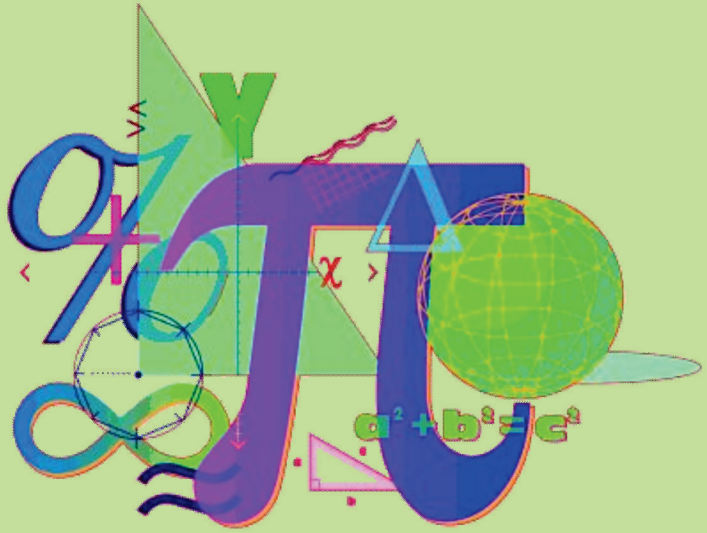
پوهنځی ساینس بلخ

الجبر معاصر



داکتر عبدالله مهمند

همراه با سی دی

فروش منع است

۱۳۹۸

الجبر معاصر

Algebra

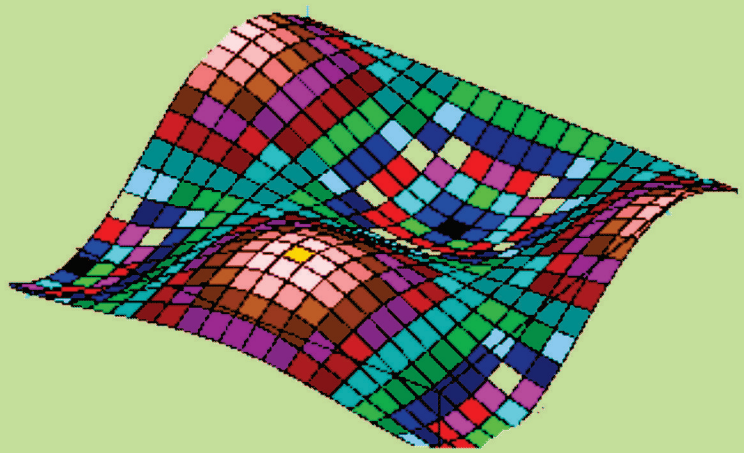
داکتر عبدالله مهمند

Balkh Science Faculty

Afghanic

Dr Abdullah Mohmand

Algebra



Funded by
Afghanistan-Schulen-VUSAF

With CD

ISBN 978-9936-633-14-8

Not for Sale

2019

الجبر معاصر

داکتر عبدالله مهمند

افغانیک
Afghanic

Dari PDF
2019

Balkh Science Faculty
پوهنځی ساینس بلخ

Funded by
Afghanistan-Schulen-VUSAF

Algebra

Dr Abdullah Mohmand

Download:
www.ecampus-afghanistan.org

اقرأ باسم ربك الذي خلق

الجبر معاصر

داکتر عبدالله مهمند

چاپ اول

این کتاب را به فورمت پی دی اف همراه با سی دی آن هم مطالعه میتوانید:

نام کتاب	الجبر معاصر
مؤلف	داکتر عبدالله مهمند
ناشر	پوهنتون بلخ، پوهنځی ساینس
ویب سایت	www.ba.edu.af
سال چاپ	۱۳۹۸، چاپ اول
تعداد	۱۰۰۰
نمبر مسلسل	۲۷۹
داونلود	www.ecampus-afghanistan.org
محل چاپ	مطبعه افغانستان تایمز، کابل، افغانستان

این کتاب توسط مؤسسهٔ اتحادیه معاونت برای مکاتب در افغانستان (Afghanistan-Schulen-VUSAF) تمویل شده است.
امور اداری و تخنیکی کتاب توسط افغانیک انجام یافته است.
مسؤولیت محتوا و نوشتن کتاب، مربوط نویسنده و پوهنځی مربوطه میباشد.
ارگان های کمک کننده و تطبیق کننده مسؤول نمی باشند.

اگر میخواهید که کتابهای تدریسی شما چاپ شود با ما به تماس شوید:
داکتر یحیی وردک، وزارت تحصیلات عالی، کابل
دفتر ۰۷۵۶۰۱٤٦٤۰
ایمیل textbooks@afghanic.de

ای اس بي ان ۸ – ۱۴ - ٦۳۳ –۹۹۳٦– ۹۷۸

پیام وزارت تحصیلات عالی

در جریان تاریخ بشریت کتاب و اثر علمی برای کسب، حفظ، پخش و نشر علم و دانش نقش عمدهٔ را بازی کرده و جز اساسی پروسه درسی پنداشته میشود که در ارتقای کیفیت تحصیلات دارای ارزش خاص میباشد. از اینرو باید با در نظر داشت نیازهای روز، معیارهای شناخته شدهٔ جهانی و ضروریات جوامع بشری، کتب و مواد درسی جدید برای محصلین آماده و چاپ گردد.

از اساتید و مؤلفین محترم کشور قلباً اظهار سپاس و قدردانی مینمایم که با سعی وتلاش دوامدار در جریان سالهای متمادی با تألیف و ترجمهٔ کتب درسی دَین ملی خود را اداء و موتور علم و دانش را به حرکت در آورده اند.

از سایر اساتید و دانشمندان گرانقدر نیز صمیمانه تقاضا مینمایم که در رشته های مربوطهٔ خود کتب و سایر مواد درسی را تهیه و به چاپ برسانند، بعد از چاپ به دسترس محصلین گرامی قرار داده تا در ارتقای کیفیت تحصیلات و در پیشرفت پروسه علمی، قدم نیکی را برداشته باشند.

وزارت تحصیلات عالی وظیفهٔ خود میداند تا در جهت ارتقای سطح دانش محصلین عزیز، کتب و مواد درسی جدید و معیاری را به رشته های مختلف علوم آماده و چاپ نماید.

در اخیر از مؤسسه اتحادیه معاونت برای مکاتب در افغانستان (Afghanistan-Schulen-VUSAF) و همکار ما داکتر یحیی وردک صمیمانه تشکر و قدر دانی مینمایم، که زمینهٔ چاپ و تکثیر کتب درسی اساتید و سایر دانشمندان گرانقدر را مهیا و مساعد ساخته اند.

امیدوارم این کار سودمند ادامه و توسعه یابد، تا در آینده نزدیک در هر مضمون درسی حد اقل یک کتاب درسی معیاری داشته باشیم.

با احترام

پوهنمل دوکتور نجیب الله خواجه عمری

وزیر تحصیلات عالی

کابل، ۱۳۹۸

چاپ کتب درسی

استادان گرامی و محصلان عزیز!

کمبود و نبود کتب درسی در پوهنتون های افغانستان یکی از مشکلات عمده به شمار میرود که محصلان و استادان را با مشکلات زیاد روبرو ساخته است. آنها اکثراً به معلومات جدید دسترسی نداشته و از چپتر ها ولکچرنوت های استفاده مینمایند که کهنه بوده و در بازار به کیفیت پایین فوتوکاپی وعرضه میگردد.

برای رفع این مشکلات ما تا به حال به تعداد ۲۷۹ عنوان کتب مختلف درسی پوهنځی های طب، ساینس، انجنیری، اقتصاد، ژورنالیزم و زراعت (۹۶ عنوان کتب طبی توسط کمک مالی انجمن همکاریهای عملی آلمان DAAD، ۱۶۰ عنوان کتب مختلف طبی و غیر طبی توسط کمیتۀ جرمنی برای اطفال افغانستان kinderhilfe-Afghanistan، ۷عنوان کتاب توسط جمیعت پوهنتونهای آلمانی و افغانی DAUG، ۲ عنوان کتاب توسط جنرال کنسلگری آلمان در مزار شریف، ، ۳ کتاب توسط Afghanistan-Schulen، ۱کتاب توسط بنیاد صافی، ۱ کتاب دیگر توسط سلواک اید، ۸ عنوان کتاب توسط بنیاد کانراد ادناور KAS) پوهنتون های ننگرهار، خوست، کندهار، بلخ، هرات، البیرونی، کابل، پوهنتون پولی تخنیک کابل و پوهنتون طبی کابل را چاپ نموده ایم. قابل یاد آوری است که تمام کتب چاپ شدۀ مذکور بصورت مجانی برای تمام پوهنتون ها، تعداد زیات ادارات و مؤسسات کشور توزیع گردیده اند.

تمام کتاب های چاپ شدۀ طبی و غیرطبی را از پورتال www.ecampus-afghanistan.org داونلود نموده میتوانید.

در حالیکه پلان ستراتیژیک وزارت تحصیلات عالی (۲۰۱۰ – ۲۰۱۴) کشور بیان می دارد:

« برای ارتقای سطح تدریس، آموزش و آماده سازی معلومات جدید، دقیق و علمی برای محصلان، باید برای نوشتن و نشر کتب علمی به زبان های دری و پشتو زمینه مساعد گردد. برای ریفورم در نصاب تعلیمی، ترجمه از کتب و مجلات انگلیسی به دری و پشتو حتمی و لازمی میباشد. بدون امکانات فوق ناممکن است تا محصلان و استادان در تمامی بخش ها به پیشرفت های مدرن و معلومات جدید زود تر دسترسی بیابند.»

ما میخواهیم که این روند را ادامه داده، تا بتوانیم در زمینۀ تهیه کتب درسی با پوهنتون های کشور همکاری نماییم و دوران چپتر و لکچرنوت را خاتمه دهیم. نیاز است برای مؤسسات تحصیلات عالی کشور سالانه حداقل به تعداد ۱۰۰ عنوان کتاب درسی چاپ گردد.

از تمام استادان محترم خواهشمندیم که در بخش های مسلکی خویش کتب جدید تألیف، ترجمه و یا هم لکچرنوت ها و چپتر های خود را ایدیت و آمادۀ چاپ نمایند و در اختیار ما قرار دهند، تا با کیفیت عالی چاپ و به طور مجانی به دسترس پوهنځی های مربوطه، استادان و محصلین قرار داده شود.

همچنان در مورد نکات ذکر شده پیشنهادات و نظریات خود را به آدرس ما شریک ساخته، تا بتوانیم مشترکاًدر این راستا قدم های مؤثرتری را برداریم.

ازمحصلین عزیز نیز خواهشمندیم، که در امور ذکر شده با ما و استادان محترم همکاری نمایند.

قابل تذکر است که از طرف مؤلف وناشر نهایت کوشش گردیده تا محتویات کتب به اساس معیار های بین المللی آماده گردد. درصورت موجودیت مشکلات درمتن کتاب، از خوانندگان محترم خواهشمندیم تا نظریات و پیشنهادات شانرا بصورت کتبی به آدرس ما و یا مؤلف بفرستند، تا در چاپ های آینده اصلاح گردد.

از مؤسسه اتحادیه معاونت برای مکاتب در افغانستان (Afghnistan-Schulen-VUSAF) بسیار تشکر مینمائیم که مصرف چاپ این کتاب را به عهده گرفته است. قابل تذکر است که اینها مصرف چاپ ۳ عنوان کتاب درسی را تا کنون پرداخته اند.

بطور خاص از دفتر جی آی زیت (GIZ) و CIM (Center for International Migration & Development) یا مرکز برای پناهندگی بین المللی و انکشاف، که برایم امکانات کاری را از ۲۰۱۰ الی ۲۰۱٦ در افغانستان مهیا ساخته بود، اظهار سپاس و امتنان مینمایم.

از محترم پوهنمل دوکتور نجیب الله خواجه عمری وزیر تحصیلات عالی، محترم پوهنمل دیپلوم انجنیر عبدالتواب بالاکرزی معین علمی، محترم داکتر احمد سیر مهجور معین مالی و اداری، محترم احمد طارق صدیقی رئیس مالی و اداری، محترم داکتر گل رحیم صافی مشاور در وزارت تحصیلات عالی، ر رؤسای پوهنتونها، رؤسای محترم پوهنځی ها و استادان گرامی تشکر مینمایم که پروسۀ چاپ کتب درسی را تشویق و حمایت نموده اند.

همچنان ازهمکاران محترم دفتر هرکدام حکمت الله عزیز و فهیم حبیبی نیز تشکر مینمایم که در قسمت چاپ نمودن کتب همکاری نموده اند.

داکتر یحیی وردک، مشاور وزارت تحصیلات عالی
کابل، مارچ ۲۰۱۹
نمبر تیلیفون دفتر: ۰۷۵٦۰۱۴٦۴۰
ایمیل آدرس: textbooks@afghanic.de

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

ازآنجائیکه الجبر معاصر درپوهنځی های ساینس افغانستان مربوط نصاب تحصیلی گردیده و درین بخش کمبود کتاب به لسان های پښتو و دری حس میشود. ازاینرو وظیفه خود دانسته تا راجع به الجبرمعاصر (که بنام الجبر مدرن ویا الجبر مجرد نیز یاد میشود) بعضی اساسات و مفاهیمی را که در الجبر معاصرعمومیت دارد و ازان امروز در ریاضیات زیاد استفاده میشود، به پښتو و دری درتحریربیاورم. در محتویات این کتاب لکچرهای سال های اخیر پوهنتون های المان ودیگرممالک نیزدرنظرگرفته شده است.

باپیشرفت علم درساحات مختلف عملیات (operations) کلاسیک جمع "+" و ضرب "." نمی توانست بعضی مسایل را حل نماید. این سبب شد که علما برای حل اینوع موضوعات عملیات (operations) جدید را تعریف نمایند. وقتیکه N.H. Abel درسال 1826 موفق به دریافت یک فورمول برای حل معادلات الجبری که درجه ان بزرگتراز 3 باشد، نشد .دران وقت به فکرتعریف یک ساختمانی الجبری نظربه یک رابطه دوگانه (binary operation) شد. که این البته شروع الجبرمعاصر بود. بعدترعلمای دیگر مثل D. Hilbert , R.Dedekind و E. Steinitz الجبرمعاصر را انکشاف دادند. که امروز ان در ساحات مختلف بطورمثال Groups (گروپ) , Rings (حلقه) , Fields (ساحه) وغیره تقسیم شده است.

همچنان کوشش نمودم که قضایای مهم الجبر معاصربا مثال ها را دراخیرعلاوه نمایم.

استفاده ازالجبرمعاصردر کریپتوگرافیCryptography (رمز نویسی) بامثال هانیزدرین کتاب گنجانیده شده است. کوشیش کردم که در اینجا از سمبولهاي رياضي که امروز در جهان براي حل مسائل رياضي از آن استفاده ميشود وتابع یک لسان مشخص نمی باشد، استعمال نمایم .

هم چنان در استعمال نام واصطلاحات درصورت امکان ازهردولسان (دری و انگلسی) استفاده شده است. مگر برای بعضی مفاهیمی الجبرمعاصرما هنوز درلسان دری نام های ستندردی نداریم، مجبوراً نام های انگلسی رادران استعمال نمودم. البه این براي کسانیکه کتاب های ریاضی را به لسانهاي بين المللي مطالعه مينمايند ، هم مفید خواهد بود. سمبولهاي رياضي و اختصاراتی که درینجا ازان استفاده شده دراخیرکتاب تشریح نمودم. امکان دارد که درتحریر ویادر ساختن جملات اشتباهات ویا غلطی های موجود باشد، معذرت میخواهم.

(داکتر عبدالله مهمند)

فهرست موضوعات

فصل چهارم

دایرکت پرودکت گروپ (Direct product of groups)
ایکسترنیل دایرکت پرودکت (External direct product)
اینترنیل دایرکت پرودکت (Enternal direct product)

فصل پنجم

گروپ های دورانی (cyclic group)
ایولرفنکشن (Euler function)
گروپ پرایم رسیوکلاس (prime residue class group)

فصل ششم

حلقه (Ring)
رینگ فرعی (Subring)
ادیال (ideal)
رینگ هومورفیزم (Ring homomorphism)
قضیه رینگ هومورفیزم (Ring homomorphism theorem)
قضیه رینگ اسومورفیزم (Ring isomorphism theorem)
اینتگرال دومین (Integral domain) (ناحیه تمامی)
گوس رینگ (Gaussian Ring)
اویکلیدین دومین (Euclidean Domain)
مشخصه یی رینگ (Characteristic of Ring)
رینگ پولینوم (Polynomial Ring)
دویسن الگوریتم یی پولینوم (Polynomial Division Algorithm)
قضیه یی ریمیندر (Remainder Theorem)

فصل هفتم

ساحه (Field)

فصل هشتم

توسعه فیلد (extensions field)
درجه یی توسعه فیلد (degree of extension field)
توسعه الجبری(algebraic extension)
قضیه لاگرنج برای ساحه (The theorem of Lagrange for fields)
مینیمال پولینوم (minimal polynomial)
ساحه سپلیتینگ (Splitting field)

قضیه اساسی الجبر(The fundamental theorem of algebra)
ساحه کیوسینت (quotient field)
معیارهای ایزن شتاین برای پولینوم (Eisenstein's criterion)

فصل نهم

قضیه کیلی (Cayley Theorem)
قضیه چینای (Chinese remainder theorem)
معادلات کلاس های باقیمانده (Equations of congruent classes)
فورمول ویتا (Vieta's formulas)
کریپتوگرافی (Cryptography)
سیستم کریپتوگرافی RSA

اساسات رياضي

(مجموعه ، تصویر(نقش) ، رابطه ومنطق رياضی)

[Set , Mapping , Relation and mathematical logic]

درین فصل میخواهم بعضی اساسات ریاضی ، مفاهیم وقضایا که بعد درالجبر معاصر ازان استفاده میشود ، به شکل مختصرتشریح نمایم.

تعریف 0.1: مجموعه ویا سیت (set) را Georg Cantor درسال 1874 میلادی طوری تعریف نموده است:

set یک مجموعه از اوبجیکتهای (Objects) که دارای مشخصاتی معین مگر ازهمدیگرمختلف اند ، میباشد. بطورمثال اگرX سیت محصیلین شعبه ریاضی پوهنځی ساینسی پوهنتون هرات باشد . مشخصاتی معین درینجا محصل بودن در شعبه ریاضی پوهنځی ساینسی پوهنتون هرات است. مگرهرمحصل ازهمدیگرفرق دارد. ما سیت را به شکل ذیل نشان میدهیم :

$$X = \{x_1, x_2, \dots \dots \dots \dots .\}$$

درینجا $\dots . x_3, x_2, x_1$ Objects اند که بنام عناصر(elements) از سیت X یادمیشوند. تعدادعناصریک سیت X را cardinality ان سیت میگویند وبه $|X|$ نشان داده میشود. سیت خالی را به $\emptyset$ نشان میدهند .

تعریف 0.2 :

(a) اگر X و Y دو سیت باشند . X سیت فرعی (subset) از Y گفته میشود $(X \subseteq Y)$ در صورتیکه :

$$\forall x \in X \implies x \in Y$$

یک سیت فرعی X را (proper subset) ازY $(X \subset Y)$ گفته میشود ، به شرطیکه در Y عناصرموجود باشند که درX شامل نباشند . یعنی:

$\exists a \in Y ; a \notin X$

بطورمثال:

$X = \{2,4,5\}, Y = \{2,4,5,a,b\} \implies X \subset Y$

هرسیت یک سیت خالی فرعی دارد . X وY باهم مساوی گفته میشود در صورتیکه $(X \subseteq Y)$ و $(Y \subseteq X)$ باشد. یعنی

$$X = Y \Leftrightarrow (X \subseteq Y) \wedge (Y \subseteq X)$$

نوت: درینجا بعضی اوقات بجای کلیمه „ متناهی „ کلیمه „ معین „ استعمال شده است. یعنی درینجا عین معنی رادارد.

(b) R . Dedekind (1831-1916) سیت معین*(finite set)* را طوری تعریف نموده است :

یک سیت X متناهی است، درصورتکه درX هیچ *proper subset* (سیت فرعی) موجود نباشد که *Cardinality* (تعدادعناصر) ان مساوی به X باشد . یعنی

$$\nexists\, A \subset X\,;\ |A| = |X|$$

ویا اینکه :

$$\forall\ A \subset X\,;\ |A| < |X|$$

ما سیت متناهی را به $X = \{x_1, x_2, \dots, x_n\}$ نشان میدهیم. دراینجا تعداد عناصر X مساوی به $n \neq \infty$ n است. یعنی $|X| = n$

هرسیت که متناهی نباشد ، سیت لامتناهی (infinite set) گفته میشود.

یعنی: $|X| = \infty$

مثال :

$\mathbb{N} = \{\ 1,2,3\ ,3,4, \dots\}$

$\mathbb{N}_0 = \{\ 0, 1,2,3\ ,3,4, \dots\}$

$\mathbb{Z} = \{\ \dots, -3, -2, -1\ ,0,1,2,3\ , \dots\}$

$2\mathbb{Z} = \{\ \dots, -6, -4, -2\ ,0,2,4,6\ , \dots\}$

$\mathbb{Q} = \{\frac{p}{q}\ \ |\ p, q \in \mathbb{Z}, q \neq 0\}$

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

سیت های فوق لامتناهی اند . زیرا :

$$(\ \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}\ ,\ 2\mathbb{Z} \subset \mathbb{Z}\ )$$

$$\wedge$$

$$(\ |\mathbb{N}| = \infty, |\mathbb{Z}| = \infty, |2\mathbb{Z}| = \infty, |\mathbb{Q}| = \infty, |\mathbb{R}| = \infty, |\mathbb{C}| = \infty\ )$$

مثال : سیت های ذیل متناهی اند

$X = \{x \mid x$ یک بحری ا عظم$\}$

$Y = \{y \in \mathbb{Z} \mid -2 \leq y \leq 2\}$

X و Y هرکدام 5 عنصر دارد . یعنی $|X| = |Y| = 5$

مگر $X \nsubseteq Y$ و $Y \nsubseteq X$

$W_1 : = \{w \in \mathbb{Z} \mid -15 \leq w \leq 16 \quad \}$

$W_2 : = \{w \in \mathbb{Z} \mid (1 \leq w \leq 16 \ ) \wedge (w \text{ even } (\text{جفت}))\}$

$= \{2,4,6,8,10,12,14,16\}$

دیده میشود که $W_2 \subseteq W_1$ و $|W_2| = 8$

سیت های ذیل خالی اند

$W_3 : = \{n \in \mathbb{N} \mid n < 0 \}$, $W4 : = \{x \in \mathbb{Z} \mid x^2 = 3 \}$

$|W_3| = |W_4| = 0$ و

تعریف 0.3: اگر $X_1, X_2, \dots, X_n$ سیت ها باشند

اتحاد (Union):

$X_1 \cup X_2 \cup \dots \cup X_n := \{x \mid \exists i \in \{1,2,3,\dots,n\}; x \in X_i\}$

تقاطع (intersection):

$X_1 \cap X_2 \cap \dots \cap X_n := \{x \mid x \in X_i, \forall i \in \{1,2,\dots,n\}\}$

درمثال فوق $W_1 \cup W_2 = W_1$ و $W_1 \cap W_2 = W_2$ است

مثال: اگر $\mathbb{R}_+$ سیت اعداد حقیقی که بزرگترویا مساوی به صفرباشد و $\mathbb{R}_-$ سیت اعداد حقیقی که کوچکتر ویا مساوی به صفرباشد . یعنی

$\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0 \quad \}$

$\mathbb{R}_- = \{x \in \mathbb{R} \mid x \leq 0 \quad \}$

اتحاد انها سیت اعداد حقیقی و تقاطع شان صفر است. یعنی $\mathbb{R}_+ \cup \mathbb{R}_- = \mathbb{R}$ و $\mathbb{R}_+ \cap \mathbb{R}_- = \{0\}$

مثال:

$X := \{x \in \mathbb{Z} \mid (-8 \leq x \leq 8)\}$

$Y := \{x \in \mathbb{Z} \mid (-8 < x < 8)\}$

$8 \in X \implies 8 \in X \cup Y$

$-8 \in X \wedge -8 \notin Y \implies -8 \notin X \cap Y$

$5 \in X \wedge 5 \in Y \implies 5 \in X \cap Y$

مثال :

$A = \{a,b,c,d\}$, $B = \{d,e,f\}$, $C = \{a,b\}$

$A \cup B = \{a,b,c,d,e,f\}$, $A \cap B = \{d\}$

$C \subseteq A$, $A \cup C = \{a,b,c,d\} = A$, $A \cap C = \{a,b\} = C$

$A \setminus B = \{ a \in A \mid a \notin B \} = \{a,b,c\}$
$A \setminus C = \{ a \in A \mid a \notin C \} = \{ c, d \}$, $C \setminus A =$
چون $C \subseteq A$ است. سیت $A \setminus C$ complement از C در A وسیت $A \setminus B$ relative Complement از B نطربه A است

مثال:

$$W_1 := \{x \in \mathbb{R} \mid x < 0 \vee x > 0\}$$
$$W_2 := \{x \in \mathbb{R} \mid x < 0 \wedge x > 0\}$$

سیت W_1 ازاعداد حقیقی که از صفربزرگ و یا ($\vee$) از صفرکوچک باشد، تشکیل شده است . یعنی:

$$W_1 = \mathbb{R} \setminus \{0\} = \mathbb{R}^*$$

سیت W_2 ازاعداد حقیقی که از صفربزرگ و ($\wedge$) از صفرکوچک باشد، تشکیل شده است. چون ان نوع عدد حقیقی وجود ندارد . پس W_2 خالی است یعنی:

$$W_2 = \emptyset$$

تمرین 0.1 : عناصر (elements) سیت های ذیل رادریافت نماید :

(a)

$$X := \{x \in \mathbb{Z} \mid (-1 \leq x \leq 6)\}$$

(b)

$$Y := \{x \in \mathbb{Z} \mid (1 \leq x \leq 7)\}$$

(c)

$$A: \{n \in \mathbb{Z} \mid 0 \leq n \leq 4\}$$
$$M := \{x \in \mathbb{Z} \mid x = n^2 - 4 \ , n \in A\}$$

(d) $X \cup Y$ و $X \cap Y$ رادریافت نماید. البته X و Y سیت های فوق اند

تعریف : X یک سیت است. ما تمامی سیت های فرعی X را p(X) نشان میدهیم. یعنی: $p(X) := \{A \mid A \subseteq X\}$

P(X) بنام power set از X یادمیشود. اگر X یک سیت متناهی و تعداد عناصر (elements) ان n باشد. درانصورت p(X) هم متناهی ودارای 2^n عناصرمیباشد. یعنی: $|p(X)| = 2^n$

مثال: اگر $X = \{a,b\}$ باشد . سیت های فرعی ان $A_1=\{a\}$ $A_2=\{b\}$, $A_3=\{a,b\}$, و $\emptyset$ اند. یعنی:

$$P(X) = \{ A_1, A_2, A_3, \emptyset \} \text{ و } |p(X)| = 2^2 = 4$$

اگر X سیت خالی باشد. درانصورت $p(X) = p(\emptyset) = \{\emptyset\}$ و
$|p(\emptyset)| = 1$

قضیه : برای سیت های X و Y افادهای ذیل صدق میکند:

(a)

$$X \subseteq Y \iff p(X) \subseteq P(Y)$$

(b)

$$p(X \cap Y) = p(X) \cap P(Y)$$

(c)

$$p(X) \cup p(Y) \subseteq p(X \cup Y)$$

ثبوت(a):

" $\Rightarrow$ "

$$A \in \mathrm{p(X)} \Rightarrow A \subseteq X \Rightarrow A \subseteq Y \Rightarrow A \in \mathrm{p(Y)}$$
$$\Rightarrow p(X) \subseteq P(Y)$$

$$x \in X \Rightarrow \{x\} \subseteq X \Rightarrow \{x\} \in p(X)$$
$$\Rightarrow \{x\} \in p(Y) \quad [\text{نظربه فرضیه}]$$
$$\Rightarrow \{x\} \subseteq Y \Rightarrow x \in Y \Rightarrow X \subseteq Y$$

ثبوت(b):

$$A \in p(X \cap Y) \Rightarrow A \subseteq X \cap Y \Rightarrow A \subseteq X \wedge A \subseteq Y$$
$$\Rightarrow A \in p(X) \wedge A \in p(Y) \Rightarrow A \in p(X) \cap P(Y)$$
$$A \in p(X) \cap P(Y) \Rightarrow A \subseteq X \wedge A \subseteq Y \Rightarrow A \subseteq X \cap Y$$
$$\Rightarrow A \in p(X \cap Y)$$

در نتیجه : $p(X \cap Y) = p(X) \cap P(Y)$

ثبوت(c):

$$A \in p(X) \cup p(Y) \Rightarrow A \subseteq X \vee A \subseteq Y$$
$$\Rightarrow A \subseteq (X \cup Y) \Rightarrow A \in p(X \cup Y)$$

مگررابطه ذیل صدق نمی کند:

$$p(X \cup Y) \subseteq p(X) \cup p(Y)$$

مثال:

$$X := \{1,2\}, Y = \{2,3\}$$
$$p(X) = \{\emptyset, \{1\}, \{2\}, \{1,2\}, \}$$
$$p(Y) = \{\emptyset, \{2\}, \{3\}, \{2,3\}\}$$

$p(X) \cup p(Y) = \{\emptyset, \{1\}, \{2\}, \{1,2\}, \{3\}, \{2,3\}\}$
$X \cup Y = \{1,2,3\}$
$p(X \cup Y) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}\{2,3\}, \{1,2,3\}\}$
دیدیه میشودکه $\{1,3\} \notin p(X) \cup p(Y)$

قضیه: اگرتعداد عناصر(elements) یک سیت معین A_n مساوی به n $(n \geq 0)$ باشد، درانصورت تعداد عناصر Power set ان 2^n است .

ثبوت:میخواهیم این قضیه راازطریقه complete induction نظرn ثبوت نمایم.

درثبوت complete induction سه حالت ذیل موجود است:

شروع ایندکشن : باید برای n = 0 صدق نماید

فرضیه ایندکشن: ما فرض میکنیم برای تمامی سیت که تعداد عناصر شان $n \geq 1$ باشد ، صدق میکند

ثبوت ایندکشن : باید ثبوت شود که برای n+1 هم صدق میکند

شروع ایندکشن:

$$n = 0 \implies A_n = \emptyset \implies p(A_n) = \{\emptyset\} \implies |p(A_n)| = 1 = 2^0$$

دیده شد که این حالت صدق میکند

فرضیه ایندکشن: قبل می نمایم که برای n صدق میکند. یعنی: $|p(A_n)| = 2^n$

ثبوت ایندکشن: ما A_n و A_{n+1} رابه شکل تعریف مینایم:

$$A_n := \{a_1, a_2, \dots, a_n\}$$
$$A_{n+1} := \{a_1, a_2, \dots, a_n, a_{n+1}\}$$
$$A_n \subseteq A_{n+1} \implies p(A_n) \subseteq p(A_{n+1})$$

نظر به فرضیه ایندکشن تعداد عناصر $p(A_n)$ مساوی 2^n است. ما این عناصررابه شکل ذیل نشان میدهیم :

$$p(A_n) = \{s(1), s(2), \dots, s(2^n)\}, \quad |p(A_n)| = 2^n$$
$$p(A_{n+1}) = p(A_n) \cup \{a_{n+1}\} = \{ s(1), s(2), \dots, s(2^n),$$
$$s(1) \cup \{a_{n+1}\}, s(2) \cup \{a_{n+1}\}, \dots, s(2^n) \cup \{a_{n+1}\} \}$$

درفوق دیده میشودکه $\{a_{n+1}\}$ در اتحاد 2^n دفعه تکرارمیشود، پس میتوان نوشت:

$$|p(A_{n+1})| = |p(A_n)| + 2^n = 2^n + 2^n = 2.2^n = 2^{n+1}$$

مثال:

$A_n := \{a_1, a_2\}$

$A_{n+1} := \{a_1, a_2, a_3\}$

درین مثال $n = 2$ است

$p(A_n) = \{\emptyset, \{a_1\}, \{a_2\}, \{a_1, a_2\}\}$

$|p(A_n)| = 2^2 = 4$

$p(A_{n+1}) = p(A_n) \cup \{a_3\} = \{\emptyset, \{a_1\}, \{a_2\}, \{a_1, a_2\},$
$\{\emptyset, a_3\}, \{a_1, a_3\}, \{a_2, a_3\}, \{a_1, a_2, a_3\}\}$

$|p(A_{n+1})| = |p(A_n)| + 4 = 2^2 + 2^2 = 2.2^2 = 2^{2+1} == 2^3 = 8$

تمرین:

(a) اگر $X = \{a, b, c\}$ باشد. $P(X)$ و $|p(X)|$ رادریافت نماید

(b) اگر $\{x \in \mathbb{Z} \mid 4 \leq x^2 \leq 16\} =: X$ باشد. عناصر سیت X و $|p(X)|$ رادریافت نماید .

تعریف 4. 0: تابع ویا نقش (function or mapping) از سیت A بالای سیت B یک رابطه بین این دو سیت است . که برای هر عنصر $a \in A$ فقط تنها یک عنصر در B موجود باشد که ان نقش ویا تصویر از a میباشد . ما آنرا به شکل ذیل نشان میدهیم :

$$f: A \longrightarrow B$$
$$a \longmapsto f(a) = b$$

f (a) بنام mapping (تصویر و یا نقش) از a نظر به A , f به نام Domain ، B به نام Codomain و f(A) بنام Range (image) یاد میشود.

تابع ذیل بنام identity function یاد میشود .

$$id : B \longrightarrow B$$
$$a \longmapsto id(a) = a$$

مثال: $B := \{d, e, g, h\}$, $A := \{a, b, c\}$

$$f: A \longrightarrow B$$
$$a \longmapsto f(a) = e$$
$$a \longmapsto f(a) = g$$
$$b \longmapsto f(b) = d$$

تعریف f درفوق درست نیست. زیرا اول اینکه a دو نقش (یا تصویر) دارد و دوم c هیچ تصویر ندارد.

مثال 0. 1 : تعریف های ذیل از f درست نیست

(a)

$$f: \mathbb{Z} \longrightarrow \mathbb{N}$$
$$a \longmapsto 2a$$

زیرا :

$$a = -1 \in \mathbb{Z} \Longrightarrow f(a) = f(-1) = -2 \notin \mathbb{N}$$

(b)

$$f: \mathbb{R} \longrightarrow \mathbb{R}$$
$$r \longmapsto \sqrt{r}$$

زیرا بطور مثال $f(-2) = \sqrt{-2} \notin \mathbb{R}$

مگرتابع ذیل درست است

$$f: \mathbb{R} \to \mathbb{C}$$
$$r \longmapsto \sqrt{r}$$

مثال: $B := \{0 , 1\}$, $A := \{a , b , c\}$

(a)

$$f: A \to B \quad , f(a) = 0 , f(b) = 1 , f(c) = 1$$

درین مثال range و codomain مساوی به B اند

(b)

$$g: A \to B \quad , g(a) = 1 , g(b) = 1 , g(c) = 1$$

درین مثال domain مساوی به A ، codomain مساوی به B و range مساوی به {1} نظربه g است

نوت: دو تابع f و g وقتی باهم مساوی اند که هردودارای عین domain (بطور مثال A) وبرای هر $a \in A$ باید $f(a) = g(a)$ صدق نماید.

تعریف 0.5 : $f : A \longrightarrow B$ یک نقش (Mapping) است.

f injective: $a, b \in A \ , \ f(a) = f(b) \quad \Longrightarrow \quad a = b$

(یعنی اگرما $a, b \in A$ داشته باشیم که $f(a) = f(b)$ باشد، درانصورت باید a = b شود) . ویااینکه :

$$a, b \in A \ , \ a \neq b \ \Longrightarrow f(a) \neq f(b)$$

f surjective : $\forall \ b \in A \ \exists \ a \in A \ ; \ f(a) = b$

(يعنى براى هر $b \in B$ بايد يک $a \in A$ موجود باشد كه $f(a) = b$ شود)

f bijective : f injective $\wedge$ f surjective

مثال: $A:=\{ a , b , c \}$, $B:=\{d , e , g \}$

$$f: A \longrightarrow B$$
$$a \longmapsto f(a) = e$$
$$b \longmapsto f(b) = e$$
$$c \longmapsto f(c) = d$$

f يک injective نيست. زيرا $f(a) = f(b) = e$ مگر $a \neq b$ است

f يک surjective نيست. زيرا براى $g \in B$ هيچ عنصر در A موجود نيست كه نقش ان g باشد. يعنى:

$$\nexists\ x \in A\ ;\ f(x) = g$$

مثال: $A:=\{ a , b , c \}$, $B:=\{d , e \}$

$$f: A \longrightarrow B$$
$$a \longmapsto f(a) = d$$
$$b \longmapsto f(b) = d$$
$$c \longmapsto f(c) = e$$

f يک surjective است مگر injective نيست. زيرا $f(a) = f(b) = d$ مگر $a \neq b$ است .

مثال: $A:=\{ a , b , c \}$, $B:=\{d , e , g , h \}$. ما نميتوانيم يک تابع $f: A \longrightarrow B$ را دريافت نمايم كه surjective باشد. زيرا:

$$|A| = 3 < 4 = |B|$$

مگرامكان injective موجود است.

مثال 0.2 :

$$f: \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$a \longmapsto 2a$$

f يک injective است .اگرما $a , b \in A$ داشته باشيم كه $f(a) = f(b)$ شود. درانصورت بايد ثبوت كه $a = b$ است

$$f(a) = f(b) \implies 2a = 2b \Rightarrow a = b$$

f Surjective نیست زیرا در $\mathbb{Z}$ هیچ عنصری وجود ندارد که نقش آن نظربه f اعداد طاق (بطورمثال یک) شود . یعنی:

$$\nexists x \in \mathbb{Z}; f(x) = 1$$

مثال 0.3 :

(a) تابع ذیل Bijective است

$$f: \mathbb{R} \longrightarrow \mathbb{R}$$
$$a \longmapsto 2a$$

Injective بودن آن واضح است و surjective نیز است . زیرا :

$$b \in \mathbb{R}, a: = \frac{b}{2} \in \mathbb{R} \implies f(a) = f\left(\frac{b}{2}\right) = 2.\frac{b}{2} = b$$

(b) تابع ذیل Injective است. مگر surjective نیست

$$f: \mathbb{N} \longrightarrow \mathbb{N}$$
$$n \longmapsto f(n) = n + 1$$

$m,n \in \mathbb{N}$, $f(m) = f(n) \Rightarrow m + 1 = n + 1 \Rightarrow m = n \Rightarrow$ f injective

surjective نیست .زیرا برای عدد1 هیچ یک عدد m در $\mathbb{N}$ موجود نیست که $f(m) = 1$ شود.

مثال: تابع ذیل نه injective و نه surjective است

$$f: \mathbb{C} \longrightarrow \mathbb{R}$$
$$z = a+ib \longmapsto |z| = \sqrt{a^2 + b^2}$$

$z_1 = 3 + 4i$, $z_2 = -3 - 4i$

$$f(z_1) = |z_1| = \sqrt{3^2 + 4^2} = \sqrt{25} = 5$$
$$f(z_2) = |z_2| = \sqrt{(-3)^2 + (-4)^2} = \sqrt{25} = 5$$

مگر $z_1 \neq z_2$ است. پس injective نیست.

Surjective هم نیست. زیرا $f(z) \geq 0$ است (برای هر $z \in \mathbb{C}$)

تمرین 0.2: نشان دهید که چرا تابع ذیل نه injective ونه surjective شده میتواند

$$f: \mathbb{Z} \to \mathbb{Z}$$
$$x \longmapsto x^2$$

تعریف 0.6 : اگر ما دو تابع $f: A \to B$ و $g: B \to C$ داشته باشیم .تابع $g \circ f : A \to C$ بنام ترکیب تابع(mapping combination) از f و g یاد میشود. بصورت عموم ترکیب دو تابع را به "∘"نشان میدهند .

مثال :

$$f: \mathbb{N} \longrightarrow \mathbb{Z} \qquad g: \mathbb{Z} \longrightarrow \mathbb{R}$$
$$a \longmapsto a+1 \qquad b \longmapsto b^2-1$$

$f(a) = a+1 \in \mathbb{Z}$, $b := a+1$

$g \circ f\,(a) = g(a+1) = g(b) = b^2 - 1 = (a+1)^2 - 1$
$= a^2 + 2a + 1 - 1 = a^2 + 2a$

تمرین: $g \circ f$ رادریافت نماید

(a)

$$f: \mathbb{N} \longrightarrow \mathbb{N} \qquad g: \mathbb{N} \longrightarrow \mathbb{R}$$
$$a \longmapsto a+1 \qquad b \longmapsto 2\sqrt{b}$$

(b)

$$f: \mathbb{N} \longrightarrow \mathbb{N} \qquad g: \mathbb{N} \longrightarrow \mathbb{Q}$$
$$a \longmapsto a+1 \qquad b \longmapsto 2\sqrt{b}$$

لیما 0.1: اگر ما دو تابع $f: X \to Y$, $g: Y \to Z$ را داشته باشیم . بعداً :

(a) f injective $\wedge$ g injective $\implies$ g $\circ$ f injective
(b) f surjective $\wedge$ g surjective $\implies$ g $\circ$ f surjective
(c) g $\circ$ f injective $\implies$ f injective
(d) g $\circ$ f surjective $\implies$ g surjective

ثبوت (a) : اگر برای $a, b \in X$ $g \circ f(a) = g \circ f(b)$ باشد. باید ثبوت شود که $a = b$

$g \circ f(a) = g \circ f(b) \implies f(a) = f(b)$ [زیرا g یک injective]
$\implies a = b$ [زیرا f یک injective]

ثبوت (b) : باید ثبوت شود که :

$\forall z \in Z, \exists x \in X; g \circ f(x) = y$

f surj $\implies \forall y \in Y \; \exists\, x \in X; f(x) = y$
g surj $\implies \forall z \in Z \;\; \exists\, y \in Y ; g(y) = z$

در نتیجه :

$g\big(f(x)\big) = g(y) = z \implies g \circ f$ surjective

تمرین 0.3 : (c) و (d) لیمای فوق را ثبوت نمائید .

تمرين 0.4:

$f: \mathbb{Z} \longrightarrow \mathbb{Z}$, $g: \mathbb{Z} \longrightarrow \mathbb{Z}$, $h: \mathbb{Z} \longrightarrow \mathbb{Z}$

$n \longmapsto 2n$ $n \longmapsto 3n + 5$ $n \longmapsto -6n$

(a) تركيب توابع ذيل را دريافت نمايد

$f \circ g$, $g \circ f$, $f \circ h$, $h \circ f$, $g \circ h$, $h \circ g$

(b) كدام ان تركيب ها injective وكدام ان surjective است

تعريف 0.7 : $f: A \to B$ يک تابع Bijective است . تابع معكوس (inverse function) آن به شكل ذيل تعريف شده است :

$$f^{-1}: B \longrightarrow A$$
$$b \longmapsto a := f^{-1}(b)$$

يعنى تصوير $b \in B$ نظره به f^{-1} همان عنصر $a \in A$ كه $f(a) = b$ و f^{-1} نيز Bijective است

$$f \circ f^{-1} = id: B \to B \quad \wedge \quad f^{-1} \circ f = id: A \to A$$

مثال : تابع ذيل يک Bijective است

$$f: \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto 3x + 2$$

تابع معكوس آن (f^{-1}) شكل ذيل را دارد

$$f^{-1}: \mathbb{R} \longrightarrow \mathbb{R}$$
$$y \longmapsto \frac{y-2}{3}$$

زيرا:

$$f^{-1}(y) = \frac{y-2}{3} \Longrightarrow f \circ f^{-1}(y) = f\left(\frac{y-2}{3}\right) = \frac{3(y-2)}{3} + 2 = y$$

تمرين 0.5:

(a) ثبوت نمايد كه f در مثال فوق bijective است .

(b) معكوس تابع ذيل رادريافت نمايد

$$f: \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto 2x + 1$$

تعريف 0.8 :

(a) سيت متناهى به شكل ذيل هم تعريف شده است:

يک سيت M وقتى متناهى گفته ميشود كه:

$$f: M \to M \quad \text{injective} \quad \Leftrightarrow \quad f: M \to M \quad \text{surjective}$$

ویا به شکل ذیل :

$\exists\, n \in \mathbb{N} \wedge \exists$ bijective $f: M \to \{1,2,\dots,n-1\}$
$\Longrightarrow$ M finite (متناهی)

(b) countable set (سیت قابل شمارش):

یک سیت X بنام countable Set (سیت قابل شمارش) یاد میشود، درصورتکه دربین X ویک سیت فرعی (subset) ازاعداد طبعی $\mathbb{N}$ یک bijective موجود باشد. درغیران بنام uncountable یادمی شود.

یک سیت X بنام infinite countable (سیت قابل شمارش لامتناهی) یاد میشود درصورتکه دربین X و اعداد طبعی $\mathbb{N}$ یک تابع bijective موجود باشد.

بطورمثال اعداد تام $\mathbb{Z}$ و اعداد ناطق $\mathbb{Q}$ سیت های قابل شمارش لامتناهی اند.

مگرسیت اعدادحقیقی $\mathbb{R}$ یک uncountable است. ما میخواهیم نشان دهیم که $\mathbb{Z}$ یک سیت قابل شمارش غیرمعین است.

$$f: \mathbb{Z} \longrightarrow \mathbb{N}$$

$$k \longmapsto f(k) = \begin{cases} 2k & (k \geq 0) \\ 2(-k) - 1 & (k < 0) \end{cases}$$

:f injective

$m,n \in \mathbb{Z}$, $f(m) = f(n)$

برای m و n سه حالت ذیل موجود است:

1 . $m,n \geq 0 \Longrightarrow f(m) = 2m \wedge f(n) = 2n \Longrightarrow m = n$
$\Longrightarrow$ f injective

2 . $m \geq 0 \wedge n < 0 \Longrightarrow f(m) = 2m \wedge f(n) = 2(-n)-1$

چون $n < 0$ انتخاب شده، پس $2(-n) > 0$ و $2(-n)-1$ یک عدد طاق است.

درتیجه حالت $f(m) = 2m = 2(-n)-1 = f(n)$ امکان ندارد

3 . $m,n < 0 \Longrightarrow f(m) = 2(-m)-1 \wedge f(n) = 2(-n)-1$

$f(m) = 2(-m)-1 = f(n) = 2(-n)-1 \Longrightarrow m = n$

$\Longrightarrow$ f injective

f surjective: برای $x \in \mathbb{N}$ دوحالات ذیل موجود است:

حالت اول: x یک عدد جفت است

$$x \text{ even}, x \geq 0 \implies \exists k \in \mathbb{Z}; 2k = x \implies k = \frac{x}{2}$$

$$\implies f(k) = f(\frac{x}{2}) = 2.\frac{x}{2} = x \implies f \text{ surjective}$$

حالت دوم: x یک عدد طاق است

$$x = 2.(-k) - 1 \implies k = -\frac{x+1}{2} \in \mathbb{Z}$$

$$f(k) = f(-\frac{x+1}{2}) = 2.(-(-\frac{x+1}{2}) - 1 = x + 1 - 1 = x$$

$\implies$ f surjective

درنتیجه f بایجکتیف است و $\mathbb{Z}$ نظر به تعریف سیت قابل شمارش لامتناهی است

قضیه 0.1 : اگر A یک سیت متناهی باشد . بعدآ برای یک تابع $f: A \longrightarrow A$ افادهای ذیل معادل اند .

(i) f یک injective است

(ii) f یک surjective است .

(iii) f یک bijective است .

ثبوت : چون A متناهی است وما فرض میکنیم که n عنصر دارد . یعنی $A = \{a_1, a_2, \dots, a_n\}$ وهر جوره a_i مختلف هستند $i=(1,2,\dots,n)$.

(ii)⇐(i) اگر f یک surjective نباشد

$$f \text{ not surjective} \implies f(A) \neq A \implies \exists a \in A; a \notin f(A)$$

یعنی تعداد عناصر f(A) کمتر از n است .

نظر به پرنسیپ Birichlet اگر n اوبجکت (objects) در m (m<n) روک یا قفسه تقسیم شود حتما در یک قفس دو object است . از این نتیجه میشود که f یک injective نیست . مگر این در تضاد به فرضیه است پس باید f یک surjective باشد .

(i) ⇐ (ii) اگر f یک injective نباشد .

$$f \text{ not injective} \implies \exists a, b \in A; a \neq b \wedge f(a) = f(b)$$

درین حالت میتواند f(A) اعظمی n-1 عنصر داشته باشد. یعنی باید $f(A) \neq A$ باشد . مگر این در تضاد به فرضیه است زیرا f یک surjective است. پس f باید injective باشد .

نوت:

(a) قصیه 1.1 برای هر دوسیت متناهی A و B نیز صدق میکند، به شرطیکه $|A| = |B|$ باشد.

(b) مگر قضیه 0.1 برای سیت لامتناهی قابل تطبیق نیست. بطورمثال

$$f : \mathbb{N} \longrightarrow \mathbb{N}$$

$$n \longmapsto f(n) = \begin{cases} n & (\text{اگر } n \text{ طاق باشد}) \\ \frac{n}{2} & (\text{اگر } n \text{ جفت باشد}) \end{cases}$$

f یک surjective است : $k \in \mathbb{N}$

حالت اول : اگر k طاق باشد. درانصورت $f(k) = k$ میشود و f یک Surjective است

حالت دوم: اگر k جفت باشد. درانصورت:

$$\exists\, n \in \mathbb{N} ;\ k = \frac{n}{2} \implies n = 2k \implies f(n) = f(2k) = \frac{2k}{2} = k$$

$$\implies f \text{ surjective}$$

f مگر injective نیست. زیرا:

$$f(3) = 3 = \frac{6}{2} = f(6) \implies f \text{ not injective}$$

(c) اگر B سیت معین و A یک proper subset (یعنی $A \subset B$) باشد. درانصورت نمیتوانیم یک تابع ***bijective*** را دربین ان دو سیت دریافت نمود. مگردربین سیت های لامتناهی این امکان موجود است. مثال های ذیل انرا واضح میسازد

مثال 0.5:

(a)

$$f : \mathbb{N}_0 \longrightarrow \mathbb{Z}$$

$$x \longmapsto f(x) = \begin{cases} \frac{x}{2} & (\text{اگر } x \text{ جفت}) \\ \frac{-(x+1)}{2} & (\text{اگر } x \text{ تاق}) \end{cases}$$

البته درینجا 0 عدد جفت فرض شده است

f یک *injective* :

$x,y \in \mathbb{N}_0$

حالت $f(x) = f(y)$ برای($x = 0 \wedge y \neq 0$) ویا ($y = 0 \wedge x \neq 0$) صدق نمی کند. پس x و y را خلاف صفرفرض میکنیم. برای ثبوت *injective* سه حالت ذیل را در نظرمیگریم :

case 1: $f(x) = \frac{x}{2}$, $f(y) = \frac{y}{2}$

$$f(x) = f(y) \implies \frac{x}{2} = \frac{y}{2} \implies 2.x = 2.y \implies x = y$$

case 2: $f(x) = \frac{-(x+1)}{2}$, $f(y) = \frac{-(y+1)}{2}$

$$f(x) = f(y) \implies \frac{-(x+1)}{2} = \frac{-(y+1)}{2}$$

$$\implies -2.x - 2 = -2.y - 2 \implies x = y$$

case 3 : $f(x) = \frac{x}{2}$, $f(y) = \frac{-(y+1)}{2}$

$$f(x) = f(y) \implies \frac{x}{2} = \frac{-(y+1)}{2}$$

$$\implies 2.x = -2.y - 2 \implies x + y = 1$$

$x + y = 1$ امکان ندارد . زیرا x و y اعداد طبعی وخلاف صفراند .

دیده شد که حالت سوم امکان ندارد. یعنی اگرx جفت وy طاق باشد، درانصورت هیچ امکان ندارد که $f(x) = f(y)$ شود. مگردرحالت اول ودوم f اینجکتیف است

f یک surjective :

برای $y \in \mathbb{Z}$ سه حالت ذیل موجود است:

case 1 : y = 0

باید یک x در $\mathbb{N}_0$ یافت شود که :

$$\frac{x}{2} = y = 0 \quad \vee \quad \frac{-(x+1)}{2} = y = 0$$

$$\implies x = 0 \vee -(x+1) = 0$$

$$-(x+1) = 0 \implies x = -1 \notin \mathbb{N}_0$$

$$f(0) = \frac{0}{2} = 0$$

case 2 : y > 0

$x := 2y \in \mathbb{N}_0$

$\Longrightarrow f(x) = f(2y) = \frac{2y}{2} = y$ [زیرا 2y جفت است]

case 3 : $y < 0$

$x := -2y-1 \in \mathbb{N}_0 \Longrightarrow f(x) = f(-2y-1)$

$= \frac{-(-2y-1+1)}{2}$ [زیرا 2y-1- طاق]

$= \frac{2y}{2} = y$

در هرسه حالت دیده شد که برای هر $y \in \mathbb{Z}$ یک x در $\mathbb{N}_0$ پیدا میشود که $f(x) = y$ شود. $\mathbb{Z}$ و $\mathbb{N}_0$ هردو لامتناهی اند و $\mathbb{N}_0 \subset \mathbb{Z}$ هم صدق میکند. بازهم ***bijective*** دربین هردوسیت موجود است

(b) تابع Exponentialfunction ذیل بایجکتیف است:

$$\exp : \mathbb{R} \longrightarrow \mathbb{R}_+$$
$$x \longmapsto e^x$$

e بنام عدد اویلر (Eulers Number) یادمیشود

$e = 2.718281828459$

:injective

$x,y \in \mathbb{R}, \exp(x) = \exp(y)$

$\Longrightarrow e^x = e^y \Longrightarrow x = y \Longrightarrow$ exp injective

:surjective

$y \in \mathbb{R}_+$

$x := \ln(y) \Longrightarrow y = e^x = \exp(x) \Longrightarrow$ exp surjective

$\mathbb{R}_+$ و $\mathbb{R}$ هردولامتناهی اند و $\mathbb{R}_+ \subset \mathbb{R}$ هم صدق میکند. بازهم دربین هردو سیت یک ***bijective*** موجود است.

تمرین 0.6 : معلوم نمائید که کدام یکی از توابع ذیل surjective , injective و bijective است .

(a)

$$f : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto x^2 + 1$$

(b)

$$f: \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto 3x - 4$$

تعریف 0.9 : direct product of Sets برای سیت های A_i (i=1,2,3,…,n) به شکل ذیل تعریف شده است :

$$A_1 \times A_2 \times A_3 \times \ldots \times A_n$$
$$:= \{(a_1, a_2, a_3, \ldots, a_n) \mid a_i \in A_i, i = 1,2,3, \ldots, n\}$$

اگر ما $A = A_1 \times A_2 \times A_3 \times \ldots \times A_n$ وضع نمائیم در آنصورت هرعنصر $a \in A$ شکل ذیل را دارد:

$$a = (a_1, a_2, a_3, \ldots, a_n)$$

$(a_1, a_2, a_3, \ldots, a_n)$ بنام n-tupel یاد میشود ومساوی بودن دو n – tupel طوری تعریف شده است :

$$a = (a_1, a_2, a_3, \ldots, a_n), b = (b_1, b_2, b_3, \ldots, b_n) \in A$$
$$a = b \iff a_i = b_i \; \forall i \in \{1,2, \ldots, n\}$$

اگر $A = A_1 = A_2 = A_3 = \cdots = A_n$ باشد در آنصورت direct product از A_i را به شکل A^n نیز مینویسند

direct product بنامی Cartesian product نیزیاد میشود و درهندسه ازان زیاد استفاده میشود

اگر سیت A دارای m عنصر و سیت B دارای n عنصرباشد. یعنی $|A| = m$ و $|B| = n$. سیت G اگر direct product از A و B باشد. یعنی G = AxB . درانصورت G دارای m.n عنصرمیباشد. یعنی

$$|G| = |AxB| = |A|.|B| = m.n$$

رابطه فوق برای سیت های معین A_i (i=1,2,…,n) نیزصدق میکند.

مثال:

A = {1,2,3} , B = {a,b,c,d}
G = AxB = {1,2,3} x {a,b,c,d}
= { (1,a),(2,a),(3,a),{1,b),(2,b),(3,b),
(1,c),(2,c),(3,c),(1,d),(2,d),(3,d) }

دیده میشود که |G| = 3.4 = 12 است

مثال 0.6:

$\mathbb{R}^2 := \mathbb{R}$ x $\mathbb{R}$

$f: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$

$(x_1, x_2) \mapsto (2x_1\ ,\ x_2)$

f injective:

$x = (x_1,x_2)\ ,\ y = (y_1,y_2)\ \in \mathbb{R}^2$

اگر $f(x) = f(y)$ باشد. باید ثبوت شود که $x = y$ است

$f(x) = f(y) \implies (\ 2x_1\ ,\ x_2\ ) = (\ 2y_1\ ,\ y_2\ )$

$\implies 2x_1 = 2y_1 \wedge x_2 = y_2 \implies x_1 = y_1 \wedge x_2 = y_2$

$\implies x = y$

$\implies$ f injective

f surjective:

$y = (y_1,y_2)\ \in \mathbb{R}^2$

باید یک $x = (x_1,x_2) \in \mathbb{R}^2$ موجود باشد که $f(x) = y$ شود

$f(x) = f(x_1\ ,\ x_2) = (\ 2x_1\ ,\ x_2\ ) := y = (y_1,y_2)$

$\implies 2x_1 = y_1 \wedge x_2 = y_2 \implies x_1 = \frac{y_1}{2} \wedge x_2 = y_2$

$\implies f(x) = f(x_1\ ,\ x_2) = f(\frac{y_1}{2}\ ,\ y_2) = (\ 2.\frac{y_1}{2}\ ,\ y_2\ ) = (\ y_1\ ,\ y_2\ ) = y$

$\implies$ f surjective

در نتیجه f یک bijective است.

تمرین 0.7:

(a) عناصر (elements) سیت های ذیل کدام اند :

$$W := \{(x,y) \in \mathbb{Z}x\mathbb{Z} \mid (x + y = 0) \wedge (-3 \leq x,y \leq 3)\}$$

$$X := \{(x,y) \in \mathbb{Z}x\mathbb{Z} \mid (x^2 = y^2) \wedge (-3 \leq x,y \leq 3)\}$$

$$Y := \{(x,y) \in \mathbb{Z}x\mathbb{Z} \mid (x = 0 \vee y = 0) \wedge (-3 \leq x,y \leq 3)\}$$

(b)

$$W := \{(x_1,x_2,x_3) \in \mathbb{R}^3 \mid x_2 = x_3\}$$

$u = (1,0,1)\ ,\ v = (2,0,3),\ w = (0,1,0)$

معلوم نماید که کدام یکی از w,v,u شامل W و کدام یکی ان شامل نیستند

(c)

$H := \{\ (x_1,x_2,x_3,x_4) \in \mathbb{R}^4 \mid x_1+3x_2+2x_4=0\ ,\ 2x_1,x_2+x_3=0\}$

u=(1,2,0,2) , v=(3,-1,-5,0) , w=(-1,1,1,-1

معلوم نماید که کدام یکی از w,v,u شامل H و کدام یکی ان شامل نیستند

تمرین 0.8 : کدام یک از توابع ذیل injective , surjective و Bijective اند .

(a)

$$f : \mathbb{R}x\mathbb{R} \longrightarrow \mathbb{R}$$
$$(x_1, x_2) \longmapsto x_1 + x_2$$

(b)

$$f : \mathbb{R}x\mathbb{R} \longrightarrow \mathbb{R}$$
$$(x_1, x_2) \longmapsto {x_1}^2 + {x_2}^2 - 1$$

تعریف 0.10: یک رابطه (relation) „ ~" بالای یک سیت $A \neq \phi$ باخواص ذیل بنام equivalence relation (رابطه معادل) یاد میشود .

$a, b, c \in A$

(i) a~a (reflexive)

(ii) a~b ⇒ b~a (symmetric)

(iii) a~b ∧ b~c ⇒ a~c (transitive)

دربعضی کتاب های دری به جای reflexive کلیمه انعکاس، متناظر به جای symmetric و به جای transitive انتقالي استعمال می شود .

مثال: رابطه مساوات **"="** بالای یک $A \neq \phi$ رابطه معادل (eq-relation) است .

reflexive: a = a ⇒ a ~ a (∀ $a \in A$)

symmetric: a~b ⇒ a = b ⇒ b = a

⇒ b~a (∀ $(a, b) \in AxA$)

transitive: a~b ∧ b~c ⇒ a = b ∧ b = c ⇒ a = c

⇒ a~c ∀ $(a, b), (b, c) \in AxA$

مثال: بالای $\mathbb{Z}$ رابطه ذیل را درنظرمیگریم:

$a \sim b :\Leftrightarrow a \leq b$ ($(a, b) \in \mathbb{Z}x\mathbb{Z}$)

رابطه فوق reflexive و transitive است. مگر symmetric نیست. زیرا:

$2 \leq 3 \Rightarrow 2 \sim 3$

$3 \not\leq 2 \Rightarrow 3 \not\sim 2$

پس رابطه فوق رابطه معادل (eq-relation) نیست .

مثال 0.7: بالای $\mathbb{Z}$ رابطه ذیل رابطه معادل (eq-relation) است .

$(a, b) \in \mathbb{Z}x\mathbb{Z}$

$a \sim b :\Leftrightarrow 2 \mid a - b$ ($a - b$ بالای 2 قابل تقسیم است)

:reflexive

$a - a = 0 \Rightarrow 2 \mid 0 \Rightarrow a \sim a$

: symmetric

$(a, b) \in \mathbb{Z}x\mathbb{Z}$, $a \sim b \Rightarrow 2 \mid a - b \Rightarrow \exists\, q \in \mathbb{Z}\,;\, a - b = 2q$

$\Rightarrow b - a = 2.(-q)$

$\Rightarrow 2 \mid b - a \Rightarrow b \sim a \Rightarrow$ "$\sim$" symmetric

: transitive

$(a, b), (b, c) \in \mathbb{Z}x\mathbb{Z}$, $a \sim b \wedge b \sim c \Rightarrow 2 \mid a - b \wedge 2 \mid b - c$

$\Rightarrow \exists\, m \in \mathbb{Z}\,;\, a - b = 2m \wedge \exists\, n \in \mathbb{Z}\,;\, b - c = 2n$

$\Rightarrow b = a - 2m \wedge c = b - 2n$

$\Rightarrow c = a - 2m - 2n = a - 2(m+n)$

$\Rightarrow c - a = -2(m+n) \Rightarrow a - c = 2(m+n) \Rightarrow 2 \mid a - c$

$\Rightarrow$ "$\sim$" transitive

ثبوت شد که "$\sim$" یک رابطه معادل (eq-relation) است .

مثال: بالای $\mathbb{Z}$ (اعداد تام) این "$\sim$" رابطه (relation) به شکل ذیل تعریف شده است : $a,b,c \in \mathbb{Z}$

$a \sim b :\Leftrightarrow a.b \neq 0$

$a \sim b \Rightarrow a.b \neq 0 \Rightarrow b.a \neq 0 \Rightarrow b \sim a \Rightarrow$ "$\sim$" symmetric

$a \sim b \wedge b \sim c \Rightarrow a.b \neq 0 \wedge b.c \neq 0$

$\Rightarrow a \neq 0 , b \neq 0 , c \neq 0$

$\Rightarrow a.c \neq 0 \Rightarrow a \sim c \Rightarrow$ "$\sim$" transitive

مگر reflexive نیست . زیرا اگر $0 \sim 0$ صدق کند ، باید $0 \neq 0.0$ شود.
پس "$\sim$" یک رابطه معادل (eq-relation) نیست.

تمرین 0.9 :

(a) X شاگردان یک مکتب است. بالای X رابطه (relation) ذیل تعریف شده است:

$a,b \in X$

$a \sim b: \Leftrightarrow$ a همرای b دریک صنف است

ثبوت نماید که "$\sim$" یک رابطه معادل (eq-relation) است

(b) X محصلین پوهنځي ساینس است. بالای X رابطه (relation) ذیل تعریف شده است:

$a,b \in X$

$a \sim b: \Leftrightarrow$ a هم قد b است

ثبوت نماید که "$\sim$" یک رابطه معادل (eq-relation) است

تمرین 0.10 : بالای $\mathbb{Q}$ (اعداد ناطق) رابطه ذیل تعریف شده است:

$a, b \in \mathbb{Q}$

$a \sim b: \Leftrightarrow a - b \in \mathbb{Z}$

(a) ثبوت نماید که "$\sim$" یک رابطه معادل (eq-relation) است

(b) کدام روابط درذیل درست است

$\frac{26}{12} \sim \frac{14}{12}$, $\frac{9}{3} \sim \frac{10}{5}$, $\frac{2}{3} \sim \frac{1}{6}$, $\frac{8}{7} \sim \frac{1}{7}$, $\frac{6}{7} \sim \frac{1}{8}$

تعریف 0.11: بالای سیت $X \neq \phi$ یک „ $\sim$ „ equivalence relation
(رابطه معادل) تعریف شده است

$[x]_{\sim} := \{ y \in X \mid x \sim y \}$

$[x]_{\sim}$ را equivalence class (کلاس معادل) میگویند. اگرما رابطه معادل (eq-relation) از مثال 0.6 رادر نظربگیریم . بطور مثال

$[5]_{\sim} = \{ y \in X \mid 5 \sim y \} = \{ y \in X \mid 2 \mid 5 - y \}$

$= \{ \ldots., -5,-3,-1,1,3,5, 7, 9, 11, \ldots\ldots. \}$

قضیه 0.2 : $X \neq \phi$ سیت و „ ~ „ یک رابطه معادل (eq-relation) بالای X است. درانصورت افاده ذیل صدق میکند :

(a) $X = \bigcup_{x \in X} [x]_{\sim}$

(b) $[x]_{\sim} \neq \phi \quad \forall x \in X$

(c) $[x]_{\sim} \cap [y]_{\sim} \neq \emptyset \Leftrightarrow x \sim y \Leftrightarrow [x]_{\sim} = [y]_{\sim}$

ثبوت (a) : $\bigcup_{x \in X} [x]_{\sim} \subseteq X$ واضح است

$x \in X \implies x \in [x]_{\sim}$ [~ reflexive]

$\implies [x]_{\sim} \neq \phi \wedge X \subseteq \bigcup_{x \in X} [x]_{\sim}$

درعین وقت (b) هم ثبوت شد.

(c) ثبوت :

$u \in [x]_{\sim} \cap [y]_{\sim}$

$\implies x \sim u \wedge y \sim u$

$\implies x \sim u \wedge u \sim y$ [~ symetric]

$\implies x \sim y$ [~ transitive]

$x \sim y \implies \forall u \in [x]_{\sim} ; x \sim u$

$\wedge\ x \sim y$ [~ symetric $\wedge$ transitive]

$\implies y \sim u$ [~ symetric $\wedge$ transitive] $\implies u \in [y]_{\sim}$

$\implies [x]_{\sim} \subseteq [y]_{\sim}$

به همین شکل میتوان ثبوت نمود که $[y]_{\sim} \subseteq [x]_{\sim}$

ازجانب دیگراگر :

$[x]_{\sim} = [y]_{\sim} \implies x \sim y \implies [x]_{\sim} \cap [y]_{\sim} \neq \emptyset$

تعریف 1.12: $n, k \in \mathbb{N}$

$n! = 1.2.3.....n$

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!.(n-k)!} & 0 \leq k \leq n \\ 0 & k > n \end{cases}$$

$n!$ بنام factorial و $\binom{n}{k}$ بنام binomial coefficient یاد میشود. البته درینجا $\binom{n}{k}$ برای k مساوی به n ویامساوی به صفرطوری ذیل تعریف شده

$\binom{n}{0} = \binom{n}{n} = 1$

مثال:

$5! = 1.2.3.4.5 = 120$

$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{120}{6.2} = \frac{120}{12} = 10$

تعریف0.13 : (mathematical logic and De Morgan`s Laws)

ما میخواهیم درینجا مختصر منطق ریاضیات (mathematical logic) و قانون De Morgan را با مثال تشریح نمایم.

(a) Boolean Operators : عملیات (operatotrs) ذیل بنام Boolean Operators یادمیشود:

∧ : logical **and** (conjuction) (و)

∨ : logical **or** (disjuction (یا)

بطورمثال ما افادهای (statments) ذیل راداریم:

P : محصل بودن در پوهنتون کابل

Q : به لسان پشتو سخن زدن

R : باشینده هرات

مثال: احمد باشینده بلخ ، محصل پوهنتون کابل وپه پشتو میتواند صحبت نماید.

