BSMM301CCT

الجبرا

(Algebra)

مع

لیب مینول

(Lab Manual)

فاصلاتی اور روایتی نصاب پر مبنی خود اکتسابی مواد

برائے

بیچلر آف سائنس (بی۔ایس سی۔)

(تیسرا سمسٹر)

نظامت فاصلاتی تعلیم

مولانا آزاد نیشنل اردو یونیورسٹی

حیدرآباد-32، تلنگانہ-انڈیا

Course- Algebra

ISBN: 978-93-95203-14-2

First Edition: **2022**

ناشر	:	رجسٹرار، مولانا آزاد نیشنل اردو یونیورسٹی، حیدرآباد
اشاعت	:	2022
تعداد	:	600 کاپیاں
ترتیب و تزئین	:	ڈاکٹر کاشف خان، نظامت فاصلاتی تعلیم، مولانا آزاد نیشنل اردو یونیورسٹی، حیدرآباد
سرورق	:	ڈاکٹر محمد اکمل خان، نظامت فاصلاتی تعلیم، مولانا آزاد نیشنل اردو یونیورسٹی، حیدرآباد
مطبع	:	پرنٹ ٹائم اینڈ بزنس اینٹرپرائزس، حیدرآباد

Copy Editor

Dr. Khaja Moinuddin

Bachelor of Science (B.Sc.)

Algebra

3rd Semester

On behalf of the Registrar, Published by:

Directorate of Distance Education

Maulana Azad National Urdu University

Gachibowli, Hyderabad-500032 (TS), India

*Director:*dir.dde@manuu.edu.in *Publication :*ddepublication@manuu.edu.in

Phone number: 040-23008314 Website: manuu.edu.in

کورس کوآرڈی نیٹر

ڈاکٹر خواجہ معین الدین
اسسٹنٹ پروفیسر، شعبہ ریاضی
اسکول برائے سائنسی علوم، مولانا آزاد نیشنل اردو یونیورسٹی، حیدرآباد

مصنفین	اکائی نمبر
• ڈاکٹر محمد امین الدین، اسوسی ایٹ پروفیسر (رٹایرڈ)، گورنمنٹ ڈگری کالج فور گرلس، گول کونڈا، حیدرآباد	اکائی 1تا12
• ڈاکٹر کاشف خان، ریاضی، ڈی ڈی ای، مانو، حیدرآباد	اکائی 13
• ڈاکٹر افروز، اسوسی ایٹ پروفیسر، شعبہ ریاضی، مانو، حیدرآباد	اکائی 14
• ڈاکٹر خواجہ معین الدین، اسسٹنٹ پروفیسر، شعبہ ریاضی، مانو، حیدرآباد	اکائی 15،16

لیب مینول

• ڈاکٹر خواجہ معین الدین، اسسٹنٹ پروفیسر، شعبہ ریاضی، مانو، حیدرآباد	اکائی 17تا 20
• ڈاکٹر سید وسیم راجا، گیسٹ فیکلٹی (ریاضی)، شعبہ ریاضی، مانو، حیدرآباد	اکائی 21تا 24

مترجمین(Translators)

• ڈاکٹر کاشف خان، ریاضی، ڈی ڈی ای، مانو، حیدرآباد	اکائی 1،2،14

پروف ریڈرس:

اول	:	ڈاکٹر کاشف خان
دوم	:	ڈاکٹر افروز
فائنل	:	ڈاکٹر خواجہ معین الدین

فہرست

پیغام

مولانا آزاد نیشنل اُردو یونیورسٹی 1998 میں وطنِ عزیز کی پارلیمنٹ کے ایکٹ کے تحت قائم کی گئی۔اس کے چار نکاتی مینڈیٹس یہ ہیں۔ (1)اردو زبان کی ترویج و ترقی (2)اردو میڈیم میں پیشہ ورانہ اور تکنیکی تعلیم کی فراہمی (3)روایتی اور فاصلاتی تدریس سے تعلیم کی فراہمی اور (4)تعلیم نسواں پر خصوصی توجہ۔ یہ وہ بنیادی نکات ہیں جو اِس مرکزی یونیورسٹی کو دیگر مرکزی جامعات سے منفرد اور ممتاز بناتے ہیں۔ قومی تعلیمی پالیسی 2020 میں بھی مادری اور علاقائی زبانوں میں تعلیم کی فراہمی پر کافی زور دیا گیا ہے۔

اُردو کے ذریعے علوم کو فروغ دینے کا واحد مقصد و منشا اُردو داں طبقے تک عصری علوم کو پہنچانا ہے۔ ایک طویل عرصے سے اُردو کا دامن علمی مواد سے لگ بھگ خالی رہا ہے۔ کسی بھی کتب خانے یا کتب فروش کی الماریوں کا سرسری جائزہ اس بات کی تصدیق کر دیتا ہے کہ اُردو زبان سمٹ کر چند ''ادبی'' اصناف تک محدود رہ گئی ہے۔ یہی کیفیت اکثر رسائل واخبارات میں دیکھنے کو ملتی ہے۔ اُردو قاری اور اُردو سماج دورِ حاضر کے اہم ترین علمی موضوعات سے نابلد ہیں۔ چاہے یہ خود ان کی صحت و بقا سے متعلق ہوں یا معاشی اور تجارتی نظام سے، یا مشینی آلات ہوں یا ان کے گرد و پیش ماحول کے مسائل ہوں، عوامی سطح پر اِن شعبہ جات سے متعلق اردو میں مواد کی عدم دستیابی نے عصری علوم کے تئیں ایک عدم دلچسپی کی فضا پیدا کر دی ہے۔ یہی وہ چیلنجز ہیں جن سے اُردو یونیورسٹی کو نبرد آزما ہونا ہے۔ نصابی مواد کی صورت حال بھی کچھ مختلف نہیں ہے۔ اِسکولی سطح پر اُردو کتب کی عدم دستیابی کے چرچے ہر تعلیمی سال کے شروع میں زیر بحث آتے ہیں۔ چوں کہ اُردو یونیورسٹی کا ذریعہ تعلیم اُردو ہے اور اس میں عصری علوم کے تقریباً سبھی اہم شعبہ جات کے کورسز موجود ہیں لہٰذا اِن تمام علوم کے لیے نصابی کتابوں کی تیاری اِس یونیورسٹی کی اہم ترین ذمہ داری ہے۔

مجھے اِس بات کی بے حد خوشی ہے کہ یونیورسٹی کے ذمہ داران بشمول اساتذہ کرام کی انتھک محنت اور ماہرین علم کے بھرپور تعاون کی بنا پر کتب کی اشاعت کا سلسلہ بڑے پیمانے پر شروع ہو چکا ہے۔ ایک ایسے وقت میں جب کہ ہماری یونیورسٹی اپنی تاسیس کی 25ویں سالگرہ منا رہی ہے، مجھے اس بات کا انکشاف کرتے ہوئے بہت خوشی محسوس ہو رہی ہے کہ یونیورسٹی کا نظامتِ فاصلاتی تعلیم از سرِ نو اپنی کارکردگی کے نئے سنگِ میل کی طرف رواں دواں ہے اور نظامتِ فاصلاتی تعلیم کی جانب سے کتابوں کی اشاعت اور ترویج میں بھی تیزی پیدا ہوئی ہے۔ نیز ملک کے کونے کونے میں موجود تشنگانِ علم فاصلاتی تعلیم کے مختلف پروگراموں سے فیضیاب ہو رہے ہیں۔ گرچہ گزشتہ دو برسوں کے دوران کووڈ کی تباہ کن صورتِ حال کے باعث انتظامی امور اور ترسیل و ابلاغ کے مراحل بھی کافی دشوار کن رہے تاہم یونیورسٹی نے اپنی حتی المقدور کوششوں کو بروئے کار لاتے ہوئے نظامتِ فاصلاتی تعلیم کے پروگراموں کو کامیابی کے ساتھ روبہ عمل کیا ہے۔ میں یونیورسٹی سے وابستہ تمام طلبا کو یونیورسٹی سے جڑنے کے لیے صمیم قلب کے ساتھ مبارک باد پیش کرتے ہوئے اس یقین کا اظہار کرتا ہوں کہ ان کی علمی تشنگی کو پورا کرنے کے لیے مولانا آزاد اردو یونیورسٹی کا تعلیمی مشن ہر لمحہ ان کے لیے راستے ہموار کرے گا۔

پروفیسر سید عین الحسن
وائس چانسلر

پیغام

فاصلاتی طریقۂ تعلیم پوری دنیا میں ایک انتہائی کارگر اور مفید طریقۂ تعلیم کی حیثیت سے تسلیم کیا جاچکا ہے اور اس طریقۂ تعلیم سے بڑی تعداد میں لوگ مستفید ہورہے ہیں۔ مولانا آزاد نیشنل اُردو یونیورسٹی نے بھی اپنے قیام کے ابتدائی دنوں ہی سے اردو آبادی کی تعلیمی صورت حال کو محسوس کرتے ہوئے اِس طرزِ تعلیم کو اختیار کیا۔ مولانا آزاد نیشنل اردو یونیورسٹی کا آغاز 1998 میں نظامتِ فاصلاتی تعلیم اور ٹرانسلیشن ڈِویژن سے ہوا اور اس کے بعد 2004 میں باقاعدہ روایتی طرز تعلیم کا آغاز ہوا اور بعد ازاں متعدد روایتی تدریس کے شعبہ جات قائم کیے گئے۔ نو قائم کردہ شعبہ جات اور ٹرانسلیشن ڈِویژن میں تقرریاں عمل میں آئیں۔ اس وقت کے اربابِ مجاز کے بھرپور تعاون سے مناسب تعداد میں خود مطالعاتی مواد تحریر و ترجمے کے ذریعے تیار کرائے گئے۔

گزشتہ کئی برسوں سے یو جی سی۔ ڈی ای بی UGC-DEB اس بات پر زور دیتا رہا ہے کہ فاصلاتی نظامِ تعلیم کے نصابات اور نظامات کو روایتی نظامِ تعلیم کے نصابات اور نظامات سے کما حقہم آہنگ کرکے نظامتِ فاصلاتی تعلیم کے طلبا کے معیار کو بلند کیا جائے۔ چوں کہ مولانا آزاد نیشنل اردو یونیورسٹی فاصلاتی اور روایتی طرزِ تعلیم کی جامعہ ہے، لہٰذا اس مقصد کے حصول کے لیے یو جی سی۔ ڈی ای بی کے رہنمایانہ اصولوں کے مطابق نظامتِ فاصلاتی تعلیم اور روایتی نظامِ تعلیم کے نصابات کو ہم آہنگ اور معیار بلند کرکے خود اکتسابی مواد SLM از سرِ نو بالترتیب یو جی اور پی جی طلبا کے لیے چھ بلاک چوبیس اکائیوں اور چار بلاک سولہ اکائیوں پر مشتمل نئے طرز کی ساخت پر تیار کرائے جارہے ہیں۔

نظامتِ فاصلاتی تعلیم یو جی، پی جی، بی ایڈ، ڈپلوما اور سرٹیفکیٹ کورسز پر مشتمل جملہ پندرہ کورسز چلا رہا ہے۔ بہت جلد تکنیکی ہنر پر مبنی کورسز بھی شروع کیے جائیں گے۔ متعلمین کی سہولت کے لیے 9 علاقائی مراکز بنگلورو، بھوپال، دربھنگہ، دہلی، کولکاتا، ممبئی، پٹنہ، رانچی اور سری نگر اور 6 ذیلی علاقائی مراکز حیدرآباد، لکھنؤ، جموں، نوح، وارانسی اور امراوتی کا ایک بہت بڑا نیٹ ورک تیار کیا ہے۔ ان مراکز کے تحت سرِدست 144 متعلم امدادی مراکز (Learner Support Centres) نیز 20 پروگرام سنٹرس (Programme Centres) کام کررہے ہیں، جو طلبا کو تعلیمی اور انتظامی مدد فراہم کرتے ہیں۔ نظامت فاصلاتی تعلیم نے اپنی تعلیمی اور انتظامی سرگرمیوں میں آئی سی ٹی کا استعمال شروع کردیا ہے، نیز اپنے تمام پروگراموں میں داخلے صرف آن لائن طریقے ہی سے دے رہا ہے۔

نظامتِ فاصلاتی تعلیم کی ویب سائٹ پر متعلمین کو خود اکتسابی مواد کی سافٹ کاپیاں بھی فراہم کی جارہی ہیں، نیز جلد ہی آڈیو۔ ویڈیو ریکارڈنگ کا لنک بھی ویب سائٹ پر فراہم کیا جائے گا۔ اس کے علاوہ متعلمین کے درمیان رابطے کے لیے ایس ایم ایس کی سہولت فراہم کی جارہی ہے، جس کے ذریعے متعلمین کو پروگرام کے مختلف پہلوؤں جیسے کورس کے رجسٹریشن، مفوضات، کونسلنگ، امتحانات وغیرہ کے بارے میں مطلع کیا جاتا ہے۔

امید ہے کہ ملک کی تعلیمی اور معاشی حیثیت سے پچھڑی اردو آبادی کو مرکزی دھارے میں لانے میں نظامتِ فاصلاتی تعلیم کا بھی نمایاں رول ہوگا۔

پروفیسر محمد رضاءاللہ خان

ڈائرکٹر، نظامت فاصلاتی تعلیم

کورس کا تعارف

زیر نظر کتاب الجبرا کے موضوعات سے متعلق ہے اور یہ مولانا آزاد نیشنل اردو یونیورسٹی کے بی ایس سی کورس کے تیسرے سمسٹر کے نصاب پر مشتمل ہے۔ ابسٹراکٹ الجبرا سادہ ریاضیاتی عددی نظامی کے بجائے گروپس، رنگس اور ویکٹرس کے ابسٹراکٹ کانسپٹ (تصورات) سے متعلق ہے۔ گروپ تھیوری اور رنگ تھیوری ابسٹراکٹ الجرا کے دو اہم حصے ہیں۔ ابسٹراکٹ الجبرا کمپیوٹر سائنس، طبیعیات اور فلکیات میں متعدد اطلاقات تلاش کرتا ہے۔ اس کتاب کی نمایاں خصوصیت یہ ہے کہ اس میں مواد کو سہل طریقے سے آسان زبان میں مثالوں کے ساتھ سمجھایا گیا ہے تاکہ طلبا اپنے مضمون کو از خود سمجھ سکیں۔ کتاب کو دو حصوں میں تقسیم کیا گیا ہے۔ جس میں پہلا حصہ نظریات (تھیوری) پر مبنی ہے اور دوسرا حصہ پریکٹکل (تجربوں) پر منحصر ہے۔ پہلا حصہ سولہ (16) اکائیوں پر مشتمل ہے۔ اکائی 1 تا 3 میں گروپس، تحت گروپس، ہم سٹس کا تعارف، چند مثالیں، نظریات اور لگرانج کا قضیہ اور اس کے نتائج دیے گئے ہیں۔ اکائی 4 تا 8 میں نارمل تحت گروج، خارج قسمت گروپ، مبادلہ اور سائیکلی گروپ کے مسائل اور نظریات دیے گئے ہیں۔ نیز گروپ کے ہم معرفیت، یک معرفیت اور آٹو معرفزم کے بارے میں تفصیلی جانکاری دی گئی ہے۔ اکائی 9 تا 16 رنگ تھیور پر مشتمل ہے جس میں اکائی 9 تا 11 میں رنگس، تحت رنگس، انتگرال دامنہ،، فیلڈ پر کئی مسائل اور نظریات پیش کیے گئے ہیں۔ اکائی 12 میں رنگ ہم معرفیت اور یک معرفیت پر کئی مسائل اور نظریات دیے گئے ہیں۔ اکائی 13 تا 16 کثیر رکنی رنگ پر مشتمل ہے جس میں کئی نظریات، ان کے متعلق مسائل درج ہیں۔

طلبہ سے توقع کی جاتی ہے کہ وہ عملی کلاسوں ہیں شرکت کریں اور کونسلر کی رہنمائی ہیں تجرباتی مینول میں دیے گئے مسائل کو حل کرنے کی مہارت حاصل کریں۔ طلبہ کی مسئلہ حل صلاحیت کو بہتر بنانے کے لیے اس مینول میں اکائی 17 سے 24 تک تجرباتی حصہ دیا گیا ہے۔ طلبہ کی طرف سے کیے گئے کام کا ریکارڈ وہ عملی امتحان کے وقت جمع کریں۔

اس کتاب کی تدوین میں مصنفین، مترجمین، تدریسی و غیر تدریسی و انتظامی عملے کے تعاون کا شکریہ ادا کرتا ہوں۔ کتاب کو معیاری اور قابل عمل و فہم بنانے کی ممکن کوشش کی گئی ہے، تاہم کوئی بھی کوشش اپنے آپ میں مکمل نہیں ہوتی۔ اس ضمن میں اساتزہ اکرام، ماہرین طلبا کی آرا و مشوروں کا خیر مقدم کیا جائے گا۔

ڈاکٹر خواجہ معین الدین
کورس کوآرڈی نیٹر

الجبرا

(Algebra)

اکائی 1۔ گروپس

(Groups)

اکائی کے اجزا

1.0 تمہید(Introduction)

