه قیمتو څخه لوی ترین یې په A سره وینيو ، نو :

$$|a_{n-1} z^{n-1} + \dots + a_1 z + a_0| \leq |a_{n-1} z^{n-1}| + \dots + |a_1 z| + |a_0| = |a_{n-1}| |z|^{n-1} + \dots + |a_1| |z| + |a_0| \leq$$

$$\leq A |z|^{n-1} + \dots + A |z| + A = A(|z|^{n-1} + \dots + |z| + 1) = A \frac{|z|^n - 1}{|z| - 1} \dots(2)$$

د یادونې وړ ده چې د قوس په داخل کې د هندسی ترادف جمع ده ، پدې معنی چې :

$$|z|^{n-1} + \dots + |z| + 1 = \frac{|z|^n - 1}{|z| - 1}$$

دی. اوس نو داخیاری $M > 0$ د پاره د $N > 0$ عدد داسی ټاکو چې د $|z| > N$ د اړیکې څخه $|f(z)| > M$ استنباط سی.

د z متحول ته د $|z| > 1 \dots(3)$ شرط ایږدو. پدې معنی چې د متحول مطلقه قیمت باید تر یوه لوی وی. ځکه نو

$$A \frac{|z|^n - 1}{|z| - 1} < A \frac{|z|^n}{|z| - 1} \dots(4)$$

د (2) او (4) نامساوات څخه په استفاده سره د (1) نامساوات په یوه مطلق نامساوات اوږی، پدې معنی چې :

$$|f(z)| \geq |a_n| |z|^n - A \frac{|z|^n - 1}{|z| - 1} > |a_n| |z|^n - A \frac{|z|^n}{|z| - 1} = |z|^n \cdot \frac{|a_n| |z| - |a_n| - A}{|z| - 1} \dots(5)$$

$$= |z|^n \left(|a_n| - \frac{A}{|z| - 1} \right)$$

$$N_1 = \frac{2A}{|a_n|} + 1 \dots(6) \quad \text{فرضوو چې :}$$

اوس نو که $|z| > N_1$ وی ، پدې معنی چې $|z| > \frac{2A}{|a_n|} + 1$ دی. ځکه نو $|z| - 1 > \frac{2A}{|a_n|}$ او

$$\frac{A}{|z| - 1} < \frac{|a_n|}{2} \quad \text{دی. ځکه نو :}$$

$$|a_n| - \frac{A}{|z|-1} > |a_n| - \frac{|a_n|}{2} = \frac{|a_n|}{2} \quad \dots(7)$$

پدی معنی که $|z| > N_1$ وی ، نو (5) نامساوات خانته لاندی شکل غوره کوی:

$$|f(z)| > |z|^n - \frac{|a_n|}{2} \quad \dots(8)$$

د یادونی وړ ده چې د $|z| > \sqrt[n]{\frac{2M}{|a_n|}}$ دپاره لاندنی نامساوات صدق کوی :

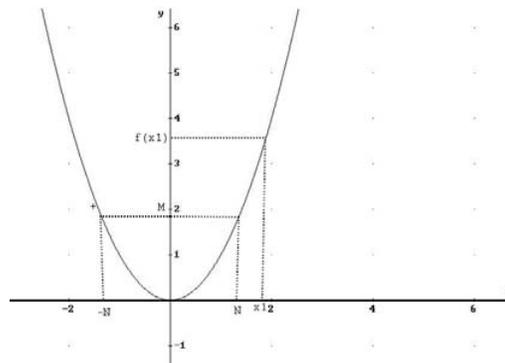
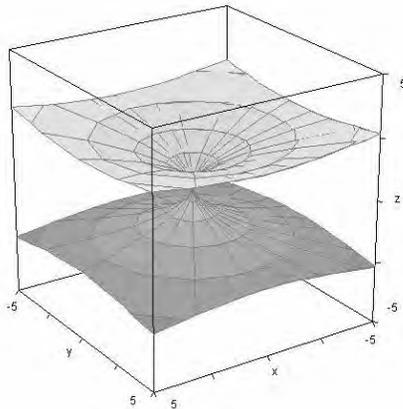
$$|z|^n \cdot \frac{|a_n|}{2} > \frac{2M}{|a_n|} \cdot \frac{|a_n|}{2} = M \quad \dots(9)$$

اوس د N عدد په لاندی ډول ټاکو:

$$N = \max \left\{ N_1, \sqrt[n]{\frac{2M}{|a_n|}} \right\}$$

پدی حالت کی د $|z| > N$ د نامساوات څخه د (8) او (9) نامساواتونه استنباط کیږی . پدی معنی چې:

$$|f(z)| > M \quad \text{او} \quad |z|^n \cdot \frac{|a_n|}{2} > M \quad \text{استنباط کیږی . پدی ترتیب} \quad |f(z)| > M \quad \text{کیږی.}$$



ثابته سوی قضیه په بله اصطلاح څرگندوی ، هر څونه چې د $f(z)$ د پولینوم مطلقه قیمت په هغه صورت کی چې د z متحول د مبداء څخه په نامحدوده ډول لیری سی ، نو دهغه قیمت هم په نامحدوده شکل زیاتیږی ($|z|$ عبارت دی د کمیات وضعیه دسیستم د مبداء څخه د z تر نقطی پوری ، د فاصلی څخه).

په پورتنی شکلو کی د بنی خوا شکل دغه واقعیت په سطحه کی انځوروی، خو د کینی خوا شکل دغه حقیقت په دری بعدی فضاء کی انځوروی.

نتیجه ۱- د $f(z)$ پولینوم یوازی هغه جذرونه درلودای سی چي مطلقه قیمت یې د $N_0 = 1 + \frac{A}{|a_n|}$ تر عدد کوچنی وی ، پداسی حال کی چي $A = \max\{|a_{n-1}|, \dots, |a_1|, |a_0|\}$ دی.

په رشتیا هم ، که $|z| \geq 1 + \frac{A}{|a_n|}$ وی ، پدی معنی چي $|z| \cdot |a_n| - |a_n| - A \geq 0$ دی. نو د (5) اړیکی پر بنسټ استدلال کولای سو چي $f(z) > 0$ دی، یعنی د z دغه ډول عدد د $f(z) = 0$ د معادلی جذر نسی کیدای.

نتیجه ۲- که $|z| > 1 + \frac{A}{|a_n|}$ وی ، نو د $f(z)$ د پولینوم د لور ترین حد مطلقه قیمت د پاته حدونو د مطلقه قیمت د جمع تر حاصل زیاد دی.

په رشتیا هم ، که $|z| > 1 + \frac{A}{|a_n|}$ وی ، نو $|a_n||z|^n - A \frac{|z|^n}{|z|-1} = |z|^n \cdot \frac{|a_n||z| - |a_n| - A}{|z|-1} > 0$ دی.

پدی معنی چي $|a_n z^n| > A \frac{|z|^n}{|z|-1}$ دی. که د (2) او (4) نا مساوات څخه استفاده وکړو، نو د نتبجی ادعا لاسته راځي یعنی:

$$|a_n z^n| > A \frac{|z|^n}{|z|-1} > A \frac{|z|^n - 1}{|z|-1} \geq |a_{n-1} z^{n-1} + \dots + a_1 z + a_0|$$

§II. د پولینومو د الجبر اساسی قضیه

اوس به نو د مختلطو ضریبو سره د پولینومو د جذر د موجودیت مسئله په جزئیاتو سره وڅیړو. د پنځم فصل د §XV څخه پوهیږو چي هر پولینوم چي درجه یې صفر نه وی د مختلطو عددو \mathbb{C} د فیلډ د پراخولو (وسعت) په نتبججه کی لاسته راغلی فیلډ باندی جذر لری.

موږ کولای سو چي د تبری ادعا یو مهمه نتیجه چي د پولینومو د الجبر د اساسی قضیې په نامه یادیری ثابتو کړو.

په §I د ثابتی سوی قضیې او د هغه د نتبجو څخه ډیر مهم حقیقت استنباط کیدای سی چي په لاندی ډول یې فورمول بندی کوو.

قضیه ۱- هر پولینوم چي درجه یې طاق وی ، او د حقیقی عددو \mathbb{R} پر فیلډ باندی راکړه سوی وی ، لږ ترلږه یو حقیقی جذر لری.

ثبوت - فرضوو چي د $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ پولینوم چي ضریبونه یې حقیقی عددونه دی، داسی راکره سوی وی چي د x متحول قیمتونه یوازې حقیقی عددونه، یعنی $x \in \mathbb{R}$ ، وی. پدی حالت کی د $f(x)$ پولینوم د تابع په صفت چي د تعریف ساحه یې حقیقی عددونه \mathbb{R} دی، مشاهده کولای سو. د ریاضی د انا لایز څخه پوهېږو چي نوموړی تابع پر حقیقی محور باندې متمادی ده، ځکه نو ددی فصل د $I\&S$ د ثابتی سوی قضیې د دوهمې نتجې پر اساس د $|x|$ په کافی اندازه لویو عددی قیمتو دپاره صدق کوی چي د $|a_n x^n|$ حد د پاته حدونو د جمع د حاصل تر مطلقه قیمت لوی دی. ځکه نو د x ددغه ډول قیمتو دپاره د $f(x)$ پولینوم او دهغه لوی ترین حد یو ډول علامی لری.

په رشتیا هم که $a_n x^n > 0$ وی، نو د $a_n x^n > |a_{n-1} x^{n-1} + \dots + a_1 x + a_0|$

$$a_n x^n - |a_{n-1} x^{n-1} + \dots + a_1 x + a_0| > 0$$

لاسته راځی. ځکه نو :

$$f(x) = a_n x^n + (a_{n-1} x^{n-1} + \dots + a_1 x + a_0) \geq a_n x^n - |a_{n-1} x^{n-1} + \dots + a_1 x + a_0| > 0$$

پدی معنی چي $f(x) > 0$ دی.

همدا ډول د $a_n x^n < 0$ استنباط کیری چي $-a_n x^n > 0$ او

$$-a_n x^n > |a_{n-1} x^{n-1} + \dots + a_1 x + a_0|$$

$$a_n x^n + |a_{n-1} x^{n-1} + \dots + a_1 x + a_0| < 0$$

څرنگه چي :

$$a_n x^n + |a_{n-1} x^{n-1} + \dots + a_1 x + a_0| \geq a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = f(x)$$

دی، پدی معنی چي $f(x) < 0$ دی.

د قضیې د شرط له مخی د n عدد طاق عدد دی. پدی معنی که $x < 0$ وی، نو $x^n < 0$ دی، او که $x > 0$ وی، نو $x^n > 0$ دی. پدی معنی چي د x د مختلفو عددو دپاره چي مختلفې علامی ولری، لوی ترین حد $a_n x^n$ مختلفې علامی اخلی. ددغه اسیته د $|x|$ د هغو عددی قیمتو دپاره چي په کافی اندازه لوی وی د $f(x)$ تابع هم مثبت او هم منفی قیمت ځانته اخلی. پدی معنی چي د $x=a$ او $x=b$ داسی قیمتونه وجود لری چي $f(a)$ او $f(b)$ د مختلفو علامو درلودونکی دی.

د ریاضی په انا لایز کی د بلزانو د قضیې پر اساس د $[a, b]$ په انتروال کی د α داسی عدد وجود لری چي $f(\alpha) = 0$ کیری. پدی معنی چي α د $f(x)$ د پولینوم جذر دی.

اوس نو د حقیقی عددو پر فیلډ باندې پولینومونه د اختیاری درجي سره مطالعه کوو. ددغه ډول پولینومو د پاره لاندنی مهمه قضیه صدق کوی.

قضیه ۲- هر پولینوم چي درجه یې تر $n \geq 1$ او ضریبونه یې د حقیقی عددو څخه وی، لږ تر لږه د یوه مختلط جذر درلودونکی دی.

ثبوت - لمړی د یادولو وړ ده چې هر طبیعي عدد د $n=2^k \cdot q$ په څېر داسی ارائه کولای سوچي ک غیر منفي تام عدد او q طبیعي طاق عدد دی. د بېلګې په ډول $120=2^3 \cdot 15$ او $321=2^0 \cdot 321$.

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \dots (1) \text{ فرضوو چې}$$

اختیاری پولینوم دی چې ضریبونه یې حقیقی عددونه دی او درجه یې $n=2^k \cdot q$ دی. قضیه د استقراء په طریقته ثابتوو.

که $k=0$ وی، نو $n=q$ طاق عدد دی، پدې معنی چې د $f(x)$ د پولینوم درجه طاق ده او د لمړی قضیې پر اساس زموږ قضیه صدق کوی.

اوس به نو فرض کړو چې زموږ قضیه د حقیقی عددو پر فیلډ باندی د $q \cdot 2^{k-1}$ په درجه باندی صدق کوی. زموږ قضیه د هغو پولینومو دپاره چې درجه یې پر 2^{k-1} دوپش وړ وی، خو پر 2^k ($k \geq 1$) دوپش وړ نه وی، صدق کوی.

د پورتنی حقیقت څخه په استفاده سره باید ثابتته کړو چې قضیه د حقیقی عددو پر فیلډ باندی د $n=2^k \cdot q$ په درجه باندی هم صدق کوی.

د پنځم فصل په $XV \S$ د دوهمی قضیې څخه پوهیږو چې د حقیقی عددو \mathbb{R} پر فیلډ باندی د $f(x)$ د پولینوم د K د تجزیې فیلډ وجود لری. د K د تجزیې په فیلډ کی د $f(x)$ پولینوم n جذرونه لری. نوموړی جذرونه په $\alpha_1, \alpha_2, \dots, \alpha_n$ سره نښو(امکان لری چې ځنی د ذکر سوبو جذرو څخه په خپل منځ کی سره مساوی وی).

فرضوو چې λ د حقیقی عددو څخه یو اختیاری خو تثبیت سوی عدد دی. د K د فیلډ لاندنی عنصرونه څېرو:

$$\begin{aligned} \beta_{12} &= \alpha_1 \alpha_2 + \lambda(\alpha_1 + \alpha_2) \\ \beta_{13} &= \alpha_1 \alpha_3 + \lambda(\alpha_1 + \alpha_3) \\ &\vdots \\ \beta_{1n} &= \alpha_1 \alpha_n + \lambda(\alpha_1 + \alpha_n) \quad \dots (2) \\ \beta_{23} &= \alpha_2 \alpha_3 + \lambda(\alpha_2 + \alpha_3) \\ &\vdots \\ \beta_{(n-1)n} &= \alpha_{n-1} \alpha_n + \lambda(\alpha_{n-1} + \alpha_n) \end{aligned}$$

د پورتنیو عناصرو عمومی شکل $\beta_{ij} = \alpha_i \alpha_j + \lambda(\alpha_i + \alpha_j)$ دی پداسی حال کی چې $i < j$ دی. د نوموړو عناصرو شمېر په $q \cdot 2^{k-1}$ سره مساوی کیږی، ځکه چې:

$$\begin{aligned} (n-1) + (n-2) + \dots + 2 + 1 &= \frac{(n-1)+1}{2} (n-1) = \frac{n(n-1)}{2} = \frac{2^k \cdot q(2^k \cdot q - 1)}{2} = \\ &= 2^{k-1} \cdot \underbrace{q(2^k q - 1)}_{q_1} = 2^{k-1} \cdot q_1 \end{aligned}$$

پداسی حال کی چي q_1 طاق عدد دی.

اوس نو د K پر فیله بانندی د $g(z)$ پولینوم داسی جوړو:

$$g(z) = (z - \beta_{12})(z - \beta_{13}) \dots (z - \beta_{(n-1)n}) = \prod_{i < j} (z - \beta_{ij}) \quad \dots(3)$$

د نوموړی پولینوم درجه به $\deg g(z) = 2^{k-1} \cdot q_1$ وی او جذرونه یی یوازی د $\beta_{(n-1)n}, \dots, \beta_{13}, \beta_{12}$ عددونه دی. څرنګه چي $\lambda \in \mathbb{R}$ ده، نو د $g(z)$ د پولینوم ضریبونه عبارت دی د هغو پولینومو څخه چي د β_{ij} له جنسه جوړ سوی دی، پدی معنی چي نوموړی پولینومونه د α_i او α_j د جنسه د حقیقی ضریبونه په ذریعه ارائه سوی دی. په (2) او (3) فورمولو کی لیدل کیږی چي د $g(z)$ په پولینوم کی د $\alpha_1, \alpha_2, \dots, \alpha_n$ د عنصر و د اختیاری تعویض په نتیجه کی تغییر نه راځي، ځکه چي:

$$g(z) = \prod_{i < j} (z - \beta_{ij}) = \prod_{i < j} (z - [\alpha_i \alpha_j + \lambda(\alpha_i + \alpha_j)])$$

دی، خو یوازی په ضرب کی د ضربی عاملو په ترتیب کی تغییر راځي. ځکه نو د $g(z)$ پولینوم متناظر دی چي ضریبونه یی حقیقی عددونه دی او د $\alpha_1, \alpha_2, \dots, \alpha_n$ د جنسه جوړ سوی دی.

$\alpha_1, \alpha_2, \dots, \alpha_n$ د حقیقی عددو پر فیله د $f(x)$ د پولینوم جذرونه دی. د متناظرو پولینومو د اساسی قضیې څخه (د شپږم فصل، §V وګورئ) نتیجه اخیستلای سو چي د $g(z)$ د پولینوم ضریبونه حقیقی عددونه دی. ددغه ډول جوړ سوی پولینوم درجه $\deg g(z) = 2^{k-1} \cdot q_1$ ده او د استقراء د فرضیې پر بنسټ لږ تر لږه یو مختلط جذر $\beta_{ij} = \alpha_i \alpha_j + \lambda(\alpha_i + \alpha_j)$ (د $i < j$ دپاره) لری.

پدی ترتیب د هر $\lambda \in \mathbb{R}$ دپاره د i او j ($1 \leq i \leq n, 1 \leq j \leq n$) د اندکسو داسی جوړه موندلای سو چي د $\beta_{ij} \in K$ مختلط عدد دی.

د λ او λ' د دوو مختلفو عددو جواب ورکونکی به مختلف اندکسونه وی. څرنګه چي د \mathbb{R} سیټ نا متناهی سیټ دی، خو د $\{(i,j) / i < j, 1 \leq i \leq n, 1 \leq j \leq n\}$ سیټ متناهی سیټ دی، ددی اسیته د λ_1 او λ_2 دوه مختلف عددونه داسی موندلای سو چي د i او j داندکسو عین جوړه د هغوی جواب ورکونکی ده. پداسی ډول چي:

$$\begin{aligned} \alpha_i \alpha_j + \lambda_1 (\alpha_i + \alpha_j) &= \gamma_1 \\ \alpha_i \alpha_j + \lambda_2 (\alpha_i + \alpha_j) &= \gamma_2 \end{aligned} \quad \dots(4)$$

مختلط عددونه دی. د پورتنیو مساواتو د تفریق په نتیجه کی:

$$\alpha_i + \alpha_j = \frac{\gamma_1 - \gamma_2}{\lambda_1 - \lambda_2} \quad \dots(5)$$

لاسته راځي. علاوه پر دی:

$$\alpha_i \alpha_j = \gamma_1 - \lambda_1 (\alpha_i + \alpha_j) = \gamma_1 - \lambda_1 \frac{\gamma_1 - \gamma_2}{\lambda_1 - \lambda_2} \quad \dots(6)$$

دی. پدی معنی چي د $\alpha_i + \alpha_j$ او د $\alpha_i \alpha_j$ عددونه مختلط عددونه دی. د α_i او α_j د جذرو د موندلو دپاره $u^2 - (\alpha_i + \alpha_j)u + \alpha_i \alpha_j = 0$ دوهمه درجه معادله د مختلطو ضریبو سره حلوو. په نتیجه کی یې بیا هم مختلط عددونه لاسته راځي. په نتیجه کی ویلای سو چي د $f(x)$ پولینوم حتی د دوو مختلطو جذرو خاوند دی. پدی معنی چي زموږ قضیه د داسی پولینوم دپاره چي د هغه درجه $n=2^k \cdot q$ ده، صدق کوی. د استقراء د پرنسیب له مخي زموږ قضیه د ټولو طبیعی عددو $n \geq 1$ دپاره صدق کوی. اوس نو د پولینومو د الجبر اساسی قضیه په اسانې سره ثابتولای سو.