درینجا افادهای P وQ صدق میکند. مگر افاده R صدق نمی کند. اگر ان افادهای که صدق می کند به T (true) و که صدق نمی نماید به F (false) نشان دهیم، درانصورت میتوان انرا دریک جدول به شکل نشان دهیم

and (∧) :

P	Q	R	P ∧ Q	P ∧ R	Q∧ R
T	T	F	T	F	F

or (∨):

P	Q	R	P ∨ Q	P ∨ R	Q ∨ R
T	T	F	T	T	T

مثال: ما افاده ذیل راداریم:

P : کباب خوردن

Q : کولا نوشیدن

R : شربت نوشیدن

$P \wedge Q$: محمود میخواهد کباب بخورد و کولا بنوشد

$Q \vee R$: محمود میخواهد کولا یا شربت بنوشد

$P \wedge (Q \vee R)$: محمود میخواهد کباب بخورد و (کولا یا شربت بنوشد)

$Q \vee (P \wedge R)$ **:** محمود میخواهد کولا بنوشد یا (کباب بخورد و شربت بنوشد)

نوت : P ، Q و R سه افاده (statments) است. به صورت عموم Operators Boolean خواص ذیل را دارد:

تبدیلی (commutative) : $P \wedge Q = Q \wedge P$

اتحادی (associative) : $P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$

$P \vee (Q \vee R) = (P \vee Q) \vee R$

توزیعی (distributive)

$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$

$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$

(b) قانون دمرجن (De Morgen`s Laws) :

ما سه افاده p ، Q و R را ازمثال فوق درنظرمیگریم

logic not: $\neg$

$\neg P$: کباب نخوردن

$\neg Q$: کولا نه نوشیدن

$\neg R$: شربت نه نوشیدن

Negation of a conjunction

$\neg(P \wedge Q)$: محمود نمی خواهد کباب بخورد یا کولا بنوشد

Negation of a disjunction

¬(PVQ) : محمود نمی خواهد کباب بخورد و نمی خواهد کولا بنوشد

De Morgen`s Laws in Boolean Algebra :

$\neg(P \wedge Q) = \neg P \vee \neg Q$

$\neg(P \vee Q) = \neg P \wedge \neg Q$

مثال:

$P: \{x \in \mathbb{N} \mid x \leq 15$, $Q: \{x \in \mathbb{N} \mid x > 8\}$

$P \wedge Q = \{x \in \mathbb{N} \mid x \leq 15 \wedge x > 8\} = \{9,10,11,12,13,14,15\}$

$\neg(P \wedge Q) = \neg P \vee \neg Q = \{x \in \mathbb{N} \mid (x > 15) \vee (x \leq 8)\}$

$= \{16,17,..,8,7,\ldots,1\}$

$P: x = 10$, $Q: x = -10$, $R: x^2 = 100$

$P \Longrightarrow R \wedge Q \Longrightarrow R$, $R \nRightarrow P$, $R \nRightarrow Q$, $R \Leftrightarrow PVQ$

De Morgen`s Laws in Sets :

$A,B \subseteq X$

$A^c := A \backslash B = \{ a \in A \mid a \notin B \}$

A^c denotes the set complement of A in X

$(A \cup B)^c = A^c \cap B^c$

$(A \cap B)^c = A^c \cup B^c$

مثال :

$A \cup B = \{a,b,c,d,e,f\}$, $A \cap B = \{c,d\}$

$X := \{ a,b,c,d,e,f,g,h,8,9\}$, $A := \{ a,b,c,d\}$, $B := \{c,d,e,f,\}$

$A^c = \{e,f,g,h,8,9\}$, $B^c = \{a,b,g,h,8,9\}$

$(A \cup B)^c = \{g,h,8,9\} = A^c \cap B^c$

$(A \cap B)^c = \{a,b,e,f,g,h,8,9\} = A^c \cup B^c$

فصل اول

گروپ(Group)

تعریف 1.1 : رابطه دوگانه(Binary operation) $\oplus$ بالای یک سیت $M \neq \phi$ عبارت از یک نقش و یا تابع (mapping)

$$\oplus : M \times M \longrightarrow M$$
$$(a, b) \longmapsto a \oplus b$$

است. یعنی برای هر $(a, b) \in M \times M$ فقط تنها یک عنصر $c \in M$ موجود است که $c = a \oplus b$ شود.

مثال 1.1 : در مثال ذیل رابطه دوگانه (Binary operation) " $\oplus$ "بالاي $\mathbb{Z}$ (اعداد تام) تعریف شده است

$$\oplus : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a, b) \longmapsto a \oplus b = 2a - b$$

اما اگر $\oplus$ بشکل ذیل بالاي $\mathbb{N}$ (اعداد طبيعي) تعریف نمائیم

$$\oplus : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$
$$(a, b) \longmapsto a \oplus b = 2a - b$$

این تعریف $\oplus$ بالای $\mathbb{N}$ درست نیست. زیرا برای $a = 2 , b = 6$

$$a \oplus b = 2 \cdot 2 - 6 = -2 \notin \mathbb{N}$$

مثال :

$$\odot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$
$$(a, b) \longmapsto a \odot b = \frac{1}{2}(a + b)$$

" $\odot$ " یک رابطه دو گانه (Binary operation) بالای $\mathbb{R}$ (حقیقی اعداد) است اگر $\odot$ به شکل ذیل بالای $\mathbb{Z}$ (تام اعداد) تعریف شود:

$$\odot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(a, b) \longmapsto a \odot b = \frac{1}{2}(a + b)$$

مگر این یک رابطه دوگانه نیست. زیرا اگر $a = 2$ و $b = 3$ باشد

$$a \odot b = \frac{1}{2}(a + b) = \frac{1}{2}(2 + 3) = \frac{5}{2} \notin \mathbb{Z}$$

تعریف 1.2 : یک سیت $M \neq \phi$ با یک رابطه دوگانه $\oplus$ بنام ساختمان الجبری (algebraic structure) یاد میشود و ما آن را به شکل $(M, \oplus)$ نشان میدهیم.
یک سیت M با دو رابطه دوگانه $\oplus$ و $\odot$ را به شکل $(M, \oplus, \odot)$ نشان میدهیم.
بطور مثال $(\mathbb{Z}, +, .)$ و$(\mathbb{R}, +, .)$ و $(\mathbb{C}, +, .)$ ساختماني الجبري اند که هرکدام ان داراي دو رابطه دوگانه "+" و " . " میباشد.
برای یک ساختمان الجبری نظر به عملیات آن خواص ذیل تعریف شده اند:

اگر $(M, \oplus, \odot)$ یک ساختمان الجبری باشد و $a, b, c \in M$:

(i) اتحادی(associativity)

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c \quad (\forall a, b, c \in M)$$

(ii) دارای عنصر عینیت چپ(Left identity) نظر به $\oplus$ است،
درصورتکه یک $e \in M$ موجود باشد که $e \oplus a = a$ و بنام عینیت راست (right identity) درصورتکه $a \oplus e = a$ برای هر $a \in M$ شود
اگر e عینیت چپ و هم راست باشد، بنام عنصرعینیت یاد میشود.

(iii) عنصر $b \in M$ بنام معکوس چپ (Left inverse) از عنصر $a \in M$ نظر به $\oplus$ یاد میشود، درصورتکه $b \oplus a = e$ باشد وبنام معکوس راست (right inverse) یاد میشود اگر $a \oplus b = e$ شود. البته درینجا e عنصرعینیت است .

(iv) تبدیلی(commutative)

$$a \oplus b = b \oplus a \quad (\forall a, b \, M)$$

نوت: اگر $(M, \oplus, \odot)$ یک ساختمان الجبری باشد. خواص ذیل بنام توزیعی (distributive) یاد میشود

$\forall a, b, c \in M$

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$
$$\wedge$$
$$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$$

مثال:
(a) سیت $M:=\{-1,1\} \subset \mathbb{R}$ نظربه به ضرب ".„ یک ساختمان الجبری دارد مگرنظربه جمع "+„ ندارد. زیرا $1 + 1 = 2 \notin M$
(b) سیت $M:=\{-1,1,i,-i\} \subset \mathbb{C}$ نظربه به ضرب ".„ یک ساختمان الجبری دارد. زیرا:

$(-1).(-1) = 1 \in M$, $(-1).(1) = -1 \in M$,

$(-1).i = -i \in M$, $(-1).(-i) = i \in M$, $1.1 = 1 \in M$,

$1.i = i \in M$, $1.(-i) = -i \in M$, $i.i = -1 \in M$,

$i.(-i) = -1.(i^2) = (-1).(-1) = 1 \in M$,

$(-i).(-i) = 1.(i^2) = 1.(-1) = -1$

مگرنظر به جع "+" ساختمان الجبری نیست. زیرا: $(-1)+(-1) = -2 \notin M$

مثال: رابطه دوگانه ذیل تبدیلی نیست:

$$\odot: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$
$$(a, b) \longmapsto a \odot b = a^b$$

$$2 \odot 3 = 2^3 = 8 \text{ و } 3 \odot 2 = 3^2 = 9$$

مثال: X یک سیت است. P(X) نظر به اتحاد و تقاطع سیت ها ساختمان الجبری دارد. یعنی $(P(X), \cap)$ و $(P(X), \cup)$ ساختمان الجبری اند. زیرا:

$$A,B \in P(X) \implies A,B \in X \implies A \cup B \in X \wedge A \cap B \in X$$

$$\implies A \cup B \in P(X) \wedge A \cap B \in P(X)$$

مثال: یک سیت $M(2x2, \mathbb{R})$ شکل ذیل رادارد

$$M: = \{A \in M(2x2, \mathbb{R}) \mid A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \}$$

$(M,+)$ یک ساختمان الجبری (algebraic structure) است. زیرا نظر به خواص متریکس ها میتوان نوشت :

$$A , B \in M , A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} , B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} \Rightarrow A + B \in M$$

$-A = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} \in M$

(M,+) تبديلي هم است.

(M,.) هم یک ساختمان الجبری (algebraic structure) است. زیرا درینجا نیزنظربه خواص متریکس ها میتوان نوشت:

$A,B \in M \Longrightarrow A.B \in M$

(M,.) مگر خاصیت تبدیلي را ندارد. زیرا:

$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix},\ B = \begin{pmatrix} 2 & -2 \\ 2 & -1 \end{pmatrix} \in M$

$A.B = \begin{pmatrix} 1.2 + 2.2 & 1.(-2) + 2.(-1 \\ 2.2 + 1.2 & 2.(-2) + 1.(-1) \end{pmatrix} = \begin{pmatrix} 6 & -4 \\ 6 & -5 \end{pmatrix}$

$B.A = \begin{pmatrix} 2 & -2 \\ 2 & -1 \end{pmatrix}.\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 2 \\ 0 & 3 \end{pmatrix}$

دیده می شود که $A.B \neq B.A$ است
البته درینجا رابطه دوگانه "+„ جمع متریکس و ".„ضرب متریکس است. به صورت عموم میتوان گفت که سیت $M(nxn, \mathbb{R})$ نظر به جمع و ضرب متریکس ساختمان الجبري دارد.

تمرین 1.1:

$M:= \{ a \in \mathbb{R} \mid -5 \geq a \leq 3 \}$ (a)

ایا (M,+) نظربه جمع ساختمانی الجبری دارد؟

$M:= \{A \in M(2x2, \mathbb{R}) \mid A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, a^2 + b^2 \neq 0\}$ (b)

(i)

. : MxM ⟶ M
(A,B) ⟼ A.B

ثبوت نماید که (M,.) نظربه ضرب ماتریکس یک ساختمانی الجبری (Algebraic structure) است

(ii)

$+ : MxM \longrightarrow M$

$(A,B) \longmapsto A+B$

ثبوت نماید که چرا $(M,+)$ یک ساختمان الجبری ندارد

(c) اگر بالای $\mathbb{R}$ رابطه دوه گانه یی ذیل تعریف شده باشد:

$\oplus : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

$(a,b) \longmapsto a \oplus b = \frac{1}{2}(a+b)$

ثبوت نماید که $\oplus$ خاصیت اتحادی ندارد .

(d) ماسیت ذیل راداریم:

$$G := \{z \in \mathbb{C} \mid |z| = 1\}$$

$$\cdot : GxG \longrightarrow G$$

$$(z_1,z_2) \longmapsto z_1 . z_2$$

برای $z = a + ib \in \mathbb{C}$ البته $|z| = \sqrt{a^2 + b^2}$ تعریف شده است

ثبوت نماید که $(G,.)$ یک ساختمان الجبري (Algebraic structure) است

تعریف 1.3 : اگر $(G,\oplus)$ یک ساختمان الجبری (algebraic structure) باشد ، درانصوت با استفاده از تعریف **1.2** میتوان نوشت:

اگر $(G,\oplus)$ خاصیت(i) را داشته باشد بنام semigroup , اگر (i),(ii) را داشته باشد بنام monoid واگر (i),(ii),(iii) راداشته باشد بنام group یاد میشود.

اگر یک گروپ خاصیت (iv) رانیز داشته باشد. بنام گروپ تبدیلي (commutative group) یاد میشود.

نوت: عنصرعینیت چپ را بعدازاین به e وعنصرمعکوس چپ a را به a^{-1} نشان میدهیم.

مثال: $(\mathbb{N},+)$ یک semi group است. چون عنصرعینیت "0„ شامل $\mathbb{N}$ نیست ، پس monoid شده نمی تواند

قضیه 1.1 : $(G,\oplus)$ یک گروپ است. بعداً :

(1) برای هر عنصر $a \in G$ فقط تنها یک معکوس چپ(left-inverse) وجوددارد که این درعین حال معکوس راست (right-inverse) نیز است.

(2) تنها یک عینیت چپ (left-identity) وجود دارد که این در عین حال عینیت راست (right-identity) است.

ثبوت (1): اگر e عینیت چپ (left-identity) و $\bar{a}$ معکوس چپ (left-inverse) از a در G باشد. باید ثبوت شود که $\bar{a}$ معکوس راست (right -inverse) نیز است. یعنی:

$$\bar{a}\oplus a = e \quad \Longrightarrow \quad a \oplus \bar{a} = e$$

چون G یک گروپ است پس برای $\bar{a}$ نیز معکوس چپ $\bar{\bar{a}}$ موجود است که $\bar{\bar{a}}\oplus\bar{a} = e$ شود. پس

$$\forall a \in G\ \exists\ \bar{a} \in G, \bar{a}\oplus a = e\ \wedge \exists\ \bar{\bar{a}} \in G, \bar{\bar{a}}\oplus\bar{a} = e$$

$a\oplus\bar{a} = e\oplus(a\oplus\bar{a})$ [زیرا e عینیت چپ است]

$= (\bar{\bar{a}}\oplus\bar{a})\oplus(a\oplus\bar{a})$ [زیرا $\bar{\bar{a}}\oplus\bar{a} = e$]

$= \bar{\bar{a}} \oplus (\bar{a}\oplus(a\oplus\bar{a}))$ [خاصیت اتحادی]

$= \bar{\bar{a}} \oplus ((\bar{a}\oplus a)\oplus\bar{a})$ [خاصیت اتحادی]

$= \bar{\bar{a}}\oplus(e\oplus\bar{a})$ [زیرا $\bar{a}$ معکوس چپ است]

$= \bar{\bar{a}} \oplus\bar{a}$ [زیر e عینیت چپ است]

$= e$ [زیرا $\bar{\bar{a}}$ معکوس چپ است]

نشان داده شد که $\bar{a}$ همچنان معکوس راست نیز است.

ثبوت (2): اگر $e \in G$ عینیت چپ (left-identity) باشد. یعنی:

$$\forall a \in G \quad a = e\oplus a$$

درانصورت باید ثبوت شود: $\forall a \in G \quad a = a\oplus e$

ما معکوس a رابه $\bar{a}$ نشان میدیهم

$a\oplus e = a\oplus(\bar{a}\oplus a) = (a\oplus\bar{a})\oplus a$ [خاصیت اتحادی]

$= e\oplus a$ [نظر به **(1)**]

$= a$ [زیرا e عینیت چپ است]

دیده شد که e عینیت راست (left-identity) نیزاست

اگر $\bar{e} \in G$ نیزعینیت در G باشد, بعداً:

$$e \oplus \bar{e} = e \ \wedge \ e \oplus \bar{e} = \bar{e} \ \Rightarrow \ e = \bar{e}$$

ثبوت شد که دریک گروپ فقط تنها یک عنصرعینت (identity) موجود است
اگر $a' \in G$ هم یک معکوس از a باشد. درانصورت

$$a' = a' \oplus e = a' \oplus (a \oplus \bar{a}) = (a' \oplus a) \oplus \bar{a}) = e \oplus \bar{a} = \bar{a}$$

دیده شد که دریک گروپ فقط تنها یک عنصرمعکوس (inverse) موجود است
یادداشت: چون معکوس چپ یک عنصر a در عین حال معکوس راست آن است ، ما بعد ازاین آن را تنها بنام معکوس (inverse) یاد میکنیم و به a^{-1} نشان میدهیم, همچنان برای عنصر عینیت (identity) .

مثال:

$(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{Z}, +)$ گروپ های تبدیلی اند که عنصرعنیت ان صفر"0„ و a- معکوس از a است .

$(\mathbb{R}^*, .), (\mathbb{Q}^*, .)$ گروپ های تبدیلی اند که عنصر عنیت ان یک "1„ و $a^{-1} = \frac{1}{a}$ معکوس از a است. زیرا $a.\frac{1}{a} = 1$ میشود

مثال 1.1: اگرما سیت $M := M(2x2, \mathbb{R})$ را در نظربگیریم . میدانیم که (M,+) و (M,.) ساختمانی الجبري دارند. M نظربه جمع وضرب متریکس monoid است. زیرا نظربه خواص متریکس میتوان نوشت:

خاصیت اتحادي (associativity):

$A,B,C \in M$

$A+(B+C) = (A+B)+C \ \wedge \ A.(B.C) = (A.B).C$

عنصرعینیت: صفرمتریکس عنصرعینیت از (M,+) وواحد متریکس از(M,.) است. یعني:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+0 & b+0 \\ c+0 & d+0 \end{pmatrix} = A$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a+0 & 0+b \\ c+0 & 0+d \end{pmatrix} = A$$

(M,+) گروپ هم است. زیرا:

$$-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

$$A+(-A) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} = \begin{pmatrix} a-a & b-b \\ c-c & d-d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

دیده شد که $-A$ معکوس از A است
نظربه خواص متریکس (M,+) گروپ تبدیلی نیز است.
مگر (M,.) گروپ نیست. زیرا صفرمتریکس معکوس ندارد. همچنان بطورمثال متریکس ذیل معکوس ندارد

$$A = \begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix}$$

خواصی فوق از(M,+) و (M,.) نه تنها برای $M(2x2, \mathbb{R})$ بلکه به صورت عموم برای $M(nxn, \mathbb{R})$ هم صدق میکند.

نوت: سیت اعداد موهومی ویا مختلط (complex number) را به $\mathbb{C}$ نشان میدهیم و هر $z \in \mathbb{C}$ شکل $z=a+ib$ را دارد. که $a,b \in \mathbb{R}$ اند.

a = real part , i = imaginary unit , b = imaginary part ,

absolute value:= $|z| = \sqrt{a^2 + b^2}$,

complex conjugate:= $\bar{z} = a - ib$

$(\mathbb{C},+)$ یک گروپ تبدیلی است که عنصر عنیت ان صفر "0" و $-z=-a-ib$ معکوس از $z=a+ib$ است

$(\mathbb{C}^*,.)$ نیز یک گروپ تبدیلی است که عنصر عنیت ان یک "1„ است.

معکوس $z=a+ib \in \mathbb{C}^*$ که $z^{-1} = \frac{1}{z}$ به شکل ذیل به دست می اید:

$$z^{-1} = \frac{1}{z} = \frac{1}{a+ib} = \frac{1}{a+ib} \cdot \frac{a-i}{a-ib} = \frac{a-ib}{a^2 + iab - iab - i^2 b^2}$$

$$= \frac{a-ib}{a^2 - (-1) b^2} = \frac{a-ib}{a^2 + b^2} = \frac{\bar{z}}{|z|^2}$$

$$z.\, z^{-1} = \frac{z.\bar{z}}{|z|^2} = \frac{a^2 + b^2}{a^2 + b^2} = 1$$

دیده شد که z^{-1} معکوس از z است. دیگر خواص گروپ نیزصدق میکند

مثال: $z = 2\text{-}i3 \in \mathbb{C}^*$. ما میخواهیم معکوس z را درگروپ $(\mathbb{C}^*, .)$ دریافت نمایم

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{2+i3}{2^2+(-3)^2} = \frac{2+i3}{4+9} = \frac{2+i3}{13} = \frac{2}{13} + \frac{3}{13}i$$

$$z.z^{-1} = (2 - 3i) . \left(\frac{2+i3}{13}\right) = \frac{(2-3i).(2+i3)}{13}$$

$$= \frac{4-9(i.i)}{13} = \frac{4-9(-1)}{13} = \frac{13}{13} = 1$$

درنتیجه $z^{-1} = \frac{2+i3}{13}$ معکوس از $z = 2 - 3i$ است

تعریف 1. 4 : اگرما یک سیت متناهی $G := \{ a_1, a_2, a_3, \ldots, a_n \}$ داشته باشیم و G نظر به رابطه دوگانه (Binary Operation) „ * „ یک گروپ و a_1 عنصر عینیت (identity) ان باشد . درانصورت میتوان تطبیق رابطه دوگانه را بالای تمای عناصران را دریک جدول بشکل ذیل نشا ن داد

*	a_1	a_2	a_3	.	.	.	.	.	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$	.	.	.	.	.	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$	.	.	.	.	.	$a_2 * a_n$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$	.	.	.	.	.	$a_3 * a_n$
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
a_n	$a_n * a_1$	$a_n * a_2$	$a_n * a_3$	.	.	.	.	.	$a_n * a_n$

درجدول فوق باید درهرسطر (همچنان درهرستون) فقط تنها عناصرمختلف از G باشند. اینوع جدول بنام Cayley Table یادمیشود.

هرجدول Cayley گروپ نیست. وقتی گروپ شده میتواند ، که جدول خواص ذیل راداشته باشد:

(i) عنصر عینت موجود باشد

(ii) معکوس چپ و راست باهم مساوی باشند

(iii) خاصیت اتحادی داشته باشد

مثال: G:={a,b,c,d,e}

$*$	a	b	c	d	e
a	a	b	c	d	e
b	b	a	d	e	c
c	c	d	e	a	b
d	d	e	b	c	a
e	e	c	a	b	d

درجدول عنصر عیتیت a است. مگر $(G, *)$ گروپ نیست. زیرا

$c * d = a \neq b = d * c$

d معکوس چپ c است ، مگرمعکوس راست ان نیست

مثال : $A^{(2)} := \{e, a\}$. جدول Cayley از $A^{(2)}$ نظر به رابطه دوگانه $\odot$ شکل ذیل رادارد

$\odot$	e	a
e	e	a
a	a	e

$e \odot e = e$, $e \odot a = a = a \odot e$, $a \odot a = e$

$(A^{(2)}, \odot)$ یک گروپ تبدیلی است.

تمرین 1.2

(a) نشان دهید که چرا $(\mathbb{N}, +)$, $(\mathbb{Z}, .)$ و $(\mathbb{R}, .)$ ساختمان گروپی ندارند.

(b) نشان دهید که $(\mathbb{Q}^*, .)$ یک گروپ است.

(c) $G = \{1, -1\}$ ثبوت نماید که G نظربه ضرب یک گروپ است ونشان دهید که جدول Cayley ان چه شکل را دارد

(d) $G:=\{-1,1,i,-i\} \subset \mathbb{C}$. ثبوت نماید که G نظربه ضرب یک گروپ است و جدول Cayley ان چه شکل دارد

مثال 1.2 : بالای سیت $A^{(4)}=\{a_0,a_1,a_2,a_3\}$ یک رابطه دوگانه $\oplus$ به شکل زیر در یک جدول(Cayley Table) تعریف شده است:

$\oplus$	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

درجدول فوق رابطه دوگانه $\oplus$ به شکل ذیل عمل می نماید

$$a_\lambda \oplus a_\mu = \begin{cases} a_{\lambda+\mu} & if \quad \lambda+\mu < 4 \\ a_{\lambda+\mu-4} & if \quad \lambda+\mu \geq 4 \end{cases}$$

$A^{(4)}$ نظربه رابطه دوگانه $\oplus$ یک گروپ را تشکیل میدهد, زیرا:

(1) اتحادی (Associativity) ($\lambda,\mu,\nu \in \mathbb{N}$ و $0 \leq \lambda,\mu,\nu \leq 3$)

$$(a_\lambda \oplus a_\mu) \oplus a_\nu = \begin{cases} a_{\lambda+\mu} \oplus a_\nu & \text{if} \quad \lambda+\mu < 4 \\ a_{\lambda+\mu-4} \oplus a_\nu & \text{if} \quad \lambda+\mu \geq 4 \end{cases}$$

$$= \begin{cases} a_{\lambda+\mu+\nu} & if \quad \lambda+\mu+\nu < 4 \\ a_{\lambda+\mu+\nu-4} & if \quad 4 \leq \lambda+\mu+\nu < 8 \\ a_{\lambda+\mu+\nu-8} & if \quad \lambda+\mu+\nu \geq 8 \end{cases}$$

عین نتیجه را بدست می آوریم اگر ما $a_\lambda \oplus (a_\mu \oplus a_\nu)$ را در نظر بگیریم .
پس لهذا:

$$a_\lambda \oplus (a_\mu \oplus a_\nu) = (a_\lambda \oplus a_\mu) \oplus a_\nu$$

(1) عنصر عینیت a_0 است
(2) عنصر معکوس: برای هر a_λ یک عنصر a_μ عنصر معکوس آن است بشرطیکه $a_{\lambda+\mu} = 4$ شود. بطور مثال: $a_1 \oplus a_3 = a_0$
مثال 1.3 : بالای سیت $A^{(2,2)} := \{b_1, b_2, b_3, b_4\}$ یک رابطه دوگانه به شکل ذیل در یک جدول(Cayley Table) تعریف شده است.

$\odot$	b_1	b_2	b_3	b_4
b_1	b_1	b_2	b_3	b_4
b_2	b_2	b_1	b_4	b_3
b_3	b_3	b_4	b_1	b_2
b_4	b_4	b_3	b_2	b_1

در جدول دیده میشود که b_1 عنصر عینیت است و

$$b_2 \odot b_2 = b_3 \odot b_3 = b_4 \odot b_4 = b_1$$

پس هر عنصر معکوس خودش است.
برای $\lambda, \mu, \nu \in \mathbb{N}$ که $2 \le \lambda, \mu, \nu \le 4$ و λ, μ, ν ازهمدیگرمختلف باشند، رابطه دوگانه(binary operation) فوق بطورذیل تعریف شده است.

$$b_\lambda \odot b_\mu = b_\nu$$

خاصیت اتحادی: برای $\lambda, \mu, \nu \in \mathbb{N}$ که $2 \le \lambda, \mu, \nu \le 4$ و λ, μ, ν ازهمدیگرمختلف باشند میتوان نوشت :

$$\left(b_\lambda \odot b_\mu\right) \odot b_\nu = b_\nu \odot b_\nu = b_1$$

$$b_\lambda \odot \left(b_\mu \odot b_\nu\right) = b_\lambda \odot b_\lambda = b_1$$

$$\left(b_\lambda \odot b_\lambda\right) \odot b_\lambda = b_1 \odot b_\lambda = b_\lambda$$

$$b_\lambda \odot \left(b_\lambda \odot b_\lambda\right) = b_\lambda \odot b_1 = b_\lambda$$

$$\left(b_\mu \odot b_\mu\right) \odot b_\nu = b_1 \odot b_\nu = b_\nu$$

$$b_\mu \odot \left(b_\mu \odot b_\nu\right) = b_\mu \odot b_\lambda = b_\nu$$

$$\left(b_\mu \odot b_\nu\right) \odot b_\nu = b_\lambda \odot b_\nu = b_\mu$$

$$b_\mu \odot (b_\nu \odot b_\nu) = b_\mu \odot b_1 = b_\mu$$

$$\left(b_\mu \odot b_\nu\right) \odot b_\mu = b_\lambda \odot b_\mu = b_\nu$$

$$b_\mu \odot \left(b_\nu \odot b_\mu\right) = b_\mu \odot b_\lambda = b_\nu$$

در نتیجه دیده میشود که $\left(A^{(2,2)}, \odot\right)$ یک گروپ است. گروپ $A^{(2,2)}$ بنام Klein four-group(F.Klein 1849-1925) یاد میشود.

لیما 1.1: برای هردوعنصر $a, b \in G$ یک گروپ $(G, \oplus)$ معادله زیر صدق میکند :

$$(a \oplus b)^{-1} = b^{-1} \oplus a^{-1}$$

ثبوت: باید ثبوت شود که $a^{-1} \oplus b^{-1}$ هم یک عنصر معکوس از $a \oplus b$ است.
یعنی باید ثبوت شود که:

$$(b^{-1} \oplus a^{-1}) \oplus (a \oplus b) = e$$

$$(b^{-1} \oplus a^{-1}) \oplus (a \oplus b) = b^{-1} \oplus \left(a^{-1} \oplus (a \oplus b)\right)$$

$$= b^{-1} \oplus ((a^{-1} \oplus a) \oplus b)$$

$$= b^{-1} \oplus (e \oplus b) = b^{-1} \oplus b = e$$

قضیه 1.2: برای یک گروپ $(G, \oplus)$ افاده های زیر صدق میکند:

$a, b, c \in G$ **(1)**

$$c \oplus a = c \oplus b \Rightarrow a = b$$

$$\wedge$$

$$a \oplus c = b \oplus c \Rightarrow a = b$$

يعني ما ميتوانيم كه در يك گروپ عمليه اختصار را انجام دهيم .

(2)

$$a,b \in G\ ,\ \exists!\, x \in G\ ;\ x \oplus a = b\ \ \wedge\ \ \exists!\, y \in G\ ; a \oplus y = b$$

ثبوت (1): ما فرض ميكنيم كه $c \oplus a = c \oplus b$ است

$$c \oplus a = c \oplus b \Rightarrow c^{-1} \oplus (c \oplus a) = c^{-1} \oplus (c \oplus b)$$

$$\Rightarrow (c^{-1} \oplus c) \oplus a = (c^{-1} \oplus c) \oplus b$$

$$\Rightarrow e \oplus a = e \oplus b$$

$$\Rightarrow a = b$$

با عين شكل ميتوان قسمت ديگر را نيز ثبوت كرد.

ثبوت(2):

$$a,b \in G \Rightarrow \exists a^{-1} \in G \qquad [\ \text{زيرا } G \text{ يک گروپ است}\ ]$$

$$\Rightarrow\ b \oplus a^{-1} \in G$$

اگرما $x := b \oplus a^{-1}$ وضع نمايم. درانصورت

$$x = b \oplus a^{-1} \Rightarrow x \oplus a = (b \oplus a^{-1}) \oplus a = b \oplus (a \oplus a^{-1})$$
$$= b \oplus e = b$$

ديده شد كه انوع يک x در G موجود است. حلا ثبوت می نمايم كه فقط تنها يک ان نوع x موجود است. اگر $w \in G$ هم همانطور يک عنصر باشد

$$w \oplus a = b \Rightarrow (w \oplus a) \oplus a^{-1} = b \oplus a^{-1}$$

$$\Rightarrow w \oplus (a \oplus a^{-1}) = b \oplus a^{-1}$$

$$\Rightarrow w \oplus e = b \oplus a^{-1}$$

$$\Rightarrow w = b \oplus a^{-1} = x$$

ديده شد كه فقط تنها يک x به ان خاصيت موجود است.

قضيه 1.3: اگر $\oplus$ يک رابطه دوگانه بالای سيت $G \neq \emptyset$ باشد. بعداً افادهای ذيل بايكديگر معادل اند:

(1) $(G, \oplus)$ يک گروپ است

(2)

(a) $\oplus$ خاصیت اتحادی دارد

(b) برای هر دو عنصر $a, b \in G$ دوعنصر $x, y \in G$ با خواص زیر وجود دارند.

$$x \oplus a = b \quad \wedge \quad a \oplus y = b$$

ثبوت:

(1) $\Leftarrow$ **(2)** : نظر به خواص گروپ و قضیه 1.2 بدست میآید.

(2) $\Leftarrow$ **(1)** : نظر به (b) میتوان نوشت:

$c \in G \Rightarrow \exists e \in G\,;\, e \oplus c = c$ [اگر $c = a = b$ باشد]

$a \in G \Rightarrow \exists y \in G\,;\, c \oplus y = a$

$$\Rightarrow e \oplus a = e \oplus (c \oplus y) = (e \oplus c) \oplus y = a$$

پس عنصر عینیت e موجود است.

$e, a \in G \Rightarrow \exists x \in G\,;\, x \oplus a = e$

یعنی x معکوس از a است.

تمرین 1. 3 :

$G := \{A \in M(2x2, \mathbb{R}) \mid A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, a^2 + b^2 \neq 0\}$

$\cdot : G \times G \longrightarrow G$

$(A,B) \longmapsto A \cdot B$

ثبوت نماید که $(G,.)$ یک گروپ است

تمرین 1.4: $G := \{z \in \mathbb{C} \mid |z| = 1\}$ و $|z| = \sqrt{a^2 + b^2}$ برای $z=a+ib$ تعریف شده است.

$\cdot : G \times G \rightarrow G$

$(z_1, z_2) \mapsto z_1 \,.\, z_2$

ثبوت نماید که $(G,.)$ یک گروپ است

نوت : مابعد ازین رابطه دوگانه (Binary operation) را به "." نشان میدهیم وهدف ازان عملیه ضرب عادی نیست.

مثال 1.4: بالای سیت $D_4 := \{e, a, b, c, d, f, g, h\}$ یک رابطه دوگانه (Binary operation) به شکل ذیل در یک جدول تعریف شده است :

.	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	f	g	h	d
b	b	c	e	a	g	h	d	f
c	c	e	a	b	h	d	f	g
d	d	h	g	f	e	c	b	a
f	f	d	h	g	a	e	c	b
g	g	f	d	h	b	a	e	c
h	h	g	f	d	c	b	a	e

D_4 نظر به رابطه دوگانه ئی فوق یک گروپ است که عنصرعینیت آن e میباشد. چون a.c = e بوده پس معکوس a عنصر c است. یعنی $a^{-1} = c$ وچون h.h = e بوده پس معکوس h خودش است . یعنی $h^{-1} = h$. به همین شکل میتوان از روی جدول معکوس تمامی عناصر را پیدا نمود .
خاصیت اتحادی (assosative) نیز صدق میکند . بطور مثال :

a. (d . f)= a . c = e ∧ (a . d). f = f . f = e

گروپ D_4 بنام Dihedral group یاد میشود .

مثال 1.5 : Q_8:={ e,a,b,c,d,f,g,h} نظر به جدول کیلی (cayley table) ذیل یک گروپ است .

.	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	a	e	g	h	f	d
c	c	b	e	a	h	g	d	f
d	d	f	h	g	a	e	b	c
f	f	d	g	h	e	a	c	b
g	g	h	d	f	c	b	a	e
h	h	g	f	d	b	c	e	a

e عنصرعینیت (identety) از Q_8 است

مثال 1.6 : Q_6:={ e,a,b,c,d,f } نظربه جدول کیلی (cayley table) ذیل یک گروپ است .

.	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

نوت: گروپ های ذیل متناهی اند:

$A^{(2)}$, $A^{(4)}$, $A^{(2,2)}$, D_4, Q_8, Q_6

$|A^{(2)}| = 2$, $|A^{(4)}| = |A^{(2,2)}| = 4$, $|Q_6| = 6$,$|D_4| = |Q_8| = 8$

تمرین 1.5 :

(a) G={ e,a,b } و GxG→ G: ٠ یك رابطه دوگانه است . جدول ذیل را طوري تکمیل نمائید که (G,.) یك گروپ شود .

.	e	a	b
e	e	a	b
a	a		e
b	b	e	

(b) G={ e,a,b,c } و GxG→ G: ٠ یك رابطه دوگانه است . جدول ذیل را طوري تکمیل نمائید که (G,.) یك گروپ شود .

.	e	a	b	c
e	e	a	b	c
a	a		e	b
b	b	e		
c	c	b		

(c) درگروپ های $A^{(2,2)}$, $A^{(4)}$, D_4 , Q_6 و Q_8 کدام ان تبدیلی نیستند

تمرین 1.6 : $(G,\oplus)$ يك گروپ داراي عنصرعينيت $e \in G$ است. ثبوت نمائيد :

$$a \in G; a \oplus a = a \Rightarrow a = e$$

تمرین 1.7: چرا $\mathbb{R}$ (اعدادحقیقی) نظربه رابطه دوگانه ذیل یک گروپ شده نمیتواند

$$\odot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$
$$(a,b) \longmapsto a \odot b = \frac{1}{2}(a + b)$$

مثال 1.7 : اگرماتریکس ها ی ذیل راداشته باشیم

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

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

$$Q: = \{\pm E , \pm I , \pm J , \pm K\}$$

البته هر ماتریکس منفی ان به شکل ذیل تعریف شده است:

$$-E = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad , \quad -I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad ,$$

$$-J = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \quad , \quad -K = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

$$. : Q \times Q \longrightarrow Q$$

$$(A,B) \longmapsto A.B$$

Q نظر به ضرب ماتریکس یک گروپ بوده که E عنصر عینیت آن است وبرای $A \in Q \setminus \{\pm E\}$ عنصر معکوس آن $-A$ ومعکوس $-E$ خود $-E$ است. مگر $(Q , .)$ گروپ تبدیلی نیست زیرا

$I.J = K \ , J.I = -K \ \Rightarrow \ I.J \neq J.I$

تمرين 1.8 : درمثال فوق ديديم كه $Q := \{\pm E , \pm I , \pm J , \pm K\}$ نظربه ضرب ماتريكس يک گروپ است. دريافت نمايد كه جدول كيلی (caley table) ان چه شكل رادارد

تمرين 1.9 : ايا $G = \{ 0,1,2 \}$ نظربه رابطه دوگانه جمع و ضرب ساختمانی گروپی دارد. اگرندارد نشان دهيد كه چرا

تمرين 1. 10 : $\mathbf{D}_6 = \{ a,b,c,x,y,z \}$ و " . " يك رابطه دوگانه بالای $\mathbf{D}_6$ است . جدول ذيل را طوري تكميل نمائيد كه $(\mathbf{D}_6 , .)$ يك گروپ شود .

.	a	b	c	x	y	z
a					c	b
b		x	z			
c		y				
x				x		
y						
z		a			x	

تمرين 1.11:

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

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

$Q_4 := \{E,A,B,C\}$

ثبوت نمايد كه Q_4 نظربه ضرب ماتريكس يک گروپ است

تعريف 1.5: $(G,.)$ يک ساختمان الجبری (algeb-struct) و $a \in G$ است.

$\tau_a : G \to G$
$x \mapsto a.x$
${}_a\tau : G \to G$
$x \mapsto x.a$

τ_a بنام right-translation و ${}_a\tau$ بنام left-translation یاد میشود

لیما 1.2: $(G,.)$ یک ساختمان الجبری است. بعداً:

(1) اگر $(G,.)$ یک گروپ باشد. درانصورت برای $\forall a \in G$ تابع τ_a یک bijective است

(2) اگر$(G,.)$ اتحادی (associativity) و τ_a برای $\forall a \in G$ یک surjective باشد. درانصورت $(G,.)$ ساختمانی گروپی دارد.

ثبوت (1)

$b \in G \Rightarrow \exists!\ x \in G\ ;\ a.x = b$ [نظر به قضیه 1.2]
$\Rightarrow \tau_a(x) = b \Rightarrow \tau_a$ surjective
$x,y \in G\ ;\ \tau_a(x) = \tau_a(y)$
$\Rightarrow a.x = a.y \Rightarrow x = y$ [نظر به قضیه 1.2]
$\Rightarrow \tau_a$ injecetiv

ثبوت شد که τ_a بیجکتیف است

ثبوت (2)

$a \in G$
$\Rightarrow \exists\ x \in G\ ;\ \tau_a(x)\ a.x = a$ [زیرا τ_a یک surjective]
از $a.x = a$ نتیجه میشود که یک عنصرعینیت e موجود است. پس
$e \in G \Rightarrow \exists\ x \in G\ ;\ \tau_a(x) = a.x = e$ [زیرا τ_a یک surjective]
از $a.x = e$ نتیجه میشود که یک معکوس برای a موجود است. پس ثبوت شد که $(G,.)$ گروپ است. لیما فوق **برای** ${}_a\tau$ نیزصدق میکند

نوت: $(G, *)$ یک گروپ است . ازلیما فوق نتیجه میشود که برای هر $a \in G$ تابع ذیل bijecktive است

$f : G \longrightarrow G$
$x \longmapsto a*x$
$g : G \to G$

$x \mapsto x*a$

بطور مثال درگروپ های $(\mathbb{Z}, +)$ و $(\mathbb{R}^*, .)$ توابع ذیل bijective اند

$$f : \mathbb{R}^* \longrightarrow \mathbb{R}^* \qquad x \longmapsto \frac{2}{3} \cdot x$$

$$f : \mathbb{Z} \longrightarrow \mathbb{Z} \qquad x \longmapsto 5 + x$$

تمرین 1.12:

$$\odot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$
$$(a,b) \longmapsto a \odot b = a + b + 3$$

ثبوت نماید که $(\mathbb{R}, \odot)$ یک گروپ است

فصل دوم

گروپ هوموورفیزم(Group Homomorphism)

تعریف 2.1 : اگر $(G,\oplus)$ و $(G_1,\odot)$ دو گروپ باشند.یک تابع $\varphi: G \longrightarrow G_1$ با خواص زیر بنام Group Homomorphism (گروپ هوموورفیزم) (G–Hom) یاد میشود.

$$\varphi\ (a \oplus b) = \varphi(a) \odot \varphi(b) \quad (\ \forall a, b \in G\ )$$

یک G-Hom اگر injective باشد. بنام Group Monomorphism (G-Monom) ، اگر surjective باشد، بنام Group Epimorphism (G-Epim) و اگر bijective باشد بنام Group Isomorphism (G-Isom) یاد میشود .

تعریف **2.2** : یک G-Hom بنام Group Endomorphism (G-Endo) یاد میشود درصورتکه $G = G_1$ باشد. یک G-Endo که درعین حال bijective باشد بنام Group Automorphism (گروپ آوتومورفیزم) (G-Auto) یاد میشود .

مثال :

$$\varphi\ : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$$
$$x \ \longmapsto \ 2x$$

مامیدانیم که سیت اعداد حقیقی $\mathbb{R}$ نظربه جمع "+" یک گروپ است .

$x,y \in \mathbb{R}$

$\varphi(x+y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y)$

دیده شد که φ یک G-Hom است . چون φ اینجکتیف و سورجیکتیف است . پس Monomorphism وEpimorphism هم است. در نتیجه یک G-Isom است.

اگر φ به شکل ذیل تعریف شود :

$$\varphi\ : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$$
$$x \ \longmapsto \ 2x$$

مامیدانیم که سیت اعداد تام ($\mathbb{Z}$) نظربه جمع "+" یک گروپ است. همچنان دیده میشود که φ انجکتیف و G-Hom است. پس یک G-Monom است. مگر φ سورجکتیف نیست . پس G-Epim شده نمی تواند .

اگر φ به شکل ذیل تعریف شود :

$$\varphi : \left(\mathbb{R}^*, .\right) \longrightarrow (\mathbb{R}^*, .)$$
$$x \longmapsto 2x$$

مامیدانیم که سیت اعداد حقیقی بدون صفر $\mathbb{R}^*$ نظربه ضرب "." یک گروپ است

$x,y \in \mathbb{R}^*$

$\varphi(x.y) = 2(x . y) = 2x.y \neq 2x .2y = \varphi(x) . \varphi(y)$

دیده شد که φ یک G-Hom نیست

اگر φ به شکل ذیل تعریف شود :

$$\varphi : \left(\mathbb{R}^*, .\right) \longrightarrow (\mathbb{R}, +)$$
$$x \longmapsto 2x$$

$x,y \in \mathbb{R}^*$

$\varphi(x.y) = 2(x . y) = 2x.y \quad \wedge \quad \varphi(x) + \varphi(y) = 2x + 2y$

$\Rightarrow \quad \varphi(x.y) \neq \varphi(x) . \varphi(y)$

درنتیجه φ یک G-Hom نیست . اگر φ به شکل ذیل تعریف شود :

$$\varphi : \left(\mathbb{R}, +\right) \longrightarrow (\mathbb{R}, +)$$
$$x \longmapsto -x$$

$x,y \in \mathbb{R}$

$\varphi(x+y) = -(x + y) = -x - y = \varphi(x) + \varphi(y)$

درنتیجه φ یک G-Hom است.

اگر φ به شکل ذیل تعریف شود :

$$\varphi : \left(\mathbb{R}^*, .\right) \longrightarrow (\mathbb{R}^*, .)$$
$$x \longmapsto -x$$

$x,y \in \mathbb{R}^*$

$\varphi(x.y) = -x.y \quad \wedge \quad \varphi(x) . \varphi(y) = (-x) . (-y) = x.y$

$\Rightarrow \quad \varphi(x.y) \neq \varphi(x) . \varphi(y)$

پس φ یک G-Hom نیست

نوت 2.1: به صورت عموم میتوان نوشت:

(a) برای هر $a \in \mathbb{R}$ تابع ذیل یک G-Isom است

$$\varphi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$$
$$x \longmapsto ax$$

(b) برای هر $m \in \mathbb{Z}$ تابع ذیل یک G-Monom است

$$\varphi : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$$
$$x \longmapsto mx$$

مثال: Exponentialfunction ذیل یک G-Isom است

$$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, .)$$
$$x \longmapsto e^x$$

: G-Hom

$x,y \in \mathbb{R}$, $\exp(x+y) = e^{x+y} = e^x . e^y = \exp(x) . \exp(y)$

ازجانب دیگردرمثال 0.4 دیدیم که exp بایجکتیف است. درنتیجه exp یک G-Isom است.

قضیه 2.1: $(G_1, \oplus)$ و $(G_2, \odot)$ دو گروپ دارای عناصر عینیت $e_1 \in G_1$ و $e_2 \in G_2$ اند و $\varphi: G_1 \longrightarrow G_2$ یک G-Hom . بعدآ خواص زیر صدق میکند:

(1) $\varphi(e_1) = e_2$

(2) $\varphi(a^{-1}) = (\varphi(a))^{-1}$

ثبوت (1): ما میدانیم که در یک گروپ تنها عنصر عینیت خاصیت $x \odot x = x$ را دارد.

$$\varphi(e_1) = \varphi(e_1 \oplus e_1)$$
$$= \varphi(e_1) \odot \varphi(e_1) \quad [\text{ G-Hom } \varphi \text{ زیرا }]$$

این نشان میدهد که $\varphi(e_1)$ عنصرعینیت از G_2 است. ما میدانیم که یک گروپ تنها یک عنصر عینیت دارد, پس $\varphi(e_1) = e_2$

ویا ثبوت بشکل ذیل

$e_2 \odot \varphi(e_1) = \varphi(e_1) = \varphi(e_1 \oplus e_1) = \varphi(e_1) \odot \varphi(e_1)$

$\Rightarrow \varphi(e_1) = e_2$ [نظر به قضیه 1.2]

ثبوت (2): برای یک $a \in G_1$

$e_2 = \varphi(e_1)$ [نظر به (1)]

$= \varphi(a \oplus a^{-1}) = \varphi(a) \odot \varphi(a^{-1})$

ازاین نتیجه میشود که $\varphi(a^{-1})$ عنصر معکوس $\varphi(a)$ است پس

قضیه 2.2 ؛ (ترکیب هوموموفیزم (Homomorphism composition))

$(G,\oplus)$ و $(G_1,\odot)$ و $(G_2,\ominus)$ سه گروپ هستند . اگر $\varphi: G \longrightarrow G_1$ و $\varphi_1: G_1 \longrightarrow G_2$ دو G-Hom باشند. درینصورت $\varphi_1 o \varphi : G \longrightarrow G_2$ هم G-Hom است.

ثبوت $a, b \in G$:

$\varphi_1 \circ \varphi\,(a \oplus b) = \varphi_1\big(\varphi(a) \odot \varphi(b)\big)$ [زیرا φ یک G-Hom]

$= \varphi_1 \circ \varphi(a) \ominus \varphi_1 \circ \varphi(b)$ [زیرا φ_1 یک G-Hom]

درنتیجه $\varphi_1 \circ \varphi$ یک G-Hom است

تعریف 2.3: $(G,\oplus)$ و $(G_1,\odot)$ گروپ اند که $e \in G$ و $e_1 \in G_1$ عناصر عینیت ان هستند و $\varphi: G \longrightarrow G_1$ یک G-Hom است. بعداً سیت زیر بنام هسته (kernal) از φ یاد میشودو ومانرابه $\ker\varphi$ نشان میدهیم

$$\operatorname{Ker}\varphi := \{a \in G \mid \varphi(a) = e_1\}$$

قضیه 2.3: $(G,\oplus)$ و$(G_1,\odot)$ دوگروپ اند که $e \in G$ و $e_1 \in G_1$ عناصر عینیت آن میباشند و $\varphi: G \longrightarrow G_1$ یک G-Hom است. بعداً:

$$\varphi \text{ injective} \Leftrightarrow \operatorname{Ker}\varphi = \{e\}$$

ثبوت: "$\Rightarrow$" باید ثبوت شود که $\operatorname{Ker}\varphi = \{e\}$ است.

اگر $\operatorname{Ker}\varphi \neq \{e\}$ باشد درآنصورت:

$\text{Ker}\varphi \neq \{e\} \Rightarrow \exists a \in G;\ \varphi(a) = e_1$

همچنان نظر به قضیه (2.1): $\varphi(e) = e_1$ است.پس

$\varphi(a) = e_1 = \varphi(e)$

$\Rightarrow a = e$ [زیرا φ یک injective]

ثبوت: " $\Leftarrow$ " برای $a, b \in G$ ما فرض میکنیم که $\varphi(a) = \varphi(b)$ است

$\varphi(a \oplus b^{-1}) = \varphi(a) \odot \varphi(b^{-1})$ [زیرا φ یک G-Hom]

$= \varphi(a) \odot \big(\varphi(b)\big)^{-1}$ [نظر به قضیه 2.1]

$= \varphi(b) \odot (\varphi(b))^{-1} = e_1$ [نظر به فرضیه]

$\Rightarrow a \oplus b^{-1} \in Ker\varphi$

$\Rightarrow a \oplus b^{-1} = e$ [زیرا $Ker\varphi = \{e\}$]

$\Rightarrow a \oplus b^{-1} \oplus b = e \oplus b = b$

$\Rightarrow a = b$

$\Rightarrow \varphi$ injective

مثال 2.1 : تابع ذیل یک G-Aut است

$\varphi: (\mathbb{C}, +) \longrightarrow (\mathbb{C}, +)$

$z = (x + iy) \mapsto \bar{z} = (x - iy)$

حل:

φ G-Hom :

$z = x + iy\ ,\ z_1 = x_1 + iy_1 \in \mathbb{C}$

$\varphi(z + z_1) = \varphi(x + iy + x_1 + iy_1) = \varphi(x + x_1 + (y + y_1)i)$

$= (x + x_1 - (y + y_1)i = (x + x_1 - iy - iy_1)$

$= x - iy + x_1 - iy_1 = \bar{z} + \bar{z}_1 = \varphi(z) + \varphi(z_1)$

φ injective :

$z = x + iy\ ,\ z_1 = x_1 + iy_1 \in \mathbb{C}$

$\varphi(z) = \varphi(x + iy) = \varphi(z_1) = \varphi(x_1 + iy_1)$

$\Rightarrow \bar{z} = x - iy = x_1 - iy_1 = \bar{z}_1 \Rightarrow x = x_1 \wedge -iy = -iy_1$

$\Rightarrow x = x_1 \wedge iy = iy_1 \Rightarrow z = x + iy = x_1 + iy_1 = z_1$

$\Rightarrow \varphi$ injective

: surjective φ

برای $z = x + iy \in \mathbb{C}$ ما z_1 را مساوی به $x - iy$ وضع مینمایم

$\varphi(z_1) = \varphi(x - iy) = x + iy = z$

چون φ یک G-Hom و بیجکتیف است. پس یک G-Aut است

$\ker\varphi = \{0\}$ است. زیرا φ یک injective و صفرعنصرعینیت از $(\mathbb{C}, +)$ است.

مثال 2.2 : ما تابع ذیل را بالاي گروپ $(A^{(2,2)}, \odot)$ تعریف مینمائیم :

$$\varphi: (A^{(2,2)}, \odot) \longrightarrow (\boldsymbol{A^{(2,2)}}, \odot)$$
$$a \longmapsto a \odot a$$

: φ G-Hom باید نشان دهیم که براي $\forall x, y \epsilon (A^{(2,2)})$ افاده ذیل صدق میکند :

$$\varphi(x \odot y) = \varphi(x) \odot \varphi(y)$$

ما میدانیم که b_1 عنصر عینیت از $A^{(2,2)}$ است ونظر به رابطه دوگانه " $\odot$" میتوان نوشت :

$z := x \odot y \in (A^{(2,2)}$

$\varphi(x \odot y) = \varphi(z) = z \odot z = b_1$

$\varphi(x) = x \odot x = b_1 \ \wedge \ \varphi(y) = y \odot y = b_1$

$\varphi(x) \odot \varphi(y) = b_1 \odot b_1 = b_1$

درنتیجه

$\varphi(x \odot y) = b_1 = \varphi(x) \odot \varphi(y)$

ازین نتیجه میشود که φ یك G-Hom است .چون تابع φ یك تابع از $A^{(2,2)}$ بالاي خودش است پس φ یك G-Endom نیز است .

:Injective براي $x, y \epsilon A^{(2,2)}$ اگر $\varphi(x) = \varphi(y)$ باشد باید ثبوت شود که $x = y$ شود یعني :

$$x, y \epsilon (A^{(2,2)}) \ ; \ \varphi(x) = \varphi(y) \Rightarrow x = y$$

$\varphi(b_3) = b_3 \odot b_3 = b_1 = b_2 \odot b_2 = \varphi(b_2)$

مگر $b_2 \neq b_3$ است . پس φ يك injective نيست .

Surjective: بايد ثبوت شود كه براي هر $y\epsilon\ A^{(2,2)}$ يك $x\epsilon\ A^{(2,2)}$ موجود باشد كه $\varphi(x) = y$ يعني :

$\forall y \in \left(A^{(2,2)}\right),\ \exists x\epsilon\ A^{(2,2)}\ ;\ \varphi(x) = y$

چون براي $b_3 \in A^{(2,2)}$ هيچ عنصر در $x\epsilon\ A^{(2,2)}$ وجود ندارد كه $\varphi(x) = b_3$ شود. پس surjective نيست. در نتيجه φ يك G-Autom هم نيست .

چون φ يک G-Hom است و b_1 عنصرعنت از $A^{(2,2)}$ است . ميخواهيم $Ker\ \varphi$ رادريافت نمايم

$Ker\ \varphi := \{a \in A^{(2,2)} \mid \varphi(a) = b_1\}$

$\forall\ a \in A^{(2,2)}\ ;\ \varphi(a) = a \odot a = b_1 \Rightarrow\ Ker\ \varphi = A^{(2,2)}$

مثال 2.3: اگر $G=\{1,-1\}$ باشد و ماميدانيم كه G نظر به ضرب يک گروپ است. تابع φ به شكل ذيل تعريف شده است:

φ: $(Q_6, *) \longrightarrow (G, .)$

$\varphi(e) = \varphi(a) = \varphi(b) = 1 \quad \wedge \quad \varphi(c) = \varphi(d) = \varphi(f) = -1$

به اسان ميتوان نشان داد كه φ يک G-Hom است. به طورمثال

$\varphi(d*f) = \varphi(b) = 1 = (-1).(-1) = \varphi(d).\ \varphi(f)$

$\ker \varphi$: چون عينيت در G عدد 1 است. پس

$ker\varphi = \{x \in Q_6 \mid \varphi(x) = 1\} = \{ e,a,b \}$

مثال 2.4 :

ما سيت $G:= \left\{A \in M(2x2, \mathbb{R}) \middle| A = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix}, xt \neq 0\right\}$ راداريم

(a) سيت G نظربه ضرب ماتريكس يک گروپ است.

(b) تابع ذيل يک G-Hom است.

$$\varphi: (G,.) \longrightarrow (\mathbb{R}^*,.)$$
$$A=\begin{pmatrix} x & y \\ 0 & t \end{pmatrix} \longmapsto xt$$

ثبوت (a)
(G,.) **ساختمانی الجبری دارد.** زیرا:

$$A = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix}, B = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$$

$$A.B = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix} . \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} xa & xb+yc \\ 0 & tc \end{pmatrix}$$

ازجانب دیگر

$xt \neq 0 \ \wedge \ ac \neq 0 \ \Rightarrow \ x \neq 0 , t \neq 0 , a \neq 0 , c \neq 0$
$\Rightarrow$ xa.tc $\neq 0$
$\Rightarrow A.B \in G$

ویابه طریقه دیگر

$xt \neq 0 \ \wedge \ ac \neq 0$
$\Longrightarrow$ det(A) $\neq 0 \ \wedge$ det(B) $\neq 0$
$\Longrightarrow$ det(A.B) = xa.tc = xt.ac $\neq 0 \Longrightarrow A.B \in G$

عنصرعینیت: ماتریکس E_2 که نظربه ضرب ماتریکس عینیت (identity) است در G شامل است
خاصیت اتحادی (associativity) نیز صدق میکند

موجودیت معکوس (inverse) **:**

$$A = \begin{pmatrix} x & y \\ 0 & t \end{pmatrix} \in G$$

$$\begin{pmatrix} x & y \\ 0 & t \end{pmatrix} \Big| \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \frac{1}{x}$$

$$\begin{pmatrix} 1 & \frac{y}{x} \\ 0 & t \end{pmatrix} \Big| \begin{pmatrix} \frac{1}{x} & 0 \\ 0 & 1 \end{pmatrix} . \frac{1}{t}$$

$$\begin{pmatrix}1 & \frac{y}{x}\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}\frac{1}{x} & 0\\ 0 & \frac{1}{t}\end{pmatrix} \quad -\frac{y}{x}\cdot$$

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}\frac{1}{x} & \frac{-y}{xt}\\ 0 & \frac{1}{t}\end{pmatrix}$$

پس $A^{-1} = \begin{pmatrix}\frac{1}{x} & \frac{-y}{xt}\\ 0 & \frac{1}{t}\end{pmatrix}$

به اسانی میتوان نشان داد که $A^{-1} \in G$ و $A \cdot A^{-1} = E_2$

ویا به شکل مختصر:

$x.t \neq 0 \implies \det(A) \neq 0 \implies A$ invertible

ثبوت (b)

$A = \begin{pmatrix}x & y\\ 0 & t\end{pmatrix}, B = \begin{pmatrix}a & b\\ 0 & c\end{pmatrix} \in G$

$\varphi(A.B) = \varphi\left(\begin{pmatrix}xa & xb+yc\\ 0 & tc\end{pmatrix}\right) = (xa)(tc) = (xt).(ac)$

$= \varphi(A).\varphi(B)$

$\ker\varphi$: چون عینیت در $\mathbb{R}^*$ عدد 1 است. پس

$$ker\varphi = \{A \in G \mid \varphi(A) = 1\} = \{A \in G \mid A = \begin{pmatrix}x & y\\ 0 & t\end{pmatrix}, xt = 1\}$$

$$= \{A \in G \mid A = \begin{pmatrix}x & y\\ 0 & t\end{pmatrix}, t = \frac{1}{x}\}$$

تقسیم بالای x درست است. زیرا x خلاف صفر است . بطورمثال

$$\begin{pmatrix}2 & y\\ 0 & \frac{1}{2}\end{pmatrix}, \begin{pmatrix}-2 & y\\ 0 & -\frac{1}{2}\end{pmatrix} \in \ker\varphi$$

چون $\{1\} \neq \ker\varphi$ است ، پس نظربه قضیه 2.3 یک اینجکتیف نیز نیست.

بطورمثال:

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}, B = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$$

φ(A) = 2 = φ(B) است، مگر A و B باهم مساوی نیستند

تمرین 2.1:

(a) ماتابع ذیل راداریم

$$\varphi: (\mathbb{C}, +) \longrightarrow (\mathbb{R}, +)$$
$$z = a+ib \longmapsto |z| = \sqrt{a^2 + b^2}$$

ایا φ یک G-Hom است.

(b) ماتابع ذیل راداریم

$$\varphi: (\mathbb{C}^*, .) \longrightarrow (\mathbb{R}^*, .)$$
$$z = a+ib \longmapsto |z| = \sqrt{a^2 + b^2}$$

ثبوت نماید که φ یک G-Hom است و $\ker\varphi$ رادریافت نماید

قضیه2.4: $(G, \oplus)$و $(G_1, \odot)$ گروپ اند که دارای عناصرعینیت $e \in G$ و $e_1 \in G_1$. اگر $\varphi: G \longrightarrow G_1$ یک G-Hom باشد، درانصورت $\varphi(G)$ و $Ker\varphi$ هم ساختمان گروپی دارند.

ثبوت: ما ثبوت مینماییم که $(Ker\varphi, \oplus)$ یک گروپ است.

$$a, b \in Ker\varphi$$
$$\Rightarrow \varphi(a \oplus b) = \varphi(a) \odot \varphi(b)$$
$$= e_1 \odot e_1 \quad [\ a, b \in Ker\varphi \quad \text{زیرا}\ ]$$
$$= e_1 \Rightarrow a \oplus b \in Ker\varphi$$

نشان داده شد که رابطه دوگانه $\oplus$ همچنان بالای $Ker\varphi$ قابل تطبیق است و $(Ker\varphi, \oplus)$ ساختمان الجبری دارد

خاصیت اتحادی: چون $Ker\varphi \subseteq G$ است و رابطه دوگانه $\oplus$ بالای $Ker\varphi$ نیز قابل تطبیق است. درنتیجه $Ker\varphi$ هم خواص اتحادی را دارد.

موجودیت عنصر خنثی:

$e \in G \Rightarrow \varphi(e) = e_1$ [نظر به قضیه 2.1]

$\Rightarrow e \in Ker\varphi$

موجودیت عنصر معکوس:

$a \in Ker\varphi \subseteq G \Rightarrow \varphi(a) = e_1$

$\Rightarrow \big(\varphi(a)\big)^{-1} = e_1$

$\Rightarrow \varphi(a^{-1}) = e_1$ [نظر به قضیه 2.1]

$\Rightarrow a^{-1} \in Ker\varphi$

ثبوت $\varphi(G)$:

رابطه دوگانه:

$a_1, b_1 \in \varphi(G) \Rightarrow \exists a, b \in G; \varphi(a) = a_1 \wedge \varphi(b) = b_1$

$\Rightarrow a_1 \odot b_1 = \varphi(a \oplus b) = \varphi(a) \odot \varphi(b)$

$\Rightarrow a_1 \odot b_1 \in \varphi(G)$

دیده شد که رابطه دوگانه $\odot$ نیز بالای $\varphi(G)$ قابل تطبیق است $(\varphi(G), \odot)$ ساختمان الجبری دارد

خاصیت اتحادی:

$a_1, b_1, c_1 \in \varphi(G)$

$\Rightarrow \exists a, b, c \in G; \varphi(a) = a_1 \wedge \varphi(b) = b_1 \wedge \varphi(c) = c_1$

$a_1 \odot (b_1 \odot c_1) = \varphi(a) \odot \big(\varphi(b) \odot \varphi(c)\big)$

$= \big(\varphi(a) \odot \varphi(b)\big) \odot \varphi(c)$

$= (a_1 \odot b_1) \odot c_1$

عنصر خنثی:

$\varphi(e) = e_1 \Rightarrow e_1 \in \varphi(G)$

عنصر معکوس:

$a_1 \in \varphi(G)$

$\Rightarrow \exists a \in G; \varphi(a) = a_1 \wedge \exists a^{-1} \in G; a \oplus a^{-1} = e$

$\Rightarrow \varphi(a) \odot \varphi(a^{-1}) = \varphi(a \oplus a^{-1}) = \varphi(e) = e_1$

$\Rightarrow a_1 . \varphi(a^{-1}) = e_1$

بنابراین عنصر معکوس از a_1 عبارت از $\varphi(a^{-1})$ است.

قضیه 2.5: $(G , \oplus)$ و $(G_1, \odot)$ و $(G_2, \ominus)$ گروپها اند بعدآ :

(1) اگر $\varphi: G \longrightarrow G_1$ یک G-Isom باشد درینصورت تابع معکوس آن $\varphi^{-1}: G_1 \longrightarrow G$ هم G-Isom است.

(2) اگر $\varphi: G \longrightarrow G_1$ و $\varphi_1: G_1 \longrightarrow G_2$ گروپ G-Isom باشند درانصورت همچنان $\varphi_1 o\varphi: G \longrightarrow G_2$ هم G-Isom است.

ثبوت(1): ما میدانیم که تابع معکوس یک تابع بایجکتیف (Bijective) بازهم بایجکتیف (Bijective) است. پس کفایت میکند ثبوت شود که φ^{-1} یک G-Hom است.

$a_1, b_1 \in G_1$

$\Rightarrow \exists a, b \in G: \varphi(a) = a_1 \ \wedge \ \varphi(b) = b_1$

$\Rightarrow \ a \ = \varphi^{-1}(a_1) \ \wedge \ \ b \ = \varphi^{-1}(b_1)$

$\varphi(a \oplus b) = \varphi(a) \odot \varphi(b) = a_1 \odot b_1$

$\Rightarrow \varphi^{-1}(a_1 \odot b_1) = \varphi^{-1}\left(\varphi(a \oplus b)\right)$

$= \varphi^{-1} o \varphi(a \oplus b) = id(a \oplus b)$

$= a \oplus b$

$= \varphi^{-1}(a_1) \oplus \varphi^{-1}(b_1)$

$\Rightarrow \varphi^{-1}$ G-Hom

بنابراین φ^{-1} یک G-Isom است.

ثبوت (2): نظر به قضیه 2.2 کفایت میکند ثبوت شود که $\varphi_1 o\varphi$ یک بایجکتیف bijective است.

: Injective

$a, b \in G, \varphi_1 o\varphi(a) = \varphi_1 o\varphi(b)$

$\Rightarrow \varphi(a) = \varphi(b)$ [زیرا φ_1 یک injective]

$\Rightarrow a = b$ [زیرا φ یک injective]

$\Rightarrow \varphi_1 o \varphi$ injective

: **Surjective**

$g_2 \in G_2$

$\Rightarrow \exists g_1 \in G_1 ; \varphi_1(g_1) = g_2 \wedge \exists g \in G; \varphi(g) = g_1$

$\Rightarrow \varphi_1\big(\varphi(g)\big) = \varphi_1(g_1) = g_2$

بنابراین $\varphi_1 o \varphi$ یک surjective است.

تمرین 2. 2: کدام یکی از توابع ذیل injective , surjective و G-Hom است و کدامی ان نیست

(a) $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$
$z \longmapsto 2z$

(b) $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$
$z \longmapsto z+1$

(c) $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}^*, .)$
$x \longmapsto x^2+1$

(d) $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{R}^*, .)$
$x \longmapsto \frac{2}{3} . (x-1)$

(e) $f : (\mathbb{R}^*, .) \longrightarrow (\mathbb{R}^*, .)$
$x \longmapsto x^2$

تمرین 2. 3 : (G,.) یک گروپ و e عنصر عینیت ان است. $a \in G$

$L_a : G \longrightarrow G$
$x \longmapsto a.x.a^{-1}$

نشان دهید که L_a یک G-Aut است و $\ker(L_a)$ را دریافت نمایید

تمرین 2. 4 : $(G, \odot)$ یک گروپ و e عنصرعینیت ان است.

$f : G \longrightarrow G$
$a \longmapsto a \odot a$

اگر f یک G-Hom باشد. ثبوت نماید که G یک گروپ تبدیلی (commutative) است

تمرین 2.5 : ایا تابع ذیل یک G-Hom است

$$f : (A^{(2,2)}, \odot) \longrightarrow (Q_4, .)$$
$$b_1 \longmapsto E , \quad b_2 \longmapsto A$$
$$b_3 \longmapsto B , \quad b_4 \longmapsto C$$

تمرین **2.6** : $\varphi : (G,.) \longrightarrow (G_1,*)$ یک G – isom است. بعدآ :

(a) G Commutative $\Leftrightarrow$ G_1 Commutative

(b) $|G| = |G_1|$

فصل سوم

گروپ فرعی (Subgroup)

تعریف 3.1: $(G,\oplus)$ یک گروپ است و $H \subseteq G$. H به نام گروپ فرعی (Subgroup) یاد میشود, وقتیکه H خودش نظر به رابطه دوگانه $\oplus$ ساختماني گروپي داشته باشد . یعني ($\oplus$, H) يك گروپ باشد .

مثال:

(a) G و {e} هر دوی آنها گروپ های فرعی ازگروپ G اند. البته e عنصر عینت است .

(b) $\mathbb{Z}$ یک گروپ فرعی از $\mathbb{Q}$ نظر به جمع "+" است.

(c) $\mathbb{Q}$ یک گروپ فرعی از $\mathbb{R}$ نظر به جمع "+" است.

(d) $\mathbb{Q}^*$ یک گروپ فرعی از $\mathbb{R}^*$ و $\mathbb{R}^*$ یک گروپ فرعی از $\mathbb{C}^*$ نظر به ضرب "." است.

(e) H={a_0,a_2} یک گروپ فرعی از $A^{(4)}$ است.

قضیه3.1: $(G,\oplus)$ یک گروپ و e عنصر عینیت از G و $H \subseteq G$. بعداً:

$$\left.\begin{array}{l}(1)\ a,b \in H, a\oplus b \in H \\ (2)\ e\in H \\ (3)\ a \in H \Rightarrow a^{-1} \in H\end{array}\right\} \Leftrightarrow (H,\oplus) \text{ یک گروپ فرعي}$$

ثبوت" ⇐ ": از اینکه H یک گروپ فرعی از G است پس (1) صدق میکند.

ثبوت (2): اگر $\tilde{e}$ عنصر عینیت از H باشد، پس:

$$\tilde{e} \in H \Rightarrow \tilde{e} \in G \ \wedge\ \tilde{e}\oplus\tilde{e} = \tilde{e}$$

این وقتی امکان دارد که $\tilde{e}$ یک عنصر عینیت از G باشد یعنی $\tilde{e} = e$.

بنابراین $e\in H$ است.

ثبوت (3):

$a \in H \Rightarrow \exists b \in H; a\oplus b = e$ [زیرا H گروپ فرعی است]

پس b باید معکوس از a (یعنی $b = a^{-1}$) باشد. درنتیجه $b = a^{-1} \in H$.

ثبوت" ⇒ **":** نظر به (2) سیت H خالی نیست, نظر به (1) رابطه دوگانه $\oplus$ صدق میکند و نظر به (2) و (3) سیت H دارای عنصر عینیت و معکوس میباشد. پس لهذا H یک گروپ فرعی ازG است.

قضیه 3.2: $(G,\oplus)$ یک گروپ ، $e \in G$ عنصرعینیت و $H \subseteq G$ است. بعداً:

$$\left.\begin{array}{l}(\text{i})\ H \neq \emptyset \\ (\text{ii})\ \forall a,b \in H, a\oplus b^{-1} \in H\end{array}\right\} \Leftrightarrow (H,\oplus) \text{ یک گروپ فرعي}$$

ثبوت" ⇐ " : واضح است که هر گروپ فرعی این خواص را دارد یعنی:

$e \in H \ \Rightarrow \ H \neq \emptyset$

$\forall a,b \in H,\ \exists\, b^{-1} \in H \ \wedge \ a\oplus b^{-1} \in H$

ثبوت" ⇒ " : نطربه قضیه 3.1 باید ثبوت شود که H خواص (1) , (2) و (3) آن قضیه را دارد.

$H \neq \emptyset \Rightarrow \exists\, a \in H \Rightarrow e = a\oplus a^{-1} \in H \Rightarrow (2)$

$a,e \in H \Rightarrow e\oplus a^{-1} \in H \Rightarrow e\oplus a^{-1} = a^{-1} \in H \Rightarrow (3)$

$a,b \in H \Rightarrow a\oplus b^{-1} \in H$ [نظر به (ii)]

چون در فوق نشان دادیم که (3) از قضیه 3.1 صدق میکند. بنابراین $b^{-1} \in H$ است.