انیسویں صدی کے آخر میں ایک جرمن(German) ریاضی داں(Mathematician) جارج کینٹر(George Cantor) نے ریاضی کی ایک نئی شاخ کو متارف کروایا جسے بعد میں نظریہ سٹ(Set Theory) کا نام دیا گیا۔ بعد میں ایک فرانسیسی ریاضی داں ایوارسٹ گیلوا (Everiste Galois) نے اس مضمون پر تحقیقی کام کر کے تحقیق کا میدان ہموار کیا۔ ایک اور مشہور ریاضی داں نیلس ہینرک آبیل(Neils Henrik Abel, 1802-1829)نے متناہی نامعلوم اشیا کی سائمل ٹینیس(Simultaneous) خطی مساوات کے حلوں اور ان کے مبادلات(Permutations) پر کام کیا۔ بعد ازاں آبیل کے اعزاز میں ایک گروپ جو تقلیبی اصول کی تکمیل کرتا ہے، کو آبیلین گروپ کا نام دیا گیا۔

کسی سٹ **G** کے لیے ثنائی عمل (Binary Operation) ایک تفاعل ہے جو **G** کے ہر ایک مرتب جوڑے (Ordered Pair) کو G کے دوسرے عنصر(Element) سے جوڑتا ہے۔

کسی سٹ کو بہ لحاظ ثنائی عمل تین اور اصولوں(Axioms) تلازمی(Associative) اکائی کے وجود(Existence of Identity) اور معکوس کے وجود(Existence of Identity) کے لیے جانچا جاتا ہے۔ اگر یہ تینوں اصول متعرف ہو جاتے ہیں تب وہ سٹ گروپ کہلاتا ہے۔

اس اکائی میں ہم گروپ کی کچھ خصوصیات پر بھی بحث کریں گے۔ نیز کچھ مثالوں کو حل کیا گیا ہے جس سے یہ ظاہر ہوتا ہے کہ وہ معمول کے عمل (Usual Operations) کے تحت($+,\times,\times_{mod}, +_{mod}$) اور کچھ خاص عوامل (Special Operations) کے تحت گروپ یا آبیلین گروپ بناتے ہیں۔

1.1 مقاصد(Objectives)

اس اکائی کے مکمل ہونے پر آپ اس قابل ہو جائیں گے کہ :

- ثنائی عمل کیا ہے اور کوئی سٹ بند (Closed) ہوگا اگر وہ بند شی خاصیت (Closure Property) کی تکمیل کرتا ہے۔
- آپ اس اکائی میں گروپائڈ (Groupoid) یا کواضی گروپ(Quasi Group)، نصف گروپ (Semigroup)، مونائڈ(Monoid) اور گروپ سے متعارف ہو جائیں گے۔
- آبیلین گروپ(Abelian Group) یا تقلیبی(Commutative Group) گروپ کو سمجھ سکیں گے۔
- آپ یہ جانچ کر سکیں گے کہ کوئی سٹ کسی عمل کے تحت کن خصوصیات کی وجہ سے گروپ اور آبیلین گروپ ہوگا۔
- کسی گروپ کے اور اس کے عنصر(Element) کے رتبے(Order) کو سمجھ سکیں گے۔
- متناہی اور لا متناہی(Finite and Infinite) گروپس کی تعریف کر سکیں گے۔
- کسی گروپ کے عنصر کے رتبے کو حاصل کر سکیں گے۔

1.2 گروپس(Groups)

1.2.1 تعریفات اور مثالیں(Definitions and Examples)

کسی سٹ G پر ثنائی عمل $' * '$ ایک تفاعل ہے جو G کے ارکان کے مرتب ہر ایک جوڑے کو G کے دوسرے رکن سے جوڑتا ہے۔
دوسرے الفاظ میں اگر $\forall a, b \epsilon G \Rightarrow a * b \epsilon G$ ہے، تب G پر $*$ ایک ثنائی عمل کہلاتا ہے۔

مثال1۔ صحیح اعداد(Integers) کے سٹ $\mathbb{Z}$ پر جمع $(+)$ کا عمل ایک ثنائی عمل ہے۔
چوں کہ سبھی $a, b \epsilon \mathbb{Z}$ کے لیے $a + b \epsilon \mathbb{Z}$ یعنی دو صحیح اعداد کی جمع ایک صحیح عدد ہوتا ہے۔اس لیے صحیح اعداد کے سٹ پر جمع کا عمل ایک ثنائی عمل ہے۔

مثال2۔ صحیح اعداد کے سٹ پر ضرب $(\times)$ کا عمل بھی ایک ثنائی عمل ہے۔کیوں کہ دو صحیح اعداد کا حاصل ضرب صحیح عدد ہوتا ہے۔

مثال3۔ صحیح اعداد کے سٹ پر منفی $(-)$ کا عمل ایک ثنائی عمل ہوتا ہے۔
چوں کہ سبھی $a, b \in \mathbb{Z}$ کے لیے $a - b \in \mathbb{Z}$ یعنی دو صحیح اعداد کی منفی کا حاصل بھی ایک صحیح عدد ہوتی ہے۔اس لیے صحیح اعداد کے سٹ پر ممنفی کا عمل ایک ثنائی عمل ہے۔

مثال4۔ طبیعی اعداد(Natural Numbers) کے سٹ پر منفی $(-)$ کا عمال ایک ثنائی عمل نہیں ہوتا ہے۔
چوں کہ $3,10 \in \mathbb{N}$ کے لیے $3 - 10 = -7 \notin \mathbb{N}$، اس لیے طبیعی اعداد کے سٹ پر منفی کا عمل ایک ثنائی عمل نہیں ہے۔

نوٹ: ایک یا زیادہ ثنائی عوامل کے ساتھ کوئی سٹ الجبرائک اسٹرکچر کہلاتا ہے۔ جیسے $(\mathbb{Z}, +)$، $(\mathbb{Q}, \cdot)$، $(\mathbb{Z}, +, \cdot)$ الجبرائک اسٹرکچرس ہیں۔

گروپ کی تعریف: اپنے عناصر پر معرفہ عمل $' o '$ کے ساتھ ایک غیر خالی سٹ G گروپ کہلاتا ہے اگر یہ درجہ ذیل موضوعات کی تکمیل کرتا ہے:

G_1: ثنائی موضوع(Closure axiom): $\forall a, b \in G \Rightarrow aob \in G$

G_2: تلازمی موضوع (Associative axiom): $\forall a, b, c \in G \Rightarrow ao(boc) = (aob)oc$

G_3: اکائی موضوع (Identity axiom): $\forall a \in G \ \exists \ e \in G, s.t. \ aoe = eoa = a$

G_4: معکوس موضوع (Inverse axiom): ہر ایک $a \in G$ کے لیے $\exists \ b \in G, s.t. \ aob = boa = e$

نوٹ:

1. اگر کوئی گروپ تقلیبی موضوع(Commutative Axiom) $aob = boa, \ \forall a, b \in G$ کی بھی تکمیل کرتا ہو، تو یہ گروپ آبیلین گروپ(Abelian Group) یا تقلیبی گروپ کہلاتا ہے۔
2. اگر کوئی سٹ موضوعات G_1، G_2 اور G_3 کی تکمیل کرتا ہے تو یہ مونائڈ(Monoid) کہلاتا ہے۔
3. اگر کوئی سٹ موضوعات G_1 اور G_2 کو پورا کرتا ہے تو یہ نصف گروپ(Semi-Group) کہلاتا ہے۔

4. اگر کوئی سٹ موضوع G_1 کی تکمیل کرتا ہے تو یہ کواضی گروپ(Quasi-Group) یا گروپائڈ(Groupoid) کہلاتا ہے۔
5. کسی گروپ میں کم از کم ایک رکن(Element) ضرور ہوتا ہے جو کہ اکائی(e) ہوگا۔
6. کسی گروپ میں اکائی عنصر یکتا(Unique) ہوتا ہے۔
7. کسی گروپ میں ہر ایک عنصر کا معکوس(Inverse) یکتا ہوتا ہے۔

مثالیں:

مثال1۔ ثابت کرو کہ ضرب کے عمل کے تحت سٹ $\{1, -1, i, -i\}$ گروپ کی تشکیل کرتا ہے۔

حل۔ فرض کرو کہ $G = \{1, -1, i, -i\}$، جہاں $i = \sqrt{-1}$

درجہ ذیل جدول(Table)پر غور کریں

·	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

G_1: ثنائی موضوع(Closure axiom): جدول سے ہم دیکھتے ہیں کہ ثنائی موضوع کی تکمیل ہوتی ہے کیوں کہ $\forall a, b \in G \Rightarrow a \cdot b \in G$

G_2: تلازمی موضوع (Associative axiom): جدول سے ہم دیکھتے ہیں کہ تلازمی موضوع کی تکمیل ہوتی ہے کیوں کہ $\forall a, b, c \in G \Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$

e.g.

$$1.(i.(-i)) = (1.i).(-i)$$
$$\Rightarrow \quad 1.1 = i.(-i)$$
$$\Rightarrow \quad 1 = 1$$

G_3: اکائی موضوع (Identity axiom): $\forall a \in G \ \exists \ e = 1 \in G, s.t. \ a \cdot e = e \cdot a = a$ جدول سے ثابت ہے کہ $1 \in G$ ایک اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): ہر ایک $a \in G$ کے لیے $b \in G$ اس طرح وجود رکھتا ہے کہ $a.b = b.a = 1$

ہمیں حاصل ہے

1 کا معکوس $= 1$

-1 کا معکوس $= -1$

i کا معکوس $= -i$

i کا معکوس $= -i$

اوپر دیے گئے سبھی عناصر (Elements) سٹ G میں موجود ہیں۔اس لیے ضرب کے عمل کے تحت سٹ $\{1, -1, i, -i\}$ گروپ کی تشکیل کرتا ہے۔

مثال2۔ ثابت کرو کہ ضرب کے عمل کے تحت اکائی کے جذرالمکعب (Cube Roots of Unity) کا سٹ $\{1, w, w^2\}$ تقلیبی گروپ کی تشکیل کرتا ہے۔

حل۔ فرض کرو کہ $G = \{1, w, w^2\}$، جہاں $w^3 = 1$

درجہ ذیل جدول (Table) پر غور کریں

·	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

G_1: ثنائی موضوع (Closure axiom): جدول سے ہم دیکھتے ہیں کہ ثنائی موضوع کی تکمیل ہوتی ہے کیوں کہ ہر ایک حاصل کردہ عنصر G کا ایک عنصر ہے یعنی $\forall a, b \in G \Rightarrow a \cdot b \in G$

G_2: تلازمی موضوع (Associative axiom): جدول سے ہم دیکھتے ہیں کہ تلازمی موضوع کی تکمیل ہوتی ہے کیوں کہ $\forall a, b, c \in G \Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$

e.g.

$$1 \cdot (w \cdot w^2) = (1 \cdot w) \cdot w^2$$
$$\Rightarrow \quad 1 \cdot 1 = w \cdot w^2 \qquad [\because w^3 = 1]$$
$$\Rightarrow \quad 1 = 1$$

G_3: اکائی موضوع (Identity axiom): $\forall a \in G \ \exists \ e = 1 \in G, s.t. \ a \cdot e = e \cdot a = a$ اس لیے $1 \in G$، G کی اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): $\forall a \in G \ \exists \ b \in G$ کے لیے $a \cdot b = b \cdot a = 1$

ہمیں حاصل ہے

1 کا معکوس $= 1$

w کا معکوس $= w^2$

w^2 کا معکوس $=$ w

G_5: تقلیبی موضوع (Commutative axiom): $\forall a, b \in G \Rightarrow a \cdot b = b \cdot a$

e.g. $w \cdot 1 = 1 \cdot w$

$w = w$

چوں کہ G تقلیبی گروپ کے سبھی موضوعات کی تکمیل کرتا ہے، اس لیے G ایک تقلیبی گروپ ہے۔

مثال3۔ ثابت کرو کہ جمع بہ مقیاس 5 (Addition Modulo 5) یا $\oplus_5$ کے عمل کے تحت سٹ $\{0,1,2,3,4\}$ گروپ کی تشکیل کرتا ہے۔

حل۔ فرض کرو کہ $G = \{0,1,2,3,4\}\ mod\ 5$

درجہ ذیل جدول(Table) پر غور کریں

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

G_1: ثنائی موضوع(Closure axiom): جدول سے ہم دیکھتے ہیں کہ ثنائی موضوع کی تکمیل ہوتی ہے کیوں کہ ہر ایک حاصل کردہ عنصر G کا ایک عنصر ہے یعنی $\forall a,b \in G \Rightarrow a \oplus b \in G$، اس لیے $(G,\oplus_5)$ بند شی ہے۔

G_2: تلازمی موضوع (Associative axiom): جدول سے ہم دیکھتے ہیں کہ تلازمی موضوع کی تکمیل ہوتی ہے کیوں کہ

$$\forall a,b,c \in G \Rightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

$$\textbf{e.g.} \quad 2 \oplus (3 \oplus 4) = (2 \oplus 3) \oplus 4$$

$$\Rightarrow \quad 2 \oplus 2 = 0 \oplus 4$$

$$\Rightarrow \quad 4 = 4$$

G_3: اکائی موضوع (Identity axiom): $\forall a \in G\ \exists\ e = 0 \in G, s.t.\ a \oplus e = e \oplus a = a$ جدول سے $0 \in G$، G کی اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): $\forall a \in G\ \exists\ b \in G$ کے لیے $a \oplus b = b \oplus a = 0$ ہمیں حاصل ہے

0 کا معکوس = 0

1 کا معکوس = 4

2 کا معکوس = 3

3 کا معکوس = 2

4 کا معکوس = 1

اوپر دیے گئے سبھی عناصر(Elements) سٹ G میں موجود ہیں۔اس لیے جمع بہ مقیاس 5 یا $\oplus_5$ کے عمل کے تحت سٹ $\{0,1,2,3,4\}$ گروپ کی تشکیل کرتا ہے۔

مثال4۔ ثابت کرو کہ ضرب بہ مقیاس 5 (Multiplication Modulo 5) یا $\otimes_5$ کے عمل کے تحت سٹ $\{1,2,3,4\}$ گروپ کی تشکیل کرتا ہے۔

حل۔ فرض کرو کہ

$$G = \{1,2,3,4\}\ mod\ 5$$

درجہ ذیل جدول(*Table*) پر غور کریں

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

G_1: ثنائی موضوع(Closure axiom): جدول سے ہم دیکھتے ہیں کہ ثنائی موضوع کی تکمیل ہوتی ہے کیوں کہ $\otimes_5$ کے عمل سے حاصل کردہ ہر ایک عنصر، G کا ایک عنصر ہے یعنی $\forall a, b \in G \Rightarrow a \otimes b \in G$، اس لیے $(G, \otimes_5)$ بند شی ہے۔

G_2: تلازمی موضوع (Associative axiom): جدول سے ہم دیکھتے ہیں کہ ضرب بہ مقیاس 5 کے تحت تلازمی موضوع کی تکمیل ہوتی ہے کیوں کہ

$$\forall a, b, c \in G \Rightarrow a \otimes (b \otimes c) = (a \otimes b) \otimes c$$

e.g. $2 \otimes (3 \otimes 4) = (2 \otimes 3) \otimes 4$

$\Rightarrow$ $2 \otimes 2 = 1 \otimes 4$

$\Rightarrow$ $4 = 4$

G_3: اکائی موضوع (Identity axiom): $\forall a \in G \ \exists \ e = 1 \in G, s.t. \ a \otimes e = e \otimes a = a$ جدول سے $1 \in G$ اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): ہر ایک $a \in G$ کے لیے $b \in G$ اس طرح وجود رکھتا ہے کہ

$a \otimes b = b \otimes a = 1$

ہمیں حاصل ہے

1 کا معکوس = 1

2 کا معکوس = 3

3 کا معکوس = 2

4 کا معکوس = 4

اوپر دیے گئے سبھی عناصر(Elements) سٹ G میں موجود ہیں۔ اس لیے ضرب بہ مقیاس 5 یا $\otimes_5$ کے عمل کے تحت سٹ $\{1, 2, 3, 4\}$ گروپ کی تشکیل کرتا ہے۔

مثال5۔ جانچ کرو کہ کیا ضرب بہ مقیاس 6 (Multiplication Modulo 6) کے عمل کے تحت سٹ $\{1, 2, 3, 4, 5\}$ گروپ کی تشکیل کرتا ہے؟

حل۔ فرض کرو کہ

$$G = \{1, 2, 3, 4, 5\} \ mod \ 6$$

درجہ ذیل جدول(Table) پر غور کریں

$\otimes 6$	1	2	3	4	5

1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

G_1: ثنائی موضوع(Closure axiom): جدول سے ہم دیکھتے ہیں کہ ثنائی موضوع کی تکمیل نہیں ہوتی ہے کیوں کہ $\otimes_6$ کے عمل سے حاصل کردہ سبھی عناصر، G میں موجود نہیں ہیں

e.g. $2 \otimes 3 = 0 \notin G$

اس لیے دیا گیا سٹ گروپ کی تشکیل نہیں کرتا۔

مثال6۔ ثابت کرو کہ جمع کے عمل کے تحت ملتف اعداد (Complex Numbers) کا سٹ ایک آبیلین گروپ کی تشکیل کرتا ہے۔