قضیه ۳ - هر پولینوم چي درجه یې صفر نه وی، د مختلطو عددو \mathbb{C} پر فیلډ باندی لږ تر لږه یو مختلط جذر لری.

ثبوت - د قضیې د ثبوت دپاره د مختلطو عددو د ځینو خاصیتو یادونه، چي د لمړي برخي په دوهم فصل کی مو ولوستل، ضروری ده. د مختلط عدد $z = a + bi$ مزدوج عدد Conjugate عبارت دی له $\bar{z} = a - bi$ څخه. همدا ډول د مختلط عدد او د هغه د مزدوج د جمع او ضرب په نتیجه کی حقیقی عدد لاسته راځي، پدی معنی چي $(z + \bar{z}) \in \mathbb{R}$ او $(z \cdot \bar{z}) \in \mathbb{R}$ دی. علاوه پردی: $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$ ، $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$ او $\bar{\bar{z}} = z$ کیری.

وروستیو خاصیتو ته د څو عددو دپاره عمومي شکل ورکولای سو.

اوس به نو فرض کړو چي د $f(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$ پولینوم چي درجه یې $n \geq 1$ ده د مختلطو عددو \mathbb{C} پر فیلډ باندی راکړه سوی دی.

په عین حال کی د $g(z) = \bar{a}_n z^n + \bar{a}_{n-1} z^{n-1} + \dots + \bar{a}_1 z + \bar{a}_0$ پولینوم چي ضریبونه یې په ترتیب سره د $f(z)$ د پولینوم د ضریبو مزدوج ضریبونه دی، څېرو. د $h(z) = f(z) \cdot g(z)$ د پولینوم درجه $2n$ ده.

$$h(z) = f(z) \cdot g(z) = (a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0) \cdot (\bar{a}_n z^n + \bar{a}_{n-1} z^{n-1} + \dots + \bar{a}_1 z + \bar{a}_0) = (a_n \bar{a}_n) z^{2n} + (a_n \bar{a}_{n-1} + a_{n-1} \bar{a}_n) z^{2n-1} + \dots + (\bar{a}_1 a_0 + \bar{a}_0 a_1) z + a_0 \bar{a}_0$$

څرگنده ده چي $a_n \bar{a}_n, a_0 \bar{a}_0 \in \mathbb{R}$ دی. همدا ډول

$$\overline{a_n \bar{a}_{n-1} + a_{n-1} \bar{a}_n} = \overline{a_n \bar{a}_{n-1}} + \overline{a_{n-1} \bar{a}_n} = \bar{a}_n a_{n-1} + \bar{a}_{n-1} a_n$$

دی. پدی معنی چي د z^{2n-1} د ضریب مزدوج بیرته د خپله ځانه سره مساوی کیری. ددی اسیته استدلال کولای سو چي نوموړی ضریبونه حقیقی عددونه دی. همدا ډول آزمویلای سو چي د $h(z)$ د پولینوم ټوله ضریبونه حقیقی عددونه دی. ځکه نو دوهمی قضیې پر بنسټ د $h(z)$ پولینوم د z_0 مختلط جذر لری، یعنی $h(z_0) = 0$ دی. ددی ځایه استدلال کولای سو چي $f(z_0) \cdot g(z_0) = 0$ دی. اوس نو که $f(z_0) = 0$ وی، نو قضیه ثابتې سوه، ځکه چي z_0 د $f(z)$ د پولینوم جذر دی.

فرضوو چي $f(z_0) \neq 0$ دی، نو پدی صورت کی باید $g(z_0) = 0$ وی. یعنی:

$$g(z) = \bar{a}_n z_0^n + \bar{a}_{n-1} z_0^{n-1} + \dots + \bar{a}_1 z_0 + \bar{a}_0 = 0$$

$$\overline{a_n z_0^n + a_{n-1} z_0^{n-1} + \dots + a_1 z_0 + a_0} = \bar{0}$$

$$\overline{a_n z_0^n + a_{n-1} z_0^{n-1} + \dots + a_1 z_0 + a_0} = \bar{0}$$

$$a_n \bar{z}_0^n + a_{n-1} \bar{z}_0^{n-1} + \dots + a_1 \bar{z}_0 + a_0 = 0$$

وروستی مساوات څرگندوی چې $f(\bar{z}_0) = 0$ دی ، پدی معنی چې \bar{z}_0 د $f(z)$ د پولینوم جذر دی.

پدی ترتیب قضیه په پوره ډول سره ثابته سوه.

نن ورځ د پولینومو د تیوری د اساسی قضیې څو ډوله ثبوتونه وجود لری. ټوله ثبوتونه لږ یا ډیر پر کومکی قضیو چې د هغوی ثبوت ډیر پیچلی دی او د پولینومو پر تابعی خاصیتو (په خاص ډول د حقیقی عددو پر فیلد باندی د هغو پر متمادیت) تکیه کوی. پورتنی ثبوت و اویلر-گاوس ته نسبت ورکول کیری چې تر ډیره حده په اصطلاح د یو «الجبری» ثبوت په صفت قبول سوی دی ، ځکه چې نوموړی ثبوت پر دوهمه قضیه استوار او د هغه د ثبوت دپاره د متناظرو پولینومو د اساسی قضیې څخه کار اخیستل سوی دی.

همدا راز د یادولو وړ ده چې په نولسمه پېړی کی نوموړی قضیه د الجبر د اساسی قضیې په نامه یادیدله ، دا ځکه چې په هغه وخت کی د الجبر موضوع اساساً د معادلو څېړنه تشکیلوله ، خو نن ورځ د الجبر د څېړنې موضوع نه یوازی معادلی ، بلکه تر ډیره حده الجبری سیستمونه (لکه گروپ ، رینگ او فیلد) ، ماترکسونه او دیترمانتونه تشکیلوی ، څه ډول چې په لمړی برخه او ددی برخې په مخکنیو فصلو کی مطالعه کړل. ددی اسپته اوس دغه قضیه د الجبر داساسی قضیې په نامه نه بلکه د پولینومو د الجبر د اساسی قضیې په نامه یادېږی.

په پای کی د یادولو وړ ده چې ثابته سوی قضیه یوازی تیوریکی خصوصیت لری ، پدی معنی چې عملاً د پولینوم د جذر د موندلو دپاره په درد نه خوری.

§III. د پولینومو تجزیه په خطی ضربی عاملو باندی – د ویتا قضیه

فرضوو چې د مختلطو عددو \mathbb{C} پر فیلد باندی د $f(z)$ پولینوم چې درجه یی $n \geq 2$ ده ، راکړه سوی دی. اوس نو د پولینومو د الجبر د اساسی قضیې نتیجې پر دغه ډول پولینومو مطالعه کوو.

قضیه ۱- هر پولینوم چې درجه یی تر یوه اضافه وی ، د مختلطو عددو په فیلد کی د تجزیې وړ دی.

ثبوت - فرضوو چې $f(z) \in \mathbb{C}[z]$ او $\deg f(z) \geq 2$ دی. ددی مبحث ددریمی قضیې پر اساس نوموړی پولینوم لږ تر لږه د z_0 یو جذر لری. د §XIII د دوهم تعریف پر بنسټ د $f(z)$ پولینوم پر $z - z_0$ دوېش وړ دی. پدی معنی چې $f(z) = (z - z_0) \cdot f_1(z)$ ، پداسی حال کی چې $dcgf(z) = 1 + dcg f_1(z)$ دی. څرنګه چې $\deg f(z) \geq 2$ دی ، نو $\deg f_1(z) \geq 1$ دی. په نتیجه کی ویلای سو چې د $f(z)$ پولینوم د مختلطو عددو په فیلد \mathbb{C} کی دتجزیې وړ دی.

نتیجه - د مختلطو عددو په فیلد کی یوازی هغه پولینومونه چې درجه د یوه سره مساوی وی د تجزیې وړ ندی .

قضیه ۲ - د مختلطو عددو په فیلد کی هر پولینوم چي درجه یی د صفر څخه خلاف وی په هم هغه فیلد کی په خطی عاملو باندی تجزیه کیدای سی. پدی معنی چي :

$$f(z) = a_n(z-z_1)(z-z_2)\dots(z-z_n) \quad \dots(1)$$

پداسی ډول چي Z_1, Z_2, \dots, Z_n د $f(z)$ د پولینوم جذرونه او a_n د هغه د لوی ترین حد ضریب دی. پورتنی تجزیه د ضربی عاملو تر ترتیب پوری بی ساری ده.

ثبوت - فرضوو چي د $f(z)$ د پولینوم درجه مساوی په $n \geq 1$ ده. که $f(z) = az + b$ وی نو د پولینوم تجزیه $f(z) = a(z + \frac{b}{a})$ شکل لری او قضیه صدق کوی .

فرضوو چي $n \geq 2$ دی، نو د XI § د لمړی قضیې پر اساس د مختلطو عددو \mathbb{C} پر فیلد باندی د $f(z)$ پولینوم په ضربی نه تجزیه کیدونکی عاملو باندی تجزیه کولای سو. پدی معنی چي :

$$f(z) = p_1(z)p_2(z)\dots p_k(z) \quad \dots(2)$$

څرنګه چي د مختلطو عددو \mathbb{C} په فیلد کی یوازی هغه پولینومونه د تجزیې وړ ندی چي درجه یی مساوی په یوه سره وی ، پدی معنی چي د $p_1(z), p_2(z), \dots, p_k(z)$ د پولینومو څخه د هر یوه درجه د یوه سره مساوی ده. علاوه پردی د k ضربی عاملو شمېر باید د $f(z)$ د پولینوم درجی ، یعنی n سره مساوی وی. فرضوو چي :

$$p_1(z) = b_1z + c_1, p_2(z) = b_2z + c_2, \dots, p_k(z) = b_nz + c_n$$

دی. په (2) اړیکه کی د هغوی د تعویض څخه وروسته

$$\begin{aligned} f(z) &= (b_1z + c_1)(b_2z + c_2)\dots(b_nz + c_n) = b_1b_2\dots b_n(z + \frac{c_1}{b_1})(z + \frac{c_2}{b_2})\dots(z + \frac{c_n}{b_n}) \\ &= A(z-z_1)(z-z_2)\dots(z-z_n) \end{aligned}$$

پداسی حال کی چي $A = b_1b_2\dots b_n$ او $z_n = -\frac{c_n}{b_n}, \dots, z_2 = -\frac{c_2}{b_2}, z_1 = -\frac{c_1}{b_1}$ دی.

څرنګه چي $f(z) = a_nz^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0$ دی ، نو د $A(z-z_1)(z-z_2)\dots(z-z_n)$ سره $f(z)$ د لوی ترین حد تر پرتلی وروسته دی نتیجی ته رسیرو چي $A = a_n$ سره دی. په نتیجه کی :

$$f(z) = a_n(z-z_1)(z-z_2)\dots(z-z_n)$$

لاسته راځي.

نتیجه - د مختلطو عددو \mathbb{C} پر فیلد باندی د $f(z)$ هر پولینوم چي درجه یی مساوی په $n (n \neq 0)$ سره وی ، پر نوموړی فیلد باندی فقط n جذرونه لری. البته په هغه صورت کی چي د جذرو د تضاعف درجه په نظر کی ورسره ونیسو.

تعريف - د P فيلډ د الجبري ترلی فيلډ په نامه يادېږي ، که د $P[x]$ د رينگ داختياري پولينوم ټوله جذرونه د P د فيلډ عنصر ونه وي.

د ثابتی سوی قضیې او د هغی د نتیجو څخه استنباط کيږی چې د مختلطو عددو فيلډ \mathbb{C} الجبري ترلی فيلډ دی.

پدی ډول مو د مختلطو عددو \mathbb{C} پر فيلډ باندی د پولينومو د جذرو د تعداد مسئله په پوره ډول حل کړه . اوس به نو د پولينوم د جذرو اړیکه د هغه د ضريبو سره تر مطالعی لاندی ونیسو.

قضیه (ویټا Viète) - که د مختلطو عددو \mathbb{C} پر فيلډ باندی Z_1, Z_2, \dots, Z_n د

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$$

پولينوم جذرونه وي ، نو لاندني فورمولونه صدق کوی:

$$Z_1 + Z_2 + \dots + Z_n = -\frac{a_{n-1}}{a_n}$$

$$Z_1 Z_2 + Z_1 Z_3 + \dots + Z_{n-1} Z_n = \frac{a_{n-2}}{a_n}$$

$$Z_1 Z_2 Z_3 + Z_1 Z_2 Z_4 + \dots + Z_{n-2} Z_{n-1} Z_n = -\frac{a_{n-3}}{a_n} \quad \dots(3)$$

⋮

$$Z_1 Z_2 Z_3 \dots Z_n = (-1)^n \frac{a_0}{a_n}$$

ثبوت - د دوهمی قضیې پر اساس

$$a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = a_n (z - Z_1)(z - Z_2) \dots (z - Z_n)$$

صدق کوی . په پورتنی مساوات کی د بڼی خوا د قوسو د ضرب په نتیجه کی لاندی افاده لاسته راځي:

$$a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0 = a_n z^n - (Z_1 + Z_2 + \dots + Z_n) z^{n-1} + a_n (Z_1 Z_2 + Z_1 Z_3 + \dots + Z_{n-1} Z_n) z^{n-2} + \dots + (-1)^n a_n Z_1 Z_2 Z_3 \dots Z_n$$

اوس نو که د وروستی مساوات بڼی او کینه خوا سره پرتله کړو ، نو لاندی مساواتونه به لاسته راسی:

$$a_n = a_n$$

$$a_{n-1} = -a_n (Z_1 + Z_2 + \dots + Z_n)$$

$$a_{n-2} = a_n (Z_1 Z_2 + Z_1 Z_3 + \dots + Z_{n-1} Z_n) \quad \dots(4)$$

⋮

$$a_0 = (-1)^n a_n Z_1 Z_2 Z_3 \dots Z_n$$

که د (4) اړیکي دواړی خواوی پر $a_n \neq 0$ ووېشو ، نو د (3) فورمولونه لاسته راځي.

د (3) فورمولونه د فرانسوی گنک (ریاضیدان) ویټا Viète د فورمولو په نامه یادیری.

که د $f(z)$ پولینوم دوهمه درجه معادله وی، نو د جذرو د جمع د حاصل او د ضرب د حاصل هغه فورمولونه چې په بنوونځی کی ورسره آشنا سوی یاست لاسته راځي. پدی معنی چي:

$$z_1 + z_2 = -\frac{a_1}{a_2}$$

$$z_1 z_2 = \frac{a_0}{a_2}$$

§IV. د حقیقی عددو د ضریبو سره د پولینومو د مختلطو جذرو خاصیتونه

په ډیرو عملی مسئلو کی د داسی معادلو سره مخامخ کیږو چي ضریبونه یی حقیقی عددونه وی. پدی معنی چي د $f(x)=0$ په څېر معادلی چي کینه خوايي د حقیقی عددو د فیله څخه تشکیله سوی ده. څرنګه چي دحقیقی عددو فیله د مختلطو عددو د فیله سب فیله دی، نو د $f(x)$ پولینوم د مختلطو عددو پر فیله باندی n جذرونه لری (§III، دوهمی قضیې نتیجه وګوری). څرګنده ده چي ددغه ډول معادلو مختلط جذرونه په زړه پوری خاصیتونه لری.

قضیه ۱ - که د z_0 مختلط عدد د حقیقی ضریبو سره د

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$$

د پولینوم جذر وی، نو دهغه مزدوج یعنی \bar{z}_0 هم د نوموړی پولینوم جذر دی.

ثبوت - فرضوو چي $f(z_0)=0$ دی. یعنی $a_n z_0^n + a_{n-1} z_0^{n-1} + \dots + a_1 z_0 + a_0 = 0$ دی.

څرنګه چي د صفر مزدوج بیا هم صفر دی، نو

$$\overline{a_n z_0^n + a_{n-1} z_0^{n-1} + \dots + a_1 z_0 + a_0} = 0$$

دی. د مزدوجو عددو د خاصیتو پر بنسټ (§II) لیکلای سو:

$$\bar{a}_n \bar{z}_0^n + \bar{a}_{n-1} \bar{z}_0^{n-1} + \dots + \bar{a}_1 \bar{z}_0 + \bar{a}_0 = 0$$

څرنګه چي $a_n, a_{n-1}, \dots, a_1, a_0$ حقیقی عددونه دی، نو $\bar{a}_n = a_n, \bar{a}_{n-1} = a_{n-1}, \dots, \bar{a}_1 = a_1, \bar{a}_0 = a_0$ دی.

$$a_n \bar{z}_0^n + a_{n-1} \bar{z}_0^{n-1} + \dots + a_1 \bar{z}_0 + a_0 = 0 \quad \text{او}$$

او یا په بله اصطلاح $f(\bar{z}_0) = 0$ دی. پدی معنی چي \bar{z}_0 هم د $f(z)$ د پولینوم جذر دی.

قضیه ۲ - فرضوو چي د $f(z)$ د پولینوم درجه $k > 1$ او ضریبونه یی حقیقی عددونه دی، که د z_0 مختلط عدد د $f(z)$ د پولینوم مضاعف جذر وی، نو دهغه مزدوج یعنی \bar{z}_0 هم د $f(z)$ د پولینوم مضاعف جذر دی.

ثبوت - فرضوو چي د $f(z)$ د پولینوم درجه $k > 1$ ده. د پنځم فصل د §XIV دوه می قضیې پر اساس $f(z_0) = f'(z_0) = \dots = f^{(k-1)}(z_0) = 0$ او $f^k(z_0) \neq 0$ دی. څرنگه چي د $f(z)$ د پولینوم ټول مشتقونه د حقیقی عددو ضریب لرونکي پولینومونه دی، نو د لمړی قضیې پر اساس $f(\bar{z}_0) = f'(\bar{z}_0) = \dots = f^{(k-1)}(\bar{z}_0) = 0$ دی. که $f^k(\bar{z}_0) = 0$ وی، نو د $\bar{z}_0 = z_0$ په نتیجه کی z_0 د

$f(z)$ د پولینوم د k -ام مشتق جذر هم دی، پدی معنی چي $f^k(z_0) = 0$ دی. خو دغه حالت زموږ د مخکنی شرط، یعنی $f^k(z_0) \neq 0$ ، سره مغایرت لری. په نتیجه کی ویلای سو چي $f^k(\bar{z}_0) \neq 0$ دی پدی معنی چي \bar{z}_0 هم د $f(z)$ د پولینوم مضاعف جذر دی.