$\Rightarrow a\oplus(b^{-1})^{-1} \in H$ [نظر به (ii)]

$\Rightarrow \ a\oplus(b^{-1})^{-1} = a\oplus b \in H \Rightarrow (1)$

مثال : درگروپ $(A^{(2,2)}, \odot)$ علاوه بر $A^{(2,2)}$ و $\{b_1\}$ سیت $H:=\{b_1, b_2\}$ نیز گروپ فرعی از $A^{(2,2)}$ است. زیرا عنصرعینیت b_1 شامل H و $b_2 \odot b_2 = b_1$

مثال: در گروپ $(D_4,.)$ علاوه بر D_4 و {e} سیت های {e,b} و $H:=\{e,a,b,c\}$ نیزگروپ های فرعی از D_4 اند .

برای اینکه ثبوت شود ، که $H:=\{e,a,b,c\}$ یک گروپ فرعی از D_4 است باید خواص (1) , (2) و (3) از قضیه 3.1 را داشته باشد .

$e \in H \Longrightarrow (2)$

نظربه جدول D_4 میتوان نوشت:

$a.a = b \in H$, $a.b = c \in H$, $a.c = e \in H$,
$b.b = e \in H, c.c = b \in H$
$\Longrightarrow (1)$

چون معکوس از a عنصر c و از c عنصر a است و b معکوس خودش است پس (3) نیز صدق میکند .در نتیجه H={e,a,b,c} یک گروپ فرعی از D_4 است .

تمرین : کدام سیت های ذیل گروپ فرعی از D_4 اند

$H_1 = \{b,f,h\}$, $H_2 = \{e ,b,d,g \}$, $H_3 = \{e , f \}$, $H_4 = \{e,b,c\}$,
$H_5 = \{e,a\}$

مثال : درگروپ $(Q_8 , .)$ علاوه بر Q_8 و {e} سیت {e,a,d,f} =:H نیز گروپ فرعی ان است زیرا :

(1) و (2) از قضیه 3.1 صدق میکنند. حالا باید نشان دهیم که برای $\forall x \in H$ معکوس آن نیز مربوط H است .

$d.f = e \implies d^{-1} = f \ \wedge \ f^{-1} = d \implies d^{-1}, f^{-1} \in H$
$a.a = e \implies a = a^{-1} \implies a^{-1} \in H$

در نتیجه H={e,a,d,f } یک گروپ فرعی از Q_8 است .

تمرین : کدام یکی ازسیت ذیل گروپ فرعی از$(\boldsymbol{Q}_8 , .)$ است

$H_1 = \{b,f,h\}$, $H_2 = \{e ,a,g,h \}$, $H_3 = \{e , f \}$, $H_4 = \{e,b,c\}$,
$H_5 = \{e,a\}$

مثال : سیت Q_1:= {E,-E,I,-I} یک گروپ فرعی از $(Q , .)$ است. زیرا ما میدانیم که E عنصرعینیت از Q است

$E \in Q_1$

ازروی جدول کیلي Q میتوان نوشت:

$E \in Q_1$, $(-E).(-E) = E$, $(-E).I = -I$, $(-E).(-I) = I$,
$I.I = -E$, $I.(-I) = E$, $(-I).(-I) = -E$

معکوس E- خود E– ، I معکوس I– و I– معکوس I است. پس :

$\forall A,B \in Q_1 \implies A.B \in Q_1 \ \wedge \ A^{-1} \in Q_1$

نظر به قضه **3.1** سیت Q_1 یک گروپ فرعي از Q است

تمرین: کدام یکی ازسیت ذیل گروپ فرعی از$(Q,.)$ است

$H_1 = \{E,-E\}$, $H_2 = \{E\ ,I,K\ \}$, $H_3 = \{-E\ ,\ -K\ \}$,
$H_4 = \{E,-E,I,-I\}$, $H_5 = \{E,K\}$

مثال:

$$H := \{a \in \mathbb{Z} \mid -6 \leq a \leq 6\} \qquad (a)$$

H یک گروپ فرعی از $(\mathbb{Z}, +)$ نیست. زیرا: $5 + 6 = 11 \notin H$

$$\mathbb{R}^+ := \{x \in \mathbb{R} \mid x > 0\} \qquad (b)$$

$\mathbb{R}^+$ گروپ فرعی (subgroup) از $(\mathbb{R}, +)$ نیست. زیرا صفر "0" که عنصرعینیت از $\mathbb{R}$ نظر به جمع "+" است در $\mathbb{R}^+$ شامل نیست.

تمرین 3.2:

(a)

$$M := \{A \in M(2x2, \mathbb{R})\};$$

$$N := \{A \in M(2x2, \mathbb{R}) \mid A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\}$$

در مثال 1.1 دیدیم که (M,+) ساختمان گروپی دارد. ثبوت نماید که N یک گروپ فرعی از (M,+) است

(b) ثبوت نماید که $\mathbb{R}^+ := \{x \in \mathbb{R} \mid x > 0\}$ یک گروپ فرعی در $(\mathbb{R}^*, .)$ است.

قضیه 3.3: $(G, \oplus)$ و $(G_1, \odot)$ دو گروپ که دارای عناصر عینیت $e \in G$ و $e_1 \in G_1$ اند. اگر $H \subseteq G$ و $H_1 \subseteq G_1$ گروپ های فرعی و $\varphi: G \longrightarrow G_1$ یک G-Hom باشد. بعداً:

(a) $\varphi^{-1}(H_1)$ یک گروپ فرعی از G است.

(b) $\varphi(H)$ یک گروپ فرعی از G_1 است.

ثبوت(a):

$\varphi(e) = e_1$ [نظر به قضیه 2.1]

$\Rightarrow \varphi^{-1}(e_1) = e \Rightarrow e \in \varphi^{-1}(H_1)$

$\Rightarrow \varphi^{-1}(H_1) \neq \phi$

نظر به قضیه (3.2) کفایت میکند ثبوت شود که برای هر $a,b \in \varphi^{-1}(H_1)$ باید همچنان $a \oplus b^{-1} \in \varphi^{-1}(H_1)$ صدق نماید

$$a,b \in \varphi^{-1}(H_1)$$
$$\Rightarrow \varphi(a),\varphi(b) \in H_1$$
$$\Rightarrow \varphi(a \oplus b^{-1}) = \varphi(a) \odot \varphi(b^{-1}) = \varphi(a) \odot \varphi(b)^{-1} \in H_1$$
$$\Rightarrow a \oplus b^{-1} \in \varphi^{-1}(H_1)$$

پس $\varphi^{-1}(H_1)$ يك گروپ فرعي از G است .

ثبوت(b):

$$\varphi(e) = e_1 \in \varphi(H) \Rightarrow \varphi(H) \neq \phi$$
$$a_1, b_1 \in \varphi(H) \Rightarrow \exists\, a,b \in H;\ \varphi(a) = a_1 \wedge \varphi(b) = b_1$$
$$\Rightarrow \varphi(a \oplus b^{-1}) = \varphi(a) \odot \varphi(b^{-1}) = \varphi(a) \odot \varphi(b)^{-1}$$
$$= a_1 \odot {b_1}^{-1} \in \varphi(H)$$

لهذا $\varphi(H)$ نظر به قضیه 3.2 یک گروپ فرعی است.

مثال: بالای گروپ فرعی $H=\{a_0,a_2\} \subseteq A^{(4)}$ و گروپ $A^{(2)}$ تابع ذیل را تعریف مینماییم

$$f : H \to A^{(2)}$$

$$x \to \begin{bmatrix} e & if & x = a_0 \\ a & if & x = a_2 \end{bmatrix}$$

f یک G-Isom است. زیرا:

$$f(a_0 \oplus a_0) = f(a_0) = e = e \odot e = f(a_0) \odot f(a_0)$$
$$f(a_0 \oplus a_2) = f(a_2) = a = e \odot a = f(a_0) \odot f(a_2)$$
$$f(a_2 \oplus a_2) = f(a_0) = e = a \odot a = f(a_2) \odot f(a_2)$$

همچنان دیده میشود که f یک بایجکتیف bijective است. در نتیجه f یک G-Isom است.

تعریف 3.2 : یک گروپ $(G,.)$ که تمام عناصر آن مولد (generator) تنها یک عنصر ان باشد بنام گروپ دورانی (cyclic group) یاد میشود. به عباره

دیگراگر یک a∈ G موجود باشد که تمامی عناصراز G دراثرتطبیق رابطه دوگانه "„ بالای a به دست بیاید. یعنی:

$\forall b \in G$, $\exists i \in \mathbb{N}$; a.a.....a (دفعه - i) = a^i = b

اگر a مولد (generator) گروپ G باشد، درانصورت ما آن را به شکل $\langle a \rangle = G$ نشان میدهیم.

مثال: $\langle 1 \rangle = (\mathbb{Z}, +)$ گروپ دورانی است. زیرا: $\mathbb{Z} = \{n.1 | n \in \mathbb{Z}\}$

بطورمثال 5=5.1=1+1+1+1+1 و -5=-5.1=-(1+1+1+1+1)

همچنان$\langle -1 \rangle = (\mathbb{Z}, +)$ یک گروپ دورانی است. زیرا:

$$\mathbb{Z} = \{n.(-1) | n \in \mathbb{Z}\}$$

مثال:-گروپ$A^{(4)}$ یک گروپ دورانی است. زیرا:

$\langle a_1 \rangle = \left(A^{(4)}, \oplus\right)$

$a_1{}^1 = a_1$, $a_1{}^2 = a_1 \oplus a_1 = a_2$,

$a_1{}^3 = a_1 \oplus a_1 \oplus a_1 = a_2 \oplus a_1 = a_3$,

$a_1{}^4 = a_1 \oplus a_1 \oplus a_1 \oplus a_1 = a_3 \oplus a_1 = a_0$

همچنان $(A^4, \oplus) =< a_3 >$ است. پس لهذا دیده میشود که تنها یک عنصر متناهی نه، بلکه عناصر دیگر هم میتوانند مولد همان گروپ شوند.

$A^{(2)}$ نیز یک گروپ دورانی (cyclic group) است.

مگر $A^{(2,2)}$ یک گروپ دورانی نیست، زیرا:

$\forall b \in A^{(2,2)} \Rightarrow b^2 = b_1 \Rightarrow < b > = \{b, b_1\}$

یعنی هر عنصر b فقط مولد $\{b, b_1\}$ است. به طور مثال $< b_2 >= \{b, b_1\}$

در نتیجه هیچ عنصر در $A^{(2,2)}$ وجود ندارد که مولد گروپ $A^{(2,2)}$ باشند.

نوت : میتواند دو عنصر یك گروپ مولد آن باشد . بطور مثال در گروپ $A^{(2,2)}$.

$<b_2, b_3 > = A^{(2,2)}$

$b_1 = b_2 \odot b_2 \ \wedge \ b_4 = b_2 \odot b_3$

همچنان $< b_3, b_4 >$ و $< b_2, b_4 >$ مولد گروپ $A^{(2,2)}$ هستند .

نوت: ماميتوانيم گروپ دورانی متناهی (G,.) را که G = <a> و e عنصرعینیت ان است به شکل ذیل نشان دهیم

$$G = \{ a, a^2, a^3, \ldots\ldots, a^n = e \}$$

مثال: ماگروپ دورانی متناهی (G,.) را که G = <a> و e عصنرعینیت ان است به شکل ذیل داریم

$$G = \{ a, a^2, a^3, a^4, a^5, a^6 = e \}$$

یکی از گروپ های فرعی ان $H = \{a^2, a^4, a^6 = e\}$ است. زیرا:

$a^2 . a^2 = a^4$, $a^2 . a^4 = a^6 = e$,

$a^4 . a^4 = a^8 = a^2 . a^6 = a^2 . e = a^2$

تمرین 3.3:

(a) در مثال فوق دیگرعناصرمولد وگروپ های فرعی در G کدام اند

(b)

$H:=\{e,a,b,c\}$, $W:=\{e,b,f,h\} \subseteq D_4$

ماميدانيم كه H و W گروپ های فرعي در D_4 اند. معلوم نماید که کدام ان دوراني نيست.

تمرین3.4 : ماگروپ دورانی متناهی (G,.) را که G = <a> و e عصنر عینیت ان است به شکل ذیل داریم. گروپ های فرعی (subgroups) انرا دریافت نماید

(a) $G = \{ a, a^2, a^3, \ldots, a^9, a^{10}, a^{11} = e \}$

(b) $G = \{ a, a^2, a^3, \ldots, a^{14}, a^{15}, a^{16} = e \}$

تعریف 3.3: $X \neq \emptyset$ یک سیت است. تابع $f: X \to X$ بنام پرموتیشن (Permutation) یاد میشود، درصورتکه f بایجکتیف (Bijective) باشد. ما تمامی پرموتیشنهای بالای X را به S(X) نشان میدهیم یعنی:

$$S(X) := \{f: X \to X \mid f \quad bijective\}$$

مثال : X={1,2} بالای X تنها دو پرموتیشن ذیل وجود دارد:

$f_0: X \to X$ $\quad$ $f_1: X \longrightarrow X$

$1 \longmapsto 1$ $\quad$ $1 \longmapsto 2$

$2 \longmapsto 2$ $\quad$ $2 \longmapsto 1$

تعداد پرموتیشن بالای یک سیت, تابع عناصر آن سیت میباشد. به طور مثال برای X={a,b,c} تعداد پرموتیشن آن به شش میرسد. به صورت عموم اگر X دارای n عنصر باشد در آن صورت تعداد پرموتیشن آن به $n!$ (factorial) میرسد . یعني

$|X| = n \Rightarrow |S(X)| = n!$ $\quad (n! = 1.2.3 \ldots . n)$

قضیه 3.4: $X \neq \emptyset$ یک سیت است بعداً S(x) نظر به ترکیب تابع "map-composition" ساختمان گروپی دارد.

ثبوت:

رابطه دوگانه (binary operation) : باید ثبوت شود که رابطه ذیل بالای S(X) قابل تطبیق است.

$$\circ : S(X) \times S(X) \longrightarrow S(X)$$

$$(f,g) \quad \longmapsto f \circ g$$

این واضح است زیرا اگر دو تابع بایجکتیف باشند ، درانصورت ترکیب آنها نیز بایجکتیف میباشد.

عنصر عینیت (Identity) : تابع id عنصر عینیت آن است زیرا:

$(id \circ f)(x) = id \circ \big(f(x)\big) = f(x) \Rightarrow id \circ f = f$

خاصیت اتحادی (Associative) : این هم نظر به تعریف ترکیب تابع این واضح است.

عنصر معکوس (Inverse) :

$f \in S(X) \Rightarrow f \ \ bijective$

$\Rightarrow f^{-1} \ \ bijective$

$\Rightarrow f^{-1} \in S(X)$

$(f^{-1} \circ f)(x) = x = id(x) \Rightarrow f^{-1} \circ f = id$

نوت3.1 : گروپ S(X) برای $|X| > 2$ تبادلوی نیست. به طورمثال برای X={1,2,3}

$$f_1 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad f_2 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

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

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

دیده میشود که $f_2 \circ f_1 \neq f_1 \circ f_2$ است.

یادداشت : اگر X={1 ,2,3,……n} باشد در اینصورت گروپ S(X) را به S_n نشان میدهند وبنام (symmetric group) n درجه ئي (degree) یاد میشود .

تعریف 3.4 : $a,b \in \mathbb{Z}$. مامیگوئیم که b بر a قابل تقسیم (a divided b) است وقتیکه یک عدد $c \in \mathbb{Z}$ موجود باشد که b = a.c شود وما آن را به a|b نشان میدهیم .

قضیه 3.5 : (division algorithm) $a,b \in \mathbb{z}$ و $b \neq 0$, بعدآ فقط تنها یک $r \in \mathbb{z}$ و یک $q \in \mathbb{z}$ باخواص ذیل موجود است:

$$a = q.b + r \qquad 0 \leq r < |b|$$

q بنام حاصل تقسیم (the quotient) و r بنام (the remainder) باقیمانده یاد میشود .

ثبوت : ما سیت H راطوری ذیل تعریف می نمایم

$$H:=\{ a - bq \mid q \in \mathbb{z} \; ; a - bq \geq 0\}$$

(a) $H \neq \emptyset$:

ما برای b دو حالت را در نظر میگیریم .

حالت اول : برای b > 0 میتوان q را $q \leq \frac{a}{b}$ انتخاب نمود درینصورت:

$$q \leq \frac{a}{b} \Rightarrow q.b \leq a \Rightarrow q.b - a \leq 0 \Rightarrow a - q.b \geq 0$$

حالت دوم : برای b < 0 میتوان q را $q \geq \frac{a}{b}$ انتخاب نمود درینصورت

$$q \geq \frac{a}{b} \Rightarrow q.b \leq a \Rightarrow a - q.b \geq 0$$

دیده شد که در هردو حالت یک عدد q پیدا میشود که $a\text{-}q.b \in H$ باشد .

ما خورد ترین عنصر H را به r نشان میدهیم

$$r \in H \Rightarrow \exists\, q \in \mathbb{z} \; ; r = a - b.q \;\wedge\; r \geq 0$$

$\Rightarrow \quad a = b.q+r$

(b) $r<|b|$:

اگر $r < |b|$ نباشد پس باید $r \geq |b|$ باشد. درانصورت $r \geq b$ است .
چون $b \neq 0$ است ،پس باید $b > 0$ ویا $b < 0$ باشد
حالت $b > 0$:

$b > 0 \quad \wedge \quad r \geq b \Rightarrow r - b \geq 0 \wedge r - b \leq r$
$\Rightarrow \quad a - b(q+1) = r - b \geq 0$
$\Rightarrow r - b \in H$

حالت $b < 0$:

$b < 0 \quad \wedge \quad r \geq b \Rightarrow r + b \geq 0 \wedge r + b \leq r$
$\Rightarrow \quad a-b(q-1) = r + b \geq 0$
$\Rightarrow r + b \in H$

در هر دو حالت دیده شد که خورد ترین عنصر از r موجود است. مگر این در تضاد به آن است که ما r را کوچکترین عنصر در H انتخاب نمودیم . پس لهذا باید $r < |b|$ باشد
حالا ثبوت مینمائیم که فقط تنها یک q ویک r به آن خواص موجود است .
ما فرض می نمایم که q_1 و r_1 نیز آن خواص را دارند .یعنی

$q.b + r = a = q_1.b + r_1 \Rightarrow q.b - q_1.b = r - r_1$
$\Rightarrow b.(q - q_1) = r - r_1$
$\Rightarrow |b|\,|q - q_1| = |r - r_1|$

اگر $q \neq q_1$ باشد درآنصورت $|r_1 - r| \geq |b|$ میشود. مگر این در تضاد به آن است که $r_1, r < |b|$ انتخاب شده بودند. پس لهذا باید $q = q_1$ و $r = r_1$ باشد .

مثال:

$a = 55 , b = 24 \Rightarrow \quad 55 = 2.24 + 7$
$a = -55 , b = 24 \Rightarrow -55 = (-3).24 + 17$
$a = -55 , b = -24 \Rightarrow -55 = 3.(-24) + 17$

لیما 3.2 :

(a) برای هر $m \in \mathbb{N}$ سیت $m\mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}$ یك گروپ فرعي از $(\mathbb{Z}, +)$ است .

(b) تقاطع گروپ های فرعي بازهم یک گروپ فرعي است
ثبوت(a): نظر به قضیه 3.2 کفایت میکند که ثبوت شود

1. $m\mathbb{Z} \neq \emptyset$
2. $\forall\, a, b \epsilon m\mathbb{Z}\,, a - b \epsilon m\mathbb{Z}$

حالت اول : m=0
در این صورت $m\mathbb{Z} = \{0\}$ میشود و {0} یك گروپ فرعي از $(\mathbb{Z}, +)$ است .
حالت دوم : m≠ 0

$$0 \epsilon \mathbb{Z} \Rightarrow m.0 = 0 \,\epsilon\, m\mathbb{Z} \Rightarrow m\mathbb{Z} \neq \emptyset \Rightarrow (1)$$

$$a,b \epsilon\, m\mathbb{Z} \Rightarrow \exists\, a_1, b_1 \,\epsilon\mathbb{Z}\,; a = ma_1 \wedge b = mb_1$$
$$\Rightarrow a - b = ma_1 - mb_1 = m(a_1 - b_1)$$
$$\Rightarrow a - b \,\epsilon\, m\mathbb{Z} \quad [a_1 - b_1 \epsilon\, \mathbb{Z} \text{ زیـرا است}]$$
$$\Rightarrow (2)$$

ثبوت نوع دیگر:
به اساس نوت 2.1 تابع ذیل یک G-Hom است

$$f: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$$
$$z \longmapsto mz$$

$f(\mathbb{Z}) = m\mathbb{Z}$ نظر به قضیه 3.3 یک گروپ فرعي از $(\mathbb{Z}, +)$ است.
ثبوت (b): اگرما یک گروپ $(G, .)$ با عنصرعینیت e داشته باشیم و $I := \{1,2, \ldots, n\}$ گروپ های فرعی در G باشد . H_i $(i \epsilon I)$ تقاطع انرا به H نشان دهیم. یعنی

$$H := \cap_{i \epsilon I}\, H_i$$

حالا میخواهیم ثبوت نمایم که H یک گروپ فرعی در G است .

$$e \epsilon\, H_i \quad (\forall\, i \,\epsilon I) \Rightarrow e \,\epsilon\, H$$
$$a,b \,\epsilon\, H \Rightarrow a,b \,\epsilon\, H_i \quad (\forall\, i \,\epsilon I)$$
$$\Rightarrow a.b \,\epsilon\, H_i \quad (\forall\, i \,\epsilon I) \quad [\text{زیرا } H_i \text{ فرعی گروپ}]$$
$$\Rightarrow a.b \,\epsilon\, H$$
$$a \,\epsilon\, H \Rightarrow a \,\epsilon\, H_i \quad (\forall\, i \,\epsilon I) \Rightarrow a^{-1} \,\epsilon\, H_i \quad (\forall\, i \,\epsilon I)$$
$$\Rightarrow a^{-1} \,\epsilon\, H$$

در نتیجه H نظر به قضیه 3.1 یک فرعی گروپ در G است.

مثال: نظر به لیما **3.2** میدانیم که $5\mathbb{Z} = \{ 5z \mid z\epsilon\ \mathbb{Z} \}$ یک گروپ فرعی در $(\mathbb{Z}, +)$ است. حالا میخواهیم که بااستفاده از قضیه 3.2 گروپ فرعی بودن انرا ثبوت نمایم

$5.1\ \epsilon\ 5\mathbb{Z} \Rightarrow 5\mathbb{Z} \neq \emptyset$

$a,b\epsilon\ 5\mathbb{Z} \Rightarrow \exists\ a_1, b_1\ \epsilon\mathbb{Z}\ ; a = 5a_1\ \wedge\ b = 5b_1$

$\Rightarrow a - b = 5a_1 - 5b_1 = 5(a_1 - b_1)$

$\Rightarrow a - b\ \epsilon\ 5\mathbb{Z}$ [زیرا $a_1 - b_1\epsilon\ \mathbb{Z}$ است]

درنتیجه $5\mathbb{Z}$ گروپ فرعی در $\mathbb{Z}$ است.

تمرین 3.5: با استفاده از قضیه 3.2 ثبوت نماید که $11\mathbb{Z}$ و $6\mathbb{Z}$ گروپ های فرعی در$(+, \mathbb{Z})$ اند

قضیه 3.6: هر گروپ فرعي H از $(\mathbb{Z}, +)$ شکل $H = n\mathbb{Z}$ را دارد.
در اینجا $n\epsilon\mathbb{N}$ بوده و مساوي به صفر ویا خورد ترین عدد طبیعي در H است .

ثبوت:

حالت اول : $H=\{0\}$

$H=\{0\} \Rightarrow n = 0\ \wedge\ H = \{0.a | a\epsilon\mathbb{Z}\} = 0.\mathbb{Z}$

حالت دوم : $H \neq \{0\}$

چون H يك گروپ فرعي از $\mathbb{Z}$ است پس داراي عناصر طبيعي نيز ميباشد وما فرض ميكنيم كه خورد ترين عدد طبيعي در H عدد n است

$m\epsilon H \Rightarrow m\epsilon\mathbb{Z}$

$\Rightarrow \exists\ q, r\ \epsilon\mathbb{Z}\ ; m = nq + r \quad 0 \leq r < n$ [division algorithm]

$\Rightarrow m - nq = r$

از جانب ديگر:

$m, n\ \epsilon H \Rightarrow r = m - nq\ \epsilon H$

چون n خورد ترين عدد طبيعي در H بود پس بايد r = 0 باشد .

$\Rightarrow m = nq\ \epsilon H \Rightarrow H = n\mathbb{Z}$

تعريف 3.5 : يک عدد $c\in\ \mathbb{Z}$ بنام قاسم مشترک (commen divisor) اعدادی $a_i \in \mathbb{Z}$ (i=1,….,n) يادميشود. در صورتيكه تمامی a_i بالايی c قابل تقسيم باشند. يعنی

$c \mid a_i$ (i= 1,2,……..,n)

تعریف 3.6: اگر $a_1,a_2,\dots,a_n \in \mathbb{Z}$. قاسم های $d, d_1,d_2,\dots,d_k$ مشترک از $a_i \in \mathbb{Z}$ $(i=1,2,\dots,n)$ باشند و $d_i \mid d$ $(i=1,2,\dots,k)$ صدق کند .در آنصورت d بنام greatest commen divisor (بزرگترین قاسم مشترک) از اعداد $a_1,a_2,\dots,an$ یاد میشود وما آن را به $d=gcd(a_1,a_2,\dots,an)$ نشان میدهیم .

قضیه 3.7 : (Euclidean Algorithm)

$a_1,a_2 \in \mathbb{Z}$, $a_2 \geq 1$, $a_1 \neq 0$, و اعداد $a_3,a_4,\dots\dots \in \mathbb{Z}$ باخواص ذیل در اثر استفاده چندین بار از Division Algorithm بدست آورده شده اند .

$$
\begin{aligned}
a_1 &= q_1a_2+a_3 && q_1 \in \mathbb{Z}\ ,\ 0 \leq a_3 < a_2\\
a_2 &= q_2a_3+a_4 && q_2 \in \mathbb{Z}\ ,\ 0 \leq a_4 < a_3\\
&\vdots && \vdots \qquad (*)\\
a_{n-4} &= q_{n-4}\,a_{n-3}+a_{n-2} && q_{n-4} \in \mathbb{Z}\ ,\ 0 \leq a_{n-2} < a_{n-3}\\
a_{n-3} &= q_{n-3}\,a_{n-2}+a_{n-1} && q_{n-3} \in \mathbb{Z}\ ,\ 0 \leq a_{n-1} < a_{n-2}\\
a_{n-2} &= q_{n-2}\,a_{n-1}+a_n && q_{n-2} \in \mathbb{Z}\ ,\ 0 \leq a_n < a_{n-1}\\
a_{n-1} &= q_{n-1}\,a_n+a_{n+1} && q_{n-1} \in \mathbb{Z}\ ,\ 0 = a_{n+1}
\end{aligned}
$$

بصورت عموم میتوان نوشت:

$$a_i = q_i . a_{i+1} + a_{i+2}\ , \qquad q_i \in \mathbb{Z}, 0 \leq q_{i+2} < q_{i+1}$$

بعداً :

$$\exists\, n \in \mathbb{N}\ , a_n \neq 0 \ \wedge\ a_{n+1} = 0 \ \wedge\ a_n = gcd\,(a_1, a_2)$$

ثبوت :

$$a_2 > a_3 > \dots > 0 \quad \Rightarrow \quad \exists\, n \in \mathbb{N};\ a_n \neq 0 \ \wedge\ a_{n+1} = 0$$

اگر ما حالا معادلات فوق از پایان به طرف بالا تحت مطالعه قرار دهیم ، دیده میشود که :

$$a_{n-1} = q_{n-1}\,a_n + a_{n+1} = q_{n-1}\,a_n + 0 \Rightarrow a_n \mid a_{n-1}$$

$$a_{n-2} = q_{n-2}\,a_{n-1} + a_n \ \wedge\ a_n \mid q_{n-2}\,a_{n-1}\ [\ a_n \mid a_{n-1}\ \text{زیـر ا}\ ]\ \wedge\ a_n \mid a_n$$

$$\Rightarrow \quad a_n \mid a_{n-2}$$

به همین ترتیب اگر به پیش برویم بالاخره میتوان نوشت :

$a_n \mid a_{n-1} \Rightarrow a_n \mid a_{n-2} \Rightarrow \ldots \Rightarrow a_n \mid a_2 \ \wedge \ a_n \mid a_1$

در نتیجه a_n قاسم مشترک a_1 و a_2 است .
فرض کنیم که t نیز یک قاسم مشترک از a_1 و a_2 است حالا ما معادلات فوق را از بالا به طرف پائین مورد مطالعه قرار میدهیم .

$t \mid a_1, a_2$

$a_1 = q_1 a_2 + a_3 \Rightarrow a_3 = a_1 - q_1 a_2$

$\Rightarrow t \mid a_3$ [زیرا $t \mid a_2 \wedge t \mid a_1$]

اگر ما به همین شکل ادامه بدهیم بالاخره بدست میآوریم :

$t \mid a_1, a_2 \Rightarrow t \mid a_3 \Rightarrow \ldots\ldots \Rightarrow t \mid a_{n-1} \Rightarrow t \mid a_n$

از این نتیجه میشود که a_n بالای t قابل تقسیم است پس a_n بزرگترین قاسم مشترک از a_1, a_2 است. یعنی $a_n = \gcd(a_1, a_2)$
بعد ازاینکه ما به کمک algorithm euclidean قاسم مشترک a_n را از a_1, a_2 یافتیم ، میتوان با استفاده از معادلات (*) اعداد $r,s \in \mathbb{Z}$ رادریافت نمایم که معادله ذیل راصدق کند

$a_n = ra_1 + sa_2$

$a_{n-2} = q_{n-2} . a_{n-1} + a_n \Rightarrow a_n = a_{n-2} - q_{n-2} a_{n-1}$

از جانب دیگر

$a_{n-3} = q_{n-3} . a_{n-2} + a_{n-1} \Rightarrow a_{n-1} = a_{n-3} - q_{n-3} . a_{n-2}$

حالا به جای a_{n-1} قیمت آنرا میگذاریم

$a_n = a_{n-2} - q_{n-2} a_{n-1} = a_{n-2} - q_{n-2} (a_{n-3} - q_{n-3} a_{n-2})$

$a_{n-4} = q_{n-4} . a_{n-3} + a_{n-2} \Rightarrow a_{n-2} = a_{n-4} - q_{n-4} . a_{n-3}$

حالا به جای a_{n-2} قیمت آنرا میگذاریم

$a_n = a_{n-2} - q_{n-2} (a_{n-3} - q_{n-3} a_{n-2})$

$= (a_{n-4} - q_{n-4} . a_{n-3}) - q_{n-2} (a_{n-3} - q_{n-3} (a_{n-4} - q_{n-4} . a_{n-3}))$

اگر ما به همین طریق به پیش برویم بالاخره درمعادله فوق فقط a_1 و a_2 باقی میمانند، که ضریب a_1 عدد r و ضریب a_2 عدد s است. پس:

$a_n = a_{n-2} - q_{n-2} (a_{n-3} - q_{n-3} . a_{n-2})$

$= (a_{n-4} - q_{n-4} . a_{n-3}) - q_{n-2} (a_{n-3} - q_{n-3} (a_{n-4} - q_{n-4} . a_{n-3}))$

$= \ldots\ldots\ldots = ra_1 + sa_2$

یعنی:

$gcd(a_1, a_2) = ra_1 + sa_2$

مثال3.1 : مامیخواهیم اعداد r و s را دریافت نمایم که رابطه ذیل صدق نماید:

$gcd(9692,360) = r.9692 + s.360$

حل:

$9692 = 26 . 360 + 332$
$360 = 1 . 332 + 28$
$332 = 11 . 28 + 24$
$28 = 1 . 24 + 4$
$24 = 6.4 + 0$

$4 = 28 - 1 . 24$
$= 28\text{-}1(332\text{-}11.28)$
$= 12.28 - 1.332$
$= 12. (360\text{-}1 .332) \text{-}1 .332$
$= 12.360 - 13.332$
$= 12 . 360 - 13 .(9692\text{-}26.360)$
$= 12.360 + 13.26(360) - 13.9692$
$= 350 . 360 - 13 . 96\ 92$

دیده میشود که

$gcd (96\ 92 , 360) = 4 = (-13) . 96\ 96 + 350 .360$

مثال: میخواهیم $r,s \in \mathbb{Z}$ رادریافت نمایم که رابطه ذیل صدق نماید:

$gcd (-65,25) = r.(-65) + s25$

حل:

$-65 = -3.25 + 10$
$25 = 2.10 + 5$
$10 = 2.5 + 0$

$5 = 25 - 2.10$
$= 25 \text{-}2(-65 + 3.25)$
$= 25 + (-2).(-65) \text{ - } 6.25$
$= (-2).(-65) + (-5).25$

$r = -2 , s = -5 , gcd(-65,25) = 5 = \textbf{-2}.(-65) + -5.25$

تمرین 3.6: $r,s \in \mathbb{Z}$ راطوری دریافت نماید که روابط ذیل صدق نمایند

(a) $gcd(150,40) = r.150 + s.40$
(b) $gcd(170,30) = r.170 + s.30$
(c) $gcd(2615,315) = r.2615 + s.315$

(d) gcd(-60,36)= r . (-60)+s.36

یادداشت : اگر ما سه عدد $a, b, c \in \mathbb{Z}$ داشته باشیم در انصورت بزرگترین قاسم مشترک (gcd) آن طوری بدست میآید :

$$gcd(a,b,c) = gcd(gcd(a,b),c) = gcd\,(a, gcd(b,c))$$

اگر ما به تعداد زیاد اعداد داشته باشیم میتوان بزرگترین قاسم مشترک شان را به همین ترتیب دریافت نمود

مثال 3.2: میخواهیم gcd(30,66,93) را پیدا کنیم .

$$\gcd(30, 66, 93) = \gcd(\gcd(30,66),93)$$

$$66 = 2 .30 + 6$$

$$30 = 5 \ . \ 6 + 0$$

دریافت نمودیم که gcd(30,66)=6

$$93 = 15 .6 + 3$$

$$6 = 2.3 + 0$$

دیده میشود که gcd(6 , 93)=3 پس:

$$\gcd(30,66,93) = \gcd(\gcd(30,66) ,93)$$

$$= \gcd(6,93)=3$$

مثال 3.3: میخواهیم gcd(36,60,150) را دریافت نمایم .

: gcd(36,60)

60 = 1.36+24

36 = 1.24+12

24 = 2.12+0

پس gcd(36, 60)= 12 است

gcd(12,150)=6 است: زیرا :

$$150 = 12.12 + 6$$

$$12 = 2.6 + 0$$

$$\gcd(36,60,150) = \gcd\,(\gcd(36,60), 150) = \gcd(12,150) = 6$$

لیما 3.3: $a, b, c \in \mathbb{Z}$. بعداً :

(a) $a \mid b.c \ \wedge gcd(a,b) = 1 \Longrightarrow a \mid c$

(b) $a \mid c \ \wedge \ b \mid c \ \wedge gcd(a,b) = 1 \Longrightarrow a.b \mid c$

(c) $gcd(a,c) = 1 \ \wedge gcd(b,c) = 1 \Longrightarrow gcd(a.b,c) = 1$

(d) P prime $\wedge$ p | a.b $\Longrightarrow$ p | a $\vee$ p | b

ثبوت (a):

$$gcd(a,b) = 1 \Longrightarrow \exists\, r,s \in \mathbb{Z}\,; ra + sb = 1$$
$$\Longrightarrow c.1 = rac + sbc$$
$$a \mid b.c \wedge\ a \mid a.c\ \Longrightarrow a \mid\ rac + sbc \Longrightarrow a \mid c$$

ثبوت (b):

$$gcd(a,b) = 1 \Longrightarrow \exists\, r,s \in \mathbb{Z}\,; 1 = ra + sb$$
$$\Longrightarrow c = rac + sbc$$
$$a \mid c\ \wedge\ b \mid c\ \Longrightarrow ab \mid rac\ \wedge ab \mid abc \Longrightarrow ab \mid c$$

ثبوت (c) :

$$gcd(a,c) = 1 \Longrightarrow\ r_1, s_1 \in \mathbb{Z};\ r_1 a + s_1 c = 1$$
$$gcd(b,c) = 1 \Longrightarrow\ \exists\, r_2 s_2 \in \mathbb{Z}\,; r_2 b + s_2 c = 1$$

معادلات فوق را باهم ضرب میکنیم :

$$r_1 r_2 ab + r_2 s_1 bc + r_1 s_2 ac + s_1 s_2 cc = 1$$
$$\Longrightarrow r_1 r_2 ab + (r_2\, s_1 b + r_1 s_2 a + s_1\, s_2 c).c = 1$$

اگرما m و n را طوری وضع نمایم

$$m := r_1 r_2\ , n := r_2 s_1 b + r_1 s_2 a + s_1 s_2\ \in \mathbb{Z}$$
$$\Longrightarrow m(ab) + nc = 1\ \Longrightarrow gcd(ab,c) = 1$$

ثبوت (d) : مافرض میکنیم که a بالای p قابل تقسیم نیست. یعنی p ł a

P ł a $\Longrightarrow$ gcd(p,a) = 1 $\Longrightarrow\ \exists\, r,s \in \mathbb{Z}$; r.p + s.a = 1

$\Longrightarrow$ b. r.p + b.s.a = b

$$p \mid \text{br}p\ \wedge\ p \mid bsa\ \Longrightarrow\ p \mid b$$

مثال:

(a)

a = 7 , b = 11 , c = 84

$$a = 7 \mid b.c = 924\ \wedge\ gcd(a,b) = \text{gcd}\,(7{,}11) = 1$$

$$\Longrightarrow\ a = 7 \mid c = 84$$ [نظر به لیما 3.3 (a)]

(b)

a = 7 , b = 11 , c = 385

$a = 7 \mid c = 385 \wedge\ b = 11 \mid c = 385\ \wedge$
$\gcd(a, b) = \gcd(7,11) = 1$
$\Longrightarrow a.b = 77 \mid c = 385$ [نظر به لیما 3.3 (b)]

(c)

a = 7 , b = 11 , c = 15
$gcd(a, c) = \gcd(7,15) = 1\ \wedge gcd(b, c) = \gcd(11,15) = 1$

$\Longrightarrow gcd(a.b, c) = \gcd(7.11,15) = 1$ [نظر به لیما 3.3 (c)]

تعریف 3.7 : $d \in \mathbb{Z}$ بنام Lcm:= Least Commen Multiple
(کوچکترین مضرب مشترک) **از** اعداد $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ یاد میشود درصورتکه:

(i) $a_i \mid d \quad \forall\ i \epsilon \{1,2,.....,n\}$

(ii) $a_i \mid d' \quad \forall\ i \epsilon \{1,2,.....,n\} \Rightarrow d \mid d'$

برای دریافت Lcm دوطریقه ذیل موجود است:

اول: دربین gcd و Lcm رابطه ذیل موجود است:

$m, n \in \mathbb{Z}$
$\gcd(m, n) . \text{Lcm}(m, n) = |m. n|$

یعنی میتوانیم Lcm ازراه gcd بدست بیاوریم

دوهم: اعداد داده شده رابه فکتورهای اولیه تجزیه میشود. بعدآ ان اعددیکه درهمه شامل وبلندترین طاقت را داشته باشد، انتخاب مینمایم وبه فکتورهای متباقی صرب میکنیم

مثال : میخواهیم Lcm(36,15) رادریافت نمایم

اول: ازطریقه gcd

$m = 36\ , n = 15$
$36 = 2.15 + 6$
$15 = 2.6 + 3$
$6 = 2.3 + 0$
$\gcd(36,15) = 3$
$\gcd(36,15) . \text{Lcm}(36,15) = |36.15|$

$$\Longrightarrow \text{Lcm}(36,15) = \frac{540}{\gcd(36,15)} = \frac{540}{3} = 180$$

دوهم: ازطریقه تجزیه فکتوری

$36 = 2.2.3.3$

$15 = 3.5$

چون 3 درهردوشامل است ، پس 3^2 راانتخاب نموده وبه متباقی اعداد ضرب میشود. یعنی:

$\text{Lcm}(36,15) = 2.2.3.3.5 = 180$

مثال : میخواهیم Lcm(72,108) رادریافت نمایم

$72 = 2^3 . 3^2$

$108 = 2^2 . 3^3$

چون 2 و 3 درهردو شامل اند. پس 2^3 و 3^3 راباهم ضرب نوده وحاصل ضرب ان (Lcm) است. یعنی:

$\text{Lcm}(72,108) = 2^3 . 3^3 = 8 . 27 = 216$

216 بالای هردو اعداد داده شده قابل تقسیم است

مثال: میخواهیم Lcm(-24,10) رادریافت نمایم

$m = -24 \ , n = 10$

$-24 = -3.10 + 6$

$10 = 1.6 + 4$

$6 = 1.4 + 2$

$4 = 2.2 + 0$

$\gcd(-24,10) = 2$

$$\text{Lcm}(-24,10) = \frac{|-24.10|}{\gcd(-24,10)} = \frac{240}{2} = 120$$

ازطریقه دیگر:

$-24 = 2^3.(-3)$

$10 = 2.5$

از علامه منفی صرف نظرمیکنیم. زیرا Lcm عدد مثبت تعریف شده

$\text{Lcm}(-24,10) = 2^3.3.5 = 120$

مثال : Lcm(8,10,12,16) را دریافت می نمایم

$8 = 2^3$
$10 = 2 . 5$
$12 = 2^2 . 3$
$16 = 2^4$
چون عدد 2 درهمه شامل است. پس 2^4 (یعنی 2 بابزرگترین طاقت) را به 3 و 5 ضرب مینمایم. که حاصل ان کوچکترین مضرب مشترک (Lcm) است.

$Lcm(8,10,12,16) = 2^4 . 3 . 5 = 240$

مثال : Lcm(72,108) را دریافت می نمایم

$72 = 2^3 . 3^2$
$108 = 2^2 . 3^3$
چون عدد 2 و 3 درهردو شامل است. پس 2^3 **و** 3^3 (بابزرگترین طاقت) را باهم ضرب مینمایم و حاصل ان کوچکترین مضرب مشترک (Lcm) است.

$Lcm(72,108) = 2^3 . 3^3 = 216$

تمرین 3.7 : Lcm(180 , 600) را دریافت نماید
نوت: بااستفاده ازکوچکترین مضرب مشترک (Lcm) میتوان تقاطع گروپهای فرعی از $(\mathbb{Z}, +)$ رادریافت نمایم
اگر $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ و d کوچکترین مضرب مشترک ان باشد. درانصورت:

$$d = Lcm(a_1, a_2, \ldots, a_n) \Rightarrow \bigcap_{i=1}^{n} a_i \mathbb{Z} = d\mathbb{Z}$$

بطورمثال $2\mathbb{Z} \cap 3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$ است. زیرا :

$Lcm(2,3,4) = 3 . 2^2 = 12$

تمرین 3.8 :
(a) ما گروپ های فرعی $10\mathbb{Z}$, $6\mathbb{Z}$ و$4\mathbb{Z}$ را در گروپ $(\mathbb{Z}, +)$ داریم تقاطع انرا دریافت نماید
(b) ما گروپ های فرعی $8\mathbb{Z}$, $6\mathbb{Z}$ را در گروپ $(\mathbb{Z}, +)$ داریم. تقاطع انرا دریافت نماید
تعریف 3.8 : تعداد عناصر یک گروپ (G,.) بنام group order (مرتبه گروپ) یاد میشود وآنرا به ord(G) و یا $|G|$ نشان میدهیم. اگرگروپ غیر متناهی باشد درآنصورت $ord(G)=\infty$.

یادداشت : ما برای آسانی به جای $a \oplus a \oplus \ldots\ldots \oplus a$ (m دفعه) a آنرا به a^m نشان میدهیم .

تعریف 3.9 : $(G, \oplus)$ یک گروپ با عنصرعینیت (خنثی) e و $a \in G$ است. کوچکترین $m \in \mathbb{N}$ که $a^m = e$ شود بنام order (مرتبه) از a یاد میشود و ما انرا به $ord_G(a)$ نشان میدهیم. یعنی :

$$ord_G(a) = \min \{ i \in \mathbb{N} \mid a^i = e \}$$

اگرمعلوم باشد که کدام گروپ است درانصورت آنرا به شکل ord(a) می نویسیم بطورمثال $ord(D_4) = 8$

$e^1 = e \Rightarrow ord(e) = 1$

$b.b = b^2 = e \Rightarrow ord(b) = 2$

$c.c = b$

$c^3 = c.c.c = b.c = a$

$c^4 = c.c.c.c = a.c = e \Rightarrow ord(c) = 4$

تمرین 3.9 : ord(d) , ord(f) و ord(g) را درگروپ $(D_4,.)$ و $(Q_8,.)$ دریافت نماید

قضیه 3.8 : $(G, \odot)$ یک گروپ معین ، $a \in G$ و e عنصر عینیت ان است. بعدآ مرتبه (order) از a خورد تر یا مساوی به مرتبه (order) از G است .

یعنی $ord(a) \leq ord(G)$

ثبوت : $|G| = ord(G)$, $k = ord(a)$

اگر $ord(a) \leq ord(G)$ نباشد در اینصورت $k > |G|$ و $k \geq |G|+1$

ما تابع ذیل را بالای سیت $X=\{1,2,3,\ldots\ldots,k\}$ و G به شکل ذیل تعریف می نمائیم .

$$f: X \longrightarrow G$$
$$i \longmapsto a^i$$

چون $k > |G|$ پس باید $i, j \in X$ با خواص ذیل موجود باشد .

$i > j$, $f(i) = a^i = f(j) = a^j \Rightarrow a^i . (a^j)^{-1} = a^j (a^j)^{-1}$

$\Rightarrow a^{i-j} = e \wedge (0 < i - j < k)$

از اینجا نتیجه میشود که ord(a) مساوی به $i - j$ است . مگر این درتضاد به تعریف مرتبه (order) یک عنصر است . زیرا k خورد ترین عدد است که $a^k = e$ میشود، پس لهذا

$Ord(a) \leq ord(G)$

قضیه 3.9 : (theorem of fermat): (G, .) یک گروپ معین , e عنصر عینیت و $a \in G$. بعدآ $a^{ord(G)} = e$

ثبوت : چون G معین است پس میتوان نوشت $G= \{ g_1 , g_2, \ldots , g_n \}$ و $ord(G)=|G| = n$. ماتابع ذیل را در نظر میگیریم :

$$f: G \longrightarrow G$$
$$g \longmapsto a.g$$

$$x, y \in G , f(x) = a.x = f(y) = a.y$$
$$ax = ay \Rightarrow a^{-1}.a.x = a^{-1}.a.y \Rightarrow x = y \Rightarrow f \ injective$$
$$y \in G , y := a.x \Rightarrow x = a^{-1}.y$$
$$\Rightarrow f(x) = (a^{-1}.y) = a.(a^{-1}.y) = y$$
$$\Rightarrow f \ surjective$$

چون f یك bijective است پس :

$$G = f(G) \Rightarrow \{g_1, g_2, \ldots, g_n\} = \{ag_1, ag_2, \ldots, ag_n\}$$

$$\Rightarrow \prod_{i=1}^{n} g_i = \prod_{i=1}^{n} ag_i = a^n \prod_{i=1}^{n} g_i$$

$$\Rightarrow (\prod_{i=1}^{n} g_i) . (\prod_{i=1}^{n} g_i)^{-1} = a^n (\prod_{i=1}^{n} g_i) . (\prod_{i=1}^{n} g_i)^{-1}$$

$\Rightarrow a^n = e$

$\Rightarrow \quad a^n = a^{ord(G)} = e$

قضیه 3.10: (G ,.) یك گروپ معین که عنصرعینیت آن e و $a \in G$ است. بعدآ ord(G) بالاي ord(a) قابل تقسیم است . یعني ord(a)| ord(G) .

ثبوت : اگر $ord(G) = m$ و $ord(a) = n$ باشد وما فرض کنیم که ord(G) قابل تقسیم بالای ord(a) نیست پس درینصورت :

$\exists q,r \in \mathbb{N} ; m=q.n+r \qquad 0< r < n$

$\Rightarrow r = m-q.n$

نظربه قضیه fermat میدانیم که $a^{ord(G)} = a^m = e$ است. پس:

$a^r = a^{m-qn} = a^m . (a)^{-qn} = a^m . (a^n)^{-q} = e.(e)^{-q} = e.(e^q)^{-1} = e$

مگر این در تضاد به تعریف ord(a) قرار میگیرد زیرا n خورد ترین عدد طبیعی است که $a^n = e$ میشود. مگر در فوق دیده شد که $a^r = e$ و $r < n$ است.

در نتیجه ord(a)| ord(G)

لیما 3.4 : هرگروپ که مرتبه (order) آن یک عدد اولیه باشد، آن گروپ دورانی (cyclic group) است .

ثبوت : ما فرض میکنیم که (G, .) یک گروپ است که مرتبه (order) آن عدد اولیه p و e عنصرعینیت ان است.

اگر {e} = G باشد. درانصورت دورانی بودن G واضح است.

اگر {e} ≠ G باشد

$G \neq \{e\} \Rightarrow \exists\, a \in G$,$a \neq \{e\}$

$ord(G) = p \Rightarrow ord(a) \mid p$ [نظر به قضیه (3.10)]

چون p عدد اولیه است پس باید ord(a) = p باشد و در نتیجه G= <a> است.

یعنی G یک گروپ دورانی است .

مثال 3.4 : در گروپ$(A^{(4)},\oplus)$ دیده میشود که :

$ord(A^{(4)}) = \left|A^{(4)}\right| = 4$

مامیدانیم که عنصر عینیت آن گروپ a_0 است.

$a_1 \oplus a_1 = a_2$

$a_1 \oplus a_1 \oplus a_1 = a_2 \oplus a_1 = a_3$

$a_1 \oplus a_1 \oplus a_1 \oplus a_1 = a_3 \oplus a_1 = a_0 \quad \Rightarrow a_1^4 = a_0$

$\Rightarrow ord(a_1) = 4 \quad \wedge \quad ord(a_1) \mid ord(A^{(4)})$

$a_2 \oplus a_2 = a_0 \quad \Rightarrow a_2^2 = a_0$

$\Rightarrow ord(a_2) = 2 \quad \wedge ord(a_2) \mid ord(A^{(4)})$

$a_3 \oplus a_3 = a_2$

$a_3 \oplus a_3 \oplus a_3 = a_2 \oplus a_3 = a_1$

$a_3 \oplus a_3 \oplus a_3 \oplus a_3 = a_3 \oplus a_1 = a_0 \Rightarrow a_3^4 = a_0$

$\Rightarrow ord(a_3) = 4 \ \wedge ord(a_3) \mid ord(A^{(4)})$

هم چنان دیده میشود که $ord(a_1), ord(a_2), ord(a_3) \leq ord(A^{(4)})$

تمرین 3.10

(a) ord(E),ord(K),ord(-E),ord(I) را در گروپ (Q,.) دریافت نماید

(b) ord(f),ord(h) ,ord(x) را در گروپ (Q_8,.) دریافت نماید

تعریف 3.10: (G, ⊕) یک گروپ ، H یک گروپ فرعی آن و a ∈ G است .

a ⊕ H ={a⊕h | h∈H} بنام left coset (کلاس چپ) و

H ⊕ a ={h⊕a | h∈H} بنام right coset (کلاس راست) یاد میشود .

مثال : اگر ما گروپ فرعي H:={b_1, b_2} از گروپ $A^{(2.2)}$ را در نظر بگيريم . کلاسهای چپ ان عبارت اند از:

$b_1 \odot H = \{b_1 , b_2 \}$
$b_2 \odot H = \{b_2, b_1\}$
$b_3 \odot H = \{b_3, b_4\}$
$b_4 \odot H = \{b_4, b_3\}$

ديده ميشود که:

$H_1 := b_1 \odot H = b_2 \odot H$, $H_2 := b_3 \odot H = b_4 \odot H$

تعداد تمامي left-coset (کلاس هاي چپ) نظر به H در گروپ $A^{(2.2)}$ مساوي 2 است . همچنان $A^{(2.2)} = H_1 \cup H_2$

قضيه3.11 : (G, .) يک گروپ ، U يک گروپ فرعی ان و a,b∈G است ، بعدآ :

a.U = U ⇔ a∈ U
a.U = b.U ⇔ a^{-1}.b∈U
a.U∩b.U≠ ∅ ⇔ a.U =b.U

معنی (c) اينکه دو left-coset باهم مساوی اند ويا تقاطع شان خالی است .

ثبوت (a)

" ⇐"

g∈ aU ⇒ ∃ u∈U ; g=a.u
⇒ g∈U [a,u ∈ U گروپ U زيرا فرعی و]
⇒ aU ⊆ U

g∈ U ⇒ g = e.g = a. a^{-1}.g = a.(a^{-1}.g)
⇒ g∈aU [a ,g ∈U زيرا]

در نتيجه aU = U

„ ⇒"

g∈ aU = U ⇒ ∃ u∈U ; g = a.u , g.u ∈ a.U = U
⇒ a = g. u^{-1} ⇒ a∈U [g,u∈ U زيرا]

ثبوت (b)

" ⇐"

a^{-1}.b ∈ U ⇒ a^{-1} . b . U = U [(a) به نظر]
⇒ a. a^{-1} . b . U = a . U
⇒ b .U = a .U

„⇒ "

$g \in aU = bU \Rightarrow u_1, u_2 \in U;\ g = a.u_1 = b.u_2$

$\Rightarrow a^{-1}.a.u_1.u_2^{-1} = a^{-1}.b\,u_2.u_2^{-1}$

$\Rightarrow u_1.u_2^{-1} = a^{-1}.b$

$\Rightarrow a^{-1}.b \in U \quad [u_1, u_2 \in U$ زیرا$]$

ثبوت (c)

„⇐"

$g \in a.U = b.U \Rightarrow \exists\ u_1, u_2 \in U;\ g = a.u_1 = b.u_2$

$\Rightarrow g \in a.U \cap b.U$ [زیرا $a.u_1 \in a.U$ و $b.u_2 \in b.U$ است]

درنتیجه: $a.U \cap b.U \neq \emptyset$

„⇒ "

$a.U \cap b.U \neq \emptyset \Rightarrow \exists\ g \in aU \cap bU \Rightarrow \exists\ u_1, u_2 \in U;\ g = a.u_1 = b.u_2$

$\Rightarrow a^{-1}.a.u_1.u_2^{-1} = a^{-1}b.u_2.u_2^{-1}$

$\Rightarrow u1.u_2^{-1} = a^{-1}.b$

$\Rightarrow a^{-1}.b \in U \quad [u_1, u_2 \in U$ زیرا$]$

$\Rightarrow a.U = b.U \quad [$ نظر به (b) $]$

لیما 3.5 : $(G,.)$ یک گروپ و U گروپ فرعی آن است . بعداً

(1) $G = \bigcup_{a \in G} aU$, در صورتیکه هردو left-coset باهم مساوی و یا دارای تقاطع خالی باشند .

(2) $|a.U| = |U| = |Ua|$. یعنی برای هر $a \in G$ تعداد عناصر U , U.a و باهم مساوی اند

ثبوت (1):

$\forall a \in G,\ a = a.e \in a.U \quad [e \in U$ زیرا$]$

$\Rightarrow G \subseteq \bigcup_{a \in G} a.U \qquad \Rightarrow G = \bigcup_{a \in G} a.U$

نظر به قضیه 3.11 هردو left- coset (کلاس چپ) یا با هم مساوی ویا متقاطع شان خالی میباشد . یعنی برای $a,b \in G$

$a.U \cap b.U \neq \emptyset \Leftrightarrow a.U = b.U$

ثبوت (2) : $a \in G$ برای ثبوت ما تابع ذیل را در نظر میگیریم :

$f:U \longrightarrow aU$

$u \longmapsto a.u$

f یک تابع bijective است زیرا :

$u_1, u_2 \in U ; f(u_1) = au_1 = au_2 = f(u_2)$

$\Rightarrow u_1 = a^{-1}.a\ u_2 = u_2 \quad \Rightarrow$ injective

$b \in aU \Rightarrow \exists\ u \in U; b = a.u = f(u) \Rightarrow$ f surjective

چون f یک bijective است پس تعداد عناصر U و aU باهم مساوی اند یعنی $|aU| = |U|$

به همین طور میتوانیم ثبوت نمائیم که تابع ذیل bijective است .

$f :U \longrightarrow Ua$

$u \longrightarrow u.a$

در نتیجه $|aU|=|U|=|Ua|$

مثال: $H= \{e,a,g,h\}$ یک گروپ فرعي درگروپ $(Q_8,.)$ است و $b \in Q_8$

$b.H = b.\{e,a,g,h\} = \{ b,c,f,d\} \Longrightarrow |b.H| = 4 = |H|$

حالامیخواهیم نشان دهیم:

$Q_8 = \bigcup_{a \in Q_8} aH$

نظر به قضیه 3.11 میدانیم:

$e,a,g,h \in H \Longrightarrow e.H = a.H = g.H = h.H = H$

حالا عناصرمتباقی Q_8 رادرنظرمیگریم

$b.H = b.\{e,a,g,h\} = \{ b,c,f,d\}$

$c.H = c.\{e,a,g,h\} = \{ c,b,d,f\}$

$d.H = d.\{e,a,g,h\} = \{ d,f,b,c\}$

$f.H = f.\{ e,a,g,h \} = \{ f,d,c,b \}$

دیده میشود که :

$U:=b.H = c.H = d.H = f.H$

در نتیجه:

$Q_8 = H \cup U$

مثال 3.5 : اگر ما گروپ فرعی $U = 6\mathbb{Z}$ از $(+, \mathbb{Z})$ را در نظر بگیریم، دیده میشود که:

$5+6\mathbb{Z}\ , 4+6\mathbb{Z}\ , 3+6\mathbb{Z}\ , 2+6\mathbb{Z}\ , 1+6\mathbb{Z}\ , 6\mathbb{Z}$

Left-coset (کلاسهای چپ) نظر به U هستند وهمه شان دارای تعداد عناصر مساوی اند .

بطور مثال نظر به لیما 3. 5 $|3 + 6\mathbb{Z}| = |6\mathbb{Z}|$ و علاوه برآن تمامي اين Left-coset ها مختلف هستند . زيرا :

$U=6\mathbb{Z}=\{\ldots -18, -12, -6, 0, 6, 12, 18\ldots\}$

$1+6\mathbb{Z}=\{\ldots -17, -11, -5, 1, 7, 13, 19\ldots\}$

$2+6\mathbb{Z}=\{\ldots -16, -10, -4, 2, 8, 14, 20\ldots\}$

Left coset کلاس های چپ $1+6\mathbb{Z}$ و $7+6\mathbb{Z}$ باهم مساوی اند. زيرا

$7+6\mathbb{Z} = 1+(6+6\mathbb{Z}) = 1+6\mathbb{Z}$ [نظر به قضیه 3.11]

تعریف 3.11 : (G , .) یک گروپ U گروپ فرعی آن است . تعداد تمامی leftcoset مختلف از U در G را بنام Index از U در G یاد میکنند . وآنرا $ind_G(U)$ ویا [G : U] نشان میدهند . یعنی

$ind_G(U) = |\{a.U \mid a \in G\}| = |U.a \mid a \in G| = [G:U]$

مثال :

(a) $ind_G(G) = |G:G| = 1$

$ind_G(e) = [G:\{e\}] = |G|$

(b) $ind_{\mathbb{Z}}(n\mathbb{Z}) = [\mathbb{Z} : n\mathbb{Z}] = n \quad \forall n \in \mathbb{N}$

زیرا تمامی کلاس های چپ از $n\mathbb{Z}$ در $\mathbb{Z}$ مساوی به n است . بطورمثال اگر ماگروپ فرعی $5\mathbb{Z}$ رادرنظربگیریم. درانصورت:

$$ind_{\mathbb{Z}}(5\mathbb{Z}) = [\mathbb{Z} : 5\mathbb{Z}] = 5$$

قضیه 3.12 : $(G,.)$ یک گروپ معین، H و H_1 گروپهای فرعی آن میباشند و $H_1 \subseteq H$ بعداً:

$[G:H_1]=[G:H].[H:H_1]$

ثبوت: نظر به لما (3.5) میتوان G را به شکل اتحاد تمامی left coset از H بنویسیم یعنی:

$$G = \bigcup_{i \in I} a_i H$$

$a_i \in G$ طوری انتخاب شده که در اتحاد H-left coset دو دفعه ظاهر نشود یعنی تمامی a_iH به شکل جوره از هم دیگر مختلف هستند و در نتیجه عدد I مساوی به [G:H] است.
به همین شکل میتوان H_1 را به شکل اتحاد تمامی H_1-left coset نوشت،یعنی:

$$H = \bigcup_{j \in J} b_j H_1$$

در اینجا هم $b_j \in H$ طوری انتخاب شده که در اتحاد H_1-leftcoset دو دفعه ظاهر نشود و عدد J مساوی به $[H:H_1]$ است.

$G = \cup_{i\in I} a_iH = \cup_{i\in I} a_i (\cup_{j\in J} b_jH_1) = \cup_{i\in I}(\cup_{j\in J} a_ib_jH)$

در این اتحاد H_1-leftcoset از همدیگر مختلف هستند پس:

$[G:H_1]= I.J$

و از این نتیجه میشود: $[G:H_1] = [G:H].[H:H_1]$

مثال: $H_1 = \{b_1\}$ و $H = \{b_1,b_4\}$ گروپ های فرعی در $(A^{(2,2)}, \odot)$ اند.
چون b_1 عنصرعینت از $A^{(2,2)}$ است. پس Liftcoset های H_1 نظر به $A^{(2,2)}$ عبارت اند از $\{b_1\}$,$\{b_2\}$,$\{b_3\}$ و $\{b_4\}$

$ind_{A(2,2)}(H_1) = 4$

$b_2 \odot H = b_2 \odot \{b_1,b_4\} = \{ b_2 \odot b_1, b_2 \odot b_4\} = \{b_2,b_3\}$

$b_3 \odot H = b_3 \odot \{b_1,b_4\} = \{ b_3 \odot b_1, b_3 \odot b_4\} = \{b_3,b_2\}$

Liftcoset های H نظر به $A^{(2,2)}$ عبارت اند از $\{b_1,b_4\}$ و $\{b_2,b_3\}$
ودر نتیجه $ind_{A(2,2)}(H) = 2$

Liftcoset های H_1 نظر به H عبارت اند از $\{b_1\}$, و $\{b_4\}$ ودر نتیجه $Ind_H(H_1) = 2$

قضیه 3.13: (Lagrange) H یک گروپ فرعی ازگروپ معین $(G,.)$ و e عنصر عینیت (identity) ان است. بعداً:

$$Ord(G)= ord(H) \,.\, ind(H)$$

ثبوت:- اگر $E := \{e\}$ باشد درانصورت E یک گروپ فرعی از G و H است پس:

$Ord(G) = [G:E] \quad \wedge \quad ord(H) = [H:E]$

ویا به شکل دیگر

$|G| = ind_G(E) \qquad \wedge \qquad |H| = ind_H(E)$

بنابراین نظر به قضیه 3.12 میتوان نوشت:

[G:E]=[G:H] . [H:E]

ویا

ord(G)=ind(H). ord(H)

نوت: ازقضیه Lagrange نتیجه میشود که مرتبه (order) یک گروپ معین باید بالای مرتبه هرگروپ فرعی ان قابل تقسیم باشد

مثال: { H={e,a,d,f یک گروپ فرعی در $\mathbf{Q_8}$ است. $Ind_{Q8}(H)$ رامیخواهیم دریافت نمایم

چون ord(H) = 4 و $ord(Q_8) = 8$ است. پس نظر به قضیه Lagrange میتوان نوشت

$ord(Q_8) = ind(H).\ ord(H) \Rightarrow\ 8 = ind(H).\ 4$

$\Rightarrow\ ind(H) = \frac{8}{4} = 2$

تمرین 3.11 :

(a) درگروپ ($(D_4,.$ ما گروپ های فرعی $H_1 = \{e,b\}$ و $H = \{e,a,b,c\}$ را داریم.

(i) $Ind_{D4}(H_1), ind_{D4}(H), ind_H(H1)$ را دریافت نماید

(ii) مربوطه left-coset های ان کدام اند. یعني عناصرسیت های ذیل رادریافت نماید.

$\{a.H \mid a \in G\}$, $\{a.H_1 \mid a \in G\}$, $\{a.H_1 \mid a \in H\}$

(b) (G,.) یک گروپ است ، H_1 و H گروپ های فرعي G است ، $H_1 \subseteq H$ ، $ind_G(H) = 6$, $ind_H(H_1) = 4$. معلوم نماید که تعداد left-coset نظربه G چند است. یعني $ind_G(H_1)$ رادریافت نماید .

(c) ما گروپ (G,.) ذیل راداریم:

$G = \{ a, a^2, a^3, \ldots, a^{14}, a^{15}, a^{16} = e \}$,

$H = \{ a^4, a^8, a^{12}, a^{16} = e \}$, $H_1 = \{ a^8, a^{16} = e \}$

(i) ثبوت نماید که H و H_1 گروپ های فرعي دوراني در G اند
(ii) $ind_G(H)$ و $ind_G(H_1)$ را دریافت نماید .

مثال 3.5 : درین مثال ما گروپ S_3 را تحت مطالعه قرار میدهیم , تعداد عناصر S_3 مساوی به 6 است . زیرا

$|S_3|= 3! = 1.2.3=6$

حالا آن 6 عنصر را به شکل ذیل نام گذاری می نمائیم :

$$id = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \quad f_1 := \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \quad f_2 := \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

$$f_3 := \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \quad f_4 := \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \quad f_5 := \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

پس S_3={ id ,f_1,f_2,f_3,f_4,f_5}
نظر به قضیه 3.4 میدانیم که S_3 نظر به ترکیب تابع (Map composition) یک ساختمان گروپی دارد. جدول کیلی (Cayley Table) از (S_3, o) شکل ذیل رادارد:

o	id	f_1	f_2	f_3	f_4	f_5
id	id	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_3	f_4	id	f_5	f_2
f_2	f_2	f_5	i_d	f_4	f_3	f_1
f_3	f_3	id	f_5	f_1	f_2	f_4
f_4	f_4	f_2	f_1	f_5	id	f_3
f_5	f_5	f_4	f_3	f_2	f_1	id

بطور مثال در جدول فوق $f_3 \circ f_4 = f_2$

$$f_3 \circ f_4 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} o \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} = f_2$$

ویا به شکل مفصل :

$f_4(1)=2 \quad f_4(2)=1 \quad f_4(3)=3$
$f_3 \circ f_4(1) = f_3(2) = 1$, $f_3 \circ f_4(2) = f_3(1) = 3$,

$f_3 \circ f_4(3) = f_3(3) = 2$

$$f_3 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2 \qquad \text{پس}$$

چون $|S_3|=6$ است پس نظر به قضیه Lagrange میتواند S_3 تنها گروپ های فرعی داشته باشد که مرتبه (order) آن 1,2,3 و 6 باشد زیرا 6 بالای همین اعداد قابل تقسیم است .

نوت: بعضی مشخصات گروپ $(S_3,\circ)$:

(a) S_3 دارای گروپ های فرعی ذیل میباشد .

(1) {id} که مرتبه (order) آن مساوی به یک است .

(2) S_3 که دارای مرتبه (order) 6 میباشد .

(3)

$U_1:=\langle f_2\rangle = \{id, f_2\}$, $U_2:=\langle f_4\rangle = \{id, f_4\}$, $U_3:=\langle f_5\rangle = \{id, f_5\}$

همه این گروپ های فرعی دورانی (cyclic) بوده و دارای مرتبه 2 میباشند.

یعنی :

$ord(U_1) = ord(U_2) = ord(U_3) = 2$

بطورمثال نشان میدهیم که U_3 گروپ فرعی دورانی است.زیرانظربه جدول:

$id \circ id = id$, $id \circ f_5 = f_5$, $f_5 \circ f_5 = id$

از جانب دیگر دیده میشود که f_5 مولد از U_3 است. یعنی $\langle f_5\rangle = U_3$

(4)

$Ord(U)=3$, $U:=\langle f_1\rangle = \{id, f_1, f_3\}$

(b) اگر H یک گروپ فرعی از S_3 باشد. Index ویا تعداد تمامی left costes گروپ های فرعی فوق را نظر به قضیه Lagrange میتوان به شکل ذیل دریافت نمود :

$|S_3| = |H| . [S_3:H]$

$ord(S_3) = ord(H) . ind(H)$ ویا

$ind(\{id\}) = \frac{|S_3|}{|\{id\}|} = \frac{6}{1} = 6$ پس

$ind(S_3) = \frac{|S_3|}{|S_3|} = \frac{6}{6} = 1$

$\text{ind}(U_1) = \text{ind}(U_2) = \text{ind}(U_3) = \frac{|S_3|}{2} = \frac{6}{2} = 3$

$\text{ind}(U) = \frac{|S_3|}{|U|} = \frac{6}{3} = 2$

حالا میخواهیم تمامی (left coset) کلاس های چپ بطور مثال از U_3 را بدون در نظر گرفتن قضیه lagrange محاسبه نمائیم. چون $U_3 = \{id, f_5\}$ است. پس در گروپ S_3 امکانات ذیل وجود دارد .

$U_3 , f_1 o U_3 , f_2 o U_3 , f_3 o U_3 , f_4 o U_3$

$f_1 o U_3 = f_1 o \{id , f_5\} = \{ f_1 o id , f_1 o f_5\} = \{ f_1, f_2\}$

$f_2 o U_3 = f_1 o \{id , f_5\} = \{ f_2 o id , f_2 o f_5\} = \{ f_2, f_1\}$

دیده میشود که $f_3 o U_3 = f_2 o U_3$ است

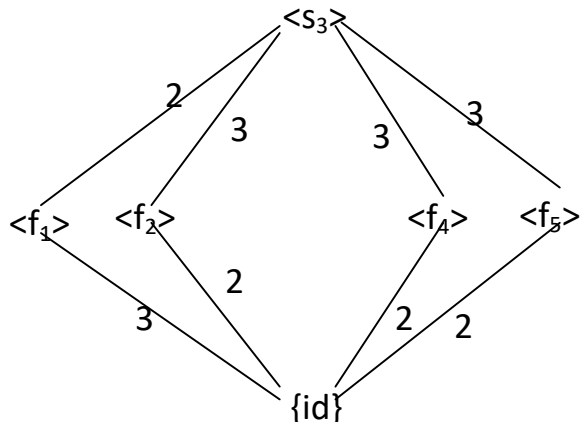
$f_3 o U_3 = f_3 o \{id , f_5\} = \{ f_3 o id , f_3 o f_5\} = \{ f_3, f_4\}$

$f_4 o U_3 = f_4 o \{id , f_5\} = \{ f_4 o id , f_4 o f_5\} = \{ f_4, f_5\}$

در اینجا هم دیده میشود که $f_3 o U_3 = f_4 o U_3$

بالآخره نتیجه میشود که تعداد left coset (کلاس های چپ) از U_3 در S_3 مساوی به 3 است. علاوه بران دیدیم که به استعمال طریقه Lagrange هم همین نتیجه را داشتیم .