حل۔ فرض کرو کہ $\mathbb{C} = \{a + bi \ / \ a, b \in \mathbb{R}\}$

G_1: ثنائی موضوع(Closure axiom): ہم دیکھتے ہیں کہ

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i \in \mathbb{C}$$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom): ہم دیکھتے ہیں کہ

$$\begin{aligned}(a_1 + b_1 i) + \{(a_2 + b_2 i) + (a_3 + b_3 i)\} &= (a_1 + b_1 i) + \{(a_2 + a_3) + (b_2 + b_3)i\} \\ &= \{a_1 + (a_2 + a_3)\} + \{b_1 + (b_2 + b_3)\}i \\ &= \{(a_1 + a_2) + a_3\} + \{(b_1 + b_2) + b_3\}i \\ &= \{(a_1 + a_2) + (b_1 + b_2)i\} + (a_3 + b_3 i) \\ &= \{(a_1 + b_1 i) + (a_2 + b_2 i)\} + (a_3 + b_3 i)\end{aligned}$$

اس لیے تلازمی موضوع کی تکمیل ہوتی ہے۔

G_3: اکائی موضوع (Identity axiom): $a = 0, \ b = 0$ کے لیے $a + bi = 0 + 0i = 0 \in \mathbb{C}$ اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): $\forall (a + bi) \in \mathbb{C} \ \exists \{-a + (-b)i\} \in \mathbb{C}$ اس طرح سے کہ

$$(a + bi) + \{-a + (-b)i\} = 0$$

اس لیے C میں ہر ایک کومپلیکس نمبر کا معکوس موجود ہے۔

G_5: تقلیبی موضوع (Commutative axiom): ہم دیکھتے ہیں کہ

$$\begin{aligned}(a_1 + b_1 i) + (a_2 + b_2 i) &= (a_1 + a_2) + (b_1 + b_2)i \\ &= (a_2 + a_1) + (b_2 + b_1)i \\ &= (a_2 + b_2 i) + (a_1 + b_1 i)\end{aligned}$$

چوں کہ $\mathbb{C}$ تقلیبی گروپ کے سبھی موضوعات کی تکمیل کرتا ہے، اس لیے $(\mathbb{C}, +)$ ایک تقلیبی گروپ ہے۔

مثال7۔ ثابت کرو کہ ضرب کے عمل کے تحت غیر صفری کومپلیکس نمبرات (Non Zero Complex Numbers) کا سٹ ایک آبیلین گروپ کی تشکیل کرتا ہے۔

حل۔ فرض کرو کہ $C_0 = \{a + bi \ / \ a, b \in \mathbb{R}, a^2 + b^2 \neq 0\}$

G_1: ثنائی موضوع(Closure axiom):ہم دیکھتے ہیں کہ

$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 \cdot a_2 - b_1 \cdot b_2) + (a_1 \cdot b_2 + b_1 \cdot a_2) i \in C_0$$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom):ہم جانتے ہیں کہ کومپلیکس نمبرات کا سٹ ضرب کے عمل کے تحت تلازمی موضوع کی تکمیل کرتا ہے۔یعنی

$$(a_1 + b_1 i) \cdot \{(a_2 + b_2 i) \cdot (a_3 + b_3 i)\} = \{(a_1 + b_1 i) \cdot (a_2 + b_2 i)\} \cdot (a_3 + b_3 i)$$

G_3: اکائی موضوع (Identity axiom): $a + bi = 1 + 0i = 1$ کے لیے $b = 0,\ a = 1$ ، $1 \in C_0$ اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): فرض کرو کہ

$$(a + bi) . x = 1$$

$$\Rightarrow \quad x = \frac{1}{a + bi} \times \frac{a - bi}{a - bi}$$

$$= \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \in C_0 \ \because a^2 + b^2 \neq 0$$

اس لیے C_0 میں ہر ایک غیر صفری کا مپلیکس نمبر کا معکوس موجود ہے۔

G_5: تقلیبی موضوع (Commutative axiom):ہم دیکھتے ہیں کہ

$$\begin{aligned}(a_1 + b_1 i) \cdot (a_2 + b_2 i) &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i \\ &= (a_2 a_1 - b_2 b_1) + (a_2 b_1 + b_2 a_1) i \\ &= (a_2 + b_2 i) \cdot (a_1 + b_1 i)\end{aligned}$$

چوں کہ C_0 تقلیبی گروپ کے سبھی موضوعات کی تکمیل کرتا ہے،اس لیے $(C_0, \cdot)$ ایک تقلیبی گروپ ہے۔

مثال8۔ ثابت کرو کہ جمع کے عمل کے تحت سبھی 2 x 2 حقیقی ماترس(Real Matrices) کا سٹ ایک آبیلین گروپ بناتا ہے۔

حل۔ فرض کرو کہ $M = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \ / \ a, b, c, d \in \mathbb{R}\right\}$

G_1: ثنائی موضوع(Closure axiom):ہم دیکھتے ہیں کہ

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} \in \mathrm{M}$$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom): ہمیں معلوم ہے کہ

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \left\{\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}\right\} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 + a_3 & b_2 + b_3 \\ c_2 + c_3 & d_2 + d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 + (a_2 + a_3) & b_1 + (b_2 + b_3) \\ c_1 + (c_2 + c_3) & d_1 + (d_2 + d_3) \end{bmatrix}$$

$$= \begin{bmatrix} (a_1 + a_2) + a_3 & (b_1 + b_2) + b_3 \\ (c_1 + c_2) + c_3 & (d_1 + d_2) + d_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$
$$= \left\{ \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \right\} + \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$$

اس لیے جمع کے عمل کے تحت سبھی 2 x 2 حقیقی ماترس کاسٹ تلازمی موضوع کی تکمیل کرتا ہے۔

G_3: اکائی موضوع (Identity axiom): $a = 0,\ b = 0,\ c = 0,\ d = 0$ کے لیے

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M$$

ماترس کے لیے جمع کے عمل کے تحت اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$ کے لیے ہمیں معلوم ہے کہ

$$\exists \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in M \ \ s.t. \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

اس لیے M میں ہر ایک ماترس کا معکوس موجود ہے۔

G_5: تقلیبی موضوع (Commutative axiom): ہم دیکھتے ہیں کہ

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{bmatrix}$$
$$= \begin{bmatrix} a_2 + a_1 & b_2 + b_1 \\ c_2 + c_1 & d_2 + d_1 \end{bmatrix}$$
$$= \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} + \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

چوں کہ M تقلیبی گروپ کے سبھی موضوعات کی تکمیل کرتا ہے، اس لیے $(M, +)$ ایک تقلیبی گروپ ہے۔

مثال 9۔ ثابت کرو کہ ضرب کے عمل کے تحت سبھی 2 x 2 کے غیر نادر ماترس (Non Singular Matrices) کا سٹ ایک غیر آبیلین (Non Abelian) گروپ بناتا ہے۔

حل۔ فرض کرو کہ $M_0 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} a, b, c, d \in \mathbb{R} \ / \ ad - bc \neq 0 \right\}$

G_1: ثنائی موضوع (Closure axiom): ہم دیکھتے ہیں کہ

اگر $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in M_0$ تب

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom): ہمیں معلوم ہے کہ ضرب کے عمل کے تحت سبھی 2 x 2 ماترس کاسٹ تلازمی موضوع کی تکمیل کرتا ہے۔ یعنی

$$A.(B.C) = (A.B).C$$

G_3: اکائی موضوع (Identity axiom): $a = 1,\ b = 0,\ c = 0,\ d = 1$ کے لیے

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_0$$

ماترس کے لیے ضرب کے عمل کے تحت ایک اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_0$ کے لیے ہمیں معلوم ہے کہ

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \in M_0, \qquad \because ad - bc \neq 0$$

اس لیے M_0 میں ہر ایک ماترس کا معکوس موجود ہے۔اس لیے ضرب کے عمل کے تحت سبھی 2 x 2 ماترس کا سٹ معکوس موضوع کی تکمیل کرتا ہے۔

G_5: تقلیبی موضوع (Commutative axiom): ہم دیکھتے ہیں کہ

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}.\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}.\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$$

$$\begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} \neq \begin{bmatrix} a_2a_1 + b_2c_1 & a_2b_1 + b_2d_1 \\ c_2a_1 + d_2c_1 & c_2b_1 + d_2d_1 \end{bmatrix}$$

چوں کہ M_0 تقلیبی موضوع کی تکمیل نہیں کرتا ہے،اس لیے $(M_0,\cdot)$ ایک تقلیبی گروپ کی تشکیل نہیں کرتا ہے۔اس لیے غیر تقلیبی گروپ ہے۔

مثال10۔ ثابت کرو کہ ماترسی ضرب کے عمل کے تحت سبھی $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \alpha \in \mathbb{R}$ کا سٹ ایک گروپ بناتا ہے۔

حل۔ فرض کرو کہ $G = \{A_\alpha / \alpha \in \mathbb{R}\}$

G_1: ثنائی موضوع(Closure axiom): مان لو کہ

$$\begin{aligned} A_{\alpha.}A_\beta &= \begin{bmatrix} cos\alpha & -sin\alpha \\ sin\alpha & cos\alpha \end{bmatrix}\begin{bmatrix} cos\beta & -sin\beta \\ sin\beta & cos\beta \end{bmatrix} \\ &= \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\sin\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{bmatrix} \\ &= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} \\ &= A_{\alpha+.\beta} \in G \end{aligned}$$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom): ہمیں معلوم ہے کہ ضرب کے عمل کے تحت سبھی ماترس کا سٹ تلازمی موضوع کی تکمیل کرتا ہے۔یعنی

$$\begin{aligned} A_\alpha.(A_\beta.A_\gamma) &= A_\alpha.A_{\beta+\gamma} \\ &= A_{\alpha+(\beta+\gamma)} \\ &= A_{(\alpha+\beta)+\gamma} \\ &= A_{\alpha+\beta}.A_\gamma \\ &= (A_\alpha.A_\beta).A\gamma \end{aligned}$$

G_3: اکائی موضوع (Identity axiom): ہم جانتے ہیں کہ $A_0 = \begin{bmatrix}\cos 0 & -\sin 0\\ \sin 0 & \cos 0\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \in G$

اس لیے ضرب کے عمل کے تحت $\begin{bmatrix}\cos 0 & -\sin 0\\ \sin 0 & \cos 0\end{bmatrix}$ اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): $\begin{bmatrix}a & b\\ c & d\end{bmatrix} \in M_0$ کے لیے ہمیں معلوم ہے کہ

$$A_\alpha^{-1} = \begin{bmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{bmatrix}^{-1} = \frac{1}{\cos^2\alpha + \sin^2\alpha}\begin{bmatrix}\cos\alpha & \sin\alpha\\ -\sin\alpha & \cos\alpha\end{bmatrix}$$

$$= \frac{1}{1}\begin{bmatrix}cos(-\alpha) & -sin(-\alpha)\\ sin(-\alpha) & cos(-\alpha)\end{bmatrix} = A_{(-\alpha)} \in G$$

اس لیے G میں ہر ایک ماترس کا معکوس موجود ہے۔اس سے ہم کہہ سکتے ہیں کہ ضرب کے عمل کے تحت ماترس کا سٹ G معکوس موضوع کی تکمیل کرتا ہے۔

چوں کہ G گروپ کے سبھی موضوعات کی تکمیل کرتا ہے،اس لیے $(G,\cdot)$ ایک گروپ کی تشکیل کرتا ہے۔

مثال 11۔ ثابت کرو کہ $\oplus$ کے عمل کے تحت سبھی صحیح اعداد کا سٹ $\mathbb{Z}$ ایک گروپ بناتا ہے،جب کہ

$$a \oplus b = a + b + 1, \qquad \forall a, b \in \mathbb{Z}$$

حل۔ دیا گیا ہے کہ $(\mathbb{Z},\oplus)$

G_1: ثنائی موضوع(Closure axiom): ہمیں جانچ کرنی ہے کہ $\forall a, b \in \mathbb{Z} \Rightarrow a \oplus b \in \mathbb{Z}$ ،جب کہ دیا گیا ہے

$$a \oplus b = a + b + 1, \qquad \forall a, b \in \mathbb{Z}$$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom):

$$\forall a, b, c \in \mathbb{Z} \Rightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$$
$$a \oplus (b + c + 1) = (a + b + 1) \oplus c$$
$$a + b + c + 1 + 1 = a + b + 1 + c + 1$$
$$a + b + c + 2 = a + b + c + 2$$

G_3: اکائی موضوع (Identity axiom):

$$\forall a \in \mathbb{Z} \Rightarrow \exists e \in \mathbb{Z}$$
$$\text{s.t.} \quad a \oplus e = a$$
$$a + e + 1 = a$$
$$e = -1 \in \mathbb{Z}$$

اس لیے $e = -1$ اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom):

$$\forall a \in \mathbb{Z} \ \exists b \in \mathbb{Z}$$
$$\text{s.t. } a \oplus b = -1$$
$$a + b + 1 = -1$$
$$b = -2 - a \in \mathbb{Z}$$

اس لیے $\mathbb{Z}$ میں ہر ایک عنصر کا معکوس موجود ہے۔اس سے ہم کہہ سکتے ہیں کہ $\oplus$ کے عمل کے تحت صحیح اعداد کا سٹ معکوس موضوع کی تکمیل کرتا ہے۔

چوں کہ $\mathbb{Z}$ گروپ کے سبھی موضوعات کی تکمیل کرتا ہے،اس لیے $(\mathbb{Z},\oplus)$ ایک گروپ کی تشکیل کرتا ہے۔

مثال12۔ ثابت کرو کہ $*$ کے عمل کے تحت سبھی صحیح اعداد کا سٹ $\mathbb{Z}$ ایک گروپ بناتا ہے،جب کہ

$$a * b = a + b - 1, \qquad \forall a, b \in \mathbb{Z}$$

حل۔ دیا ہے کہ $(\mathbb{Z},*)$

G_1: ثنائی موضوع(Closure axiom): ہمیں جانچ کرنی ہے کہ $\forall a, b \in \mathbb{Z} \Rightarrow a * b \in \mathbb{Z}$ ہمیں دیا گیا ہے

$$a * b = a + b - 1, \qquad \forall a, b \in \mathbb{Z}$$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom):

$$\forall a, b, c \in \mathbb{Z} \Rightarrow a * (b * c) = (a * b) * c$$
$$a * (b + c - 1) = (a + b - 1) * c$$
$$a + b + c - 1 - 1 = a + b - 1 + c - 1$$
$$a + b + c - 2 = a + b + c - 2$$

G_3: اکائی موضوع (Identity axiom):

$$\forall a \in \mathbb{Z} \Rightarrow \exists e \in \mathbb{Z}$$
$$\text{s.t} \quad a * e = a$$
$$a + e - 1 = a$$
$$e = 1 \in \mathbb{Z}$$

اس لیے $e = 1$ اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom):

$$\forall a \in \mathbb{Z} \ \exists b \in \mathbb{Z}$$
$$\text{s.t. } a * b = 1$$
$$a + b - 1 = 1$$
$$b = 2 - a \in \mathbb{Z}$$

اس لیے $\mathbb{Z}$ میں ہر ایک عنصر کا معکوس موجود ہے۔اس سے ہم کہہ سکتے ہیں کہ $*$ کے عمل کے تحت صحیح اعداد کا سٹ معکوس موضوع کی تکمیل کرتا ہے۔

چوں کہ $\mathbb{Z}$ گروپ کے سبھی موضوعات کی تکمیل کرتا ہے،اس لیے $(\mathbb{Z},*)$ ایک گروپ کی تشکیل کرتا ہے۔

مثال13۔ ثابت کرو کہ $*$ کے عمل کے تحت سبھی غیر صفری ناطق اعداد(Non Zero Rational Numbers)کا سٹ $\mathbb{Q}_0$ ایک گروپ بناتا ہے،جب کہ $*$ اس طرح سے متعارف ہے

$$a * b = \frac{ab}{4}, \ \forall a, b \in \mathbb{Q}_0$$

حل۔ دیا ہے کہ $(\mathbb{Q}_0,*)$

G_1: ثنائی موضوع(Closure axiom): ہمیں جانچ کرنی ہے کہ $\forall a, b \in \mathbb{Q}_0 \Rightarrow a * b \in \mathbb{Q}_0$

ہمیں حاصل ہے

$$a * b = \frac{ab}{4}, \qquad \forall a, b \in \mathbb{Q}_0$$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom):

$$\forall a, b, c \in \mathbb{Q}_0 \Rightarrow a * (b * c) = (a * b) * c$$
$$a * \left(\frac{bc}{4}\right) = \left(\frac{ab}{4}\right) * c$$
$$\frac{a\left(\frac{bc}{4}\right)}{4} = \frac{\left(\frac{ab}{4}\right)c}{4}$$
$$\frac{abc}{16} = \frac{abc}{16}$$

اس لیے تلازمی موضوع کی تکمیل ہوتی ہے۔

G_3: اکائی موضوع (Identity axiom):

$$\forall a \in \mathbb{Q}_0 \Rightarrow \exists e \in \mathbb{Q}_0$$
$$\text{s.t.} \quad a * e = a$$
$$\frac{ae}{4} = a$$
$$e = 4 \in \mathbb{Q}_0$$

اس لیے $e = 4$ اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom):

$$\forall a \in \mathbb{Q}_0 \ \exists b \in \mathbb{Q}_0$$
$$\text{s.t. } a * b = 4$$
$$\frac{ab}{4} = 4$$
$$b = \frac{16}{a} \in \mathbb{Q}_0 \qquad \because a \neq 0$$