اوس نو کولای سو چي پر حقیقی فیله باندي د پولینومو د تجزیه کیدو او یا نه تجزیه کیدو د ورتوب مسأله تر مطالعی لاندی ونیسو.

قضیه ۳ - د حقیقی عددو پر فیله باندي هر پولینوم چي درجه یی تر 2 اضافه وی، په نوموړی فیله کی د تجزیې وړ دی.

ثبوت - فرضوو چي د حقیقی عددو پر فیله \mathbb{R} باندي د $f(z)$ پولینوم چي درجه یی $n > 2$ ده، داسی راکړه سوی دی چي z_0 یی جذر دی. که z_0 حقیقی عدد وی، نو $f(z) = (z - z_0)s(z)$ دی. پدی حالت کی د $s(z)$ ضریبونه حقیقی عددونه دی او $\deg s(z) > 1$ دی. په نتیجه کی ویلای سو چي د $f(z)$ پولینوم د حقیقی عددو په فیله کی د تجزیې وړ دی.

که فرض کړو چي z_0 مختلط عدد وی، نو د لمړی قضیې پر اساس د نوموړی عدد مزدوج یعنی \bar{z}_0 هم د $f(z)$ د پولینوم جذر دی. ځکه نو $f(z) : (z - z_0)$ او $f(z) : (z - \bar{z}_0)$ دی. څرنگه چي د $(z - z_0)$ او $(z - \bar{z}_0)$ پولینومونه سره متبائن دی، نو د $f(z)$ پولینوم د هغوی د ضرب پر حاصل یعنی $g(z) = (z - z_0)(z - \bar{z}_0)$ هم دوپش وړ دی.

$$g(z) = (z - z_0)(z - \bar{z}_0) = z^2 - (z_0 + \bar{z}_0)z + z_0\bar{z}_0$$

څرنگه چي $z_0 + \bar{z}_0$ او $z_0\bar{z}_0$ حقیقی عددونه دی، نو د $g(z)$ د پولینوم ضریبونه حقیقی عددونه دی. لکه مخ کی چي مو وویل د $f(z)$ پولینوم د $g(z)$ پر پولینوم دوپش وړ دی یعنی $f(z) = g(z)h(z)$ سره. څرنگه چي $\deg f(z) > 2$ او $\deg g(z) = 2$ ده، نو $\deg h(z) \geq 1$ دی. ځکه نو په دغه حالت کی هم د $f(z)$ پولینوم د حقیقی عددو په فیله کی د تجزیې وړ دی.

د پورتنی قضیې څخه لاندنی نتیجه استنباط کیری.

نتیجه - د حقیقی عددو په فیله کی یوازی هغه پولینومونه د تجزیې وړ ندی چي درجه یی یا د یوه یا دوو سره مساوی وی او حقیقی جذرونه ونلری.

قضیه ۴ - د حقیقی عددو په فیله کی هر د $f(z)$ پولینوم چي درجه یی د صفر څخه خلاف وی په نوموړی فیله کی په نه تجزیه کیدونکی ضربی عاملو باندي په یوازی (بی ساري) شکل تجزیه کیدای سی. یعنی:

$$f(z) = a_n(z - z_1)^{k_1}(z - z_2)^{k_2} \dots (z - z_m)^{k_m}(z^2 + b_{m+1}z + c_{m+1})^{k_{m+1}} \dots (z^2 + b_rz + c_r)^{k_r}$$

ثبوت - فرضوو چي :

$$f(z) = [p_1(z)]^{k_1} \cdot [p_2(z)]^{k_2} \dots [p_r(z)]^{k_r}$$

د حقيقي عددو په فيلډ کې په نه تجزيه کېدونکي پولینومو باندې د $f(z)$ د پولینوم معیاري (سټنډرډ) تجزيه ده . ددغه ډول تجزيې موجودیت او یوازی والی (بی ساری توب) مو د پنځم فصل په § XIV کې ثابتې کړه . د دریمې قضیې څخه استنباط کېږي چې د هر یو د $p_1(z), p_2(z), \dots, p_r(z)$ پولینومو درجه تر دوه زیاته نده ، پدې معنی چې د هغوی درجه یا په یوه او یا په دوه سره مساوی کېږي .

فرضوو چې د $p_1(z), p_2(z), \dots, p_m(z)$ د پولینومو درجې د یوه سره مساوی کېږي او د $p_r(z), \dots, p_{m+1}(z)$ پولینومو درجې د دوو سره مساوی کېږي . پدې شرط که د نوموړو پولینومو د لوی ترین حد ضریب یو وی ، نو هغوی په یوازینی (بی ساری) شکل ټاکل کېدای سی . پدې معنی چې :

$$f(z) = A(z - z_1)^{k_1} (z - z_2)^{k_2} \dots (z - z_m)^{k_m} (z^2 + b_{m+1}z + c_{m+1})^{k_{m+1}} \dots (z^2 + b_rz + c_r)^{k_r}$$

د $f(z)$ د پولینوم د لوی ترین حد ضریب او لاسته راغلی د ضرب د حاصل د پرتلی په نتیجه کې $A = a_n$ لاسته راځي .

باید ووايو چې که د پولینومو پورتنی په زړه پوری خاصیتونه مورته د هغو پولینومو چې درجه یې تر دوه اضافه وی ، د جزرو د موندلو او یا محاسبی عملی وسایل په لاس نه راځوی . د کتاب پاته برخه به د دغه ډول معادلو د جذر د شمېرنی عملی طریقو ته وقف کړو .

§ V. د دریمې درجې معادلو حل

د حقيقي ضریبو سره د لمړی او دوهمی درجې معادلاتو حل مو د ښونځي په وخت کې مطالعه کړیدی . د دوهمی درجې معادلی د $ax^2 + bx + c = 0$ په شکل په هغه صورت کې چې دهغی دیسکریمینانت $b^2 - 4ac \geq 0$ وی ، نو حل یې د لاندنیو فورمولو په بڼه طرح کېدی :

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

ددی کتاب په لمړی برخه کې (لمړی برخه ، دوهم فصل ، § XIV) د مختلطو عددو د څېړنی په پای کې مو ثابتې کړه چې پورتنی فورمول د دوهمی درجې معادلو دپاره چې اختیاری مختلط ضریبونه ولری هم صدق کوی .

اوس به نو داخیاری مختلطو ضریبو سره د دریمې درجې معادلو حل تر څېړنی لاندی ونیسو .

فرضوو چې د دریمې درجې معادله

$$a_3y^3 + a_2y^2 + a_1y + a_0 = 0 \quad \dots(1)$$

د a_2, a_1, a_0 او $a_3 \neq 0$ دمختلطو ضریبو سره راکړه سویده . پورتنی معادله کله کله د مکعبی معادلي په نامه هم یادېږي. څرنگه چې $a_3 \neq 0$ دی ، نو د (1) معادلي دواړی خواوی پر a_3 تقسیموو او د (1) معادلي سره معادله (همتولی) معادله لاسته راځي :

$$y^3 + ay^2 + by + c = 0 \quad \dots(2)$$

پداسی حال کی چې $a = \frac{a_2}{a_3}, b = \frac{a_1}{a_3}, c = \frac{a_0}{a_3}$ دی . د (2) معادلي حل د داسی دریمی درجی معادلي سره تعویضو چې په هغه کی ددوهمی درجی د حد ضریب ، یعنی y^2 ضریب ، د صفر سره مساوی وی . په واقعیت کی که $y = x - \frac{a}{3}$ سره کښېږدو ، نو لاندنی معادله به لاسته راسی :

$$\left(x - \frac{a}{3}\right)^3 + a\left(x - \frac{a}{3}\right)^2 + b\left(x - \frac{a}{3}\right) + c = 0$$

یا

$$x^3 - 3x^2 \frac{a}{3} + 3x \frac{a^2}{9} - \frac{a^3}{27} + a\left(x^2 - 2\frac{ax}{3} + \frac{a^2}{9}\right) + bx - \frac{ab}{3} + c = 0$$

$$x^3 + \left(-\frac{1}{3}a^2 + b\right)x + \left(c - \frac{ab}{3} + \frac{2a^3}{27}\right) = 0$$

که $p = b - \frac{1}{3}a^2$ او $q = c - \frac{ab}{3} + \frac{2a^3}{27}$ سره کښېږدو ، نو زموږ معادله به لاندی بڼه ونیسی .

$$x^3 + px + q = 0 \quad \dots(3)$$

اوس نو که د (3) معادلي جذرونه پیدا کړای سو ، نو د (1) معادلي جذرونه په اسانی سره موندلای سو . پدی معنی چې لمړی باید د دریمی درجی نامکملی معادلي (3) حل پیدا کړای سو .

د (3) معادلي حل د $x = u + v$ په بڼه لټوو ، داځکه چې په وروسته کامو کی د نوی متحولو څخه یوه ته یی تکمیلی شرطونه اېږدو .

$$(u + v)^3 + p(u + v) + q = 0$$

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0$$

وروستی معادله بڼی چې د u او v پر متحولو باندی $3uv + p = 0$ د شرط دایښودلو په نتیجه کی د معادلو لاندنی سیستم لاسته راتلای سی :

$$\begin{cases} uv = -\frac{p}{3} \\ u^3 + v^3 = -q \end{cases} \quad \dots(4)$$

د معادلو د (4) سیستم د حل په موخه د سیستم لمړی معادله د درو په طاقت لورو، چې په نتیجه کې یې لاندی سیستم لاسته راځي:

$$\begin{cases} u^3 v^3 = -\frac{p^3}{27} \\ u^3 + v^3 = -q \end{cases} \dots(5)$$

پدی حالت کې د $u^3 v^3 = -\frac{p^3}{27}$ د معادلی د حل سبب نظر د $uv = -\frac{p}{3}$ د معادلی د حل وسبب ته

وسپېږه دی، ځکه نو د نوی سیستم، یعنی (5) سیستم حل باید د $uv = -\frac{p}{3}$ په معادله کې د تعویض په نتیجه کې امتحان سی.

که (5) سیستم ته نظر واچوو، نو د ویتا د قضیې پر اساس استدلال کولای سو چې u^3 او v^3 دمختلطو ضریبو سره د لاندنی دوهمی درجی معادلی جذرونه دی:

$$z^2 + qz - \frac{p^3}{27} = 0$$

څرنګه چې $z_{1,2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ دی، پدی معنی چې او $u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$

$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \text{ دی. ددی ځایه:}$$

$$\begin{aligned} u &= \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \\ v &= \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \end{aligned} \dots(6)$$

دی پدی ترتیب د $x = u + v$ څخه د x قیمت لاسته راځي:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \dots(7)$$

د (7) فورمول د (3) معادلی جذرونه د هغی د ضریبو د جنسه د دریم او دوهم جذر په مرسته ارائه کوی. نوموړی فورمول د کاردانو (ایتالوی ریاضیدان کاردانو Cardano) د فورمول په نامه یادیری.

د (6) فورمول پر اساس د u او v متحولونه دری مختلفه قیمتونه ځانته اخلی. دکاردانو د فورمولو د

عملی کولو دپاره باید یوازی هغه قیمتونه وټاکو چې $uv = -\frac{p}{3}$ وی.

څرگنده ده چې (لمړۍ برخه، دوهم فصل، § XIV) په مختلطو عددو کې د يوه عدد مکعب جذر درې قيمته 1، $\varepsilon = -\frac{1}{2} + \sqrt{\frac{3}{2}}i$ او $\varepsilon^2 = -\frac{1}{2} - \sqrt{\frac{3}{2}}i$ لري.

فرضوو چې u_1 د u د جذر د درو قيمتو څخه يو قيمت دی، نو $u_1 \varepsilon^2$ او $u_1 \varepsilon$ يې د باقیمانده و جذرو دوه قيمته دی. په رشتيا هم:

$$(u_1 \varepsilon)^3 = u_1^3 \varepsilon^3 = 1.1 = 1; (u_1 \varepsilon^2)^3 = u_1^3 \varepsilon^6 = 1.(\varepsilon^3)^2 = 1^2 = 1$$

په همدا ډول که v_1 د v د جذر د درو قيمتو څخه يوداسی قيمت وی چې $u_1 v_1 = -\frac{p}{3}$ وی، نو $v_1 \varepsilon$ او $v_1 \varepsilon^2$ د نوموړی جذر پاته دوه قيمتونه دی.

همدا ډول، څرنگه چې $(u_1 \varepsilon)(v_1 \varepsilon^2) = u_1 v_1 \varepsilon^3 = u_1 v_1 = -\frac{p}{3}$ او $(u_1 \varepsilon^2)(v_1 \varepsilon) = u_1 v_1 \varepsilon^3 = u_1 v_1 = -\frac{p}{3}$ دی، نو پدی لحاظ د (3) معادلي درې جذرونه په لاندی شکل ليکلای سو.

$$\begin{cases} x_1 = u_1 + v_1 \\ x_2 = u_1 \varepsilon + v_1 \varepsilon^2 \\ x_3 = u_1 \varepsilon^2 + v_1 \varepsilon \end{cases} \quad \dots(8)$$

د ε او ε^2 د قيمتو د تعویض په نتيجه کې لاندنی فورمولونه لاسته راځي:

$$\begin{cases} x_1 = u_1 + v_1 \\ x_2 = u_1 \left(-\frac{1}{2} + \sqrt{\frac{3}{2}}i\right) + v_1 \left(-\frac{1}{2} - \sqrt{\frac{3}{2}}i\right) = -\frac{u_1 + v_1}{2} + \frac{u_1 - v_1}{2} \sqrt{3}i \\ x_3 = u_1 \left(-\frac{1}{2} - \sqrt{\frac{3}{2}}i\right) + v_1 \left(-\frac{1}{2} + \sqrt{\frac{3}{2}}i\right) = -\frac{u_1 + v_1}{2} - \frac{u_1 - v_1}{2} \sqrt{3}i \end{cases} \quad \dots(9)$$

پورتني فورمولونه بنسټي چې د (3) معادلي د درو جذرو د شمېرنې دپاره کافی ده چې د u_1 او v_1 قيمتونه داسی لاسته راوړو چې هغوی د (4) د معادلو د سيستم حل وی.

په هغه صورت کې چې د p او q عددونه حقيقي عددونه وی، (3) معادله د هغي په جزئیاتو سره تر مطالعی لاندی نیسو. $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$ ايردو.

قضيه ۱- که $\Delta > 0$ وی، نو د (10) $x^3 + px + q = 0$ معادله د چې ضریبونه يې حقيقي عددونه وی، يو حقيقي جذر او دوه مختلط مزدوج جذرونه لري.

ثبوت - فرضوو چې $\Delta > 0$ ده. بیا نویه (6) فورمول کې د مربع تر جذر لاندی عددونه مثبت دی. پدی معنی چې د مکعب جذر هر قيمت حقيقي عدد دی. که فرض کړو چې u_1 او v_1 د مکعب جذر حقيقي

قیمتونه وی ، نو د (9) فورمول پر اساس استنباط کیری چې x_1 یې حقیقی جذر ، x_2 او x_3 د معادلي مختلط مزدوج جذرونه دی. څرنگه چې $u_1 \neq v_1$ دی ، نو x_2 او x_3 حقیقی عددونه نسی کیدای.

قضیه ۲- که $\Delta=0$ وی ، نو (10) معادله درې حقیقی جذرونه لری ، پداسی حال کی چې دوه جذرونه یې سره مساوی دی.

ثبوت - که $\Delta=0$ وی ، نو $u = \sqrt[3]{-\frac{q}{2}}$ او $v = \sqrt[3]{-\frac{q}{2}}$ دی . که فرض کړو چې u_1 د لمری حقیقی جذر قیمت دی ، نو v_1 هم حقیقی عدد دی ، ځکه چې $u_1 v_1 = -\frac{p}{3}$ دی. د $u_1 = v_1$ په حالت کی (9) فورمولونه لاندی بڼه غوره کوی:

$$\begin{cases} x_1 = 2u_1 \\ x_2 = -u_1 \\ x_3 = -u_1 \end{cases}$$

لیدل کیری چې $x_1, x_2, x_3 \in \mathbb{R}$ او $x_2 = x_3$ دی.

قضیه ۳- که $\Delta < 0$ وی ، نو (10) معادله درې مختلفه حقیقی جذرونه لری.

ثبوت - د $\Delta < 0$ د شرط پر اساس د (6) تر مکعب جذر لاندی مختلط مزدوج عددونه دی. پدی معنی چې u او v ټول قیمتونه مختلط عددونه دی. همدا ډول د (10) معادلی د جذرو څخه لږ تر لږه یو جذر باید حقیقی عدد وی. که فرض کړو چې د $x_1 = u_1 + v_1$ جذر یې حقیقی عدد وی ، نو $u_1 + v_1 \in \mathbb{R}$ او

$u_1 v_1 = -\frac{p}{3} \in \mathbb{R}$ دی . ځکه نو u_1 او v_1 د $t^2 - x_1 t - \frac{p}{3} = 0$ دوهمی درجی معادلی ، چې ضریبونه

یې حقیقی عددونه دی، جذرونه دی. $-x_1$ او $-\frac{p}{3}$ حقیقی عددونه دی. پدی صورت کی $u_1 - v_1 = -d$

موهومی عدد دی ، د (9) فورمول پر اساس $x_3 = -\frac{1}{2}x_1 + d\frac{\sqrt{3}}{2}$ او $x_2 = -\frac{1}{2}x_1 - d\frac{\sqrt{3}}{2}$ دی ، پدی معنی چې ټوله درې جذرونه په خپل منح کی مختلف او حقیقی عددونه دی.

پدی ترتیب مو د دریمي درجی معادلو د جذرو د شمېرنی د پاره فورمولونه پیدا کړل. لاسته راوړل سوی فورمولونه دونه عملی اړخ نلری ، ځکه په هغه صورت کی چې راکړه سوی معادله چې ضریبونه یې حقیقی عددونه وی او $\Delta < 0$ وی ، نو کاردانو د فورمولو څخه په استفادی سره باید دمختلطو عددو دریم جذر وشمېرو. اکثرأ د معادلو نام جذرونه لا په پیچلي بڼه ارائه کوی.

بیلگه - د $x^3 - x - 6 = 0$ معادلي جذرونه پیدا کړو.

حل - څرنگه چې $\Delta = \frac{36}{4} - \frac{1}{27} = 8\frac{26}{27} > 0$ ده ، نو راکړه سوی معادله یو حقیقی جذر لری چې هغه د کاردانو د فورمول پر اساس عبارت دی له :

$$x_1 = \sqrt[3]{3 + \sqrt{\frac{242}{27}}} + \sqrt[3]{3 - \sqrt{\frac{242}{27}}}$$

خو اسانه امتحان کيدای سى چي $x_1=2$ د نوموړى معادلي جذر دى.

VI§. د څلرمي درجي معادلو حل

فرضوو چي دڅلرمي درجي معادله داسى راکړه سوى ده چي ضريبونه يي مختلط عددونه دى:

$$a_4y^4 + a_3y^3 + a_2y^2 + a_1y + a_0 = 0 \quad \dots(1)$$

څرنګه چي $a_4 \neq 0$ دى ، نو د (1) معادله داسى هم ليکلای سو:

$$y^4 + ay^3 + by^2 + cy + d = 0 \quad \dots(2)$$

پداسى حال کى چي $a = \frac{a_3}{a_4}, b = \frac{a_2}{a_4}, c = \frac{a_1}{a_4}, d = \frac{a_0}{a_4}$ دى.