مثال فوق را میتوان بشکل گرافیک تمامی گروپ فرعی با index آن طوری ذیل نوشت



بطور مثال ind<f_4> نظر به S_3 مساوی به 3 است ونظر به {id} مساوی به 2 است .

تمرين 3.12:

(a) ثبوت نمائيد كه در مثال 3.5 افاده ذيل صدق ميكند

$<f_1> = \{id , f_1 , f_3 \}$

(b) آيا f_3 مولد كدام يكى از گروپ فرعى از S_3 شده ميتواند .

(c) ثبوت نمايد كه $H:=\{f\epsilon S_4 \ | \ f(4) = 4\}$ يک گروپ فرعى از S_4 است. $|H|$ و ind(H) را دريافت نمائيد .

مثال 3.6 : درمثال 1.7 ديديم كه سيت

$$Q = \{ \pm E , \pm I , \pm J , \pm K \}$$

نظر به ضرب ماتريكس يک گروپ و E عنصر عينيت آن است. به اسانى ميتوان ثبوت نمود كه $H:= \{E,-E,I,-I\}$ يک گروپ فرعى از Q است

علاوه بران H يک گروپ دورانى كه ماتريكس I موٴلد ان ميباشد . زيرا:

$I^2 = I.I = -E$, $I^3 = I.I.I = = -E.I = -I$, $I^4 = I^3 . I = -I.I = E$

درنتيجه $H = <I>$ و ind(H) مساوى به 2 است. زيرا :

$[Q: H] = [Q:<I>] = \frac{ord(Q)}{ord(<I>)} = \frac{8}{4} = 2$

تعريف 3.12: (G ,.) يک گروپ و N يک گروپ فرعى آن است . N را بنام نورمال (normal) ويا invariant ياد ميشود درصورتيكه $a .N=N .a$ براى هر $a\epsilon G$ باشد . ماآنرا به شكل $N \trianglelefteq G$ نشان ميدهيم .

مثال

(a) گروپ فرعى {e} از يک گروپ (G,.) در G نورمال Normal است . زيرا براي $\forall a\epsilon G$

$a .\{e\} a^{-1} =\{e\} \Rightarrow a .\{e\} a^{-1} .a =\{e\}.a \Rightarrow a.\{e\}= \{e\} .a$

ويااينكه دريک گروپ عينيت راست درعين زمان عينيت چپ است

(b) هرگروپ فرعى از يک گروپ تبديلى (commutative) نورمال (normal) است .

مثال 3 .7 : مادر مثال 3.5 ديديم كه $U_3:=<f_5> = \{id ,f_5\}$ يک گروپ فرعى از S_3 است . مگر نورمال نيست زيرا :

$f_1 \circ U_3 = \{ f_1 \circ id , f_1 \circ f_5\} = \{ f_1, f_2\}$

$U_3 \circ f_1 = \{id \circ f_1 , f_5 \circ f_1\}= \{f_1 , f_4\}$

يعنى $f_1 \circ U_3 \neq U_3 \circ f_1$ ودر نتيجه U_3 نورمال (Normal) نيست .

تمرین 3.13 : ثبوت نمائید که $U_1 := \{id , f_1, f_3\}$ درمثال 3.5 یک گروپ فرعی نورمال است .

لیما 3.6: اگر (G ,.) یک گروپ و N یک گروپ فرعی آن باشد . بعداً :

$$\forall a\epsilon G; a.N\,a^{-1} \subseteq N \quad \Leftrightarrow \quad (\text{G نورمال در N یعنی }) \; N \trianglelefteq G$$

ثبوت : " $\Leftarrow$ "

$$N \trianglelefteq G \;\Rightarrow\; \forall a\epsilon G;\; aN = Na$$
$$\Rightarrow \forall x\epsilon N;\; a.x = x.a \;\Rightarrow\; a.x.a^{-1} = x$$
$$\Rightarrow a.x\,.a^{-1}\epsilon N \;\Rightarrow\; \forall a\epsilon G; a.N\,a^{-1} \subseteq N$$

ثبوت" $\Rightarrow$ "

$$\forall a\epsilon G;\; a.N\,.a^{-1} \subseteq N \;\wedge\; a^{-1}\,N\,a \subseteq N$$
$$\Rightarrow\; \forall x\epsilon N\;\; \exists y\epsilon N;\; a.x.a^{-1} = y \;\Rightarrow \text{a.x} = \text{y.a} \;\Rightarrow \text{a.x}\epsilon Na.$$
$$\Rightarrow\; aN \subseteq Na$$

به همینطورمیتوان ثبوت نمود، که $Na \subseteq \text{a}N$

درنتیجه aN=Na و $N \trianglelefteq G$. یعنی N نورمال در گروپ G است.

از این لیما نتیجه گرفته میشود که خود G نیز نورمال(Normal) در خودش است . زیرا برای $a\epsilon G$:

$$\forall g\epsilon G;\; a.g\,.a^{-1}\,\epsilon\, a\,G\;\; a^{-1}$$

از طرف دیگر $a.g\,.a^{-1}\epsilon G$ هم است . پس $a.G\,.a^{-1} \subseteq G$

تعریف 3.13 : (G , .) یک گروپ و $A,B \subseteq G$

$A.B:=\{a.b \mid a\epsilon A\,,\; b\epsilon B\}$

A.B بنام complex product یاد میشود .

$$A^{-1} := \{a^{-1} \mid a\epsilon A\}, \qquad a.B := \{a\}.B\;, \qquad A\,.\,b := A\{b\}$$

مثال: اگرمادرگروپ Q_8 داشته باشیم: $B:=\{a,f,g,h\}, A:=\{a,b,d\}$

$A.B = \{a,b,d\}\,.\,\{a,f,g,h\}$

$= \{ a.a, b.a, d.a, a.f, b.f, d.f, a.g, b.g , d.g, a.h, b.h, d.h \}$

$= \{ e, b, c, d, f , g, h \}$

$A^{-1} = \{ a^{-1}, b^{-1}, d^{-1}\} = \{ a, c, f \}$

تمرین 3.14 : $B:= \{e, b,f, h\}, A:=\{a, b, c,d\} \subseteq D_4$

A.B و B^{-1} را دریافت نماید

لیما 3.7 : (G,.) یک گروپ $\emptyset \neq U \subseteq G$. بعدآ افاده های ذیل یک به دیگر معادل اند :

(1) U گروپ فرعی از G است

(2) $U.U \subseteq U$, $U^{-1} \subseteq U$

(3) $U.U^{-1} \subseteq U$

ثبوت

(1) ⇐ (2)

$u \in U\ U \Rightarrow \exists\, u_1, u_2 \in U\ , u = u_1 . u_2$

$\Rightarrow u = u_1 . u_2 \in U$ [زیرا U یک گروپ فرعی است]

$\Rightarrow U.U \subseteq U$

$a \in U^{-1} \Rightarrow \exists\ b \in U\ ;\ a.b = e$

$\Rightarrow a = b^{-1} \in U$ [$b \in U$ زیرا]

$\Rightarrow U^{-1} \subseteq U$

(3) ⇐ (2)

$u \in U\ U^{-1} \Rightarrow \exists\, u_1 \in U \wedge u_2^{-1} \in U^{-1};\ u = u_1 . u_2^{-1}$

$\Rightarrow u_1 \in U \wedge u_2^{-1} \in U$ [$U^{-1} \subseteq U$ زیرا]

$\Rightarrow u = u_1 . u_2^{-1} \in U . U \subseteq U \Rightarrow U . U^{-1} \subseteq U$

(1) ⇐ (3)

در اینجا ما ثبوت مینمائیم که U داراي خواص (1) ، (2) و (3) (قضیه 3.1) میباشد

$a, b \in U \Rightarrow e = b . b^{-1} \in U . U^{-1} \subseteq U$

$\forall\, b \in U , b^{-1} = e . b^{-1} \in U . U^{-1} \subseteq U$

$a . b = a(b^{-1})^{-1} \in U . U^{-1} \subseteq U$

ثبوت شد که U یک گروپ فرعی از G است .

تمرین 3.15 :

(a) مامیدانیم که $(\mathbb{Z}, +)$ یک گروپ است. ثبوت نماید که

$3\mathbb{Z} + 3\mathbb{Z} \subseteq 3\mathbb{Z}$ و $3\mathbb{Z} \subseteq (3\mathbb{Z})^{-1}$ است

(b) ما سیت فرعی $W := \{x \in \mathbb{R} \mid x > 0\}$ را در گروپ $(\mathbb{R}^*, .)$ درنظرمیگیریم . ثبوت نماید که $W.W^{-1} \subseteq W$ است

(c) با استفاده از لیما 3.7 ثبوت نماید که H={e,b,f,h} گروپ فرعی از D_4 است

یادداشت 3.1 : اگر (G , .) یک گروپ و U و V گروپ های فرعی آن باشد بصورت عموم Complex product ازU و V یعنی (U.V) یک گروپ فرعی ازG را تشکیل نمی دهند .
برای این هدف ما مثال 3.5 را بار دیگر تحت مطالعه قرار میدهیم . گروپ های فرعی U و V را طوری ذیل تعریف مینمائیم .

$U:=< f_2 >=\{id , f_2\}$
$V:=< f_4 >=\{id , f_4\}$
$U.V =\{ id , f_2 , f_4 , f_2 o f_4\}$
$=\{ id , f_2 , f_4 , f_3\}$
$\Rightarrow ord(U.V) = 4$

نظر به قضیه Lagrange نمیتواند S_3 گروپ فرعی که مرتبه (order) آن 4 است داشته باشد .

لیما 3.8 : (G , .) یک گروپ و Uو V گروپ های فرعی آن است . بعداً:
$U.V = V.U \Leftarrow$ UV یک گروپ فرعی از G است

ثبوت : نظر به لیما 3.7 میدانیم که $V V^{-1} \subseteq V$ و $U U^{-1} \subseteq U$ است

$(UV) . (UV)^{-1} = U V V^{-1} U^{-1} \subseteq U V U^{-1}$
$= V U U^{-1}$ [نظر به فرضیه]
$\subseteq V .U = U . V$
$\Rightarrow U . V$ sub group (گروپ فرعی) [نظر به لیما 3.7]

از لیما فوق نتیجه میشود که Complex product دو گروپ فرعی وقتی یک گروپ فرعی رابوجود می آورد در صورتیکه یکی از آنها نورمال باشد .

قضیه 3.15 : (G, .) و (G_1, *) دو گروپ که دارای عناصر عینیت $e \epsilon G$, $e_1 \epsilon G_1$ میباشند و $\varphi: G \to G_1$ یک G-Hom است . بعداً:

(a) $\varphi^{-1}(V) =\{a \epsilon G \mid \varphi(a) \epsilon V \} \trianglelefteq G \quad \Leftarrow \quad V \trianglelefteq G_1$

(یعنی اگر V نورمال در G_1 باشد در آن صورت هم چنان $\varphi^{-1}(V)$ نیز نورمال در G است)

(b) $ker \varphi \trianglelefteq G$ [یعنی ker φ نورمال در G است]

(c) اگر φ هم surjective باشد د ر آن صورت :

$$N \trianglelefteq G \Rightarrow \varphi(N) \trianglelefteq G_1$$

(یعنی اگر N نورمال در G باشد در آنصورت $\varphi(N)$ نورمال در G_1 است)

ثبوت (a) **:** نظر به قضیه 3.3 میدانیم که $\varphi^{-1}(V)$ یک گروپ فرعی از G است

$x \in \varphi^{-1}(V),\ a \in G \Rightarrow \varphi(x) \in V\ ,\ \varphi(a) \in G_1\ ,\ \varphi(a^{-1}) \in G_1$

$\Rightarrow \varphi(a.x.a^{-1}) = \varphi(a) * \varphi(x) * \varphi(a^{-1}) \in V$ [$V \trianglelefteq G_1$ زیرا]

$\Rightarrow a.x.a^{-1} \in \varphi^{-1}(V)$

$\Rightarrow \varphi^{-1}(V)$ (normal) نورمال [نظر به لیما 3.6]

ثبوت (b) **:**

$a \in G\ , x \in ker\varphi$

$\Rightarrow \varphi(x) = e_1$

$\Rightarrow \varphi(a.x.a^{-1}) = \varphi(a) * \varphi(x) * \varphi(a^{-1})$

$= \varphi(a) * e_1 * \varphi(a^{-1}) = e_1$

$\Rightarrow a.x.a^{-1} \in ker\varphi$

$\Rightarrow ker\varphi \trianglelefteq G$ [نظر به لیما 3.6]

ثبوت (c) **:** $\varphi(N)$ نظر به قضیه 3.3 یک گروپ فرعی از G_1 است .

$b \in G1 \Rightarrow \exists\ a \in G\ ;\ \varphi(a) = b$ [surjective φ زیرا]

$\Rightarrow \forall x \in N\ ;\ b\,\varphi(x)\,b^{-1} = \varphi(a).* \varphi(x) * \varphi(a^{-1})$

$= \varphi(a.x.a^{-1})$

چون N یک normal در G است پس نظر به لیما 3.6 $a.x.a^{-1} \in N$

$a.x.a^{-1} \in N \Rightarrow$ $b.\varphi(x).b^{-1} = \varphi(a.x.a^{-1}) \in \varphi(N)$

در نتیجه نظر به لیما 3.6 $\varphi(N)$ یک Normal در G_1 است .

لیما 3.9 : $(G, +)$ يك گروپ , $e \in G$ عنصر عينيت و H يك گروپ فرعي آن است، $x \in G$.

بعداً : $x^{-1}.H.x = \{x^{-1}.h.x \mid h \in H\}$ يك گروپ فرعي از G است

ثبوت :

$e = x^{-1}.e.x \in x^{-1}.H.x$

$a,b \in x^{-1}.H.x$

$\Rightarrow \exists\, h,k \in H ; a = x^{-1}.h.x \wedge b = x^{-1}.k.x$

$\Rightarrow a.b = (x^{-1}.h.x)(x^{-1}.k.x)$

$= x^{-1}.h\,x\,.x^{-1}.k.x = x^{-1}.hkx$

$\Rightarrow a.b = x^{-1}.hkx \in x^{-1}.H.x$ [$h,k \in H$ و H گروپ فرعي]

$a = x^{-1}.h.x$

$\Rightarrow a^{-1} = (x^{-1}.(h.x))^{-1} = (hx)^{-1}.(x^{-1})^{-1} = x^{-1}.h^{-1}.x$

$\Rightarrow a^{-1} \in x^{-1}.H.x$ [زيرا $h \in H$ و H يك گروپ فرعي]

در نتيجه $x^{-1}.H.x$ نظربه قضيه 3.1 يك گروپ فرعي در G است .

ليما 3.10 : (G ,.) يك گروپ، e عنصر عينت و $a \in G$ است. سيت $C_G(a)$ به شكل ذيل تعريف شده است:

$$C_G(a) = \{x \in G \mid x^{-1}.a.x = a\}$$

$C_G(a)$ يك گروپ فرعي از G است كه a نيز شامل آن ميباشد .

ثبوت :- براي ثبوت از قضيه 3.1 استفاده ميكنيم .

$e^{-1}.a.e = a \Rightarrow e \in C_G(a)$

$\Rightarrow x,y \in C_G(a) \Rightarrow x^{-1}a.x = a \wedge y^{-1}.a.y = a$

$\Rightarrow (xy)^{-1}a\,(xy) = y^{-1}.x^{-1}.a.x.y = y^{-1}a\,y = a$

$\Rightarrow xy \in C_G(a)$

$x \in C_G(a) \Rightarrow x^{-1}a.x = a$

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

$\Rightarrow x^{-1} \in C_G(a)$

ثبوت شد كه $C_G(a)$ يك گروپ فرعي از G است . $C_G(a)$ بنام centralizer از a در G يادميشود

مثال: ميخواهيم بااستفاده از ليما 3.10 گروپ فرعى C_{D_4} (c) رادريافت نمايم

$$C_{D_4}(c) = \{x \in D_4 \mid x^{-1}.c.x = c\}$$

$e^{-1}.c.e = e.c.e = c \Rightarrow e \in C_{D_4}$ (c)

$a^{-1}.c.a = c.c.a = b.a = c \implies a \in C_{D_4}(c)$
$b^{-1}.c.b = b.c.b = a.b = c \implies b \in C_{D_4}(c)$
$c^{-1}.c.c = a.c.c = e.c = c \implies c \in C_{D_4}(c)$
$d^{-1}.c.d = d.c.d = f.d = a \implies d \notin C_{D_4}(c)$

همچنان f,g,h شامل $C_{D_4}(c)$ نيستند. يعنى: $f,g,h \notin C_{D_4}(c)$
درنتيجه $C_{D_4}(c) = \{e,a,b,c\}$

تمرين 3.16: ما درگروپ $(D_4,.)$ گروپ فرعى $H:=\{e,h\}$ را در نظرميگيريم. بااستفاده از ليما 3.9 براى $a \in D_4$ گروپ فرعى $U:=\{a^{-1}.H.a\}$ رادريافت نمايد

تمرين 3.17: بااستفاده از ليما 3.10
(a) گروپ فرعى $C_{D_4}(h)$ رادريافت نمايد
(b) گروپ فرعى $C_{S_3}(f_3)$ رادريافت نمايد
(c) گروپ فرعى $C_{Q_8}(g)$ رادريافت نمايد

تعريف 3.14: $(G,.)$ يك گروپ و $e \in G$ عنصر عينيت ان است.
(a) $x \in G$ بنام central ويا self-conjugate ياد ميشود، درصورتكه $x^{-1}\,a\,.\,x = a$ صدق كند
(b) سيت تمامي عناصر كه central در G باشد بنام centre (مركز) از G ياد ميشود ومآن را به Z(G) نشان ميدهيم يعني :

$$Z(G) := \{x \in G \mid x^{-1}\,a\,.\,x = a \quad \forall a \in G\}$$
$$= \{x \in G \mid a\,.\,x = xa \quad \forall a \in G\}$$

اگر G يك گروپ تبديلي (commutative) باشد در ان صورت Z(G)=G است

مثال 3.8 : درگروپ $(D_4, .)$ گروپ فرعي {e,b} centre (مركز) از D_4 است يعني :

$$Z(D_4) = \{e, b\}$$

زيرا:

$\forall x \in D_4 ; e^{-1}\,x\,.\,e = x \implies e \in Z(D_4)$
$b^{-1}\,.\,a\,.\,b = b.a.b = c.b = a$
$b^{-1}\,.\,c\,.\,b = b.c.b = c$
$b^{-1}\,.\,d\,.\,b = b.d.b = g.b = d$

به همين شكل اگر ادامه داده شود ديده ميشود كه براى f,g,h نيز صدق ميكند. پس:

$$\forall\, x \in D_4\,;\, b^{-1}.x.b = x \Rightarrow b \in Z(D_4)$$

در نتيجه $Z(D_4) = \{e, b\}$

قضيه 3.16 : اگر (G , .) يك گروپ باشد، درنصورت $Z(G)$ يك گروپ فرعي از G است .

ثبوت :- براي ثبوت از قضيه 3.1 استفاده مينمائيم .

$$\forall\, x \in G\,;\, e^{-1}.x.e = x \;\Rightarrow e \in Z(G)$$

$$x,y \in Z(G) \Rightarrow x^{-1}a.x = a \;\wedge\; y^{-1}.a.y = a \qquad \forall\, a \in G$$

$$\Rightarrow x,y \in C_G(a) \quad \forall\, a \in G \qquad [3.10 \text{ درليما } C_G(a)]$$

$$\Rightarrow\; x.y\,, x^{-1} \in C_G(a) \quad [\text{زيرا } C_G(a) \text{ يك گروپ فرعي}]$$

$$\Rightarrow\; (x.y)^{-1}.a.(x.y) = a \;\wedge\; (x^{-1})^{-1}.a.x^{-1} = a \quad \forall\, a \in G$$

$$\Rightarrow x.y\,, x^{-1} \in Z(G)$$

ثبوت شد كه Z(G) يك گروپ فرعي از G است .

تعريف 3.15 : براي يك گروپ (G,.) ماسيت AutG را طوري تعريف مينمائيم

$$AutG = \{f: G \to G \mid f \;\; G - Autom\}$$

AutG نظر به تركيب تابع (mapping composition) يك گروپ است كه عنصر عينيت آن تابع Id وعنصر معكوس f ∈AutG عبارت از تابع f^{-1} ميباشد. ماآنرا به (AutG , o) نشان ميدهيم .

قضيه 3. 17 : (G ,.) يك گروپ است بعدآ :

(a) در بين G و Auto(G) يك گروپ هومورفيزم φ موجود است

(b) ker(φ) در عين زمان Z(G) (يعني centre (**مركز**)) از G است

ثبوت (a) ما براي $g \in G$ تابع φ ذيل را تعريف مينمائيم .

$$\varphi : G \longrightarrow Aut\, G$$
$$g \longmapsto \varphi(g)$$

حالا $\varphi(g)$ را به شکل ذیل تعریف مینمائیم .

$$\varphi(g): G \longrightarrow G$$
$$a \longmapsto g\,.ag^{-1}$$

باید ثبوت شود که $\varphi(g)$ یك G-Autom است .

$\boldsymbol{\varphi(g)}$ یك **G-Hom** است :

$a, b \in G$

$\varphi(g)(ab) = g\,a\,b\,g^{-1} = g.ag^{-1}$g . bg^{-1}

$= (gag^{-1}).(gbg^{-1})$

$=(\varphi(g)(a)).(\varphi(g)(b))$

$\Rightarrow \varphi(g)\ \ G - Hom$

$\boldsymbol{\varphi(g)}$ یک **injective** :

a$\in ker(\varphi(g)) \Rightarrow \varphi(g)(a) = e = g.a.g^{-1}$

$\Rightarrow g^{-1}.eg = a \ \Rightarrow \ a = e$

چون $ker(\varphi(g)) = \{\boldsymbol{e}\}$ است پس نظر به قضیه 2.3 تابع φ(g) یك injective است .

$\boldsymbol{\varphi(g)}$ یك **surjective** :

x$\in G$, $\varphi(g)(x) = g\,x\,g^{-1}; y := g\,x\,g^{-1} \ \Rightarrow x = g^{-1}$y g

$\varphi(g)(x) = \varphi(g)(g^{-1}y\,g) = g(g^{-1}y\,g)g^{-1} = e.y.e = y$

$\Rightarrow \varphi(g)\ \ surjective$

در نتیجه $\varphi(g) \in Aut\ G$. حالا ما ثبوت مینمائیم که $\boldsymbol{\varphi}$ یك G-Hom است .

g,h$\in G$

$\Rightarrow \forall\, a \in G\ ;\ \varphi(gh)(a) = (gh).a.(gh)^{-1}$

$= (gh).a.(h^{-1}\,g^{-1}) = g(h\,a\,h^{-1})g^{-1}$

$= \varphi(g)\ (hah^{-1}) = \varphi(g)\big(\varphi(h)(a)\big)$

$= \varphi(g)o\ \varphi\big(h(a)\big)$

$\Rightarrow \varphi(gh) = \varphi(g)o\ \varphi(h)$

ثبوت (b)

g$\in$ker$\varphi \Leftrightarrow \varphi(g) = id_G\ ,\ \varphi(g)(x) = x \quad \forall\, x \in G$

$\Leftrightarrow gxg^{-1} = x \quad \forall\, x \in G$

$$\Leftrightarrow gx = xg \quad \forall x \in G \qquad \Leftrightarrow g \in Z(G)$$

تعريف 3.16: (G ,.) يک گروپ و N يک گروپ فرعی نورمال (Normal) در G است. ما set (مجموعه) تمامی left-coset از N در G را به G/N نشان ميدهيم . يعنی:

$$G/N := \{a.N \mid a \epsilon G\}$$

G/N را G مودلو N (modulo) ميگويند .

قضيه 3.18 : (G ,.) يک گروپ و N يک گروپ فرعی نورمال در G است . بعدآ :

(a) G/N با رابطه دوگانه ذيل يک گروپ است :

$$.: G/N \; x \; G/N \rightarrow G/N$$
$$(aN, bN) \rightarrow (aN).(bN) = a.bN$$

(b) $|G/N|$ = [G:N]

(c) اگر ما بالای G و $(G/N, .)$ تابع ذيل را تعريف نمائيم :

$$\varphi: G \rightarrow G/N$$
$$a \mapsto a\,N$$

بعدآ :

(i) φ يک G-Hom و surjective است .

(ii) $ker\varphi = N$

ثبوت (a): چون N يک گروپ فرعی نورمال است ، پس برای $a, b \in G$:

$$aN = Na \quad \wedge \quad bN = Nb$$

$$\Rightarrow (aN).(bN) = a(Nb)N = a(bN)N = a.b\,NN$$

نظربه ليما 3.7 ميدانيم که $NN \subseteq N$ است. ازجانب ديگر:

$$n \epsilon N \Rightarrow n = e.n \epsilon NN \Rightarrow N \subseteq NN$$

درنتيجه N.N = N است

$$(a\,N).(b\,N) = a\,b\,N\,N = a\,b\,N \epsilon G\,/\,N$$

پس $(G/N, .)$ يک ساختمانی الجبری دارد

از طرف ديگر

$$N(a\,N) = a\,NN = a\,N$$
$$(a^{-1}N)(a\,N) = a^{-1}(Na\,N) = a^{-1}(aN) = (a.a^{-1})N = e\,.\,N = N$$

از اين نتيجه ميشود که G/N دارای عينيت N و معکوس aN عنصر $a^{-1}N$ است

خاصیت اتحادی صدق میکند. زیرا برای $a,b,c \in G$

$$(a\,N).(b\,N\,.cN) = (a\,N)\,(b(Nc).N = (aN)b(cN).N$$
$$= (aN)(bc)N.N = (a\,N)(b\,c\,N)$$
$$= a(N\,b\,c)N = a.(b\,c\,NN)$$
$$= (a\,b\,c)N.N = a\,b\,c\,N$$
$$(aN\,.bN).cN = (a(Nb)N).cN = (abN.N).cN$$
$$= (abN).cN = ab(Nc).N = ab(cN).N$$
$$= (abc)\,NN = abcN$$

G/N بنام گروپ فکتوری (factor group) از G نظر به N یاد میشود .

ثبوت (b): نظر به تعریف [G:N] صدق میکند .

ثبوت (c) (i):

$$a,b \in G\ ;\ \varphi(ab) = a\,b\,N = (aN)(bN)$$
$$= \varphi(a)\,.\varphi\,(b) \Rightarrow \varphi \quad G-Hom \Rightarrow \quad (i)$$

φ (a)=aN : surjective φ این معنی را دارد که هر Left-coset به حیث نقش (یاتصویر) تحت φ می آید .

ثبوت (c) (ii):

$$a\epsilon\, ker\varphi \Rightarrow \varphi(a) = N \ \wedge\ \varphi(a) = a.N$$
$$\Rightarrow N = a\,N \Rightarrow a \in N \quad \text{[نظر به قضیه 3.11]}$$
$$\Rightarrow ker\,\varphi \subseteq N$$

$$a\epsilon N \Rightarrow N = a\,N = \varphi(a) \Rightarrow a \in ker\,\varphi \Rightarrow N \subseteq ker\,\varphi$$

در نتیجه $ker\,\varphi = N$. φ بنام canonical Epimorphysm یاد میشود .

مثال 3.9 : مادرگروپ D_4 دیدیم که مرکز (center) آن مساوي به {e,b} است .

یعني $Z(D_4)=\{e,b\}$

چون $Z(D_4)$ نورمال نیز است ،پس میتوانیم فکتور گروپ (factor group) آنرا (یعني $D_4/\ Z(D_4)$) نظر به قضیه گذشته تشکیل دهیم . به این معني که تمامي left-coset هاي $Z(D_4)$ نظر به D_4 را در نظر میگیریم .

$E:= Z(D_4) =\{e,b\}$

$A:= Z(D_4)\ .\ a = \{e,b\}\ .a = \{a\ ,\ ba\ \}=\{a\ ,\ c\}$

$= Z(D_4)\ .c\ = \{a\ ,c\ \}$

$B:= Z(D_4)\ .\ d =\{e,b\ \}\ .\ d = \{d\ ,\ bd\}= \{d\ ,g\ \}$

$= Z(D_4) . g = \{ g,d\}$

$C:= Z(D_4) . f = \{e,b\} .f = \{f , bf \}= \{ f ,h\}$

$= Z(D_4).h = \{h , f \}$

تعداد left-coset در گروپ D_4 نظر به $Z(D_4)$ چهار است. پس فکتور گروپ ان $D_4/ Z(D_4)=\{ E ,A , B , C \}$ و $E= Z(D_4)$ عنصرعینیت ان است

$$\left|{}^{D_4}/_{Z(D_4)}\right| = [D_4 : Z(D_4)] = 4$$

جدول کیلی ان شکل ذیل را دارد:

	E	A	B	C
E	E	A	B	C
A	A	E	C	B
B	B	C	E	A
C	C	B	A	E

در جدول فوق بطور مثال :

$$A.B = Z(D_4).a \;\; Z(D_4) . d = (Z(D_4)).(Z(D_4))a.d$$

$$= Z(D_4)\, a.d \;\; = Z(D_4) . f = C$$

$$A.A \;= Z(D_4).a.Z(D_4) . a \;= Z(D_4).Z(D_4).a.a$$

$$= Z(D_4) . b = Z(D_4) = E$$ [نظربه قصیه 3.11]

تمرین 3.18 : ماگروپ فرعی نورمال $N:= \{e,a,b,c\}$ رادر گروپ $(D_4,.)$ درنظرمیگیریم

(a) گروپ فکتوری (Factor Group) $(G/N\ ,.)$ رادریافت نماید

(b) گروپ G/N را به شکل جدول کیلی (cayley table) نشان دهید

تمرین 3.19: ما گروپ $(Q_8,.)$ رابه G نشان میدهیم

(a) ثبوت نماید که $Z(G) = \{e,a\}$ است

(b) تمامی left-coset های G نظربه Z(G) رادریافت نماید

(c) ثبوت نماید که:

$G = Z(G) \cup Z(G).b \cup Z(G).d \cup Z(G).g$

(d) G/Z(G) را دریافت نماید وبه جدول کیلی انرا نشان دهید

لیما 3.11 :

(1) تقاطع گروپ های فرعی نورمال پس یک گروپ فرعی نورمال است.

(2) $(G,.)$ یک گروپ و U یک گروپ فرعی و N گروپ فرعی نورمال در G است. بعدآ:

(a) UN گروپ فرعی در G است

(b) $U \cap N$ نورمال در U است (یعنی: $U \cap N \trianglelefteq U$)

(c) N نورمال در UN است (یعنی: $N \trianglelefteq UN$)

ثبوت (1) : اگر ما یک گروپ $(G, .)$ دارای عنصرعینیت e داشته باشیم که $(i \in I := \{1,2,\ldots,n\})$ Ni نورمال در G باشند.

$$N := \cap_{i \in I} N_i$$

ما ثبوت می نمائیم که N نورمال در G است . در لیما 3.2 ثبوت کردیم که N یک گروپ فرعی است

$a \in G$

$g \in a\,N$

$\Rightarrow \exists\, h \in N\,;\; g = a.h \Rightarrow a.h \in a\,N_i \quad (\forall\, i \in I)$

$\Rightarrow a.h = h.a \in N_i.a \quad (\forall\, i \in I)$ [زیرا Ni نورمال اند]

$\Rightarrow a.N \subseteq N.a$

به همین شکل میتوان ثبوت کرد که $N.a \subseteq a.N$ است

در نتیجه $a.N = N.a$ میباشد. پس N نورمال در G است .

ثبوت (2) :

: (a)

$$X, y \in UN \implies \exists\, a_1, a_2 \in U \ \wedge\ \exists\, b_1, b_2 \in N\ ;\ \ x = a_1.b_1 \ \wedge\ y = a_2.b_2$$

$$\implies \mathrm{x.y} = a_1.b_1.a_2.b_2 = a_1.a_2.b_1.b_2$$ [زيرا N نورمال]

چون N و U گروپ های فرعی اند، پس:

$$a_1.a_2 \in U \ \wedge\ b_1.b_2 \in N \implies \mathrm{x.y} \in UN$$

$$x = a_1.b_1 \implies x^{-1} = (a_1.b_1)^{-1} = {b_1}^{-1}.{a_1}^{-1} = {a_1}^{-1}.{b_1}^{-1}$$

[زيرا N نورمال]

چون N و U گروپ های فرعی اند، پس:

$${a_1}^{-1} \in U \ \wedge\ {b_1}^{-1} \in N \implies x^{-1} = {a_1}^{-1}.{b_1}^{-1} \in UN$$

درنتیجه UN نظر به قضیه 3.1 گروپ فرعی در G است.

(b) : مامیدانیم که $\mathrm{U} \cap \mathrm{N}$ یک گروپ فرعی در U است.

نظر به لیما 3.6 باید ثبوت شود:

$$\forall a \epsilon U \implies a.\mathrm{U} \cap \mathrm{N}\, a^{-1} \subseteq \mathrm{U} \cap \mathrm{N}$$

$$\mathrm{a}\epsilon\mathrm{U}\ ,\ \ \mathrm{x}\epsilon\ a.\mathrm{U} \cap \mathrm{N}\, a^{-1}$$

$$\implies \exists\, b \epsilon \mathrm{U} \cap \mathrm{N}\ ;\ \mathrm{x} = a.b\, a^{-1} = b\,\mathrm{a}.a^{-1} = \mathrm{b}$$ [زيرا N نورمال و $b \in N$]

$$\implies \mathrm{x}\,\epsilon \mathrm{U} \cap \mathrm{N} \implies a.\mathrm{U} \cap \mathrm{N}\, a^{-1} \subseteq \mathrm{U} \cap \mathrm{N}$$

ثبوت شد که $\mathrm{U} \cap \mathrm{N}$ نورمال در U است.

(c) : نظر به لیما 3.6 باید ثبوت شود:

$$\forall x \epsilon UN \implies x.\mathrm{N}\, x^{-1} \subseteq \mathrm{N}$$

$$\mathrm{x}\epsilon\mathrm{UN}\ ,\ \ \mathrm{y}\epsilon\ x.\mathrm{N}\, x^{-1}$$

$$\implies (\exists\, a \epsilon \mathrm{U}, \mathrm{b}\epsilon\mathrm{N}\ ;\ \mathrm{x} = a.b\ ) \wedge (\exists\, s \epsilon \mathrm{N}\ ;\ \mathrm{y} = x.\mathrm{s}\, x^{-1}$$

$$\implies \mathrm{y} = x.\mathrm{s}\, x^{-1} = a.b.s.(ab)^{-1} = \mathrm{a.b.s.b}^{-1}.\mathrm{a}^{-1}$$

$$= \mathrm{a.b.}\ \mathrm{b}^{-1}.\mathrm{a}^{-1}.\mathrm{s}$$ [زيرا N نورمال و $s \in N$]

$$= \mathrm{a.e.a}^{-1}.\mathrm{s} = \mathrm{e.s} = s \in N$$

$$\implies x.\mathrm{N}\, x^{-1} \subseteq \mathrm{N}$$

ثبوت شد که N نورمال در UN است.

قضيه 3.19 : (Theorem of group homomorphism)
(G,.) و (G_1 ,*) دوگروپ داراي عناصرعينيت $e \in G$, $e_1 \in G_1$ و
$\varphi: G \to G_1$ يك G-Hom است. بعدآ تابع ذيل يک G-Isom است.

$$\varphi^- : G/ker\varphi \to \varphi(G)$$
$$a.ker\varphi \to \varphi(a)$$

يعنى گروپ فكتورى $G/ker\varphi$ و گروپ $\varphi(G)$ نظر φ^- بايكديگر ايزومورف (Isomorph) اند (يعنى: $G/ker\varphi \cong \varphi(G)$)

ثبوت : نظر به قضيه 3.15 ميدانيم كه $ker\varphi$ يك گروپ فرعي نورمال وهم چنان $\varphi(G)$ نظر به 3.3 يك گروپ فرعي است . پس لهذا تعريف φ^- درست است.
a,b∈ G

$$a.ker\varphi\ , b.ker\varphi \in G/ker\varphi$$

$$\varphi^-(a.ker\varphi) = \varphi^-(b.ker\varphi) \Rightarrow \varphi(a) = \varphi(b)$$

$$\Rightarrow \varphi(a) = \varphi(b) * e_1 \Rightarrow \varphi(b)^{-1} * \varphi(a) = e_1$$

$$\Rightarrow \varphi(b)^{-1} * \varphi(a) = \varphi(b^{-1}.a) = e_1 \Rightarrow b^{-1}.a \in ker\,\varphi$$

$$\Rightarrow a.\ker\varphi = b.ker\varphi \quad [\text{نظر به قضيه } 3.11]$$

$$\Rightarrow \varphi^- \quad injective$$

نظر به تعريف φ^- ميتوان نوشت كه $\varphi^-(G/ker\varphi) = \varphi(G)$ است.

درنتيجه φ^- هم surjective است .

φ^- يک G-Hom :
چون $ker\varphi$ نورمال است. پس ميتوان نوشت:

$$\varphi^-\big((a.ker\varphi).(b\ ker\varphi)\big) = \varphi^-\big(ab\ (ker\varphi.ker\varphi)\big)$$
$$= \varphi^-(abker\varphi)$$
$$= \varphi(a.b) = \varphi(a) * \varphi(b)$$

$\Rightarrow \varphi^-$ G-Hom

در نتيجه φ^- يک G_Isom است. يعنى $G/\ker\varphi \cong \varphi(G)$

قضیه 3.19-A : (theorem of group isomomorphism)
(G ,.) یک گروپ ، U یک گروپ فرعی و N گروپ فرعی نورمال در G است.
بعدآ $U/\mathrm{U}\cap\mathrm{N}$ و UN/N باهم دیگر گروپ ایزومورف اند. یعنی:

$$UN/\mathrm{N} \cong U/\mathrm{U}\cap\mathrm{N}$$

ثبوت: نظربه قضیه 3.18 تابع ذیل نیز G-Hom است:

$$\varphi: U \longrightarrow G/N$$
$$a \longmapsto a\,N$$

$$\varphi(U) = \{\,\mathrm{uN}\,|\mathrm{u}\in\mathrm{U}\,\}$$
$$= \{\,\mathrm{uvN}\,|\mathrm{u}\in\mathrm{U},\mathrm{v}\in\mathrm{N}\}\quad [\text{نظر به قضیه } 3.11\ ]$$
$$= UN/\mathrm{N}\qquad [\varphi \text{ نظر به تعریف }]$$

$$\mathrm{u}\in\ker\varphi \implies \mathrm{u}\in\mathrm{U}\ \wedge\ \mathrm{N} = \varphi(u) = uN$$
$$\implies \mathrm{u}\in\mathrm{N}\quad [\text{نظر به قضیه } 3.11\ ]$$
$$\implies \mathrm{u}\in\mathrm{U}\cap\mathrm{N}$$
$$\mathrm{u}\in\mathrm{U}\cap\mathrm{N} \implies \mathrm{u}\in\mathrm{U}\ \wedge\ \mathrm{u}\in\mathrm{N} \implies \varphi(u) = uN = N$$
$$\implies \mathrm{u}\in\ker\varphi$$

درنتیجه: $\ker\varphi = \mathrm{U}\cap\mathrm{N}$
نظربه قضیه 3.19 تابع ذیل G-Isom است:

$$\varphi^{-}: G/ker\varphi \longrightarrow \varphi(G)$$
$$\mathrm{a}.\ker\varphi \longmapsto \varphi(a)$$

درلیما3.11 ثبوت شد که UN گرپ فرعی در G ، N نورمال در UN و $\mathrm{U}\cap\mathrm{N}$ نورمال در U است. علاوه بران $\varphi(U) = UN/\mathrm{N}$ و $\ker\varphi = \mathrm{U}\cap\mathrm{N}$ است.
پس قضیه 3.19 بالای گرپ فرعی U نیز صدق میکند. یعنی تابع ذیل یک G-Isom است

$$\varphi^{-}: U/\mathrm{U}\cap\mathrm{N} \longrightarrow \varphi(U)$$
$$\mathrm{a}.\ker\varphi \longmapsto \varphi(a)$$

چون $\varphi(U) \cong U/\mathrm{U}\cap\mathrm{N}$ و $\varphi(U) = UN/\mathrm{N}$ است. درنتیجه:

$$UN/\mathrm{N} \cong U/\mathrm{U}\cap\mathrm{N}$$

یاداشت : مامیدانیم که برای $n \in \mathbb{N}$ سیت $n\mathbb{Z} = \{n.k \mid k \in \mathbb{Z}\}$ یك گروپ فرعي از $(\mathbb{Z}, +)$ است . چون $(\mathbb{Z}, +)$ یك گروپ تبدیلي (Commutative) است پس $n\mathbb{Z}$ یك گروپ فرعي نورمال است .

تعریف 3.17 : $a \in \mathbb{Z}$, $0 \neq n \in \mathbb{N}$

$a + n\mathbb{Z} := \{a + nk \mid k \in \mathbb{Z}\}$

$a + n\mathbb{Z}$ رابنام کلاس باقیمانده (congruence class) یا (residue class) از a نظر به مودول(modulo) n یاد میشود .

اگردوعدد $a, b \in \mathbb{Z}$ درعین کلاس باقیمانده باشند. یعنی $a+n\mathbb{Z} = b+n\mathbb{Z}$ ، در آنصورت a را congrouent به b نظربه مودولو (modulo) n یاد میکند وبه شکل $a \equiv b \pmod n$ نوشته میشود .

بصورت عموم میتوان گفت که اگر یک عدد a تقسیم بر n شود و r باقي بماند آنرا بشکل modulo طوري مینویسند: $0 \le r < n$ $a \equiv r \pmod n$

ما کلاس های باقیمانده $a \in \mathbb{Z}$ (residue class or congruence class) نظر به مودولو (modulo) n را به $\bar{a}$ نشان میدهیم . یعنی :

$\bar{a} = a + n\mathbb{Z} = \{a+nk \mid k \in \mathbb{Z}\}$

مثال:

$8 \bmod 3 : \quad 8 = 2.3 + 2 \Rightarrow 8 \bmod 3 = 2$

$\Rightarrow 8 \equiv 2 \pmod 3$

$-8 \bmod 3 : \quad -8 = (-3).3 + 1 \Rightarrow -8 \bmod 3 = 1$

$\Rightarrow -8 \equiv 1 \pmod 3$

$18 \bmod 5: \quad 18 = 3.5 + 3 \Rightarrow 18 \bmod 5 = 3$

$\Rightarrow 18 \equiv 3 \pmod 5$

$-18 \bmod 5: \quad -18 = (-4).5 + 2 \Rightarrow -18 \bmod 5 = 2$

$\Rightarrow -18 \equiv 2 \pmod 5$

$14 \equiv 2 \pmod 6$, $12 \equiv 0 \pmod 6$,

$13 \equiv 3 \pmod 5$, $26 \equiv 1 \pmod 5$

لیما 3.12 : برای $a, b \in \mathbb{Z}$ و $0 \neq n \in \mathbb{N}$ افادهای ذیل بایکدیگرمعادل اند

(1) $a \equiv b \pmod n$

(2) $a + n\mathbb{Z} = b + n\mathbb{Z}$

(3) $a - b \in n\mathbb{Z}$

(4) اگر a,b ذریعه n تقسیم شود باقیمانده مساوی دارند. یعنی

$a = q_1.n + r_1 \quad \wedge \quad b = q_2.n + r_2 \implies r_1 = r_2$

ثبوت:

(1) $\Leftarrow$ (2) : میخواهیم ثبوت نمایم که $a + n\mathbb{Z} = b + n\mathbb{Z}$ است

$h \in a + n\mathbb{Z} \implies \exists\ k \in \mathbb{Z}\ ;\ h = a + k.n$

ازجانب دیگر:

$a \equiv b\ (mod\ n) \implies \exists\ q \in \mathbb{Z}\ ;\ a = q.n + b$

پس

$h = a + k.n = q.n + b + k.n = b + (q+k).n \in (b + n\mathbb{Z})$

$\implies a + n\mathbb{Z} \subseteq b + n\mathbb{Z}$

به همین ترتیت میتوان ثبوت نمود که $b + n\mathbb{Z} \subseteq a + n\mathbb{Z}$

(2) $\Leftarrow$ (1) :

$a + n\mathbb{Z} = b + n\mathbb{Z} \implies \exists\ q_1, q_2 \in \mathbb{Z}\ ;\ a + q_1.n = b + q_2.n$

$\implies a = (q_2 - q_1)n + b$

$\implies a \equiv b\ (mod\ n)$

(3) $\Leftarrow$ (2) :

$h \in a + n\mathbb{Z} = b + n\mathbb{Z}$

$\implies \exists\ q_1, q_2 \in \mathbb{Z}\ ;\ h = a + q_1.n = b + q_2.n$

$\implies a - b = q_2.n - q_1.n = (q_2 - q_1)n \in n\mathbb{Z}$

(2) $\Leftarrow$ (3) :

$h \in a + n\mathbb{Z} \implies \exists\ q \in \mathbb{Z}\ ;\ h = a + q.n$

ازجانب دیگر:

$a - b \in n\mathbb{Z} \implies \exists\ k \in \mathbb{Z}\ ;\ a - b = k.n \implies a = b + k.n$

$\implies h = a + q.n = b + k.n + q.n$

$= b + (k+q).n \in b + n\mathbb{Z}$

$\implies a + n\mathbb{Z} \subseteq b + n\mathbb{Z}$

به همین ترتیت میتوان ثبوت نمود که $b + n\mathbb{Z} \subseteq a + n\mathbb{Z}$ است. پس

$b + n\mathbb{Z} = a + n\mathbb{Z} \implies (2)$

(4) $\Leftarrow$ (1) :

$a \equiv b\ (mod\ n) \implies \exists\ q \in \mathbb{Z}\ ;\ a = qn + b$

ازجانب دیگر چون $b < n$ است. پس $b = 0.n + b$ است. دیده میشود که a و b باقیمانده مساوی دارند

به همین شکل میتوان افادهای دیگررا ثبوت نمود
ست تمامی کلاس های باقیمانده (residue class) $\mathbb{Z}$ مودلو (modulo) n را به $\mathbb{Z} / n\mathbb{Z}$ ویا $\mathbb{Z}_n$ نشان میدهند . یعني :

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{\bar{a} \mid a \in \mathbb{Z}\}$$

$\mathbb{Z}_n$ به تعداد n کلاس های باقیمانده (residue class) مختلف دارد .

$\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \}$, $|\mathbb{Z}_n| = n$

در بعضی کتاب ها کلاس باقیمانده (residue class) را به شکل ذیل نیز نوشته میکنند :

$[a]_n = \{a \epsilon \mathbb{Z} \mid a \equiv b \ (mod\ n)\}$

$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots [n-1]_n\}$

$= \{a \epsilon \mathbb{Z} \mid a \equiv b \ (mod\ n)\}$ [a]

ویا

$\mathbb{Z}_n = \{[0], [1], [2], \ldots [n-1]\}$

بطور مثال $\mathbb{Z}_3 = \{ [0]_3, [1]_3, [2]_3 \}$
اگرما کلاس های باقیمانده (residue class) a را به $\bar{a}$ نشان دهیم.
درانصورت عناصر کلاس های باقیمانده از $\mathbb{Z}_3$ عبارت اند از :

$\bar{0} = \{ \ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots \}$

$\bar{1} = \{ \ldots, -14, -11, -8, -5, -2, 1, 4, 7, 10, 14, \ldots \}$

$\bar{2} = \{ \ldots, -13, -10, -7, -4, -1, 5, 8, 11, 14, 17, \ldots \}$

قضیه 3.20 : $\mathbb{Z}_n$ نظر به رابطه دوگانه ذیل یک گروپ دورانی (cyclic group) است .

$+: \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$(a + nZ, b + n\mathbb{Z}) \longmapsto (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a+b) + n\mathbb{Z}$

ویا

$$(\bar{a}, \bar{b}) \longmapsto \bar{a} + \bar{b} = \overline{a + b}$$

نظر به قضیه (3.18) $(\mathbb{Z}_n, +)$ یک گروپ است . عنصر عینیت ویا خنثی آن $\bar{0} = n\mathbb{Z}$ ومعکوس $\bar{a}=a+n\mathbb{Z}$ عبارت است از $-\bar{a}= -a +n\mathbb{Z}$

گروپ فکتوری $(\mathbb{Z}_n , +)$ بنام residue class group (گروپ کلاس باقیمانده) مودولو n یاد میشود. $\bar{1} = 1 + n\mathbb{Z} \in \mathbb{Z}_n$ یک عنصر مولد از $\mathbb{Z}_n$ است. نظربه لیما 3.7 و قضیه 3.18 میتوان نوشت:

$n\mathbb{Z} = n\mathbb{Z} + n\mathbb{Z} + ...+ n\mathbb{Z} = k.n\mathbb{Z}$ ((دفعه k)

$\mathbb{Z}_n$ = { k+ $n\mathbb{Z}$ | k ∈ $\mathbb{Z}$ } = { k+k.$\boldsymbol{n}\mathbb{Z}$ | k ∈ $\mathbb{Z}$ }]

={ k.(1+ $n\mathbb{Z}$) | k ∈ $\mathbb{Z}$ }

$= \{ k.\bar{1} \mid k \in \mathbb{Z} \} = < \bar{1} >$

در نتیجه $(\mathbb{Z}_n , +)$ یک گروپ دورانی (cyclic) است و

$$ord(< \bar{1} >) = |\mathbb{Z}_n| = n$$

مثال 3.10 : ما گروپ $(\mathbb{Z}_6 , +)$ را در نظر میگیریم . درین گروپ $ord(\mathbb{Z}_6) = |\mathbb{Z}_6| = 6$ ورابطه دوگانه "+" بالای $\mathbb{Z}_6$ را در جدول cayley نشان میدهیم .

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

عنصرعینیت ان $\bar{0} = 6\mathbb{Z}$ وبطورمثال $\mathbb{Z}$ 6+2=$\bar{2}$- معکوس از $\mathbb{Z}$ 6+2= $\bar{2}$ است . زیرا :

$$\bar{2} + (-\bar{2}) = (2 + 6\mathbb{Z}) + (-2 + 6\mathbb{Z}) = 2 + (-2) + 6\mathbb{Z} + 6\mathbb{Z}$$
$$= 0 + 6\,\mathbb{Z} + 6\,\mathbb{Z} = 6\,\mathbb{Z} = \bar{0}$$

دیده میشود که $(\mathbb{Z}_6 , +)$ یک گروپ تبدیلی (commutative) است .

نوت : میخوهیم تشریح نمایم که چطور $\bar{4} = -\bar{2}$ است

$\bar{4} + \bar{2} = \bar{6} = \bar{0} \Rightarrow \bar{4} = \bar{0} - \bar{2} = -\bar{2}$

برای تشریح بیشتر جدول بطور مثال اگر کلاس های باقیمانده (residue class) $\bar{4}$, $\bar{5}$ ر ا مطالعه می نمائیم .

$\bar{4} + \bar{5} = \bar{9} = \bar{6} + \bar{3} = \bar{0} + \bar{3} = \bar{3}$

$\bar{2} + \bar{5} = \bar{7} = \bar{6} + \bar{1} = \bar{0} + \bar{1} = \bar{1}$

درجدول چون $\bar{2} + \bar{4} = \bar{0}$ و $\bar{1} + \bar{5} = \bar{0}$ است پس $\bar{2}$و$\bar{4}$ معکوس یک دیگروهم چنان $\bar{1}$و$\bar{5}$ معکوس یک دیگر اند

$H:=\{\bar{0}, \bar{3}\}$ گروپ فرعی آن است. چون $(\mathbb{Z}_6, +)$ یک گروپ تبدیلی است پس H یک گروپ فرعی نورمال است . حالا coset های $(\mathbb{Z}_6)$ نظر به H را تحت مطالعه قرار میدهیم .

$U_0 = \bar{0} + H = \{\bar{0}, \bar{3}\}$

$U_1 = \bar{1} + H = \bar{1} + \{\bar{0}, \bar{3}\} = \{\bar{1}, \bar{4}\}$

$U_2 = \bar{2} + H = \bar{2} + \{\bar{0}, \bar{3}\} = \{\bar{2}, \bar{5}\}$

$\bar{3} + H = \bar{3} + \{\bar{0}, \bar{3}\} = \{\bar{3}, \bar{0}\} = H = U_0$

$\bar{4} + H = \bar{4} + \{\bar{0}, \bar{3}\} = \{\bar{4}, \bar{1}\} = \bar{1} + H = U_1$

$\bar{5} + H = \bar{5} + \{\bar{0}, \bar{3}\} = \{\bar{5}, \bar{2}\} = \bar{2} + H = U_2$

دیده میشود که تعداد کوسیت (coset) های $\mathbb{Z}_6$ نظر به H مساوی به 3 هستند.

یعنی انها U_0, U_1, U_2 اند . اگر ما $G := (\mathbb{Z}_6, +)$ نام گذاری نمایم . بعدآ

$G/H = \{H, \bar{1} + H, \bar{2} + H\} = \{U_0, U_1, U_2\}$

$ind(H) = 3$

مثال 3.11: جدول ذیل نشان میدهد که $(\mathbb{Z}_7^*, .)$ یک گروپ است و کلاس های باقیما نده ان عبارت اند از :

$Z_7^* = \{[1], [2], [3], [4], [5], [6]\} \wedge |Z_7^*| = 6$

$[1] = 1 + 7\mathbb{Z}$

$[2] = 2 + 7\mathbb{Z}$

$[6] = 6 + 7\mathbb{Z}$

.	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

.

دیده میشود که عنصر عینیت آن کلاس باقیمانده $[1]$ است .
برای تشریح جدول

$[4].[5] = [20] = [2].[7] + [6] = [2].[0] + [6] = [6]$
$[3].[6] = [18] = [2].[7] + [4] = [4]$

عناصر معکوس : بطور مثال
$[2]$ و $[4]$ معکوس یکدیگر اند زیرا $[4].[2] = [8] = [7] + [1] = [1]$ و $[6]$ معکوس خودش است. زیرا $[6].[6] = [36] = [5].[7] + 1 = [1]$
بصورت خلاصه هرجایکه در جدول حاصل ضرب دو عنصر $[1]$ با شد این دو عنصر معکوس یکدیگر اند . ما $G := (\mathbb{Z}_7^*, .)$ وضع می نمائیم
$H:=\{[1],[2],[4]\}$ گروپ فرعی از G است زیرا :
(i) رابطه دوگانه "." بالای H قابل تطبیق است زیرا

$[1].[1] = [1] \in H$, $[1].[2] = [2] \in H$, $[1].[4] = [4] \in H$

$[2].[4] = [8] = [1] \in H$, $[4].[4] = [16] = [2] \in H$

(ii) $[1] \in H$
(iii) $[4]$ و $[2]$ معکوس یکدیگر اند
(iV) چون $H \subseteq G$ است پس خواص اتحادی (Assosiative) نیزصدق میکند .

حالا تمامی کوسیت ها (cosets) از $\mathbb{Z}_7^*$ نظر به H را تحت مطالعه قرار میدهیم .

$[3].H = [3].\{[1],[2],[4]\} = \{[3],[6],[12]\}$
$= \{[3],[6],[5]\}$
$[5].H = [5].\{[1],[2],[4]\} = \{[5],[10],[20]\}$
$= \{[5],[3],[6]\}$
$[6].H = [6].\{[1],[2],[4]\} = \{[6],[12],[24]\}$
$= \{[6],[5],[3]\}$

دیده میشود که $H.H = [6].H = [5].[3]$ است . پس:
$ind(H) = 2$, $\{H, 3H\} = \mathbb{Z}_7^*/H$

اگر قضیه Lagrange را تطبیق نمائیم :

$|Z_7^*| = ord(H).ind(H) \Rightarrow 6 = 3.ind(H)$

$$\Rightarrow \text{ind (H)} = \frac{6}{3} = 2$$

تمرين 3.20: درگروپ $(Z_7^*, .)$ مرتبه [3] [4] و[6] چند است . یعنی ord([3]), ord([4]) و ord([6]) را پیدا نماید

قضیه 3.21 : اگر رابطه دوگانه (binary operation) ذیل بالای $\mathbb{Z}_n$ در نظر گرفته شود :

$$\cdot : \mathbb{Z}_n \; x \; \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$
$$(a + n\mathbb{Z}, b + n\mathbb{Z}) \longmapsto (a + n\mathbb{Z}).(b + n\mathbb{Z}) := ab + n\mathbb{Z}$$

به شکل مختصر آنرا میتوان $\overline{a}.\overline{b} = \overline{a.b}$ نوشت در صورتیکه:

$\overline{a} := a + n\mathbb{Z}$ و $\overline{b} := b + n\mathbb{Z}$ وضع شود . بعداً :

(a) $(\mathbb{Z}_n, .)$ یک semigroup است .

(b) $(\mathbb{Z}_n{}^*, .)$ یک گروپ است در صورتیکه n یک عدد اولیه باشد .

ثبوت :

(a) باید ثبوت شود :

(i) $\overline{a} = \overline{a_1} \; \wedge \; \overline{b} = \overline{b_1} \Rightarrow \overline{a_1 b_1} = \overline{ab} \quad (\overline{a}, \overline{b}, \overline{a_1}, \overline{b_1} \in \mathbb{Z}_n)$

(ii) $\forall \overline{a}, \overline{b} \in \mathbb{Z}_n \Rightarrow \overline{ab} \in \mathbb{Z}_n$

(iii) $associativity$ (اتحادی)

ثبوت (i)

$\overline{a} = \overline{a_1} \; \wedge \; \overline{b} = \overline{b_1}$

$\Rightarrow a + n\mathbb{Z} = a_1 + n\mathbb{Z} \; \wedge \; b + n\mathbb{Z} = b_1 + n\mathbb{Z}$

$\Rightarrow a_1 - a \in n\mathbb{Z} \; \wedge \; b_1 - b \in n\mathbb{Z}$ [3.12 لیما]

$\Rightarrow a_1 - a \,|\, n \; \wedge \; b_1 - b \,|\, n$

$\Rightarrow \exists r, s \in \mathbb{Z} \; ; \; a_1 - a = nr \; \wedge \; b_1 - b = ns$

$\Rightarrow a_1 = a + nr \; \wedge \; b_1 = b + ns$

$\Rightarrow a_1 b_1 = (a + nr)(b + ns)$

$= ab + n(br + as + nrs)$

$\Rightarrow \overline{a_1 b_1} = \overline{ab + n(br + as + nrs)} = \overline{ab} + \overline{0} = \overline{ab}$

ثبوت (ii)

$\bar{a} = a + n\mathbb{Z}, \bar{b} = b + n\mathbb{Z} \in \mathbb{Z}_n$
$\Rightarrow a, b \in \{0,1,2, \dots, n-1\}$

حالت اول : اگر a.b < n باشد در آنصورت واضح است که $\overline{ab} \in \mathbb{Z}_n$ است

حالت دوم : اگر $a.b \geq n$ باشد در انصورت:

$ab \geq n$
$\Rightarrow \exists q, r \in \mathbb{N}; ab = nq + r \quad 0 \leq r < n \; [division\ algorithm]$

$\Rightarrow \overline{ab} = \overline{nq + r} = \overline{nq} + \bar{r} = \bar{0} + \bar{r} = \bar{r}$

$\Rightarrow \overline{ab} \in \mathbb{Z}_n \qquad [0 \leq r \leq n]$

ثبوت :(iii)

$\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$
$\bar{a}.(\bar{b}.\bar{c}) = \bar{a}.\overline{bc} = \overline{a.b.c} = \overline{ab}.\bar{c} = (\bar{a}.\bar{b}).\bar{c}$

ثبوت (b) : ما فرض میکنیم که n یک عدد اولیه است .

$\mathbb{Z}_n^* = \{\bar{1}, \overline{2}.\bar{3}, \dots, \overline{n-1})$
$\bar{a} \in \mathbb{Z}_n^* \Rightarrow a \in \{1,2, \dots, n-1\}$
$\Rightarrow gcd(a,n) = 1$ [زیـرا n عدد اولـیـه]
$\Rightarrow \exists r, s \in \mathbb{Z}; ar + ns = 1$ $[Euclidean\ algorithm]$
$\Rightarrow \bar{1} = \overline{ra + ns} = \overline{ra} + \overline{ns} = \bar{r}.\bar{a} + \bar{0}.\bar{s} = \bar{r}.\bar{a}$

پس دیده شد که $\bar{r}$ معکوس از $\bar{a}$ است .
در نتیجه$(\mathbb{Z}_n^*, .)$ یک گروپ است در صورتیکه n یک عدد اولیه باشد
وعنصرعینیت ان $\bar{1} = 1 + n\mathbb{Z}$ است .

مثال : $(\mathbb{Z}_4^*, .)$ را در نظر میگیریم چون 4 یک عدد اولیه نیست لذا پس باید نظر به قضیه 3.21 گروپ نباشد .
دیده میشود که $\bar{2}.\bar{2} = \bar{0}$ و $\bar{0}$ یک عنصر از $(\mathbb{Z}_4^*, .)$ نیست واز جانب دیگر برای $\bar{2}$ عنصر معکوس موجود نیست . جدول کیلی ان شکل ذیل رادارد:

.	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

تمرين 3.21: كدام يكی از سيت های ذيل گروپ شده نميتواند

$(\mathbb{Z}_6^*,.)$, $(\mathbb{Z}_{11}^*,.)$, $(\mathbb{Z}_4,+)$ و $(\mathbb{Z}_{11},+)$

فصل چهارم

Direct product of groups

تعریف 4.1 : $(G_i, .)$گروپ اند که دارای عناصر عینیت $e_i \epsilon G_i$ هستند . $(i = 1,2, \dots, n)$. سیت G بطور ذیل تعریف شده است

$$G := G_1 \, x \, G_2 \, x \, G_3 \, x \, \dots x \, G_n$$
$$= \{(a_1 \, , a_2 \, , a_3 \dots . , a_n \,) \mid a_i \in G_i \;\; (i = 1,2,3, \dots , n)\}$$

G بنام cartesian product گروپ های G_i (i= 1,2,3, . . . ,n) یاد میشود ونظربه رابطه دوگانه (binary operation) ذیل یک گروپ است :

$$. : G \times G \longrightarrow G$$
$$(a,b) \longmapsto a \, . \, b$$

$$a = (a_1 \, , a_2 \, , a_3 \, , . \, . \, . \, , a_n \,)$$
$$b = (b_1 \, , b_2 \, , b_3 \, , . \, . \, . \, , b_n \,)$$
$$a \, . \, b \; = \; (a_1 \, . b_1 \, , \; a_2 \, . b_2 \, , \dots \, , a_n \, . b_n \,)$$

خاصیت اتحادی (associativity) :

$$a = (a_1 \, , a_2 \, , a_3 \, , . \, . \, . \, , a_n \,), \;\; b = (b_1 \, , b_2 \, , b_3 \, , . \, . \, . \, , b_n \,),$$
$$c = (c_1 \, , c_2 \, , c_3 \, , . \, . \, . \, , c_n \,)$$
$$(a \, . b) . c \; = [\; (a_1 \, , a_2 \, , \; \dots \; , a_n \,) . (b_1 \, , b_2 \, , . \, . \, . \, , b_n \,)]$$
$$. (c_1 \, , c_2 \, , . \, . \, . \, , c_n \,)$$
$$= (a_1 \, . b_1 \; , a_2 \, . b_2 \; , \; \dots \; , \; a_n \, . b_n \;)$$
$$. (c_1 \, , c_2 \, , \dots \; , c_n \,)$$

$$= (a_1 \;\; b_1 \;\; c_1 \;\; , a_2 \;\; b_2 \;\; c_2 \;\; , \; \dots \; , \; a_n \;\; b_n \;\; c_n \;)$$
$$= (a_1 \, , a_2 \, , a_3 \, , . \, . \, . \, , a_n \,)$$
$$. [\; (b_1 \, , b_2 \, , \dots \; , b_n \,) \; . (c_1 \, , c_2 \, , \dots \; , c_n \,)]$$
$$= \; a \, . (b . c)$$

عنصر عینیت (identity): $e = (e_1 \, , e_2 \, , \dots \; , e_n \,)$

عنصر معکوس (inverse):

از $a = (a_1 , a_2 , . . . , a_n)$ معکوس آن $a^{-1}=(a_1^{-1} , a_2^{-1} , \dots , a_n^{-1})$ است زیرا :

$$a . a^{-1} = (a_1 , a_2 , a_3 , . . . , a_n).(a_1^{-1} , a_2^{-1} , a_3^{-1} , \dots , a_n^{-1})$$
$$= (a_1 . a_1^{-1} , a_2 . a_2^{-1} , . . . , a_n . a_n^{-1})$$
$$= (e_1 , e_2 , \dots , e_n) = e$$

گروپی (G,.) بنام External direct product یاد میشود .

مثال 4.1 : $\{1 , -1\} = G_1 = G_2$ ومامیدانیم که $(G_1 , .)$ و $(G_2 , .)$ نظربه ضرب گروپ اند . که عنصر عینیت آن 1 و عنصر معکوس 1- خودش میباشد .

$$G = G_1 \ x \ G_2 = \{1, -1\} x \{1 , -1\}$$
$$= \{(1,1) , (1, -1) , (-1,1) , (-1, -1)\}$$

رابطه دوگانه (Binary operation) بالای گروپ G درجدول کیلی (cayley table) به طور ذیل دیده میشود .

.	(1 ,1)	(1 ,-1)	(-1 ,1)	(-1 ,-1)
(1 ,1)	(1 ,1)	(1 ,-1)	(-1 ,1)	(-1 ,-1)
(1 ,-1)	(1 ,-1)	(1 ,1)	(-1 ,-1)	(-1 ,1)
(-1 ,1)	(-1 ,1)	(-1 ,-1)	(1 ,1)	(1 ,-1)
(-1 ,-1)	(-1 ,-1)	(- 1 ,1)	(1 ,-1)	(1 ,1)

گروپ G یک External direct product (Ext – dir – prod) از G_1 و G_2 است که عنصرعینیت آن e = (1,1) و ord G = 4 است .

بصورت عموم میتوان گفت که اگر ما سه گروپ A , B و C داشته باشیم که ord A= 3 , ordB=5 و ordC=6 باشد و G=AxBxC . در اینصورت ordG = 3.5.6=90 است یعنی G دارای 90 عنصر میباشد .

مثال: ماگروپ های $(\mathbb{R}, +)$ و$(\mathbb{R}^*, .)$ رادر نظرمیگیریم

اگر $G := \mathbb{R}^* x \mathbb{R}$ باشد درانصورت G نظربه رابطه دوگانه ذیل یک گروپ ویک (Ext – dir – prod) از $\mathbb{R}$ و $\mathbb{R}^*$ است که عنصرعینت ان (1,0) میباشد.

$$* : G \times G \rightarrow G$$
$$(a,b) \longmapsto a*b$$

برای $a = (a_1,a_2)$, $b = (b_1, b_2) \epsilon G$ حاصل ان طوری ذیل است

$a*b = (a_1,a_2) * (b_1, b_2) = (a_1 . b_1, a_2+ b_2)$

$a^{-1} = (\frac{1}{a_1}, - a_2)$

بطورمثال اگر $a = (3,5), b = (2,4)$ باشد درانصورت

$a*b = (3,5) * (2,4) = (3.2,5+4) = (6,9)$ $\wedge$ $a^{-1} = (\frac{1}{3}, -5)$

تمرین 4.1 :

(1) ما گروپ های $A^{(4)}$, $A^{(2,2)}$ و D_4 را درنظرمیگریم و $G:= D_4 \times A^{(2,2)} \times A^{(4)}$ وضع مینمایم

(a) عنصر عینیت (identity) از G کدام است

(b) معکوس (inverse) از (c,b_4,a_3) را در G دریافت نماید

(c) G دارای چند عنصراست. یعنی $ordG = |G|$ رادریافت نماید

(d) چهار عنصررا در G دریافت نماید که معکوس شان خودشان باشند

(2) مامیدانیم که $(\mathbb{Z}_3, +)$ یک گروپ است. اگر $G:= \mathbb{Z}_3 \times \mathbb{Z}_3$ باشد درانصورت G یک Ext- dir – prod آن است .

(a) عنصر عینیت (identity) G کدام است

(b) معکوس (inverse) از $(\overline{1}, \overline{2})$ را در G پیدا نماید

(c) تعداد عناصرG چند است . یعنی $ordG = |G|$ رادریافت نماید

(d) گروپ G را در جدول Cayley نشان دهید

(3) ما گروپ های $(\mathbb{Z}_{11}, +)$ و $(\mathbb{Z}_{11}^{*}, .)$ راداریم

$G:= \mathbb{Z}_{11}^{*} \times \mathbb{Z}_{11}$

(a) عنصر عینیت (identity) از G کدام است

(b) $\bar{x}.\bar{y}$ ذیل را پیداکنید

$\bar{x} = (\bar{5}, \bar{6}) , \bar{y} = (\bar{4}, \bar{9}) \in G$

(c) تعداد عناصرG چند است . یعنی $ordG = |G|$ رادریافت نماید

تمرین 4. 2

$G_1 = \{1, -1 \subseteq \mathbb{R}, G_2 = \{1, -1, i, -i\} \subseteq \mathbb{C}$, $G: = G_1 \times G_2$

ما میدانیم که G_1 ، G_2 نظر به ضرب "." گروپ اند و $(G, .)$

Ext- dir – prod آن است . گروپ $(G , .)$ را نظر به رابطه دو گانه ان در جدول Cayley نشان دهید .