اس لیے $\mathbb{Q}_0$ میں ہر ایک عنصر کا معکوس موجود ہے۔اس سے ہم کہہ سکتے ہیں کہ $*$ کے عمل کے تحت غیر صفری ناطق اعداد کا سٹ معکوس موضوع کی تکمیل کرتا ہے۔

چوں کہ $\mathbb{Q}_0$ گروپ کے سبھی موضوعات کی تکمیل کرتا ہے،اس لیے $(\mathbb{Q}_0, *)$ ایک گروپ کی تشکیل کرتا ہے۔

مثال14۔ ثابت کرو کہ $\oplus$ کے عمل کے تحت -1 کو چھوڑ کر سبھی حقیقی اعداد کا سٹ $\mathbb{R}_{-1}$ ایک آبیلین گروپ کی تشکیل کرتا ہے، جب کہ

$$a \oplus b = a + b + ab, \qquad \forall a, b \in \mathbb{R}_{-1}$$

حل۔ دیا ہے کہ $(\mathbb{R}_{-1}, \oplus)$

G_1: ثنائی موضوع(Closure axiom): ہمیں جانچ کرنی ہے کہ $\forall a, b \in \mathbb{R}_{-1} \Rightarrow a \oplus b \in \mathbb{R}_{-1}$

ہمیں دیا گیا ہے

$$a \oplus b = a + b + ab, \qquad \forall a, b \in \mathbb{R}_{-1}$$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom):

$$\forall a, b, c \in \mathbb{R}_{-1} \Rightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$$
$$a \oplus (b + c + bc) = (a + b + ab) \oplus c$$
$$a + b + c + bc + a(b + c + bc) = a + b + ab + c + (a + b + ab)c$$
$$a + b + c + bc + ab + ac + abc = a + b + ab + c + ac + bc + abc$$

اس سے تلازمی موضوع کی تکمیل ہو جاتی ہے۔

G_3: اکائی موضوع (Identity axiom):

$$\forall a \in \mathbb{R}_{-1} \Rightarrow \exists e \in \mathbb{R}_{-1}$$
$$\text{s.t.} \quad a \oplus e = a$$
$$a + e + ae = a$$
$$e = 0 \in \mathbb{R}_{-1}$$

اس لیے $e = 0$ اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom):

$$\forall a \in \mathbb{R}_{-1} \ \exists b \in \mathbb{R}_{-1}$$
$$\text{s.t. } a \oplus b = 0$$
$$a + b + ab = 0$$
$$b = \frac{-a}{1+a} \in \mathbb{R}_{-1} \qquad \because a \neq -1$$

اس لیے $\mathbb{R}_{-1}$ میں ہر ایک عنصر کا معکوس موجود ہے۔اس سے ہم کہہ سکتے ہیں کہ $\oplus$ کے عمل کے تحت صحیح اعداد کا سٹ معکوس موضوع کی تکمیل کرتا ہے۔

G_5: تقلیبی موضوع (Commutative axiom):

$$\forall a, b \in \mathbb{R}_{-1} \Rightarrow a \oplus b = a + b + ab$$
$$= b + a + ba$$
$$= b \oplus a$$

چوں کہ $\mathbb{R}_{-1}$ آبیلین گروپ کے سبھی موضوعات کی تکمیل کرتا ہے،اس لیے $(\mathbb{R}_{-1}, \oplus)$ ایک آبیلین گروپ ہے۔

مثال15۔ ثابت کرو کہ عام ضرب کے عمل کے تحت سٹ $G = \{\cdots 2^{-3}, 2^{-2}, 2^{-1}1, 2^1, 2^2, \cdots\}$ ایک آبیلین گروپ ہے۔

حل۔ دیا گیا ہے کہ $G = \{2^n, n \in \mathbb{Z}\}$

G_1: ثنائی موضوع(Closure axiom): مان لیجیے کہ $2^p \cdot 2^q = 2^{p+q} \in G, \ \forall \ p, q \in \mathbb{Z}$

اس لیے ثنائی موضوع کی تکمیل ہوتی ہے۔

G_2: تلازمی موضوع (Associative axiom):

$$2^p, 2^q, 2^r \in G, \ \forall \ p, q, r \in \mathbb{Z} \Rightarrow 2^p \cdot (2^q \cdot 2^r) = 2^p \cdot 2^{q+r}$$
$$= 2^{p+(q+r)}$$

$$= 2^{(p+q)+r}$$
$$= 2^{p+q} \cdot 2^r$$
$$= (2^p \cdot 2^q) \cdot 2^r$$

اس سے تلازمی موضوع کی تکمیل ہو جاتی ہے۔

G_3: اکائی موضوع (Identity axiom): ہمیں دیا گیا ہے

$$2^0 \in G \Rightarrow 1 \in G$$

اس لیے $e = 1$ اکائی ہے۔

G_4: معکوس موضوع (Inverse axiom): ہمیں دیا گیا ہے

$$\forall\, 2^p \in G\ \exists 2^{-p} \in G\ \ s.t.\ 2^p \cdot 2^{-p} = 2^0 = 1$$

اس سے ہم کہہ سکتے ہیں کہ سٹ G معکوس موضوع کی تکمیل کرتا ہے۔

G_5: تقلیبی موضوع (Inverse axiom): مان لیجیے کہ

$$2^p \cdot 2^q = 2^{p+q}$$
$$= 2^{q+p}$$
$$= 2^q \cdot 2^p$$

چوں کہ دیا گیا سٹ آبیلین گروپ کے سبھی موضوعات کی تکمیل کرتا ہے، اس لیے G ایک آبیلین گروپ ہے۔

کسی گروپ کا رتبہ (Order of a Group): کسی گروپ $(G,*)$ میں موجود عناصر کی تعداد کو اس گروپ کا رتبہ کہتے ہیں۔ گروپ کے رتبے کو $o(G)$ یا $|G|$ سے ظاہر کرتے ہیں۔ جیسے

1. $G = \{1, -1, i, -i\}$ ضرب کے عمل کے تحت ایک گروپ ہے جس کا رتبہ $o(G) = 4$ ہے۔
2. $G = \{1, w, w^2\}$ ضرب کے عمل کے تحت ایک گروپ ہے جس کا رتبہ $o(G) = 3$ ہے۔
3. $\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2 \cdots\}$ جمع کے عمل کے تحت ایک گروپ ہے جس کا رتبہ $o(Z) = \infty$ ہے۔

کسی عنصر کا رتبہ (Order of an Element): فرض کرو کہ $(G,*)$ ایک گروپ ہے۔ تب $a \in G$ کے لیے اگر ایک ادنیٰ ترین مثبت نمبر m اس طرح وجود رکھتا ہو کہ $a^m = e$، تب a کا رتبہ m ہوگا۔ یعنی

$$o(a) = m$$

اگر ایسا کوئی نمبر وجود نہ رکھتا ہو تو

$$o(a) = \text{صفر}$$

1. $G = \{1, -1, i, -i\}$ ضرب کے عمل کے تحت ایک گروپ ہے۔

$$(1)^1 = 1 \quad \Rightarrow o(1) = 1$$
$$(-1)^1 = -1, (-1)^2 = 1 \Rightarrow o(-1) = 2$$
$$(i)^1 = i, \quad (i)^2 = -1, \quad (i)^3 = -i, \quad (i)^4 = 1 \Rightarrow o(i) = 4$$
$$(-i)^1 = -i, \quad (-i)^2 = -1, \quad (-i)^3 = -i, \quad (-i)^4 = 1 \Rightarrow o(-i) = 4$$

2. صفر کو چھوڑ کر حقیقی اعداد کا سٹ $\mathbb{R}_0$ ضرب کے عمل کے تحت گروپ ہے۔

1 کو چھوڑ کر کسی بھی عنصر کا رتبہ (0) صفر ہوتا ہے۔ جیسے

$$o(1) = 1$$

$$3^0 = 1 \Rightarrow o(3) = 0$$

ایسی کوئی غیر صفری قیمت نہیں ہے جس کی کوئی قوت لینے پر اکائی حاصل ہوتی ہو۔

نوٹ: $(G,+)$ کی صورت میں کسی $a \in G$ کے لیے اگر ایک ادنی ترین مثبت نمبر m اس طرح وجود رکھتا ہے کہ $ma = 0$ تب $o(a) = m$ ہوگا۔

قضیہ (Theorem) 1: اگر کسی گروپ 'G' میں کوئی عنصر **a** اس طرح وجود رکھتا ہے کہ $o(a) = n$ تب $a^m = e$ iff n/m یعنی n تقسیم کرتا ہے m کو۔

ثبوت: فرض کرو کہ n/m، اب ہمیں ثابت کرنا ہے کہ $a^m = e$

$$\because n/m \Rightarrow q \in \mathbb{Z} \quad s.t. \quad m = nq$$

تب

$$a^m = a^{nq} = (a^n)^q = e^q \qquad [\because o(a) = n \Rightarrow a^n = e]$$
$$\Rightarrow \quad a^m = e$$

یہ ثابت ہوا۔

بالعکس (<u>Conversely</u>): مان لیجیے کہ $a^m = e$، اب ہمیں تقسیمی الگورزم (Division Algorithm) کی مدد سے ثابت کرنا ہے کہ n/m

$$\Rightarrow \quad \exists q, r \in \mathbb{Z} \ s.t. \ m = nq + r, \quad 0 \le r < n$$
$$\because a^m = e$$
$$\Rightarrow \quad a^{nq+r} = e$$
$$\Rightarrow \quad a^{nq} . a^r = e$$
$$\Rightarrow \quad (a^n)^q . a^r = e$$
$$\Rightarrow \quad e^q . a^r = e$$
$$\Rightarrow \quad e . a^r = e$$
$$\Rightarrow \quad a^r = e$$

جو کہ بے معنی ہے کیوں کہ

$$o(a) = n \ \& \ r < n$$

یہ تبھی ممکن ہے جب $r = 0$

$$\Rightarrow \quad m = nq + 0$$
$$\Rightarrow \quad n/m$$

قضیہ ثابت ہوا۔

1.3 اکتسابی نتائج (Learning Outcomes)

اس اکائی میں ہم نے پڑھا:

- ایک غیر خالی سٹ اگر چار موضوعات: بند شی، تلازمی، اکائی کی موجودگی اور معکوس کی موجودگی کو پورا کرتا ہے تو یہ سٹ گروپ کہلاتا ہے۔ ان چار موضوعات کے علاوہ اگر یہ تقلیبی موضوع کی بھی تکمیل کرے تب یہ سٹ تقلیبی (یا

آبیلین) گروپ کہلایے گا۔

- کسی گروپ میں ایک عنصر ضرور ہوگا جو کہ اکائی ہوتا ہے۔ کسی گروپ میں اکائی یکتا ہوتی ہے۔
- کسی گروپ میں موجود ہر ایک عنصر کا ایک یکتا معکوس وجود رکھتا ہے۔
- ضرب کے عمل کے تحت اکائی کے جذر المکعب (Cube Roots of Unity) کا سٹ $\{1, w, w^2\}$ اور اکائی کے چہار جزر (Forth Roots of Unity) کا سٹ گروپ کی تشکیل کرتا ہے۔
- جمع کے عمل کے تحت کومپلیکس اعداد (Complex Numbers) کا سٹ ایک آبیلین گروپ ہے۔
- غیر صفری کومپلیکس اعداد کا سٹ بھی ضرب کے عمل کے تحت آبیلین گروپ کی تشکیل کرتا ہے۔
- کسی گروپ اور اسکے کسی عنصر کا رتبہ۔

1.4 کلیدی الفاظ (Key Words)

بند شی، تلازمی، معکوس، تقلیبی، آبیلین، مونائڈ، گروپائڈ، نصف گروپ، یکتا، معکوس

1.5 نمونہ امتحانی سوالات (Model Examination Questions)

1.5.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. گروپ کی تعریف کرو۔
2. گروپ کے کسی عنصر کے رتبے سے آپ کیا سمجھتے ہو۔

1.5.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. ضرب کے عمل کے تحت گروپ $G = \{1, -1, i, -i\}$ کے ہر ایک عنصر کا رتبہ حاصل کرو۔

1.5.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. ثابت کرو کہ ماترس جمع کے عمل کے تحت سبھی 2×2 حقیقی ماترس (Real Matrices) کا سٹ ایک آبیلین گروپ بناتا ہے۔
2. $\oplus$ کے عمل کے تحت -1 کو چھوڑ کر حقیقی اعداد کا سٹ ایک آبیلین گروپ بناتا ہے۔ جب کہ
$$a \oplus b = a + b + ab \quad \forall a, b \in \mathbb{R}_{-1}$$
3. دکھاؤ کہ جمع کے عمل کے تحت کومپلیکس اعداد (Complex Numbers) کا سٹ آبیلین گروپ کی تشکیل کرتا ہے۔
4. ثابت کرو کہ $\otimes_5$ کے عمل کے تحت سٹ، $\{1, 2, 3, 4\}\ mod\ 5$ گروپ بناتا ہے۔
5. $\oplus$ کے عمل کے تحت 1 کو چھوڑ کر ناطق اعداد (Rational Numbers) کا سٹ G ایک آبیلین گروپ بناتا ہے۔ جب کہ
$$a \oplus b = a + b - ab \quad \forall a, b \in G$$

1.6 مزید مطالعے کے لیے تجویز کردہ کتابیں(Suggested Books for further Readings)

1. I.N. Herstein: Topics in Algebra , Vikas Publishers
2. Surjeet Singh and Qazi Zameeruddin: Modern Algebra, Vikas Publishers
3. J.B. Fraleigh: A First course in Abstract Algebra

اکائی 2۔ تحت گروپس

(Subgroups)

اکائی کے اجزا

2.0 تمہید(Introduction)

ہم تحت سٹ کے تصور سے پہلے سے ہی واقف ہیں۔ بنیادی طور پر کوئی گروپ ایک سٹ ہی ہے جو کچھ خاص موضوعات(بند شی، تلازمی، اکائی کی موجودگی اور معکوس کی موجودگی) کی تکمیل کرتا ہے۔ ہم یہاں مطالعہ کریں گے کہ گویہ کسی گروپ کا تحت سٹ اوپر دیے گیے موضوعات کی تکمیل کرتا ہے۔ جب کسی گروپ کا تحت سٹ گروپ ہونے کی سبھی موضوعات کی تکمیل کرتا ہے تو ہم اس تحت سٹ کو تحت گروپ کہتے ہیں۔

کیوں کہ کسی گروپ کا تحت سٹ تلازمی موضوع کی تکمیل کرتا ہے اس لیے گروپ کے سبھی موضوعات کی جانچ کرنا ضروری نہیں ہے۔ کسی غیر خالی تحت سٹ کے تحت گروپ ہونے کے لیے کچھ خاص اور کافی شرائط ہوتی ہیں، جن کے ثبوت پیش کیے گیے ہیں۔ یہ بھی ثابت کیا گیا ہے کہ دو تحت گروپس کا اجماع(Union) اور تقاطع(Intersection) دوبارہ تحت گروپ ہوتا ہے۔ مثالوں کی مدد سے یہ بھی دیکھا جایے گا کہ کون سے تحت سٹس تحت گروپ کی تشکیل کرتے ہیں۔

2.1 مقاصد(Objectives)

اس اکائی کے مکمل ہونے کے بعد آپ اس قابل ہو جائیں گے کہ:

- تحت گروپ کی تعریف سمجھ سکیں۔
- کسی غیر خالی تحت سٹ کو تحت گروپ بنانے کی کامل(Sufficient) شرط حاصل کر پائیں گے۔
- کسی دیے گیے تحت سٹ کو جانچ سکیں گے کہ یہ تحت گروپ ہے یا نہیں۔
- دو تحت گروپس کا اجماع(Union) اور تقاطع(Intersection) کن شرائط کے ساتھ دوبارہ تحت گروپ ہوگا۔

2.2 تحت گروپس (Subgroups)

2.2.1 تعریفات اور مثالیں(Definitions and Examples)

تحت گروپ کی تعریف(Definition of Subgroup): کسی گروپ (G, o) کا غیر خالی تحت سٹ H ایک تحت گروپ کہلایے گا اگر (H, o) بھی گروپ کی تشکیل کرے۔ یا

اگر H کسی گروپ (G, o) کا تحت سٹ ہے اور اگر (H, o) خود ایک گروپ ہے، تب H کو G کا تحت گروپ کہتے ہیں۔ تحت گروپ کو $H \leq G$ یا $G \geq H$ کی علامت سے ظاہر کرتے ہیں۔ اس کے ساتھ ہی $H < G$ یا $G > H$ سے مراد یہ ہے کہ $H < G$ لیکن $H \neq G$

نوٹ:

1. کسی گروپ کے کسی تحت سٹ کو G کا کامپلیکس کہتے ہیں۔
2. $\{e\}$ اور G ہمیشہ G کے تحت گروپ ہوتے ہیں، ان کو غیر واجب(Non-Proper) یا معمولی(Trivial) تحت گروپس کہا جاتا ہے۔ ان کے علاوہ تحت گروپس کو واجب یا غیر معمولی(Non-Trivial) تحت گروپس کہتے ہیں۔