که د $y = x - \frac{a}{4}$ پر اساس د راکړه سوى معادلي متحول ته تغيير ورکړو، نو لاندني معادله به لاسته راسى:

$$\left(x - \frac{a}{4}\right)^4 + a\left(x - \frac{a}{4}\right)^3 + b\left(x - \frac{a}{4}\right)^2 + c\left(x - \frac{a}{4}\right) + d = 0$$

پورتني مساوات ساده کوو:

$$x^4 - 4x^3 \frac{a}{4} + 6x^2 \frac{a^2}{16} - 4x \frac{a^3}{64} + \frac{a^4}{256} + ax^3 - 3 \frac{a^2}{4} x^2 + 3 \frac{a^3}{4} x - \frac{a^4}{64} +$$

$$+ bx^2 - \frac{ab}{2} x + \frac{a^2b}{16} + cx - \frac{ac}{4} + d = 0$$

د مساوات غړي د x د طاقت پر اساس سره يوځای کوو:

$$x^4 + \left(b - \frac{3a^2}{8}\right)x^2 + \left(c + \frac{11a^3}{16} - \frac{ab}{2}\right)x + \left(\frac{a^2b}{16} - \frac{ac}{4} + d - \frac{3a^4}{256}\right) = 0$$

اوس نو که $r = \frac{a^2b}{16} - \frac{ac}{4} + d - \frac{3a^4}{256}$ او $q = c + \frac{11a^3}{16} - \frac{ab}{2}, p = b - \frac{3a^2}{8}$ کښېږدو، نو وروستي معادله به ځانته لاندی بڼه غوره کي:

$$x^4 + px^2 + qx + r = 0 \quad \dots(3)$$

پدی ډول مو وښودل چي د (1) معادلي حل و لږڅه ساده تری معادلي (3) و حل ته راجع کولای سو.

اوس به نو دلته د ایټالوی ریاضی پوه فراری (Lodovico Ferrari) چې د کاردانو تر تربیې لاندی را لوی سوی و، طریقه تشریح کړو. په نوموړي طریقه کی ددی واقعیت څخه کار اخلی چې (3) معادله د

$$[f(x)]^2 - [g(x)]^2 = 0 \quad \dots(4)$$

په شکل پداسی ډول راوړی چې د $f(x)$ او $g(x)$ د پولینومو درجه تر دوه اضافه نه وی. څرگنده ده چې په عمومی شکل و مرستتي پارامتر و ته ضرورت پیداکیږی. (4) معادله په اسانی سره حلیدای سی، ځکه چې د معادلو د لاندني مجموعي سره همثولي(معادل) دی:

$$\begin{cases} f(x) - g(x) = 0 \\ f(x) + g(x) = 0 \end{cases}$$

عملاً د (3) معادلي څخه پورتنی د معادلو مجموعه په لاندی ډول سره لاسته راوړای سو:

$$\begin{aligned} x^4 + px^2 + qx + r &= (x^4 + 2\frac{p}{2}x^2 + \frac{p^2}{4} + \alpha^2 + 2\alpha x^2 + \alpha p) + \\ + qx + r - 2\alpha x^2 - \frac{p^2}{4} - \alpha^2 - \alpha p &= \\ &= (x^2 + \frac{p}{2} + \alpha)^2 - (2\alpha x^2 - qx + (\frac{p^2}{4} + \alpha^2 + \alpha p - r)) = 0 \end{aligned}$$

پداسی حال کی چې α د مرستتي پارامتر و څخه یو پارامتر دی. ځکه نو (3) معادله په لاندی ډول لیکلای سو:

$$(x^2 + \frac{p}{2} + \alpha)^2 - (2\alpha x^2 - qx + (\frac{p^2}{4} + \alpha^2 + \alpha p - r)) = 0 \quad \dots(5)$$

اوس نو α داسی ټاکو څو د $h(x) = 2\alpha x^2 - qx + (\frac{p^2}{4} + \alpha^2 + \alpha p - r)$ مکمله مربع جوړه سی. ددی اسیته باید $h(x)$ دوهمه درجه مضاعف جذرونه ولری، پدی معنی چې د هغه دیسکریمینانت باید د صفر سره مساوی وی. یعنی:

$$q^2 - 4.2\alpha(\frac{p^2}{4} + \alpha^2 + \alpha p - r) = 0 \quad \dots(6)$$

لکه چې لیدل کیږی (6) معادله د مختلطو ضریبو سره دریمه درجه معادله ده.

$$8\alpha^3 + 8p\alpha^2 + (2p^2 - 8r)\alpha - q^2 = 0 \quad \dots(7)$$

د پنجم فصل د § XIII څخه پوهیږو چې (7) معادله دری مختلط جذرونه لری. فرضوو چې α_0 یې دهغو درو جذرو څخه یو جذر وی. د کاردانو د فورمول پر اساس α_0 تعینولای سو.

(7) مه معادله د (3) می معادلي تجزیه کونکي (Resolvent) په نامه یادیری. د α د پارامتر ددی ډول شمېرنی په نتیجه کی د $h(x)$ پولینوم په لاندی ډول سره لیکلای سو:

$$h(x) = 2\alpha_0 \left(x - \frac{q}{4\alpha_0}\right)^2$$

ځکه نو (5)مه معادله په لاندې ډول لیکلای سو:

$$\left(x^2 + \frac{p}{2} + \alpha_0\right)^2 - 2\alpha_0 \left(x - \frac{q}{4\alpha_0}\right)^2 = 0$$

$$\left(x^2 + \frac{p}{2} + \alpha_0\right)^2 - \left[\sqrt{2\alpha_0} \left(x - \frac{q}{4\alpha_0}\right)\right]^2 = 0$$

وروستنې معادله د معادلاتو د لاندینو مجموعې سره معادله ده:

$$\begin{cases} x^2 - \sqrt{2\alpha_0}x + \left(\frac{p}{2} + \alpha_0 + \frac{q}{2\sqrt{2\alpha_0}}\right) = 0 \\ x^2 + \sqrt{2\alpha_0}x + \left(\frac{p}{2} + \alpha_0 - \frac{q}{2\sqrt{2\alpha_0}}\right) = 0 \end{cases} \quad \dots(8)$$

څرنگه چې ټوله تر سره سوی تبدیلات په خپل منځ کی معادل دی ، ځکه نو (3)مه معادله د (8)مې معادلاتو د مجموعې سره معادل دی. پدی ترتیب سره د (3)مې معادلې د ټولو جنرو دپاره د α_0 د پارامتر له جنسه فورمولونه طرح کولای سو. خو دغه فورمولونه اوږده او د استفادې وړ ندی. ځکه نو بڼه به داوی چې پر هری مشخصې معادلې باندې په بیله توگه تبدیلات صورت ونیسی.

په نتیجه کی استنباط کیدای سی چې د څلرمې درجې د (3)مې معادلې حل د (7) تجزیه کیدونکی او (8) دوهمې درجې ددو معادلو و مجموعې ته څرمه کیږی.

بیلگه - لاندنې معادله حلوو.

$$y^4 - 2y^3 + 2y^2 + 4y - 8 = 0$$

حل - که د $y = x + \frac{1}{2}$ پر اساس د y متحول ته تغییر ورکړو. نو لاندې معادله به لاسته راسی:

$$\left(x + \frac{1}{2}\right)^4 - 2\left(x + \frac{1}{2}\right)^3 + 2\left(x + \frac{1}{2}\right)^2 + 4\left(x + \frac{1}{2}\right) - 8 = 0$$

تر ساده کولو وروسته د $x^4 + \frac{x^2}{2} + 5x - \frac{91}{16} = 0$ معادله لاسته راځي.

اوس نو د α پارامتر ور داخلوو او مکمله مربع جلا کوو:

$$(x^2 + \frac{1}{4})^2 + 5x - \frac{91}{16} - \frac{1}{16} = 0$$

$$(x^2 + \frac{1}{4} + \alpha)^2 - 2\alpha x^2 - \frac{\alpha}{2} - \alpha^2 + 5x - \frac{28}{4} = 0$$

$$(x^2 + \frac{1}{4} + \alpha)^2 - (2\alpha x^2 - 5x + \frac{\alpha}{2} + \alpha^2 + \frac{23}{4}) = 0$$

تجزیه کونکی او د هغه حلونه بیلوو:

$$25 - 4.2\alpha(\frac{\alpha}{2} + \alpha^2 + \frac{23}{4}) = 0$$

$$8\alpha^3 - 4\alpha^2 + 46\alpha - 25 = 0$$

د کاردانو د فورمولو څخه په استفادی سره په اسانۍ سره لیدل کیږی چې $\alpha = \frac{1}{2}$ د نوموړی معادلی

حل دی. ځکه نو معادله ځانته لاندی ډول بڼه غوره کوی:

$$(x^2 + \frac{3}{4})^2 - (x^2 - 5x + \frac{25}{4}) = 0$$

$$(x^2 + \frac{3}{4})^2 - (x - \frac{5}{2})^2 = 0$$

د وروستی معادلی څخه د معادلو لاندنی مجموعه لاسته راځی:

$$\begin{cases} x^2 - x + \frac{3}{4} = 0 \\ x^2 + x + \frac{7}{4} = 0 \end{cases}$$

د معادلو د وروستی مجموعی تر حلولو ورسته

$$x_{1,2} = \frac{1 \pm \sqrt{1-13}}{2} = \frac{1 \pm 2\sqrt{3}i}{2}$$

$$x_{3,4} = \frac{1 \pm \sqrt{1+7}}{2} = \frac{-1 \pm 2\sqrt{2}}{2}$$

لاسته راځی.

بلاخره د اصلی معادلی جذرونه داسی لاسته راوړای سو:

$$y_1 = x_1 + \frac{1}{2} = \frac{1+2\sqrt{3}i}{2} + \frac{1}{2} = 1 + \sqrt{3}i$$

$$y_2 = x_2 + \frac{1}{2} = \frac{1 - 2\sqrt{3}i}{2} + \frac{1}{2} = 1 - \sqrt{3}i$$

$$y_3 = x_3 + \frac{1}{2} = \frac{-1 + 2\sqrt{2}}{2} + \frac{1}{2} = \sqrt{2}$$

$$y_2 = x_2 + \frac{1}{2} = \frac{-1 - 2\sqrt{2}}{2} + \frac{1}{2} = -\sqrt{2}$$

لکه مخ کی چي مو ذکر کړه دریمي او څلرمي درجي معادلو د حل فورمولونه په شپاړسمي پېرې کی د ایټالوی ریاضی پوهانو کاردانو او فراری له خوا طرح سوه تر هغه وروسته په طبیعي شکل د پنځمو او تر هغه لوړو درجو معادلو د حل د فورمولو د پیدا کولو سوال طرح سو. پدی لاره کی څه ناڅه دری سوه کاله ریاضی پوهان د ورته فورمولو په طرح کولو بریالی نسول، تر څوچي په شلمه پېرې کی نارویژی ریاضی پوه ابل Abel ثابته کړه چي و ذکر سوو فورمولوته ورته فورمولونه د n درجه ای (n ≥ 5) معادلو دپاره وجود نلری. روسته له هغه فرانسوی ریاضی پوه گالوا Galois دغه مسئله چي په کومو حالتو کی د الجبری څلوریزو عملیو او د جذر د عملیې څخه په استفادی سره د n درجه ای (n ≥ 5) معادلو جذرونه د هغوی د ضریبو د جنسه لاسته راوړلای سو، په پوره ډول حل کړه. د گالوا د څېړنو نتیجه په الجبر کی دداسی تیوری لکه د گروپ تیوری منځ ته راوړه او د هغه راهیسی الجبر د معادلو دڅېړنو په څیر نه بلکه د یوه داسی علم په څیر چي په طبیعت کی پر مختلفو شیانو باندی د عملیو خاصیتونه څېری، تبارز وکی.

ددی کتاب په مخکنیو فصلو کی ددی ډول څېړنو، لکه ماترکسونه، تعویضونه، د باقیمانده و ټولگی او پولینومو، د بېلگو سره مخامخ سوو.

VIII. د حقیقی ضریبو سره د پولینومو د حقیقی جذرو سرحد

په دوو تېرو پاراگرافو کی مو د دریمي او څلرمي درجي معادلو چي ضریبونه یی مختلط عددونه وی، د حل طریقې و څېړلی. د ځینو عملی مسئلو د حل په وخت کی اکثرأ دداسی معادلو سره مخامخ کیږو چي د هغوی درجه تر څلورو لوړه او ضریبونه یی په ندرت سره تام عددونه وی. ځکه نو د حقیقی جذرو د تعداد د تعیین طریقه، د جذرو د سرحدو او یا د جذرو په منځ کی د فاصلی د محاسبی د طریقو مسئله طرح کولای سو. د ذکر سوو مسئلو په هکله څېړني په خپل وخت کی د الجبر د کورس محتوی وه.

پدی برخه کی به مور یوازی په هغو نتېجو اکتفاء وکو چي پوهیدل یی د ریاضی د بنونکی دپاره ضروری ده.

د حقیقی ضریبو سره د پولینومو د حقیقی جذرو پر تعیین باندی یو لنډ مکث کوو. لمړی خو د II § څخه پوهیږو چي هر پولینوم چي درجه یی طاق وی لږ تر لږه یو حقیقی جذر لری. په ډیرو حالتو کی د حقیقی ضریبو سره د معادلی حقیقی جذرونه په ډیره ساده طریقه چي دفرانسوی ریاضی پوه او فیلسوف دیکارت له خوا ثابته سویده، و ټاکو. تر ټولو دمخه باید لاندني دوه ټکی په پام کی ولرو:

۱- فرضوو چي د $f(x)$ پولینوم د $f(x)=0$ په معادله کی مضاعف جذرونه نلری، ځکه چي ټوله جذرونه جلا کولای سو (پنځم فصل، §XIV وگوری).

۲- که د C_1, C_2, \dots, C_m د حقیقی عددو لار (ترادف) راکړه سوی وی، نو په نوموړې لار کې د علامو د تغییراتو د مجموعی تر مفهوم لاندی د هغو گاونډیو عددو مجموعه چي مختلفې علامی ولری، افاده کوو. په دغه ډول لار کی د صفر څخه صرف نظر کوو. د بېلگي په ډول:

د $1, -5, -4, 3, -2$ په لار کی د علامو د تغییر شمېر مساوی په درې سره دی. او د $6, 1, 2, 3$ په لاری کی د علامی تغییر وجود نلری. خو د $-4, -1, 0, 2, -8$ په لار کی دوه د علامی تغییرونه وجود لری.

د دیکارت طریقہ، د حقیقی ضریبو سره د

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad \dots(1)$$

د پولینوم د مثبتو جذرو شمېر یا د $a_0, a_1, \dots, a_{n-1}, a_n$ په لار کی د علامو د تغییر د شمېر سره مساوی کیری او یا شمېر یې د علامو د تغییر د شمېر څخه د طاق عدد په اندازه لږ دی. لوستونکی د پورتنی واقعیت ثبوت په [1] کی موندلای سی.

د دیکارت د طریقې څخه د پولینوم د منفی جذرو د شمېر د موندلو دپاره هم کار اخیستلای سو. ددی موخې دپاره د (1) په مساوات کی د x متحول د $-y$ یعنی $x = -y$ سره عوض کړو.

بیلگه ۱- د $x^5 + 2x^3 + x^2 - 2x - 3 = 0$ معادله یوازې یو مثبت جذر لری.

که $x = -y$ سره عوض کړو، نو د $-y^5 - 2y^3 + y^2 + 2y - 3 = 0$ معادله لاسته راځي. څرنگه چي د ضریبو په علامو کی یې دوه تغییره راځي، نو یا دوه او یا هیڅ منفی جذر نلری.

په §II کی د لمړی قضیې د نتبجي څخه یې مشاهده کولای سو چي د حقیقی ضریبو سره د پولینومو د جذرو د سرحد په هکله لاندنی قضیه صدق کوی.

قضیه ۱- د حقیقی ضریبو سره د $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ د پولینوم ټول جذرونه د $]-N_0, N_0[$ په انتروال کی پراته دی، پداسی حال کی چي:

$$N_0 = 1 + \frac{A}{|a_n|} \quad \text{او} \quad A = \max\{|a_{n-1}|, |a_{n-2}|, \dots, |a_1|, |a_0|\} \text{ دی.}$$

بیلگه - د $3x^5 - 2x^4 + x^3 + x^2 - 2x - 3 = 0$ په پولینوم کی $A=3$ او $a_5 = 3$ دی، ځکه نو

$$N_0 = 1 + \frac{3}{3} = 2 \quad \text{دی. په نتیجه کی زموږ د معادلي د حقیقی جذرو انتروال }]-2, 2[\text{ دی.}$$

د پولینومو د حقیقی جذرو د دقیقو سرحدو د پیدا کولو دپاره نوری طریقې هم وجود لری، چي یو د هغو څخه د نیوتن د طریقې په نامه یادیری او پر لاندنی قضیه استوار ده.

قضیه ۲ (نیوتن) - د M عدد د $f(x)$ د پولینوم د مثبتو جذرو لورنی (فوقانی) سرحد دی ، که د $x=M$ دپاره د $f(x)$ د پولینوم قیمت مثبت او دهغه د ټولو مشتقو قیمتونه غیر منفي وی.

د قضیې ثبوت د ټایلور د فورمول څخه چې په انالایز کی ورسره مخامخ سوی یاست ، نیغ استنباط کیږی.

$$f(x) = f(M) + \frac{f'(M)}{1}(x-M) + \frac{f''(M)}{2!}(x-M)^2 + \dots + \frac{f^{(n)}(M)}{n!}(x-M)^n$$

په رشتیا هم د $x \geq M$ دپاره $f(x) > 0$ دی. پدی معنی چې د $f(x)$ د پولینوم جذر تر M کوچنی دی. څرنګه چې د $f(x)$ د پولینوم د حقیقی جذرو لورنی سرحد پیدا کولای سو ، نو د لورنی سرحد څخه په استفادی سره د منفي جذرو لورنی او کبنتی سرحدونه ټاکلای سو او همدا ډول د مثبتو جذرو کبنتی سرحد هم لاسته راوړلای سو. ددی حقیقت د څرګندولو دپاره لاندنی پولینومونه مشاهده کوو:

$$g_1(x) = x^n f\left(\frac{1}{x}\right)$$

$$g_2(x) = f(-x)$$

$$g_3(x) = x^n f\left(-\frac{1}{x}\right)$$

که فرض کړو چې N_3, N_2, N_1 په ترتیب سره د $g_2(x), g_1(x)$ او $g_3(x)$ د پولینومو د جذرو لورنی سرحدونه وی، نو د بیلګې په ډول $\frac{1}{N_1}$ د $f(x)$ د پولینوم د مثبتو جذرو کبنتی سرحد دی.

حقیقتاً ، که α د $f(x)$ د پولینوم مثبت جذر وی ، نو $\frac{1}{\alpha}$ د $g_1(x)$ د پولینوم مثبت جذر دی. ځکه نو

$$\frac{1}{\alpha} < N_1 \quad \text{او} \quad \alpha > \frac{1}{N_1} \quad \text{دی.}$$

همدا ډول د N_2 او $-\frac{1}{N_3}$ عددونه ازمویلای سو چې د $f(x)$ د پولینوم د منفي جذرو کبنتی او لورنی پولی (سرحدونه) دی.