تمرين 4.3 : ماميدانيم كه $(\mathbb{Z}_2, +)$ يک گروپ است. اگر $G := \mathbb{Z}_2 \mathbf{x} \mathbb{Z}_2$ باشد درانصورت $(G, .)$ يک Ext- dir – prod آن است . گروپ بودن G را در جدول Cayley نشان دهيد

ليما 4.1 : $(G, .)$ يک گروپ که $e \in G$ عنصر عينيت آن است و H_1, H_2 گروپ های فرعی آن با خواص ذيل اند

i. $H_1 \cap H_2 = \{e\}$
ii. $H_1 . H_2 = G$
iii. $\forall x \in H_1$ و $\forall y \in H_2$: $x . y = y . x$

بعدآ تابع ذيل يک G- isom است :

$$\varphi: H_1 x H_2 \to G$$
$$(x, y) \mapsto x . y$$

ثبوت :

φ $G-Hom$:

$$x = (x_1, x_2), y = (y_1, y_2) \in H_1 \ x \ H_2$$
$$\varphi(x.y) = \varphi\big((x_1, x_2).(y_1, y_2)\big) = \varphi(x_1 . y_1, x_2 . y_2)$$
$$= x_1 y_1 . x_2 y_2$$
$$\varphi(x) = \varphi(x_1, x_2) = x_1 . x_2$$
$$\varphi(y) = \varphi(y_1, y_2) = y_1 . y_2$$
$$\varphi(x).\varphi(y) = x_1 x_2 . y_1 y_2$$
$$= x_1 y_1 . x_2 y_2 \quad [\text{ iii. نظربه }]$$
$$= \varphi(x.y)$$

$$\Rightarrow \varphi \ G - Hom$$

φ surjective :

$$g \in G$$
$$\Rightarrow \exists h_1 \in H_1 \wedge h_2 \in H_2 \ ; \ g = h_1 . h_2 \quad [H_1 . H_2 = G \text{ زيـر ا }]$$
$$\Rightarrow \varphi(h_1, h_2) = h_1 . h_2 = g$$
$$\Rightarrow \varphi \ surjective$$

:φ injective

$(x,y) \in \ker\varphi \Rightarrow \varphi(x,y) = e = x.y \Rightarrow x = y^{-1}$

$\Rightarrow x \in H_1 \wedge y^{-1} \in H_2 \quad [y^{-1}, y \in H_2$ زیـرا $]$

$\Rightarrow x, y^{-1} \in H_1 \cap H_2$

$\Rightarrow x = e \wedge y^{-1} = e \quad [H_1 \cap H_2 = e$ زیرا $]$

$\Rightarrow (x,y) = (e,e)$

$\Rightarrow \varphi$ injective [نظر به قضیه 2.3]

در نتیجه ثبوت شد که φ یک G- isom است .

مثال 4.2 : ما دو گروپ دورانی A و B که عناصرعینیت $e_1 \in A$ و $e_2 \in B$ اند ، باخواص ذیل داریم:

$< a > = A = \{e_1, a\} \wedge a^2 = e_1$

$< b > = B = \{e_2, b, b^2\} \wedge b^3 = e_2$

$G := AxB = \{e_1, a\}.\{e_2, b, b^2\}$

$= \{(e_1,e_2), (e_1,b), (e_1,b^2), (a,e_2), (a,b), (a,b^2)\}$

G نظر به رابطه دو گانه ذیل یک گروپ و Ext-dir – prod از A و B است

$\cdot : GxG \longrightarrow G$

$(x,y) \mapsto x.y$

البته درینجا $x = (x_1,x_2)$, $y = (y_1,y_2)$ و

$x.y = (x_1,x_2).(y_1,y_2) = (x_1.y_1, x_2.y_2)$

عنصرعینیت $e = (e_1, e_2)$ است و معکوس (x,y) عنصر (x^{-1}, y^{-1}) است

بطورمثال میخواهیم معکوس (a, b^2) رادریافت نمایم

$a.a = a^2 = e_1 \Rightarrow a^{-1} = a$

$b^2.b = b^3 = e_2 \Rightarrow (b^2)^{-1}.b^2.b = (b^2)^{-1}.e_2$

$\Rightarrow e_2.b = b = (b^2)^{-1}$

دیده میشود که a^{-1} معکوس a و b معکوس از b^2 است .

اگر ما داشته باشیم :

$A' := \{(x,e_2) \mid x \in A\} = \{(e_1,e_2), (a,e_2)\}$

$B' := \{(e_1, x) \mid x \in B\} = \{(e_1, e_2), (e_1, b), (e_1, b^2)\}$

ما میخواهیم نشان دهیم که A´ و B´ گروپ های فرعی نورمال در G اند .

به آسانی میتوان نشان داد که A´ و B' گروپ های فرعی از G اند . حالا ثبوت می نمائیم که A´ و B´ نورمال در G نیز اند

نظر به لیما 3.6 باید ثبوت شود :

$\forall x = (x_1, x_2) \in G;\ x\, B'\, x^{-1} \subseteq B'$

$y = (y_1, y_2) \in x.B'x^{-1}$

$\Rightarrow \exists b' = (b_1, b_2) \in B';\ y = x\, b'x^{-1}$

$= (x_1, x_2).(b_1, b_2).(x_1^{-1}, x_2^{-1})$

$b' = (b_1, b_2) \in B'$

$\Rightarrow b_1 = e_1 \in A \wedge b_2 \in B'$ [نظر به تعریف]

$y = (y_1, y_2) = x\, b'x^{-1} = (x_1\, b_1 x_1^{-1}, x_2 b_2 x_2^{-1})$

$= (x_1\, e_1\, x_1^{-1}, x_2\, b_2 x_2^{-1})$

$= (e_1, x_2\, b_2 x_2^{-1})$

ازجانب دیگر

$x_2, b_2 \in B$

$\Rightarrow x_2 . b_2 \in B \Rightarrow x_2 . b_2 . x_2^{-1} \in B$ [زیرا B یک گروپ فرعی است]

$\Rightarrow y = (e_1, x_2\, b_2\, x_2^{-1}) \in B' \Rightarrow B'\ normal$

به همین ترتیب میتوان ثبوت نمائیم که A' نیز نورمال در G است .

تعریف 4.2 : (G,.) یک گروپ و $e \in G$ عنصرعینیت (identity) آن است . $N_1, N_2, \ldots, N_n$ گروپ های فرعی نورمال د رG اند . گروپ G بنام enternal direct product (ent- dir – prod) از N_i (i= 1 ,2 …,n) یاد میشود، در صورتیکه :

(i) $G = N_1 . N_2 . \ldots . N_n$

$= \{(a_1 . \ldots . a_n) \mid a_i \in N_i\ (i = 1,2, \ldots, n)\}$

(ii) $N_k \cap (N_1 . N_2 . \ldots . N_{k-1} . N_{k+1} \ldots N_n)$

$= \{e\} \quad (k = 1,2,3, \ldots, n)$

اگر G یک ent- dir – prod از N_i (i= 1, 2 ,3 ,…,n) باشد و آنرا به شکل ذیل مینویسند :

$$G = N_1 \otimes N_2 \otimes \ldots . \otimes N_n$$

مثال 4.3 : در گروپ $(A^{(2,2)}, \odot)$ ما داریم :

$< b_2 > = \{b_1 , b_2\}$, $< b_3 > = \{b_1 , b_3\}$

چون $A^{(2,2)}$ یک گروپ تبدیلی است. پس گروپ های فرعی <b_2> و <b_3> نورمال اند

$$< b_2 > . < b_3 > = \{b_1 , b_2\}.\{b_1 , b_3\}$$
$$= \{b_1, b_3, b_2 , b_4\} = A^{(2,2)}$$
$$< b_2 > \cap < b_3 > = \{b_1 , b_2\} \cap \{b_1 , b_3\} = \{b_1\}$$

در نتیجه $A^{(2,2)}$ یک ent- dir –prod از $< b_2 >$ و $< b_3 >$ است .

یعنی: $A^{(2,2)} = < b_2 > \otimes < b_3 >$

مثال 4.4: - در گروپ $(\mathbb{Z}_6 , +)$ ما گروپ های فرعی ذیل را در نظر میگیریم :

$< \bar{2} > = \{\bar{0} , \bar{2} , \bar{4}\}$, $< \bar{3} > = \{\bar{0}, \bar{3}\}$

چون گروپ $\mathbb{Z}_6$ یک گروپ تبدیلی (commutative) است پس گروپ های فرعی آن نورمال اند .

$$< \bar{2} > + < \bar{3} > = \{\bar{0} , \bar{2} , \bar{4}\} + \{\bar{0}, \bar{3}\} = \{\bar{0}, \bar{2}, \bar{4}, \bar{3}, \bar{5}, \bar{1}\} = \mathbb{Z}_6$$
$$< \bar{2} > \cap < \bar{3} > = \{\bar{0}\}$$

پس $< \bar{2} > \otimes < \bar{3} > = \mathbb{Z}_6$ است. یعنی $\mathbb{Z}_6$ یک ent-dir-prod از $< \bar{2} >$ و $< \bar{3} >$ است .

مثال 4.5 : $(\mathbb{Z}_8^*, .)$ گروپ شده نمیتواند . زیرا 8 یک عدد اولیه نیست. بطورمثال

$\bar{4} \in \mathbb{Z}_8^*$, $\bar{4}.\bar{4} = \overline{16} = \bar{0} \notin \mathbb{Z}_8^*$

اگر ما سیت تمامی عناصر معکوس پذیر از $(\mathbb{Z}_8^*, .)$ را به $\mathbb{Z}_8^x$ نشان دهیم پس :

$\mathbb{Z}_8^x = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

ما میدانیم که $(\mathbb{Z}_8^x, .)$ یک گروپ است. $< \bar{3} >$ و$< \bar{5} >$ گروپ های فرعی ان اند. وعلاوه بران $\mathbb{Z}_8^x$ یک ent-dir-prod از $< \bar{3} >$ و $< \bar{5} >$ است.

زیرا :

$< \bar{3} > = \{\bar{1} , \bar{3}\}$, $<\bar{5} > = \{\bar{1}, \bar{5}\}$

$< \bar{3} > . < \bar{5} > = \{\bar{1}, \bar{3}\}.\{\bar{1}, \bar{5}\} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7} > = \mathbb{Z}_8^x$

$< \bar{3} > \cap < \bar{5} >= \bar{1}$

درنتیجه $\mathbb{Z}_8^x =< \bar{3} > \otimes < \bar{5} >$ است

تمرین 4.5 : ثبوت نمائید که روابط ذیل صدق میکنند:

$\mathbb{Z}_8^x =< \bar{5} > \otimes < \bar{7} >$

$\mathbb{Z}_8^x = < \bar{3} > \otimes < \bar{7} >$

تمرین 4.6: گروپ های $\mathbb{Z}_6^x$ و $\mathbb{Z}_{10}^x$ را دریافت نماید

تمرین 4.7 : گروپ (Q,.) دارای گروپ های فرعی < l > , < k > و <J> اند

(a) نشان دهید که گروپ های فرعی فوق دارای کدام عناصر اند و مرتبه انرا نیز دریافت نماید

(b) ایا گروپ Q یک ent-dir-prod از < l > , < k > و <J> است. یعنی:

$Q = < I > \otimes < K > \otimes < J >$

فصل پنجم

گروپ های دورانی (cyclic group)

اگر ما یک گروپ (G , .) دارای عنصر عینیت e داشته باشیم و a ∈G . گروپ فرعی که مولد (generator) آن a باشد به <a> نشان دادیم یعنی

$$<a> = \{a^k | \ k \in \mathbb{Z}\}$$

قضیه 5.1: (G , .) یک گروپ و e∈ G عنصر عینیت (identity) ان است و a∈ G . بعداً :

(a) اگر ord(a) = n معین باشد در آنصورت :

(i)

$$Ord(a) = |< a >| \ \wedge < a > = \{ e , a^1, a^2, \dots, a^{n-1}\}$$

(ii)

$$a^s = e \iff ord(a) \mid s$$

(b) اگر ord(a) = ∞ باشد در آنصورت :

$$\forall \ i,j \ \in \mathbb{N} , i \neq j \implies a^i \neq a^j$$

ثبوت (a) چون ord(a) = n است پس n کوچکترین عدد طبعی است که $a^n = e$ است .

ما سیت H را طوری تعریف می نمائیم : $H := \{k \in \mathbb{Z} \mid a^k = e\}$

H یک گروپ فرعی $(\mathbb{Z} , +)$ است. زیرا:

n∈ $H \implies H \neq \emptyset$

$k, m \in H \implies a^k = a^m = e$

$\implies a^k . a^{-m} = a^{k-m} = e \implies k + (-m) \in H$

از این نظر به قضیه 3.2 نتیجه میشود که H گروپ از $(\mathbb{Z} , +)$ است .

ونظر به قضیه 3.6 باید H=n$\mathbb{Z}$ باشد . در حالیکه n درینجا خورد ترین عدد طبعی است که $a^n = e$ میشود .

$$m \in \mathbb{Z} \implies \exists q, r \in \mathbb{Z} ; m = q.n + r \qquad 0 \leq r < n$$

$\Longrightarrow a^m = (a^n)^{q+r} = (a^n)^q \,.a^r = e\, a^r = a^r$

$\Longrightarrow a^m = a^r \in \{e, a^1, a^2, \ldots, a^{n-1}\}$ [r < n]

دیده شد که برای هر $m \in \mathbb{Z}$ عنصر a^m در سیت $\{e, a^1, a^2, \ldots, a^{n-1}\}$ واقع است پس:

$$< a >= \{a^k \mid k \in \mathbb{Z}\} = \{e, a^1, a^2, \ldots, a^{n-1}\}$$

چون $|< a >| = n$ است . پس $ord\,(a) = |< a >|$

ثبوت (ii)

"⇐"

$ord(a) \mid s = n|s$

$\Longrightarrow \exists q \in \mathbb{N} \quad ; s = q\,.n$

$\Longrightarrow a^s = a^{q.n} = (a^n)^q = (e)^q = e$

"⟹"

$a^s = e \Longrightarrow s \in \{k \in \mathbb{Z} \mid a^k = e\} = n\,.\mathbb{Z}$

$\Longrightarrow \exists z \in \mathbb{Z}; s = n.z \quad \Longrightarrow n|s$

ثبوت (b) : اگر آنطور نباشد پس باید j وi موجود باشد که $i \neq j$ مگر $a^i = a^j$ باشد. البته دراینجا i و j اعداد طبعی اند. ما فرض میکنیم که i < j است :

$a^i = a^j \Longrightarrow a^{i-j} = e$

ازین نتیجه میشود که یک عدد k پیدا میشود که $a^k = e$ میشود . پس باید ord(a) معین باشد . مگر این در تضاد به فرضیه است که ord(a)=∞

بالاخره : $\forall \; i, j \in \mathbb{N}, i \neq j \Longrightarrow a^i \neq a^j$

لیما 5.1 : (G, .) و $(G_1, *)$ دو گروپ که دارای عناصرعینیت $e \in G$ و $e_1 \in G_1$ اند. $a \in G$ دارای مرتبه (order) معین و $\varphi: G \longrightarrow G_1$ یک G-Hom است. بعدآ :

$(\boldsymbol{a})$ $ord(\varphi(a)) \mid ord\,(a)$

$(\boldsymbol{b})$ $\varphi\ injective \Longrightarrow ord(\varphi(a)) = ord(a)$

ثبوت (a): چون φ یک G-Hom است پس میتوان نوشت:

$$(\varphi(a))^{ord(a)} = (\varphi(a)) * \varphi(a) * \ldots * \varphi(a)) \quad [\ \varphi(a) \text{ دفعه } ord(a)\ ]$$

$= \varphi$ (a . a . ... .a) [a دفعه $ord(a)$]
$= \varphi(a^{ord(a)})$
$= \varphi\ (e) = e_1$ [نظر به قضیه 2.1]

$\Longrightarrow ord(\varphi(a))|\ ord(a)$ [نظربه قضیه 5.1]

ثبوت (b):

$(\varphi(a))^{ord(\varphi(a))}$ $= ((\varphi(a)) * \varphi(a) *$
$\ldots * \varphi(a)$) [$\varphi(a)$ دفعه $ord(\varphi(a))$]
$= \varphi$ (a . a . ... .a) [a دفعه $ord(\varphi(a))$]
$= \varphi\ (a^{ord(\varphi(a))})$

$\Longrightarrow\ e_1 = (\varphi(a))^{ord(\varphi(a))} = \varphi\ (a^{ord(\varphi(a))})$
از جانب دیگر $\varphi(e) = e_1$ است. پس مادریم:

$$\varphi\ (a^{ord(\varphi(a))}) = \varphi(e) = e_1$$

چون φ یک injective است پس باید $a^{ord(\varphi(a))} = e$ شود
پس نظر به قضیه 5.1 باید $ord(a)|\ ord(\varphi(a))$ ونظر به (a)
$ord(\varphi(a))|\ ord(a)$ باشد. در نتیجه ord(φ(a)) = ord(a) .

لیما 5.2 : (G ,.) یک گروپ و $e \in G$ عنصر عینیت آن است . برای $a \in G$ ما $a^0 = e$ و $(a^{-i}) = (a^i)^{-1}$ تعریف می نمائیم . بعدآ:
$< a >= \{\ a^i \mid i \in \mathbb{Z}\ \}$ یک گروپ فرعی از G است .

ثبوت :

$i = 0\ ,\ a^0 = e \in < a > \Longrightarrow < a > \neq 0$
$x, y \in < a > \Longrightarrow \exists\ m, n \in \mathbb{Z}\ ; x = a^m \wedge y = a^n$
$\Longrightarrow x\ .\ y^{-1} = a^m\ .(a^n)^{-1}$
$= a^m\ .\ a^{-n} = a^{m-n}$
$\Longrightarrow x\ .\ y^{-1} \in < a >$

در نتیجه <a> نظر به قضیه 3.2 یک گروپ فرعی از G است که در عین زمان گروپ دورانی نیز است .

مثال: بااستفاده ازلیما فوق میخواهیم گروپ فرعی <f> رادر گروپ Q_6 دریافت نمایم

$f^0 = e \ , f^1 = f \ , f^2 = e \implies <f> = \{ e, f \}$

تمرین: برای حل ازلیمای 5.2 استفاده نماید

(a) گروپ فرعی <b> رادر گروپ $Q_6 \ , D_4$ و Q_8 دریافت نماید

(b) گروپ فرعی های <k> و <l-> را درگروپ Q دریافت نماید

قضیه 5.2: هر گروپ فرعی یک گروپ دورانی (cyclic group) هم یک گروپ دورانی است .

ثبوت : ما فرض میکنیم که (G , .) یک گروپ دورانی است. $G =< x >$ ، $e \in G$ عنصر عینیت و H یک گروپ فرعی آن است .

حالت اول : اگر H={e} باشد در اینصورت H=<e> یک گروپ دورانی است

حالت دوم : $H \neq \{e\}$:

$$H \neq \{e\} \implies \exists y \in H , y \neq e$$
$$\implies \exists m > 0 ; y = x^m \quad [y \in G \text{ زیـرا}]$$

کوچکترین m را انتخاب میکنیم که $x^m \in H$ باشد .

چون H یک گروپ فرعی است ، پس با x^m همه طاقت های ان شامل H میباشد یعنی:

$$x^m \ , (x^m)^2 \ , (x^m)^3 \ , \ldots \ldots \in H$$
$$\implies < x^m > \subseteq H$$

حالا نشان میدهیم که $H \subseteq < x^m >$ است .

$$h \in H \implies \exists \, i \in \mathbb{Z} ; h = x^i$$
$$\implies \exists q, r \in \mathbb{Z} \ ; i = mq + r \ , \ 0 \leq r < m$$
$$\implies x^i = x^{mq+r} = x^{mq} . x^r$$
$$\implies x^r = x^{-m} \ . x^i \in H \quad [\, x^m , x^i \in H \quad \text{زیرا} \,]$$

چون ما m را خورد ترین عدد $x^m \in H$ انتخاب کرده بودیم . اما می بینیم که r < m و $x^r \in H$ است .پس باید r = 0 باشد .

$$r = 0 \implies i = mq \implies x^i = (x^m)^q \in < x^m >$$
$$\implies H \subseteq < x^m >$$

بنا بر این $H =< x^m >$ یک گروپ دورانی است .

مثال 5.1 : گروپ $(\mathbb{Z}_7^*, .)$ یک گروپ دورانی (cyclic group) بوده ومولد (generator) آن $\bar{3}$ است . یعنی $\mathbb{Z}_7^* = < \bar{3} >$. زیرا:

$ord(\mathbb{Z}_7^*) = |\mathbb{Z}_7^*| = 6 , \mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$(\bar{3})^1 = \bar{3}$

$(\bar{3})^2 = \bar{9} = \bar{7} + \bar{2} = \bar{2}$

$(\bar{3})^3 = \bar{2}.\bar{3} = \bar{6}$

$(\bar{3})^4 = \bar{6}.\bar{3} = \overline{18} = \overline{2.7} + \bar{4} = \bar{4}$

$(\bar{3})^5 = \bar{4}.\bar{3} = \overline{12} = \bar{7} + \bar{5} = \bar{5}$

$(\bar{3})^6 = \bar{5}.\bar{3} = \overline{15} = \overline{14} + \bar{1} = \bar{1}$

دیده شد که از $\bar{3}$ ذریعه $(\bar{3})^i$ (i= 1,2,3,4,5,6) تمامی عناصر از $\mathbb{Z}_7^*$ بدست آمد . پس $\mathbb{Z}_7^* =< \bar{3} >$ است .

$H = \{\bar{1}, \bar{2}, \bar{4}\}$ یک گروپ فرعی از $\mathbb{Z}_7^*$ است . H دورانی است زیرا :

$(\bar{4})^1 = \bar{4}$

$(\bar{4})^2 = \bar{4}.\bar{4} = \overline{16} = \overline{14} + \bar{2} = \bar{2}$

$(\bar{4})^3 = \bar{2}.\bar{4} = \bar{8} = \bar{7} + \bar{1} = \bar{1}$

در نتیجه $H =< \bar{4} >$

تمرین 5.1 : گروپ های فرعی دیگر از $\mathbb{Z}_7^*$ را پیدا نمائید ونشان دهید که دورانی اند .

تمرین 5.2 : $\varphi : (G,.) \longrightarrow (G_1,*)$ یک G - isom و $a \in G$ دارای مرتبه (order) متناهی است. بعداً

G cyclic (دورانی) $\Leftrightarrow$ G_1 cyclic (دورانی)

لیما 5.3 : (G , .) = <a> یک گروپ دورانی (cyclic) معین و $e \in G$ عنصرعینیت (identity) آن است . اگر ord(G)=n و n بالای یک $d \in \mathbb{N}$ قابل تقسیم باشد. در آنصورت فقط تنها یک گروپ فرعی وجود دارد که مرتبه (order) آن مساوی به d باشد وان گروپ فرعی $< a^{\frac{n}{d}} >$ است .

ثبوت : نظر به قضیه 5.2 $< a^{\frac{n}{d}} >$ یک گروپ فرعی از G= <a> است.

$Ord(a) = |< a >| = n \Longrightarrow a^n = e$ [n خورد ترین عدد طبعی]

$(a^{\frac{n}{d}})^l \ (l = 1,2, \dots, d) \Longrightarrow \frac{n}{d}\, l < n$ [$l \neq d$ برای]

$\Longrightarrow a^{\frac{n}{d}.l} \neq e$ [$a^n = e$ زیرا n خوردترین عدد است که]

$a^{\frac{n}{d}.l} = a^n = e \qquad [l = d \quad \text{برای}]$

از این نتیجه میشود که d خورد ترین عدد است که $(a^{\frac{n}{d}})^d = e$

$\Longrightarrow d = ord(a^{\frac{n}{d}}) = \left|< a^{\frac{n}{d}} >\right|$

حالا ثبوت می نمائیم که $< a^{\frac{n}{d}} >$ یگانه گروپ فرعی از G است که مرتبه (order) آن d است .

ما فرض میکنیم که H هم یک گروپ از G با خاصیت $ordH = |H| = d$ است. نظر به قضیه 5.2 یک $t \in \mathbb{N}$ موجود است که $H = < a^t >$

$\Longrightarrow (a^t)^d = e \qquad [\text{نظر به قضیه } fermat]$

$\Longrightarrow n|t.d \qquad [\text{نظر به قضیه5.1}]$

$\Longrightarrow \quad \frac{n}{d} | \, t \quad \Longrightarrow \quad \frac{n}{d} \leq$ t

$\Longrightarrow a^t \in < a^{\frac{n}{d}} > \Longrightarrow H \subseteq < a^{\frac{n}{d}} >$

چون $\left|< a^{\frac{n}{d}} >\right|$ = d = $|H|$ است. پس در نتیجه $H = (a^{\frac{n}{d}})$

مثال: ما میدانیم $(\mathbb{Z}_{11}^*, .)$ یک گروپ دورانی (cyclic group) بوده وبه اسانی میتوان ثبوت نمود که $\bar{2}$ مولد (generator) آن است . یعنی

$< \bar{2} > = \mathbb{Z}_{11}^*$

از لیما 5.3 استفاده نموده و گروب های فرعی دورانی انرادریافت می نمایم

$ord(\mathbb{Z}_{11}^*) = |\mathbb{Z}_{11}^*| = 10$

عدد 10 بالای1 ، 2 ، 5 و 10 قابل تقسیم است. برای d=1 و d=10 واضح ست

برای d=2

$(\bar{2})^{\frac{10}{2}} = (\bar{2})^5 = \overline{32} = \overline{22} + \overline{10} = \overline{10}$

$(\overline{10})^1 = \overline{10}$

$(\overline{10})^2 = \overline{10}.\overline{10} = \overline{100} = 9.\overline{11} + \bar{1} = \bar{1}$

درنتیجه:

$< \overline{10} >$ = { $\bar{1}, \overline{10}$ } , ord($< \overline{10} >$) = 2 = d

برای d=5

$(\bar{2})^{\frac{10}{5}} = (\bar{2})^2 = \bar{4}$

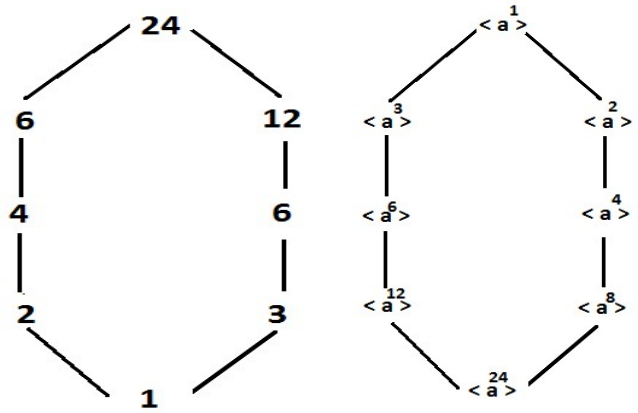
$(\bar{4})^1 = \bar{4}$
$(\bar{4})^2 = \bar{4}.\bar{4} = \overline{16} = \overline{11} + \bar{5} = \bar{5}$
$(\bar{4})^3 = \bar{5}.\bar{4} = \overline{20} = \overline{11} + \bar{9} = \bar{9}$
$(\bar{4})^4 = \bar{9}.\bar{4} = \overline{36} = \overline{11} + \bar{3} = \bar{3}$
$(\bar{4})^5 = \bar{3}.\bar{4} = \overline{12} = \overline{11} + \bar{1} = \bar{1}$

درنتیجه:

$< \bar{4} >$ = { $\bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9}$ } , ord($< \bar{4} >$) = 5 = d

مثال 5.2 : اگر G=<a> یک گروپ دورانی که $|G| = 24$ باشد . در آنصورت میتوان تمامی اعدادیکه که 24 بالای آن قابل تقسیم است وتمامی گروپ های فرعی آنرا بشکل گراف نشان داد .

$$G = \{a^1, a^2, \dots, a^{23}, a^{24} = e\}$$



یادداشت : اگر G یک گروپ معین مگر دورانی نباشد . درآنصورت تعین تمامی گروپ فرعی آن مغلق تراست . بطور مثال $|s_4| = 24$ است مگر تعداد گروپ های فرعی آن 30 است .

لیما 5.4 : (G , .) یک گروپ دورانی که دارای عنصرعینیت e است . بعداً

(a) اگرمرتبه (order) گروپ G غیر معین (infinite) باشد در آنصورت در بین G و $(\mathbb{Z}, +)$ یک G-Isom موجود است . یعنی $G \cong \mathbb{Z}$

(b) اگر G یک گروپ معین (finite) دارای مرتبه (order) n باشد، در آنصورت در بین G و $(\mathbb{Z}_n, +)$ یک G-Isom موجود است.
یعنی: $G \cong \mathbb{Z}_n$

ثبوت : چون G یک گروپ دورانی (cyclic) است پس یک $a \in G$ موجود است که G=<a> شود . ما تابع ذیل را در نظر میگیریم :

$$\varphi: (\mathbb{Z}, +) \longrightarrow (G, .)$$
$$k \longmapsto a^k$$

که البته درینجا $\varphi(0) = a^0 = e$ است

φ surjective :

چون G یک گروپ دورانی و G = <a> است. پس

$$x \in G \implies \exists k \in \mathbb{Z} \ ; \quad x = a^k = \varphi(k)$$
$$\implies \varphi \ surjective$$

φ G − Hom :

$$k, r \in \mathbb{Z} \ , \varphi(k + r) = a^{k+r} = a^k . a^r = \varphi(k) . \varphi(r)$$

Kerφ نظر به قضیه 2.4 یک گروپ فرعی از $(\mathbb{Z}, +)$ است . نظر به قضیه 3.6 میتواند kerφ به حیث گروپ فرعی از $\mathbb{Z}$ فقط تنها اشکال ذیل را داشته باشد :

$ker\varphi = \{0\}$ یا $ker\varphi = n\mathbb{Z}$ برای $n \in \mathbb{N}$

ثبوت (a) :

ord(G) = ∞

Kerφ = {k ∈ $\mathbb{Z}$ |$\varphi(k) = e$} = {k ∈ $\mathbb{Z}$ | $a^k = e$} = {0}

$\implies \varphi$ injective [نظربه قضیه 2.3]

درنتیجه φ یک G-Isom است. یعنی $G \cong \mathbb{Z}$

ثبوت (b) :

ord(G) = n ∧ <a> = G

k: = n ∧ m: = 2n $\implies$ e = $a^k = a^m$ [نظر به قضیه 5.1]

$\implies \varphi(k) = \varphi(m)$ ∧ k ≠ m

$\implies \varphi$ not injective

$\implies$ ker $\varphi \neq \{0\}$ [نظربه قضیه 2.3]

$\implies$ ker $\varphi = n\mathbb{Z}$

نظر به قضیه (همو مورفیزم) 3.19 یک G-Isom در بین $\varphi(\mathbb{Z})$ و $\mathbb{Z}/_{ker\varphi}$ موجود است . یعنی

$$\mathbb{Z}_n = \mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}/_{ker\varphi} \cong \varphi(\mathbb{Z})$$

چون φ یک surjective است پس باید $\varphi(\mathbb{Z}) = G$ باشد.

درنتیجه $G \cong \mathbb{Z}_n = \mathbb{Z}/_{n\mathbb{Z}}$ است.

قضیه 5.3 : $a_1, a_2, \ldots, a_n \in \mathbb{Z}^*$ و اگر $d = gcd(a_1, a_2, \ldots, a_n)$ باشد بعدآ :

(a) $< a_1, a_2, \ldots, a_n > = d\mathbb{Z}$
$\wedge \ \exists \ r_1, r_2, \ldots, r_n \in \mathbb{Z}\,; d = r_1a_1 + r_2a_2 + \cdots + r_na_n$

(b) $k \mid a_i \ (i = 1,2,\ldots,n) \Longrightarrow \ k \mid d$

ثبوت (a) : نظر به لیما 3.2 هر a_i مولد (generator) از $a_i\mathbb{Z}$ است. پس لهذا میتوان نوشت :

$$< a_1, a_2, \ldots, a_n > = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$$

$$= \{ \textstyle\sum_{i=1}^{n} s_i a_i \mid s_i \in \mathbb{Z} \}$$

چون $< a_1, a_2, \ldots, a_n >$ یک گروپ فرعی از $(\mathbb{Z}, +)$ است پس یک $k \in \mathbb{Z}$ موجود است که :

$< a_1, a_2, \ldots, a_n > = k\mathbb{Z} = < k >$
$a_i \in < a_1, a_2, \ldots, a_n > = k\mathbb{Z}$
$\Longrightarrow \exists s_i \in \mathbb{Z} \ ; \ a_i = s_i k \quad (i = 1,2,\ldots,n)$
$\Longrightarrow k = cd(a_1, a_2, \ldots, a_n)$

یعنیk یک قاسم مشترک از $a_1, a_2, \ldots, a_n$ است. چون $k \in k\mathbb{Z}$ است . پس :

$k \in k\mathbb{Z} = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}$
$\Longrightarrow \exists r_1, r_2, \ldots, r_n \in \mathbb{Z} \ ; k = r_1a_1 + r_2a_2 + \cdots + r_na_n$

ثبوت (b): اگر m نیز یک قاسم مشترک از $a_1, a_2, \ldots, a_n$ باشد .
یعنی: $m = cd(a_1, a_2, \ldots, a_n)$. پس :

$m \mid a_i \ (i = 1,2,\ldots,n) \Longrightarrow \ m \mid r_i a_i \quad (i = 1,2,\ldots,n)$
$\Longrightarrow m \mid r_1a_1 + r_2a_2 + \cdots + r_na_n = k$
$\Longrightarrow k = gcd(a_1, a_2, \ldots, a_n)$

چون اعداد $a_1, a_2, \ldots, a_n$ فقط تنها یک بزرگترین قاسم مشترک (gcd) میتواند داشته باشد پس:

$$d = gcd(a_1, a_2, \ldots, a_n) = k$$

مثال: چون gcd(9,12) = 3 است. پس نظربه قضیه 5.3 میتوان نوشت:

$< 9,12 > = 9\mathbb{Z} + 12\mathbb{Z} = 3\mathbb{Z}$

حالا میخواهیم رابطه فوق را ثبوت نمایم

$h \in 9\mathbb{Z} + 12\mathbb{Z} \Longrightarrow \exists a,b \in \mathbb{Z} ; h = 9a + 12b = 3(3a+4b)$

$\Longrightarrow h \in 3\mathbb{Z} \Longrightarrow 9\mathbb{Z} + 12\mathbb{Z} \subseteq 3\mathbb{Z}$

$h \in 3\mathbb{Z} \Longrightarrow \exists c \in \mathbb{Z} ; h = 3c$

$gcd(9,12) = 3$

$\Longrightarrow \exists s,r \in \mathbb{Z} ;\ 3 = r.9 + s.12$ [division algorithm نظربه]

$\Longrightarrow h = 3.c = (r.9 + s.12).c = r.c.9 + s.c.12$

$\Longrightarrow h \in 9\mathbb{Z} + 12\mathbb{Z} \Longrightarrow 3\mathbb{Z} \subseteq 9\mathbb{Z} + 12\mathbb{Z}$

تمرین 5.3: یک گروپ فرعی $d\mathbb{Z}$ رادر گروپ $(\mathbb{Z}, +)$ دریافت نماید که

(a) $d\mathbb{Z} = < 40, 24, 16 >$ باشد

(b) $d\mathbb{Z} = < 45,12 >$ باشد

تعریف5.1 اعداد $0 \neq a_i \in \mathbb{Z}$ (i=1,2,…,n) بنام relatively prime (عدد اولیه نسبی) یاد میشود در صورتیکه $gcd(a_1, a_2, \dots, a_n) = 1$ باشد. نظر به قضیه 3.7 اعداد $r_i \in \mathbb{Z}$ (i=1,2,…,n) با خواص ذیل موجود است :

$$r_1 a_1 + r_2 a_2 + \cdots + r_n a_n = 1$$

مثال : اعداد 5 و 9 با یکدیگر relatively prime (rel -prim) اند زیرا :

$9 = 1 * 5 + 4$ $\quad$ $1 = 5 - 1 * 4$

$5 = 1 * 4 + 1$ $\quad$ $= 5 - 1 * (9 - 1 * 5)$

$4 = 4 * 1 + 0$ $\quad$ $= 2 * 5 - 1 * 9$

دیده میشود که gcd(9,5)=1 است. پس 5 و 9 باهم relat-prime اند ، r = 2 و s = -1 است

لیما 5.6: (G , .) یک گروپ و $e \in G$ عنصر عینیت آن است و $a \in G$ دارای مرتبه متناهی است . یعنی ord(a) = n . بعداً

$$\forall k \in \mathbb{Z} ; ord(a^k) = \frac{n}{gcd\ (n,k)}$$

ثبوت : اگر $t := ord(a^k)$ و $d := gcd\,(n,k)$ باشد. درانصورت

$(a^k)^t = a^{kt} = e \implies n \mid tk$ [نظر به قضیه 5.1]

$\implies \frac{n}{d} \mid t.\frac{k}{d}$

$\frac{k}{d}$ و $\frac{n}{d}$ با یکدیگر relative prime (عدد اولیه نسبی) اند. زیرا اگرنباشند. درانصورت یک $m \in \mathbb{N}$ موجود است که

$$\gcd(\tfrac{k}{d}\ ,\ \tfrac{n}{d}\ ) = m \neq 1 \implies m \mid \tfrac{k}{d} \wedge m \mid \tfrac{n}{d}$$
$$\implies m.d \mid k \wedge m.d \mid n$$
$$\implies m.d = cd\ (k,n)$$

چون $m.d > d$ است. پس $d = gcd(k,n)$ شده نمیتواند. مگراین با تضاد در انتخاب d است. پس باید $\frac{k}{d}$ و $\frac{n}{d}$ با یکدیگر rel-prim (عدد اولیه نسبی) باشند.

$\frac{n}{d} \mid t.\frac{k}{d} \wedge\ ) = 1\ \frac{n}{d}\ , \gcd(\frac{k}{d}\ , \frac{n}{d}) = 1$

$\implies \frac{n}{d} \mid t$ [نظر به لیما 3.3]

$\implies \frac{n}{d} \leq t$

از جانب دیگر :

$(a^k)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = (e)^{\frac{k}{d}} = e$

چون $t = ord(a^k)$ خورد ترین عدد در $\mathbb{N}$ است که $(a^k)^t = e$ شود پس $t \leq \frac{n}{d}$ است .در نتیجه :

$$ord(a^k) = t = \frac{n}{d} = \frac{n}{gcd\ (n,k)}$$

مثال 5.4: ماگروپ $G = \{a^1, a^2, \dots, a^{24} = e\}$ رادر نظر میگیریم. $a^3 \in G$

$$< a^3 > = \{\ a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24} = e\}$$

گروپ فرعی $< a^3 >$ دارای مرتبه 8 میباشد . یعنی $ord(< a^3 >) = 8$ وهم چنان $ord(\mathrm{a}^3) = 8$ است زیرا :

$a^3, a^3.a^3 = a^6 = (a^3)^2$, $a^6.a^3 = a^9 = (a^3)^3$

$a^9.a^3 = a^{12} = (a^3)^4$, $a^{12}.a^3 = a^{15} = (a^3)^5$

$a^{15}.a^3 = a^{18} = (a^3)^6$, $a^{18}.a^3 = a^{21} = (a^3)^7$
$a^{21}.a^3 = a^{24} = e = (a^3)^8$

اگر ما k = 6 داشته باشیم :

$(a^3)^6 = a^{18}$
$a^{2.18} = a^{18}.a^{18} = a^{36} = a^{24}.a^{12} = e.a^{12} = a^{12}$

$a^{3.18} = a^{12}.a^{18} = a^{30} = a^{24}.a^6 = a^6$

$a^{4.18} = a^{3.18}.a^{18} = a^6.a^{18} = a^{24} = e$

دیده میشود که $ord(a^3)^6 = 4$ است. اگر ما لیما فوق را تطبیق نمایم ،عین نتیجه بدست مآید. یعنی :

$$ord((a^3)^6) = \frac{ord(a^3)}{gcd\,(ord(a^3),6)} = \frac{8}{2} = 4$$

لیما 5.7: اگر $(G, .) = < a >$ یک گروپ دورانی (cyclic) دارای مرتبه متناهی (finite order) n باشد . در آنصورت برای $k \in \mathbb{Z}$ افاده ذیل صدق میکند :

$$G =< a^k > \iff gcd(n, k) = 1$$

ثبوت " $\Longrightarrow$

$< a > = G =< a^k > \Longrightarrow ord\,(a^k) = n$

در لیما 5.6 دیدیم که :

$$ord\,(a^k) = \frac{n}{gcd(n,k)}$$

$$\Longrightarrow n = \frac{n}{gcd(n,k)} \Longrightarrow gcd(n,k) = \frac{n}{n} = 1$$

" $\Longleftarrow$ " ما در لیما 5.6 دیدیم که $ord\,(a^k) = \frac{n}{gcd(n,k)}$ و چون

$ord(a^k) = \frac{n}{gcd(n,k)} = \frac{n}{1}$ = n پس $gcd(n\,,k) = 1$ و است .

در نتیجه $< a^k > = G$

یاد داشت : با استفاده از لیما 5.7 میتوان تمامی عناصرمولد (generating) از گروپ $(\mathbb{Z}_n\,, +)$ را دریافت نمود. بطور مثال گروپ $(\mathbb{Z}_{12}\,, +)$ دورانی , $\mathbb{Z}_{12} =< \bar{5} >$ و ord($\mathbb{Z}_{12}$) = 12 است.

$\{k \in \mathbb{N} \mid 1 \le k \le 12 \wedge gcd(12,k) = 1\}$ = { 1,5,7,11}

چون دراین مثال $\bar{5}$ = a است. ما برای k = 7 لیما 5.7 راتطبیق می نمایم

$(\bar{5})^7 = \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} + \bar{5} = \overline{35} = \overline{11}$

$\Longrightarrow$ $<\overline{11}>$ = $\mathbb{Z}_{12}$

همچنان $\mathbb{Z}_{12} =< \bar{1} > = < \bar{7} >$ است

مثال: مامیخواهیم سیت { $M:=\{\bar{a} \in (\mathbb{Z}_5^*, .) \mid < \bar{a} > = \mathbb{Z}_5^*$ } رادریافت نمایم.

به اسانی میتوان ثبوت نمود که $\mathbb{Z}_5^*$ یک گروپ دورانی و

$\mathbb{Z}_5^* = < \bar{3} >$ است. چون ord($\mathbb{Z}_5^*$) = 4 است. پس:

$\{k \in \mathbb{N} \mid 1 \le k \le 4 \wedge gcd(4,k) = 1\}$ = { 1,3 }

چون دراین مثال $\bar{3}$ = a است. ما برای k = 3 لیما 5.7 راتطبیق می نمایم

$(\bar{3})^3 = \bar{3} \,.\, \bar{3} \,.\, \bar{3} = \overline{27} = \bar{2}$

پس $\mathbb{Z}_5^* = < \bar{3} > = < \bar{2} >$ و { $\bar{2}, \bar{3}$ } = M

تمرین 5.4 :

(a) سیت { $\bar{M}:=\{\bar{a} \in (\mathbb{Z}_{11}^*, .) \mid < \bar{a} > = \mathbb{Z}_{11}^*$ } رادریافت نماید

(b) سیت { $\bar{N}:=\{\bar{a} \in (\mathbb{Z}_{14}, +) \mid < \bar{a} > = \mathbb{Z}_{14}$ } رادریافت نماید

لیما 5.8: گروپ های دورانی (cyclic groups) گروپ های تبدیلی اند .

ثبوت : اگر $(G\,, .)$ یک گروپ دورانی باشد . پس باید یک $a \in G$ موجود باشد که $< a >= G$

$$x, y \in < a > \Longrightarrow \exists\, m, n \in \mathbb{N}\,; x = a^m \wedge y = a^n$$
$$\Longrightarrow x.y = a^m.a^n = a^{m+n} = a^{n+m}$$
$$= a^n.a^m = y.x$$
$$\Longrightarrow G\ commutative$$

تعریف 5.2: برای $n \in \mathbb{N}$ تابع ذیل بنام Euler function یاد میشود :

$$\varphi : \mathbb{N} \to \mathbb{N}$$
$$n \to \varphi(n) = |\{k \in \mathbb{N} \mid 1 \leq k \leq n \wedge gcd(n,k) = 1\}|$$

یعنی $\varphi(n)$ مساوی به تعداد تمامی k که $1 \leq k \leq n$ و $gcd(n,k) = 1$ باشد، است . بطور مثال

$n = 1$
$\varphi(1) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 1 \wedge \gcd(1,k) = 1\}|$
$= |\{1\}| = 1$

$n = 2$
$\varphi(2) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 2 \wedge \gcd(2,k) = 1\}|$
$= |\{1\}| = 1$

$n = 3$
$\varphi(3) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 3 \wedge \gcd(3,k) = 1\}|$
$= |\{1,2\}| = 2$

$n = 4$
$\varphi(4) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 4 \wedge \gcd(4,k) = 1\}|$
$= |\{1,3\}| = 2$

$n = 5$
$\varphi(5) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 5 \wedge \gcd(5,k) = 1\}|$
$= |\{1,2,3,4\}| = 4$

$n = 6$
$\varphi(6) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 6 \wedge \gcd(6,k) = 1\}|$
$= |\{1,5\}| = 2$

$n = 7$
$\varphi(7) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 7 \wedge \gcd(7,k) = 1\}|$
$= |\{1,2,3,4,5,6\}| = 6$

$n = 8$
$\varphi(8) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 8 \wedge \gcd(8,k) = 1\}|$
$= |\{1,3,5,7\}| = 4$

دیده میشود که اگر p یک عدد اولیه باشد در آنصورت:

$\varphi(p) = |\{k \in \mathbb{N} \mid 1 \leq k \leq p-1\}| = p-1$

زیرا برای تمامی $1 \leq k \leq p-1$ رابطه gcd(k,p) = 1 صدق میکند

لیما 5.9 : در یک گروپ دورانی G که مرتبه (order) آن n باشد، درانصورت تعداد عناصری که مولد (generator) از G اند ،مساوی به $\varphi(n)$ (Euler function) است .

ثبوت : ثبوت از لیما 5.7 وتعریف تابع $\varphi(n)$ (Euler function) بدست می اید بطور مثال در گروپ دورانی $(\mathbb{Z}_{10}, +)$ تعداد عناصر مولد (generator) آن مساوی به 4 است. یعنی:

$\varphi(10) = |\{1,3,7,9\}| = 4$

$\mathbb{Z}_{10} = <\bar{1}> = <\bar{3}> = <\bar{7}> = <\bar{9}>$

اگر p یک عدد اولیه باشد در آنصورت تعداد عناصر مولد (generator) از $(\mathbb{Z}_p, +)$ مساوی به $\varphi(p) = p-1$ است .

بطورمثال ما گروپ $(\mathbb{Z}_5, +)$ رادرنظرمیگیریم. چون 5 یک عدد اولیه است. پس باید $\varphi(5)$ = 5 -1 = 4 باشد

$\varphi(5) = |\{1,2,3,4\}| = 4$

$\mathbb{Z}_5 = <\bar{1}> = <\bar{2}> = <\bar{3}> = <\bar{4}>$

یاداشت: مرتبه گروپ $(\mathbb{Z}_5^*, .)$ مساوی به 4 و φ یک Euler function است

$\varphi(4) = |\{1,3\}| = 2$

لیما 5.9 فقط تعداد عناصرمولد را معلوم میکند. درمثال فوق:

$<\bar{2}> = <\bar{3}> = (\mathbb{Z}_5^*, .)$, $<\bar{1}> \neq \mathbb{Z}_5^*$

تمرین 5.5 : با استفاده از Euler function اعداد m و n راکه در ذیل تعریف شده است دریافت نماید

(a) m:= $|\{\bar{a} \in (\mathbb{Z}_{16}, +) \mid <\bar{a}> = \mathbb{Z}_{16}\}|$

(b) n:= $|\{\bar{a} \in (\mathbb{Z}_7^*, .) \mid <\bar{a}> = \mathbb{Z}_7^*\}|$

تعریف 5.3 :

$\mathbb{Z}_n^x := \{\bar{a} \in (\mathbb{Z}_n, .) | \bar{a} : invertible$ (معکوس پذیر)$\}$

$(\mathbb{Z}_n^x, .)$ یک گروپ است وبنام prime residue class group یاد میشود

لیما 5.10: $n \in \mathbb{N}$ و φ یک Euler function است . بعداً :

$(\boldsymbol{a})\ \mathbb{Z}_n^x = \{\bar{k} \in \mathbb{Z}_n \mid gcd(n,k) = 1\}$

(b) $|\mathbb{Z}_n^x| = \varphi(n)$

ثبوت (a) :

$\bar{k} \in \mathbb{Z}_n^x \Longrightarrow \exists \bar{r} \in \mathbb{Z}_n\ ;\ \bar{1} = \bar{k}.\bar{r} = \overline{k.r}$

$\Longrightarrow 1 - kr \in n\mathbb{Z}$ [نظربه لیما 5.12]

$\Longrightarrow \exists s \in \mathbb{Z}\ ; 1 - kr = sn$

$\Longrightarrow 1 = rk + sn \Longrightarrow gcd(n,k) = 1$

$\Longrightarrow \mathbb{Z}_n^x \subseteq \{\bar{k} \in \mathbb{Z}_n \mid gcd(n,k) = 1\}$

از جانب دیگر: $k \in \mathbb{Z}\ ;\ gcd(n,k) = 1$

$k \in \mathbb{Z}$

$\Longrightarrow \exists\, r,s \in \mathbb{Z}\ ; r.k + s.n = 1$

$\Longrightarrow \bar{1} = \overline{r.k + s.n} = \bar{r}\,.\bar{k} + \bar{s}\,.\bar{n} = \bar{r}\,.\bar{k} + \bar{s}\,.\bar{0} = \bar{r}\,.\bar{k}$

$\Longrightarrow\ \bar{k}\ invertible \Longrightarrow \bar{k} \in \mathbb{Z}_n^x$

در نتیجه : $\mathbb{Z}_n^x = \{\bar{k} \mid gcd(n,k) = 1\}$

ثبوت (b) از تعریف φ $Euler\ function$ بدست می اید .

مثال :

با استفاده ا ز لیما 5.10 گروپ های ذیل prime residue class group اند

$\mathbb{Z}_1^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_1 \mid \gcd(1,k) = 1\} = \{\bar{1}\}$

$\mathbb{Z}_2^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_2 \mid \gcd(2,k) = 1\} = \{\bar{1}\}$

$\mathbb{Z}_3^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_3 \mid \gcd(3,k) = 1\} = \{\bar{1}, \bar{2}\}$

$\mathbb{Z}_4^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_4 \mid \gcd(4,k) = 1\} = \{\bar{1}, \bar{3}\}$

$\mathbb{Z}_5^{\mathrm{x}} = \{\bar{k} \in \mathbb{Z}_5 \mid \gcd(5,k) = 1\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

تمرین 5.6 : با استفاده ا ز لیما 5.10 گروپ های $(\mathbb{Z}_{16}^x, .)$, $(\mathbb{Z}_{20}^x, .)$ و $(\mathbb{Z}_{36}^x, .)$ رادریافت نماید

فصل ششم
حلقه (Ring)

تعریف 6.1 : یک ساختمان الجبری $(R, \oplus, \odot)$ با خواص ذیل بنام حلقه (Ring) یاد میشود.

(1) $(R, \oplus)$ یک گروپ تبدیلی (Commutative group) باشد

(2) اتحادی (Associative) نظربه "$\odot$" :

$$(a \odot b) \odot c = a \odot (b \odot c) \qquad (\forall a, b, c \in R)$$

(3) توزیعی (Disterbutive) نظربه $\odot$-$\oplus$:

$$\forall a, b, c \in R$$
$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$
$$\wedge$$
$$(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a)$$

ما عنصر عینیت (identity) R نظر به "$\oplus$" را به 0_R نشان میدهیم.
اگر رینگ R نظر به "$\odot$" عنصر عینیت (identity) داشته باشد بنام "رینگ با عینیت " (Ring with identity) یاد میشود وما انرابه 1_R نشان میدهیم. یعنی:

$$\exists 1_R \in R;\ a \odot 1_R = a \qquad (\forall a \in R)$$

ما عنصر عینیت را نظر به "$\odot$" بعد از این بنام واحد (unity) یاد میکنیم.
اگر R نظر به "$\odot$" تبدیلی باشد بنام رینگ تبدیلی (Commutative) یاد میشود. یعنی اگر:

$$a \odot b = b \odot a \qquad (\forall a, b \in R)$$

مثال: $(\mathbb{R}, +, .), (\mathbb{Q}, +, .), (\mathbb{Z}, +, .)$ رینگهای تبدیلی اند که عنصر واحد (unity) آن عدد یک "1" است. همچنان $(\mathbb{Z}_n, +, .)$ برای $n \in \mathbb{N}$ یک رینگی تبدیلی که عنصر واحد ان $\bar{1}$ است

يادداشت: ما برای سهولیت به جای $(R, \oplus, \odot)$ بعد از این (R,+,.) مینویسیم، مگربه شرطیکه غلط فهمی صورت نگیرد. نظر به عملیه $\oplus$ عنصر عینیت را به "0" و معکوس a رابه a- نشان میدهیم. نظر به "$\odot$" عنصر واحد را به "1" ومعکوس a رابه a^{-1} نشان میدهیم

مثال6.1: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ نظربه رابطه دوگانه (binary operation) که در جدول نشان داده شده است یک Ring (حلقه) است .

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

مثال 6.2 : R=(0,1,2)

بالاي R رابطه دوگانه (binary operation) ذیل تعریف شده است .

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

به آساني ميتوان ثبوت نمود كه (R ,+ , .) يك Ring (حلقه) است .

تمرين 6.1: M:= **{** $A \in M(2x2, \mathbb{R}) \mid A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ }

ثبوت نماید که (M,+,.) یک حلقه (Ring) است. یعنی M نظربه جمع وضرب ماتریکس ساختمانی رینگی دارد

تمرين 6.2:

S:= $\{2x + 1 \mid x \in \mathbb{Z}\ \}$, R:= { 2x $\mid x \in \mathbb{Z}$ }

ایا (R,+,.) و (S,+,.) رینگ اند

لیما 6.1 **:** (R,+,.) یک رینگ است. برای یک $a \in R$ تابع ذیل G- End است.

$$\rho_a : (R,+) \longrightarrow (R,+)$$
$$x \longmapsto a.x$$

ثبوت:

$$x, y \in R, \rho_a(x+y) = a.(x+y) = \text{a.x + a.y}$$
$$= \rho_a(x) + \rho_a(y)$$

قضیه 6.1 **:** (R,+,.) یک رینگ و صفر ("0") عنصر خنثی نظر به "+" است. برای $a, b, c \in R$ افاده های ذیل صدق میکند.

(1) 0 = 0.a = a. 0

(2) a.(-b) = (-a).b = -(a.b)

(3) (-a).(-b) = a.b

(4) a.(b-c) = (a.b) - (a.c)

ثبوت (1)

(a . 0) + 0 = a.0 = a.(0+0)
= (a.0) + (a.0) [نظربه خاصیت توزیعی]
$\Longrightarrow a.0 = 0$ [نظر به قضیه 1.2]

به همین ترتیب میتوان ثبوت نمود که 0.a = 0 است

ثبوت (2) :

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

پس لهذا (-a).b عنصر معکوس (inverse) از (a.b) است یعنی

-(a. b) = (-a).b

ثبوت (3) : برای ثبوت از تابع $\boldsymbol{\rho_a}$ از لما (6.1) استفاده می نماییم:

(-a).(-b) = $\rho_{-a}(-b) = -\big(\rho_{-a}(b)\big)$ [نظر به قضیه 2.1]

$= -(-a\,.\,b) = a.b$ [معکوسی معکوس خودش است]

ثبوت (4) : در اینجا هم از تابع ρ_a استفاده می نماییم:

$\rho_a : (R,+) \longrightarrow (R,+)$
$b - c \mapsto a.(b-c)$

a.(b –c) = $\rho_a(b-c)$
$= \rho_a b - \rho_a c$ [G-Hom یک "+" نظربه ρ_a زیرا]
$= (a.b) - (a.c)$

تعریف 6.2 **:** (R,+,.) یک رینگ با واحد (unity) است. یک عنصر $a \in R$ بنام unit و یا invertible (معکوس پذیر) یاد میشود درصورت که در R عناصر d,c با خواص ذیل موجود باشند:

c.a=1 ∧ a.d=1

یعنی وقتیکه a نظر به "." معکوس پذیر چپ و راست باشد.

مثال

(a) در رینگ $(\mathbb{Z},+,.)$ تنها 1- و 1 معکوس پذیر(invertible) اند
(b) در رینگ $(\mathbb{Q},+,.)$ غیر از صفر تمام عناصر آن unit اند.
(c) رینگ $(2\mathbb{Z},+,.)$ هیچ عنصر معکوس پذیر(invertible) ندارد .

زیرا عنصر واحد (unity) موجود نیست.

(d) د ر رینگي $(\mathbb{Z}_6, +, .)$ عناصر معکوس پذیر (invertible) $\bar{1}$ و $\bar{5}$ اند . مگر در $(\mathbb{Z}_5, +, .)$ عناصر معکوس پذیر $\bar{1}$ ، $\bar{2}$، $\bar{3}$ و $\bar{4}$ اند

قضیه 6.2 : (R,+,.) یک رینگ با عنصر واحد (unity) است. اگر R_u سیت تمام عناصر معکوس پذیر (invertible) از R باشد. بعداً :

$$a \in R_u, b \in R, (b.a = 1 \vee a.b = 1) \Rightarrow b \in R_u \quad \textbf{(1)}$$

(2) $(R_u, .)$ یک گروپ است.

ثبوت (1) :

$$a \in R_u \Rightarrow \exists c \in R; a.c = 1$$

ما فرض میکنیم که b.a = 1 نیز صدق میکند. بعداً :

$$b = b.1 = b.(a.c) = (b.a).c = 1.c = c$$

$$\Rightarrow a.b = a.c \Rightarrow b.a = 1 = a.c = a.b \Rightarrow b \in R_u$$

ثبوت(2) :

رابطه دوگانه : باید ثبوت شود که "رابطه دوگانه" . " بالای R_u هم قابل تطبیق است. یعنی برای $a, a' \in R_u$ همچنان $a.a' \in R_u$ باشد.

$$a, a' \in R_u \Rightarrow \exists b, b', c, c' \in R; b.a = a.c = 1$$

$$\wedge \quad b'.a' = a'.c' = 1$$

$$(a.a').(c'.c) = a.(a'.c').c = a.1.c = a.c = 1$$

$$(b'.b).(a.a') = b'.(b.a).a' = b'.1.a' = b'.a' = 1$$

$$\Rightarrow a.a' \in R_u$$

$$1.1 = 1 \Rightarrow 1 \in R_u$$

$$\forall a \in R_u, \exists b \in R; a.b = 1 \Rightarrow b \in R_u \quad [\text{ نظر به (1) }]$$

به این معنی که b نظر به "." عنصر معکوس از a است.

تعریف 6.3 : (R,+,.) یک رینگ و $\phi \neq \bar{R} \subseteq R$. سیت $\bar{R}$ بنام رینگ فرعی (subring) یادمیشود، درصورتکه $(\bar{R}, +, .)$ خواص رینگ را داشته باشد.

لیما 6.2 : (R,+,.) یک رینگ، $\phi \neq \bar{R} \subseteq R$. بعداً افاده های ذیل معادل اند:

(1) $\bar{R}$ یک رینگ فرعی (Subring) است.

(2) برای هر $x, y \in \bar{R}$ باید داشته باشیم:

i. $x - y \in \bar{R}$

ii. $x.y \in \bar{R}$

ثبوت "$(\mathbf{1}) \Leftarrow (\mathbf{2})$" : چون هر رینگ فرعی در عین حال یک رینگ است پس $(\bar{R}, +, .)$ نیز رینگ است. بنابراین $(\bar{R}, +)$ یک گروپ فرعی از (+,R) میباشد. نظر به قضیه3.2 افاده $(\boldsymbol{i})$ صدق میکند. شرط $(\boldsymbol{ii})$ نیز صدق میکند. زیرا $\bar{R}$ به حیث رینگ فرعی این خواص (یعنی رابطه دوگانه نظر به ".") را دارد.

ثبوت"$(\mathbf{2}) \leftarrow (\mathbf{1})$"**:** از **(i)** نتیجه میشود که $(\bar{R}, +)$ نظر به قضیه 3.2 يك گروپ فرعي از (+,R) است .

از شرط $(\boldsymbol{ii})$ نتیجه میشود که عملیه "." بالای $\bar{R}$ قابل تطبیق است. "." در R اتحادی (Associative) است، بنابراین در $\bar{R}$ هم صدق میکند. همچنان خاصیت توزیعی (Distributive) نیز در $\bar{R}$ صدق میکند. پس $(\bar{R}, +, .)$ یک رینگ فرعی از R است.

مثال:

(a) $(\mathbb{Q}, +, .), (\mathbb{Z}, +, .)$ رینگهای فرعی در $(\mathbb{R}, +, .)$ اند.

(b) $(2\mathbb{Z}, +, .)$ یک رینگ فرعی در $(\mathbb{Z}, +, .)$ است. مگر بدون عنصر واحد „ 1 “

(c) اگر $(R, +, .)$ یک رینگ باشد، R خودش و {0} رینگهای فرعی آن میباشند.

(d) M(nxn, $\mathbb{Z}$) یک رینگی فرعی از M(nxn, $\mathbb{R}$) است

مثال 3. 6 :

(a) سیت S بشکل ذیل تعریف شده است:

$$S := \{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \} \}$$

S یک رینگی فرعی از M(2x2, $\mathbb{R}$) است و عنصر واحد ان ماتریکس ذیل است:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

که این خلاف عنصر واحد از (M(2x2, ℝ **است**. یعنی:

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} \neq \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

یعنی میتواند عنصرواحد (unity) یک رینگ فرعی S درریںگ R از عنصرواحد ان متفاوت باشد. مگرعناصرعینیت (identity) شان باید متفاوت نباشند

(b)

$$\mathrm{M}:=\{A \in M(2x2,\mathbb{R})\},\ \mathrm{S}:=\{A \in M(2x2,\mathbb{R}) \mid A=\begin{pmatrix}a & b\\ -b & a\end{pmatrix}\}$$

S یک subring در (M,+,.) است. زیرا:

$$A=\begin{pmatrix}a & b\\ -b & a\end{pmatrix}, \mathrm{B}=\begin{pmatrix}c & d\\ -d & c\end{pmatrix} \in \mathrm{S}$$

$$\mathrm{A}-\mathrm{B}=\begin{pmatrix}a & b\\ -b & a\end{pmatrix}-\begin{pmatrix}c & d\\ -d & c\end{pmatrix}=\begin{pmatrix}a-c & b-d\\ -b+d & a-c\end{pmatrix} \in S$$

$$\mathrm{A}.\mathrm{B}=\begin{pmatrix}a & b\\ -b & a\end{pmatrix}.\begin{pmatrix}c & d\\ -d & c\end{pmatrix}=\begin{pmatrix}ac-bd & ad+bc\\ -bc-ad & -bd+ac\end{pmatrix} \in \mathrm{S}$$

S نظربه لیما 6.2 یک رینگ فرعی در (M,+,.) است.

تعریف 6.4 : $(R,+,.)$ یک رینگ است و I یك گروپ فرعي از(R,+) است. I بنام left-ideal یا د میشود درصورتیکه :

$$\forall r \in R, \forall a \in I \Rightarrow r.a \in I \qquad (\ \text{یعنی}\ R.I \subseteq I\ )$$

I بنام right-ideal یاد میشود اگر :

$$\forall r \in R, \forall a \in I \Rightarrow a.r \in I \qquad (\ \text{یعنی}\ I.R \subseteq I\ )$$

I بنام ideal یاد میشود که اگر I یك left-ideal و right-ideal باشد .

مثال 6. 4 : ما میدانیم که سیت R:=M(2x2, ℚ) نظر به ضرب وجمع ماتریکس یک رینگ است یعنی :

(a) **(R,+)** یک گروپ تبدیلی (commutative) است .

(b) $\forall A, B \in R \Rightarrow A.B \in R$

(c) دیگر خواص های رینگ نیز صدق میکند .
عنصرعینت ان ماتریکس صفر وعنصرواحد ان ماتریکس واحد است. یعنی:

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

مثال:

$R:=M(2x2, \mathbb{Z})$, $S:=\{ \begin{pmatrix} 0 & a \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \}$

S رینگی فرعی ازرینگ R نیست. زیرا:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in S$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin S$$

مثال:

$S:= \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$

سیت S یک رینگ فرعی بدون عنصرواحد در رینگ $(\mathbb{Z}_8, +, .)$ است. زیرا:

+	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

.	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{6}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$

جدول های فوق نشان میدهند که بالای S هردو رابطه دوگانه تطبیق میشود. پس یک رینگ فرعی در $\mathbb{Z}_8$ است

مثال: ما L را به شکل ذیل تعریف میکنیم :

$$L:=\{ \begin{pmatrix} 0 & p \\ 0 & q \end{pmatrix} \mid p,q \in \mathbb{Q} \}$$

L یک Left ideal از **(** $\mathbb{Q}$, R=M(2x2) است . زیرا :

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in L$$

$$A = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} , B = \begin{pmatrix} 0 & c \\ 0 & d \end{pmatrix} \in L$$

$$\Rightarrow A + B = \begin{pmatrix} 0 & a+c \\ 0 & b+d \end{pmatrix} \in L , \ -A = \begin{pmatrix} 0 & -a \\ 0 & -b \end{pmatrix} \in L$$

پس (L,+) نظربه قضیه 3.1 یک گروپ فرعی از (R,+) است
علاوه بران:

$$D = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in M(2x2, \mathbb{Q})$$

$$D \cdot A = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \cdot \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & xa+yb \\ 0 & za+tb \end{pmatrix} \in L$$

پس L یک Left ideal در M(2x2, $\mathbb{Q}$) است . مگر right-ideal نیست.

زیرا:

$$A:= \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \in L \ , \ D:= \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \in M(2x2, \mathbb{Q})$$

$$A.D = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} . \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 4 & 6 \end{pmatrix} \notin L$$

تمرین 6.3:

$$R:=M(2x2, \mathbb{Q}) , \ S:=\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x,y,z \in \mathbb{Q} \}$$

ثبوت نماید که S یک Subring (رینگی فرعی) دررینگ R است

تمرین 6.4:

$$M:=\{A\in M(2x2,\mathbb{R})\,|\,A=\begin{pmatrix}a & b\\ -b & a\end{pmatrix}, a^2+b^2\neq 0\}$$

ایا (M,+,.) نظربه جمع "+„ و ضرب ".„ ماتریکس یک حلقه (Ring) است

قضیه 6.2-A : $(R,+,.)$ یک رینگ باعنصرواحد „ 1" است و $I\subseteq R$. بعداً:

(1)

$$\left.\begin{array}{l}(1)\ I\neq\phi\\ (2)\ a,b\in I\Rightarrow a+b\in I\\ (3)\ r\in R, a\in I\Rightarrow r.a\in I\end{array}\right\}\Longleftrightarrow$$

I یک Left ideal

(2)

$$\left.\begin{array}{l}(1)\ I\neq\phi\\ (2)\ a,b\in I\Rightarrow a+b\in I\\ (3)\ r\in R, a\in I\Rightarrow a.r\in I\end{array}\right\}\Longleftrightarrow$$

I یک right-ideal

ثبوت (1) :

" ⇐ " : نظر به تعریف Left ideal (ایدیال چپ) واضح است.

" ⇒ " : اگر $I=\{0\}$ باشد. درانصورت واضح است که I یک ایدیال چپ است.
حالافرض میکنیم که $I\neq\{0\}$ است

$I\neq\phi\ \wedge\ I\neq\{0\}\ \Longrightarrow \exists a\in I$, a ≠ 0
$0\in R, a\in I\Rightarrow 0.a=0\in I$ [نظر به (3)]
$1\in R,\ a\in I\Rightarrow -a=-(1.a)=-1.a$
$\Rightarrow -a\in I$
∀ a, b $\in I\Rightarrow a+b\in I$ [نظر به (2)]
$\Rightarrow (I,+)$ is Subgroup (گروپ فرعی) [نظر به قضیه 3.1]
$\Rightarrow$ Left ideal يك I [نظر به (3)]

به همین ترتیب میتوان (2) را ثبوت نمود.

مثال:

(a) (R,+,.) یک رینگ است. {0} (Zero-ideal) و R خودش ایدیال هستند.

(b) برای رینگ $(\mathbb{Z}, +, .)$ ، گروپ فرعی $(n\mathbb{Z}, +)$ یک ایدیال است. زیرا:

$$\forall\ z \in \mathbb{Z}, nz \in n\mathbb{Z} \Rightarrow nz.z = n(z.z) \in n\mathbb{Z}$$

(c) $(\mathbb{Z}, +, .)$ یک رینگ فرعی از $(\mathbb{Q}, +, .)$ است، مگر ایدیال نیست. زیرا:

$$\frac{1}{2} \in \mathbb{Q}, 1 \in \mathbb{Z}, \frac{1}{2}.1 = \frac{1}{2} \notin \mathbb{Z}$$

لیما 3.6: (R,+,.) یک رینگ است.

(1) $J := \{1, \dots, n\}$ و (I_i) ایدیال ها($i \in J$) در R اند. اگر $I := \cap_{i \epsilon J} I_i$ باشد ، درانصورت I نیز یک ایدیال است

(2) I یک ادیال و S یک رینگ فرعی در R است. بعدآ:

(a) سیت ذیل یک رینگ فرعی در R است

$$S + I = \{ x+y \mid x \in S, y \in I \}$$

(b) $S \cap I$ یک ادیال در S است

(c) I یک ادیال در رینگ فرعی S + I

ثبوت(1):

I نظربه لیما 3.11 یک گروپ فرعی در (R,+) است

$$a \epsilon I, r \epsilon R \Rightarrow a \epsilon I_i \ (\forall\ i \epsilon J)$$
$$\Rightarrow r.a \epsilon I_i \ (\forall\ i \epsilon J) \quad [\text{ زیرا } I_i \text{ ایدیال اند }]$$
$$\Rightarrow r.a \epsilon I$$

ازین نتیجه میشود که I نیز یک ایدیال است.

ثبوت(2):

(a)

$$u, w \in S+I$$
$$\Rightarrow \exists\ u_1, w_1 \in S \wedge \exists\ u_2, w_2 \in I\ ;\ u = u_1+u_2\ ,\ w = w_1+w_2$$
$$\Rightarrow u - w = (u_1 - w_1) + (u_2 - w_2) \in S+I$$

$u.w = (u_1 + u_2) . (w_1 + w_2)$
$= u_1 . w_1 + (u_2 . w_1 + u_1 . w_2 + u_2 . w_2)$
$u_1 . w_1 \in S$ [زیرا S رینگ فرعی]
$u_2 . w_1 + u_1 . w_2 + u_2 . w_2 \in I$ [زیرا I ادیال]
$\Rightarrow u.w \in S + I$

پس S+I نظربه لیما 6.2 رینگ فرعی است

ثبوت(b):

تقاطع سیت های I و S خالی نیست. زیرا عنصرعینیت (identity) شامل هردوی شان است.