مثال1۔ ہم جانتے ہیں کہ $G = \{1, -1, i, -i\}$ ضرب کے عمل کے تحت ایک گروپ ہے۔ تب G کا تحت گروپ $H = \{1, -1\}$ ہے۔

مثال2۔ ہم جانتے ہیں کہ $\mathbb{Z} = \{\ldots\ldots -2, -1, 0, 1, 2 \ldots\ldots\}$ جمع کے عمل کے تحت ایک گروپ ہے۔ تب صفر کے ساتھ جفت نمبر (Even Number) کا سٹ $E = \{\ldots\ldots -4, -2, 0, 2, 4, 6 \ldots\ldots\}$ گروپ $\mathbb{Z}$ کا تحت گروپ ہوگا۔

مثال3۔ صفر کے ساتھ طاق نمبر کا سٹ $S = \{\ldots\ldots -3, -1, 0, 1, 3 \ldots\ldots\}$ جمع کے عمل کے تحت $\mathbb{Z}$ کا تحت گروپ نہیں ہے۔ کیوں کہ دو طاق نمبرات کا جمع ایک جفت نمبر ہوتا ہے نہ کہ طاق نمبر، یعنی بند شی موضوع کی تکمیل نہیں ہوتی۔

مثال4۔ $(\mathbb{Z}, +) < (\mathbb{R}, +)$

مثال5۔ ضرب کے عمل کے تحت سٹ $(\mathbb{Q}^+, .)$ جمع کے عمل کے تحت سٹ $(\mathbb{R}, +)$ کا تحت گروپ نہیں ہے۔

مثال6۔ $\mathbb{C}$ میں اکائی کے n ویں جذر (n^{th} Roots of Unity) کا سٹ U_n ضرب کے عمل کے تحت غیر صفری کامپلیکس نمبرات کا گروپ $\mathbb{C}^*$ کا ایک تحت گروپ بناتا ہے۔

عام خطی گروپ (General Linear Group):

ضرب کے عمل کے تحت سبھی **2 x 2** کے غیر نادر حقیقی ماترس (Non Singular Real Matrices) کا سٹ ایک گروپ بناتا ہے۔ اس گروپ کو رتبہ 2 کا حقیقی نمبرات کے سٹ $\mathbb{R}$ پر عام خطی گروپ کہتے ہیں۔ اس کو درجہ ذیل سے ظاہر کرتے ہیں

$$GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

مخصوص خطی گروپ (Special Linear Group): ضرب کے عمل کے تحت سبھی **2 x 2** کے غیر نادر حقیقی ماترس (Non Singular Real Matrices) کا سٹ جن کے لیے مقطعہ (Determinant) یعنی $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1$ ہو، ایک گروپ بناتا ہے۔ اس گروپ کو رتبہ 2 کا حقیقی نمبرات کے سٹ $\mathbb{R}$ پر مخصوص خطی گروپ کہتے ہیں۔ اس کو درجہ ذیل سے ظاہر کرتے ہیں

$$SL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

نوٹ: GL(2, R) کا ایک تحت گروپ SL(2, R) ہوگا۔

قضیہ (Theorem): کسی گروپ G کا کوئی غیر خالی کامپلیکس H اس گروپ کا تحت گروپ ہوتا ہے اگر اور صرف اگر

(i) $\forall a, b \in H \Rightarrow ab \in H$ (ii) $\forall a \in H \Rightarrow a^{-1} \in H$

ثبوت: فرض کرو کہ G کا ایک تحت گروپ H ہے۔ تب بند شی موضوع سے $\forall a, b \in H \Rightarrow ab \in H$ اور معکوس کے موضوع سے $\forall a \in H \Rightarrow a^{-1} \in H$

اس سے قضیہ ثابت ہو جاتا ہے۔

بالعکس (Conversely): فرض کرو کہ (i) $\forall a, b \in H \Rightarrow ab \in H$ (ii) $\forall a \in H \Rightarrow a^{-1} \in H$

تب ہمیں ثابت کرنا ہے کہ H کا G ایک تحت گروپ ہے۔

کیوں کہ ہمیں جو دیا گیا وہ بند شی موضوع اور معکوس کے وجود کا موضوع ہیں اور کیوں کہ G کا H ایک تحت سٹ ہے اس لیے تلازمی کا موضوع آسانی سے تکمیل کو پہنچتا ہے۔ تب اکائی کے موضوع کے لیے (ii) میں ہمیں دیا گیا ہے

$$\forall a \in H \Rightarrow a^{-1} \in H$$

تب (i) سے

$$aa^{-1} \in H \Rightarrow e \in H$$

یعنی اکائی H میں موجود ہے۔

کیوں کہ گروپ کے سبھی موضوعات کی تکمیل H کے لیے ہو جاتی ہے۔ اس لیے H کا G ایک تحت گروپ ہے۔

اس لیے قضیہ ثابت ہوتا ہے۔

مثال 1۔ ثابت کرو کہ $GL(2,\mathbb{R})$ کا $SL(2,\mathbb{R})$ ایک تحت گروپ ہوگا۔

ثبوت: ہم جانتے ہیں کہ

$$GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

اور

$$SL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in \mathbb{R}, ad - bc = 1 \right\}$$

تب یہ ثابت کرنے کے لیے کہ $SL(2,\mathbb{R})$ کا $GL(2,\mathbb{R})$ ایک تحت گروپ ہوگا یہی کافی ہے کہ ہم ثابت کر دیں کہ ضرب کے عمل کے تحت بند شی اور معکوس موضوع کی تکمیل ہوتی ہے۔

فرض کرو کہ $A, B \in SL(2,\mathbb{R})$ جہاں

$$A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, a_1 d_1 - b_1 c_1 = 1$$

اور

$$B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}, a_2 d_2 - b_2 c_2 = 1$$

اب

$$\text{A.B} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} . \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{bmatrix}$$

تب مقطعہ (Determinant) ہوگا

$$\begin{aligned} \left(a_1 a_2 + b_1 c_2\right)\left(c_1 b_2 + d_1 d_2\right) - \left(c_1 a_2 + d_1 c_2\right)\left(a_1 b_2 + b_1 d_2\right) &= a_1 a_2 c_1 b_2 + a_1 a_2 d_1 d_2 + b_1 c_2 c_1 b_2 \\ &+ b_1 c_2 d_1 d_2 - c_1 a_2 a_1 b_2 - c_1 a_2 b_1 d_2 - d_1 c_2 a_1 b_2 - d_1 c_2 b_1 d_2 \\ &= a_1 a_2 d_1 d_2 + b_1 c_2 c_1 b_2 - c_1 a_2 b_1 d_2 - d_1 c_2 a_1 b_2 \\ &= a_2 d_2 (a_1 d_1 - b_1 c_1) - c_2 b_2 (a_1 d_1 - c_1 b_1) \\ &= a_2 d_2 \cdot 1 - c_2 b_2 \cdot 1 \\ &= a_2 d_2 - c_2 b_2 \\ &= 1 \quad \Rightarrow A \cdot B \in SL(2,\mathbb{R}) \quad \ldots\ldots\ldots\ldots (1) \end{aligned}$$

اور

$$A^{-1} = \frac{1}{a_1 d_1 - b_1 c_1}\begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix} = \frac{1}{1}\begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix} = \begin{bmatrix} d_1 & -b_1 \\ -c_1 & a_1 \end{bmatrix}$$

اور

$$\det A^{-1} = a_1 d_1 - (-c_1)(-b_1) = a_1 d_1 - b_1 c_1 = 1$$

$$\Rightarrow \quad A^{-1} \in SL(2,\mathbb{R}) \quad \ldots\ldots\ldots\ldots(2)$$

مساوات(1) اور(2) سے ہمیں حاصل ہوتا ہے کہ $GL(2,\mathbb{R})$ کا $SL(2,\mathbb{R})$ ایک تحت گروپ ہے۔

قضیہ ثابت ہوا۔

قضیہ(Theorem): کسی گروپ G کے غیر خالی تحت سٹ H کے اس گروپ کا تحت گروپ ہونے کے لیے ضروری (Necessary)اور کافی(Sufficient)شرائط یہ ہے کہ $\forall a, b \in H \Rightarrow ab^{-1} \in H$

ثبوت: ضروری شرط(Necessary Condition)

فرض کرو کہ GکاHایک تحت گروپ ہے۔اس لیے معکوس کے وجود کے موضوع سے

$$b \in H \Rightarrow b^{-1} \in H$$

بند شی موضوع سے

$$\forall a, b^{-1} \in H \Rightarrow ab^{-1} \in H$$

یہ ثابت ہوا۔

کافی شرط(Sufficient Condition)

فرض کرو کہ

$$\forall a, b^{-1} \in H \Rightarrow ab^{-1} \in H$$

تب ہمیں ثابت کرنا ہے کہ G کا H ایک تحت گروپ ہے۔ $a = b$ لینے پر

$$aa^{-1} \in H \Rightarrow e \in H$$

تب اکائی وجود رکھتی ہے۔اب $a = e$ لینے پر

$$eb^{-1} \in H \Rightarrow b^{-1} \in H$$
$$i.e. \forall b \in H \Longrightarrow b^{-1} \in \mathrm{H}$$

اس لیے معکوس وجود رکھتا ہے۔تب

$$a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H$$
$$\Rightarrow ab \in H$$

اس سے بند شی موضوع کی تکمیل ہو جاتی ہے۔

تلازمی موضوع کی تکمیل آسانی سے ہوتی ہے کیوں کہ G کا H ایک تحت سٹ ہے۔

کیوں کہ گروپ کے سبھی موضوعات کی تکمیل H کے لیے ہو جاتی ہے۔اس لیے GکاHایک تحت گروپ ہے۔

قضیہ(Theorem): کسی متناہی گروپ G کا غیر خالی کامپلیکس تحت سٹ H گروپ Gکاایک تحت گروپ ہوتا ہے اگر اور صرف اگر $\forall a, b \in H \Rightarrow ab \in H$

ثبوت: فرض کرو کہ Hکاایک تحت گروپ ہے۔تب بند شی کے موضوع سے

$$\forall a, b \in H \Rightarrow ab \in H$$

یہ ثابت ہوا۔

بالعکس(Conversely): فرض کرو کہ $\forall a, b \in H \Rightarrow ab \in H$ تب ہمیں ثابت کرنا ہے کہ Gکاایک تحت گروپ ہے۔

ہم جانتے ہیں کہ دی گئی شرط بند شی موضوع کی تکمیل کرتی ہے۔اور کیوں کہ Gکاایک تحت گروپ ہے اس لیے تلازمی موضوع کی تکمیل باآسانی ہو جاتی ہے۔تب $a = b$ لینے پر ہمیں حاصل ہو گا

$$a, a \in H \Rightarrow a^2 \in H$$

اور اسی طرح

$$aa^2 = a^3 \in H$$

اوراسی طرح $a^n \in H$

اوراسی طرح مسلسل حاصل کیاجاسکتاہے $aa^n \in H$

اب کیوں کہ G ایک متناہی گروپ ہے۔اس سے ہم کہہ سکتے ہیں کہ H بھی متناہی گروپ ہو گا تب عناصر میں مکررات ہوں گے۔

اب پھر سے فرض کرو کہ

$$\begin{aligned} a^r &= a^s, \quad r > s \\ \Rightarrow \quad a^r a^{-s} &= a^s a^{-s} \\ \Rightarrow \quad a^{r-s} &= a^0 = e \in H \end{aligned}$$

اب کیوں کہ $r-s$ایک صحیح عدد(Integer)ہے۔اس لیے $r - s \geq 1$ تب $r - s - 1 \geq 0$ اس لیے

$$a^{r-s-1} \in H \quad s.t. \ a.a^{r-s-1} = a^{r-s} = e$$

اس لیے معکوس موضوع کی تکمیل ہوتی ہے۔

کیوں کہ گروپ کے سبھی موضوعات کی تکمیل H کے لیے ہو جاتی ہے۔اس لیے Hکاایک تحت گروپ ہے۔

اس لیے یہ ثابت ہوا۔

قضیہ(Theorem):کسی گروپ Gکاایک متناہی غیر خالی کامپلیکس H گروپ G کا تحت گروپ ہوتاہے اگراور صرف اگر

$$\forall a, b \in H \Rightarrow ab \in H$$

ثبوت: فرض کرو کہ H ایک G کا متناہی تحت گروپ ہے۔تب بند شی کے موضوع سے

$$\forall a, b \in H \Rightarrow ab \in H$$

اس لیے یہ ثابت ہوا۔

بالعکس(Conversely): فرض کرو کہ $\forall a, b \in H \Rightarrow ab \in H$ تب ہمیں ثابت کرنا ہے کہ H گروپ G کا متناہی تحت گروپ ہے۔ ہم جانتے ہیں کہ دی گئی شرط بند شی موضوع کی تکمیل کرتی ہے۔اور کیوں کہ Gکاایک تحت گروپ ہے اس لیے تلازمی موضوع کی تکمیل باآسانی ہو جاتی ہے۔تب $a = b$ لینے پر ہمیں حاصل ہو گا

$$a, a \in H \Rightarrow a^2 \in H$$

اور

$$aa^2 = a^3 \in H$$

اوراسی طرح $a^n \in H$

اوراسی طرح مسلسل حاصل کیاجاسکتاہے $aa^n \in H$

اب کیوں کہ H متناہی سٹ ہے تب عناصر میں مکررات ہوں گے۔اب پھر سے فرض کروکہ

$$a^r = a^s, \quad r > s$$
$$\Rightarrow \quad a^r a^{-s} = a^s a^{-s}$$
$$\Rightarrow \quad a^{r-s} = a^0 = e \in H$$

اب کیوں کہ $r-s$ایک صحیح عدد(Integer)ہے۔اس لیے$r - s \geq 1$ تب $r - s - 1 \geq 0$ اس لیے

$$a^{r-s-1} \in H \quad s.t. \; a.a^{r-s-1} = a^{r-s} = e$$

اس لیے معکوس موضوع کی تکمیل ہوتی ہے۔

کیوں کہ گروپ کے سبھی موضوعات کی تکمیل H کے لیے ہوجاتی ہے۔اس لیےG کا Hایک تحت گروپ ہے۔

یہ قضیہ ثابت ہوا۔

قضیہ(Theorem): کسی گروپ G کے غیر خالی تحت سٹ H کے تحت گروپ ہونے کے لیے کافی(Sufficient)اور ضروری(Necessary)شرط یہ ہے کہ $HH^{-1} = H$

ثبوت: ضروری شرط:

فرض کروکہ GکاHایک تحت گروپ ہے۔اس لیے

$$HH^{-1} \subset H \qquad .....(1)$$

فرض کروکہ H میں ایک اکائی e ہے۔مان لوکہ $h \in H$ تب

$$h = he = he^{-1} \in HH^{-1}$$

اس لیے

$$H \subset HH^{-1} \qquad .....(2)$$

مساوات(1)اور(2)سے ہمیں حاصل ہوتاہے

$$HH^{-1} = H$$

کافی شرط:

فرض کروکہ

$$HH^{-1} = H$$

تب

$$HH^{-1} \subset H$$

اس لیےGکاHایک تحت گروپ ہے۔

نوٹ: اگرHایک تحت گروپ ہے تب $H^{-1} = H$۔

قضیہ(Theorem):اگر کسی گروپ G کے دو تحت گروپس Hاور K ہوں تب HK تحت گروپ ہوتا ہے اگر اور صرف اگر

$$HK = KH$$

ثبوت: فرض کرو کہ $HK = KH$ تب ہمیں ثابت کرنا ہے کہ HK تحت گروپ ہوگا۔

تب

$$\begin{aligned}(HK)\,(HK)^{-1} &= HK(K^{-1}H^{-1}) \\ &= H(KK^{-1})H^{-1}\end{aligned}$$

کیوں کہ K ایک تحت گروپ ہے۔اس لیے $KK^{-1} = K$

$$\begin{aligned}&= HKH^{-1} \\ &= KHH^{-1} \qquad \because\ HK = KH\end{aligned}$$

کیوں کہ Hایک تحت گروپ ہے۔اس لیے $HH^{-1} = H$

$$\begin{aligned}&= KH \\ &= HK\end{aligned}$$

لہٰذا HK تحت گروپ ہوا۔

بالعکس(Conversely): فرض کرو کہ HK کسی گروپ کا تحت گروپ ہے۔تب ہمیں ثابت کرنا ہے کہ $HK = KH$

ہمیں حاصل ہے

$$(HK)^{-1} = HK$$

$$\Rightarrow \quad K^{-1}H^{-1} = HK$$

کیوں کہ Hاور K دو تحت گروپس ہیں

$$\Rightarrow \quad KH = HK$$

اب قضیہ ثابت ہوا۔

قضیہ(Theorem):اگر کسی گروپ G کے دو تحت گروپس H_1اور H_2 ہوں تب $H_1 \cap H_2$ بھی G کا تحت گروپ ہوتا ہے۔

ثبوت: چوں کہ

$$H_1 \cap H_2 \neq \varphi \quad \because\ e \in H_1 \cap H_2$$

فرض کرو کہ

$$a, b \in H_1 \cap H_2$$

کیوں کہ H_1ایک تحت گروپ ہے۔ اس لیے $ab^{-1} \in H_1 \Leftarrow \forall\ a, b \in H_1$