بیلګه ۲- غواړو چې د $f(x) = 3x^5 - 2x^4 + x^3 + x^2 - 2x - 3$ د حقیقی جذرو سرحدونه پیدا کړو.

حل - په لمړې بیلګه کی مو ولیدل چې د نوموړی پولینوم حقیقی جذرونه د $[-2, 2]$ په انتروال کی پراته دی. لاندنی پولینوم څېړو:

$$\begin{aligned} g(x) &= x^5 \left(3\left(\frac{1}{x}\right)^5 - 2\left(\frac{1}{x}\right)^4 + \frac{1}{x^3} + \frac{1}{x^2} - \frac{2}{x} - 3 \right) = \\ &= 3 - 2x + x^2 + x^3 - 2x^4 - 3x^5 = \\ &= -(3x^5 + 2x^4 - x^3 - x^2 + 2x - 3) = -s(x) \end{aligned}$$

د $s(x)$ پر پولینوم باندی د نیوتن طریقہ عملی کوو:

$$s(x) = 3x^5 + 2x^4 - x^3 - x^2 + 2x - 3$$

$$s'(x) = 15x^4 + 8x^3 - 3x^2 - 2x + 2$$

$$s''(x) = 60x^3 + 24x^2 - 6x - 2$$

$$s'''(x) = 180x^2 + 48x - 6$$

$$s^{(iv)}(x) = 360x + 48$$

$$s^{(v)}(x) = 360$$

لیدل گیری چي د پورتنی ټولو پولینومو قیمتونه د $x=1$ دپاره مثبت دی. یعنی $N_1=1$ دی. ددی خایه استدلال کولای سو چي د $f(x)$ د پولینوم مثبت جذرونه د $[1,2[$ په انټروال کی پراته دی.

همدا ډول که د

$$g_2(x) = x^5 f\left(\frac{1}{x}\right) = x^5 \left(-3\frac{1}{x^5} - \frac{2}{x^4} - \frac{1}{x^3} + \frac{1}{x^2} + \frac{2}{x} - 3\right) = \\ = -(3x^5 - 2x^4 - x^3 + x^2 + 2x + 3)$$

پولینوم مشاهده کوو، نو $N_3=1$ پیدا کوو. ځکه نو د $f(x)$ د پولینوم جذرونه د $]-2,-1[$ په انټروال کی پراته دی.

ددی دپاره چي وکولای سو چي د پولینومو د جذرو د تقریبی محاسبی متودو څخه (لکه د خطی انټرپولیشن، نیوتن، ... او داسی نور) کار واخلو، نو، څه ډول چي په انالایز کی ورسره بلد یاست، انټروالونه داسی جدا کوو، څو په هغه کی دقیقاً یو جذر پروت وی. دغه مسئله به په لاندنی پاراگراف کی تر مطالعی لاندی ونیسو.

VIII §. د شتورم (Charles-Francois Sturm) په طریقہ د پولینوم د جذرو تعیینول

فرضوو چي د حقیقی ضریبو سره د $f(x)$ پولینوم داسی راکړه سوی دی چي مضاعف جذرونه نلری او

$\deg f(x) > 2$ وی. پدی حالت کی د $f(x)$ پولینوم د خپل مشتق سره، یعنی $f'(x)$ سره متبائن دی (د

پنځم فصل، § XIV، د لمړی قضیې نتیجی وگوری). د $f(x)$ او $f'(x)$ د پولینومو دپاره د

$$f_1(x), f_2(x), \dots, f_m(x) = \text{Const}$$

د $f(x)$ پولینوم د $f'(x)$ پر پولینوم وپشو:

$$\begin{aligned}
f(x) &= f'(x).s_1(x) + r_1(x) \rightarrow f_1(x) = -r_1(x); \\
f'(x) &= f_1(x).s_2(x) + r_2(x) \rightarrow f_2(x) = -r_2(x); \\
f_1(x) &= f_2(x).s_3(x) + r_3(x) \rightarrow f_3(x) = -r_3(x); \\
&\vdots \\
f_{k-1}(x) &= f_k(x).s_{k+1}(x) + r_{k+1}(x) \rightarrow f_{k+1}(x) = -r_{k+1}(x); \\
&\vdots \\
f_{m-2}(x) &= f_{m-1}(x).s_m(x) + r_m(x) \rightarrow f_m(x) = -r_m \in \mathbb{R}; \\
f_{m-1}(x) &= f_m(x).s_{m+1}(x)
\end{aligned} \tag{1}$$

د پورتنیو افادو (1) د سیستم د اقلیدس د الگوریتم سره چي په پنځم فصل ، § VI کی مو تشریح کی ، دادی چي ددو هم گام په شمول په ټولو وروستیو قدمو کی دوپش عملیه پر پاتی پولینوم باندی د مخالفی علامی سره صورت نیسی.

تعریف ۱- د (2) $f(x), f'(x), f_1(x), f_2(x), \dots, f_{m-1}(x), f_m(x)$ د پولینومو لار (ترادف) د $f(x)$ د پولینوم دپاره د شتورم د پولینومو د لار په نامه یادیری.

د شتورم په طریقه کی مورته د شتورم پولینومونه دونه مهم ندی ، بلکه یوازی قیمتونه یی او هغه هم د عددی قیمتو علامی مورته په زړه پوری دی ، ځکه نو د (2) لار پولینومونه تر مثبت ثابتته ضریب په دقت سره پیدا کولای سو. پدی معنی چي د نامکمل وپش په پروسه کی اجازه لرو چي د ضرورت په وخت کی پولینوم په مثبت حقیقی عدد کی ضرب کړو.

بیلگه ۱- د $f(x) = x^4 - 2x^3 - 2x - 1$ د پاره د شتورم د پولینومو لار پیدا کړو.

حل -

$$f'(x) = 4x^3 - 6x^2 - 2 = 2(2x^3 - 3x^2 - 1)$$

د $\frac{1}{2}f'(x) = 2x^3 - 3x^2 - 1$ پر پولینوم باندی نامکمل وپشاجراء کوو:

$$\begin{array}{r}
x^4 - 2x^3 - 2x - 1 \\
2x^4 - 4x^3 - 4x - 2 \\
\hline
-2x^4 + 3x^3 + x \\
\hline
- x^3 - 3x - 2 \\
-2x^3 - 6x - 4 \\
\hline
+2x^3 + 3x^2 + 1 \\
\hline
-3x^2 - 6x - 5
\end{array}$$

دوپش په پورتنی پروسه کی مو دوه واری (په لمړی او دوهم گام کی) وپشونکی (مقسوم) د 2 په عدد کی ضرب کړیدی.

څرنګه چې $r_1(x) = -3x^2 - 6x - 5$ دی ، نو $f_1(x) = 3x^2 + 6x + 5$ دی. په دوهم ګام کې $\frac{1}{2}f'(x)$ د $f_1(x)$ پر پولینوم باندې وېشو.

$$\begin{array}{r|l} 2x^3 - 3x^2 - 1 & 3x^2 + 6x + 5 \\ 6x^3 - 9x^2 - 3 & 2x - 7 \\ \hline -6x^3 + 12x^2 + 10x & \\ \hline -21x^2 - 10x - 3 & \\ \hline \mp 21x^2 \mp 42x \mp 35 & \\ \hline 32x + 32 & \end{array}$$

په لمړۍ قدم کې مو وېشونکې (مقسوم) د 3 په عدد کې ضرب کېږدی.

څرنګه چې $r_2(x) = 32x + 32$ دی ، نو $f_2(x) = -x - 1$ دی . اوس نو $f_1(x)$ پر $f_2(x)$ باندې وېشو.

$$\begin{array}{r|l} 3x^2 + 6x + 5 & -x - 1 \\ \hline -3x^2 + 3x & -3x - 3 \\ \hline 3x + 5 & \\ \hline -3x + 3 & \\ \hline 2 & \end{array}$$

څرنګه چې $r_3 = 2$ دی ، نو $f_3 = -1$ سره اېږدو.

پدې ډول د راکړه سوی پولینوم دپاره د شتورم د پولینومو لار (ترادف) مو لاسته راوړی او هغه عبارت دی له:

$$x^4 - 2x^3 - 2x - 1, 2x^3 - 3x^2 - 1, 3x^2 + 6x + 5, -x - 1, -1$$

څرګنده ده چې دوهم ، دریم ، څلرم او پنځم پولینوم په ترتیب سره د (2) لار دوهم ، دریم ، څلرم او پنځم پولینوم سره د ثابت ضریب په اندازه تفاوت لری ، خو په راتلونکې کې به وویږو چې دغه تفاوت د جذرو په تفکیک کم رول نلری.

فرضوو چې $x = a \in \mathbb{R}$ دی. اوس نو د (2) لار د پولینومو قیمتونه مطالعه کوو ، یعنی :

$$f(a), f'(a), f_1(a), f_2(a), \dots, f_{m-1}(a), f_m(a) \quad \dots(3)$$

تعریف ۲- په (3) یم لار کې د علامو د تغیر شمېر په $t(a)$ سره ښو او د $x = a$ په نقطه کې د شتورم په لار کې د علامو د تغیر د شمېر په نامه یې یادوو.

بیلګه ۲- د $f(x) = x^4 - 2x^3 - 2x - 1$ پولینوم (لمړۍ بیلګه وګورئ) دپاره د $x = 0$ په نقطه کې د $-1, -1, 5, -1, -1$ لار لاسته راځي او $t(0) = 2$ سره کیږی.

که $x = -1$ وی ، نو $f(-1) = 4, f'(-1) = -6, f_1(-1) = 2, f_2(-1) = 0$ دی ، لار یې $4, -6, 2, 0, -1$ دی او $t(-1) = 3$ دی.

په (2) هم لار کی د شتورم د پولینومو مهمترین خاصیتونه په لاندی ډول سره دی:

خاصیت ۱- د شتورم په لار کی (2) هیڅ دوه گاونډی پولینومونه عین جذر نلری.

په رشتیا هم ، که α د $f_k(x)$ او $f_{k-1}(\alpha)$ د پولینومو جذر وی ، پدی معنی چي $f_{k-1}(\alpha) = f_k(\alpha) = 0$ دی. ځکه نو د لمړی شیمما (1) پر اساس $f_{k-1}(\alpha) = f_k(\alpha) \cdot s_{k+1}(\alpha) + r_{k+1}(\alpha) = 0$ دی.

په همدا ډول $f_{k-2}(\alpha) = \dots = f'(\alpha) = f(\alpha) = 0$ لاسته راوړلای سو. پدی معنی چي α د $f(x)$ د پولینوم مضاعف جذر دی. مور په لمړی سر کی فرض کړی وه چي د $f(x)$ د پولینوم مضاعف جذر نلری. ځکه نو دغه حالت زموږ د فرضیې خلاف دی.

خاصیت ۲- که د α عدد د شتورم د پولینومو د لار په منځ کی د یوه پولینوم جذر وی نو د α په عدد کی دهغه پولینوم د مخکی او وروسته پولینومو قیمتونه مختلفې علامې لری.

حقیقتاً ، که $f_k(\alpha) = 0$ وی ، نو د لمړی خاصیت له مخی $f_{k-1}(\alpha) \neq 0$ او $f_{k+1}(\alpha) \neq 0$ دی . همدا ډول د (1) شیمما څخه $f_{k-1}(\alpha) = f_k(\alpha) \cdot s_{k+1}(\alpha) + r_{k+1}(\alpha) = -f_{k-1}(\alpha)$ لاسته راځی.

خاصیت ۳- که د $f(x)$ د پولینوم د $[\alpha, \beta]$ په انتروال کی جذر ونلری ، نو د هر $a \in [\alpha, \beta]$ دپاره د شتورم په لار کی د $t(a)$ عدد تغییر نه کوی.

په رشتیا هم ، که د $[\alpha, \beta]$ په انتروال کی د $f'(x), \dots, f_{m-1}(x)$ پولینومونه جذر ونلری ، نو د پولینومو د متماذیت د خاصیت له مخی ټوله پولینومونه خپله علامه ساتی ، پدی معنی چي $t(a)$ ثابت دی.

که فرض کړو چي $\alpha \leq \gamma \leq \beta$ ، د شتورم د پولینومو د لار په منځ کی د کم پولینوم جذر وی ، د بېلګی په توګه د $f_k(\alpha) = 0$ وی ، نو د دوهم خاصیت له مخی $f_{k-1}(\alpha)$ او $f_{k+1}(\alpha)$ باید مختلفې علامی ولری. دلته بیا د ریاضی د انا لایز پر قضیه باندی تکیه کوو او د $[\gamma - \delta, \gamma + \delta]$ شاوخوا داسی موندلای سو چي $f_{k-1}(\alpha)$ او $f_{k+1}(\alpha)$ خپله علامه ساتی.

په اسانی سره لیدل کیری چي د $[\gamma - \delta, \gamma + \delta]$ د انتروال د ټولو عددو a دپاره د

$f_{k-1}(a), f_k(a), f_{k+1}(a)$ په لار کی د علامی د تغییر شمېر ثابت او مساوی په یوه سره کیری.

که $f_{k-1}(a) < 0$ وی ، نو د $+, -, -$ ؛ $+, 0, -$ ؛ یا $+, +, -$ امکانات وجود لری. که $f_{k-1}(a) > 0$ وی ، نو د $-, -, +$ ؛ $-, 0, +$ ؛ او یا $-, +, +$ امکانات وجود لری.

د شتورم د لار د ټولو پاته پولینومو دپاره یوازی لاندنی دوه امکانه وجود لری:

(1) د $x = \gamma$ دپاره ټوله پاته پولینومونه مساوی په صفر سره کیری ، پدی معنی چي γ د هغو ټولو جذر دی.

(2) ځنی گاونډی پولینومونه (خو هغه پولینومونه چي د $f_k(x)$ سره گاونډی نه وی !) د $x = \gamma$ دپاره د صفر سره مساوی کیری.

په لمړۍ حالت کې د $x=\gamma$ په کوچني شاوخوا کې خپله علامه ساتي. په دوهم حالت کې ، څرنگه لکه مخکې چې مو ولیدل، د هر یوه دغه ډول پولینومو او د هغه دوو گاونډیو پولینومو د علامې تغیر ثابت او مساوی په یوه سره کیږي.

په نتیجه کې ویلای سو چې د ټولو $a \in [\alpha, \beta]$ دپاره د علامو عمومي تغیر ثابت پاته کیږي.

خاصیت ۴ - که د x د تزايد په وخت کې ، د $f(x)$ د پولینوم د جذر سره منطبق سی، نو شتورم په لار کې د علامو تغیر د یوه په اندازه کميږي.

ثبوت - فرضوو چې $f(\gamma)=0$ دی ، نو $f'(\gamma) \neq 0$ دی . د δ عدد داسی ټاکو چې د $[\gamma-\delta, \gamma+\delta]$ په شاوخوا کې د $f'(x)$ پولینوم خپله علامه وساتي.

که $f'(x) > 0$ وی ، نو د $[\gamma-\delta, \gamma+\delta]$ په انټروال کې $f(x)$ متزایده ده او د $x=\gamma$ په نقطه کې خپلی علامې ته د منفي څخه مثبت ته تغیر وروکوي. پدې معنی چې د $f(a), f'(a)$ د عددو په لار کې د $x=\gamma$ د نقطې و کیني خواته د علامې یو تغیر وجود لري ، خو و بنی خواته یې د علامې هیڅ تغیر وجود نلري. پدې معنی چې د علامو د تغیر شمېر د یوه په اندازه لږ سو. د $f'(x) < 0$ په عین شکل استدلال کولای سو.

د پورتنیو خاصیتو څخه په اسانۍ سره لاندني قضیه چې و شتورم ته منسوبه ده استنباط کیدای سی.

قضیه (شتورم Sturm) -

که $a < b; a, b \in \mathbb{R}$ وی او نوموړي عددونه د $f(x)$ د پولینوم جذرونه نه وی ، نو د $f(x)$ د پولینوم حقیقي جذرونه د $[a, b]$ په انټروال کې په $t(a)-t(b)$ سره مساوی کیږي چې په p سره یې بنیو. پدې معنی چې $p=t(a)-t(b)$ سره.

په رشتیا هم که د $f(x)$ پولینوم د $[a, b]$ په انټروال کې جذر ونلري ، نو $t(a)-t(b)=0$ دی .

که د $f(x)$ د پولینوم د جذرو شمېر د $[a, b]$ په انټروال کې p وی ، نو د څلرم خاصیت له مخې د هر جذر څخه د x د قینت د تېریدو په وخت کې $t(a)$ د یوه په اندازه لږیږي. په نتیجه کې بیا هم $p=t(a)-t(b)$ دی.

د ثابتې سوی قضیې پر اساس د پولینوم د حقیقي جذرو شمېر ټاکلای سو او هغو څخه هر یو په انټروال کې جلا کولای سو. په لاندني بیلگه کې نوموړی واقعیت مطالعه کوو.

بیلگه ۳- د $f(x) = x^4 - 2x^3 - 2x - 1$ د پولینوم حقیقي جذرونه تفکیک کوو.

حل - د VII § د لمړۍ قضیې پر اساس د $f(x)$ د پولینوم حقیقي جذرونه د $]-N_0, N_0[$ په انټروال کې پراته وی. پداسی حال کې چې $N_0 = 1 + \frac{A}{|a_n|}$ دی. زموږ په مشخصه بیلگه کې $N_0 = 1 + \frac{2}{1} = 3$ او

زموږ انټروال $]-3, 3[$ دی.

لاندني جدول جوړوو:

| x | f(x) | f'(x) | f ₁ (x) | f ₂ (x) | f ₃ (x) = 1 | t(x) |
|----|------|-------|--------------------|--------------------|------------------------|------|
| -3 | + | - | + | + | - | 3 |
| -2 | + | - | + | + | - | 3 |
| -1 | + | - | + | 0 | - | 3 |
| 0 | - | - | + | - | - | 2 |
| 1 | - | - | + | - | - | 2 |
| 2 | - | + | + | - | - | 2 |
| 3 | + | + | + | - | - | 1 |

جدول 17

د $f(x)$ د پولینوم دپاره مو په لمړي بیلگه کی د شتورم د پولینومو لار پیدا کی او په جدول کی مو یوازی دهغه د قیمتو علامی خای پر خای کری.

په جدول کی لیدل کیږی چی د $f(x)$ پولینوم د $[-1, 0]$ او $[2, 3]$ په انتروالو کی جذر لری ، پدی معنی چی د $f(x)$ پولینوم دوه حقیقی جذرونه لری.

نوموری طریقه د شتورم د پولینومو د حقیقی جذرو د تفکیک د طریقی په نامه یادیری .

د یادولو وړ ده په هغه صورت کی چی پولینوم مضاعف جذرونه ولری ، نویه لمړی قدم کی پولینوم په ضربی عاملو تجزیه کوو (د پنجم فصل ، § XIV وگورئ) .

د پولینومو حقیقی جذرو په هکله نور جزئیات لوستونکی په [7] کتاب کی هم موندلای سی.