$w \in S \cap I \Rightarrow \exists a \in S \wedge \exists b \in I ; w = a , w = b$
$\Rightarrow w.x = a.x = b.x \quad (\forall x \in S)$
$\Rightarrow w.x = a.x \in S \wedge w.x = b.x \in I$
$\Rightarrow w.x \in S \cap I$

درنتجه $S \cap I$ یک ادیال در S است

ثبوت(c):

نظر به (a) میدانیم که S+I یک رینگ فرعی در R است. اکنون میخواهیم ثبوت نمایم که I یک ادیال در S+I است

$x \in S + I \Rightarrow \exists a \in S \wedge \exists b \in I; \; x = a + b$
$y \in I , yx = y(a + b) = ya + yb$

چون I یک ادیال است،پس:

$ya , yb \in I \Rightarrow yx = ya + yb \in I$
$\Rightarrow I \text{ ideal in } S + I$

تعریف 6.5 : (R,+,.) و (S,+,.) دو رینگ اند. تابع $\varphi: R \to S$ بنام Ring homomorphism (R-Hom) یادمیشود،درصورتکه برای هر $a, b \in R$ افاده های ذیل صدق نمایند

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\wedge$$
$$\varphi(a.b) = \varphi(a).\varphi(b)$$

نوت: اگررینگ های فوق عناصرواحد داشته باشند، درانصورت دربعضی کتاب ها در تعریف رینگ هوموموفیزم شرط ذیل راعلاوه می نمایند:

$$\varphi(1_R) = 1_S$$

البته درینجا 1_s عنصرواحد (unity) از S و 1_R عنصرواحد **از R است**.
مگرما درینجا شرط فوق رادرنظرنمی گیریم.
یک R-Hom اگر injective باشد بنام Ring Monomorphism (R-Monom) ، اگر surjective باشد بنام Ring Epimorphism (R-Epim) و اگر bijective باشد بنام Ring Isomorphism (R-Isom) یاد میشود .
یک R-Hom بنام Ring Endomorphism (R-End) یاد میشود، درصورتکه S = R باشد . یک R-End که درعین حال bijective باشد بنام Ring Automorphism ((R-Auto) یاد میشود.
اگر 0_s عنصرعینیت (identity) از S و 0_R عنصرعینیت از R باشد ، در آن صورت:

$$\varphi(0_R) = 0_s$$

زیرا:

$$\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R) \implies \varphi(0_R) = 0_s$$

مثال 6.5 : مامیدانیم که $(\mathbb{C}, +, .)$ یک رینگ است. حالانشان میدهیم که تابع ذیل یک R-Hom است

$$\varphi: (\mathbb{C}, +, .) \longrightarrow (\mathbb{C}, +, .)$$
$$z = (x + iy) \longmapsto \bar{z} = (x - iy)$$

حل:

$z = x + iy$, $z_1 = x_1 + iy_1 \in \mathbb{C}$
درمثال 2.1 دیدیم که φ نظر به "+" درگروپ($\mathbb{C}, +$) یک G-Hom است. یعنی

$$\varphi(z + z_1) = \varphi(z) + \varphi(z_1)$$

ازجانب دیگر:

$$\varphi(z.z_1) = \varphi\big((x + iy).(x_1 + iy_1)\big)$$
$$= \varphi(xx_1 + iyx_1 + ixy_1 - yy_1)$$
$$= \varphi(xx_1 - yy_1 + (yx_1 + xy_1)i)$$
$$= (xx_1 - yy_1) - (yx_1 + xy_1)i$$
$$\varphi(z).\varphi(z_1) = (x - iy).(x_1 - iy_1)$$
$$= xx_1 - iyx_1 - ixy_1 - yy_1$$

$= (xx_1 - yy_1) - (yx_1 + xy_1)i$

در نتیجه $\varphi(z.z_1) = \varphi(z).\varphi(z_1)$

مثال 6.6 : ما بالای رینگ $(\mathbb{Z}_2, +, .)$ تابع ذیل را تعریف مینمایم:

$$\varphi: \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$$
$$\bar{x} \longmapsto \bar{x} \,.\, \bar{x} = (\bar{x})^2$$

φ یک **R-Hom** است. زیرا برای $\bar{x}, \bar{y} \in \mathbb{Z}_2$

$$\varphi(\bar{x} + \bar{y}) = (\bar{x} + \bar{y})^2 = (\bar{x})^2 + \bar{x}.\bar{y} + \bar{x}.\bar{y} + (\bar{y})^2$$

برای $\bar{x}.\bar{y}$ دوحالت ذیل امکان دارد

حالت اول: $\bar{x}.\bar{y} = \bar{0}$ درینصورت

$$\varphi(\bar{x} + \bar{y}) = (\bar{x})^2 + (\bar{y})^2 = \bar{x}.\bar{x} + \bar{y}.\bar{y} = \varphi(\bar{x}) + \varphi(\bar{y})$$

حالت دوم: $\bar{x}.\bar{y} = \bar{1}$ درینصورت

$$\bar{x}.\bar{y} = \bar{1} \Rightarrow \bar{x} = \bar{1} \wedge \bar{y} = \bar{1}$$

$$\Rightarrow \varphi(\bar{x} + \bar{y}) = (\bar{x})^2 + \bar{x}.\bar{y} + \bar{x}.\bar{y} + (\bar{y})^2$$
$$= (\bar{1})^2 + \bar{1}.\bar{1} + \bar{1}.\bar{1} + (\bar{1})^2 = \bar{4} = \bar{0}$$

$$\varphi(\bar{x}) + \varphi(\bar{y}) = (\bar{x})^2 + (\bar{y})^2 = \bar{1}.\bar{1} + \bar{1}.\bar{1}$$
$$= \bar{1} + \bar{1} = \bar{2} = \bar{0}$$

درنتیجه

$$\varphi(\bar{x} + \bar{y}) = \bar{0} = \varphi(\bar{x}) + \varphi(\bar{y})$$
$$\varphi(\bar{x}.\bar{y}) = (\bar{x}.\bar{y})^2 = (\bar{y})^2 \,.\, (\bar{x})^2$$
$$= (\bar{x})^2 \,.\, (\bar{y})^2 \quad [\text{ زیرا } \mathbb{Z}_2 \text{ تبدیلی است }]$$
$$= \varphi(\bar{x}) \,.\, \varphi(\bar{y})$$

درنتیجه φ یک R-Hom است

تمرین 6.5 : در رینگی $(\mathbb{Z}, +, .)$ تابع ذیل تعریف شده است:

$$\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$x \longmapsto 2x$$

ایا φ یک R-Hom است

تمرین 6.6 **:** ایا در رینگی **$(\mathbb{Z}_3, +, .)$** توابع ذیل R-Hom اند **:**

(a) $\varphi: \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$
$\bar{x} \longmapsto \bar{x} \,.\, \bar{x} = (\bar{x})^2$

(b) $\varphi: \mathbb{Z}_3 \to \mathbb{Z}_3$
$\bar{x} \to \bar{x} \,.\, \bar{x} \,.\, \bar{x} = (\bar{x})^3$

تمرین 6.7 :

(a) ثبوت نماید که تابع ذیل یک R-Aut است

$$\varphi: (\mathbb{c}, +, .) \longrightarrow (\mathbb{c}, +, .)$$
$$z = (x + iy) \longmapsto (x - iy)$$

(b) ثبوت نماید که تابع ذیل یک R-Isom است

$$R: = \{A \in M(2x2, \mathbb{R}) \,|\, A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\}$$

$$\varphi: (\mathbb{c}, +, .) \longrightarrow R$$
$$z = a + ib \longmapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

تمرین 6.8 : (R,+,.) یك رینگ دارای عنصر واحد (unity) "1" است و $a \in \boldsymbol{R}$ معکوس پذیر (invertible) است. ثبوت نمائید که تابع ذیل یك R-Aut است

$$L_a: R \longrightarrow R$$
$$x \longmapsto a\, x\, a^{-1}$$

تعریف 6.6 : (R,+,.) یک رینگ است. یک ایدیال I بنام Prime Ideal یاد میشود، اگر:

(a) $I \neq R$

(b) $\forall x, y \in R\,,\ x.y \in I \Rightarrow x \in I \ \vee y \in I$

مثال:

(a) در رینگ $(\mathbb{Z}, +, .)$ سیت $p\mathbb{Z}$ یک Prime Ideal است، درصورتکه P یک عدد اولیه باشد

حل: $p\mathbb{Z} \neq \mathbb{Z}$ است. زیرا برای یک عدد الیه p عدد 4 شامل $p\mathbb{Z}$ شده نمیتواند. وازجانب دیگر:

$$a, b \in \mathbb{Z}\ , a.b \in p\,\mathbb{Z} \Rightarrow p \,|\, a.b \ \Rightarrow p \,|\, a \ \vee \ p \,|\, b$$
$$\Rightarrow a \in p\,\mathbb{Z} \ \vee \ b \in p\,\mathbb{Z}$$

درنتیجه $p\mathbb{Z}$ یک prime ideal است

(b) در رینگ $(\mathbb{Z}, +, .)$ سیت $2\mathbb{Z}$ یک Prime Ideal است
حل: $p\mathbb{Z} \neq \mathbb{Z}$ است. زیرابطور مثال $3 \notin 2\mathbb{Z}$. وازجانب دیگر:

$$a, b \in \mathbb{Z}\ , a.b \in 2\mathbb{Z} \Rightarrow 2 \mid a.b \Rightarrow 2 \mid a \ \vee\ 2 \mid b$$
$$\Rightarrow a \in 2\mathbb{Z} \ \vee\ b \in 2\mathbb{Z}$$
$$\Rightarrow\ 2\mathbb{Z} \text{ prime ideal}$$

مگر در رینگ $(2\mathbb{Z}, +, .)$ ادیال $4\mathbb{Z}$ پرایم ادیال نیست. زیرا:
$2 \in 2\mathbb{Z} \quad \Rightarrow \quad 2.2 = 4 \in 4\mathbb{Z}$
مگر $2 \notin 4\mathbb{Z}$

قضیه 6.4 : اگر (R,+,.)و (S,+,.) دو رینگ و $\varphi: R \to S$ یک R-Hom باشد. بعدآ :

(a) $\ker\varphi$ یک ایدیال در R است .

(b) $\varphi(R)$ یک subring (رینگ فرعی) در S است .

(c) اگر φ یک Surjective باشد و I یک ایدیال در R باشد در آنصورت $\varphi(I)$ یک ایدیال در S است

ثبوت (a) : نظربه قضیه 2.4 میدانیم که $\ker\varphi$ یک گروپ فرعی در R نظر به "+" است و:

$$\text{Ker}\ \varphi := \{a \in R | \varphi(a) = 0_s\}$$
$$r \in R\ ,\ x \in \ker\varphi \ \Rightarrow\ \varphi(r.x) = \varphi(r).\ \varphi(x) = \varphi(r).0_s = 0_s$$
$$\Rightarrow\ r.x \in \ker\varphi$$

درنتیجه $\ker\varphi$ یک ادیال است

ثبوت (b) : نظر به قضیه 2.4 میدانیم $\text{Im}(\varphi) = \varphi(R)$ یک گروپ فرعی در S نظر به رابطه دوگانه "+" می باشد .

$$s_1, s_2 \in \varphi(R) \Rightarrow \exists r_1, r_2 \in R;\ \varphi(r_1) = s_1\ \wedge\ \varphi(r_2) = s_2$$
$$\varphi(r_1.r_2) = \varphi(r_1).\varphi(r_2) = s_1.s_2$$
$$\Rightarrow s_1.s_2 \in \varphi(R)$$

نشان داده شد که رابطه دوگانه (Binary operation) "." بالای $\varphi(R)$ قابل تطبیق است . پس در نتیجه $\varphi(R)$ یک حلقه فرعی (Subring) از S است

ثبوت (c) : چون I یک ایدیال است , پس نظر به تعریف ایدیال یک گروپ فرعی در (R,+) نیز است و $\varphi(I)$ نظر به قضیه 3.3 یک گروپ فرعی در S است .

$b \in \varphi(I), s \in S$

$\Rightarrow \exists a \in I \ \wedge \ r \in R;\ \varphi(a) = b\ , \varphi(r) = s$ [Surjective φ زیرا]

r.a $\in I$ [زیرا I یک ادیال]

$\Rightarrow s.b = \varphi(r).\varphi(a) = \varphi(ra) \in \varphi(I)$

وهم چنان:

$b.s = \varphi(a).\varphi(r) = \varphi(ar) \in \varphi(I)$

در نتیجه $\varphi(I)$ یک ایدیال در S است .

تبصره: در(c) اگر φ سورجیکیف نباشد، درانصورت $\varphi(I)$ ادیال در S نیست. بطورمثال:

$$\varphi: (\mathbb{Z}, +, .) \to (\mathbb{R}, +, .)$$
$$n \mapsto n$$

نظر به تعریف φ یک R-Hom و $\varphi(\mathbb{Z})=\mathbb{Z}$ است. مگر $\mathbb{Z}$ ادیال در $\mathbb{R}$ نیست. زیرا برای $\sqrt{2} \in \mathbb{R}$ و $2 \in \mathbb{Z}$ حاصل ضرب ان شامل $\mathbb{Z}$ نیست.

یعنی: $2.\sqrt{2} \notin \mathbb{Z}$

قضیه 6.5 : (R,+,.) و (S,+,.) دو رینگ و $I \subseteq S$ ، $\rho: R \to S$ یک R-hom. بعداً:

I یک ایدیال در $S \Leftarrow \rho^{-1}(I)$ یک ایدیال در R است.

ثبوت:

$r_1, r_2 \in \rho^{-1}(I) \Rightarrow \rho(r_1), \rho(r_2) \in I$

$\Rightarrow \rho(r_1) + \rho(r_2) = \rho(r_1 + r_2) \in I$

$\Rightarrow r_1 + r_2 \in \rho^{-1}(I)$

$r \in R, r_1 \in \rho^{-1}(I) \Rightarrow \rho(r) \in S \ \wedge \ \rho(r_1) \in I$

$\Rightarrow \ \rho(r).\rho(r_1) \in I$ [زیرا I ادیال]

$\Rightarrow \ \rho(r.r_1) = \rho(r).\rho(r_1) \in I$

$$\Rightarrow r.r_1 \in \rho^{-1}(I)$$

در نتیجه $\rho^{-1}(I)$ یک ایدیال در R است

تعریف*A-6.6*: (R,+,.) یک رینگ و I یک ادیال در R است. ما set (مجموعه) تمامی left-coset از I در R را به R/I نشان میدهیم . یعنی:

$$R/I := \{ a + I \mid a \epsilon R \}$$

نظر به تعریف رینگ (R,+) یک گروپ تبدیلی (ablean group) است و ادیال I یک گروپ فرعی نورمال در R است. $(R/I, +)$ نظر به قضیه 3.18 با رابطه دوگانه ذیل یک فکتور گروپ (factor group) است :

$$+ : R/I \; x \; R/I \longrightarrow R/I$$
$$(a + I, b + I) \mapsto (a + I) + (a + I) = (a + b) + I$$

حالا رابطه دوگانه "." رابه شکل ذیل بالای R/I تعریف می نمایم:

$$. : R/I \; x \; R/I \longrightarrow R/I$$
$$(a + I, b + I) \mapsto (a + I).(a + I) = (a.b) + I$$

درنتیجه $(R/I, +, .)$ یک رینگ است و بنام فکتوررینگ (factor ring) یاد میشود

مثال: ما رینگ $(\mathbb{Z}_6, +, .)$ رادرنظرمیگریم، که دران سیت I به شکل ذیل تعریف شده است:

$$I := \{\bar{0}, \bar{2}, \bar{4}\}$$

I یک ادیال در $\mathbb{Z}_6$ است. زیرا:

اول: I یک گروپ فرعی در $(\mathbb{Z}_6, +)$ است.

دوم: رابطه ذیل نیزصدق میکند

$$\forall \bar{a} \in I \; \wedge \; \forall \bar{b} \in \mathbb{Z}_6 \implies \bar{a}.\bar{b} \in I$$

پس فکتوررینگ $(\mathbb{Z}_6/I, +, .)$ شکل ذیل را دارد:

$$\mathbb{Z}_6/I = \{\bar{a} + I \mid \bar{a} \epsilon \mathbb{Z}_6\} = \{ I, \{\bar{1}, \bar{3}, \bar{5}\} \}$$

اگرما $H := \{\bar{1}, \bar{3}, \bar{5}\}$ بنوسیم، درانصورت :

$$\mathbb{Z}_6/I = \{ I, H \}$$

نظر به رابطه دوگانه "+„ عنصرعینیت ان I و معکوس H خودش است. زیرا:

$$\begin{aligned} \mathrm{I}+\mathrm{H} &= \{\{\bar{0},\bar{2},\bar{4}\}+\{\bar{1},\bar{3},\bar{5}\} = \{\bar{0}+\bar{1},\bar{0}+\bar{3},\bar{0}+\bar{5},\bar{2}+\bar{1},\\ &\quad \bar{2}+\bar{3},\bar{2}+\bar{5},\ \bar{4}+\bar{1},\bar{4}+\bar{3},\bar{4}+\bar{5}\}\\ &= \{\bar{1},\bar{3},\bar{5},\bar{3},\bar{5},\bar{1},\bar{5},\bar{2},\bar{3}\} = \{\bar{1},\bar{3},\bar{5}\} = \mathrm{H}\\ \mathrm{H}+\mathrm{H} &= \{\{\bar{1},\bar{3},\bar{5}\}+\{\bar{1},\bar{3},\bar{5}\}\\ &= \{\bar{1}+\bar{1},\bar{1}+\bar{3},\bar{1}+\bar{5},\bar{3}+\bar{1},\bar{3}+\bar{3},\bar{3}+\bar{5},\\ &\quad \bar{5}+\bar{1},\bar{5}+\bar{3},\bar{5}+\bar{5}\}\\ &= \{\bar{2},\bar{4},\bar{0},\bar{4},\bar{0},\bar{2},\bar{0},\bar{2}\} = \{\bar{0},2,\bar{4}\} = \mathrm{I} \end{aligned}$$

خواص دیگری گروپ نیز صدق میکند. درنتیجه $(\mathbb{Z}_6/I\ ,+)$ یک گروپ تبدیلی است. بالای $\mathbb{Z}_6/I$ رابطه دوگانه "."„ برای $\bar{a},\bar{b}\in\mathbb{Z}_6$ به شکل ذیل تعریف شده :

$$(\bar{a}+I).(\bar{b}+I) = (\bar{a}.\bar{b})+I$$

$\mathbb{Z}_6/I$ نظر به رابطه دوگانه "."„ ساختمان الجبری دارد. بطورمثال:

$$\bar{a}=\bar{3}\ ,\bar{b}=\bar{5} \implies \bar{a}.\bar{b}+I = \bar{3}.\bar{5}+\{\bar{0},\bar{2},\bar{4}\} = \bar{3}+\{\bar{0},\bar{2},\bar{4}\}$$
$$= \{\bar{3},\bar{5},\bar{1}\} = H \in (\mathbb{Z}_6/I\ ,\ .)$$

این رابطه دوگانه بالای عناصردیگر نیز صدق میکند. پس $(\mathbb{Z}_6/I\ ,+,.)$ فکتوررینگ است

قضیه 6.4-A **(theorem of ring homomorphism) :**

اگر (R,+,.) و (S,+,.) دو رینگ و $\varphi: R\to S$ یک R-Hom باشد، درانصورت دربین $R/\mathrm{Ker}\ \varphi$ و S یک R-Hom موجود است که $R/\mathrm{Ker}\ \varphi$ و $\varphi(R)$ ایزومورف اند. یعنی: $\varphi(R)\ \cong\ R/\mathrm{Ker}\ \varphi$

ثبوت:

نظر به قضیه 4.6 ما میدانیم که $\mathrm{Ker}\ \varphi$ یک ادیال است و انرا به I نشان میدهیم. پس R/I نظر به تعریف 6.6-A یک فکتوررینگ است

حالا تابع ذیل را درنظرمیگریم:

$$\psi:\ R/\mathrm{I}\longrightarrow \mathrm{S}$$
$$\mathrm{a}+I\ \longmapsto\ \varphi(a)$$
$$\psi\big((a+I)+(b+I)\big) = \psi\big((a+b)+I\big) \quad [\text{ نظربه قضیه } 3.18\ ]$$
$$= \varphi(a+b)$$

$= \varphi(a) + \varphi(b)$ [R-Hom يک φ]
$= \psi(a + I) + \psi(b + I)$
$\psi\big((a + I).(b + I)\big) = \psi\big((a.b) + I\big)$ [نظر به تعريف "."]
$= \varphi(a.b) = \varphi(a).\varphi(b)$
$= \psi(a + I).\ \psi(b + I)$

درنتيجه ψ يک R-Hom است.

: $injective\ \psi$

$\psi(a + I) = \psi(b + I)$
$\Longrightarrow \varphi(a) = \varphi(b) \Longrightarrow \varphi(a) - \varphi(b) = 0_s$
$\Longrightarrow \varphi(a - b) = 0_s \Longrightarrow a - b \in I$ [زيرا $I = \ker\varphi$]
$\Longrightarrow a + I = b + I$ [نظربه قضيه 3.11]
$\Longrightarrow \psi$ injective

ازجانب ديگر:

$y \in \varphi(R) \subseteq S$
$\Longrightarrow \exists x \in R\ ; \varphi(x) = y \Longrightarrow \psi(x + I) = \varphi(x) = y$
$\Longrightarrow \psi : R/I \longrightarrow \varphi(R)$ surjective

درنتيجه: $\varphi(R) \cong R/N$

قضيه 6.4-B (**theorem of ring isomorphism**) :
اگر S رينگ فرعی و I اديال دررينگ (R,+,.) باشد، درانصورت:
(1) $S/S \cap I$ و $(S + I)/I$ فکتوررينگ ها (ring-factors) اند

(2) $(S + I)/I \cong S/S \cap I$
(يعنی $S/S \cap I$ و $(S + I)/I$ باهم ديگر رينگ ايزومورف اند)

ثبوت (1): نظر به ليما 6.3 ميدانيم:
$S + I$ يک رينگ فرعی در R ، $S \cap I$ اديال در S و I اديال در $S + I$
پس $S/S \cap I$ و $(S + I)/I$ فکتوررينگ (ring-factors) اند

ثبوت (2): نظربه قضيه 6.4-A تابع ذيل نيز R-Hom است:

$\varphi: S \longrightarrow R/I$
$a \longmapsto a + I$
$\varphi(S) = \{ s + I \mid s \in S \}$

$= \{ (s + v) + I \mid s \in S, v \in I\}$ [نظر به قضیه 3.11]

$= (S + I)/I$ [نظر به تعریف φ]

نظربه قضیه 6.4-A تابع ذیل R-Isom است:

$$\varphi^{-} : R/ker\varphi \longrightarrow \varphi(R)$$
$$a.\ker\varphi \longmapsto \varphi(a)$$

در (1) دیدیم که $S \cap I$ ادیال در S است. پس قضیه 3.19 بالای رینگ فرعی S نیز صدق میکند. یعنی تابع ذیل یک R -Isom است

$$\varphi^{-} : S/S \cap I \to \varphi(S)$$
$$a.\ker\varphi \to \varphi(a)$$

چون $S/S \cap I \cong \varphi(S)$ و $\varphi(S) = (S + I)/I$ است. درنتیجه:

$$(S + I)/I \cong S/S \cap I$$

تعریف 6.7 : یک ایدیال I از رینگ R بنام Principle Ideal (ادیال اساسی) یاد میشود، درصورتکه I تنها از یک عنصر بوجود آمده باشد. یعنی:

$\exists a \in R$; $<a> = I$

مثال: سیت ذیل برای $n \in \mathbb{N}$ یک Principle Ideal است:

$$< n >:= n\mathbb{Z} = \{n.a \mid a \in \mathbb{Z}\}$$

تعریف 6.8 : (R ,+,.) یک رینگ $a \in R$ و $a \neq 0$. عنصر a بنام Left-zero-divisor (l.z.divisor) (قاسم صفراز چپ) یاد میشود اگر یک $b \in R$ و $b \neq 0$ با خاصیت a.b=0 موجود باشد.اگرb.a=0 باشد دراینصورت a یک Right-zero-divisor(r.z.divisor) (قاسم صفر از راست) یاد میشود. اگر a هم l.z.divisor وهم r.z.divisor باشد بنام zero divisor (قاسم صفر) یاد میشود.

تعریف 6.9 : یک رینگ (R,+,.) بنام Ring without zero divisor (رینگ بدون قاسم صفر) یاد میشود. اگر:

$$r_1, r_2 \in R\ , r_1 . r_2 = 0 \Rightarrow r_1 = 0 \ \vee \ r_2 = 0$$

یعنی بدون صفر دیگر هیچ zero-divisor نداشته باشد.

قضیه 6.6 : (R,+,.) و (S,+,.) دورینگ که 1_R و 1_S عناصر واحد (Unity) اند.ماداریم:

$\varphi: R \to S$ $Ring\ Epimorphism$ $\wedge$ $\varphi(1_R) = 1_S$

بعداً افاده های ذیل معادل هستند:

(1) S بدون قاسم صفر (without zero-divisor) و $0_S \neq 1_S$

(2) $Ker\varphi$ یک Prime ideal است.

ثبوت: ما عنصرعینیت R رابه 0_R واز S رابه 0_S نشان میدهیم

: "$(\mathbf{1}) \Rightarrow (\mathbf{2})$"

$x, y \in R, x.y \in Ker\varphi$

$\Rightarrow \varphi(x.y) = 0_S$

$\Rightarrow \varphi(x).\varphi(y) = \varphi(x.y) = 0_S$

$\Rightarrow \varphi(x) = 0_S \ \vee \ \varphi(y) = 0_S$ [زیرا S بدون قاسم صفر]

$\Rightarrow x \in Ker\ \varphi \ \vee \ y \in Ker\ \varphi$

$1_S \in S \Rightarrow \exists r \in R, \varphi(r) = 1_S$ [زیرا φ یک سوریکتیف]

$\Rightarrow r \notin Ker\varphi$ [زیرا $0_S \neq 1_S$]

$\Rightarrow Ker\varphi \neq R$

چون نظر به قضیه 6.4 میدانیم که $Ker\varphi$ یک ایدیال است. پس ثبوت شد که φ یک Prime ideal است.

ثبوت "$(\mathbf{2}) \Rightarrow (\mathbf{1})$" **:** اول نشان میدهیم که S بدون zero-divisor است.

$s_1, s_2 \in S, s_1.s_2 = 0_S$

$\Rightarrow \exists x, y \in R \ ; \ s_1 = \varphi(x) \ \wedge \ s_2 = \varphi(y)$ [φ سورجکتیف]

$\Rightarrow 0_S = s_1.s_2 = \varphi(x).\varphi(y) = \varphi(x.y)$

$\Rightarrow x.y \in Ker\ \varphi$

$\Rightarrow x \in Ker\ \varphi \ \vee \ y \in Ker\ \varphi$ [$Ker\varphi$ یک prime ideal]

$\Rightarrow \varphi(x) = 0_S \ \vee \ \varphi(y) = 0_S$

$\Rightarrow s_1 = 0_S \ \vee \ s_2 = 0_S$

پس S بدون zero-divisor (قاسم صفر) است.حالا باید ثبوت شود که $0_S \neq 1_S$ در S است.

اگر $1_S = 0_S$ باشد در آنصورت:

$\varphi(1_R) = 1_S = 0_S = \varphi(0_R)$

$\Rightarrow 1_R \in Ker\ \varphi$

$\Rightarrow R.1_R = R \subseteq Ker\ \varphi$ [زيرا Ker φ يک ايديال است]

از جانب ديگر ميدانيم که $Ker\ \varphi \subseteq R$ است. پس در نتيجه $Ker\ \varphi = R$ ميشود. که اين در تضاد با تعريف Prime ideal است. بنابراين $0_S \neq 1_S$ است.

تعريف6.10 : يك حلقه (ring) تبديلي (commutative) (R,+,.) كه داراي عنصر واحد (unity) وبدون قاسم صفر (no zero divisor) باشد بنام Integral domain (ناحيه تمامی) ياد ميشود. يعنی بايد افاده ذيل صدق كند

$r_1, r_2 \in R\ , r_1.r_2 = 0\ \Rightarrow r_1 = 0\ \vee\ r_2 = 0$

ويا

$r_1, r_2 \in R\ , r_1 \neq 0\ \wedge\ r_2 \neq 0 \Rightarrow\ r_1.r_2 \neq\ 0$

بطورمثال $(\mathbb{Z}, +, .)$ و $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ و $(\mathbb{C}, +, .)$ integral domain اند .

تعريف: سيت ذيل بنام Gaussian integers ياد ميشود

$\mathbb{Z}[i] = \{ a + ib \mid a,b \in \mathbb{Z} \} \subset \mathbb{C}$

$(\mathbb{Z}[i], +, .)$ يک رينگ است وبنام Gaussian Ring ياد ميشود

مثال: $\mathbb{Z}[i]$ يک رينگ فرعی از $(\mathbb{C}, +, .)$ و integral domain نيزاست

حل:

$a + ib, c+id \in \mathbb{Z}[i]$

$a + ib - (c+id) = (a-c) + i(b-d)$

$a - c\ , b-d \in \mathbb{Z} \Longrightarrow (a + ib) - (c+id) \in \mathbb{Z}[i]$

$(a + ib).(c+id) = ac + ibc + iad - bd = (ac - bd) + i(bc + ad)$

$(ac - bd)\ , (bc + ad) \in \mathbb{Z} \Longrightarrow (a + ib).(c+id) \in \mathbb{Z}[i]$

درنتيجه $\mathbb{Z}[i]$ نظربه ليما 6.2 يک رينگ فرعی در $(\mathbb{C}, +, .)$ است.

چون $(\mathbb{C}, +, .)$ يک اينتگرال دومين بوده، پس $\mathbb{Z}[i]$ نيز است. مگر ايديال در $(\mathbb{C}, +, .)$ نيست. زيرا:

$z := \frac{2}{3} \in (\mathbb{C}, +, .)\ ,\ \ z_1 := 1 + 2i \in \mathbb{Z}[i]$

$z.z_1 = \frac{2}{3}.(1 + 2i) = \frac{2}{3} + \frac{4}{3}\ i \notin \mathbb{Z}[i]$

پس نظر به تعريف $\mathbb{Z}[i]$ يک ايديال در $(\mathbb{C}, +, .)$ نيست.

در مثال 6.1 ديديم كه $(\mathbb{Z}_6, +, .)$يك حلقه (Ring) است مگر integral domain نيست. زيرا $\bar{0} = \bar{6} = \bar{2}.\bar{3}$ مگر $\bar{2}$ و $\bar{3}$ خلاف $\bar{0}$ اند

مثال 6.7 $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ نظر به عمليات "+" و "." كه در جدول ذيل تشريح شده است يك حلقه (Ring) است .

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$(\mathbb{Z}_5, +, .)$ يك حلقه (Ring) تبديلي داراي عنصر واحد (unity) "$\bar{1}$" ميباشد.

$\mathbb{Z}_5$ يک Integral domain نيزاست. زيرا $(\mathbb{Z}_n^*, .)$ نظر به قضيه 3.21 يک گروپ است درصورتکه n يک عدد اوليه باشد.

$\bar{b}, \bar{a} \in \mathbb{Z}_5$, $\bar{a} \neq \bar{0} \ \wedge \ \bar{a} . \bar{b} = \bar{0}$

$\Rightarrow \bar{b} = \bar{1}. \bar{b} = (\bar{a})^{-1}.\bar{a} . \bar{b} = (\bar{a})^{-1} . \bar{0} = \bar{0}$

$\Rightarrow \mathbb{Z}_5$ Integ-domain

مثال: R:= M(2x2, $\mathbb{R}$) و ماميدانيم كه (R,+,.) يک رينگ است. مگر integral domain نيست. زيرا:

$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in R$

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

دیده شد که حاصل ضرب A و B مساوی به صفراست مگرخودشان خلاف صفراند R رینگ تبدیلی هم نیست. زیرا:

$B.A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = A.B$

مثال: (D,+,.) و (S,+,.) دو integral domain که دارای عناصرعینیت (identity) $0_D \in D$ ، $0_S \in S$ وعناصرواحد (unity) 1_D و 1_S اند.
بالای R:= DxS روابط دوگانه ذیل تعریف شده است

$$+: RxR \longrightarrow R$$
$$(a,b) \longmapsto a+b$$
$$.: R \times R \longrightarrow R$$
$$(a,b) \longmapsto a.b$$

یعنی اگر $a = (d_1, s_1)$ و $b = (d_2, s_2)$ باشند. درانصورت:

$$a + b = (d_1, s_1) + (d_2, s_2) = (d_1+d_2, s_1+s_2)$$

$$a \,.\, b = (d_1, s_1) \,.\, (d_2, s_2) = (d_1.d_2, s_1.s_2)$$

(R,+,.) یک رینگ تبدیلی (commutative ring) است که عنصرعینیت ان $(0_D,0_S)$ و عنصرواحد ان $(1_D,1_S)$ است. مگریک integral domain نیست. زیرا:

$$(1_D,0_S) \,.\, (0_D,1_S) = (1_D \,.\, 0_D, 0_S \,.\, 1_S) = (0_D,0_S)$$

دیده شد که $(1_D,0_S)$ و $(0_D,1_S)$ خلاف صفراند مگرحاصل ضرب شان مساوی به صفراست

تعریف: $(R,+,.)$ یک integral domain است. اگر تابع $\varphi: R \longrightarrow \mathbb{N}_0$ باخواص ذیل موجود باشد:

(i) $\varphi(a) \leq \varphi(a.b) \quad (\forall\, a,b \in R \setminus \{0\}$

(ii) $\forall\, a,b \in R \setminus \{0\};\ \exists q,r \in R;\ a = bq + r$

که درینجا برای $r \neq 0$ باید $\varphi(r) \leq \varphi(b)$ باشد

R با φ بنام Euclidean Domain یاد میشود. ما انرا به (R, φ) نشان میدهیم

مثال: مامیدانیم که $(\mathbb{Z}, +, .)$ یک اینتگرال دومین است. حالا ثبوت می نمایم، که $\mathbb{Z}$ نظربه تابع ذیل یک Euclidean Domain است

$$\varphi: \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}_0$$
$$a \longmapsto |a|$$

$0 \neq a,b \in \mathbb{Z}$

$\varphi(a) = |a| \leq |a|.\,|b| = |ab| = \varphi(ab) \Longrightarrow$ (i)

حالا خاصیت (ii) راثبوت می نمایم . نظربه division algorithm :

$\exists q,r \in \mathbb{Z};\ a = bq + r \quad (0 \leq r < b)$

$r = 0 \Longrightarrow \varphi(0) = |0| < |b| = \varphi(b)$ [زیرا $b \neq 0$]

$r \neq 0 \Longrightarrow \varphi(r) = |r| < |b| = \varphi(b)$ [زیرا $0 \leq r$]

درنتیجه $(\mathbb{Z}, \varphi)$ یک Euclidean Domain است

تعریف 6.11 : $(R, +, .)$ يك رينگ داراي عنصر واحد (unity) "1" است .
R داراي مشخصه معين (finite characteristic) است، درصورتكه يك $n \in \mathbb{N}$ با خاصيت ذيل موجود باشد:

$0 = 1+1+1+\ldots+1$ (n terms (n دفعه))

يعني $n.1 = 0$

كوچكترين آن نوع n بنام مشخصه (characteristic) از R ياد ميشود. يعنى :

$$Char(R) := \min\{n \in \mathbb{N} \mid n.1 = 0\}$$

يا به عبارت ديگر $char(R) = ord(1)$ نظربه گروپ $(R, +)$ است.
اگر آنطور يك n پيدا نشود در آن صورت R داراى zero characteristic (مشخصه صفر) است . يعنى $char(R) = 0$

بطور مثال : رينگ $\mathbb{Z}$ داراي مشخصه (characteristic) صفر ميباشد . زيرا هيچ $n> 0$ يافته نميتوانيم كه n .1=0 شود .

$1 , 1+1 , 1+1+1 , 1+1+1+1, . . . = 1,2,3,4, ...$

ديده ميشود كه هيچ تكرار صورت نمي گيرد پس char($\mathbb{Z}$)=0

اگر ما رينگ (Ring) $\mathbb{Z}_n$ را در نظر بگيريم :

$\bar{1} , \bar{1}+\bar{1} , \bar{1}+\bar{1}+\bar{1}, \bar{1}+\bar{1}+\bar{1}+\bar{1}, . . .$

در اينجا ديده ميشود كه تكرار صورت مي گيرد .

$\bar{0} , \bar{1}, \bar{2}, \bar{3}, ..., \overline{(n-1)} , \bar{0}, \bar{1}, \bar{2}, \bar{3}, ... , \overline{(n-1)}, \bar{0}$

يعني $n . \bar{1} = \bar{0}$) و رينگ $\mathbb{Z}_n$ داراي finite characteristic

(مشخصه معين) ميباشد . يعني $\text{char}(\mathbb{Z}_n) = n$. بطور مثال در $\mathbb{Z}_5$:

$5 . \bar{1} = \bar{1} + \bar{1} + \bar{1} + \bar{1} + \bar{1} = \bar{0} \Rightarrow \text{char}(\mathbb{Z}_5) = \text{ord}(\bar{1}) = 5$

قضيه 6.7 : ما رينگ (R,+,.) با عنصر واحد (unity) و داراى مشخصه (characteristic) متناهى داريم . يعنى 0 ≠ p= char (R) .

بعدآ :

(a) $p . a = 0 \quad \forall a \in R$

(b) $R \ integral\ domain \Rightarrow p \in P$ [p يک عدد اوليه]

ثبوت (a)

$a \in R \Rightarrow p.a = p.(1.a) = (p.1).a = 0.a = 0$

ثبوت (b)

$\exists r, s \in \mathbb{N} ; p = r.s \Rightarrow 0 = p.1 = (r.1).(s.1)$

$\Rightarrow r.1 = 0 \vee s.1 = 0$ [زيرا R يک $integ - dom$ است]

از آن نتيجه ميگيريم كه r و يا s نيز مشخصه (charact) از R است .

چون $r.s = p$ است پس بايد r = p ويا s = p باشد كه در نتيجه p بايد يک عدد اوليه باشد .

ليما 6.4 : (D,+,.) يك integral Domain بعدآ :

$a,b,c \in D \ , \ c \neq 0 \quad a.c = b.c \quad \Rightarrow a = b$

(یعنی یک integral domain نظر به "." اختصار پذیر است)

ثبوت :

a.c = b.c
(a - b) .c = a.c - b.c = 0
$\Rightarrow a - b = 0 \ \vee c = 0$ [integral domain یك D زیرا]
$\Rightarrow a - b = 0$ [c≠ 0 زیرا]
$\Rightarrow a = b$

نوت: لیما 6.4 برای رینگ صدق نمی کند. یعني اختصارپذیرنیست . په طور مثال دررینگ $(\mathbb{Z}_6, +, .)$:

$\bar{2} . \bar{3} = \bar{6} = \bar{0} = \overline{12} = \bar{3} . \bar{4}$

مگر $\bar{2} \neq \bar{4}$ است

لیما 6.5 : (R,+,.) یک حلقه (ring) دارای nity (واحد) , I یک ادیال در R و $I \neq \{0\}$. بعدآ اگر I دارای یک عنصر معکوس پذیر (invertible) باشد در آنصورت I = R . یعنی :

$\exists a \in I \ \wedge \ b \in R; a.b = 1 \Rightarrow I = R$

ثبوت :

$a \in I \ \wedge \ a \ invertible \ \Rightarrow \ \exists b \in R; ba = 1$
$x \in R \Rightarrow x = x.1 = x.(b.a)$
$= (xb).a \in I$ [I یک ایدیال است]
$\Rightarrow R \subseteq I$

از جانب دیگر میدانیم که $I \subseteq R$ است پس I = R

مثال: (D,+,.) یک integ-dom است. a,b ∈ D

(a) اگر $char(D)$ صفر باشد.(بطورمثال در اعداد حقیقي $\mathbb{R}$) ، درانصورت به اساس فورمول Binomial :

$(a + b)^2 = a^2 + 2.ab + b^2$
$(a + b)^3 = a^3 + 3.a^2b + 3ab^2 + b^3$

(b) اگر $char(D) = 2$ باشد،درانصورت :

$(a + b)^2 = a^2 + 2.ab + b^2 = a^2 + 0 + b^2 = a^2 + b^2$

زیرا $char(D) = 2$ است. پس به اساس قصیه 6.7 باید $2ab = 0$ باشد

(c) اگر $char(D) = 3$ باشد. درانصورت:

$(a+b)^3 = a^3 + 3.a^2b + 3ab^2 + b^3$
$= a^3 + 0 + 0 + b^3 = a^3 + b^3$

زیرا $char(D) = 3$ است. پس به اساس قضیه 6.7 باید $3.a^2b = 0$ و $3ab^2 = 0$ باشد

دیده میشود که درالجبر فورمول Binomial تابع characteristic (مشخصه) یک integral domain(ویا Field) ان است.

حالا میخواهیم این حالت را بصورت عمومي مطالعه نمایم.

لیما 6.6 : (D,+,.) یک integ-dom و $char(\mathrm{D}) = p \neq 0$. بعداً :

(a) $(a+b)^p = a^p + b^p \quad (\forall a,b \in \mathrm{D})$

(b) $\varphi: D \longrightarrow D$
$x \longmapsto x^p$

φ یک $injective$ و $R - Hom$ $(\mathrm{R} - \mathrm{Monom})$ است و بنام frobenius function یاد میشود .

(c) $a_1, a_2, \ldots, a_n \in D$
$(a_1 + a_2 + \ldots + a_n)^p = (a_1)^p + (a_2)^p + \ldots + (a_n)^p$

ثبوت (a) : چون D تبدیلی است. پس $(a.b)^p = a^p.b^p$ $(\forall a,b \in D)$
نظر به binomial formel میتوان نوشت .

$$(a+b)^p = a^p + pa^{p-1}.b + \frac{p.(p-1)}{2!}\,a^{p-2}.b^2 + \frac{p.(p-1).(p-2)}{3!}\,a^{p-3}.b^3 + \cdots + pab^{p-1} + b^p$$

ویا

$$(a+b)^p = a^p + \sum_{i=1}^{p-1}\left(\frac{p!}{i!(p-i)!}\right).a^{\,i}.b^{p-i} + b^p$$

در معادله فوق اگر a^p و b^p در نظر گرفته نشود. درانصورت هریکی ان بصورت عموم شکل ذیل رادارد:

$$\frac{p.(p-1).(p-2)\ldots.(\mathrm{p}-\mathrm{r}+1)}{1.2.3\ldots.r}\,a^{p-r}.b^r$$

البته درینجا $1 \leq r \leq$ p-1 فرض شده است.

$k: = \frac{(p-1).(p-2).....(p-r+1)}{1.2.3....r}$, s:= 1.2.3....r

p.k به اساس *binomial formel* یک عدد مثبت تام است . پس باید p.k بالای s قابل تقسیم باشد. چون p>r و p نظر به قضیه 6.7 یک عدد اولیه است. پس باید k بالای s قابل تقسیم باشد. یعني:

$k = \frac{(p-1).(p-2).....(p-r+1)}{1.2.3....r}$ یک عدد طبعي است.

پس نظر به قضیه 6.7 :

$\frac{p.k}{s} a^{p-r} . b^r = \frac{p.(p-1).(p-2).....(p-r+1)}{1.2.3....r} a^{p-r} . b^r = 0$

$(a+b)^p = a^p + 0 + 0 + \cdots + 0 + b^p = a^p + b^p$

ثبوت (b)

$x, y \in D$; $\varphi(x+y) = (x+y)^p = x^p + y^p$ [نظر به (a)]
$= \varphi(x) + \varphi(y)$

$\varphi(x.y) = (x.y)^p = y^p . x^p$
$= x^p . y^p$ [زیرا D تبدیلی است]

$\Longrightarrow \varphi$ R-Hom

: φ *injective*

$x \in ker\varphi \Rightarrow \varphi(x) = 0 \wedge \varphi(x) = x^p$
$\Rightarrow 0 = x^P = x.x.x \ldots . x$ [p دفعه]
$\Rightarrow x = 0$ [زیرا D یک $integ - dom$]
$\Rightarrow ker\,\varphi = \{0\}$

پس نظر به قضیه 2.3 تابع φ یک injective بوده ودرنتیجه φ یک R-monom است.

ثبوت (c) نظر به (a) میتوان نوشت:

$(a_1 + a_2 + ... + a_n)^p = (a_1)^p + (a_2 + ... + a_n)^p$
$= (a_1)^p + (a_2)^p + (a_3 + ... + a_n)^p$

اگربه همین شکل ادامه داده شود، درنتیجه:

$(a1 + a2 + ... + an)p = (a1)p + (a2)p + ... + (an)p$

مثال: ما دوانتگرال دومین $(\mathbb{R}, +, .)$ و $(\mathbb{Z}_2, +, .)$ رادرنظرمیگریم. $\mathbb{R}$ دارای مشخصه صفر و $\mathbb{Z}_2$ دارای مشخصه 2 است. یعنی

$char(\mathbb{Z}_2)=2$, $char(\mathbb{R}) = 0$

(a)

$$\varphi: \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$$
$$\bar{x} \longmapsto (\bar{x})^2$$

φ R-Hom:

$\bar{x}, \bar{y} \in \mathbb{Z}_2$

$\varphi(\bar{x} + \bar{y}) = (\bar{x} + \bar{y})^2 = (\bar{x})^2 + (\bar{y})^2$ [**زیرا** $char(\mathbb{Z}_2)=2$]

$= \varphi(\bar{x}) + \varphi(\bar{y})$

$\varphi(\bar{x}.\bar{y}) = (\bar{x}.\bar{y})^2 = (\bar{x})^2 . (\bar{y})^2 = \varphi(\bar{x}) . \varphi(\bar{y})$

φ injective:

$\bar{x} \in \ker(\varphi)$

$\varphi(\bar{x}) = \bar{0} = (\bar{x})^2 = \bar{x}.\bar{x}$

$\Longrightarrow \bar{x} = \bar{0}$ [زیرا $\mathbb{Z}_2$ یک $integ - dom$]

$\Longrightarrow ker\,\varphi = \{\bar{0}\}$

چون φ یک R-Hom است، پس نظر به قضیه 2.3 یک injective باید باشد

(b)

$$\varphi: \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto x^2$$

φ R-Hom:

$x, y \in \mathbb{R}$

$\varphi(x + y) = (x + y)^2 = x^2 + 2xy + y^2 \neq x^2 + y^2 = \varphi(x) + \varphi(y)$

زیرابطورمثال:

$x = 2 , y = 3$

$\varphi(2 + 3) = (5)^2 = 25 \neq 13 = 2^2 + 3^2 = \varphi(2) + \varphi(3)$

پس R-Hom نیست
φ انجکتیف نیزنیست. زیرا: $\varphi(2) = 4 = \varphi(-2)$ بوده. مگر 2- ≠ 2 است
مثال : مامیخوهیم که $(\bar{2})^9$ را در $\mathbb{Z}_3$ دریافت نمایم. چون $\mathbb{Z}_3$ یک Integ-Domain و $Char(\mathbb{Z}_3) = 3$ است . پس در حل ان از لیما 6.6 استفاده می نمایم

$$(\bar{2})^9 = ((\bar{2})^3)^3 = ((\bar{1} + \bar{1})^3)^3$$
$$= ((\bar{1})^3 + (\bar{1})^3)^3 = (\bar{1})^3 + (\bar{1})^3 = \bar{2}$$

تمرین 6.9: برای حل **از** لیما 6.6 استفاده نماید
(a) $(\bar{2})^{49}$ را در $(\mathbb{Z}_7,+,.)$ دریافت نماید
(b) $(\bar{2})^8$ را در $(\mathbb{Z}_2,+,.)$ دریافت نماید
(c) $(\bar{3})^{25}$ رادر $(\mathbb{Z}_5,+,.)$ دریافت نماید
(d) (D,+,.) یک integ-dom و $char(D) = 11$ است. a,b∈D
$(a+b)^{121}$ رادریافت نماید

مثال: مامیدانیم که $(\mathbb{Z}_5,+,.)$ یک integ-dom و $char(\mathbb{Z}_5) = 5$ است. نظر به لیما 6.6 باید افاده ذیل صدق کند:

$$(\bar{2} + \bar{4})^5 = (\bar{2})^5 + (\bar{4})^5$$

$$(\bar{2} + \bar{4})^5 = (\bar{6})^5 = (\bar{1})^5 = \bar{1}$$
$$(\bar{2})^5 + (\bar{4})^5 = (\bar{2})^3 . (\bar{2})^2 + (\bar{4})^2 . (\bar{4})^2 . \bar{4}$$
$$= \bar{8} . \bar{4} + \overline{16} . \overline{16} . \bar{4} = \bar{3} . \bar{4} + \bar{1} . \bar{1} . \bar{4}$$
$$= \overline{12} + \bar{4} = \bar{2} + \bar{4} = \bar{6} = \bar{1}$$

دیده شد که افاده فوق صدق می نماید

مثال: حالا میخواهیم معادلات خطی ذیل را در $\mathbb{Z}_5$ حل نمایم

$$x + \bar{3}y = \bar{2}$$
$$\bar{3}x + \bar{2}y = \bar{2}$$

$$\bar{3}x + \bar{3}.\bar{3}y = \bar{3}.\bar{2} = \bar{6} = \bar{1}$$
$$\bar{3}x + \bar{2}y = \bar{2}$$

$$\bar{3}x + \bar{4}.y = \bar{1}$$

$\overline{3}x + \overline{2}y = \overline{2}$

$\overline{3}x + \overline{4}.y = \overline{1}$
$-\overline{3}x - \overline{2}y = -\overline{2}$

$\overline{2}y = -\overline{1} = \overline{4} \Rightarrow \overline{3}.\overline{2}y = \overline{3}.\overline{4} \Rightarrow y = \overline{2}$
$\overline{3}x + \overline{2}.\overline{2} = \overline{2}$
$\Rightarrow \overline{3}x = \overline{2} - \overline{4}$
$= -\overline{2} = \overline{3}$ [$\overline{2} + \overline{3} = \overline{0} \Rightarrow -\overline{2} = \overline{3}$ زيرا]
$\Rightarrow \overline{2}.\overline{3}x = \overline{2}.\overline{3} \Rightarrow x = \overline{1}$

مثال:

$\overline{3}x + \overline{2}.y = \overline{0}$
$\overline{2}x + \overline{1}y = \overline{4}$

اول معادله فوق را درررینگ $(\mathbb{Z}_7, +, .)$ حل می نمایم.برای اینکار معادله اول را ضرب $\overline{2}$ و معادله دوم را ضرب $\overline{3}$ می نمایم

$\overline{6}x + \overline{4}.y = \overline{0}$
$\overline{6}x + \overline{3}y = \overline{4}.\overline{3} = \overline{12} = \overline{5}$

$\overline{6}x + \overline{4}.y = \overline{0}$
$-\overline{6}x - \overline{3}y = \overline{4}.\overline{3} = \overline{12} = -\overline{5}$

$y = -\overline{5} = \overline{2}$ [$\overline{5} + \overline{2} = \overline{0} \Rightarrow \overline{2} = \overline{2} - \overline{5}$ زيرا]
$\overline{3}x + \overline{2}.y = \overline{0}$
$\Rightarrow \overline{3}x = -\overline{2}.y = -(\overline{2}.\overline{2}. = -\overline{4}. = \overline{3}$
$\overline{5}.\overline{3}.x = \overline{5}.\overline{3} \Rightarrow x = \overline{1}$

حلا میخواهیم معادله فوق را درررینگ $(\mathbb{Z}_5, +, .)$ حل می نمایم. درینجا نیز معادله اول را ضرب $\overline{2}$ و معادله دوم را ضرب $\overline{3}$ می نمایم

$\overline{6}x + \overline{4}.y = \overline{0} \Rightarrow \overline{1}x + \overline{4}.y = \overline{0}$
$\overline{6}x + \overline{3}y = \overline{4}.\overline{3} = \overline{12} \Rightarrow \overline{1}x + \overline{3}y = \overline{2}$

$\bar{1}x + \bar{4}.y = \bar{0}$
$-\bar{1}x - \bar{3}y = -\bar{2}$
$\Rightarrow y = -\bar{2} = \bar{3} \wedge x = -\bar{4}.y = -(\bar{4} . \bar{3}) = -\bar{2} = \bar{3}$

نوت:

(a) چون رینگ $(\mathbb{Z}_6, +, .)$ یک integ-Domain نیست ، پس:

$\bar{4}x = \bar{0} \Rightarrow x = \bar{0} \vee x = \bar{3}$

(b) چون رینگ $(\mathbb{Z}_5, +, .)$ یک integ-Domain است ، پس:

$\bar{4}x = \bar{0} \Rightarrow x = \bar{0}$

مثال: معادلات خطی ذیل را در $(\mathbb{Z}_7, +, .)$ ازطریقه ماتریکس حل می نمایم

$$x - \bar{2}y + \bar{2}z = \bar{3}$$
$$\bar{3}x - y + \bar{2}z = \bar{4}$$
$$\bar{2}x + y - z = \bar{1}$$

ماتریکس ضرایب ان شکل ذیل رادارد

$$A = \begin{pmatrix} \bar{1} & -\bar{2} & \bar{2} \\ \bar{3} & \bar{1} & \bar{2} \\ \bar{2} & \bar{1} & -\bar{1} \end{pmatrix}, \quad b = \begin{pmatrix} \bar{3} \\ \bar{4} \\ \bar{1} \end{pmatrix}$$

$$(A, b) = \begin{pmatrix} \bar{1} & -\bar{2} & \bar{2} & \bar{3} \\ \bar{3} & \bar{1} & \bar{2} & \bar{4} \\ \bar{2} & \bar{1} & -\bar{1} & \bar{1} \end{pmatrix}$$

درمرحله اول سطراول را ضرب منفی $\bar{3}$ نموده وبا سطردوم جمع می نمایم. بعداً سطراول را ضرب منفی $\bar{2}$ نموده وبا سطرسوم جمع می نمایم

$$\begin{pmatrix} \bar{1} & -\bar{2} & \bar{2} & \bar{3} \\ \bar{0} & \bar{0} & -\bar{4} & -\bar{5} \\ \bar{0} & \bar{5} & -\bar{5} & -\bar{5} \end{pmatrix}$$

$-\overline{4}z = \overline{3}z = -\overline{5} = \overline{2} \implies \overline{3}.(\overline{3})^{-1}.z = \overline{2}.(\overline{3})^{-1}$
$\implies z = \overline{2}.\overline{5}$ [زیرا $\overline{3}.\overline{5} = \overline{1} \Rightarrow (\overline{3})^{-1} = \overline{5}$]
$\implies z = \overline{10} = \overline{3}$
$\overline{5}y = \overline{5}z - \overline{5}$

معادله فوق رابه $(\overline{5})^{-1}$ ضرب می نمایم

$\overline{5}.(\overline{5})^{-1}y = \overline{5}.(\overline{5})^{-1}z - \overline{5}.(\overline{5})^{-1}$
$\implies y = z - \overline{1} = \overline{3} - \overline{1} = \overline{2}$
$x = \overline{3} + \overline{2}y - \overline{2}z = \overline{3} + \overline{4} - \overline{2}.\overline{3} = \overline{7} - \overline{6} = \overline{1}$

تمرین 6.10:

(a) معادلات ذیل را در $(\mathbb{Z}_7, +, .)$ حل نماید

$\overline{3}x + \overline{6}y = \overline{6}$
$\overline{4}x + \overline{5}y = \overline{4}$

(b) معادلات ذیل را در $(\mathbb{Z}_5, +, .)$ حل نماید

$\overline{3}x + \overline{1}y = \overline{2}$
$\overline{2}x - \overline{3}y = \overline{1}$

(c) معادلات خطی ذیل را در $(\mathbb{Z}_7, +, .)$ ازطریقه ماتریکس حل می نمایم

$$\overline{2}x + y + \overline{3}z = \overline{5}$$
$$x - y + z = \overline{4}$$
$$x + \overline{3}y + z = \overline{5}$$

تعریف 6.12 : (R,+,.) یک رینگ که دارای عنصر واحد (unity) „1“ است.

$R[x]: = \{ P(x) = \sum_{i \in \mathbb{N}_0} a_i x^i \mid a_i \in R \}$

R[x] نظربه „ +“ و „.“ یک رینگ تبدیلی (Commutative Ring) که عنصر واحد (unity) ان P(x) = 1 است

$(R[x],+,.)$ بنام Polynomial Ring (پولینوم رینگ) و $p(x) \in R[x]$ بنام Polynomial (پولینوم) نظربه رینگی R یاد میشود.

مثال $(\mathbb{Z}[x],+,.)$ یک Polynomial Ring نظربه اعداد تام ,

$(\mathbb{Q}[x],+,.)$ نظر به اعداد ناطق , $(\mathbb{R}[x],+,.)$ نظر به اعداد حقیقی و $(\mathbb{Z}_7[x],+,.)$ نظر به $\mathbb{Z}_7$ است. بطورمثال

$$f_1(x) = 5 + 2x + 3x^2 \in \mathbb{Z}[x]$$

$$f_2(y) = 2 + \frac{1}{2}y + y^3 \in \mathbb{Q}[y]$$

$$f_3(z) = 2 + \sqrt{2}\,\frac{1}{2}z^2 + \sqrt{3}z^5 \in \mathbb{R}[z]$$

$$f_4(t) = \bar{3} + \bar{2}\,t^2 + \bar{4}t^3 \in \mathbb{Z}_7[t]$$

تعریف 6.13 :(R,+,.) یک رینگ که دارای عنصر واحد (unity) "1" و (R[x],+,.) Polynomial Ring ان است.

$$P(x) = \sum_{i\in\mathbb{N}_0} a_i\, x^i \in R[x]$$

$$= a_0 + a_1x + a_2x^2 + a_3x^3 + - - - -$$

درینجا ضرایب p(x) عناصراز رینگ R اند. درجه (degree) از $P(x)$ طوری تعریف شده است:

اگر $P(x) \neq 0$ باشد درانصورت:

$$\deg(p(x)) = \max\{\, i \in \mathbb{N}_0 \mid a_i \neq 0 \,\}$$

اگر $P(x) = 0$ باشد درانصورت $\deg(p(x)) = -\infty$ تعریف شده است

پولینوم که درجه ان صفرباشد بنام Constant Polynomail (پولینومی ثابت) یاد میشود. بطور مثال $p(x) = c$ ($c \in R$)

اگرما دو پولینوم $Q(x), P(x) \in R[x]$ داشته باشیم که درجه P(x) مساوی به m و از Q(x) مساوی به n باشد. درانصورت :

$$\deg(P(x).Q(x)) \leq m + n \;\wedge\; \deg(P(x) + Q(x)) \leq \max(m,n)$$

مثال: دررینگی $(\mathbb{Z}_6[x],+,.)$ دو پولینومی ذیل را درنظرمیگیریم

$$P(x) = \bar{2}\,x^2 + \bar{1} \quad , \quad q(x) = \bar{3}\,x + \bar{1}$$

$$\deg(p(x)) = 2 \;,\; \deg(q(x)) = 1$$

$$P(x).q(x) = \bar{2}\,x^2 . \bar{3}\,x + \bar{1}.\bar{3}\,x + \bar{1}\,.\,\bar{2}\,x^2 + \bar{1}.\bar{1}$$
$$= \bar{6}.\,X^3 + \bar{2}\,x^2 + \bar{3}\,x + \bar{1}$$
$$= \bar{2}\,x^2 + \bar{3}\,x + \bar{1}$$

دیده میشود که $\deg(p(x).q(x)) < \deg(p(x)) + \deg(q(x))$ است

قضیه 6.8 :

$(D,+,.)$ integ-Domain $\Rightarrow$ $(D[x],+,.)$ integ-Domain

ثبوت : مامیدانیم که $D[x]$ یک رینگی تبدیلی دارای عنصرواحد میباشد. حالا ماثبوت مینمایم که $(D[x],+,.)$ یک انتگرال دومین است. یعنی باید افاده ذیل ثبوت شود:

$g(x), f(x) \in D[x]$, $f(x) \neq 0 \wedge g(x) \neq 0 \Rightarrow f(x) . g(x) \neq 0$

اگر پولینوم ما شکل ذیل راداشته باشد:

$f(x): = a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} + a_m x^m \quad (a_m \neq 0)$

$g(x): = b_0 + b_1x + b_2x^2 + - - - + b_{n-1}x^{n-1} + b_n x^n \quad (b_n \neq 0)$

چون :

$a_m \neq 0 \wedge b_n \neq 0 \Rightarrow f(x) , g(x) \neq 0$

$a_m \neq 0 \wedge b_n \neq 0$

$\Rightarrow a_m . b_n \neq 0$ [زیرا D یک integ-domain است]

$\Rightarrow a_m . b_n . x^{m+n} \neq 0 \Rightarrow f(x) . g(x) \neq 0$

$\Rightarrow$ D[x] is integ-Domain

یادداشت: ازقضیه فوق نتیجه میشود، که اگر D یک integral-Domain و $P(x) , Q(x) \in D[x]$ پولینموم های فوق باشند، درانصورت :

$\deg(P(x).Q(x)) = \deg(P(x)) + \deg(Q(x))$

زیرا:

$a_m \neq 0 \wedge b_n \neq 0$

$\Rightarrow a_m . b_n \neq 0 \Rightarrow a_m . b_n . x^{m+n} \neq 0$

$\Rightarrow \deg(P(x).Q(x)) = m + n = \deg(P(x)) + \deg(Q(x))$

مثال : حل پولینوم ذیل را در $\mathbb{Z}_7$ دریافت مینمایم .

$P(x) \in \mathbb{Z}_7\,[x]$

$P(x) = x^2 + x + \bar{2}$

$x^2 + x + \bar{2} = (x - \bar{3})^2$

زیرا:

$$(x - \bar{3})^2 = x^2 - \bar{2}.\bar{3}x + \bar{3}.\bar{3}$$
$$= x^2 - \bar{6}x + \bar{9}$$
$$= x^2 - \bar{6}x + \bar{2}$$
$$= x^2 + \bar{1}x + \bar{2}$$

پس حل ان

$$x^2 + x + \bar{2} = (x - \bar{3})^2 = \bar{0}$$
$$\Rightarrow x = \bar{3}$$

نوت : میخواهیم تشریح نمایم که چطور $\bar{1} = -\bar{6}$ میشود

$$\bar{6} + \bar{1} = \bar{0} \Rightarrow \bar{1} = \bar{0} - \bar{6} = -\bar{6}$$

امتحان :

$$x^2 + x + \bar{2} = \bar{3}.\bar{3} + \bar{3} + \bar{2} = \bar{9} + \bar{3} + \bar{2}$$
$$= \bar{2} + \bar{3} + \bar{2} = \bar{7} = \bar{0}$$

اگر $P(x) = x_2 + x + 2 \in \mathbb{R}[x]$ باشد درانصورت

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-1 \pm \sqrt{1^2 - 4.1.2}}{2.1} = \frac{-1 \pm \sqrt{-7}}{2}$$

دیده میشود که پولینومی $P(x)$ در اعداد حقیقی حل ندارد

مثال :

(a) حل پولینوم $P(x) = x^2 - \bar{1} \in \mathbb{Z}_8[x]$ رادر رینگ $(\mathbb{Z}_8, +, .)$ دریافت مینمایم .

$$x^2 - \bar{1} = \bar{0} \implies x^2 = \bar{1}$$

$$(\bar{1})^2 = \bar{1}, (\bar{3})^2 = \bar{9} = \bar{1}, (\bar{5})^2 = \overline{25} = \bar{1}, (\bar{7})^2 = \overline{49} = \bar{1}$$

دیده شد که $P(x)$ در رینگ $\mathbb{Z}_8$ چهارحل دارد

(b) حالاحل پولینوم $P(x) = x^2 - \bar{1} \in \mathbb{Z}_7[x]$ را در انتگرال دومین $(\mathbb{Z}_7, +, .)$ دریافت مینمایم .

$$x^2 - \bar{1} = \bar{0} \implies x^2 = \bar{1}$$
$$(\bar{1})^2 = \bar{1}, (\bar{6})^2 = \overline{36} = \bar{1}$$

دیده شد که $P(x)$ در رینگ $\mathbb{Z}_7$ دو حل دارد

نوت: بصورت عموم میتوان گفت که تعداد حل یک پولینوم درجه n کوچکتر ویا مساوی به n است

تمرین 6.11:

(a) حل پولینوم ذیل را در رینگی $\mathbb{Z}_7$ دریافت نماید .

$P(x) \in \mathbb{Z}_7 [x]$, $P(x) = x^2 + \bar{2}\, x + \bar{4}$

(b)

$Q(x),P(x) \in \mathbb{Z}_6 [x]$

$P(x) = \bar{2}x^2 + \bar{1}$, $Q(x) = \bar{3}x^2 + \bar{1}$

$P(x).Q(x)$ را دریافت نماید

قضیه 6.9 (**Polynomial Division Algorithm**) :

$(D[x],+,.)$ یک integ-Domain و $a(x), b(x) \in D[x] , b(x) \neq 0$ است. بعدآ :

$\exists \; q(x),r(x) \in D[x] \; ; a(x) = b(x).q(x) + r(x)$

درینجا $r(x) = 0$ ویا درغیران $deg(r(x)) < deg(b(x))$ است

ثبوت: ما پولینوم های ذیل رادرنظرمیگریم :

$a(x): = a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} + a_m x^m \quad (a_m \neq 0)$

$b(x): = b_0 + b_1x + b_2x^2 + - - - + b_{n-1}x^{n-1} + b_n x^n \quad (b_n \neq 0)$

ما ازطریقه complete induction نظربه درجه پولینوم این قضیه را ثبوت می نمایم. در complete induction سه حالت ذیل موجود است

اول : برای $deg(a(x)) = 0$ باید صدق کند

دوم : ما فرض میکنیم که برای تمامی پولینوم که درجه ان $m - 1$ باشد ، صدق میکند

سوم : باید ثبوت شود که برای $a(x)$ نیز صدق می کند

حالت اول :

$deg(a(x)) = 0 \implies a(x) = a_0$

درین حالت برای $b(x)$ دو امکانات ذیل موجود است:

(a) $deg(a(x)) = deg(b(x)$

$\implies b(x) = b_0 \implies a(x) = q.b(x) , q = \frac{a_0}{b_0}$

درینجا $b_0 \neq 0$ است. زیرا $b(x) \neq 0$ فرض شده

(b) $\deg(a(x)) < \deg(b(x))$

$\Longrightarrow a(x) = 0.b(x) + r(x)\ ,\ q(x) = 0,\ r(x) = a(x)$

پس حالت اول صدق میکند. حالا فرض میکنیم که برای تمامی پولینوم که درجه ان $m - 1$ باشد ، صدق میکند.