اور H_2 کے تحت گروپ ہونے کی وجہ سے $ab^{-1} \in H_2, \Leftarrow \forall\ a, b \in H_2$

$$\Rightarrow \quad ab^{-1} \in H_1 \cap H_2$$

اس لیے G کا $H_1 \cap H_2$ تحت گروپ ہے۔

نوٹ:اگر سبھی H_i کسی گروپ G کے تحت گروپس ہوں تو $H_1 \cap H_2 \cap H_3 \cdots \cap H_n = \bigcap_{i=1}^{n} H_i$ بھی G کا ایک تحت گروپ ہوگا۔

قضیہ(Theorem): کسی گروپ G کے دو تحت گروپس کا اجماع(Union) بھی G کا تحت گروپ ہوگا اگر اور صرف اگر ایک تحت گروپ دوسرے تحت گروپ میں موجود ہو۔

ثبوت: فرض کرو کہ کسی گروپ $(G,\cdot)$ کے دو تحت گروپس H_1 اور H_2 ہیں۔ اور فرض کرو کہ $H_1 \subset H_2$ تب

$$H_1 \cup H_2 = H_2$$

کیوں کہ H_2 ایک تحت گروپ ہے۔اس لیے $H_1 \cup H_2$ ایک تحت گروپ ہوگا۔ یہ ثابت ہوا۔

بالعکس(Conversely): فرض کرو کہ $H_1 \cup H_2$ ایک تحت گروپ ہے۔تب ہمیں ثابت کرنا ہے کہ گویا $H_1 \subset H_2$ یا $H_2 \subset H_1$

فرض کرو کہ اگر ممکن ہے $H_1 \not\subset H_2$ اور $H_2 \not\subset H_1$ تب

$$\exists\ a \in H_1\ \&\ a \notin H_2 \qquad .....(1)$$

$$\exists\ b \in H_2\ \&\ b \notin H_1 \qquad .....(2)$$

لیکن

$$a, b \in H_1 \cup H_2$$

کیوں کہ $H_1 \cup H_2$ ایک تحت گروپ ہے۔اس لیے بند شی موضوع کی مدد سے

$$ab \in H_1 \cup H_2$$

تب

$$ab \in H_1 \text{ یا } ab \in H_2 \text{ یا } ab \in H_1 \cap H_2$$

I. **جب** $ab \in H_1$:

تب

$$a \in H_1 \Rightarrow a^{-1} \in H_1$$
$$\Rightarrow \quad a^{-1}(ab) \in H_1$$
$$\Rightarrow \quad (a^{-1}a)b = eb = b \in H_1$$

جو کہ مساوات(2) سے تضاد کرتا ہے۔اس لیے $ab \notin H_1$

II. **جب** $ab \in H_2$:

تب

$$b \in H_2 \Rightarrow b^{-1} \in H_2$$
$$\Rightarrow \quad (ab)b^{-1} \in H_2$$
$$\Rightarrow \quad a(bb^{-1}) = ae = a \in H_2$$

جو کہ مساوات(1) سے تضاد کرتا ہے۔اس لیے $ab \notin H_2$

تب ظاہر بات ہے کہ

$$ab \notin H_1 \cap H_2 \Rightarrow ab \notin H_1 \cup H_2$$

جو کہ متضاد(*Contradiction*) ہے۔اس لیے ہمارا یہ مان لینا کہ $H_1 \not\subset H_2$ اور $H_2 \not\subset H_1$ غلط ہے۔اس لیے

$$H_2 \subset H_1 \quad \text{یا} \quad H_1 \subset H_2$$

اس طرح قضیہ ثابت ہوا۔

مثال1۔ ثابت کرو کہ جمع کے عمل کے تحت 3 کے سبھی اضعاف(Multiples)کا سٹ صحیح اعداد(Integers)کے گروپ کا تحت گروپ ہوتا ہے۔

ثبوت۔ فرض کرو کہ $3\mathbb{Z} = \{3n/\ n \in \mathbb{Z}\}$ تب

$$3\mathbb{Z} \neq \varphi \text{ اور } 3\mathbb{Z} \subset \mathbb{Z}$$

فرض کرو کہ $\boldsymbol{3m, 3n \in 3\mathbb{Z} \Rightarrow m, n \in \mathbb{Z}}$، تب

$$3m - 3n = 3(m - n) \in 3\mathbb{Z}$$

اس سے تحت گروپ کی شرط مطمئن ہو جاتی ہے۔اس لیے ہم کہہ سکتے ہیں $(3\mathbb{Z}, +)$ایک تحت گروپ ہے۔

اس طرح یہ قضیہ ثابت ہوا۔

مثال2۔ دکھلاؤ کہ کسی آبیلین گروپ G کے سبھی عناصر a کا سٹ جو $a^2 = e$ کو مطمئن کرے، تحت گروپ کی تشکیل کرتا ہے۔

ثبوت۔ فرض کرو کہ Hایک سٹ ہے جو آبیلین گروپ G کے سبھی عناصر a سے بنا ہے اور جو $a^2 = e$ کو مطمئن کرتا ہے۔یعنی

$$H = \{a \in G/\ a^2 = e\}\ and\ H \subset G$$

کیوں کہ e گروپ G میں ایک اکائی ہے اس طرح سے کہ $a^2 = e$

اس لیے $e \in H$ اور اس لیے H ایک غیر خالی سٹ ہے۔اب

$$a, b \in H \Rightarrow a, b \in G \Rightarrow ab \in G$$

اس کے علاوہ

$$a \in H \Rightarrow a^2 = e \quad \text{اور} \quad b \in H \Rightarrow b^2 = e$$

کیوں کہ ایک آبیلین گروپ ہے،اس لیے

$$\begin{aligned} (ab)^2 &= a^2\, b^2 \\ &= ee = \mathrm{e} \\ \Rightarrow \qquad ab &\in H \end{aligned}$$

اس لیے H بند شی(Closed)ہے۔لہٰذا H تحت گروپ ہے۔

مثال3۔ اگر $G = \{1, -1,\ i, -i\}$ ضرب کے عمل کے تحت ایک گروپ ہو تب اس کے سبھی تحت گروپس لکھو۔

حل۔ فرض کرو کہ $G = \{1, -1,\ i, -i\}$ ضرب کے عمل کے تحت گروپ ہے۔ یہاں 1 اکائی ہے۔ $\{1\}$ اور G خود G کے غیر واجب تحت گروپ ہیں۔اور مان لو کہ $H = \{1, -1\}$ تب کیلی کی ٹیبل درجہ ذیل ہو گی

.	1	-1
1	1	-1
-1	-1	1

یہ دیکھا جاسکتا ہے کہ H کے لیے گروپ کے سبھی موضوعات کی تکمیل ہو جاتی ہے۔اس لیے Hایک تحت گروپ ہے Gکا۔ان کے علاوہ اور کوئی تحت گروپ ممکن نہیں ہے۔

اس لیے G کے تحت گروپ $\{1\}$،$\{1,-1\}$ اور$\{1,-1,\ i,-i\}$ ہیں۔

مثال4۔ اگر G ایک گروپ ہو اور $a\in G$, $N(a)=\{x\in G/ax=xa\}$ تب ثابت کرو کہ G کا $N(a)$ تحت گروپ ہے۔

ثبوت۔ دیا گیا ہے کہ Gایک گروپ ہے اور $a\in G$, $N(a)=\{x\in G/ax=xa\}$ اس لیے

$$N(a)\subset G$$

اور مان لو کہ $x_1,x_2\in N(a)$ تب $ax_1=x_1a$ اور $ax_2=x_2a$ اور $x_2^{-1}\in G$

G میں

$$ax_2=x_2a\Rightarrow x_2^{-1}(ax_2)x_2^{-1}=x_2^{-1}(x_2a)x_2^{-1}$$
$$\Rightarrow\quad x_2^{-1}a=a\,x_2^{-1}\Rightarrow x_2^{-1}\in N(a)$$

پھر G میں

$$\begin{aligned}a(x_1x_2^{-1})&=(ax_1)x_2^{-1}=(x_1a)x_2^{-1}\\&=x_1(ax_2^{-1})=x_1(x_2^{-1}a)\\&=(x_1x_2^{-1})a\ \Rightarrow x_1x_2^{-1}\in N(a)\end{aligned}$$

اس لیے

$$x_1,x_2\in N(a)\Rightarrow x_1x_2^{-1}\in N(a)$$

اس لیے $N(a)$ایک Gکا تحت گروپ ہے۔

مثال5۔ ثابت کرو کہ $\{\mathbb{Q},+\}$ کسی گروپ $\{\mathbb{R},+\}$کا ایک تحت گروپ ہوگا اور $\{\mathbb{R}-\mathbb{Q},+\}$ گروپ $\mathbb{R}$ کا ایک تحت گروپ ہے۔

ثبوت۔ ہم جانتے ہیں کہ $\mathbb{Q}\subset\mathbb{R}$ اور $\{\mathbb{R},+\}$ ایک گروپ ہے۔تب $a,b\in\mathbb{Q}\Rightarrow a,b\in R$, اس کے علاوہ b کا معکوس $-b$ ہے۔اب $-b\in\mathbb{Q}$ اور $a+(-b)=a-b\in\mathbb{Q}$

اس لیے $\{\mathbb{Q},+\}$ گروپ $\{\mathbb{R},+\}$کا ایک تحت گروپ ہے۔

پھر سے $\mathbb{R}-\mathbb{Q}$ غیر ناطق اعداد کا سٹ ہے اور $\mathbb{R}$ کا تحت سٹ ہے۔ ہم جانتے ہیں کہ گروپ $\{\mathbb{R},+\}$ کی اکائی 0 ہوتی ہے۔ لیکن $0\notin(\mathbb{R}-\mathbb{Q})$ اور اس لیے $\mathbb{R}-\mathbb{Q}$ جمع کے عمل کے تحت $\mathbb{R}$ کا تحت گروپ نہیں ہے۔

مثال6۔ اگر G ضرب کے عمل کے تحت ایک گروپ ہے اور $a\in G$ تب ثابت کرو کہ $H=\{a^n/n\in\mathbb{Z}\}$ گروپ G کا ایک تحت گروپ ہے۔

حل۔ دیا گیا ہے کہ G ضرب کے عمل کے تحت ایک گروپ ہے اور $a\in G$ اس کے علاوہ $H=\{a^n/n\in\mathbb{Z}\}$

فرض کرو کہ $a^p,a^q\in H$ جہاں $p,q\in\mathbb{Z}$

تب $p,q \in \mathbb{Z}$ کے لیے $a^p \cdot a^q = a^{p+q} \in H$ اس لیے بند شی موضوع کی تکمیل ہوتی ہے۔حالاں کہ تلازمی موضوع کی تکمیل خد بہ خد ہو جاتی ہے کیوں کہ H کے سبھی عناصر گروپ G کے عناصر ہیں۔

$$a^0 = e \in H \; s.t. \; a^m . a^0 = a^{m+0} = a^m$$

اب ہم کہہ سکتے ہیں کہ H کے لیے a^0 ایک اکائی ہے۔اس کے علاوہ چوں کہ $-m \in \mathbb{Z}$ اور سبھی $a^m \in H$ کے لیے ہمارے پاس $a^{-m} \in H$, اس طرح سے کہ

$$a^m . a^{-m} = a^0 = e$$
$$\Rightarrow \quad (a^m)^{-1} = a^{-m}$$

یعنی a^m کا معکوس a^{-m} ہے۔اس سے معکوس کے موضوع کی تکمیل ہو جاتی ہے۔

کیوں کہ گروپ کی سبھی موضوعات کی تکمیل ہوتی ہے۔اس لیے H، گروپ G کا ایک تحت گروپ ہے۔

مثال 7۔ فرض کرو کہ G ایک گروپ ہے اور H, K اس کے دو تحت گروپس ہیں۔تب ثابت کرو کہ $HK = \{ hk / \; h \in H, k \in K \}$، گروپ G کا ایک تحت گروپ ہے۔

ثبوت۔ دیا گیا ہے کہ G ایک گروپ ہے اور H, K اس کے دو تحت گروپس ہیں۔اور تب ہمیں ثابت کرنا ہے کہ HK گروپ G کا ایک تحت گروپ ہے۔ اب فرض کرو کہ $a, b \in HK$، اور $a = h_1 k_1$ ، جہاں $h_1 \in H, k_1 \in K$ اور $b = h_2 k_2$ ، جہاں $h_2 \in H, k_2 \in K$، تب

$$\begin{aligned} ab &= (h_1 k_1)(h_2 k_2) \\ &= h_1 h_2 k_1 k_2 \\ &= hk \in HK \end{aligned}$$

جہاں $h_1 h_2 = h$ اور $k_1 k_2 = k$، اس لیے

$$ab \in HK$$

اس لیے بند شی موضوع کی تکمیل ہوتی ہے۔

چوں کہ H اور K کے سبھی عناصر (*Elements*) گروپ G کے بھی عناصر ہیں۔اس لیے یہ تلازمی موضوع کی تکمیل کرتے ہیں۔

اس لیے HK بھی تلازمی موضوع کی تکمیل کریگا۔

فرض کرو کہ گروپ G میں اکائی e ہے، تب یہ H اور K کے لیے بھی اکائی ہو گی۔اب

$$ee = e \in HK$$

اور آخر میں کسی عنصر $ab \in HK$ کے معکوس کی جانچ کرنے کے لیے ہم دیکھتے ہیں کہ

$$a = h_1 k_1 \Rightarrow a^{-1} = (h_1 k_1)^{-1} = {k_1}^{-1} {h_1}^{-1}$$

اور

$$b = h_2 k_2 \Rightarrow b^{-1} = (h_2 k_2)^{-1} = {k_2}^{-1} {h_2}^{-1}$$

تب

$$\begin{aligned} (ab)^{-1} = a^{-1} b^{-1} &= {k_1}^{-1} {h_1}^{-1} {k_2}^{-1} {h_2}^{-1} \\ &= {h_1}^{-1} {k_1}^{-1} {h_2}^{-1} {k_2}^{-1} \\ &= {h_1}^{-1} {h_2}^{-1} {k_1}^{-1} {k_2}^{-1} \in HK \end{aligned}$$

اس لیے معکوس کے موضوع کی تکمیل ہو جاتی ہے۔

کیوں کہ گروپ کے سبھی موضوعات کی تکمیل HK کے لیے ہوتی ہے۔اس لیے HK، گروپ G کا ایک تحت گروپ ہے۔اس لیے یہ ثابت ہوتا ہے۔

2.3 اکتسابی نتائج(Learning Outcomes)

اس اکائی میں ہم نے پڑھا کہ ایک تحت گروپ کیا ہوتا ہے۔کسی غیر خالی تحت سٹ کے تحت گروپ ہونے کے لیے ضروری اور کافی شرط بند شی اور معکوس موضوع ہوتی ہے۔کسی غیر خالی متناہی تحت سٹ کے تحت گروپ ہونے کے لیے بند شی موضوع کافی شرط ہے۔ہم نے دیکھا کہ دو تحت گروپس کا تقاطع(Intersection) ایک تحت گروپ بناتا ہے اور ان کا اجماع(Union) ایک تحت گروپ بناتا ہے اگر اور صرف اگر ایک تحت گروپ دوسرے میں ضم ہو۔اس کے ساتھ ہی ہم نے حاصل کیا کہ دو تحت گروپس کا حاصل ضرب خود ایک تحت گروپ ہوتا ہے۔کچھ مثالوں کی مدد سے یہ سمجھا کہ تحت سٹ ایک تحت گروپ ہوتا ہے یا نہیں۔

2.4 کلیدی الفاظ(Key Words)

تحت گروپ، تقاطع، اجماع

2.5 نمونہ امتحانی سوالات(Model Examination Questions)

2.5.1 معروضی جوابات کے حامل سوالات(Objective Answer Type Questions)

1. تحت گروپ کی تعریف کرو۔
2. واجبی تحت گروپ کی تعریف کرو۔

2.5.2 مختصر جوابات کے حامل سوالات(Short Answer Type Questions)

1. اگر G ضرب کے عمل کے تحت ایک گروپ ہو، تب ثابت کرو کہ گروپ G کا $H = \{a^n / n \in \mathbb{Z}\}$ ایک تحت گروپ ہے۔
2. اگر G ایک گروپ ہو اور $N(a) = \{x \in G / ax = xa\}, \forall a \in G$، تب ثابت کرو کہ گروپ G کا $N(a)$ ایک تحت گروپ ہے۔
3. اگر ضرب کے عمل کے تحت $G = \{1, -1, i, -i\}$ ایک گروپ ہو تب اس گروپ کے سبھی تحت گروپس لکھو۔
4. جمع کے عمل کے تحت 3 کے سبھی ضریب(Multiples) کا سٹ صحیح اعداد کے گروپ کا تحت گروپ ہوتا ہے۔

2.5.3 طویل جوابات کے حامل سوالات(Long Answer Type Questions)

1. تحت گروپ کی تعریف کرو۔اگر H_1, K_1 کسی گروپ G کے دو تحت گروپ ہیں۔ثابت کرو کہ $H_1 \cap K_1$ بھی گروپ G کا تحت گروپ ہوتا ہے۔

2. اگر H, K کسی گروپ G کے دو تحت گروپ ہیں۔ثابت کرو کہ HK بھی گروپ G کا تحت گروپ ہوگا اگر اور صرف اگر $HK = KH$