اتم فصل

د نسبتي عددو پر فيلډ باندې پولينومونه - الجبري عددونه

1.8. د تامو عددو د ضريبو سره د پولينومونام او نسبتي جذرونه

په تېر فصل کې مو وډ دريمې او څلرمې درجي معادلو د حل عمومي طريقې او همدا ډول د حقيقي ضريبو سره د پولينومو د حقيقي جذرو شمېر او د هغوی تفکيک مو وڅېړل. د څېړل سوو طريقو د اوږدوالي او مغلق والی په خاطر په ډېرو حالتو کې د هغوی عملي ارزښت لږيزی.

دلته به پولينومونه د عددو پر کوچنيزين فيلډ (نسبتي عددو فيلډ) باندې وڅېړو او د هغوی د تامو او نسبتي جذرو د پيدا کولو دپاره ځني ابتدايي طريقې تشریح کړو.

فرضوو چې د $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ پولينوم د نسبتي ضريبو سره راکړه سوی دی. د $a_n, a_{n-1}, \dots, a_1, a_0$ ضريبونه ټوله وگډ مخرج ته رالرو او هغه تر قوس څخه دباندې ايردو. پدی معنی چې:

$$f(x) = \frac{1}{\alpha} (b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0) = \frac{1}{\alpha} g(x)$$

پداسی حال کې چې د $g(x)$ د پولينوم ضريبونه ټول تام عددونه دی. څرگنده ده چې د $f(x)$ د پولينوم ټول جذرونه په عين وخت کې د $g(x)$ د پولينوم جذرونه هم دی او بر عکس.

پدی معنی چې د نسبتي عددو \mathbb{Q} پر فيلډ باندې د پولينوم د جذر د شمېرلو په وخت کې ويلای سو چې د پولينوم ضريبونه تام عددونه دی. دلته د تامو ضريبو سره دپولينوم، د نسبتي عدد $\frac{p}{q}$ د جذر والی بعضی لازمی شرطونه مطالعه کوو. فرضوو چې $(p, q) = 1$ ، يعنی د p او q عددونه متبائن دی.

قضيه ۱- که د $\frac{p}{q}$ نه لنډ پېدونکی کسر د (1) ... $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ د پولينوم

چې ضريبونه يې تام عددونه دی، جذر وی، نو د p عدد د ثابت جزء a_0 وپشونکی او د q عدد د $f(x)$ د پولينوم د لوی ترين مضرب يعنی a_n وپشونکی دی.

ثبوت - فرضوو چې د $\frac{p}{q}$ عدد د $f(x)$ د پولينوم جذر او $(p, q) = 1$ دی. ځکه نو $f(\frac{p}{q}) = 0$ کيږی،

پدی معنی چې: $a_n (\frac{p}{q})^n + a_{n-1} (\frac{p}{q})^{n-1} + \dots + a_1 (\frac{p}{q}) + a_0 = 0$ دی.

$$a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0 \quad \dots (2)$$

د (2) اړيکه داسی هم ليکلای سو:

$$p(a_n p^{n-1} + a_{n-1} p^{n-2} q + \dots + a_1 q^{n-1}) = -a_0 q^n$$

پدی معنی چي $a_0 q^n : p$ دی . څرنگه چي $(p, q^n) = 1$ دی ، نو $a_0 : p$ دی .

اوس نو که د (2) اړیکه $a_n p^{n-1} = q(-a_{n-1} p^{n-1} - \dots - a_1 p q^{n-2} - a_0 q^{n-1})$ په بڼه ولیکو ، نو د ورته استدلال په نتیجه کی $a_n : q$ لاسته راځي .

نتیجه - که د نسبتی عددو د ضریبو سره د $f(x)$ د پولینوم لوی ترین حد مساوی په یوه سره وی ، یعنی $a_n = 1$ وی ، نو د نوموړی پولینوم ټول نسبتی جذرونه ، تام عددونه دی اود پولینوم د ثابت حد د وپشونکو څخه په استفادی سره یې لاسته راوړلای سو .

د ثابتی سوی قضیې پذیرعه کولای سو چي د پولینوم نسبتی جذرونه (که یې ولری !) پیدا کړو او یا ددغه ډول جذرنشته والی په ثبوت ورسوو .

$$\text{بیلگه - د } 2y^3 + 3y^2 + 6y - 4 = 0 \text{ د معادلي نسبتی جذرونه پیدا کووړ .}$$

حل - لمړی د ثابت حد -4 اود لوی ترین حد ضریب 2 ټول وپشونکی لیکو . هغوی په ترتیب سره

عبارت دی له $\pm 1, \pm 2, \pm 4$ او $\pm 1, \pm 2$ څخه . اوس نو د $\frac{p}{q}$ ټول ممکنه کسرونه داسی جوړوو چي

$q \in \{\pm 1, \pm 2\}$ او $p \in \{\pm 1, \pm 2, \pm 4\}$ دی . په نتیجه کی د $\pm 1, \pm 2, \pm 4, \pm \frac{1}{2}$ عددونه لاسته راځي .

دثابتي سوی قضیې پر اساس یوازی او یوازی پورتنی عددونه دراکړه سوی معادلي نسبتی جذرونه کیدای سی . ځکه نو د هغو څخه هر عدد باید و آزمویو . ددی عملیې د سرته رسولو دپاره یا دهورنر د شیمای څخه کار اخلو او یا یو یو عدد په معادله وضع کوو . دا چي کومه طریقہ مناسبه ده په مشخصه معادله او مشخصو عددو پوری اړه لری . په راکړه سوی بیلگه کی د $\pm 1, \pm 2$ د عددو وضع کول بیله کومی ستونزی ممکن دی . ځکه نو :

$$f(1) = 2 + 3 + 6 - 4 = 7 \neq 0$$

$$f(-1) = -2 + 3 - 6 - 4 = -9 \neq 0$$

$$f(2) = 16 + 12 + 12 - 4 = 26 \neq 0$$

$$f(-2) = -16 + 12 - 12 - 4 = -20 \neq 0$$

د پاته عددو د آزمویلو دپاره د هورنو د شیمای څخه کار اخلو :

| | | | | |
|---------------|---|---|---|----|
| | 2 | 3 | 3 | -4 |
| $\frac{1}{2}$ | 2 | 4 | 8 | 0 |

پدی معنی چي $(y - \frac{1}{2})(2y^2 + 4y + 8) = 2y^3 + 3y^2 + 6y - 4$ کیری . پدی ډول مو یو نسبتی

جذر $y_1 = \frac{1}{2}$ مو پیدا کری.

د راکره سوی معادلی د پاته جزو د شمېرنی دپاره باید د $2y^2 + 4y + 8 = 0$ او یا د $y^2 + 2y + 4 = 0$ مربعی معادلو جذرونه پیدا کړو. هغه عبارت دی له $y_{2,3} = -1 \pm \sqrt{3}i$ څخه.

په نتیجه کی ویلای سو چي راکره سوی معادله یوازې یو نسبتی جذر چي $\frac{1}{2}$ دی ، لری.

د یادولو وړ ده چي د عددو د تعویض په طریقه کی د جذر مضاعف والی نسو تثبیتولای. خو د هورنر د شیما څخه د کار اخیستلو په نتیجه کی د جذر مضاعف والی هم تثبیتولای سی.

د تامو ضریبو سره د $f(x)$ د پولینوم چي د لوی ترین حد ضریب یی د یوه څخه خلاف وی ، د نسبتی جزو محاسبه دهغه پولینوم د تام جذر و محاسبی ته راجع کیری چي د لوی ترین حد ضریب یی د یوه سره مساوی وی.

په رشتیا هم ، که $f(x)$ چي د (1) اړیکی پذیرعه راکره سوی وی ، نو بیا په هغه کی لاندی تبدیل سرته رسوو:

$$f(x) = \frac{a_n^{n-1}}{a_n^{n-1}} f(x) = \frac{1}{a_n^{n-1}} (a_n^n x^n + a_{n-1} a_n^{n-1} x^{n-1} + \dots + a_1 a_n^{n-1} x + a_0 a_n^{n-1})$$

اوس نو د $a_n x = y$ پر اساس متحول تعویضوو:

$$f(y) = \frac{1}{a_n^{n-1}} (y^n + a_{n-1} y^{n-1} + \dots + a_1 a_n^{n-2} y + a_0 a_n^{n-1})$$

څرگنده ده چي د $f(y)$ د پولینوم جذرونه د لاندنی $h(y)$ د جزو سره منطبق دی.

$$h(y) = y^n + a_{n-1} y^{n-1} + \dots + a_1 a_n^{n-2} y + a_0 a_n^{n-1}$$

د $h(y)$ د پولینوم نسبتی جذرونه د اولی قضیې د نتجی پر اساس تام عددونه دی.

همدا ډول باید یادونه وکو چي د پورتنی تعویض په نتیجه کی ثابت حد ډیر غځیری. پدی معنی چي د a_0 څخه په $a_0 a_n^{n-1}$ اوږی. په نتیجه کی یی د ثابت حد د وپشونکی شمېر زیاتیری. ځکه نو د دغه ډول تعویض گټورتوب په مشخصه بیلگه پوری اړه لری. د مثال په ډول د

$$10x^4 - 13x^3 + 15x^2 - 18x - 6 = 0$$

د جزو د موندلو دپاره ددغه ډول تعویض طریقه گټوره نده ، ځکه چي ثابت حد یی د 6 څخه په 6000 اوږی او په مشکله سره د هغه ټول وپشونکی پیدا کولای سو.

نور لازمی شرطونه ددی دپاره چي د $\frac{p}{q}$ عدد د تاموضربو سره د $f(x)$ د پولینوم جذر کیدای سی ، هم وجود لری. دغه شرطونه د جذر په صفت د عددو ازمویل لرووی.

قضیه ۲ - که د $\frac{p}{q}$ نه لنډ پیدونکی کسر د (1) پولینوم جذر وی ، نو دهر عدد k دپاره ، پداسی ډول چي $p - qk \neq 0$ وی ، د $f(k)$ عدد پر $p - qk$ د ویش وړ دی.

ثبوت - د $f(x)$ پولینوم پر $x - k$ باندی ویشو. څرنګه چي څرګنده ده لاسته راغلی باقیمانده $r = f(k)$ او ټوله ضربونه تام عددونه دی.

$$f(x) = (x - k)(b_{n-1}x^{n-1} + \dots + b_1x + b_0) + f(k)$$

څرنګه چي $f(\frac{p}{q}) = 0$ دی ، نو لاندنی مساوات لاسته راځي:

$$(\frac{p}{q} - k)(b_{n-1}\frac{p^{n-1}}{q^{n-1}} + \dots + b_1\frac{p}{q} + b_0) - f(k) = 0$$

$$-f(k) = \frac{p - qk}{q} (b_{n-1}\frac{p^{n-1}}{q^{n-1}} + \dots + b_1\frac{p}{q} + b_0)$$

$$-q^n f(k) = (p - qk)(b_{n-1}p^{n-1} + \dots + b_1pq^{n-2} + b_0q^{n-1})$$

د قضیې د شرط له مخی $p - qk \neq 0$ دی . دوروستی مساوات دواړی خواوی تام عددونه دی ، ځکه نو د $-q^n f(k)$ عدد پر $(p - qk)$ د ویش وړ دی. علاوه پردی د p او q عددونه په خپل منځ کی متبائن دی ، ځکه نو $(q, p - qk) = 1$ او بالاخره $(q^n, p - qk) = 1$ دی . په نتیجه کی باید $f(k)$ د $(p - qk)$ پر عدد د ویش وړ وی. پدی ترتیب قضیه په ثبوت ورسیده.

څرنګه چي k اختیاری تام عدد دی ، نو دوهمه قضیه پدی هکله چي د $\frac{p}{q}$ عدد د $f(x)$ د پولینوم جذر

دی ، ډېرګوني لازمی شرطونه ارائه کوی ، خو په عمل کی $k = \pm 1$ په کار اچوی چي په لاندی ډول فورمول بندی کیری.

نتیجه - که د $\frac{p}{q}$ نه لنډ پیدونکی کسر د تامو ضربو سره د $f(x)$ د پولینوم جذر وی، نو $\frac{f(-1)}{p + q}$ او

$$\frac{f(1)}{p - q}$$

تام عددونه دی.

بیلګه - د $6x^4 + 19x^3 - 7x^2 - 26x + 12 = 0$ معادله حلوو.

حل - د لوی ترین حد د ضریب او د ثابت حد ټوله وپشونکي پیدا او لیکو:

$$\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm \frac{1}{2}, \pm \frac{3}{2}, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{4}{3}, \pm \frac{1}{6} \dots (3)$$

په اسانۍ سره يې ازمويلای سو چې راکره سوی معادله $f(1)=4$ او $f(-1)=18$ کيږی. اوس نو باید وازمويل سی چې د (3) په لار کی غیر له ± 1 د کومو عددو دپاره د $\frac{4}{p-q}$ تام عدد دی. هغوی

$$\text{عبارت دی له : } (4) \dots 2, \pm 3, \frac{1}{2}, \frac{3}{2}, \pm \frac{1}{3}, \frac{2}{3}, \frac{4}{3}$$

څرنګه چې لیدل کيږی دلته یوازې ۹ عددونه زمور د شرط سره مطابقت کوی. ددوهم شرط څخه هم استفاده کوو، پدی معنی چې د $\frac{18}{p-q}$ هم باید تام عدد وی. د (4) لار د عددو څخه یوازې د

$2, -3, \frac{1}{2}, -\frac{1}{3}$ عددونه د ذکر سوی شرط سره مطابقت لری. اوس نو په اسانۍ سره هغه عددونه چې زمور پر شرطو برابر دی ازمويلای سو:

| | | | | | | |
|---------------|---|----|-----|-----|-----|---------------------|
| | 6 | 19 | -7 | -26 | 12 | |
| 2 | 6 | 31 | 55 | 84 | 180 | $\neq 0$ |
| -3 | 6 | 1 | -10 | 4 | 0 | $y_1 = -3$ |
| $\frac{1}{2}$ | 6 | 4 | -8 | 0 | | $y_2 = \frac{1}{2}$ |

جدول ۱۹

پدی معنی چې راکره سوی معادله د $(y+3)(y-\frac{1}{2})(6y^2+4y-8)=0$ بڼه ځانته غوره کوی. پدی ځایه $6y^2+4y-8=0$ او یا $3y^2+2y-4=0$ دی. د وروستی معادلي جزرونه عبارت وی له:

$$y_{3,4} = \frac{-1 \pm \sqrt{13}}{3}$$

پلاخره ویلای سو چې راکره سوی معادله څلور حقیقی جزرونه لری چې دهغو څخه دوه جزره y_1 او y_2 یې نسبتی عددونه دی.

II§. دپولینومود نه تجزیه کېدو معیار (د آیزنشتاین معیار)

پر راکره سوی فیله باندی د پولینومو د نه تجزیه کېدو مفهوم مو د پنځم فصل په X§ د لمړی ځل دپاره طرح کی. په XI, X§§ کی مو د نه تجزیه کېدونکو پولینومو عمومی خاصیتونه مطالعه کړه، همدا ډول د مختلطو عددو پر فیله باندی (اووم فصل، II§)، د حقیقی عددو پر فیله باندی (اووم فصل، IV§) مو نه تجزیه کېدونکي پولینومونه و څېړل او ومو لیدل چې د مختلطو عددو پر فیله \mathbb{C} باندی

یوازې هغه پولینومونه چې درجه یې د یوه سره مساوی، نه تجزیه کېدونکې دی خو د حقیقی عددو پر فیلډ \mathbb{R} باندې هغه پولینومونه چې درجه یې د یوه یا دوو سره مساوی وی، نه تجزیه کېدونکې دی. اوس به وښیو چې د نسبتي عددو پر فیلډ \mathbb{Q} باندې په اختیاري درجه باندې پولینوم موندلای سو چې پر نوموړی فیلډ باندې نه تجزیه کېدونکې دی.

دمخه تردی چې وروستی ادعا ثابتہ کرو، د نسبتي عددو پر فیلډ باندې د پولینومو ځني خاصیتونه مطالعه کوو.

په §I کی مو وښودل چې د نسبتي عددو پر فیلډ \mathbb{Q} باندې هر پولینوم د $f(x) = \frac{1}{\alpha}g(x)$ په شکل

ارائه کولای سو. پداسی حال کې چې د $g(x)$ د پولینوم ضریبونه تام عددونه دی او $\alpha \in \mathbb{Z}$ دی. ددی استدلال په نتیجه کی د نسبتي ضریبو سره د $f(x)$ د پولینوم د جذرو مسأله د تامو عددو د ضریبو سره د $g(x)$ د پولینوم د جذرو و مسأله ته راجع کیږی. همدا ډول د نسبتي عددو پر فیلډ \mathbb{Q} باندې د پولینومو د نه تجزیه کیدو په هکله گامونه اخلو.

تعریف - د تامو ضریبو سره د $g(x)$ پولینوم د ابتدائي Primitive به نامه یادوو که د هغه ضریبونه غیر له 1 او -1 څخه مشترک وپشونکې ونلری.

بیلگه - د $g(x) = 5x^4 - 3x^3 + 2x^2 + 4x - 1$ پولینوم ابتدائي دی؛ خو د $f(x) = 4x^3 + 6x^2 - 2$ پولینوم ابتدائي ندی، ځکه چې ضریبونه یې غیر له ± 1 څخه یو بل گډ وپشونکې هم لری چې هغه 2 دی.

لیما (گاوس) - د دوو ابتدائي پولینومو د ضرب حاصل بیا هم ابتدائي پولینوم دی.

ثبوت - فرضوو چې لاندني دوه ابتدائي پولینومونه راځړه سوی دی:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

فرضوو چې د $f(x)g(x) = c_{m+n}x^{m+n} + \dots + c_1x + c_0$ پولینوم ابتدائي ندی. نو د p اولیه عدد داسی

وجود لری چې د ټولو ضریبو c_0, c_1, \dots, c_{m+n} گډ وپشونکې دی. څرنگه چې د $f(x)$ پولینوم ابتدائي دی، نو د هغه ټوله ضریبونه د p پر عدد د وپش وړ ندی. فرضوو چې k د a_i د ضریبو څخه کوچنی ترین اندکس دی چې a_k د p پر عدد د وپش وړ ندی. همدا ډول فرضوو چې l کوچنی ترین اندکس دی چې b_l د p پر عدد د وپش وړ ندی.

اوس نو د $f(x)g(x)$ په پولینوم کی د x^{k+l} ضریب یعنی c_{k+l} مطالعه کوو:

$$c_{k+l} = \sum_{i+j=k+l} a_i b_j = a_k b_l + a_{k-1} b_{l+1} + \dots$$

نظر و مخکنی استدلال ته $a_k b_l \not\equiv 0 \pmod{p}$ دی. د پورتنی افادی نور جزونه پر p د وپش وړدی. ځکه چې k او l کوچنی ترین اندکسونه وه چې a_k او b_l د p پر اولیه عدد د وپش وړ نه وه، ځکه نو $a_{k-1} b_{l+1}, \dots$

اوداسی نور د p پر عدد دویښ ور دی. په مجموع کی د C_{k+1} عدد p پر عدد دویښ ور کیدای نسی. خو دغه حالت زموږ د فرضیې خلاف دی.