اکنون ثبوت می نمایم که برای $a(x)$ نیز صدق میکند. درفوق برای $\deg(a(x)) = 0$ ثبوت نمودیم . حالا حالت $\deg(a(x)) > 0$ را در نظرمیگریم . درفوق دیدیم که قضیه برای $\deg(a(x)) < \deg(b(x))$ صدق میکند. حالا برای $\deg(b(x)) < \deg(a(x))$ ثبوت مینمایم. ما تابع ذیل را درنظرمیگریم:

$$f(x) = a(x) - \frac{a_m}{b_n} x^{m-n} . b(x)$$

$$= a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} + a_m x^m - \frac{a_m}{b_n} (b_0 + b_1x + b_2x^2 + - - - + b_{n-1}x^{n-1} + b_n x^n). x^{m-n}$$

$$= a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} + a_m x^m - \frac{a_m}{b_n} (b_0 + b_1x + - - - + b_{n-1}x^{n-1}) - \frac{a_m}{b_n} b_n x^n). x^{m-n}$$

$$= a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} + a_m x^m - \frac{a_m}{b_n} (b_0 + b_1x + b_2x^2 + - - - + b_{n-1}x^{n-1}) – a_m x^m$$

$$= a_0 + a_1x + a_2x^2 + - - - + a_{m-1}x^{m-1} - \frac{a_m}{b_n} (b_0 + b_1x + b_2x^2 + - - - + b_{n-1}x^{n-1})$$

$\Longrightarrow \deg(f(x)) = m - 1$

$\Longrightarrow \exists\ p(x), r(x) \in \mathbf{D}[x]\ ;$

$f(x) = b(x).p(x) + r(x)$ [نظر به حالت فرض شده]

درینجا $r(x) = 0$ ویا درغیران $\deg(r(x)) < \deg(b(x))$ است

$$b(x).p(x) + r(x) = f(x) = a(x) - \frac{a_m}{b_n} x^{m-n} . b(x)$$

$\Longrightarrow a(x) = b(x).p(x) + r(x) + \frac{a_m}{b_n} x^{m-n} . b(x)$

$= b(x)\left(p(x) + \frac{a_m}{b_n} x^{m-n}\right) + r(x)$

ما $q(x) = p(x) + \frac{a_m}{b_n} x^{m-n}$ وضع می نمایم. درنتیجه

$a(x) = b(x).q(x) + r(x)$

مثال:

$a(x) = x^3 + 4x^2 + 5x + 7 \ , b(x) = x + 1 \in \mathbb{Z}[x]$

$x^3 + 4x^2 + 5x + 7 : x + 1 = x^2 + 3x + 2$

$-(x^3 + x^2)$

$3x^2 + 5x$

$- (3x^2 + 3x)$

$2x + 7$

$- (2x + 2)$

5

درینجا $q(x) = x^2 + 3x + 2$ و $r(x) = 5$ بدست امد. یعنی:

$a(x) = q(x).b(x) + r(x)$

قضیه 6.10 (the Remainder Theorem): $(D[x],+,.)$ یک integ-Domain و $f(x) \in D[x]$, $c \in D$. بعداً :

(1) $\exists\, q(x) \in D[x] \ ; f(x) = (x-c) . q(x) + f(c)$

(2) $(x - c) | f(x) \iff f(c) = 0$

ثبوت (1) : اگر $b(x)=(x-c)$ باشد، درانصورت نظر به قضیه Division Algorithm میتوان نوشت:

$\exists\ q(x), r(x) \in D[x]\ ;\ f(x) = (x-c)\ .\ q(x) + r(x)$

برای $r(x)$ دوحالت ذیل امکان دارد :

$r(x) = 0 \implies f(c) = (c - c)\ .\ q(x) + 0 = 0$

$r(x) \neq 0 \implies \deg(r(x)) < \deg(x - c) = 1 \implies \deg(r(x)) = 0$

$\implies r(x) = r_0$

$f(c) = (c - c)\ .\ q(x) + r_0 = r_0$

$f(x) = (x-c)\ .\ q(x) + r(x) = (x-c)\ .\ q(x) + r_0$

$= (x-c)\ .\ q(x) + f(c)$

ثبوت (2) :

" $\Longrightarrow$„ نظر به (1) میتوان نوشت :

$\exists\ q(x) \in D[x]\ ;\ f(x) = (x-c)\ .\ q(x) + f(c)$

چون $f(x)$ بالای $(x-c)$ قابل تقسیم است. پس $f(c) = 0$ است

" $\Longleftarrow$„

$f(x) = (x-c)\ .\ q(x) + f(c)$ [نظربه **(1)**]

$= (x-c)\ .\ q(x) + 0$

$\implies (x - c) \mid f(x)$

مثال:

$f(x) = 2x^5 + x^4 + 7x^3 + 2x + 10$

$f(-1) = 2(-1)^5 + (-1)^4 + 7(-1)^3 + 2.(-1) + 10$

$= -2 + 1 - 7 - 2 + 10 = 0$

$\implies x + 1 \mid f(x)$

تعریف 6.14 : $(D[x],+,.)$ یک integ-Domain

$f(x), g(x) \in D[x],\ g(x) \neq 0$,

(a) $f(x)$ بالای $g(x)$ قابل تقسیم است، درصورتکه یک $h(x) \in D[x]$ با خاصیت ذیل موجود باشد:

$f(x) = h(x).g(x)$

(b) $d(x) \in D[x]$ بنام common divisor (قاسم مشترک) از $f(x)$ و $g(x)$ یاد میشود درصورتکه $f(x)$ و $g(x)$ بالای $d(x)$ قابل تقسیم باشد. یعنی:

$$d(x) \mid f(x) \ \wedge \ d(x) \mid g(x)$$

(c) قاسم مشترک $d(x)$ بنام greatest common divisor (gcd)
(بزرگترین قاسم مشترک) یاد میشود،درصورتکه افاده ذیل صدق نماید:

$$h(x) \in D[x] \ , \ h(x) \mid f(x) \ \wedge \ h(x) \mid g(x) \Longrightarrow \ h(x) \mid d(x$$

مثال:

$p_1(x) = 2x^3 + 10x^2 + 2x + 10 \ , \ p_2(x) = x^3 - 2x^2 + x - 2 \in \mathbb{Q}[x]$

میخواهم $f(x), g(x) \in \mathbb{Q}[x]$ رادریافت نمایم ، که :

$$\gcd(p_1(x), p_1(x)) = f(x).\, p_1(x) + g(x).\, p_2(x)$$

$$2x^3 + 10x^2 + 2x + 10 = 2(x^3 - 2x^2 + x - 2) + (14x^2 + 14)$$

$$x^3 - 2x^2 + x - 2 = \left(\frac{1}{14}x - \frac{1}{7}\right).(14x^2 + 14)$$

$$\Longrightarrow \ \gcd(p_1(x), p_1(x)) = 14x^2 + 14$$

$$14x^2 + 14 = 1.(2x^3 + 10x^2 + 2x + 10) - 2(x^3 - 2x^2 + x - 2)$$

$$\Longrightarrow f(x) = 1 \ , g(x) = -2$$

$$\Longrightarrow \gcd(p_1(x), p_1(x)) = 14x^2 + 14 = \ f(x).\, p_1(x) + g(x).\, p_2(x)$$

مثال:

$p_1(x) = x^4 + x^3 + x + 1 \ , \ p_2(x) = x^2 + x + 1 \in \mathbb{Q}[x]$

میخواهم $f(x), g(x) \in \mathbb{Q}[x]$ رادریافت نمایم ، که :

$$\gcd(p_1(x), p_1(x)) = f(x).\, p_1(x) + g(x).\, p_2(x)$$

$$x^4 + x^3 + x + 1 = (x^2 - 1).(x^2 + x + 1) + (2x + 2)$$

$$x^2 + x + 1 = \frac{x}{2} \ . \ (2x + 2) + 1$$

$(2x + 2) = (2x + 2).1$

$\Longrightarrow \gcd(p_1(x), p_1(x)) = 1$

$1 = (x^2 + x + 1) - \frac{1}{2}x\,.\,(2x + 2)$

$= (x^2 + x + 1) - \frac{1}{2}x\,((x^4 + x^3 + x + 1) - (x^2 - 1).(x^2 + x + 1))$

$= (x^2 + x + 1) + (\frac{1}{2}x^3 - \frac{1}{2}x).(x^2 + x + 1) - \frac{1}{2}x(x^4 + x^3 + x + 1)$

$= (\frac{1}{2}x^3 - \frac{1}{2}x + 1).(x^2 + x + 1) - \frac{1}{2}x(x^4 + x^3 + x + 1)$

$\Longrightarrow g(x) = \frac{1}{2}x^3 - \frac{1}{2}x + 1$, $f(x) = \frac{1}{2}x$

$\gcd(p_1(x), p_1(x)) = 1 = f(x).\,p_1(x) + g(x).\,p_2(x)$

تمرین:

$p_1(x) = x^3 + 5x^2 + 7x + 2$, $p_2(x) = x^3 + 2x^2 + -2x - 1 \in \mathbb{Q}[x]$

$f(x), g(x) \in \mathbb{Q}[x]$ رادریافت نماید ، که :

$\gcd(p_1(x), p_1(x)) = f(x).\,p_1(x) + g(x).\,p_2(x)$

فصل هفتم

ساحه (Field)

تعریف 7.1 : یک حلقه تبدیلی (commutative Ring) (F,+,.) که خواص ذیل را داشته باشد بنام Field (ساحه) یاد میشود .

(i) (F,+,.) دارای عنصر واحد unity باشد .

(ii) هر عنصر $a \in F - \{0\}$ معکوس پذیر Invertible باشد .

یعنی :

$$\forall\ a \in F - \{0\}, \exists\ b \in F; a.b = 1$$

مثال : $(Q,+,.)$, $(\mathbb{R},+,.)$ و $(\mathbb{C},+,.)$ ساحه (field) اند . مگر $(\mathbb{Z},+,.)$ ساحه شده نمی تواند . زیرا بطور مثال برای $2 \in \mathbb{Z}$ نظر به ضرب "." معکوس آن در $\mathbb{Z}$ موجود نیست .

مثال : $(\mathbb{Z}_5,+,.)$ یک ساحه است . مگر $(\mathbb{Z}_6,+,.)$ ساحه (Field) نیست. زیرا برای $\bar{2} \in \mathbb{Z}_6$ در $\mathbb{Z}_6$ نظر به ضرب معکوس وجود ندارد .

تمرین 7.1 :

$$M:= \{ A \in M(2x2,\mathbb{R}) \mid A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, a^2 + b^2 \neq 0 \}$$

ثبوت نماید که چرا (M,+,.) نظربه جمع "+„ و ضرب ".„ متریکس یک ساحه (Field) شده نمی تواند.

تعریف 7.2: $(F, +, .)$ یک ساحه (Field) است که "0" عنصر عینیت آن نظر به "+" و "1" عنصر عینیت آن نظر به "." میباشد . $\emptyset \neq H \subseteq F$.

H بنام subfield (ساحه فرعی) یادمیشود در صورتیکه (H ,+,.) یک ساحه باشد ویا میتوان بگویم که H یک Subfield از F است در صورتیکه :

(1)

(i) $\forall\ a, b \in H \implies a + b \in H$

(ii) $\forall a \in H \Rightarrow -a \in H$

(2)

(i) $\forall\, a,b \in H \implies a.b \in H$

(ii) $1 \in H$

(iii) $\forall a \in H \quad a \neq 0 \quad \Rightarrow a^{-1} \in H$

بطور مثال $(\mathbb{Z}, +, .)$ رینگ فرعی $(\mathbb{R}, +, .)$ است. مگرساحه فرعی شده نمی تواند . زیرا (iii) صدق نمی کند

مثال 7.1:

(a) سیت $H := \{a + b\sqrt{2} \mid a,b \in Q\}$ یک subfield از $(\mathbb{R}, +, .)$ است

حل :

$x, y \in H \Rightarrow \exists\, a,b,c,d \in Q : x = a + b\sqrt{2}\,, y = c + d\sqrt{2}$

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

$\Rightarrow x + y \in H \quad [\ a + b\,, c + d \in Q \qquad$ زیـرا $\ ]$

$\Rightarrow$ **(1)(i)**

$x = a + b\sqrt{2} \ \Rightarrow -x = -a + (-b)\sqrt{2} \Rightarrow -x \in H \Rightarrow (\mathbf{1})(\boldsymbol{ii})$

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

$ac + 2bd\,, ad + bc \in Q \ \Rightarrow x.y \in H \ \Rightarrow (\mathbf{2})(\boldsymbol{i})$

$1 = (1 + 0.\sqrt{2}) \in H \Rightarrow (\mathbf{2})(\boldsymbol{ii})$

$0 \neq x \in H \ \Rightarrow \exists a,b \in Q\,; x = a + b\sqrt{2} \neq 0$

$\Rightarrow a - b\sqrt{2} \neq 0$

زیرا درغیر آن اگر $a - b\sqrt{2} = 0$ شود . در آنصورت باید $a = b = 0$ شود مگر این در تضاد به $a + b\sqrt{2} \neq 0$ واقع میشود .

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

$$= \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2}$$

$\frac{a}{a^2-2b^2}, \frac{(-b)}{a^2-2b^2} \in Q \ \Rightarrow \ (a + b\sqrt{2})^{-1} \in H \Rightarrow$ **(2)(iii)**

درنتیجه H یک subfield (ساحه فرعی) از $(\mathbb{R}, +, .)$ است

(b) سیت $H := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ یک integral domain است مگر subfield (ساحه فرعی) از $(\mathbb{R}, +, .)$ نیست .

حل :

به اسانی میتوان ثبوت نمود که H یک رینگ فرعی تبدیلی در $\mathbb{R}$ بوده ودارای عنصرواحد نیزمیباشد. زیرا:

$$1 = (1 + 0.\sqrt{2}) \in H$$

پس انتگرال دومین نیز است. مگرخاصیت (iii)(2) صدق نمیکند. زیرا:

$$0 \neq x \in H \Rightarrow \exists a, b \in \mathbb{Z}\,; x = a + b\sqrt{2} \neq 0$$
$$\Rightarrow a - b\sqrt{2} \neq 0$$

زیرا در غیر آن اگر $a - b\sqrt{2} = 0$ شود . در آنصورت باید $a = b = 0$ شود. مگر این در تضاد به $a + b\sqrt{2} \neq 0$ واقع میشود .

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$
$$= \frac{a}{a^2 - 2b^2} + \frac{(-b)}{a^2 - 2b^2}\sqrt{2}$$

$$\frac{a}{a^2-2b^2}, \frac{(-b)}{a^2-2b^2} \notin \mathbb{Z} \Rightarrow (a + b\sqrt{2})^{-1} \notin H$$

زیرابطورمثال اگر a = 3 و b = 1 باشد، درانصورت:

$$(3 + 1b\sqrt{2}) \in H \wedge (3 + 1b\sqrt{2}) \neq 0$$

$$\frac{a}{a^2 - 2b^2} = \frac{3}{3^2 - 2} = \frac{3}{9 - 2} = \frac{3}{7} \notin \mathbb{Z}$$

$$\frac{(-b)}{a^2-2b^2} = \frac{-1}{9-2} = \frac{-1}{7} \notin \mathbb{Z}$$

دیده شد که برای $(3 + 1b\sqrt{2})$ در H معکوس موجود نیست. پس ساحه فرعی شده نمی تواند

مثال 7.2: بالای سیت F:={0,1,a,b} دورابطه دوگانه درجدول ذیل تعریف شده است

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

F(+,.) یک ساحه (Field) بوده که دارای عنصرعینت "0„ و عنصرواحد "1„ می باشد. مشخصه ان مساوی به 2 است. زیرا:

$2.1 = 1 + 1 = 0 \implies char(F) = 2$

سیت فرعی S:={0,1} یک ساحه فرعی (subfield) در F است.

ما پولینوم $p(x) = x^2 + x + 1$ رادرنظرمیگریم

اگر $p(x) \in F[x]$ باشد، درانصورت میتوان پولینوم رادردوفکتور ذیل تجزیه نمود :

$$p(x) = x^2 + x + 1 = x^2 + (a + b)x + ab = (x + a).(x + b)$$

زیرا نظربه جدول $a + b = 1$ و $a.b = 1$ است. پولینوم حل ذیل رادارد:

$$p(x) = x^2 + x + 1 = (x + a).(x + b) = 0$$

$\implies x_1 = - a = a \ \wedge \ x_2 = -b = b$ [نظر به جدول]

امتحان:

$$p(a) = a^2 + a + 1 = b + a + 1 = 1 + 1 = 2 = 0$$
$$p(b) = b^2 + b + 1 = a + b + 1 = 1 + 1 = 2 = 0$$

مگر p(x) در S[x] حل ندارد

سیت فرعی G:={1,a,b} از F نظر به "." یک گروپ دورانی است. زیرانظر به جدول فوق:

$a^2 = b\ ,\ a^3 = b.a = 1 \Longrightarrow <a> = G \wedge ordG = 3$
$b^2 = a\ ,\ b^3 = a.b = 1 \Longrightarrow <b> = G \wedge ordG = 3$

لیما 7.1 : هر integeral Domain که متناهی باشد یک ساحه (field) است .
ثبوت : اگر $(D\ ,\ +\ ,.)$ یک integ-Dom متناهی دارای عنصر واحد "1" باشد باید ثبوت شود :

$\forall r \in D\ , r \neq 0 \Rightarrow \exists s \in D; r.s = 1$

یعنی هر عنصر از D که خلاف صفر باشد باید نظر به "." معکوس پذیر باشد.
برای ثبوت تابع ذیل را تعریف می نمائیم :

$r \in D\ ,\ r \neq 0$

$\varphi_r : D \longrightarrow D$

$x \longmapsto rx$

: φ_r injective

$x, y \in D\ , \varphi_r(x) = \varphi_r(y) \Rightarrow r.x = r.y$

$\Rightarrow x = y$ [زیرا $integ - Dom$ اختصار پذیر است]

چون D یک سیت متناهی است پس نظر به قضیه 0.1 تابع φ_r نیز surjective است. پس :

$1 \in D \Rightarrow \exists\ s \in D; \varphi_r(s) = r.s = 1$

$\Rightarrow s = r^{-1} \Rightarrow r\ invertible$ (معکوس پذیر)

$\Rightarrow D\ is\ a\ field$ (ساحه)

لیما 7.2 : (F,+,.) یک Field است. اگر I یک ادیال در F باشد ، درانصورت I={0} ویا I=F است .
ثبوت : ما فرض میکنیم که $I \neq \{0\}$ است .

$I \neq 0 \Rightarrow a \in I\ ; a \neq 0$

$\Rightarrow \exists b \in F\ ;\ a.b = 1$ [زیرا F یک ساحه است]

$\Rightarrow$ a invertible

$\Rightarrow I = F$ [نظر به لیما 6.6]

قضیه 7.1: در حلقه $(\mathbb{Z}_p, +, .)$ افاده ذیل صدق میکند :

$\mathbb{Z}_p$ ساحه است $\Leftrightarrow$ p عدد اولیه است

ثبوت "⇒" ما میدانیم که $(\mathbb{Z}_p, +, .)$ یک رینگی تبدیلی است که دارای عنصر واحد "$\bar{1}$ " است . پس کفایت میکند که ثبوت شود که هر عنصر خلاف صفر آن معکوس پذیر (invertible) است .

$\mathbb{Z}_p = \{\overline{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}$

$\bar{a} \in \mathbb{Z}_p^* \Rightarrow a \in \{1,2,\dots,p-1\} \Rightarrow gcd(a,p) = 1$

$\Rightarrow \exists\, x, y \in \mathbb{Z}_{:}\ a.x + p.y = 1$ [نظر به $Eucl.\ algorithm$]

$\Rightarrow \bar{1} = \overline{a.x + p.y} = \overline{ax} + \overline{py} = \bar{a}\,\bar{x} + \bar{p}\,\bar{y}$

$= \bar{a}\,\bar{x} + \bar{0}\,\bar{y} = \bar{a}\,.\bar{x}$

دیده شد که $\bar{x}$ معکوس (inverse) از $\bar{a}$ است . در نتیجه $\mathbb{Z}_p$ یک ساحه است ویا اینکه چون p یک عدد اولیه است. پس $(\mathbb{Z}_p^*, .)$ نظربه قضیه 3.21 یک گروپ است و هر عنصر خلاف صفر آن معکوس پذیر (invertible) است.

"⇐" اگر p عدد اولیه نباشد پس باید :

$\exists\, m, n \in \mathbb{N}; 1 < m,\ n < p,\ p = m.n$

$\Rightarrow (\bar{m}.\bar{n} = \overline{m.n} = \bar{p} = \bar{0}) \wedge (\bar{m} \neq \bar{0} \wedge \bar{n} \neq \bar{0})$

$\Rightarrow \mathbb{Z}_p\ is\ not\ integral\ Doman$ (انتیگرال دومین نیست)

$\Rightarrow \mathbb{Z}_p\ is\ not\ field$ (ساحه نیست)

مگر این در تضاد به فرضیه است . پس باید p یک عدد اولیه باشد .

قضیه 7.2 : هرساحه (Field) یک Integral Domain است

ثبوت : اگر (F,+,.) یک ساحه باشد. پس F یک رینگی تبدیلی دارای عنصر واحد „ 1 „ است

فقط باید ثبوت شود که افاده ذیل صدق میکند

$a,b \in F,\ a \neq 0 \ \wedge\ a.b = 0 \ \Rightarrow\ b = 0$

$a,b \in F, a \neq 0 \ \wedge \ a.b = 0 \ \Rightarrow \ \exists\, a^{-1} \in F \ ; \ a^{-1}.a = 1$

$b = 1.b = (a^{-1}.a).b = a^{-1}.(a.b) = a^{-1}.0 = 0$

بهین ترتیب میتوان ثبوت نمود که اگر $b \neq 0$ درانصورت $a = 0$ میشود.
درنتیجه F یک Integral Domain است.

لیما 7.3: (R,+,.) یک رینگ با عنصرعینت 0_R ، (F,+,.) یک ساحه (field) با عنصرواحد "1" و $\varphi: F \longrightarrow R$ یک R-Hom است. بعدآ:

φ بایجکتیف $\Longleftarrow$ R یک ساحه (field) است

ثبوت : برای ساحه بودن R باید ثبوت شود:
(a) R نظر به عملیه ".„ خاصیت تبدیلی دارد
(b) هرعنصر(element) خلاف صفردر R دارای معکوس میباشد.
اول باید ثبوت شود که $\varphi(1)$ عنصرواحد ازR است

$s \in R \Longrightarrow \exists\, a \in F \ ; s = \varphi(a)$ [زیرا φ یک surjective]

$\Longrightarrow s = \varphi(a) = \varphi(1.a) = \varphi(1).\varphi(a) = \varphi(1).s$

زیرادرغیران: $\varphi(1) \neq 0_R$:

$\varphi(1) = 0_R = \varphi(0_F) \Longrightarrow 1 = 0_F$ [زیرا φ یک injective]
این امکان ندارد. زیرا دریک ساحه عنصر عینیت و واحد مساوی شده نمی تواند.
درنتیجه $\varphi(1)$ عنصرواحد ازR است

ثبوت (a) :

$x,y \in R$

$\Longrightarrow \exists\, a,b \in F \ ; x = \varphi(a) \wedge y = \varphi(b)$ [زیرا φ یک surjective]

$\Longrightarrow x.y = \varphi(a).\varphi(b) = \varphi(a.b) = \varphi(b.a)$ [زیرا F خاصیت تبدیلی دارد]

$= \varphi(b).\varphi(a) = y.x$

درنتیجه R خاصیت تبدیلی دارد

ثبوت (b) : درفوق دیدیم که $\varphi(1)$ عنصرواحد از R وخلاف صفراست

$x \in R \ , x \neq 0 \Longrightarrow \exists\, a \in F \ , x = \varphi(a)$ [زیرا φ یک surjective]

$\varphi(0) = 0 \neq x = \varphi(a)$ [زیرا φ یک R-Hom]

$\Longrightarrow a \neq 0$ [زیرا φ یک injective]

$\Longrightarrow \exists\, a^{-1} \in F\ ;\ a.a^{-1} = 1$ [زیرا F یک field]

$x.\ \varphi(a^{-1}) = \varphi(a^{-1}).x$ [زیرا R خاصیت تبدیلی دارد]

$= \varphi(a^{-1}).\varphi(a) = \varphi(a^{-1}.a) = \varphi(1)$

در فوق دیدیم که $\varphi(1)$ عنصرواحد ازR است. پس $\varphi(a^{-1})$ معکوس از x است درنتیجه ثبوت شد که R یک ساحه است

فصل هشتم

توسعه فیلد (Extensions Field)

تعریف 8.1: Field extensions (توسعه فیلد)
K یک ساحه و $F \subseteq K$ یک subfield (ساحه فرعی) از K است. K بنام **extension Field (فیلد توسعه) از** F یاد میشود. ما انرا به K/F نشان میدهیم و K/F را **Field extension** میگویند

مثال 8.1: ما سیت اعداد ناطق را به $\mathbb{Q}$ ، اعداد حقیقی رابه $\mathbb{R}$ و اعداد موهومی (یا مختلط) را به $\mathbb{C}$ نشان دادیم. همچنان میدانیم که $(\mathbb{Q}, +, .)$ ، $(\mathbb{R}, +, .)$ و $(\mathbb{C}, +, .)$ ساحه ها اند.

(a) همچنان $\mathbb{C}$ یک Field extension از $\mathbb{R}$ و $\mathbb{R}$ یک توسعه فیلد از $\mathbb{Q}$ است . یعنی:

$$\mathbb{C}/\mathbb{R} \ \wedge \ \mathbb{R}/\mathbb{Q}$$

(b) سیت های $\mathbb{Q}(\sqrt{2})$ و $\mathbb{Q}(\sqrt[3]{2})$ به شکل ذیل تعریف شده اند:

$$\mathbb{Q}(\sqrt{2}) := \{ a+b\sqrt{2} \mid a,b \in \mathbb{Q} \},$$

$$\mathbb{Q}(\sqrt[3]{2}) := \{ a+b\sqrt[3]{2} + c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q} \}$$

به اسانی میتوان ثبوت نمود که ($\mathbb{Q}(\sqrt{2})$ و $\mathbb{Q}(\sqrt[3]{2})$ نظر به جمع وضرب ساحه (field) اند. چون $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ و $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ است ، پس $\mathbb{Q}(\sqrt{2})$ و $\mathbb{Q}(\sqrt[3]{2})$ توسعه فیلد ها **(Field extension)** از $\mathbb{Q}$ اند. یعنی:

$$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q} \ , \ \mathbb{Q}(\sqrt{2})/\mathbb{Q}$$

(c) سیت $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ به شکل ذیل تعریف شده است:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) := \{ x+y\sqrt{3} \mid x,y \in \mathbb{Q}(\sqrt{2}) \}$$

چون x و y شامل $\mathbb{Q}(\sqrt{2})$ اند ، پس نظر به تعریف $\mathbb{Q}(\sqrt{2})$ میتوان نوشت:

$x \in \mathbb{Q}(\sqrt{2}) \Longrightarrow \exists\, a, b \in \mathbb{Q}\,; x = a + b\sqrt{2}$
$y \in \mathbb{Q}(\sqrt{2}) \Longrightarrow \exists\, c, d \in \mathbb{Q}\,; y = c + d\sqrt{2}$

درنتیجه:

$$\begin{aligned}\mathbb{Q}(\sqrt{2},\sqrt{3}) &= \{\, x+y\sqrt{3} \mid x,y \in \mathbb{Q}(\sqrt{2})\,\} \\ &= \{\, a+b\sqrt{2}+(c+d\sqrt{2}).\sqrt{3} \mid a,b,c,d \in \mathbb{Q}\,\} \\ &= \{\, a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\,\}\end{aligned}$$

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ نظر به جمع وضرب نیز یک ساحه (field) است.

چون $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ ، پس $\mathbb{Q}(\sqrt{2},\sqrt{3})$ توسعه فیلد (Field extension) از $\mathbb{Q}$ است.یعنی: $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$

(d) $s \in \mathbb{Q}$

$$\mathbb{Q}(\sqrt{s},-\sqrt{s}) = \mathbb{Q}(\sqrt{s})$$

حل:

$$\begin{aligned}\mathbb{Q}(\sqrt{s},-\sqrt{s}) &= \{\, a+b\sqrt{s}-c\sqrt{s}+d\sqrt{s.s} \mid a,b,c,d \in \mathbb{Q}\,\} \\ &= \{\, a+b\sqrt{s}-c\sqrt{s}+d.s \mid a,b,c,d \in \mathbb{Q}\,\} \\ &= \{\, (a+d.s)+(b-c)\sqrt{s} \mid a,b,c,d \in \mathbb{Q}\,\} \\ &= \mathbb{Q}(\sqrt{s})\end{aligned}$$

(e) سیت $\mathbb{Q}(\sqrt{3},i)$ به شکل ذیل تعریف شده است:

$$\mathbb{Q}(\sqrt{3},i) := \{\, x+yi \mid x,y \in \mathbb{Q}(\sqrt{3})\,\}$$

چون x و y شامل $\mathbb{Q}(\sqrt{3})$ اند ، پس نظر به تعریف $\mathbb{Q}(\sqrt{3})$ میتوان نوشت:

$x \in \mathbb{Q}(\sqrt{3}) \Longrightarrow \exists\, a, b \in \mathbb{Q}\,; x = a + b\sqrt{3}$
$y \in \mathbb{Q}(\sqrt{3}) \Longrightarrow \exists\, c, d \in \mathbb{Q}\,; y = c + d\sqrt{3}$

درنتیجه:

$$\begin{aligned}\mathbb{Q}(\sqrt{3},i) &= \{\, x+yi \mid x,y \in \mathbb{Q}(\sqrt{3})\,\} \\ &= \{\, a+b\sqrt{3}+(c+d\sqrt{3}).i \mid a,b,c,d \in \mathbb{Q}\,\} \\ &= \{\, a+b\sqrt{3}+ci+d\sqrt{3}\,i \mid a,b,c,d \in \mathbb{Q}\,\}\end{aligned}$$

$\mathbb{Q}(\sqrt{3},i)$ نظر به جمع وضرب نیز یک ساحه (field) است. معکوس i نظربه تعریف ان –i است. زیرا: $i.(-i) = -i^2 = -(-1) = 1$

چون $\mathbb{Q}(\sqrt{3}, i) \supseteq \mathbb{Q}$ ، پس $\mathbb{Q}(\sqrt{3}, i)$ توسعه فیلد (Field extension) از $\mathbb{Q}$ است. یعنی: $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$

(f) سیت $\mathbb{Q}(i)$ به شکل ذیل تعریف شده است:

$\mathbb{Q}(i) := \{ x+yi \mid x,y \in \mathbb{Q} \}$

چون $\mathbb{Q}(i) \supseteq \mathbb{Q}$ ، پس $\mathbb{Q}(i)$ توسعه فیلد (Field extension) از $\mathbb{Q}$ است. یعنی: $\mathbb{Q}(i)/\mathbb{Q}$

تبصره 8.1: ما **Field extension** (توسعه فیلد) K/F راداریم. درانصورت K یک فضای وکتوری نظربه F نیزاست. زیرا روابط دوگانه ذیل صدق میکنند:

$$+: K \times K \longrightarrow K$$
$$(u, v) \longmapsto u + v$$
$$\cdot : F \times K \longrightarrow K$$
$$(\tau, v) \longmapsto \tau v$$

و K نظر به این دو رابطه دارای خواص ذیل است:

(v_1) $(K, +)$ یک گروپ تبادلوی (Commutative) است. عنصرعینیت آن صفر است که ما آن را به " 0" نشان می دهیم و $-v$ معکوس (inverse) از v است

(v_2) : برای $\tau, \tau_1, \tau_2 \in F$ و $v, v_1, v_2 \in K$ افاده های ذیل صدق می کنند:

I. $(\tau_1 + \tau_2)v = \tau_1 v + \tau_2 v$
II. $\tau(v_1 + v_2) = \tau v_1 + \tau v_2$
III. $\tau_1(\tau_2 v) = (\tau_1 \tau_2)v$
IV. $1.v = v$

درنتیجه K یک فضای وکتوری نظربه F است و ما انرا به (K,F) نشان میدهیم

تعریف 8.2 : degree of Field extension (درجه توسعه فیلد) از K/F عبارت از بعد (Dimension) فضای وکتوری (K,F) است و انرا به [K:F] نشان میدهند. یعنی:

$$\dim(K,F) = [K:F]$$

اگر [K:F] متناهی باشد ، درانصورت K بنام finite field extension نظربه F یاد میشود

مثال 8.2:

(a) ما توسعه فیلد $\mathbb{C}/\mathbb{R}$ را درنظرمیگریم. فضای وکتوری ($\mathbb{C}, \mathbb{R}$) دارای قاعده {1,i} میباشد.زیرا:

$$\mathbb{C} = \mathbb{R} + \mathbb{R}i$$

یعنی هروکتور از $\mathbb{C}$ را میتوان بشکل ترکیب خطی 1 و i نوشت .علاوه بران مستقل خطی نیز اند.

درنتیجه {1,i} یک قاعده از فضای وکتوری ($\mathbb{C}, \mathbb{R}$) است. پس درجه $\mathbb{C}/\mathbb{R}$ مساوی به 2 است. یعنی: $[\mathbb{C}: \mathbb{R}] = 2$

(b) درجه (degree) از $\mathbb{Q}$ /$(\mathbb{Q}(\sqrt{2})$ مساوی به 2 است.

حل: درمثال فوق دیدیم که $\mathbb{Q}(\sqrt{2})$ توسعه فیلد (**Field extension**) از $\mathbb{Q}$ است. پس $(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$ یک فضای وکتور نیز است.

چون $\mathbb{Q}\sqrt{2}$ + $\mathbb{Q}$ = $\mathbb{Q}(\sqrt{2})$ تعریف شده، پس میتوان هروکتور از $\mathbb{Q}(\sqrt{2})$ را بشکل ترکیب خطی 1 و $\sqrt{2}$ نوشت. علاوه بران 1 و $\sqrt{2}$ مستقل خطی نیز اند.

پس $\{1, \sqrt{2}\}$ یک قاعده از فضای وکتوری $(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$ است

درنتیجه:

$$\dim((\mathbb{Q}(\sqrt{2}),\mathbb{Q})) = 2 \implies [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$$

(c) درجه (degree) از $\mathbb{Q}$ /$(\sqrt{2},\sqrt{3})$ $\mathbb{Q}$ مساوی به 4 است.

حل: سیت $(\sqrt{2},\sqrt{3})$ $\mathbb{Q}$ به شکل ذیل تعریف شده بود:

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{ a+b\sqrt{2}+c\sqrt{3} + d\sqrt{6} \mid a,b,c,d \in \mathbb{Q} \}$$

درمثال فوق دیدیم که $(\sqrt{2},\sqrt{3})$) $\mathbb{Q}$ توسعه فیلد (Field extension) از $\mathbb{Q}$ است. پس $(\mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q})$ یک فضای وکتور نیز است.

هروکتوری $(\sqrt{2},\sqrt{3})$ $\mathbb{Q}$ رامیتوان بشکل ترکیب خطی $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ نوشت. علاوه بران مستقل خطی نیز اند. پس $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ یک قاعده از فضای وکتوری $(\mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q})$ است. درنتیجه:

$$\dim(\mathbb{Q}(\sqrt{2},\sqrt{3}),\mathbb{Q})) = 4 \implies [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$$

(d) درجه (degree) از $\mathbb{Q}(\sqrt{3},i)/\mathbb{Q}$ مساوی به 4 است.
حل: سیت $\mathbb{Q}(\sqrt{3},i)$ به شکل ذیل تعریف شده بود:

$$\mathbb{Q}(\sqrt{3},i) := = \{ a+b\sqrt{3}+ci+d\sqrt{3}\,i \mid a,b,c,d \in \mathbb{Q} \}$$

درمثال فوق دیدیم که $\mathbb{Q}(\sqrt{3},i)$ توسعه فیلد (Field extension) از $\mathbb{Q}$ است.
پس $(\mathbb{Q}(\sqrt{3},i)),\mathbb{Q})$ یک فضای وکتور نیز است.
هروکتوری $\mathbb{Q}(\sqrt{3},i)$ رامیتوان بشکل ترکیب خطی $\{1,\sqrt{3},i,\sqrt{3}i\}$ نوشت.
علاوه بران مستقل خطی نیز اند. پس $\{1,\sqrt{3},i,\sqrt{3}i\}$ یک قاعده از فضای وکتوری $(\mathbb{Q}(\sqrt{3},i),\mathbb{Q})$ است. درنتیجه:

$$\dim(\mathbb{Q}(\sqrt{3},i),\mathbb{Q}) = 4 \implies [\mathbb{Q}(\sqrt{3},i):\mathbb{Q}] = 4$$

(e) درجه (degree) از $\mathbb{Q}//\mathbb{Q}(\sqrt[3]{2})$ مساوی به 3 است.
حل: سیت $\mathbb{Q}(\sqrt[3]{2})$ به شکل ذیل تعریف شده بود:

$$\mathbb{Q}(\sqrt[3]{2}) := \{ a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q} \}$$

درمثال فوق دیدیم که $\mathbb{Q}(\sqrt[3]{2})$ توسعه فیلد (Field extension) از $\mathbb{Q}$ است.
پس $(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q})$ یک فضای وکتور نیز است. هروکتوری $\mathbb{Q}(\sqrt[3]{2})$ رامیتوان بشکل ترکیب خطی $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ نوشت. علاوه بران مستقل خطی نیز اند. پس $\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ یک قاعده از فضای وکتوری $(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q})$ است.
درنتیجه:

$$\dim(\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q}) = 3 \implies [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$$

(f) ما توسعه فیلد $\mathbb{Q}(i)/\mathbb{Q}$ را درنظرمیگریم. فضای وکتوری $(\mathbb{Q}(i),\mathbb{Q})$ دارای قاعده {1,i} میباشد.زیرا هروکتور از $\mathbb{Q}(i)$ را میتوان بشکل ترکیب خطی 1 و i نوشت .علاوه بران مستقل خطی نیز اند.
درنتیجه {1,i} یک قاعده از فضای وکتوری $(\mathbb{Q}(i),\mathbb{Q})$ است. پس درجه $\mathbb{Q}(i)/\mathbb{Q}$ مساوی به 2 است. یعنی: $[\mathbb{Q}(i):\mathbb{Q}] = 2$

مثال8.3 :

$$\mathbb{Q}(\sqrt{6}) := \{ a+b\sqrt{6} \mid a,b \in \mathbb{Q} \} \implies [\mathbb{Q}(\sqrt{6}):\mathbb{Q}] = 2$$

$[\mathbb{Q}(\sqrt[n]{q}):\mathbb{Q}] = n$ (درصورتکه q یک عدد اولیه باشد)

تمرین 8.1:

(1) ثبوت نماید که $(\mathbb{Q}(\sqrt{5}), +, .)$ یک ساحه (field) است.

(2) ثبوت نماید که $\mathbb{Q}$ سیت فرعی (subset) از $\mathbb{Q}(\sqrt{5})$ است. یعنی:

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{5})$

(3) قاعده (basis) فضای وکتوری $(\mathbb{Q}(\sqrt{5}), \mathbb{Q})$ رادریافت نماید.

(4) درجه (degree) از $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ چند است

تمرین 8.2:

(1) ثبوت نماید که $(\mathbb{Q}(\sqrt{3}, \sqrt{5}), +, .)$ یک ساحه (field) است.

(2) ثبوت نماید که $\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}$ یک فیلد توسعه (Field extension) است

(3) قاعده (basis) فضای وکتوری $(\mathbb{Q}(\sqrt{3}, \sqrt{5}), \mathbb{Q})$ رادریافت نماید.

(4) درجه (degree) از $(\mathbb{Q}(\sqrt{3}, \sqrt{5}))/\mathbb{Q}$ چند است

تعریف8.3 : K/F یک Field extension (توسعه فیلد) است. یک $\alpha \in K$ بنام الجبری نظر به F (algebraic over F) یاد میشود درصورتکه یک پولینوم $p(x) \in F[x]$ خلاف صفر موجود باشد ، که $p(\alpha) = 0$ شود. درغیران α بنام transcendental (تخیلی) یاد میشود. یعنی $p(\alpha) = 0$ فقط درصورتی صدق میکند، که p پولینوم صفری باشد. ما سیت عناصرالجبری K را به $\mathbb{A}$ نشان میدهیم. بطورمثال:

$$\mathbb{A} := \{\alpha \in K \mid \exists\, p(x) \in F[x]; p \neq 0 \wedge p(\alpha) = 0\}$$

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} \mid \exists\, p(x) \in \mathbb{Q}[x]; p \neq 0 \wedge p(\alpha) = 0\}$$

$$= \{\alpha \in \mathbb{C} \mid \mathbb{Q} \text{ خاصیت الجبری نظر به } \alpha\}$$

البته سیت $F[X]$ در تعریف 6.12 تشریح شده و یک رینگ نیز است

تبصره : هرعنصریک ساحه F الجبری نظر به خود F است. زیرا:

$$\forall \alpha \in F, \exists\, p(x) = x - \alpha \in F[x]\,; p(\alpha) = 0$$

مثال 8.4 : ما توسعه فیلد $\mathbb{C}/\mathbb{R}$ رادرنظرمیگریم.

$\alpha := 2+3i \in \mathbb{C}$

$$(x - \alpha).(x - \bar{\alpha}) = (x - (2+3i)).(x - (2 - 3i))$$

$$= (x - 2 - 3i).(x - 2 + 3i)$$

$$= x^2 - 2.2x + (2^2 + 3^2)$$

$$= x^2 - 4x + 13 \in \mathbb{R}[x]$$

$p(x): = x^2 - 4x + 13$

$p(\alpha) = \alpha^2 - 4\alpha + 13 = (2+3i).(2+3i) - 4(2+3i) + 13$

$= 4+6i+6i - 9 - 8 - 12i + 13 = 0$

پس یک پولینوم $p(x)$ در $\mathbb{R}[x]$ دریافت شد که $p(\alpha) = 0$ است و درنتیجه $\alpha = 2+3i$ یک عنصر الجبری (algebraic) نظر به $\mathbb{R}$ است.

مثال 8.5 : ما توسعه فیلد $\mathbb{R}/\mathbb{Q}$ رادرنظرمیگریم

(a) عدد حقیقی $\sqrt[3]{2}$ نظر به $\mathbb{Q}$ الجبری است زیر:

$P(x) = x^3 - 2 \in \mathbb{Q}[X] \wedge p(\sqrt[3]{2}) = (\sqrt[3]{2})^3 - 2 = 2 - 2 = 0$

برای $\sqrt[3]{2}$ یک پولینوم $P(x)$ دریافت شد که $\sqrt[3]{2}$ جذران است

(b) عدد حقیقی $\sqrt{2}$ نظر به $\mathbb{Q}$ الجبری است زیرا:

$p(x): x^2 - 2 \in \mathbb{Q}[X] \wedge p(\sqrt{2}) = (\sqrt{2})^2 - 2 = 0$

اعداد $\pi = 3.14159....$ و $e = 2.71828....$ در $\mathbb{R}/\mathbb{Q}$ اعداد transcendental اند. زیرا نمیتوان پولینومی $p(x) \in \mathbb{Q}[x]$ را دریافت نمود که $p(e) = 0$ شود. مگر در $\mathbb{C}/\mathbb{R}$ عناصر الجبری (algebraic) نظر به $\mathbb{R}$ اند. زیرا:

$P_1(x): = x - e \in \mathbb{R}[x]$, $P_2(x): = x - \pi \in \mathbb{R}[x]$

$P_1(e): = e - e = 0$, $P_2(\pi): = \pi - \pi = 0$

تعریف 8.4:

(a) یک توسعه فیلد K/F بنام algebraic (الجبری) یاد میشود درصورتکه هر $\alpha \in K$ الجبری نظر به F (algebraic over F) باشد و K بنام algebraic extension از F یاد می شود. یعنی درصورتکه:

$\forall \alpha \in K \implies \exists\, p \in F[X] ;\ p \neq 0 \wedge p(\alpha) = 0$

درغیر ان K/F بنام transcendental یاد میشود

(b) یک فیلد F بنام algebraic closure یاد میشود، درصورتکه:

$\forall\, p(x) \in F[X] , \deg(p(x)) > 0 \implies \exists\, a \in F \ ; p(a) = 0$

(یعنی هرپولینوم با درجه بزرکتراز صفر در F اقلاً دارای یک جذر است)

مثال 8.6 : توسعه فیلد $\mathbb{C}/\mathbb{R}$ الجبری (algebraic) است. زیرا:

$\alpha: a+ib \in \mathbb{C}$

$(x - \alpha) . (x - \bar{\alpha}) = (x - (a+ib)).(x - (a - ib))$

$= x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[X]$

$p(x) := x^2 - 2ax + (a^2 + b^2)$

$p(\alpha) = \alpha^2 - 2a\alpha + a^2 + b^2 = (a + ib)^2 - 2a(a + ib) + a^2 + b^2$

$= a^2 + 2aib - b^2 - 2a^2 - 2aib + a^2 + b^2 = 0$

چون برای هر $\alpha \in \mathbb{C}$ یک پولینوم $p(x)$ در $\mathbb{R}[X]$ دریافت شد که $p(\alpha) = 0$ است. درنتیجه $\mathbb{C}/\mathbb{R}$ الجبری (algebraic) است

لیما 8.1: K و F ساحه اند.

K/F finite (متناهی) $\Longrightarrow$ K/F algebraic

ثبوت: چون K/F متناهی است، پس ما فرض میکنیم:

n:= [K:F]= dim(K,F)

پس قاعده (basis) فضای وکتوری K دارای n وکتور میباشد. یعنی تعداد وکتورهای مستقل خطی (linearly independet) در K زیادتر از n شده نمیتواند. پس برای یک $\alpha \in K$ سیت $\{1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^n\}$ وابسته خطی است

$1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^n$ (وابسته خطی)

$\Longrightarrow \exists\ a_0, a_1, a_2, \ldots, a_n \in F$ (not all zero);

$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$

$\Longrightarrow \alpha$ algebraic

$\Longrightarrow$ K/F algebraic

قضیه 8.1: (theorem of Lagrange for fields)

اگر K/T و T/F توسعه فیلد های متناهی (finite field extensions) باشند، درانصورت:

[K:F] = [K:T] . [T:F]

ثبوت: ما بعد فضای وکتوری K نظربه T را به m و بعد فضای وکتوری T نظر به F رابه n نشان میدهیم. یعنی:

dim(K,T) = m $\wedge$ dim(T,F) = n

ویا اینکه:

[K:T] = m $\wedge$ [T:F] = n

اگر $\{u_m, \ldots, u_3, u_2, u_1\}$ یک قاعده (basis) از فضای وکتوری K و $\{v_n, \ldots, v_3, v_2, v_1\}$ یک قاعده (basis) ازفضای وکتوری T باشد،درانصورت:

$u \in K \Longrightarrow \exists\ a_1, a_2, \ldots, a_m \in T$;

$u = a_1u_1 + a_2u_2 + \ldots + a_mu_m$

$= \sum_{i=1}^{m} a_i . u_i$

$a_i \in T \implies \exists\, b_{i1}, b_{i2}, \ldots, b_{in} \in F$;

$$a_i = b_{i1}v_1 + b_{i2}v_2 + \ldots + b_{in}v_n \quad (i=1,2,\ldots,m)$$
$$= \sum_{j=1}^{n} b_{ij}\, v_j$$

$$u = (b_{11}v_1 + b_{12}v_2 + \ldots + b_{1n}v_n).u_1 + (b_{21}v_1 + b_{22}v_2 + \ldots + b_{2n}v_n).u_2 + \ldots + (b_{m1}v_1 + b_{m2}v_2 + \ldots + b_{mn}v_n).u_m$$
$$= (b_{11}v_1.u_1 + b_{12}v_2.u_1 + \ldots + b_{1n}v_n.u_1) + (b_{21}v_1.u_2 + b_{22}v_2.u_2 + \ldots + b_{2n}v_n.u_2) + \ldots + (b_{m1}t_1.k_m + b_{m2}t_2.k_2 + \ldots + b_{mn}t_n.k_m)$$
$$= \sum_{i=1}^{m} a_i . u_i = \sum_{i=1}^{m}\left(\sum_{j=1}^{n} b_{ij}\, v_j\right) . u_i$$

دیده میشود وکتورهای ذیل که تعداد شان به m.n میرسد، یک span فضای وکتوری K است

$$\{(u_i . v_j) \mid i = 1,1,\ldots,m \ \wedge\ j = 1,2,\ldots,n\}$$

حالاباید ثبوت نمایم که وکتورهای فوق مستقل خطی نیزاند.

$\sum_{i=1}^{m}(\sum_{j=1}^{n} b_{ij}\, v_j) . u_i = 0$

$\implies \sum_{j=1}^{n} b_{ij}\, v_j = 0$ [زیرا u_i قاعده است]

$\implies b_{ij} = 0 \ (i = 1,1,\ldots,m \ \wedge\ j = 1,2,\ldots,n)$ [زیرا v_j قاعده است]

ثبوت شد که $\{(u_i . v_j) \mid i = 1,1,\ldots,m \ \wedge\ j = 1,2,\ldots,n\}$ یک قاعده از فضای وکتوری K نظر به F است. پس:

$\dim((K,F)) = m.n$

$[K:F] = m.n = [K:T] . [T:F]$

تبصره 8.2:

(1) اگرمایک ساحه K و ساحه های فرعی T,F (subfield) باخاصیت $F \subseteq T \subseteq K$ داشته باشیم. درانصورت:

(a)

$r := [K:F]$, $m := [K:T]$, $n := [T:F] \implies m \mid r \ \wedge\ n \mid r$

یعنی r بالای m و n قابل تقسیم است.

(b) اگر [K:F] یک عدد اولیه باشد، درانصورت ساحه T مساوی به K ویا مساوی به F است. یعنی درانصورت دربین K و F موجودیت کدام ساحه دیگر ممکن نیست

(2)

$F_1 \subseteq F_2 \subseteq \ldots \subseteq F_n \quad \wedge \quad F_{i+1}/F_i \quad (i = 1,2,\ldots,n-1)$

finite field extension (توسعه فیلد متناهی)

$\Longrightarrow \quad [F_n:F_1] = \prod_{i=1}^{n-1} [\, F_{i+1} : F_i \,]$

تعریف 8.5 :

(a) پولینوم ذیل بنام monic plynomial یاد میشود، درصورتیکه $a_n = 1$ باشد

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots\ldots + a_2 x^2 + a_1 x + a_0$$

بطورمثال پولینوم ذیل monic است:

$$p(x) = x^4 + 5x^3 + 4x^2 + 3x + 6$$

(b) F یک ساحه (field) است. یک پولینوم $p(x) \in F[x]$ بنام reducible polynomial (قابل تجزیه) یاد میشود، درصورتکه:

(i) p(x) غیرثابت (not constant) باشد. یعنی: $\deg(p(x)) \neq 0$

(ii) دو پولینوم f(x),g(x) در $F[x]$ با خواص ذیل موجود باشند:

$$\deg(f(x)) \neq 0 \wedge \deg(g(x)) \neq 0 \wedge p(x) = f(x).g(x)$$

درغیران بنام irreducible polynomial (غیرقابل تجزیه) یاد میشود.

یعنی اگریک پولینوم به فکتورهای غیرثابت قابل تجزیه باشد ، بنام reducible polynomial ودرغیران بنام irreducible polynomial (غیرقابل تجزیه) یادمیشود

مثال 8.7:

$$P_1(x) = x^2 + 4x + 4 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$$
$$P_2(x) = x^2 - 4 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$$
$$P_3(x) = x^2 - 2 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$$
$$P_4(x) = x^2 + 1 \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$$
$$P_5(x) = x^2 - \frac{4}{9} \in \mathbb{Q}[X] \subseteq \mathbb{R}[X] \subseteq \mathbb{C}[X]$$

پولینوم های فوق رامیتوان بشکل ذیل نوشت:

$$P_1(x) = x^2 + 4x + 4 = (x + 2).(x + 2)$$
$$P_2(x) = x^2 - 4 = (x + 2).(x - 2)$$
$$P_3(x) = x^2 - 2 = (x + \sqrt{2}).(x - \sqrt{2})$$

$P_4(x) = x^2 + 1 = (x + i).(x - i)$

$P_5(x) = x^2 - \frac{4}{9} = (x + \frac{2}{3}).(x - \frac{2}{3})$

$p_6(x) = x^2 + \bar{1} \in \mathbb{Z}_2[X]$

$p_2(x), p_1(x)$ در $\mathbb{Z}$ پولینوم های reducible (قابل تجزیه) اند.

مگر $p_5(x), p_4(x), p_3(x)$ در $\mathbb{Z}$ پولینوم های irreducible اند.

$P_5(x)$ در $\mathbb{Q}$ پولینوم reducible است. مگر $p_4(x), p_3(x)$ در $\mathbb{Q}$ پولینوم های irreducible اند

$P3(x)$ در $\mathbb{R}$ پولینوم reducible ، مگر $p4(x$ در $\mathbb{R}$ پولینوم irreducible است

$p_6(x)$ در فیلد $\mathbb{Z}_2$ پولینوم reducible (قابل تجزیه) است. زیرا:

$p(x) = x^2 + \bar{1} = (x + \bar{1}).(x + \bar{1})$

مثال: مایک ساحه F و $p(x)= x^2 + 1 \in F[X]$ را داریم. $p(x)$ در F وقتی قابل تجزیه است ، درصورتکه یک λ در F موجود باشد که $\lambda^2 = -1$ صدق کند.

جدول ذیل نشان میدهد که در کدام ساحه پولینوم $p(x)= x^2 + 1$ قابل تجزیه است.

Field		p(x)
$\mathbb{C}$	$\lambda = i$, $p(i) = i^2 + 1 = -1 + 1 = 0$	reducible
$\mathbb{Z}_2$	$\lambda = \bar{1}$, $p(\bar{1}) = (\bar{1})^2 + \bar{1} = \bar{1} + \bar{1} = \bar{0}$	reducible
$\mathbb{Z}_3$		irreducible
$\mathbb{Z}_5$	$\lambda = \bar{2}$, $p(\bar{2}) = (\bar{2})^2 + \bar{1} = \bar{4} + \bar{1} = \bar{0}$	reducible

تبصره 8.3: K/F یک Field extension (توسعه فیلد) و $\alpha \in K$ یک عنصرالجبری نظر به F است

$I_\alpha := \{g \in F[x] \mid g(\alpha) = 0\}$

سیت I_α یک Ideal در رینگ F[x] است. زیرا:

$f,g \in I_\alpha \Rightarrow f(\alpha) = 0 \wedge g(\alpha) = 0 \Rightarrow (f+g)(\alpha) = 0$

$\Rightarrow f+g \in I_\alpha$

$f \in I_\alpha , g \in F[x] \Rightarrow f(\alpha) = 0 \Rightarrow f(\alpha).g(\alpha) = 0.g(\alpha) = 0$

$\Rightarrow f.g \in I_\alpha$

درنتیجه I_α یک ایدیال در $F[x]$ است

ان پولینوم که در I_α کوچکترین درجه داشته و monic باشد، بنام

minimal plynomial از α نظر به F یاد میشود و ما انرا به m_α نشان میدهیم. پولینوم m_α داراخواص ذیل میباشد:

(i) $I_\alpha = < m_\alpha >$

(یعنی m_α مولد ادیال I_α است)

(ii)

$$g \in I_\alpha \implies \exists\, f \in I_\alpha \; ; \; g = f.\, m_\alpha$$

(یعنی هرپولینوم از I_α بالای m_α قابل تقسیم بوده)

مثال 8.8 :

(a) در K/F هر $\alpha \in K$ دارای منیمال پولینوم ذیل میباشد:

$$m_\alpha(x) = x - \alpha$$

(b) در $\mathbb{C}/\mathbb{R}$ منیمال پولینوم (minimal plynomial) نظر به $i \in \mathbb{C}$ شکل ذیل را دارد:

$$m_i(x) = x2 + 1 \in \mathbb{R}[X]$$

زیرا:

$$m_i(i) = i2 + 1 = -1 + 1 = 0$$

دیگر خواص ان نیز صدق میکند

(c) ما توسعه فیلد $\mathbb{R}/\mathbb{Q}$ رادرنظرمیگریم. اعداد حقیقی $\sqrt{2}$ و $\sqrt[3]{2}$ نظر به $\mathbb{Q}$ الجبری اند. پولینوم های منیمال (minimal plynomial ان شکل ذیل را دارند:

$\alpha := \sqrt{2} \quad m_\alpha(x) = x^2 - 2 \in \mathbb{Q}[X]$

$\alpha = \sqrt[3]{2} \quad m_\alpha(x) = x^3 - 2 \in \mathbb{Q}[X]$

یعنی $x^2 - 2$ منیمال پولینوم از $\sqrt{2}$ نظر به $\mathbb{R}$ و $x^3 - 2$ منیمال پولینوم از $\sqrt[3]{2}$ نظر به $\mathbb{R}$ است.

تعریف 8.6: L/F یک توسعه فیلد است.

(a) $S \subseteq L$:(field adjunction)

ما کوچکترین ساحه فرعی (subfield) که S و F دران شامل باشد، به F(S) نشان میدهیم. گفته میشود که ساحه F(S) از F بواسطه adjunction (به معنی اتحاد) سیت S بوجود امده است.

اگر $S = \{a_1, a_2, \ldots, a_n\}$ باشد، درانصورت ما $F(a_1, a_2, \ldots, a_n)$ به جای F(S) و اگر $S = \{a\}$ باشد، درانصورت F(a) مینویسیم.

مثال:

در توسعه فیلد $\mathbb{R}/\mathbb{Q}$ فیلد $\mathbb{Q}(\sqrt{2})$ از $\mathbb{Q}$ بواسطه adjunction عدد $\sqrt{2}$ بوجود امده است. زیرا برای S:= $\{\sqrt{2}\}$:

$$S \subseteq \mathbb{R} \wedge \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(S) \subseteq \mathbb{R}$$

هم چنان در توسعه فیلد $\mathbb{C}/\mathbb{Q}$ فیلد $\mathbb{Q}(\sqrt{2}, i)$ از $\mathbb{Q}$ بواسطه adjunction اعداد $\sqrt{2}$ و i بوجود امده است. زیرا برای S:= $\{\sqrt{2}, i\}$

$$S \subseteq \mathbb{C} \wedge \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(S) \subseteq \mathbb{C}$$

(b) (Simple extention): توسعه فیلد L/F بنام Simple extention یاد میشود، درصورتکه یک $a \in$L موجودباشد که F(a) = L شود.

مثال : $\mathbb{C}/\mathbb{R}$ یک Simple extention است. زیرا برای $i \in \mathbb{C}$:

$$\mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$$

هم چنان $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ یک Simple extention است. زیرا برای $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

(c) (Splitting field): $p(x) \in F[X]$

ساحه L بنام Splitting field از p(x) نظر به F یاد میشود، درصورتکه:

(i) p(x) در L به فکتورهای خطی تجزیه شود. یعنی:

$P(x) = c(x-a_1).(x-a_2)\ldots.(x-a_n)$, $c \in F$, $a_1, a_2, \ldots, a_n \in L$

(ii)

$L = F(a_1, a_2, \ldots, a_n)$

تبصره 8.4: F یک فیلد است. اگر $p(x) \in$F[X] در F به فکتورهای خطی تجزیه شود، درانصورت F خودش Splitting field از P(x) است.

مثال 8.9:

(a)

$p_1(x) = X - 3$, $p_2(x) = x^2 - 4 = (x + 2)(x - 2) \in \mathbb{Q}[X]$

چون $p_1(x)$ و $p_2(x)$ در $\mathbb{Q}$ به فکتورهای خطی قابل تجزیه است و علاوه بران:

$$\mathbb{Q}(3) = \{a + 3b \mid a, b \in \mathbb{Q}\} = \mathbb{Q}$$

$$\mathbb{Q}(2, -2) = \mathbb{Q}(2)$$ [نظر به مثال 8.1. (d)]

$$\mathbb{Q}(2) = \{a + 2b \mid a, b \in \mathbb{Q}\} = \mathbb{Q}$$

دیده شد که $\mathbb{Q}$ نظر به $P_1(x)$ و $p_2(x)$ یک ساحه splitting است.

(b) ماتوسعه فیلد $\mathbb{R}/\mathbb{Q}$ رادرنظرمیگریم

$p(x) = x^2 - 2 \in \mathbb{Q}[X] \implies p(x) = x^2 - 2 = (x + \sqrt{2}).(x - \sqrt{2})$

چون $\sqrt{2}, -\sqrt{2} \in \mathbb{R}$ است، پس ساحه splitting از $\mathbb{R}$ نظر به p(x) مساوی است به:

$\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ [نظر به مثال 8.1. (d)]

(c) ماتوسعه فیلد $\mathbb{C}/\mathbb{R}$ رادرنظرمیگریم

$p(x) = x^2 + 1 \in \mathbb{R}[X] \implies p(x) = (x + i). (x - i)$

چون $i, -i \in \mathbb{C}$ است، پس ساحه splitting از $\mathbb{C}$ نظر به p(x) مساوی است به:

$$\mathbb{R}(i, -i) = \mathbb{R}(i) = \mathbb{C}$$

(d)

$p(x) = (x^2 - 2).((x^2 + 1) \in \mathbb{Q}[X]$

$p(x) = (x^2 - 2).((x^2 + 1) = (x - \sqrt{2}). (x + \sqrt{2})$ (x+i)(x-i)

چون $i, \sqrt{2} \in \mathbb{C}$ است، پس $\mathbb{Q}(\sqrt{2}, i)$ ساحه یی splitting از $\mathbb{C}$ نظر به p(x) است.

قضیه 8.2: (fundamental theorem of algebra)

ساحه اعداد موهومی $\mathbb{C}$ یک ساحه ***algebraic closure*** (الجبری بسته) است یعنی هرتابع غیرثابت $p(x) \in \mathbb{C}[X]$ در $\mathbb{C}$ به فکتورهای خطی تجزیه میشود.

بطورمثال اگرپولینوم p(x) شکل ذیل را داشته باشد:

$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$

درانصورت اعداد $z_1, z_2, \ldots, z_n \in \mathbb{C}$ موجود است که:

$p(x) = a_n(x-z_1). (x-z_2).... (x-z_n)$

که درینجا $z_1, z_2, \ldots, z_n$ جذرهای پولینوم اند.

این قضیه اساسی الجبر بنام قضیه Gauss نیزیاد میشود. البته گوس اینرا درقسمت اعداد حقیقی ثبوت کرده است. یعنی هرپولینوم $p(x) \in \mathbb{R}[X]$ در فکتورهای خطی وفکتورهای مربعی قابل تجزیه است.

ثبوت: از ثبوت ان صرف نظر مینمایم.

تعریف 8.7: (quotient field) **:** ما انتگرال دومین (Integral domain)

D راداریم. یک ساحه Q بنام quotient field از D یاد میشود، درصورتکه :

(i) D یک رینگ فرعی (subring) از Q باشد

(ii)

$\forall\, a \in Q \;\; \exists\, r, s \in D \;;\; a = rs^{-1} \;\; (s^{-1} \in Q)$

ما انرا به Q = *quot*(D) نشان میدهیم

مثال 8.10: ساحه $(\mathbb{Q}, +, .)$ یک quotient field از $(\mathbb{Z}, +, .)$ است. یعنی:

$\mathbb{Q} = quot(\mathbb{Z})$

حل: ما میدانیم که $\mathbb{Z}$ یک انتگرال دومین است وبه اسانی میتوان ثبوت نمود که $\mathbb{Z}$ رینگ فرعی از $\mathbb{Q}$ نیزاست.

$\alpha \in \mathbb{Q} \implies \exists a, b \in \mathbb{Z}, b \neq 0 ;\ \alpha = \frac{a}{b}$ [$\mathbb{Q}$ نظربه تعریف]

$\implies b \in \mathbb{Q} \implies \exists b^{-1} \in \mathbb{Q}$ [زیرا $\mathbb{Q}$ یک ساحه است]

$\implies \alpha = \frac{a}{b} = ab^{-1} \implies$ (ii)

درنتیجه: $\mathbb{Q} = quot(\mathbb{Z})$

نوت: هرساحه quotient field خودش است

تعریف 8.8: (Eisenstein's Irreducibility criterion)

Eisenstein یک عالم ریاضی المانی (1852 – 1823) دریافت نمود ، که چه وقت یک پولینوم irreducible (غیر قابل تجزیه) است. D یک انتگرال دومین و Q یک ساحه quotient ان است.یعنی: Q=*quot*(D) . ما پولینوم ذیل راداریم:

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in D[X]\ ,\ a_n \neq 0\ ,\ n > 1$

f(x) پولینوم irreducible (غیرقابل تجزیه) است، درصورتکه یک عنصراولیه $p \in Q$ (primelement) باخواص ذیل موجود باشد:

(i) $p \nmid a_n$ (یعنی a_n بالای p قابل تقسیم نباشد)

(ii) $p \mid a_i$ $(i = 0,1,2,\ldots, n-1)$

(iii) $p^2 \nmid a_0$ (یعنی a_0 بالای p^2 قابل تقسیم نباشد)

نوت: ازثبوت ان فعلاً صرف نظرمی نمایم.

مثال 8.11:

(a) ما دیدیم که $\mathbb{Q} = quot(\mathbb{Z})$ است

$f(x) = x^3 + 9x^2 + 6x - 3 \in \mathbb{Z}[X]$

درین مثال

$a_3 = 1, a_2 = 9, a_1 = 6, a_0 = -3$

p = 3 یک عنصراولیه (primelement) در $\mathbb{Q}$ باخواص ذیل است:

(i) $P = 3 \nmid a_3 = 1$

(ii) $p = 3 \mid a_2 = 9$, $p = 3 \mid a_1 = 6$

(iii) $p^2 = 9 \nmid a_0 = -3$

چون بالای پولینوم f(x) خواص Eisenstein صدق میکند ، پس irreducible است.

تبصره: اگرشرایط ایزین شتاین (**Eisenstein's criterion**) را یک پولینوم نداشته باشد، درانصورت عموماً گفته نمیتوانیم که پولینوم reducible (قابل تجزیه) است. بطور مثال:

$f(x) = x^3 + 3x + 18 \in \mathbb{Z}[X]$

برای عدد اولیه 3 شرط (i) و (ii) صدق میکند، مگر (iii) صدق نمی کند. زیرا:

$3^2 = 9 \nmid a_0 = 18$

مگربازهم f(x) قابل تجزیه نیست.

تعریف 8.9: F یک ساحه (field) است و ما پولینوم ذیل را داریم:

$p(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in F[X]$

از انالیزمیدانیم که هر پولینوم در یک ساحه دارای مشتق (differentiable) است. پولینوم ذیل بنام مشتق(differential) از p(x) یاد میشود:

$p'(x) = n.a_n x^{n-1} + (n-1).a_{n-1}x^{n-2} + \dots + 2.a_2 x + a_1$

همان قوانین که در انالیزبرای مشتق موجود است، درینجا نیزصدق میکند. یعنی برای $a \in F$ و $p(x), q(x) \in F[X]$ میتوان نوشت:

$(p(x) + q(x))' = p'(x) + q'(x)$, $(a.p(x))' = a.\, p'(x)$

$(p(x).q(x))' = p'(x).q(x) + p(x).\, q'(x)$

تعریف 8.10: F یک ساحه (field) ، L یک توسعه فیلد (field extension) از F و $a \in L$ است. $P(x) \in F[X]$

a بنام multiple root (جذرمضاعف) از p(x) با مرتبه r یاد میشود، درصورتکه:

$(\exists r \in \mathbb{N}, r > 1)\ ; p(x) = (x-a)^r . q(x), \quad q(x) \in F[X]$

یا به عبارت دیگر:

$(x-a)^r \mid p(x) \ \wedge \ (x-a)^{r+1} \nmid p(x)$

(یعنی p(x) بالای $(x-a)^r$ قابل تقسیم و بالای $(x-a)^{r+1}$ قابل تقسیم نباشد)

اگر r = 1 باشد، درانصورت a جذرساده گفته میشود.

مثال

$p(x) = x^3 - 3x + 2 \in \mathbb{Q}[x]$

$p(x) = x^3 - 3x + 2 = (x-1)^2 . (x+2)$

عدد 1 جذرمتضاعف پولینوم فوق با مرتبه 2 و 2- جذرساده است.

لیما 8.2: F یک ساحه (field) و L سپلیتینگ فیلد (splitting field) از $p(x) \in F[X]$ است. بعدآ:

(a) $a \in L$

a یک multiple root (جذرمضاعف) از p(x) است

$\Leftrightarrow$

$p(a) = 0 = p'(a)$

(b)

p(x) در L یک جذرمضاعف (multiple root) دارد

یک تابع غیرثابت $q(x) \in F[X]$ موجود است که p(x) و $p'(x)$ بالای ان قابل تقسیم اند

یعنی:

$\exists\, q(x) \in F[X], \deg(q(x) > 0 ; q(x) \mid p(x) \wedge q(x) \mid p'(x)$

حل (a):

" $\Leftarrow$ " نظر به تعریف multiple root میتوان نوشت:

$(\exists r \in \mathbb{N} \wedge r > 1) ; p(x) = (x-a)^r . q(x), \quad q(x) \in F[X]$

$\Rightarrow p'(x) = r.(x-a)^{r-1}.\ Q(x) + (x-a)^r . q'(x)$

$\Rightarrow p'(a) = r.(a-a)^{r-1}.\ Q(x) + (a-a)^r . q'(x) = 0$

" $\Rightarrow$ " چون L ساحه سپلیتینگ (splitting field) است ، پس نظربه تعریف ان باید پولینوم p(x) درفکتورهای خطی قابل تجزیه باشد وما فرض میکنیم که a یک جذران است.

اگر a یک multiple root (جذرمضاعف) از p(x) نباشد ، یعنی:

$\exists\, q(x) \in F[X], q(a) \neq 0 \ \wedge \ p(x) = (x-a).q(x)$

$p'(x) = q(x) + (x-a)q'(x) \Rightarrow p'(a) = q(a) + (a-a)q'(a)$

$\Rightarrow p'(a) = q(a) \neq 0$

مگر این خلاف فرضیه است. پس باید a یک multiple root (جذرمضاعف) از p(x) باشد

حل (b):

" $\Longleftarrow$ " نظربه فرضیه باید یک multiple root (جذرتضاعف) $a \in L$ از $p(x)$ در L موجود باشد. درانصورت نظر به (1) باید $p(a) = 0 = p'(a)$ صدق نماید.

مااانراغیرمستقیم ثبوت می نمایم وفرض میکنیم که انوع یک تابع وجود ندارد. یعنی:

$$\nexists\, q(x) \in F[X], \deg(q(x) > 0 ; q(x) \mid p(x) \wedge q(x) \mid p'(x)$$

$$\Longrightarrow \gcd(p(x), p'(x)) = 1$$

$$\Longrightarrow \exists\, r(x), s(x) \in F[X],\ r(x).p(x) + s(x).p'(x) = 1$$

$$\Longrightarrow r(a).p(a) + s(a).p'(a) = 1$$

$$\Longrightarrow r(a).0 + s(a).p'(a) = s(a).p'(a) = 1$$

$$\Longrightarrow p'(a) \neq 0$$

مگراین خلاف فرضیه است. پس باید:

$$\exists\, q(x) \in F[X], \deg(q(x) > 0 ; q(x) \mid p(x) \wedge q(x) \mid p'(x)$$

" $\Longrightarrow$ " نظر به فرضیه میتوان نوشت:

$$\exists\, q(x) \in F[X], \deg(q(x) > 0 ; q(x) \mid p(x) \wedge q(x) \mid p'(x)$$

$$\Longrightarrow \exists\, r(x), s(x) \in F[X] ; p(x) = q(x).r(x),\ P'(x) = q(x).s(x)$$

چون L یک سپلیتینگ فیلد(splitting field) از $p(x)$ و $\deg(q(x) > 0$ است. پس $a \in L$ موجود است که $q(a)=0$ شود

$$\Longrightarrow p'(a) = q(a).s(a) = 0.s(a) = 0 = p(a)$$

درنتیجه $p(x)$ نظربه (a) در L دارای یک جذرتضاعف میباشد.

تبصره: از لیما فوق نتیجه میگریم ، که اگر $p(a)=0$ و $p'(a) \neq 0$ باشد ، درانصورت a جذر ساده از $p(x)$ است.

مثال 8.12:

$p(x) = x^3 - 2x^2 + x \in \mathbb{Q}[X]$

$p(x)$ دارای دوجذر 0 و 1 میباشد. که 1 جذرتضاعف (multiple root) بامرتبه 2 میباشد. زیرا

$p(x) = (x-1)^2 . x$

$p'(x) = 3x^2 - 4x + 1$

نظر به (a) لیمای فوق باید $p(1) = 0 = p'(1)$ و $p(0) = 0 \neq p'(0)$ باشد.