3. کسی متناہی(Finite) گروپ G کا غیر خالی ملطف(Complex)سٹ H اس گروپ کا ایک تحت گروپ ہوگا اگر اور صرف اگر

$$\forall a, b \in H \Rightarrow ab \in H$$

4. دکھاؤ کہ کسی گروپ کے دو تحت گروپس کا اجماع(Union)ایک تحت گروپ ہوتا ہے اگر اور صرف اگر ایک تحت گروپ دوسرے تحت گروپ کو پوری طرح سمالیتا ہے۔

1.6 مزید مطالعے کے لیے تجویز کردہ کتابیں(Suggested Books for further Readings)

1. I.N. Herstein: Topics in Algebra , Vikas Publishers
2. Surjeet Singh and Qazi Zameeruddin: Modern Algebra, Vikas Publishers
3. J.B. Fraleigh: A First course in Abstract Algebra

اکائی 3۔ ہم سٹس، لگرانج کا قضیہ اور اس کے نتائج

(Cosets, Lagrange's Theorem and its Consequences)

اکائی کے اجزا

3.0 تمہید(Introduction)

گروپس اور تحت گروپس کے بارے میں معلومات حاصل ہونے کے بعد ہم سٹس(Cosets)کا تعارف پیش کیا جاتا ہے۔اگر کوئی $(G,+)$ گروپ ہے اور $(H,+)$ اس کا تحت گروپ ہو۔تب اگر $a \in G$ لیا جایے اور $a+H$ اور $H+a$ بناتے جائیں جو کہ H کے سبھی عناصر میں a جمع کیا جاتا ہے بائیں سے یا دائیں سے یہ دونوں بائیں ہم سٹس اور دائیں ہم سٹس کہلاتے ہیں۔ اسی طرح $(G,\cdot)$ گروپ اور $(H,\cdot)$ تحت گروپ ہو تب aH اور Ha گروپ G کے ہم سٹس ہیں جو بالترتیب بائیں اور دائیں ہم سٹس ہیں۔

دو ہم سٹس کے درمیان میں یہ رشتہ ہوتا ہے کہ یا تو غیر مشترک ہوتے ہیں یا بالکل مماثل ہوتے ہیں۔دائیں اور بائیں ہم سٹس کے درمیان ایک ایک بر مطابقت(One One and Onto Correspondence)بنایا جا سکتا ہے۔ایک تحت گروپ کا رتبہ اپنے متناہی گروپ کے رتبے کو ہمیشہ تقسیم کرتا ہے اور لگرانج کا قضیہ کہلاتا ہے۔اس سے متعلق چند نتائج اخذ کیے جائیں گے۔

3.1 مقاصد(Objectives)

اس اکائی کی تکمیل پر آپ اس قابل ہو جائیں گے کہ ہم سٹس کیا ہیں، دائیں اور بائیں ہم سٹس کب علٰحدہ اور کب مساوی ہوتے ہیں معادلی رشتہ کیا ہے۔ لگرانج کے قضیہ کو بیان کر سکیں گے اور اس کو ثابت کر سکیں گے۔ ہم سٹس اور لگرانج کے قضیہ کے متعلق قضیے اور مختلف نتائج کو اخذ کر سکیں گے۔

3.2 تعریفات اور مثالیں(Definitions and Examples)

ہم سٹ(Coset): اگر $(G,\cdot)$ گروپ کا کوئی تحت سٹ $(H,\cdot)$ ہو اور اگر $a \in G$، تب $aH = \{ah/h \in H\}$ سٹ H کا بایاں ہم سٹ ہوتا ہے جو کہ a سے تخلیق شدہ ہے۔اسی طرح $Ha = \{ha/h \in H\}$ سٹ H کا دایاں ہم سٹ ہے۔

مثال1۔ $G = \{1,-1,i,-i\}$ اور $(G,\cdot)$ گروپ ہے تب $H = \{1,-1\}$ گروپ G کا تحت گروپ ہے۔

H کے دائیں ہم سٹس حسب ذیل ہوں گے

$$H1 = \{1\cdot 1, -1\cdot 1\} = \{1,-1\}$$
$$H(-1) = \{1\cdot(-1), -1\cdot(-1)\} = \{-1,1\}$$
$$Hi = \{1\cdot i, -1\cdot i\} = \{i,-i\}$$
$$H(-i) = \{1\cdot(-i), -1\cdot(-i)\} = \{-i,i\}$$

اور H کے بائیں ہم سٹس حسب ذیل ہوں گے

$$1H = \{1\cdot 1, 1\cdot(-1)\} = \{1,-1\}$$
$$-1H = \{(-1)\cdot 1, (-1)\cdot(-1)\} = \{-1,1\}$$
$$iH = \{i\cdot 1, i\cdot(-1)\} = \{i,-i\}$$
$$-iH = \{(-i)\cdot 1, (-i)\cdot(-1)\} = \{-i,i\}$$

نوٹ:

1۔ اگر e کسی گروپ G کی اکائی(Identity)ہو، تب $eH = H = He$

2۔ ہر ایک ہم سٹ میں عناصر کی تعداد مساوی ہو گی۔

3۔ کوئی بھی دو ہم سٹس بالکل مماثل یا بالکل غیر مشترک ہوتے ہیں۔

4۔ آبیلین گروپ کے دائیں اور بائیں ہم سٹس میں فرق نہیں ہوتا ہے۔

5۔ اگر $a \in H$، تب $aH = H = Ha$

اگر معرفہ عمل جمع $(+)$ کا ہو، تب ہم سٹس درجہ ذیل ہوں گے

دایاں ہم سٹ: $H + a = \{h + a / h \in H\}$ جہاں $a \in G$

بایاں ہم سٹ: $a + H = \{a + h / h \in H\}$ جہاں $a \in G$

6۔ اگر $a \in G$ اور H، G کا تحت گروپ ہو، تب $aH \cap Ha \neq \varphi$ چوں کہ اگر $e \in G$ اکائی ہو تب $e \in H$ اکائی ہو گی۔ چنانچہ $ae = a = ea$ جب کہ $ae \in aH$ اور $ea \in Ha$ لہٰذا کم از کم ایک عنصر مشترک ہو گا۔

7۔ اگر گروپ G کا کوئی تحت گروپ H ہو اور $a, b \in G$ تب $ab \in G$ اور

$$a(bH) = (ab)H$$

اور

$$(Hb)a = H(ba)$$

8۔ کسی بھی Ha یا aH کے عناصر تعداد میں H کے برابر ہوتے ہیں اور سبھی عناصر ممیّز (*Distinct*) ہوتے ہیں۔

مثال 2۔ $G = \{\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\}$ جمع $(+)$ کے ساتھ گروپ ہے اور $H = \{\cdots -9, -6, -3, 0, 3, 6, 9, \cdots\}$ گروپ G کا تحت گروپ ہے۔ اب

$$0 + H = \{\cdots -9, -6, -3, 0, 3, 6, 9, \cdots\}$$
$$1 + H = \{\cdots -8, -5, -2, 1, 4, 7, 10, \cdots\}$$
$$2 + H = \{\cdots -7, -4, -1, 2, 5, 8, 11, \cdots\}$$
$$3 + H = \{\cdots -6, -3, 0, 3, 6, 9, \cdots\} = 0 + H$$
$$4 + H = \{\cdots -5, -2, 1, 4, 7, 10, \cdots\} = 1 + H$$
$$5 + H = \{\cdots -4, -1, 2, 5, 8, 11, \cdots\} = 2 + H$$

اس سے یہ نتیجہ نکلا کہ تین ہم سٹس $0 + H$، $1 + H$، $2 + H$ غیر مشترک ہیں اور

$$(0 + H) \cup (1 + H) \cup (2 + H) = G$$

اور باقی $3 + H$، $4 + H$، $5 + H$ پلٹ کر پہلے تین کے مماثل ہم سٹس بناتے ہیں۔ مزید یہ ہو گا کہ $6 + H$، $7 + H$، ... بھی وہی تین میں سے کوئی ہم سٹ بنتا چلا جائے گا۔

تحت گروپ کا اشاریہ (Index of a Subgroup): اگر H کسی متناہی گروپ G کا ایک تحت گروپ ہے، تب H کے مختلف دائیں (بائیں) ہم سٹس کی تعداد کو H کا اشاریہ (Index) کہا جاتا ہے۔ اسے $(G:H)$ یا $i_G(H)$ سے ظاہر کیا جاتا ہے۔

نوٹ: $|(G:H)| = \frac{|G|}{|H|}$

مثال3۔ (مثال1)میں جہاں$G = \{1, -1, i, -i\}$ گروپ ہےاور$H = \{1, -1\}$تحت گروپ ہے۔$(G: H) = 2$ہے چوں کہ اس کے دو ہی مختلف دائیں یا بائیں ہم سٹس ہیں۔جو کہ$\{1, -1\}, \{i, -i\}$ہیں۔

مثال4۔(مثال2)میںHکا اشاریہ$(G: H) = 3$

متوفق بہ مقیاس H (Congruence Modulo H): اگرH کسی گروپ$(G, \cdot)$کا تحت گروپ ہواور اگر$a, b \in G$تب اگر$b^{-1}a \in H$ہوتا ہےتب$a \equiv b(mod\ H)$یعنیaمتوفق ہےbکا بہ مقیاسH

3.2.1 حل شدہ مشقیں/قضیے(Solved Exercises/Theorems)

مثال5۔ اگر $H = \{0, 3, 6, 9, 12\}$ گروپ$(\mathbb{Z}_{15}, +15)$کا تحت گروپ ہو،توHکے تمام بائیں ہم سٹس معلوم کرواورHکا اشاریہ بھی معلوم کرو۔

حل۔ دیا گیا ہے کہ $(\mathbb{Z}_{15}, +_{15})$ہے۔جہاں$\mathbb{Z}_{15} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14\}$ ہےاور دیا گیا تحت گروپ $H = \{0, 3, 6, 9, 12\}$ ہے۔ہم دیکھتے ہیں کہ

$$0 \in G \Rightarrow 0+_{15}H = \{0+0, 0+3, 0+6, 0+9, 0+12\} = \{0, 3, 6, 9, 12\} = H$$

$$1 \in G \Rightarrow 1+_{15}H = \{1+0, 1+3, 1+6, 1+9, 1+12\} = \{1, 4, 7, 10, 13\}$$

$$2 \in G \Rightarrow 2+_{15}H = \{2+0, 2+3, 2+6, 2+9, 2+12\} = \{2, 5, 8, 11, 14\}$$

$$3 \in G \Rightarrow 3+_{15}H = \{3+0, 3+3, 3+6, 3+9, 3+12\}$$

چوں کہ$3 + 12 = 15 = 0$ ہوتا ہے،اس لیے $+_{15}$کے تحت

$$3 \in G \Rightarrow 3+_{15}H = \{3, 6, 9, 12, 0\} = H$$

$$4 \in G \Rightarrow 4+_{15}H = \{4+0, 4+3, 4+6, 4+9, 4+12\}$$

چوں کہ$4 + 12 = 16 = 1$ ہوتا ہے،اس لیے $+_{15}$کے تحت

$$4 \in G \Rightarrow 4+_{15}H = \{4, 7, 10, 13, 1\} = 1+_{15}H$$

$$5 \in G \Rightarrow 5+_{15}H = \{5+0, 5+3, 5+6, 5+9, 5+12\} = \{5, 8, 11, 14, 2\} = 2+_{15}H$$

چوں کہ$5 + 12 = 17 = 2$ ہوتا ہے،اس لیے $+_{15}$کے تحت

$$5 \in G \Rightarrow 5+_{15}H = \{5, 8, 11, 14, 2\} = 2+_{15}H$$

اسی طرح $6+_{15}H = 3+_{15}H$آئے گا۔

چنانچہ مختلف ہم سٹس

$$0+_{15}H = \{0, 3, 6, 9, 12\}$$

$$1+_{15}H = \{1, 4, 7, 10, 13\}$$

$$2+_{15}H = \{2, 5, 8, 11, 14\}$$

پائے گیے جن کا اجماع $(0+_{15}H) \cup (1+_{15}H) \cup (2+_{15}H) = \mathbb{Z}_{15}$ ہوتا ہے۔

چنانچہ H کا اشاریہ $(\mathbb{Z}_{15}: H) = 3$

مثال6۔ گروپ $(\mathbb{Z}, +)$ کے لیے تمام منقسم ہم سٹس معلوم کیجیے جب کہ تحت گروپ $4\mathbb{Z}$ ہو۔

حل۔ دیا گیا گروپ $(\mathbb{Z}, +)$ ہے

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

اور تحت گروپ $4\mathbb{Z} = \{\cdots -12, -8, -4,0,4,8,12, \cdots\}$ ہے۔

ہم سٹس جو حاصل ہوں گے وہ درجہ ذیل ہیں۔ دائیں اور بائیں ہم سٹس میں فرق نہیں ہے اس لیے کہ $(\mathbb{Z}, +)$ آبیلین گروپ ہے چنانچہ $4\mathbb{Z}$ بھی آبیلین ہو گا۔ فرض کرو کہ $H = 4\mathbb{Z}$ اب

$$1 + H = \{\cdots -11, -7, -3,1,5,9,13, \cdots\}$$
$$2 + H = \{\cdots -10, -6, -2,2,6,10,14, \cdots\}$$
$$3 + H = \{\cdots -9, -5, -1,3,7,11,15, \cdots\}$$
$$4 + H = \{\cdots -8, -4,0,4,8,12, \cdots\} = 0 + H = H$$
$$5 + H = \{\cdots -7, -3,1,5,9,13, \cdots\} = 1 + H$$

اسی طرح

$$6 + H = 2 + H$$

اور $7 + H = 3 + H$

وغیرہ آتے ہیں۔ چنانچہ نتیجہ یہ ہوا

$$(0 + H) \cup (1 + H) \cup (2 + H) \cup (3 + H) = \mathbb{Z}$$

یعنی $(0 + 4\mathbb{Z}) \cup (1 + 4\mathbb{Z}) \cup (2 + 4\mathbb{Z}) \cup (3 + 4\mathbb{Z}) = \mathbb{Z}$

اور $4\mathbb{Z}$ کا اشاریہ 4 ہے۔

مثال7۔ گروپ $(\mathbb{Z}_{12}, +_{12})$ میں $3\mathbb{Z}$ کا اشاریہ معلوم کرو۔

حل۔ دیا گیا گروپ ہے

$$\mathbb{Z}_{12} = \{0,1,2, 3,4,5,6,7,8,9,10,11\}$$

تحت گروپ ہے

$$3\mathbb{Z} = \{0,3,6,9\}$$

اس تحت گروپ کے ہم سٹس حسب ذیل ہوں گے

$$0 \in \mathbb{Z}_{12} \Rightarrow 0 + 3\mathbb{Z} = \{0+0, 0+3, 0+6, 0+9\} = \{0, 3, 6, 9\}$$

$$1 \in \mathbb{Z}_{12} \Rightarrow 1 + 3\mathbb{Z} = \{1+0, 1+3, 1+6, 1+9\} = \{1, 4, 7, 10\}$$

$$2 \in \mathbb{Z}_{12} \Rightarrow 2 + 3\mathbb{Z} = \{2+0, 2+3, 2+6, 2+9\} = \{2, 5, 8, 11\}$$

$$3 \in \mathbb{Z}_{12} \Rightarrow 3 + 3\mathbb{Z} = \{3+0, 3+3, 3+6, 3+9\} = \{3,6,9,0\} = 0 + 3\mathbb{Z}$$

$$4 \in \mathbb{Z}_{12} \Rightarrow 4 + 3\mathbb{Z} = \{4+0, 4+3, 4+6, 4+9\} = \{4, 7, 10, 13, 1\} = 1 + 3\mathbb{Z}$$

$$5 \in \mathbb{Z}_{12} \Rightarrow 5 + 3\mathbb{Z} = \{5+0, 5+3, 5+6, 5+9\} = \{5, 8, 11, 2\} = 2 + 3\mathbb{Z}$$

وغیرہ۔ نتیجہ یہ ہوا کہ

$$(0 + 3\mathbb{Z}) \cup (1 + 3\mathbb{Z}) \cup (2 + 3\mathbb{Z}) = \mathbb{Z}_{12}$$

لہٰذا $3\mathbb{Z}$ کا گروپ $(\mathbb{Z}_{12}, +_{12})$ میں اشاریہ 3 ہے۔

قضیہ 1۔ اگر H اور K کسی گروپ G کے دو تحت گروپس ہیں، تب

$$(H \cap K)a = Ha \cap Ka, \forall a \in G$$

ثبوت۔ فرض کرو کہ $x \in (H \cap K)a$، جہاں $a \in G$، تب

$$x \in (H \cap K)a \Leftrightarrow x = ya, y \in H \cap K$$

$$\Leftrightarrow x = ya, y \in H \text{ اور } y \in K$$

$$\Leftrightarrow x = ya, ya \in Ha \text{ اور } ya \in Ka$$

$$\Leftrightarrow x \in Ha \cap Ka$$

چنانچہ ثابت ہوا کہ $(H \cap K)a = Ha \cap Ka$ جب کہ $a \in G$

قضیہ 2۔ اگر G ایک متناہی گروپ ہے اور H_1 اور H_2 اس کے دو تحت گروپس ہیں جن کے رتبے مفرد صحیح اعداد p اور q ہیں $(p \neq q)$، تب $H_1 \cap H_2 = \{e\}$