قضیه ۱ - ددی دپاره چي د $f(x)$ پولینوم د نسبتی عددو پر فیلډ \mathbb{Q} باندی د تامو عددو د ضریبو سره د تجزیې ور وی ، لازمه او کافی ده چي د تامو عددو پر رینگ \mathbb{Z} د تجزیې ور وی. پدی معنی چي د $f_1(x)$ او $f_2(x)$ د تامو ضریبو سره داسی وجود لری چي $f(x) = f_1(x) \cdot f_2(x)$ وی.

ثبوت - فرضوو چي د تامو ضریبو سره د $f(x)$ پولینوم د نسبتی عددو و پر فیلډ \mathbb{Q} باندی د تجزیې ور دی ، یعنی $f(x) = g_1(x) \cdot g_2(x)$ ، پداسی حال کی چي د $g_1(x)$ او $g_2(x)$ د پولینومو ضریبونه نسبتی عددونه دی او درجه یی د صفر څخه خلاف ده. باید ثابتنه کړو چي د $f_1(x)$ او $f_2(x)$ پولینومونه داسی وجود لری چي درجی یی د صفر څخه خلاف ، ضریبونه یی تام عددونه دی او د هغوی د ضرب حاصل د $f(x)$ پولینوم کپری.

د $g_1(x)$ د پولینوم د ضریبو مشترک مخرج پیداوو او تر قوس دبانندی یی نیسو ، په نتیجه کی د $g_1(x)$ پولینوم داسی لیکلای سو :

$$g_1(x) = \frac{\alpha}{\beta} s_1(x)$$

پداسی ډول چي د $s_1(x)$ پولینوم د تامو ضریبو سره دی ، β د $g_1(x)$ د پولینوم د ضریبو گډ مخرج دی او α د هغوی لوی ترین گډ وېشونکی دی. څرگنده ده چي د $s_1(x)$ پولینوم ابتدائی پولینوم دی ، همدا ډول فرضولای سو چي $(\alpha, \beta) = 1$ دی (که داسی نه وی ، نو کولای سو کسر لنډ کړو). همدا ډول د $g_2(x)$ دپاره به

$$g_2(x) = \frac{\gamma}{\delta} s_2(x)$$

ولرو ، پداسی ډول چي $s_2(x)$ ابتدائی پولینوم او $(\gamma, \delta) = 1$ دی. پدی ترتیب :

$$f(x) = \frac{\alpha \cdot \gamma}{\beta \cdot \delta} s_1(x) \cdot s_2(x)$$

ثابتوو چي د $\frac{\alpha \cdot \gamma}{\beta \cdot \delta}$ عدد ، تام عدد دی.

فرضوو چي $\frac{\alpha \cdot \gamma}{\beta \cdot \delta} = \frac{p}{q}$ او $(p, q) = 1$ دی. د تبری لیمای پر اساس د $s(x) = s_1(x) \cdot s_2(x)$ ابتدائی

پولینوم دی. که d_k د $s(x)$ د پولینوم ضریب وی ، نو $\frac{p}{q} \cdot d_k$ باید تام عدد وی ، ځکه چي

$f(x) = \frac{p}{q} s(x)$ د تامو عددو سره پولینوم دی. څرنگه چي $(p, q) = 1$ دی ، نو $d_k : q$ او په نتیجه کی د

$s(x)$ د پولینوم ټوله ضریبونه پر q د وېش وړ دی ، خو د حالت ددی واقعیت چي $s(x)$ ابتدائي پولینوم دی ، خلاف دی. ځکه نو $\frac{\alpha.\gamma}{\beta.\delta} = m \in \mathbb{Z}$ دی.

بلاخره کولای سو چي $f_1(x) = ms_1(x)$ او $f_2(x) = s_2(x)$ سره کښېږدو ، نو $f(x) = f_1(x).f_2(x)$ په لاسته راسي.

د قضیې کافی شرط څرگند دی ، ځکه چي که د $f(x)$ پولینوم د تامو عددو په رینګ \mathbb{Z} کی د تجزیې وړ وی ، نو د نسبتی عددو په فیلډ \mathbb{Q} کی هم د تجزیې وړ دی.

قضیه ۲ (د آیزنشتاین معیار)۔

که د تامو ضریبو سره د $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ د پولینوم a_{n-1}, \dots, a_1, a_0 ضریبونه د p پر اولیه عدد داسی د وېش وړ وی چي $a_0 \not\equiv p^2$ او $a_n \not\equiv p$ وی ، نو د $f(x)$ پولینوم د نسبتی عددو په فیلډ کی د تجزیې وړ ندی.

ثبوت۔ فرضوو چي د $f(x)$ د پولینوم په هکله د قضیې شرطونه صدق کوی ، خو پولینوم د دوو پولینومو چي ضریبونه یې نسبتی عددونه او درجي یې د صفر څخه خلاف دی ، د ضرب حاصل دی. پدی معنی چي د تجزیې وړ دی. یعنی:

$$f(x) = (b_r x^r + b_{r-1} x^{r-1} + \dots + b_1 x + b_0)(c_s x^s + c_{s-1} x^{s-1} + \dots + c_1 x + c_0)$$

پداسی ډول چي $r+s=n$ او $r \geq s$ دی.

د لمرې قضیې پراساس د $b_r, b_{r-1}, \dots, b_1, b_0, c_s, c_{s-1}, \dots, c_1, c_0$ ضریبونه ټوله تام عددونه دی. د هغوی د ضرب په نتیجه کی لاندنی د مساواتو سیستم لاسته راځي:

$$\begin{aligned} a_0 &= b_0 c_0 \\ a_1 &= b_1 c_0 + c_1 b_0 \\ a_2 &= b_2 c_0 + b_1 c_1 + b_0 c_2 \\ &\vdots \\ a_r &= b_r c_0 + b_{r-1} c_1 + \dots + b_{r-s} c_s \\ &\vdots \\ a_n &= b_r c_s \end{aligned}$$

د قضیې د شرط له مخی $a_0 = b_0 c_0 : p$ او $a_0 \not\equiv p^2$ دی ، پدی معنی چي د b_0 او c_0 د عددو څخه یوازى یو یې د p پر عدد د وېش وړ دی. که فرض کړو چي $b_0 : p$ او $c_0 \not\equiv p$ دی ، نو دپورتنی سیستم دوهم مساوات څخه لاسته راځی چي $b_1 c_0 : p$ او $b_1 : p$ دی. په همدا ډول ددریم مساوات څخه لاسته راځي چي $b_2 : p$ کیږی ، ... او داسی نور. په پای کی د b_1, b_{r-1}, \dots, b_r ټول ضریبونه د p پر عدد د وېش وړ دی. حال داچي دا ناممکنه ده ، ځکه چي $a_n \not\equiv p$ دی. پدی ډول قضیه ثابتې سوه.

قضیه ۳ - د نسبتی عددو پر فیلاډ باندی د پولینوموپه رینگ $\mathbb{Q}[x]$ کی په اختیاری درجه سره پولینوم وجود لری چي د \mathbb{Q} پر فیلاډ باندی نه تجزیه کېدونکئ دی (د تجزیې وړ ندی).

د قضیې دثبوت دپاره کافی ده چي دغه ډول پولینوم پیدا کړو. که p اولیه عدد وی ، نو د هر طبیعی عدد $n \geq 1$ د پاره د دوهمی قضیې پر اساس $f(x) = x^n + p$ هغه پولینوم دی چي د \mathbb{Q} په فیلاډ نه تجزیه کېدونکئ دی یا په بله اصطلاح د تجزیې وړ ندی.

لانډنی ادعاوی په اسانی سره ثابتولای سو:

۱- که د $f(x)$ پولینوم د \mathbb{Q} پر فیلاډ باندی ($\text{dcgf} > 1$) لږترلږه یو نسبتی جذر ولری ، نو د $f(x)$ پولینوم د \mathbb{Q} پر فیلاډ دتجزیې وړ دی.

۲- که د $f(x)$ پولینوم چي ضریبونه یی نسبتی عددونه دی او درجه یی مساوی په 3 سره وی ، نسبتی جذر ونلری ، نو نوموړی پولینوم د \mathbb{Q} پر فیلاډ باندی دتجزیې وړ ندی.

§III. الجبری او ترانسندنت عددونه

دنسبتی عددو \mathbb{Q} فیلاډ کوچنی ترین عددی فیلاډ دی (لمری برخه، دوهم فصل ، §IV). لوی ترین عددی فیلاډ چي تر نن ورځې پوری په الجبر کی ورسره بوخت و د مختلطو عددو فیلاډ دی. په معاصره ریاضی کی ثابت سوئ ده چي د مختلطو عددو د فیلاډ اختیاری توسعه P (یعنی د مافوق مختلط عددو نه ورننوتل) فیلاډ ندی. پدی معنی چي په حقیقت کی د مختلطو عددو فیلاډ لوی ترین عددی فیلاډ دی. پدی پاراگراف کی د مختلطو عددو پر تصنیف باندی د نسبتی عددو پر فیلاډ باندی د پولینومو د رینگ $\mathbb{Q}[x]$ په اړوند لنډ مکث کوو.

تعریف ۱ - د α مختلط عدد د الجبری عدد algebraic number په نامه یادیری ، که α د $\mathbb{Q}[x]$ په رینگ کی د کوم پولینوم جذر وی.

څرگنده ده چي هر نسبتی عدد $\alpha \in \mathbb{Q}$ الجبری عدد دی. ځکه چي هغوی د $f(x) = x - \alpha$ د پولینوم جذر دی. ټول عددونه چي د $\sqrt[n]{\alpha}$ ، $\alpha \in \mathbb{Q}$ ، بڼه ولری هم الجبری عددونه دی ، ځکه چي هغوی د $g(x) = x^n - \alpha$ د پولینوم جذرونه دی. همدا ډول د $\alpha = 1 + i$ مختلط عدد هم الجبری عدد دی . ځکه چي نوموړی عدد د $h(x) = x^2 - 2x + 2$ پولینوم چي نسبتی ضریبونه لری ، جذر دی. کله چي دغه ټولو بېلگو ته گورو ، نوڅوک به وایی چي ټوله مختلط عددونه الجبری دی ، خو اصلاً داسی نده.

تعریف ۲ - د α مختلط عدد د ترانسندنت transcendental number (متعالی ، مافوق، غیر الجبری) په نامه یادیری ، که هغه د نسبتی ضریبو سره د هیڅ پولینوم جذر نه وی.

په لمړیو وختو کی د ترانسندنت عددو د موجودیت څېړنه ډیره مشکله وه په نولسمه پیری کی اولین ترانسندنت عدد پیدا سو ، هغه عبارت دی له e (د طبیعی لوگاریتم اساس) څخه. وروسته له هغه د π د عدد ترانسندنتوالی ثابت سو. وروسته له هغه د ډېرو عددو ترانسندنتوالی ثابت سو. لکه $2\sqrt{2}$. د $y = \lg x$ او $y = a^x$ تابع گانې د ترانسندنت تابع گانو په نامه یادی سوی. په زړه پوری داده چي دالجبری عددو سیټ لاینناهی ، خو د شمېر وړ Countable (یعنی د طبیعی عددو د سیټ سره معادل) دی، خو د

غير الجبري (ترانسندنت) عددو سيټ هم لايٽناهي دي ، مگر د شمېر وړ ندي پدي معني چي Uncountable دي. ويلای سو چي هغوی تر الجبري عددو ډير دي. پدي هکله به زما په بل کتاب(د سيټ د تيوري اساست) کی په تفصيل وړ غږو.

فرضوو چي α د $f(x)$ د پولينوم چي د لوی ترين حد ضريب يعنی a_n يي مساوی په يوه سره دی ، جذر

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \text{ دی.}$$

فرضوو چي د $f(x)$ پولينوم د \mathbb{Q} به فيلد کی د تجزيي وړ نه وی. که د $f(x)$ پولينوم د تجزيي وړ وی ، نو تر تجزيي وروسته د هغه ، هغه عامل چي α يي جذر وی تر مطالعي لاند نيسو. که $g(x)$ د $\mathbb{Q}[x]$ د رينگ بل پولينوم وی چي α يي جذر وی ، نو د $f(x)$ د نه تجزيه کيدو په خاطر د $g(x)$ پولينوم بايد د $f(x)$ پر پولينوم د وېش وړ وی. نموري دوه پولينومونه يو دبل سره متبائن نسي کيدای . ځکه چي هغوی دواړه د $x - \alpha$ گډ مضرب درلودونکی دی. که د $g(x)$ پولينوم هم د تجزيي وړ نه وی ، نو د $f(x)$ او $g(x)$ پولينومونه د λ د ثابت عدد په اندازو يو دبل سره تفاوت لری. پدي معني چي $\lambda \in \mathbb{Q}$ دپاره $g(x) = \lambda f(x)$ دی. ددی خايه نتيجه اخيستلای سو چي د $f(x)$ پولينوم د \mathbb{Q} پر فيلد باندی يوازنی نه تجزيه کيدونکی پولينوم دی چي د α عدد دهغه جذر دی او n ددغه ډول پولينومو د ټولو درجو په منځ کی کوچني ترينه درجه ده.

تعريف ۳ - د \mathbb{Q} پر فيلد باندی د $f(x)$ نه تجزيه کيدونکی پولينوم چي د لوی ترين حد ضريب يي مساوی په يوه او α يي جذر دی ، د α د عدد د کوچنی ترين پولينوم په نامه ياديری او د $f(x)$ د پولينوم درجه n د الجبري عدد α درجي په نامه ياديری.

څرگنده ده چي د α نسبتی عدد کوچنی ترين پولينوم $f(x) = x - \alpha$ دی. ساده ازمويل کيدای سی چي د $\sqrt{3}$ د عدد دپاره کوچنترين پولينوم $f(x) = x^2 - 3$ او د $2i$ دپاره د $g(x) = x^2 + 4$ پولينوم دی.

تعريف ۴ - الجبري عددونه چي د \mathbb{Q} پر فيلد باندی دعین نه تجزيه کيدونکی پولينوم جذر وی د مزدوج عددو Conjugte په نامه ياديری.

نوټ - پاملرنه وکی چي د الجبري عددو مزدوج والی د مختلطو عددو د مزدوج والي سره کومه اړيکه نلری ، امید دی چي دلته سو تفاهم رانسی.

د بيلگی په ډول د $\sqrt{3}$ د عدد مزدوج د $-\sqrt{3}$ عدد دی . الجبري عدد $\sqrt[3]{2}$ دوه مزدوج عددونه لری چي د $g(x) = x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$ د پولينوم جذرونه دی. د $\sqrt[3]{2}$ د عدد دپاره کوچنی ترين پولينوم $f(x) = x^3 - 2$ دی.

قضيه - د ټولو الجبري عددو سيټ په A سره بنیو ، عددی فيلد دی.

ثبوت - د قضیي د ثبوت دپاره بايد د ثابتو کړو چي دالجبري عددو د جمع ، تفريق ، ضرب او تقسيم حاصل بيا هم الجبري عدد دی.

فرضوو چي α او β دوه الجبري عددونه دی او د $f(x)$ او $g(x)$ پولينومونه د هغوی جواب ورکونکی کوچنی ترين پولينومونه د، پداسی ډول چي n او k په ترتيب سره د هغوی درجي دی.

د $\beta_k, \dots, \beta_2, \beta_1 = \beta$ د پولینوم جذرونه دی او $\alpha_n, \dots, \alpha_2, \alpha_1 = \alpha$ د $f(x)$ د پولینوم جذرونه دی. د

$$\varphi(x) = \prod_{i=1}^n \prod_{j=1}^k [x - (\alpha_i + \beta_j)]$$

پولینوم څېرو.

د $\varphi(x)$ د پولینوم جذرونه د $\alpha_i + \beta_j$ ټوله ممکنه د جمع حاصل دی. د هغوی په منځ کې $\alpha + \beta$ هم شامل دی. د نوموړی پولینوم ضریبونه نظر و $\alpha_n, \dots, \alpha_2, \alpha_1$ او $\beta_k, \dots, \beta_2, \beta_1$ ته متناظر دی. ځکه نو کولای سو چې هغوی د متناظر اساسی پولینوم له جنسه، پدی معنی چې د $f(x)$ او $g(x)$ د پولینومو د ضربیو له جنسه ارائه کولای سو. په لنډ ډول ویلای سو چې د $\varphi(x)$ ضریبونه نسبتی عددونه دی. په نتیجه کې $\alpha + \beta$ الجبری عدد دی. همدا ډول د

$$\varphi_1(x) = \prod_{i=1}^n \prod_{j=1}^k [x - (\alpha_i - \beta_j)]$$

$$\varphi_2(x) = \prod_{i=1}^n \prod_{j=1}^k [x - (\alpha_i \beta_j)]$$

پولینومو په مرسته د $\alpha - \beta$ او $\alpha \beta$ الجبری والی ثابتولای سو.

د تقسیم د حاصل د الجبری والی دپاره کافی ده چې ثابت کړو ، که د α عدد الجبری وی ، نو $\alpha^{-1} = \frac{1}{\alpha}$ هم الجبری عدد دی.

فرضوو چې د α عدد د $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Q}[x]$ د پولینوم جذری ، نو د

$$\alpha^{-1} = \frac{1}{\alpha} \text{ عدد به د } g(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + 1 \text{ د پولینوم چې ضریبونه یی نسبتی}$$

عددونه دی ، جذر وی.

پدی ډول قضیه پوره ثابته سوه.

څرگنده ده چې د ترانسندنت عددو سیټ فیلډ نه جوړوی.

پورتنیو څلورو تعریفو ته په لاندی ډول عمومیت ورکوو:

تعریف ۵- د α عدد نظر د P و فیلډ ته د الجبری عدد په نامه یادیری ، که α د $P[x]$ په رینګ کې د یوه پولینوم جذر وی. هر عدد چې نظر د P و فیلډ ته الجبری نه وی ، نظر د P و فیلډ ته د ترانسندنت عدد په نامه یادیری.

د پورتنی تعریف په نظر کې نیولو سره د α هر حقیقی عدد نظر د \mathbb{R} و فیلډ ته الجبری دی.

په هغه صورت کی چې په دریم او څلرم تعریف کی د \mathbb{Q} د فیلډ کلمه د P د فیلډ سره ایشه کړو ، نو د کوچنی ترین پولینوم او الجبری مزدوجو عددو عمومی تعریف به لاسته راسی.

IV§. د فیلډ ساده الجبری توسعه (پراختیا) او دهغه د جوړښت طریقه

فرضوو چې P د عددی فیلډو څخه یو فیلډ دی او د α عدد پدی فیلډ کی شامل ندی ، پدی معنی چې $\alpha \notin P$ دی.

تعریف - د P د فیلډ کوچنی ترینه توسعه چې د $P \notin \alpha$ عدد په ځان کی ولری د P د فیلډ د توسعی په نامه یادیری چې د P په فیلډ کی د α د عدد د اضافه کېدو په نتیجه کی لاسته راغلی دی.

د α پذیرعه پراخ سوی فیلډ په $P(\alpha)$ سره ښیو.

ددغه ډول پراختیا د موجودیت پوښتنه د لاندی واقعیت څخه استنباط کیږی:

د اختیاری فیلډو مشترکه برخه بیا هم فیلډ دی.