$P(1) = 1^3 - 2.1^2 + 1 = 1 - 2 + 1 = 0$

$p'(1) = 3.1^2 - 4.1 + 1 = 3 - 4 + 1 = 0$

$p(0) = 0^3 - 2.0^2 + 0 = 0$
$p'(0) = 3.0^2 - 4.0 + 1 = 1 \neq 0$

نظر به (b) لیمای فوق باید:

$$\exists\, q(x) \in F[X], \deg(q(x) > 0 ; q(x) \mid p(x) \wedge q(x) \mid p'(x)$$

ویااینکه:

$$\exists\, q(x) \in F[X], \deg(q(x) > 0 ; \gcd(p(x), p'(x)) = q(x)$$

مامیخواهیم $\gcd(p(x), p'(x))$ رادریافت نمایم

$$x^3 - 2x^2 + x = \frac{1}{3}x \,.\, (3x^2 - 4x + 1) + -\frac{2}{3}\,x^2 + \frac{2}{3}x$$
$$3x^2 - 4x + 1 = -\frac{9}{2} \,.\, (-\frac{2}{3}\,x^2 + \frac{2}{3}x) + (-x + 1)$$
$$-\frac{2}{3}\,x^2 + \frac{2}{3}x = -\frac{2}{3}x \,.\, (-x + 1) + 0$$

پس:

$$\gcd(p(x), p'(x)) = -x + 1 = q(x)$$

مثال 8.13 : ما فیلد $\mathbb{Z}_5$ رادرنظرمیگیریم

$$p(x) = x^3 + \bar{3}x + \bar{4} \in \mathbb{Z}_5\,[\mathbf{x}]$$
$$p(\bar{3}) = \bar{3}^3 + \bar{3}.\bar{3} + \bar{4} = (\bar{5}.\bar{5} + \bar{2}) + \bar{3}.\bar{3} + \bar{4}$$
$$= \bar{0} + \bar{2} + \bar{9} + \bar{4}$$
$$= \bar{2} + \bar{4} + \bar{4} = \overline{10} = \bar{2}\,.\,\bar{5} = \bar{2}\,.\,\bar{0} = \bar{0}$$

دیدیم که $\bar{3}$ یک جذر از p(x) است.

$$P'(x) = \bar{3}.x^2 + \bar{3}$$
$$P'(\bar{3}) = \bar{3}.\bar{3}^{\,2} + \bar{3} = \bar{3}\,.\,\bar{9} + \bar{3} = (\bar{5}.\bar{5} + \bar{2}) + \bar{3}$$
$$= \bar{2} + \bar{3} = \bar{0}$$

درنتیجه

$$P(\bar{3}) = \bar{0} = P'(\bar{3})$$

پس نظر به لیمای فوق $\bar{3}$ یک multiple root (جذرمضاعف) از p(x) در $\mathbb{Z}_5$ است. یعنی:

$$p(x) = x^3 + \bar{3}x + \bar{4} = (x - \bar{3})^2 \,.\, (x + \bar{1}$$

فصل نـهم

درین فصل میخواهیم راجع به چهار موضوعات ذیل بحث نمایم:
اول: درین بخش بعضی قضیای مهمی الجبر معاصر که درفصل های گذشته یاداورنشده، مطالعه نمایم.
دوم: راجع به فورمول Vieta معلومات میدهم و استعمال انرا برای حل پولینوم تحت مطالعه قرارمیدهم.
سوم: راجع به کریپتوگرافیCryptography (رمز نویسی) معلومات داده میشود. بعدآ کاربرد انرا تحت مطالعه قرارداده ومی بینیم که چطور برای استعمال کریپتوگرافی ازالجبرمعاصراستفاده میشود
چهارم: معادلات خطی دیوفینتنی (Diophantine linaer equation)
اول:
قضیه 9.1 (Cayley theorem) : هرگروپ به یک گروپ فرعی گروپ متناظر (symmetric group) ان گروپ ایزومورف (G-Isom) است. یعنی اگر (G ,.) یک گروپ و (S(G), ∘) گروپ متناظران باشد، درانصورت یک گروپ فرعی H در S(G) موجود است که با G ایزومورف است.
یعنی: $G \cong H$
ثبوت: (G ,.) یك گروپ دارای عنصرعینیت e است . ما براي $a \in G$ تابع φ_a را به شکل ذیل تعریف مینمائیم .

$$\varphi_a : G \longrightarrow G$$
$$x \longmapsto a.x$$

φ_a بایجیکتیف (bijective) است. زیرا:

$$\varphi_a(x) = \varphi_a(y) \Rightarrow a.x = a.y \Rightarrow a^{-1}.a.x = a^{-1}.a.y$$
$$\Rightarrow e.x = e.y \Rightarrow x = y \Rightarrow \varphi_a \; injective$$

$x := a^{-1}.y$
$\varphi_a(x) = \varphi_a(a^{-1}.y) = a.a^{-1}.y = e.y = y \Rightarrow \varphi_a \; sujective$
ما سیت تمامی پرموتیشن بلای G را به S(G) نشان میدهیم. یعنی:
$S(G) := \{f : G \to G \mid f \;\; bijective\}$

ما میدانیم که S(G) نظربه ترکیب تابع یک گروپ است و عنصرعینیت ان تابع id است. حالا ما تابع ذیل راتعریف مینمایم:

$$F : (G,.) \longrightarrow (S(G),\circ)$$
$$a \longmapsto \varphi_a$$

چون φ_a بایجکتیف است، پس تعریف تابع F درست است.

F یک G-Hom :

برای $g,h \in G$ باید ثبوت شود که:

$$F(g.h) = F(g) \circ F(h)$$
$$F(gh) = \varphi_{gh}$$
$$\varphi_{gh}(x) = (gh).x = g.\varphi_h(x) = \varphi_g\left(\varphi_h(x)\right) = \left(\varphi_g \circ \varphi_h\right)(x)$$

$$\Rightarrow \ F(g.h) = F(g) \circ F(h) \Rightarrow F \ is\ G - Hom$$

$$F(g) = F(h) \Rightarrow \varphi_g = \varphi_h \Rightarrow \varphi_g(x) = \varphi_{h(x)} \ , \qquad \forall\, x \in G$$

$$\Rightarrow g.x = h.x \ , \forall\, x \in G \ \Rightarrow g.x.x^{-1} = h.x.x^{-1} \Rightarrow g.e = h.e$$
$$\Rightarrow g = h \Rightarrow F \ injective$$

ما image (تصویر) از G نظربه F را به H نشان میدهیم. یعنی:

$$H := F(G) \subseteq S(G)$$

نظربه قضیه 2.4 سیت H یک گروپ فرعی از S(G) و $F : G \longrightarrow H$ یک G-Isom است. درنتیجه گروپ G به یک گروپ فرعی گروب سیمیتری S(G) ان G-Isom است.

مثال: بالای سیت V={1,2,3,4} رابطه دوگانه " ∗„ ذیل در جدول کیلی نشان شده است:

∗	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

در جدول دیده میشود که 1 عنصر عینیت است و

$$2 * 2 = 3 * 3 = 4 * 4 = 1$$

پس هر عنصر معکوس خودش است.

برای $\lambda, \mu, \nu \in \mathbb{N}$ که $2 \leq \lambda, \mu, \nu \leq 4$ و λ, μ, ν ازهمدیگرمختلف باشند، رابطه دوگانه(binary operation) فوق بطورذیل تعریف شده است:

$$b_\lambda * b_\mu = b_\nu$$

$(V,*)$ نظر به جدول فوق یک گروپ است و بنام Klein four-group یاد میشود.

ما گروپ متناظر (symmetric group) انرا به $S(V)$ نشان میدهیم،که عنصرعینیت ان تابع id است. چون $|V| = 4$ است، پس:

$|S(V)| = 4i = 1.2.3.4 = 24$

یعنی گروب $S(V)$ دارای 24 عناصرمیباشد. برای $a = 1,2,3,4$ تابع ذیل رادرنظرمیگریم:

$$\varphi_a : V \longrightarrow V$$
$$x \longmapsto a * x$$

$$\varphi_1(V) = \{1*1, 1*2, 1*3, 1*4\} = \{1,2,3,4\}$$

$$\varphi_2(V) = \{2*1, 2*2, 2*3, 2*4\} = \{2,1,4,3\}$$

$$\varphi_3(V) = \{3*1, 3*2, 3*3, 3*4\} = \{3,4,1,2\}$$

$$\varphi_4(V) = \{4*1, 4*2, 4*3, 4*4\} = \{4,3,2,1\}$$

حالا تابع ذیل را درنظرمیگریم:

$$F : (V,*) \longrightarrow (S(V),\circ)$$
$$a \longmapsto \varphi_a$$

$$F(V) = \{\varphi_1(V), \varphi_2(V), \varphi_3(V), \varphi_4(V)\} \quad \wedge \quad |F(V)| = 4$$

$F(V)$ یک گروپ فرعی از $(S(V),\circ)$ است و $\varphi_1(V)$ عنصرعینیت ان میباشد. چون:

$$(\varphi_2 \circ \varphi_2)(V) = (\varphi_3 \circ \varphi_3)(V) = (\varphi_4 \circ \varphi_4)(V) = \varphi_1(V)$$

پس هر عنصر معکوس خودش است.

نظر به قضیه کیلی V و $F(V)$ باهم ایزومورف اند. یعنی: $V \cong F(V)$

مثال: جدول کیلی گروپ $(\mathbb{Z}_3, +)$ شکل ذیل رادارد:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

ما گروپ متناظر (symmetric group) انرا به $S(\mathbb{Z}_3)$ نشان میدهیم،که عنصرعینیت ان تابع id است. چون $|\mathbb{Z}_3| = 3$ است، پس:

$|S(\mathbb{Z}_3)| = 3\text{i} = 1.2.3 = 6$

یعنی گروب S(V) دارای 6 عناصر میباشد. برای $a = \bar{0}, \bar{1}, \bar{2}$ تابع ذیل رادرنظرمیگریم:

$$\varphi_a : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$$
$$\text{x} \longmapsto a + x$$

$\varphi_{\bar{0}}(\mathbb{Z}_3) = \{\bar{0} + \bar{0}, \bar{0} + \bar{1}, \bar{0} + \bar{2}\ \} = \{\bar{0}, \bar{1}, \bar{2}\}$

$\varphi_{\bar{1}}(\mathbb{Z}_3) = \{\bar{1} + \bar{0}, \bar{1} + \bar{1}, \bar{1} + \bar{2}\ \} = \{\bar{1}, \bar{2}, \bar{0}\}$

$\varphi_{\bar{2}}(\mathbb{Z}_3) = \{\bar{2} + \bar{0}, \bar{2} + \bar{1}, \bar{2} + \bar{2}\ \} = \{\bar{2}, \bar{0}, \bar{1}\}$

حالا تابع ذیل را درنظرمیگریم:

$$F : (\mathbb{Z}_3, +) \longrightarrow (\ S(\mathbb{Z}_3), \circ)$$
$$\text{a} \longmapsto \varphi_a$$

$F(\mathbb{Z}_3) = (\varphi_{\bar{0}}(\mathbb{Z}_3), \varphi_{\bar{1}}(\mathbb{Z}_3), \varphi_{\bar{2}}(\mathbb{Z}_3)\ \}\ \wedge\ |F(\mathbb{Z}_3)| = 3$

$F(\mathbb{Z}_3)$ یک گروپ فرعی از $(S(\mathbb{Z}_3), \circ)$ است و $\varphi_{\bar{0}}(\mathbb{Z}_3)$ عنصرعینیت ان میباشد. $\varphi_{\bar{1}}(\mathbb{Z}_3)$ معکوسی $\varphi_{\bar{2}}(\mathbb{Z}_3)$ است . زیرا:

$(\varphi_{\bar{1}} \circ \varphi_{\bar{2}})(\mathbb{Z}_3) = \varphi_{\bar{1}}\{\bar{2}, \bar{0}, \bar{1}\} = \{\bar{1} + \bar{2}, \bar{1} + \bar{0}, \bar{1} + \bar{1}\ \}$

$= \{\bar{0}, \bar{1}, \bar{2}\} = \varphi_{\bar{0}}(\mathbb{Z}_3)$

نظر به قضیه کیلی $\mathbb{Z}_3$ و $F(\mathbb{Z}_3)$ باهم ایزومورف اند. یعنی: $\mathbb{Z}_3 \cong F(\mathbb{Z}_3)$

لیما 9.1: ما اعداد طبعی $r_1, r_2, \dots, r_n$ که خلاف صفروبالای یکدیگرقابل تقسم نیستند، داریم. یعنی:

$$\gcd(r_i, r_j) = 1 \quad (i, j = 1,2, \dots, n \wedge i \neq j)$$

برای $k \in \mathbb{N}$ تابع ذیل یک R-Isom است:

$$\psi: \mathbb{Z}_{r_1 . r_2 \dots r_n} \longrightarrow \mathbb{Z}_{r_1} x\, \mathbb{Z}_{r_2} x \dots x\, \mathbb{Z}_{r_n}$$
$$k + r_1 . r_2 \dots r_n \mathbb{Z} \mapsto (k + r_1\mathbb{Z}, k + r_2\mathbb{Z}, \dots, k + r_n\mathbb{Z})$$

ثبوت:

$r \coloneqq r_1 . r_2 \dots r_n$

ψ injective:

$k + r\mathbb{Z}, m + r\mathbb{Z} \in \mathbb{Z}_r$

$k + r\mathbb{Z} = m + r\mathbb{Z} \iff k - m \in r\mathbb{Z}$ [نظربه لیما 3.12]

$\iff r \mid k - m \iff r_i \mid k - m \quad [i = 1,2, \dots, n]$

$\iff k + r_i\mathbb{Z} = m + r_i\mathbb{Z} \quad [i = 1,2, \dots, n]$

$\iff \psi(k + r\mathbb{Z}) = \psi(m + r\mathbb{Z})$

$\iff \psi \ injective$

ψ surjective:

$$|\mathbb{Z}_r| = r = \prod_{i=1}^{n} |\mathbb{Z}_{r_i}| = |\mathbb{Z}_{r_1} x\, \mathbb{Z}_{r_2} x \dots x\, \mathbb{Z}_{r_n}|$$

چون سیت های دومین (domain) وکودومین (codomain) متناهی و تعداد عناصرشان باهم مساوی اند، پس نظر به قضیه 0.1 تابع ψ سورجیکتیف است . ازجانب دیگر ψ نظربه تعریف یک R-Hom (با نظرداشت ثبوت قضیه 3.18) نیز است. درنتیجه ψ یک R-Isom است.

مثال:

$r_1 = 2, r_2 = 3, r = r_1 . r_2 = 2.3 = 6$

$$\psi: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 x\, \mathbb{Z}_3$$
$$k + 6\mathbb{Z} \mapsto (k + 2\mathbb{Z}, k + 3\mathbb{Z})$$

نظربه لیما 9.1 تابع ψ یک R-Isom است. مگربازهم درین مثال انرا ثبوت می نمایم

$k+6\mathbb{Z}, m+6\mathbb{Z} \in \mathbb{Z}_6$

$$\psi\big((k+6\mathbb{Z})+(m+6\mathbb{Z})\big) = \psi((k+m)+6\mathbb{Z})$$
$$= ((k+m)+2\mathbb{Z}, (k+m)+3\mathbb{Z})$$
$$= ((k+2\mathbb{Z})+(m+2\mathbb{Z}), (k+3\mathbb{Z})+(m+3\mathbb{Z}))$$
$$= (k+2\mathbb{Z}, k+3\mathbb{Z}) + (m+2\mathbb{Z}, m+3\mathbb{Z})$$
$$= \psi\big((k+6\mathbb{Z})+\psi(m+6\mathbb{Z})\big)$$

$$\psi\big((k+6\mathbb{Z}).(m+6\mathbb{Z})\big)$$
$$= \psi(k.m+6\mathbb{Z}) = (\mathrm{km}+2\mathbb{Z}, \mathrm{km}+3\mathbb{Z})$$
$$= ((\mathrm{k}+2\mathbb{Z}).(\mathrm{m}+2\mathbb{Z}), (\mathrm{k}+3\mathbb{Z}).(\mathrm{m}+3\mathbb{Z}))$$
$$= ((\mathrm{k}+2\mathbb{Z}).(\mathrm{k}+3\mathbb{Z}), (\mathrm{m}+2\mathbb{Z}).(\mathrm{m}+3\mathbb{Z}))$$
$$= \psi\big((k+6\mathbb{Z}).\psi(m+6\mathbb{Z})\big)$$

درنتیجه ψ یک R-Hom است. بطورمثال ما انرا برای عناصر $\bar{3}, \bar{4} \in \mathbb{Z}_6$ امتحان می نمایم. برای مشخص شدن عناصر رینگ های $\mathbb{Z}_2$ ، $\mathbb{Z}_3$ و $\mathbb{Z}_6$ را به شکل ذیل نشان میدهیم:

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\} = \{[0]_2, [1]_2\}$$

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\} = \{[0]_3, [1]_3, [2]_3\}$$

$$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$$

$$[0]_6 = \{0+6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\}, [1]_6 = \{1+6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\},$$

$$[2]_6 = \{2+6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\}, [3]_6 = \{3+6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\},$$

$$[4]_6 = \{4+6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\}, [5]_6 = \{5+6\mathrm{n} \mid \mathrm{n}\epsilon\mathbb{Z}\}$$

$$\psi\big((3+6\mathbb{Z})+(4+6\mathbb{Z})\big) = \psi(\bar{3}+\bar{4}) = \psi(\bar{1}) = \psi(1+6\mathbb{Z})$$
$$= (1+2\mathbb{Z}, 1+3\mathbb{Z})$$
$$\psi(3+6\mathbb{Z}) = (3+2\mathbb{Z}, 3+3\mathbb{Z})$$

$\psi(\,4+6\mathbb{Z}\,)=(\,4+2\mathbb{Z}\,,4+3\mathbb{Z}\,)$

$\psi(\,3+6\mathbb{Z}\,)\;+\;\psi(\,4+6\mathbb{Z}\,)$

$=(\,3+2\mathbb{Z}\,,3+3\mathbb{Z}\,)+\;(\,4+2\mathbb{Z}\,,4+3\mathbb{Z}\,)$

$=(\,7+2\mathbb{Z}\,,7+3\mathbb{Z}\,)=(\,[7]_2\,,[7]_3\,)$

$=\;([1]_2\,,[1]_3=(\,1+2\mathbb{Z}\,,1+3\mathbb{Z}\,)$

$=\psi\big((3+6\mathbb{Z})+\;(4+6\mathbb{Z})\big)$

$\psi\big((3+6\mathbb{Z})\,.\;(4+6\mathbb{Z})\big)=\;\psi(\bar{3}\,.\;\bar{4})=\;\psi(\bar{0}\,)=\psi(\,0+6\mathbb{Z}\,)$

$=(\,0+2\mathbb{Z}\,,0+3\mathbb{Z}\,)$

$\psi(\,3+6\mathbb{Z}\,)\;.\;\psi(\,4+6\mathbb{Z}\,)$

$=(\,3+2\mathbb{Z}\,,3+3\mathbb{Z}\,)\,.\,(\,4+2\mathbb{Z}\,,4+3\mathbb{Z}\,)$

$=(\,12+2\mathbb{Z}\,,12+3\mathbb{Z}\,)\;=(\,[12]_2\,,[12]_3\,)$

$=\;([0]_2\,,[0]_3=(\,0+2\mathbb{Z}\,,0+3\mathbb{Z}\,)$

$=\psi\big((3+6\mathbb{Z})\,.\;(4+6\mathbb{Z})\big)$

درنتیجه ψ یک R-Hom است.

مثال: برای $r_1=2, r_2=4$ لیما 9.1 صدق نمیکند. زیرا عدد 4 بالای 2 قابل تقسیم است

$\mathrm{r}=\;r_1.r_2=2.4=8$

$\psi\colon \mathbb{Z}_8 \;\to\; \mathbb{Z}_2\mathrm{x}\,\mathbb{Z}_4$

$k+8\mathbb{Z}\;\mapsto(k+2\mathbb{Z}\,,k+4\mathbb{Z})$

$\mathbb{Z}_2=\;\{\,\bar{0},\bar{1}\;\}=\{[0]_2\;,[1]_2\,\}$

$\mathbb{Z}_4=\;\{\,\bar{0},\bar{1},\bar{2},\bar{3}\;\}=\{[0]_4\;,[1]_4\,,\,[2]_4\,,\;[\bar{3}\,]\}$

$\mathbb{Z}_8=\;\{\,\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\,,\bar{6},\bar{7}\}$

$=\{[0]_8\;,[1]_8\,,\,[2]_8\;,[3]_8\,,\,[4]_8\;,[5]_8,[6]_8,[7]_8\}$

$[0]_8=\{0+8\mathrm{n}\mid \mathrm{n}\epsilon\mathbb{Z}\}\;\;,[1]_8=\{1+8\mathrm{n}\mid \mathrm{n}\epsilon\mathbb{Z}\}\;\;,$

$[2]_8=\{2+8\mathrm{n}\mid \mathrm{n}\epsilon\mathbb{Z}\}\,[3]_8=\{3+8\mathrm{n}\mid \mathrm{n}\epsilon\mathbb{Z}\},$

$[4]_8=\{4+8\mathrm{n}\mid \mathrm{n}\epsilon\mathbb{Z}\}\,,[5]_8=\{5+8\mathrm{n}\mid \mathrm{n}\epsilon\mathbb{Z}\}$

$[6]_8=\{6+8\mathrm{n}\mid \mathrm{n}\epsilon\mathbb{Z}\}\;\;,[7]_8=\{7+8\mathrm{n}\mid \mathrm{n}\epsilon\mathbb{Z}\}$

تابع ψ اینجکتیف نیست. زیرا:

$$\psi(2+8\mathbb{Z}) = (2+2\mathbb{Z}, 2+4\mathbb{Z}) = ([2]_2, [2]_4)$$
$$= ([0]_2, [2]_4)$$
$$= (0+2\mathbb{Z}, 2+4\mathbb{Z})$$
$$\psi(6+8\mathbb{Z}) = (6+2\mathbb{Z}, 6+4\mathbb{Z}) = ([6]_2, [6]_4)$$
$$= ([0]_2, [2]_4) = (0+2\mathbb{Z}, 2+4\mathbb{Z})$$
$$= \psi(2+8\mathbb{Z})$$

مگر $2+8\mathbb{Z} \neq 6+8\mathbb{Z}$ است. پس ψ یک injective نیست

قضیه 9.2: (Chinese remainder theorem)

اگرما اعداد را باخواص ذیل داشته باشیم:

(i)

$$r_1, r_2, \ldots, r_n \in \mathbb{N}, \left(r_i \neq 0\ (i = 1,2,\ldots,n)\right)$$
$$\wedge\ (r_i \nmid r_j\ (i,j = 1,2,\ldots n), i \neq j)$$
$$(\gcd(r_i, r_j) = 1\ \ (i,j = 1,2,\ldots,n \wedge\ i \neq j)\quad \text{یعنی: })$$

(ii) $a_1, a_2, \ldots, a_n \in \mathbb{Z}$

بعدآ:

$$\exists! k \in \mathbb{Z};\ k \equiv a_i (\mathrm{mod}\ r_i)\ \ (i = 1,2,\ldots,n)$$

ثبوت:

$$a_i + r_i\mathbb{Z} \in \mathbb{Z}_{r_i}\ \ (i = 1,2,\ldots,n)$$
$$(a_1 + r_1\mathbb{Z}, a_2 + r_2\mathbb{Z}, \ldots, a_n + r_n\mathbb{Z}) \in \mathbb{Z}_{r_1} x\, \mathbb{Z}_{r_2}\, x \ldots x\, \mathbb{Z}_{r_n}$$

درلیما 9.1 دیدیم که تابع ذیل سورجتیکتیف (surjective) است:

$$\psi: \mathbb{Z}_{r_1 . r_2 \ldots r_n} \longrightarrow \mathbb{Z}_{r_1} x\, \mathbb{Z}_{r_2}\, x \ldots x\, \mathbb{Z}_{r_n}$$
$$k + r_1 . r_2 \ldots r_n\mathbb{Z} \mapsto (k + r_1\mathbb{Z}, k + r_2\mathbb{Z}, \ldots, k + r_n\mathbb{Z})$$

پس:

$$\exists k \in \mathbb{Z};$$
$$\psi(k + r_1 . r_2 \ldots r_n\mathbb{Z}) = (a_1 + r_1\mathbb{Z}, a_2 + r_2\mathbb{Z}, \ldots, a_n + r_n\mathbb{Z})$$

ازجانب دیگرنظربه تعریف ψ :

$$\psi(k + r_1 . r_2 \ldots r_n\mathbb{Z}) = (k + r_1\mathbb{Z}, k + r_2\mathbb{Z}, \ldots, k + r_n\mathbb{Z})$$

درنتیجه:

$$k + r_i\mathbb{Z} = a_i + r_i\mathbb{Z}\ \ (i = 1,2,\ldots,n)$$

$\Rightarrow k \equiv a_i (\mathrm{mod}\, r_i)\ \ (i = 1,2,\dots,n)$ [نظربه لیما 3.12]
ازجانب دیگرچون ψ اینجکتیف نیز است، پس فقط تنها یک انوع k موجود است

:solve equations of congruent classes

(حل معادلات کلاس های باقیمانده)

ما معادلات کلاس های باقیمانده ذیل راداریم:

$$X \equiv a_1 (\mathrm{mod}\, r_1), X \equiv a_2 (\mathrm{mod}\, r_2), \dots, X \equiv a_n (\mathrm{mod}\, r_n)$$
$$r_1, r_2, \dots, r_n \in \mathbb{N};\ \ \gcd(r_i, r_j) = 1\ \ (i,j = 1,2,\dots,n \wedge i \neq j)$$
$$a_1, a_2, \dots, a_n \in \mathbb{Z}$$

معادلات فوق رامیتوان به طریقه ذیل حل نمود:

$$r := r_1, r_2, \dots, r_n\ , s_i := \frac{r}{r_i}\qquad (i = 1,2,\dots,n)$$

حالا $k_i \in \mathbb{Z}$ باخواص ذیل دریافت مینمایم:

$$k_i . s_i \equiv 1 (\mathrm{mod}\, r_i)\qquad (i = 1,2,\dots,n)$$

چون $\gcd(r_i, s_i) = 1$ است، پس نظر به euclidean algorithm میتوان k_i رادریافت نمود. یعنی:

$$\exists k_i, m_i \in \mathbb{Z};\ \ k_i . s_i + m_i . r_i = 1\ \ (i = 1,2,\dots,n)$$
$$k := k_1 . s_1 . a_1 + k_2 . s_2 . a_2 + \dots + k_n . s_n . a_n$$

حل معادلات فوق سیت $k + r\mathbb{Z}$ است

مثال:

$$X \equiv 2(\mathrm{mod}\, 3),\qquad X \equiv 3(\mathrm{mod}\, 5),\qquad X \equiv 2(\mathrm{mod}\, 7)$$

درینجا:

$$a_1 = 2, a_2 = 3, a_3 = 2$$
$$r_1 = 3, r_2 = 5, r_3 = 7$$
$$r := r_1 . r_2 . r_3 = 3.5.7 = 105$$
$$s_1 = \frac{r}{r_1} = \frac{105}{3} = 35,\ s_2 = \frac{r}{r_2} = \frac{105}{5} = 21,\ s_3 = \frac{r}{r_3} = \frac{105}{7} = 15$$

حالا $k_1, k_2, k_3 \in \mathbb{Z}$ باخواص ذیل دریافت مینمایم:

$$k_1 . s_1 \equiv 1(\mathrm{mod}\, r_1) \Rightarrow k_1 . 35 \equiv 1(\mathrm{mod}\, 3)$$
$$k_2 . s_2 \equiv 1(\mathrm{mod}\, r_2) \Rightarrow k_2 . 21 \equiv 1(\mathrm{mod}\, 5)$$
$$k_3 . s_3 \equiv 1(\mathrm{mod}\, r_3) \Rightarrow k_3 . 15 \equiv 1(\mathrm{mod}\, 7)$$

نظر به euclidean algorithm :

$k_1 . 35 + y. 3 = 1$

$35 = 11.3 + 2$
$3 = 1.2 + 1$
$2 = 1.2 + 0$

$1 = 3 - 1.2 = 3 - 1.(35 - 11.3) = 12.3 - 1.35$
$k_1 = -1 = 2$ [زیرا : $1+2 = 0 \Longrightarrow 2 = -1$]

$k_2 . 21 + y. 5 = 1$
$21 = 4.5 + 1$
$4 = 1.4 + 0$

$1 = 21 - 4.5 = 1.21 - 4.5 \Longrightarrow k_2 = 1$

$k_3 . 15 + y. 7 = 1$
$15 = 2.7 + 1$
$7 = 1.7 + 0$

$1 = 15 - 2.7 = 1.15 - 2.7 \Longrightarrow k_3 = 1$

درنتیجه:

$k_1 = 2 , k_2 = 1 , k_3 = 1$
$k = k_1 . s_1 . a_1 + k_2 . s_2 . a_2 + k_3 . s_3 . a_3$
$= 2.35.2 + 1.21.3 + 1.15.2 = 233$

سیت حل معادلات شکل ذیل رادارد:

$k + r\mathbb{Z} = 233 + 105\mathbb{Z} = 2.105 + 23 + 105\mathbb{Z} = 23 + 105\mathbb{Z}$

$= \{23 + 105n \mid n \epsilon \mathbb{Z}\}$

بطورمثال برای $n = 1$ حل ان $23 + 105.1 = 128$ است. زیرا:

$128 = 42.3 + 2 \Longrightarrow 128 \equiv 2 (\mathrm{mod}\ 3)$

$128 = 25.5 + 3 \Longrightarrow 128 \equiv 3(\text{mod } 5)$
$128 = 18.7 + 2 \Longrightarrow 128 \equiv 2(\text{mod } 7)$
برای $n = -1$ حل ان $-82 = 23 - 105 = 23 + 105.(-1)$ است.زیرا:
$-82 = (-28).3 + 2 \Longrightarrow -82 \equiv 2(\text{mod } 3)$
$-82 = (-17).5 + 3 \Longrightarrow -82 \equiv 3(\text{mod } 5)$
$-82 = (-12).7 + 2 \Longrightarrow -82 \equiv 2(\text{mod } 7)$

مثال: سرمعلم یک مکتب میخواهد شاگردان مکتب رادرقطاراستاد کند.
اگرقطار3 نفره باشد، درانصورت 2 شاگرد باقی میماند
اگرقطار4 نفره باشد، درانصورت 1 شاگرد باقی میماند
اگرقطار7 نفره باشد، درانصورت هیچ شاگرد باقی نمی ماند
معلوم نماید که تعداد شاگردان دران مکتب اقلآچند خواهد بود

حل: معادلات کلاس های باقی مانده ان شکل ذیل رادارد:

$k \equiv 2(\text{mod } 3)\ ,\quad k \equiv 1(\text{mod } 4)\ ,\quad k \equiv 0\ b(\text{mod } 7)$

درینجا:

$a_1 = 2\ , a_2 = 1\ , a_3 = 0$
$r_1 = 3\ , r_2 = 4\ , r_3 = 7$
$r = r_1 . r_2 . r_3 = 3.4.7 = 84$

$$s_1 = \frac{r}{r_1} = \frac{r_1 . r_2 . r_3}{r_1} = r_2 . r_3 = 4.7 = 28$$

$$s_2 = \frac{r}{r_2} = \frac{r_1 . r_2 . r_3}{r_2} = r_1 . r_3 = 3.7 = 21$$

$$s_3 = \frac{r}{r_3} = \frac{r_1 . r_2 . r_3}{r_3} = r_1 . r_2 = 3.4 = 12$$

حالا $k_1, k_2, k_3 \in \mathbb{Z}$ باخواص ذیل دریافت مینمایم:

$k_1 . s_1 \equiv 1(\text{mod } r_1) \Longrightarrow k_1 . 28 \equiv 1(\text{mod } 3)$

$k_2 . s_2 \equiv 1(\text{mod } r_2) \Longrightarrow k_2 . 21 \equiv 1(\text{mod } 4)$

$k_3 . s_3 \equiv 1(\text{mod } r_3) \Longrightarrow k_3 . 12 \equiv 1(\text{mod } 7)$

نظر به euclidean algorithm :

$k_1 . 28 + y_1 . 3 = 1$
$28 = 9.3 + 1$
$3 = 1.3 + 0$
$1 = 28 - 9.3 \Longrightarrow k_1 = 1$

$k_2 . 21 + y_2 . 4 = 1$

$21 = 5.4 + 1$
$4 = 1.4 + 0$
$1 = 21 - 5.4 \Longrightarrow k_2 = 1$

$k_3 . 12 + y_3 . 7 = 1$

$12 = 1.7 + 5$
$7 = 1.5 + 2$
$5 = 2.2 + 1$
$2 = 1.2 + 0$

$1 = 5 - 2.2$
$= 5 - 2.(7 - 1.5) = 5 - 2.(7 - 1.(12 - 1.7))$
$= 12 - 1.7 - 2.7 + 2.12 - 2.7 = 3.12 - 5.7$

$\Longrightarrow k_3 = 3$

$k = k_1 . s_1 . a_1 + k_2 . s_2 . a_2 + k_3 . s_3 . a_3$
$= 1.28.2 + 1.21.1 + 3.12.0 = 77$

یک حل ان معادلات 77 بوده. یعنی ان مکتب اقلاً 77 شاگرد دارد . زیرا روابط ذیل نیزصدق میکنند:

$77 \equiv 2(\text{mod } 3)$, $77 \equiv 1(\text{mod } 4)$, $77 \equiv 0\ (\text{mod } 7)$

حل عمومی ان معادلات شکل ذیل رادارد:

$k + r\mathbb{Z} = 77 + 84\mathbb{Z} = \{77 + 84n \mid n \epsilon \mathbb{Z}\}$

برای امتحان اگر $n = 1$ باشد، درانصورت:

$k = 77 + 84.1 = 161$

زیرا:

$161 \equiv 2(\text{mod } 3)$,$161 \equiv 1(\text{mod } 4)$, $161 \equiv 0 \ (\text{mod } 7)$

دوم: فورمول ویتا (Vieta`s Formulas)

ویتا (Vieta) یک عالم فرانسوی (1540-1604) بوده که روابط بین جذرها و ضرایب یک پولینوم رابه شکل یک فورمول دراورد و بنام Vieta`s Formulas یاد میشود

قضیه polynomias und Vieta`s Formulas

اگرما پولینوم $p(x) \in \mathbb{C}[X]$ ذیل را داشته باشیم:

$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$

نظر به قضیه 8.2 پولینوم $p(x)$ به فکتورهای خطی قابل تجزیه است. یعنی اعداد $x_1, x_2, \ldots, x_n \in \mathbb{C}$ موجود است که:

$p(x) = a_n(x-x_1).(x-x_2)\ldots.(x-x_n)$

که درینجا $x_1, x_2, \ldots, x_n$ جذرهای پولینوم اند.

نظر به فورمول Vieta در بین جذرها وضرایب پولینوم فوق روابط ذیل موجود است:

$$x_1 + x_2 + x_3 + \ldots + x_n = -\frac{a_{n-1}}{a_n}$$

$$x_1x_2 + x_1x_3 + \ldots + x_1x_n + \ldots + x_{n-1}x_n = \frac{a_{n-2}}{a_n}$$

$$x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n = -\frac{a_{n-3}}{a_n}$$

$$\vdots$$

$$x_1x_2\ldots x_k + x_1x_2\ldots x_{k-1}x_{k+1} + \ldots + x_{n-k+1}x_{n-k+2}\ldots x_n = (-1)^k.\frac{a_k}{a_n}$$

$$\vdots$$

$$x_1x_2\ldots x_n = (-1)^n.\frac{a_0}{a_n}$$

البته علامات بعد ازمساوات از منفی (-) شروع شده بعداً بشکل متناوب مثبت (+) و منفی (-) میباشند. وعلامه اخیری $(-1)^n$ میباشد.

مثال8.14 : پولینوم $p(x) \in \mathbb{C}[X]$ ذیل راداریم:

$$p(x) = x^2 + x - 6$$

شکل عمومی ان:

$$p(x) = a_2x^2 + a_1x + a_0$$

درپولینوم فوق :

$$n = 2 \ , a_2 = 1 , a_1 = 1 \ , a_0 = -6$$

(a) جذرهای انرا از طریقه Vieta دریافت می نمایم

اگر x_1 و x_2 جذرهای ان باشند، درانصورت نظر به فورمل Vieta میتوان نوشت:

$$x_1 + x_2 = -\frac{a_1}{a_2} = -\frac{1}{1} = -1$$

$$x_1 . x_2 = (-1)^2 \frac{a_0}{a_2} = 1.\frac{-6}{1} = -6$$

برای دریافت جذرها باید اعداد رادریافت نمایم که معادلات فوق صدق نماید. ان اعداد عبارت اند از $x_1=2$ و $x_2=-3$. زیرا:

$$x_1 + x_2 = 2 - 3 = -1$$
$$x_1 . x_2 = 2. (-3) = -6$$

امتحان:

$$p(2) = 2^2 + 2 - 6 = 6 - 6 = 0$$
$$p(-3) = (-3)^2 + (-3) - 6 = 9 - 9 = 0$$

ازین نتیجه میشود که در پهلوی راهای دیگر میتوان جذر یک پولینومی درجه دو رابذریعه فورمل Vieta نیزدریافت نمایم.

(b) پولینوم درجه 2 را پیدا میکنیم ، که $(x_1)^2$ و $(x_2)^2$ جذرهای ان باشند

ما ان پولینوم را به $g(x)$ نشان میدهیم

$$g(x) = x^2 + b_1x + b_0$$

در (a) دیدیم:

$$x_1 + x_2 = -1$$
$$x_1 . x_2 = -6$$
$$(x_1)^2 + (x_2)^2 = (x_1 + x_2)^2 - 2. x_1. x_2$$
$$= (-1)^2 - 2.(-6) = 1+12 = 13 = -\frac{b_1}{1} = -b_1$$
$$(x_1)^2 . (x_2)^2 = (x_1. x_2)^2 = (-6)^2 = 36 = \frac{b_0}{1} = b_0$$

$b_1 = -13$, $b_0 = 36$

درنتیجه $g(x)$ شکل ذیل رادارد:

$$g(x) = x^2 + b_1x + b_0 = x^2 - 13x + 36$$

امتحان:

$$(x_1)^2 = (2)^2 = 4 \quad , \quad (x_2)^2 = (-3)^2 = 9$$
$$g(4) = 4^2 - 13.4 + 36 = 16 - 52 + 36 = 0$$
$$g(9) = (9)^2 - 13.9 + 36 = 81 - 117 + 36 = 0$$

دیدیم که 4 و 9 جذرهای پرلینوم $g(x)$ اند

مثال : ما پولینوم $p(x) \in \mathbb{C}[X]$ ذیل راداریم:

$$p(x) = 3x^2 - 2x - 1$$

شکل عمومی ان:

$$p(x) = a_2x^2 + a_1x + a_0$$

ما درپولینوم فوق داریم:

$$n = 2 \ , a_2 = 3 \ , a_1 = -2 \ , a_0 = -1$$

اگر x_1 و x_2 جذر (حل) ان باشند، درانصورت نظر به فورمل Vieta میتوان نوشت:

$$x_1 + x_2 = -\frac{a_1}{a_2} = -\frac{-2}{3} = \frac{2}{3} \qquad (I)$$
$$x_1 \, . \, x_2 = (-1)^2 \ \frac{a_0}{a_2} = -\frac{1}{3}$$

$x_1 = 1$ یک جذران معادله است. زیرا:

$$p(1) = 3.1^2 - 2.1 - 1 = 0$$

حالا از معادله (I) جذردوم را بدست میاوریم

$$x_1 + x_2 = \frac{2}{3} \implies x_2 = \frac{2}{3} - x_1 = \frac{2}{3} - 1 = -\frac{1}{3}$$

برای امتحان:

$$p(\frac{-1}{3}) = 3.(\frac{-1}{3})^2 - 2.\left(\frac{-1}{3}\right) - 1 = \frac{1}{3} + \frac{2}{3} - 1 = 0$$

مثال : ما پولینوم $p(x) \in \mathbb{C}[X]$ ذیل راداریم:

$$p(x) = x^4 - 5x^3 + 5x^2 + 5x - 6$$

شکل عمومی ان:

$p(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$

درینجا:

$n = 4 \ , a_4 = 1 \ , a_3 = -5 \ , a_2 = 5 \ , a_1 = -5 \ , a_0 = -6$

اگر x_1 ، x_2 ، x_3 و x_4 جذرهای ان باشند، درانصورت نظر به فورمل Vieta میتوان نوشت:

$$x_1 + x_2 + x_3 + x_4 = -\frac{a_3}{a_4} = -\frac{-5}{1} = 5$$

$$x_1 . x_2 + x_1 . x_3 + x_1 . x_4 + x_2 . x_3 + x_2 . x_4 + x_3 . x_4 = \frac{a_2}{a_4} = \frac{5}{1} = 5$$

$$x_1 . x_2 . x_3 + x_1 . x_2 . x_4 + x_2 . x_3 . x_4 = -\frac{a_1}{a_4} = -\frac{5}{1} = -5$$

$$x_1 . x_2 . x_3 . x_4 = (-1)^4 . \frac{a_0}{a_4} = 1 . \frac{-6}{1} = -6$$

اگر 2,-1,1 جذرهای ان باشند. میخواهیم جذرچهارم را دریافت نمایم

$$x_1 + x_2 + x_3 + x_4 = 1 - 1 + 2 + x_4 = 5 \implies x_4 = 5 - 2 = 3$$

امتحان:

$$p(1) = p(-1) = p(2) = p(3) = 0$$

مثال : ما پولینوم $p(x) \in \mathbb{C}[X]$ ذیل راداریم:

$$p(x) = 2x^3 - x^2 + 2x - 1$$

شکل عمومی ان:

$$p(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

درینجا:

$$n = 3 \ , a_3 = 2 \ , a_2 = -1 \ , a_1 = 2 \ , a_0 = -1$$

اگر x_1 ، x_2 و x_3 جذرهای ان باشند، درانصورت نظر به فورمل Vieta میتوان نوشت:

$$x_1 + x_2 + x_3 = -\frac{a_2}{a_3} = -\frac{-1}{2} = \frac{1}{2}$$

$$x_1 . x_2 + x_1 . x_3 + x_2 . x_3 = \frac{a_1}{a_3} = \frac{2}{2} = 1$$

$$x_1 . x_2 . x_3 = (-1)^3 . \frac{a_0}{a_3} = -1 . \frac{-1}{2} = \frac{1}{2}$$

اگردوجذران i و -i باشند. میخوهیم جذرسوم رادریافت نمایم

$$x_1 + x_2 + x_3 = i - i + x_3 = \frac{1}{2} \implies x_3 = \frac{1}{2}$$

مثال : ما پولینوم $p(x) \in \mathbb{C}[X]$ ذیل راداریم:

$p(x) = x^3 - 2x^2 + x - 2$
$p(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$

درینجا:

$n = 3 \ , a_3 = 1 \ , a_2 = -2 \ , a_1 = 1 \ , a_0 = -2$

اگر x_1 ، x_2 و x_3 جذرهای ان باشند، درانصورت نظر به فورمل Vieta میتوان نوشت:

$$x_1 + x_2 + x_3 = -\frac{a_2}{a_3} = -\frac{-2}{1} = 2$$

$$x_1 . x_2 + x_1 . x_3 + x_2 . x_3 = \frac{a_1}{a_3} = \frac{1}{1} = 1$$

$$x_1 . x_2 . x_3 = (-1)^3 . \frac{a_0}{a_3} = -1 . \frac{-2}{1} = 2$$

دیده میشود که دوجذر i و 2 اند. حالامیخوهیم جذرسوم رادریافت نمایم

$$x_1 + x_2 + x_3 = i + 2 + x_3 = 2 \quad \Longrightarrow \quad x_3 = 2 - 2 - i = -i$$

تمرین : ما پولینوم $p(x) \in \mathbb{C}[X]$ ذیل راداریم:

$p(x) = 2x^4 - x^3 + 5x^2 - 6x + 2$

اگر سه جذران اعداد ذیل باشند:

$x_1 = 1 \ , \ x_2 = i\sqrt{2} \ , \ x_3 = -i\sqrt{2}$

جذر چهارم ان چند است.

سوم: Cryptography (رمز نویسی)

بواسطه کرایپتوگرافی میتوان متن یک پیام را به شکل دیگری تبدیل نمود که هرکس انراخونده نتواند. فقط اشخاصیکه اجازه خواندن انرا داشته باشند، میتوانند انراپس به شکل اصلی بیاورند. برای عملی ساختن ان از الجبرمعاصراستفاده میشود. برای رمزنویسی طریقه های مختلف ازقبیل Poling-Hellan, ElGamal و RSA-Methodموجود اند.مادرینجا تنها طریقه RSA راتحت مطالعه قرارمیدهیم

:RSA-Cryptsystem

این طریقه رمزنویسی RSA از طرف سه ریاضی دان Shamir, Adleman و Rivest درسال 1978 کشف و دراختیارگذاشته شد. طرزالعمل RSA به شکل ذیل است:

(1) public key: پیام فرستنده (ارسال کننده) و گیرینده دربین خود با یک کلید عمومی (public key) باهم تفاهم می نمایند

(2) private key : این کلید فقط تنها برای پیام گیرینده معلوم است

ما شخص فرستنده پیام را به S و پیام گیرینده رابه R نشان میدهیم. طرزالعمل RSA دارای چهارمرحله ذیل است:

وظیفه پیام گیرینده R :

(i) R دوعدد اولیه بزرگ p ، q مختلف رااینتخاب میکند وبعدآ $n := p.q$ وضع مینماید

(ii) با استفاده از Euler-Function قیمت $\varphi(n)$ رادریافت می نماید. یعنی:

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$
$$n \longmapsto \varphi(n) = |\{k \in \mathbb{N} \mid 1 \leq k \leq n \wedge gcd(n,k) = 1\}|$$

$$\varphi(n) = (p-1).(q-1)$$

(iii) یک عدد ظبیعی e باخواص را ذیل انتخاب می نماید:

$$e \in \{2, \dots, \varphi(n)\} \quad \wedge \ gcd\big(e, \varphi(n)\big) = 1$$

(iv) یک عدد ظبیعی d راباخواص ذیل دریافت می نماید:

$$d \in \mathbb{N} \quad \wedge \ d.e \equiv 1 \big(\mathrm{mod}\ \varphi(n)\big)$$

یعنی: $\bar{d}$ معکوس از $\bar{e}$ در رینگ $\mathbb{Z}_{\varphi(n)}$ است

درینجا (e,n) کلید عمومی (public key) و (d,n) کلید خصوصی (private key) از R است. یعنی فقط تنها خود پیام گیرینده انرامیشناسد

وظیفه پیام فرستنده S :

(i) کلید عمومی (e,n) را از R بدست می اورد

(ii) یک پیام $\overline{m} \in \mathbb{Z}_n$ را انتخاب میکند

(iii) به کومک e و $\overline{m}$ پیام رمزی $\bar{c}$ را در $\mathbb{Z}_n$ به شکل ذیل بدست می اورد

$$\bar{c} := (\overline{m})^{e}$$

(iv) S این پیام رمزی $\bar{c}$ را به پیام گیرینده R میفریستد

حالا پیام گیرینده R ان پیام رمزی $\bar{c}$ را به پیام اصلی $\overline{m}$ طوری ذیل تبدیل میکند:

$$(\bar{c})^{d} = (\overline{m})^{ed} = \overline{m}$$

مثال: فاطمه میخواهد به مینا یک پیام ارسال نماید

فاطمه باید عملیات ذیل را اجرانماید:

(1) دوعدد اولیه p و q راانتخاب نموده وبعدآ n رابدست میاورد

$$p = 3\,,\ q = 11\,,\ n = p.q = 3.11 = 33$$

$$\varphi(33) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 33 \wedge gcd(33,k) = 1\}| = 20$$

یا:

$\varphi(n) = (\mathrm{p}-1).(\mathrm{q}-1)$

$\varphi(33) = (3-1).(11-1) = 20$

(2) عدد طبعی e را باخواص ذیل انتخاب مینماید:

$e \in \{2, \dots, \varphi(n)-1\} \quad \wedge \ gcd\big(e, \varphi(n)\big) = 1$

$e := 7$

$e = 7 \ \in \{2, \dots, 19\} \ \wedge \ \gcd(7,20) = 1$

$\overline{7} \ \in \mathbb{Z}_{20}$

(3) یک عدد ظبیعی d راباخواص ذیل را باید دریافت نماید:

$d \in \mathbb{N} \quad \wedge \ \mathrm{d.e} \ \equiv \ 1 \big(\mathrm{mod}\ \varphi(n)\big)$

یعنی: $\bar{d}$ معکوس از $\bar{e}$ در رینگ $\mathbb{Z}_{20}$ باشد

نظربه euclidean algorithm اعداد تام d و k باخواص ذیل موجود است:

$\mathrm{d.e} + \mathrm{k}.\varphi(n) = 1 = gcd\big(e, \varphi(n)\big)$

$\mathrm{d}.7 + \mathrm{k}.20 = 1 = gcd(7,20)$

$20 = 2.7 + 6$

$7 = 1.6 + 1$

$6 = 6.1 + 0$

$1 = 7 - 1.6$

$= 7 - 1.(20 - 2.7)$

$= \ 3.7 - 1.20$

$= \ 3.7 - 1.20 \Longrightarrow \ \bar{1} = \bar{3}.\bar{7} - \bar{1}.\overline{20} = \bar{3}.\bar{7} - \bar{1}.\bar{0} = \bar{3}.\bar{7}$

درنتیجه $\bar{3}$ معکوس از $\bar{7}$ در رینگ $\mathbb{Z}_{20}$ و $d = 3$ است.

(4) کلید عمومی و خصوصی ذیل را ترتیب مینماید

public key: $(\mathrm{e}, \mathrm{n}) = (7,33) \ \wedge$ private key: $(\mathrm{d}, \mathrm{n}) = (3,33)$

(5) فاطمه یک پیام ارسالی (بطورمثال عدد '4') راانتخاب نموده وبه پیام رمزی تبدیل میکند

$\bar{m} := \bar{4} \in \mathbb{Z}_{33}$

$$\bar{c} = (\bar{m})^e = (\bar{4})^7 = (\bar{4})^4.(\bar{4})^3 = \overline{256}.\overline{64}$$
$$= (7.\overline{33} + \overline{25}).(\overline{33} + \overline{31})$$
$$= (\bar{0} + \overline{25}).(\bar{0} + \overline{31}) = \overline{775} = 23.\overline{33} + \overline{16} = \overline{16}$$

پیام رمزی $\bar{c} = \overline{16}$ است

مینا باید عملیات ذیل را اجرانماید:

(1) معلومات راجع به کلید عمومی (public key) و پیام ازفاطمه بدست می اورد

$\bar{c} = \overline{16} \in \mathbb{Z}_{33}$, public key: $(e, n) = (7,33)$

(2) بعد از رسیدن پیام رمزی به مینا وی انرا دوباره به پیام اصلی به طورذیل تبدیل مینماید:

$(\bar{c})^d = (\overline{16})^3 = \overline{4096} = \overline{124}.\overline{33} + \bar{4} = \bar{4}$

درنتیجه معلوم شد که پیام اصلی عدد 4 است

مثال: درین مثال احمد میخواهد یک پیام بنام "BALKH„ رابه قادرارسال دارد.

برای اینکارهردوی شان به ترتیب جدول ذیل موافقه نمودند:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15

حالا پیام رابه جدول ترتیب می نمایم

B	A	L	K	H
02	01	12	11	08

قادردرینجا p و q مثال فوق را انتخاب میکند.

$p = 3, q = 11, n = p.q = 3.11 = 33$

public key: $(e, n) = (7,33) \wedge$ private key: $(d, n) = (3,33)$

نظر به جدول:

$B \rightsquigarrow 2, A \rightsquigarrow 1, L \rightsquigarrow 12, K \rightsquigarrow 11, H \rightsquigarrow 8$

احمد پیام اصلی رادرذیل رمزی(encryption) میسازد

$\bar{m}_1 = \bar{2} \in \mathbb{Z}_{33}, \bar{m}_2 = \bar{1} \in \mathbb{Z}_{33}, \bar{m}_3 = \overline{12} \in \mathbb{Z}_{33}$

$\bar{m}_4 = \overline{11} \in \mathbb{Z}_{33}, \bar{m}_5 = \bar{8} \in \mathbb{Z}_{33}$

$(\overline{m_1})^e = (\overline{2})^7 = \overline{128} = \overline{3}.\overline{33} + \overline{29} = \overline{29} = \overline{c_1}$

$(\overline{m_2})^e = (\overline{1})^7 = \overline{1} = \overline{c_2}$

$(\overline{m_3})^e = (\overline{12})^7 = (\overline{12})^3.(\overline{12})^3.\overline{12} = \overline{1728}.\overline{1728}.\overline{12}$

$= (\overline{52}.\overline{33} + \overline{12}).(\overline{52}.\overline{33} + \overline{12})\,\overline{12}$

$= (\overline{0} + \overline{12}).(\overline{0} + \overline{12}).\overline{12}$

$= \overline{1728} = \overline{52}.\overline{33} + \overline{12} = \overline{12} = \overline{c_3}$

$(\overline{m}_4)^e = (\overline{11})^7 = (\overline{11})^3.(\overline{11})^3.\overline{11} = \overline{1331}.\overline{1331}.\overline{11}$

$= (\overline{40}.\overline{33} + \overline{11}).(\overline{40}.\overline{33} + \overline{11})\,\overline{11}$

$= (\overline{0} + \overline{11}).(\overline{0} + \overline{11}).\overline{11}$

$= \overline{11331} = \overline{40}.\overline{33} + \overline{11} = \overline{11} = \overline{c_4}$

$(\overline{m_5})^e = (\overline{8})^7 = (\overline{8})^3.(\overline{8})^3.\overline{8} = \overline{512}.\overline{512}.\overline{8}$

$= (\overline{15}.\overline{33} + \overline{17}).(\overline{135}.\overline{33} + \overline{17})\,.\overline{8}$

$= (\overline{0} + \overline{17}).(\overline{0} + \overline{17}).\overline{8}$

$= \overline{2312} = \overline{70}\,.\overline{33} + \overline{2} = \overline{2} = \overline{c_5}$

احمد رمزهای ذیل را به محمود ارسال میدارد:

$c_1 = 29, c_2 = 1, c_3 = 12, c_4 = 11, c_5 = 2$

محمود انرا در زیر به پیام اصلی(decryption) تبدیل می نماید:

$(\overline{c_1})^d = ((\overline{m_1})^e)^d = ((\overline{2})^7)^3 = (\overline{29})^3$

$= \overline{24389} = 739.\ \overline{33} + \overline{2} = \overline{2} = \overline{m_1}$

$(\overline{c_2})^d = (\overline{1})^3 = \overline{1} = \overline{m_2}$
$(\overline{c_3})^d = (\overline{12})^3 = \overline{12} = \overline{m_3}$
$(\overline{c_4})^d = (\overline{11})^3 = \overline{11} = \overline{m_4}$
$(\overline{c_5})^d = (\overline{2})^3 = \overline{8} = \overline{m_5}$

$m_1 = 2, m_2 = 1, m_3 = 12, m_4 = 11, m_5 = 8$

اکنون قادراعداد فوق را نظر به جدول به پیام اصلی مبدل میسازد. یعنی:

$2 \rightsquigarrow B, 1 \rightsquigarrow A, 12 \rightsquigarrow L, 11 \rightsquigarrow K, 8 \rightsquigarrow H$

درنتیجه قادرمیداند که ان پیام ارسال شده *„BALKH"* بوده است.

تبصره: مادراینجا درمثال ها برای اسانی محاسبه اعداد اولیه کوچک p و q را انتخاب کردیم. مگردرحالات عمومی چون پیام ها طولانی میباشد ، این اعداد بزرگ انتخاب میشود ومحاسبه ان به بواسطه پروگرام های کمپیوتری به اسانی اجرامیشود

چهارم: معادلات خطی دیوفنتینی (**Diophantine linear equation**)

تعریف: معادله خطی ذیل بنام عالم یونانی Diophantine یاد میشود:

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = c \qquad (a_i \in \mathbb{Z}, i = 1,2,\dots,n)$$

دیوفنتینی (Diophantine) دریافت نمود که چه وقت میتواند معادله فوق دارای حل اعداد تام باشد. مگرمادرینجا فقط معادلات خطی دومجهوله را تحت مطالعه قرارمیدهیم

$$a.x + b.y = c \qquad (a, b, c \in \mathbb{Z})$$

دیوفنتینی (Diophantine) دریافت نمود که معادله فوق زمانی دارای حل اعداد تام میباشد، درصورتکه c بالای $\gcd(a, b)$ قابل تقسیم باشد. البته اینوع معادله چندین حل دارد. مافرض میکنیم که $g = \gcd(a, b)$ است. برای حل ان ماازدوطریقه ذیل استفاده مینمایم:

اول طریقه Euclidean Algorithm: نظر به Euclidean Algorithm میتوان اعداد r و s را باخواص ذیل دریافت نمود:

$$g = \gcd(a, b) = a.r + b.s$$

اگر $d := c/g$ باشد، درانصورت:

$$g.d = a.(d.r) + b.(d.s)$$
$$c = a.(d.r) + b.(d.s)$$

یک حل ان معادله مساوی است به:

$x_0 := d.r \ , y_0 := d.s$

حل معادله هوموگین (homogene) انرامیتوان به شکل ذیل دریافت نمود:

$$gcd(a,b) = g \implies \exists\, a_1, a_1 \in \mathbb{Z}\ ;\ a = g.a_1 \ , b = g.b_1$$

$$ax + by = 0$$
$$g.a_1.x + g.b_1.y = 0 \implies a_1.x = -b_1.y$$

معادله فوق دارای حل ذیل میباشد:

$$x_1 = b_1 t,\ y_1 = -a_1 t \qquad (\ t \in \mathbb{Z}\ )$$

حل عمومی ان:

$$(x,y) = (x_1,y_1) + (x_0,y_0) = (b_1 t, -a_1 t) + (x_0,y_0)$$

$$= \{(b_1 t + x_0\ , -(a_1 t + y_0)\ )\ \ (\ t \in \mathbb{Z}\ )\}$$

دوم استفاده از قضیه Fermat-Euler : نظر به قضیه Fermat-Euler :

$$gcd(a,b) = 1 \implies a^{\varphi(b)} \equiv 1 (\mathrm{mod}\ b)$$

$\varphi(b)$ اویلرفنکشن (Euler-Function) است که درگذشته انرا مطالعه کردیم وبه شکل ذیل تعریف شده:

$$\varphi(b) = |\{k \in \mathbb{N} \mid 1 \le k \le b \ \wedge\ gcd(b,k) = 1\}|$$

ومعادله $a.x + b.y = c$ دارای حل ذیل میباشد:

$$x \equiv c.a^{\varphi(b)-1} \ (\mathrm{mod}\ b)$$

یعنی:

$$x = c.a^{\varphi(b)-1} + tb \quad (\ t \in \mathbb{Z}\ )$$
$$y = c.\frac{1 - a^{\varphi(b)}}{b} - ta \quad (\ t \in \mathbb{Z}\ )$$

مثال:

$$6x + 10y = 100$$

درینجا $a = 6\ , b = 10\ , c = 100$ است

$$10 = 1.6 + 4$$

$$6 = 1.4 + 2$$
$$4 = 2.2 + 0$$

پس:

$$\gcd(10,6) = 2$$

$$\frac{c}{\gcd(a,b)} = \frac{100}{2} = 50$$

چون شرط دیوفنتینی (Diophantine) صدق میکند، پس معادله دارای حل اعداد تام میباشد.

برای حال ان اول باید اعداد r و s دریافت نمود که معادله ذیل راصدق کند:

$$\gcd(a,b) = a.r + b.s$$

$$2 = 6 - 1.4 = 6 - 1(10 - 1.6) = 2.6 - 1.10$$

دریافتیم که $r = 2, s = -1$ است و یک حل ان:

$$x_0 = r.d = 2.50 = 100, \qquad y_0 := s.d = -1.50 = -50$$

حالا حل معادله هوموگین (homogene) انرادریافت می نمایم

$$6x + 10y = 0$$
$$2.3.x + 2.5.y = 0 \implies 3.x + 5.y = 0 \implies 3.x = -5.y$$

معادله فوق دارای حل ذیل میباشد:

$$x_1 = 5t,\ y_1 = -3t \qquad (t \in \mathbb{Z})$$

حل عمومی ان:

$$(x,y) = (x_1,y_1) + (x_0,y_0) = (5t,-3t) + (100,-50)$$

$$= \{(5t + 100, -(3t + 50)) \quad (t \in \mathbb{Z})\}$$

امتحان برای $t = 2$:

$$(x,y) = (5t + 100, -(3t + 50) = (2.5 + 100, -(2.3 + 50))$$
$$= (110,-56)$$

حالا $(x,y) = (110,-56)$ رادرمعادله داده شده وضع مینمایم

$$6.110 + 10.(-56) = 660 - 560 = 100$$

دیده شد که حل معادله داده شده اعداد تام اند.

حل از طریقه قضیه Fermat-Euler :

$6x + 10y = 100\,, \gcd(6,10) = 2$

$\frac{6}{2}x + \frac{10}{2}y = \frac{100}{2} \Longrightarrow \quad 3x + 5y = 50$

درمعادله فوق $a = 3\,, b = 5\,, c = 50$

جون $\gcd(3,5) = 1$ است، پس طریقه قضیه Fermat-Euler قابل تطبیق است

$\varphi(b) = \varphi(5) = |\{k \in \mathbb{N} \mid 1 \leq k \leq 5 \wedge gcd(5,k) = 1\}| = 4$

$x = c.a^{\varphi(b)-1} + tb \quad (\ t \in \mathbb{Z}\ )$

$= 50.3^{4-1} + 5t \quad (\ t \in \mathbb{Z}\ ) = 50.3^{4-1} + 5t \quad (\ t \in \mathbb{Z}\ )$

$= 50.3^3 + 5t \quad (\ t \in \mathbb{Z}\ ) = 1350 + 5t \quad (t \in \mathbb{Z}\ )$

$y = c.\frac{1 - a^{\varphi(b)}}{b} - ta \quad (\ t \in \mathbb{Z}\ ) = 50.\frac{1 - 3^4}{5} - 3.t \quad (\ t \in \mathbb{Z}\ )$

$= 50.\frac{-80}{5} - 3.t \quad (\ t \in \mathbb{Z}\ ) = -800 - 3.t \quad (\ t \in \mathbb{Z}\ )$

امتحان برای t=0

$6x + 10y = 100$

$6.1350 + 10.(-800) = 8100 - 800 = 100$

مثال:

$168x + 238y = 126$

درینجا $a = 168\,, b = 238\,, c = 126$ است

$238 = 1.168 + 70$
$168 = 2.70 + 28$
$70 = 2.28 + 14$
$28 = 2.14 + 0$

پس:

$\gcd\,(238,168) = 14$

$$\frac{c}{\gcd(a,b)} = \frac{126}{14} = 9$$

چون شرط دیوفنتینی (Diophantine) صدق میکند، پس معادله دارای حل اعداد تام میباشد.

برای حال ان اول باید اعداد r و s دریافت نمود که معادله ذیل راصدق کند:

$$\gcd(a,b) = a.r + b.s$$

$$\begin{aligned} 14 &= 70 - 2.28 \\ &= 70 - 2(168 - 2.70) \\ &= 238 - 168 - 2(168 - 2(238 - 168)) \\ &= 238 - 168 - 2(168 - 2.238 + 2.168) \\ &= 238 - 168 - 2.168 + 4.238 - 4.168 \\ &= 5.238 - 7.168 \end{aligned}$$

دریافتیم که $r = -7, s = 5$ است و یک حل ان:

$$x_0 = r.d = -7.9 = -63, \qquad y_0 := s.d = 5.9 = 45$$

حالا حل معادله هوموگین (homogene) انرادریافت می نمایم

$$168x + 238y = 0$$

$$14.12.x + 14.17.y = 0 \implies 12x + 17.y = 0$$

$$\implies 12x = -17.y$$

معادله فوق دارای حل ذیل میباشد:

$$x_1 = 17t,\ y_1 = -12t \qquad (t \in \mathbb{Z})$$

حل عمومی ان:

$$\begin{aligned} (x,y) &= (x_1,y_1) + (x_0,y_0) = (17t,-12t) + (-63,45) \\ &= (17t - 63, -12t + 45) \quad (t \in \mathbb{Z}) \end{aligned}$$

تمرین: ما معادله ذیل را داریم:

$$4x + 6y = 16$$

(a) ثبوت نماید که شرط دیوفنتینی (Diophantine) درمعادله فوق صدق میکند

(b) برای دریافت حل عمومی از Euclidean Algorithm واز قضیه Fermat-Euler استفاده نماید

تمرين: احمد میخواهد یک کتاب را به قیمت 23 افغانی بخرد. احمد فقط 2 افغانیگی باخود و دکاندار 5 افغانیگی پول در دکان دارد. معلوم نماید که احمد برای خریدن کتاب چند دوافغانیگی به دکاندار و دکاندار چند پنج فغانیگی به احمد به دهد

(a) حل عمومی انرااززراه معادله دیوفنتینی (Diophantine) دریافت نماید

(b) از حل عمومی دریافت نماید که 14 دو افغانیگی و یک 5 افغانیگی نیزحل ان است

سمبولها (Symbols)

$a := b$	a ذریعه b تعریف شده
$a \Rightarrow b$	از افاده a افاده b نتیجه میشود
$a \Leftrightarrow b$	از a افاده b و از b افاده a نتیجه میشود
$A = \emptyset$	A یکسیت خالی است
$A \neq \emptyset$	A یکسیت خالی نیست
$a \in A$	a یک عنصر ازسیت A است
$a \notin A$	a یک عنصر ازسیت A نیست
$\forall a \in A$	برای هر عنصر a از A
$\wedge$	(conjuction)logical **and** (و)
	مثال $a \wedge b$: افادهای a **و** b صدق میکنند
$\vee$	(disjunction)logical **or** (یا)
	مثال $a \vee b$: افاده a **ویا** b صدق میکند
$\neg$	not (negation) (متناقض)
$\cup$	اتحادسیتها
$\cap$	تقاطعسیتها
$A \subset B$	Aسیت فرعی (sub set) از B
$A \subseteq B$	A سیت فرعی (sub set) از B ویا مساوی به B است
$A \setminus B$	$\{ a \in A \mid a \notin B \}$
$\exists b \in A$	یک عنصر b در A موجود است
$\exists! b \in A$	فقط تنها یک عنصر b در A موجود است
$N \trianglelefteq G$	N نورمال در G

اختصارات و تشریحات

$\mathbb{N}$ سیت اعداد طبیعی $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$

$\mathbb{Z}$ سیت اعداد تام $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$

$\mathbb{Q}$ سیت اعداد ناطق $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$

$\mathbb{R}$ سیت اعداد حقیقی $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$

$\mathbb{R}_+$ د مثبت حقیقی اعدادو سیت

$\mathbb{R}_+^0$ د مثبت حقیقی اعدادو سیت د صفرسره

$\mathbb{R}_-$ د منفی حقیقی اعدادو سیت

$\mathbb{R}_-^0$ د منفی حقیقی اعدادو سیت د صفر سره

$\mathbb{C}$ سیت اعداد موهومي ویا مختلط $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

$\mathbb{R}_+$ د مثبت حقیقی اعدادو سیت

$\mathbb{R}_+^0$ د مثبت حقیقی اعدادو سیت د صفرسره

$\mathbb{R}_-$ د منفی حقیقی اعدادو سیت

$\mathbb{R}_-^0$ د منفی حقیقی اعدادو سیت د صفر سره

$\mathbb{C}$ د موهومي اویاد مختلط اعدادو سیت $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$

Greek یونانی

homomorphism (Greek : homo same , morph form)

epimorphism (Greek: epi upon)

monomorphism (Greek: mono alone (تنها))

isomorphism (Greek: iso equal)

G-Hom	گروپ هموموفیزم	(Group Homomorphism)
G-End	گروپ اندوموفیزم	(Group Endomorphism)
G-Isom	گروپ ایزوموفیزم	Group Isomorphism)
G-Aut	گروپ اوتوموفیزم	(Group Automorphism)
R-Hom	رینگ هموموفیزم	(Ring Homomorphism)
R-End	رینگ اندوموفیزم	(Ring Endomorphism)
R-Aut	رینگ اوتوموفیزم	(Ring Automorphism)
R-Isom	رینگ ایزوموفیزم	(Ring Isomorphism)

Greek Letters

[حروف يونانى]

Uppercase (حروف كلان)		lowercase (حروف خورد)		
A	alpha	α		
B	beta	β		
Γ	gamma	γ		
Δ	delta	δ		
E	epsilon	ε	ϵ	epsilon variant
Z	zeta	ζ		
H	eta	η		
Θ	theta	θ	ϑ	theta variant
I	iota	ι		
K	kappsa	κ		
Λ	lambda	λ		
M	mu	μ		
N	nu	ν		
Ξ	xi	ξ		
O	onmicron	o		
Π	pi	π		
P	rho	ρ	ϱ	rho vaiant
Σ	sigma	σ	ς	sigma variant
T	tau	τ		
Υ	upsilon	υ		
Φ	phi	φ	ϕ	phi variant
X	chi	χ		
Ψ	psi	ψ		
Ω	omega	ω		

Bibliography

Prof.Dr.kurt meyberg	Algebra 2008 (Gruppen,Ringen,Körper)
Van der waerden	Algebra 1 1993
G.Ficher	Lehrbuch der Algebra 2008
D.A.R Wallace	Groups, Rings und Fields 2001
Chr.nelius	Grundlage der Algebra Vorlesung 2005
Prof. Dr. Annette Werner	Algebra I Vorlesung WS 2004/2005
Prof. Dr. Holger Brenner	Einführung in die Algebra Vorlesung SS 2009
Prof. Zink	Algebra I WS 2003/2004

دلیکوال ځان پیژندنه

ځه د بلخ ولسوالی د مهمندانوپه کلي زیږیدلی یم. د مهمندانود لمړی ښونځی د فارغیدو وروسته د کابل دابن سینا په منځنی ښونځی کی شامل شوم.
د دارالمعلیمین دفارغیدومی وروسته څوکاله دښونکی دنده درلوده. کابل د ساینس پوهنځی د فارغیدووروسته هلته د ریاضی په دیپارتمنت کی په علمی کادرکی وګمارل شوم. په هغه وخت کی د کابل پوهنتون د ساینس پوهنځی او د المان فدرالی دولت د Rheinischen Friedrich Wilhelms Univesity ترمینځ توامیت موجود وه. په همدي اساس ماته بورس راکړل شواوځه دریاضي په څانګه کي د لوړوزدکولپاره المان ته ولاړم. هلته می لمړی دیپلوم اووروسته مي ډاکتري دریاضی په څانګه کي د Bonn ښار په پورتنی پوهنتون کی لاسته راوړه. د 2009 کاله راهیسی دهرات اوننګرهارپه پوهنتونوکی مي څوسمیستره دمعاصرالجبر او خطي الجبر تدریس کړیدی.

Contents

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 279 different textbooks of Medicine, Engineering, Science, Economics, Journalism and Agriculture (96 medical textbooks funded by German Academic Exchange Service, 160 medical and non-medical textbooks funded by German Aid for Afghan Children, 7 textbooks funded by German-Afghan University Society, 2 textbooks funded by Consulate General of the Federal Republic of Germany, Mazar-e Sharif, 3 textbooks 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 VUSAF-Union of Assistance for Schools in Afghanistan (Afghanistan-Schulen), which has provided fund for this book. We would also like to mention that they have provided funds for 3 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 Universities, 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 and Fahim Habibi in the office for publishing books.

Dr Yahya Wardak
Advisor at the Ministry of Higher Education
Kabul, Afghanistan, March, 2019
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 VUSAF-Union of Assistance for Schools in Afghanistan (Afghanistan-Schulen) 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, 2019

Book Name	Algebra
Author	Dr Abdullah Mohmand
Publisher	Balkh University, Science Faculty
Website	www.ba.edu.af
Published	2019, First Edition
Copies	1000
Serial No	279
Download	www.ecampus-afghanistan.org
Printed at	Afghanistan Times Printing Press, Kabul

This publication was financed by VUSAF-Union of Assistance for Schools in Afghanistan (**Afghanistan-Schulen**).

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

Printed in Afghanistan 2019

ISBN 978 – 9936 – 633 – 14 – 8