همدا ډول د $P(\alpha_1, \alpha_2, \dots, \alpha_k)$ توسعه چې د P په فیلډ کی د $\alpha_1, \alpha_2, \dots, \alpha_k$ د عددو د اضافه کېدو په نتیجه کی لاسته راغلی ده ، مطالعه کړو. هغه پراختیا چې دیوه عدد داضافه کیدو په نتیجه کی لاسته راځي ، د ساده توسعی (پراختیا) په نامه یادیری. که ور اضافه سوی عدد الجبری وی ، نو هغی توسعی ته ساده الجبری توسعه وایو. غیر له هغه څخه د P د فیلډ توسعه دساده ترانسندنت پراختیا په نامه یادوو.

په اسانی سره لیدل کیږی چې د $\{a + b\sqrt{2} / a, b \in \mathbb{Q}\}$ فیلډ د \mathbb{Q} د فیلډ ساده الجبری توسعه ده چې د $\sqrt{2}$ د عدد د اضافه کېدو په نتیجه کی لاسته راغلی دی. پدی معنی چې :

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} / a, b \in \mathbb{Q}\}$$

د P د فیلډ د ساده الجبری توسعی د جوړښت طریقه لاندنی قضیه طرح کوی.

قضیه - د $P(\alpha)$ د فیلډ عنصرونه چې د P د فیلډ څخه د P په فیلډ کی د نه تجزیه کېدونکی n درجه ای پولینوم

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

د جذر α د اضافه کیدو په نتیجه کی لاسته راغلی دی ، داسی شکل لری:

$$\lambda = c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1} \quad \dots(1)$$

پداسی ډول چې c_0, c_1, \dots, c_{n-1} د P د فیلډ اختیاری عددونه دی.

ثبوت - لمړی باید ثابتته کړو چې ټوله عددونه چې د (1) پذیرعه ارائه سوی دی ، فیلډ جوړوی. څرگنده ده چې ددغه ډول عددو د جمع او تفریق حاصل بیا هم د (1) ښه لری. هر عدد چې د (1) په شکل لیکل

سوی وی د P پر فیله بانندی د $s(x)$ د پولینوم په شکل چي درجه ای تر $n-1$ اضافه نه وی ارانه کولای سو. البته که x د α سره الیش کړو $\lambda = s(\alpha)$ سره.

فرضوو چي د $\lambda_1 = s_1(\alpha)$ او $\lambda_2 = s_2(\alpha)$ دوه عددونه راکړه سوی دی. د هغوی د ضرب حاصل $\lambda_1 \cdot \lambda_2 = s_1(\alpha) \cdot s_2(\alpha) = s(\alpha)$ دی. پداسی حال کي چي د $s(\alpha)$ د پولینوم درجه امکان لری چي تر $n-1$ اضافه وی. د $s(x)$ پولینوم د $f(x)$ پر پولینوم وپشو. د ویش په نتیجه کی:

$$s(x) = f(x) \cdot g(x) + r(x) \quad \dots(2)$$

لاسته راځي. پداسی حال کي چي $\text{degr}(x) < \text{deg}f(x)$ دی، پدی معنی چي $\text{degr}(x) \leq n-1$ دی. که په (2) مه اړیکه کی x د α سره تبدیل کړو، نو $s(\alpha) = f(\alpha) \cdot g(\alpha) + r(\alpha)$ لاسته راځي، ددی ځایه $\lambda_1 \cdot \lambda_2 = r(\alpha)$ دی. پدی معنی چي د (1) په بڼه ددوو عددو ضرب بیا هم د (1) په شکل یو عدد دی.

اوس نو باید ثابتنه کړو چي د (1) په بڼه ددوو عددو د ویش حاصل بیا هم د (1) په شکل یو عدد دی.

ددی موخي دپاره کافی ده چي ثابتنه کړو چي د $\lambda = s(\alpha) \neq 0$ دپاره د هغه معکوس عدد، یعنی $\frac{1}{\lambda}$

هم د (1) په بڼه ارانه کولای سو. څرنګه چي د $f(x)$ پولینوم د P پر فیله بانندی د تجزیي وړ ندی، نو د $s(x)$ پولینوم یا د $f(x)$ د پولینوم سره متبائن دی او یا پر $f(x)$ د ویش وړ دی. څرنګه چي

$\text{deg}s(x) < \text{deg}f(x)$ دی، نو $s(x) \nmid f(x)$ دی. ځکه نو باید $(f(x), s(x)) = 1$ وی. ددی ځایه (د پنځم

فصل، § VIII وګورئ) د $u(x)$ او $v(x)$ پولینومونه داسی وجود لری چي $f(x) \cdot u(x) + s(x) \cdot v(x) = 1$ کبړي. په وروستی اړیکه کی x د α سره الیشوو، پدی معنی چي $x = \alpha$ سره ايردو. څرنګه چي

$f(\alpha) = 0$ دی، نو $s(\alpha) \cdot v(\alpha) = 1$ حاصلیږی. پدی معنی چي $\lambda \cdot v(\alpha) = 1$ او $\frac{1}{\lambda} = v(\alpha)$ لاسته

راځي.

که $\text{deg}v(x) < n$ وی، نو قضیه ثابتنه سوه. په هغه صورت کی چي $\text{deg}v(x) \geq n$ وی، نو د $v(x)$ پولینوم د $f(x)$ پر پولینوم وپشو. پدی معنی چي:

$$v(x) = f(x) \cdot \varphi(x) + r(x)$$

ددی ځایه $v(\alpha) = r(\alpha)$ کبړی او $\text{dcgr}(x) < \text{dcgf}(x) = n$ دی. پدی معنی چي د $\frac{1}{\lambda}$ عدد د (1) بڼه

لری. ددی اسیتنه ادعا کولای سو چي د ټولو هغه عددو سیټ چي د (1) په شکل وی، فیله جوړوی. نوموړی فیله په P_1 سره ښکاره کوو. څرنګه چي $P_1 \subset P$ او $\alpha \in P_1$ دی، نو $P(\alpha) \subset P_1$ دی. همدا ډول هر فیله چي د α عدد په ځان کی ولری، حتمی ده چي د P فیله، ټوله عددونه چي د (1) په بڼه وی، پداسی ډول چي د P د عددو او α څخه د جمع او ضرب په نتیجه کی لاسته راغلی وی، په ځان کی ولری. پدی معنی چي $P_1 \subset P(\alpha)$ دی. په نتیجه کی $P_1 = P(\alpha)$ دی.

نتیجه - که د P پر فیله بانندی α ددوهمی درجي پولینوم $f(x) = x^2 + px + q$ جذر وی. پداسی حال کی چي $\alpha \notin P$ ، نو د P د فیله ساده الجبری توسعه $P(\alpha)$ د P پر فیله بانندی د α د عدد د اضافه کیدو په نتیجه کی او د ټولو عددو چي د $a + b\alpha$ ، $a, b \in P$ شکل ولری، لاسته راځي.

لکه مخکی چي مو ولیدل $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ ، پداسی حال کی چي $\sqrt{2}$ د \mathbb{Q} په
فیلد کی د $f(x) = x^2 - 2$ د نه تجزیه کیدونکی پولینوم جذر دی ، د \mathbb{Q} د فیلد پراخ سوی فیلد دی.

اندکس

N

61 non positional

P

polynoms

128 Irreducible
61 positional
196 Primitive

R

49 **Relatively Primes**
57 RSA

S

185 **Sturm**
29 Subring

T

200 transcendental number

U

200 Uncountible

ا

استازی 77
افلیدس 119, 44
الجبری
توسعه 202
الگوریتم 119
اویئر 81
قضیه 84
ایراتوستینس 54

آ

آبل 7
آیدیل 33

ب

باقیمانده 77

A

199 algebraic number

B

62 Binary
74 Blaise Pascal

C

33 Cancellation law
71 Congruency
200 Conjugte
200 Countible
100 **Cryptology**

D

103 Data encoding
61 digit
90 Diophantus

E

81 Euler function

F

22 Factor Group
34 **Factor Ring**
179 Ferrari

H

62 Hexadecimal
24 Homomorphism
116 Horner

I

99 **ISBN**

L

151 Lexicographic

M

71 Modulo
201

| | | |
|---|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| غ | غلبيل 54 | تولگي 77 کامل 77 باينوم 115 بليز پاسکال 74 |
| ف | فراری 179 فرما 81 قضيه 85 فيلد الجبري ترلی 170 | پ پراختيا 202 پرته 71 پولينوم 103 ابتدائي 196 جذرونه 135 متناظر 155 |
| ق | قاموسی 151 قافول 100 | د |
| ک | کانگروينسی 71 | د رينگو ورته والي 36 د شمېر وړ 200 دگروپو تجزيه 18 دوراني 14 دوه حديزه 115 ديکارت 183 |
| گ | گالوا 6 گروپ 6 | ډ |
| ل | لاگرانژ 18, 20 | ډيفي - هيلمن 101 |
| م | متباين 49 مشترک مضرب 52 مقايساتو 71 مولد جذرونه 90 | ر رقم 61 رينگ 28 |
| ن | نارمل وېشونکی 22 نيوتن 183 | س سب رينگ 28 سبگروپ 14 |
| و | وېش نيمگري 42 ورنوب 39 وېشونکی لوی ترين مشترک 44 ويتا 169 | ش شورم 185 شفرول 100 شمېرني سيستمونه 60 |
| | | ع عدد الجبري 199 ترانسندنت 200 مزدوج 200 عددونه اوليه 54 |

۵

هسته 26
هورنر 116
هومورفيزم 24

مآخذ

1. Barnet, I.A. Elements of number theory. Prindle & Schmidt incorporated 1969.
2. Beck, M. Geoghegan, R. , The Art of Proof , Springer Verlag , 2010
3. Birkhoff, G./Bartec, T.C. Modern applied algebra, New york, Mc GrowHill 1976
4. Foster, Godron (1966) "International Standard Book Numbering, WikiPedia.org
5. Gavalec, M. ,Chval,V. Algebra I , II , PF UPJŠ, Košice, 1974
6. Juschkewitsch, A.P.:Geschichte der Mathematik im Mittelalter, B.G.Teubner Verlag.1964 Leipzig
7. Kurosh, A.G. Higher Algebra , M. Nauka 1971
8. Kurosh, A.G. Lectures on General Algebra, M. Nauka 1962
9. Niazman,S.A. Algebra and theory of numbers I , Sahar Printing Press , Kabul,2015
10. Padeberg, F. Elementare Zahlentheorie, 2.Auflage, Spektrum Akademischer Verlag, Heidelberg, Berlin 2001
11. Sarif, Gul Janan, په نړيوال کلتور کې د افغانانو ونډه , Most Verlag Marburg 2006
12. Schubert, M.:Mathematik für Informatiker, 2.Auflage , Vieweg+Teubner Verlag 2012
13. Stewart, B.M.:Theory of numbers 2nd Edition, New york, Macmillon Comp.1968
14. Van der Waerden B.L. , Algebra , M. Nauka 1971
15. Witt, K.U. Algebraische Grundlagen der Informatik 3.Auflage, Vieweg Verlag 2007
16. Wußing, H. :6000 Jahre Mathematik , Springer-Verlag Berlin Heidelberg 2009
17. Zavalo,S.T., Kostarčuk, V.N. , Chacet B.I., Algebra and Number Theory , Part I , K. Hlghschool, 1977
18. Zavalo,S.T.-Levischtschenko,S.S,Pelaev,V.V.,Rokitski, I.A.,:Algebra and Number Theory Exercises I, Hlghschool, 1983.



سلطان احمد نيازمن د ۱۹۵۷ کال د جنوري پر ۱۷مه نيټه د کندهار د عمران په کوڅه کې زيږيدلی دی . په ۱۹۷۴ کال کې د کندهار د ميرويس نيکه د ليسي څخه فارغ او د کابل په پوهنتون کې د تحصيلي بورس څخه په استفاده سره خپلې لورې زده کړې د رياضي په څانگه کې د پخواني چکوسلواکيا د کوشنيخ د ښار د پاول يوزف ښافاريک په پوهنتون کې ، د RNDr په درجه ، سرته رسولي دي . د پوهنتون د فراغت څخه وروسته يې څه ناڅه پنځه کاله د کابل د پيدا گوډي انستيتوت د رياضي د دبپارتمنت د آمر په صفت وظيفه اجراء کړيده . په تيرو پنځه ويشتو کلو کې يې د کمپيوټري علومو او خصوصاً د کمپيوټر د جال په برخه کې کار کړيدی . د لسو کالو راهيسې د جرمني د اليمپيک او سپورټ د کنفدراسيون د کمپيوټري جال او د هغه د مصونيت د مسؤل په صفت دنده اجراء کوي .

RNDr. Sultan Ahmad Niazman

Certified Network Manager (CNM)



Abstract

The 2nd part of algebra and theory of numbers is designed as a text book for the students of the science faculty of Nangarhar University, which covers the requirements for the third to fifth semester.

This book includes eight chapters. The first two chapters deal with the details of algebraic structure, such as groups and rings, which we have shortly mentioned in the first part of this book.

The third and fourth chapter explain the integers, divisibility, prime numbers and factorization of integers in prime factors, as well as modular arithmetics in the fourth chapter. At the end of this chapter, there is an example on how to calculate an ISBN and a short introduction to the Diffie-Hellman Key Exchange as an application of modular arithmetics.

The last four chapters deal with polynomial equations. Chapter 5 explores the general theory of polynomials with one variable on an arbitrary field. Here we consider polynomials as of polynomial form and polynomial function. In this chapter, there is also an explanation on the similar properties of integers, i.e. divisibility, euclidean algorithm, reducible and irreducible polynomials. Chapter 6 explores polynomials with several variables and contains the fundamental theorem of symmetric polynomials.

The last two chapters explain the properties of polynomials on concrete rational, real and complex number fields. Include such a topic as the fundamental theorem of the theory of polynomials, factorization of polynomials and Eisenstein criterion of irreducibility. The last topic introduces the algebraic and transcendent numbers.

Publishing Textbooks

Honorable lecturers and dear students!

The lack of quality textbooks in the universities of Afghanistan is a serious issue, which is repeatedly challenging students and teachers alike. To tackle this issue, we have initiated the process of providing textbooks to the students of medicine. For this reason, we have published 258 different textbooks of Medicine, Veterinary, Psychology, Pharmacy, Engineering, Science, Economics, Journalism and Agriculture (96 medical textbooks funded by German Academic Exchange Service, 140 medical and non-medical textbooks funded by German Aid for Afghan Children, 6 textbooks funded by German-Afghan University Society, 2 textbooks funded by Consulate General of the Federal Republic of Germany, Mazar-e Sharif, 2 textbook funded by Afghanistan-Schulen, 1 textbook funded by SlovakAid, 1 textbook funded by SAFI Foundation and 8 textbooks funded by Konrad Adenauer Stiftung) from Nangarhar, Khost, Kandahar, Herat, Balkh, Al-Beroni, Kabul, Kabul Polytechnic and Kabul Medical universities. The book you are holding in your hands is a sample of a printed textbook. It should be mentioned that all these books have been distributed among all Afghan universities and many other institutions and organizations for free. All the published textbooks can be downloaded from www.ecampus-afghanistan.org.

The Afghan National Higher Education Strategy (2010-2014) states: "Funds will be made available to encourage the writing and publication of textbooks in Dari and Pashto. Especially in priority areas, to improve the quality of teaching and learning and give students access to state-of-the-art information. In the meantime, translation of English language textbooks and journals into Dari and Pashto is a major challenge for curriculum reform. Without this facility it would not be possible for university students and faculty to access modern developments as knowledge in all disciplines accumulates at a rapid and exponential pace, in particular this is a huge obstacle for establishing a research culture. The Ministry of Higher Education together with the universities will examine strategies to overcome this deficit".

We would like to continue this project and to end the method of manual notes and papers. Based on the request of higher education institutions, there is the need to publish about 100 different textbooks each year.

I would like to ask all the lecturers to write new textbooks, translate or revise their lecture notes or written books and share them with us to be published. We will ensure quality composition, printing and distribution to Afghan universities free of charge. I would like the students to encourage and assist their lecturers in this regard. We welcome any recommendations and suggestions for improvement.

It is worth mentioning that the authors and publishers tried to prepare the books according to the international standards, but if there is any problem in the book, we kindly request the readers to send their comments to us or the authors in order to be corrected for future revised editions.

We are very thankful to Konrad Adenauer Stiftung (KAS) which has provided fund for this book. We would also like to mention that they have provided funds for 8 textbooks so far.

I am especially grateful to GIZ (German Society for International Cooperation) and CIM (Centre for International Migration & Development) for providing working opportunities for me from 2010 to 2016 in Afghanistan.

In our ministry, I would like to cordially thank Minister of Higher Education Dr. Najibullah K. Omary (PhD), Academic Deputy Minister Prof Abdul Tawab Balakarzai, Administrative & Financial Deputy Minister Prof Dr. Ahmad Seyer Mahjoor (PhD), Administrative & Financial Director Ahmad Tariq Sediqi, Advisor at Ministry of Higher Education Dr. Gul Rahim Safi, Chancellor of Nangarhar University, Deans of faculties, and lecturers for their continuous cooperation and support for this project .

I am also thankful to all those lecturers who encouraged us and gave us all these books to be published and distributed all over Afghanistan. Finally I would like to express my appreciation for the efforts of my colleagues Hekmatullah Aziz, Fahim Habibi and Dr. Nasim Khogiani in the office for publishing books.

Dr Yahya Wardak
Advisor at the Ministry of Higher Education
Kabul, Afghanistan, December, 2017
Office: 0756014640
Email: textbooks@afghanic.de

Message from the Ministry of Higher Education

In history, books have played a very important role in gaining, keeping and spreading knowledge and science, and they are the fundamental units of educational curriculum which can also play an effective role in improving the quality of higher education. Therefore, keeping in mind the needs of the society and today's requirements and based on educational standards, new learning materials and textbooks should be provided and published for the students.

I appreciate the efforts of the lecturers and authors, and I am very thankful to those who have worked for many years and have written or translated textbooks in their fields. They have offered their national duty, and they have motivated the motor of improvement.

I also warmly welcome more lecturers to prepare and publish textbooks in their respective fields so that, after publication, they should be distributed among the students to take full advantage of them. This will be a good step in the improvement of the quality of higher education and educational process.

The Ministry of Higher Education has the responsibility to make available new and standard learning materials in different fields in order to better educate our students.

Finally I am very grateful to Konrad Adenauer Stiftung (KAS) and our colleague Dr. Yahya Wardak that have provided opportunities for publishing this book.

I am hopeful that this project should be continued and increased in order to have at least one standard textbook for each subject, in the near future.

Sincerely,

Dr. Najibullah K. Omary (PhD)

Minister of Higher Education

Kabul, 2017



Book Name Algebra & Theory of Numbers Part II
Author Sultan Ahmad Niazman
Publisher Nangarhar University, Science Faculty
Website www.nu.edu.af
Published 2017, First Edition
Copies 1000
Serial No 256
Download www.ecampus-afghanistan.org



This publication was financed by Konrad Adenauer Stiftung (KAS).

Administrative and technical support by Afghanic.

The contents and textual structure of this book have been developed by concerning author and relevant faculty and being responsible for it. Funding and supporting agencies are not holding any responsibilities.

If you want to publish your textbooks, please contact us:
Dr. Yahya Wardak, Ministry of Higher Education, Kabul
Office 0756014640
Email textbooks@afghanic.de

All rights reserved with the author.

Printed in Afghanistan 2017

Sahar Printing Press

ISBN 978-9936-620-50-6