ثبوت۔ ہمیں معلوم ہے کہ متناہی گروپ جس کا رتبہ مفرد صحیح عدد ہے، کے لیے کوئی واجبی تحت گروپ نہیں ہوتا،

اس لیے H_1 کے دو ہی تحت گروپس $\{e\}$ اور H_1 ہوں گے

اور H_2 کے دو ہی تحت گروپس $\{e\}$ اور H_2 ہوں گے

اب چوں کہ $p \neq q$

اس لیے $H_1 = \{e\}$ اور $H_2 = \{e\}$

اس لیے ثابت ہو جاتا ہے کہ $H_1 \cap H_2 = \{e\}$

قضیہ 3۔ اگر H کسی گروپ $(G, \cdot)$ کا تحت گروپ ہے اور $h \in G$ تب $h \in H$ اگر اور صرف اگر $hH = H = Hh$

ثبوت۔ فرض کرو کہ $h \in H$ تب ثابت کرنا ہے کہ $hH = H = Hh$

مان لو کہ $h' \in H$ تب $hh' \in hH$

اور چوں کہ H گروپ G کا تحت گروپ ہے، اس لیے

$$h, h' \in H \Rightarrow hh' \in H$$

چنانچہ $hh' \in hH$

اور $hh' \in H$

$hH \subseteq H$ .....(1)

مزید یہ کہ $h' = eh' = (hh^{-1})h' = h(h^{-1}h') \in hH \ [\because e = hh^{-1},\ h^{-1}h' \in H]$

$\Rightarrow$ $H \subseteq hH$ .....(2)

مساوات (1) اور (2) کے ذریعہ

$$hH = H$$

اسی طرح

$$hH = H = Hh$$

اب اس کے برعکس فرض کرو کہ $hH = H = Hh$

چوں کہ $h \in G$، اس لیے

$$h = he \Rightarrow h \in hH$$

چوں کہ $hH = H$، اس لیے

$$h \in H$$

اسی طرح $hH = H \Rightarrow h \in H$

$\Rightarrow$ $hH = H = Hh \Rightarrow h \in H$

قضیہ ثابت ہوا۔

قضیہ 4۔ اگر $(G,\cdot)$ گروپ ہے $a, b \in G$ اور H تحت گروپ ہے تب $aH = bH \Leftrightarrow a^{-1}b \in H$

اور $Ha = Hb \Leftrightarrow ab^{-1} \in H$

ثبوت۔ فرض کرو کہ $a, b \in G$ اور $Ha = Hb$

چوں کہ $e \in G$ اس لیے $e \in H$

تب $ea \in Ha$

$\Rightarrow$ $a \in Ha$

$\Rightarrow$ $a \in Hb$ $[\because Ha = Hb]$

$\Rightarrow$ $ab^{-1} \in (Hb)b^{-1}$

$\Rightarrow$ $ab^{-1} \in H(bb^{-1})$

$\Rightarrow$ $ab^{-1} \in He$

$\Rightarrow$ $ab^{-1} \in H$

اس کے برعکس اگر $ab^{-1} \in H$، تب

$$Hab^{-1} = H$$
$$\Rightarrow \quad Hab^{-1}b = Hb$$
$$\Rightarrow \quad Ha(b^{-1}b) = Hb$$
$$\Rightarrow \quad Hae = Hb$$
$$\Rightarrow \quad Ha = Hb$$

اسی طرح اگر $a^{-1}b \in H \Leftrightarrow aH = bH$ ثابت کرنے کے لیے فرض کرو کہ

$$aH = bH$$

چوں کہ $b \in bH$

$$\Rightarrow \quad b \in aH$$
$$\Rightarrow \quad a^{-1}b \in a^{-1}(aH)$$
$$\Rightarrow \quad a^{-1}b \in (a^{-1}a)H$$
$$\Rightarrow \quad a^{-1}b \in eH$$
$$\Rightarrow \quad a^{-1}b \in H$$

اس کے برعکس اگر $a^{-1}b \in H$، تب

$$a^{-1}b \in H$$
$$\Rightarrow \quad a^{-1}bH = H$$
$$\Rightarrow \quad a(a^{-1}bH) = aH$$
$$\Rightarrow \quad (aa^{-1})bH = aH$$
$$\Rightarrow \quad ebH = aH$$
$$\Rightarrow \quad bH = aH$$

لہٰذا قضیہ ثابت کیا گیا۔

قضیہ 5۔ کسی بھی گروپ کے کوئی دو ہم سٹس بائیں (دائیں) یا تو غیر مشترک ہوں گے یا مماثل ہوں گے۔

ثبوت۔ فرض کرو کہ H کسی گروپ $(G,\cdot)$ کا ہم سٹ ہے اور اگر $a, b \in G$

تب aH، bH بھی H کے ہم سٹس ہوں گے۔

اگر $aH \cap bH = \phi$ یعنی دونوں غیر مشترک ہوں گے، تب یہ قضیہ صحیح ہوگا۔

اور اگر $aH \cap bH \neq \phi$ تب ہمیں ثابت کرنا ہوگا کہ $aH = bH$ یہاں $aH \cap bH$ غیر خالی ہونے کی وجہ سے

فرض کریں کہ $c \in aH \cap bH$

$$\Rightarrow \quad c \in aH \text{ اور } c \in bH$$

فرض کریں کہ $\quad c = ah_1, \quad h_1 \in H$

اور $\quad c = bh_2, \quad h_2 \in H$

مزید یہ کہ $\quad c = ah_1 = bh_2$

چوں کہ H ایک تحت گروپ ہے اس لیے اگر $h_1 \in H$ تب $h_1{}^{-1} \in H$

$$\Rightarrow \quad ah_1h_1{}^{-1} = bh_2h_1{}^{-1}$$

$$\Rightarrow \quad ae = bh_2{h_1}^{-1}$$
$$\Rightarrow \quad a = bh_2{h_1}^{-1}$$
$$\Rightarrow \quad aH = \left(bh_2{h_1}^{-1}\right)H$$
$$\Rightarrow \quad aH = b\left(h_2{h_1}^{-1}\right)H$$

چوں کہ H ایک تحت گروپ ہے اور یہ بند شی خاصیت کی تکمیل کرتا ہے اس لیے $h_2{h_1}^{-1} \in H$

$$\Rightarrow \quad aH = bH$$

چنانچہ قضیہ ثابت ہوا۔

قضیہ 6۔ اگر H گروپ G کا ایک تحت گروپ ہے، تب H کے تمام ممیز/مختلف بائیں اور دائیں ہم سٹس میں ایک ایک بر مطابقت (One-One Onto Relation) بنائی جاسکتی ہے۔

ثبوت۔ فرض کرو کہ $(G,\cdot)$ ایک گروپ اور H اس کا تحت گروپ ہے

فرض کرو کہ $H = G_1$ کے تمام ممیز/مختلف بائیں ہم سٹس کا سٹ ہے

اور $H = G_2$ کے تمام ممیز/مختلف دائیں ہم سٹس کا سٹ ہے

فرض کرو کہ $G_1 = \{aH/a \in G\}, G_2 = \{Ha/a \in G\}, \quad f: G_1 \to G_2$،

جہاں $f(aH) = Ha^{-1}, \forall aH \in G_1$

اگر $aH, bH \in G_1$ اور $aH = bH$

$$\Rightarrow \quad b^{-1}a \in H$$
$$\Rightarrow \quad (b^{-1}a)^{-1} \in H$$
$$\Rightarrow \quad a^{-1}(b^{-1})^{-1} \in H$$
$$\Rightarrow \quad Ha^{-1} = Hb^{-1}$$
$$\Rightarrow \quad f(aH) = f(bH)$$

لہٰذا تفاعل درست ہے۔

اب اگر $f(aH) = f(bH)$ لیا جایے، تب

$$Ha^{-1} = Hb^{-1}$$
$$\Rightarrow \quad a^{-1}(b^{-1})^{-1} \in H$$
$$\Rightarrow \quad a^{-1}b \in H$$
$$\Rightarrow \quad (a^{-1}b)^{-1} \in H$$
$$\Rightarrow \quad b^{-1}a \in H$$
$$\Rightarrow \quad aH = bH$$

اس لیے تفاعل ایک۔ایک (One-One) ہے۔

آخر میں f کو بر (Onto) تفاعل ثابت کرنے کے لیے فرض کرو کہ $Ha \in G_2$ جہاں $a \in G$ تب $a^{-1} \in G$

لہٰذا

$$a^{-1}H \in G_1$$

لیے گیے تفاعل کی مدد سے

اور $$f(a^{-1}H) = H(a^{-1})^{-1}$$

$$\Rightarrow \quad f(a^{-1}H) = Ha$$

اس لیے f ایک برتفاعل ہے۔

چنانچہ ثابت ہوا کہ $f: G_1 \to G_2$ ایک۔ایک برتفاعل ہے۔

قضیہ ثابت ہوا۔

قضیہ 7۔ اگر H گروپ $(G,\cdot)$ کا ایک تحت گروپ ہے، تب H کے دو ہم سٹس کے درمیان دور بطی (Bijection) تفاعل بنایا جاسکتا ہے۔

ثبوت۔ فرض کرو کہ $a, b \in G$ اور aH, bH دو بائیں ہم سٹس ہیں۔

فرض کرو کہ $f: aH \to bH$ اور $f(ah) = bh, h \in H$

تب

$$h_1, h_2 \in H \Rightarrow ah_1, ah_2 \in aH$$

اور $$bh_1, bh_2 \in bH$$

تب

$$f(ah_1) = f(ah_2)$$

$$\Rightarrow \quad bh_1 = bh_2$$

$$\Rightarrow \quad h_1 = h_2$$

$$\Rightarrow \quad ah_1 = ah_2$$

f ایک۔ایک ہے۔

اور اب

$$bh \in bH$$

$$\Rightarrow \quad h \in H$$

چنانچہ $$ah \in H$$

جب کہ $f(ah) = bh$، اس لیے f ایک برتفاعل ہے۔

لہٰذا ثابت ہوا کہ f دور بطی تفاعل یعنی ایک۔ایک اور برتفاعل ہے۔

نوٹ: بائیں ہم سٹس کے لیے ثابت کیا گیا قضیہ اسی طرح دو دائیں ہم سٹس کے لیے بھی پورا اترتا ہے۔

قضیہ 8۔ اگر H گروپ G کا ایک تحت گروپ ہے اور $a, b \in G$، تب رشتہ $a \equiv b(mod\ H)$ ایک معادلت (Equivalence) رشتہ ہوگا۔

ثبوت۔ ہمیں معلوم ہے کہ رشتہ معادلت کہلاتا ہے جب کہ اس میں تین شرائط پوری ہوں جو درج ذیل ہیں:

1. رجوعی خاصیت (Reflexive Property)

2. تشاکل خاصیت(Symmetric Property)

3. انتقال پزیر/عبوری خاصیت(Transitive Property)

1. دیا گیا ہے کہ H گروپ G کا ایک تحت گروپ ہے۔

اب فرض کرو کہ $a \in G$

اور $e \in G$ اکائی ہے جو کہ H کی بھی اکائی ہو گی اور

$$aa^{-1} = e \in H$$
$$\Rightarrow \quad a \equiv a(mod\ H)$$

لہٰذا یہ رشتہ رجوعی(Reflexive) ہے۔

2. اگر $a, b \in G$ اور $a \equiv b(mod\ H)$

$$\Rightarrow \quad b^{-1}a \in H$$

چوں کہ H تحت گروپ ہے۔

$$(b^{-1}a)^{-1} \in H$$
$$\Rightarrow \quad a^{-1}(b^{-1})^{-1} \in H$$
$$\Rightarrow \quad a^{-1}b \in H$$
$$\Rightarrow \quad b \equiv a(mod\ H)$$

لہٰذا یہ رشتہ تشاکل(Symmetric) ہے۔

3. اگر $a \equiv b(mod\ H)$ اور $b \equiv c(mod\ H)$، $a, b, c \in G$ تب

$$b^{-1}a \in H, c^{-1}b \in H$$
$$\Rightarrow \quad (c^{-1}b)(b^{-1}a) \in H$$
$$\Rightarrow \quad c^{-1}(bb^{-1})a \in H$$
$$\Rightarrow \quad c^{-1}(e)a \in H$$
$$\Rightarrow \quad c^{-1}a \in H$$
$$\Rightarrow \quad a \equiv c(mod\ H)$$

لہٰذا یہ رشتہ انتقال پزیر/عبوری(Transitive) ہے۔

چوں کہ مطلوبہ تینوں شرائط پوری ہوئیں، اس لیے توافقی رشتہ(Congruence Relation) ایک معادلت رشتہ ہے۔

قضیہ ثابت ہوا۔

قضیہ 9۔ اگر H گروپ $(G,\cdot)$ کا ایک تحت گروپ ہے اور اگر $a \in G$ تب معادل جماعت $\bar{a} = \{x \in G / x \equiv a(mod\ H)\}$ تب $\bar{a} = aH$ ہو گا۔

ثبوت۔ دیا گیا ہے کہ $\bar{a} = \{x \in G / x \equiv a(mod\ H)\}$

ثابت کرنا ہے کہ $\bar{a} = aH$ جب کہ $a \in G$

فرض کرو کہ $e \in G$ اکائی ہے چنانچہ $e \in H$ ہو گا۔

تب

$$x \in \bar{a} \Leftrightarrow x \equiv a(mod\ H)$$
$$\Leftrightarrow a^{-1}x \in H$$

مان لیں $\Leftrightarrow a^{-1}x = h \in H$

$$\Leftrightarrow a(a^{-1}x) = ah \in aH, \quad h \in H$$
$$\Leftrightarrow (aa^{-1})x = ah \in aH, \quad h \in H$$
$$\Leftrightarrow ex = ah \in aH, \quad h \in H$$
$$\Leftrightarrow x = ah \in aH, \quad h \in H$$
$$\Leftrightarrow x \in aH$$

اس لیے

$$\bar{a} = aH$$

ثابت کیا گیا۔

لگرانج کا قضیہ(Lagrange's Theorem):

اگر G ایک متناہی گروپ ہے اور H اس کا تحت گروپ ہے، تب H کا رتبہ G کے رتبے کو تقسیم کرتا ہے ۔

یا

کسی بھی متناہی گروپ کے رتبے کو اس کے ہر تحت گروپ کا رتبہ تقسیم کرتا ہے۔

یا

اگر G ایک متناہی گروپ ہے اور H اس کا تحت گروپ ہے، تب $O(H)/O(G)$ یعنی $|H|/|G|$

ثبوت۔ فرض کرو کہ $(G,\cdot)$ ایک متناہی گروپ ہے اور $O(G) = n$ اور

$$H = \{h_1, h_2, \cdots, h_m\} \qquad .....(1)$$

تحت گروپ ہے، جن کے عناصر ممیّز ہیں، تب

$$O(H) = m$$

ہمیں ثابت کرنا ہے کہ m/n یعنی m تقسیم کرے گا n کو۔

فرض کرو کہ

$$a \in G \text{ اور } a \notin H, \qquad .....(2)$$

تب

$$H_1 = aH = \{ah_1, a\,h_2, \cdots, ah_m\}$$

اس کے تمام عناصر ممیّز ہوں گے ورنہ اگر

$$ah_i = a\,h_j$$
$$\Rightarrow \quad h_i = h_j$$

جو کہ مساوات(1) کی تردید کرتا ہے۔

مزید یہ کہ H اور aH بالکل غیر مشترک ہوں گے۔ ورنہ اگر دونوں سے عناصر $h_i = ah_j$ لیے جائیں، تب

$$h_i h_j^{-1} = a h_j h_j^{-1}$$
$$\Rightarrow \quad h_i h_j^{-1} = ae$$

چوں کہ H ایک تحت گروپ ہے، اس لیے

$$h_i h_j^{-1} = a \in H$$

یہ مساوات(2) کی تردید کرتا ہے۔ چنانچہ نتیجہ یہ ہے کہ H اور aH میں G گروپ کے مختلف m عناصر ہر ایک میں ہیں۔ اب اگر $b \in G$ لیا جایے جو کہ $b \notin H, b \notin H_1$

تب

$$H_2 = bH = \{bh_1, b\, h_2, \cdots, bh_m\}$$

اس کے تمام عناصر ممیّز اور H_2 غیر مشترک ہو گا H اور H_1 دونوں سے۔ یہ سلسلہ ختم ہو جایے گا چوں کہ G متناہی گروپ ہے اس کے عناصر صرف ہو جائیں گے۔ اگر یہ فرض کر لیا جایے کہ ایسے k ہم سٹس بنائے جا سکیں جن کے رتبے m ہوں گے۔ تب

$$m \cdot k = n$$

یعنی m، m/n تقسیم کرتا ہے n کو یا $|H|/|G|$

دوسرے معنوں میں $O(H)/O(G)$ یا یوں کہہ لیں کہ H کا رتبہ G کے رتبے کو تقسیم کرتا ہے۔

لہٰذا لگرانج کا قضیہ ثابت ہوا۔

تبصرہ: لگرانج کے قضیہ کا معکوس (Converse) صحیح نہیں ہے۔

مثال 8۔ مثال کے طور پر اگر دیکھیں تو جفت مبادلوں (even permutations) کا گروپ A_4 کا رتبہ 12 ہے اور اس میں 6 رتبے والا کوئی تحت گروپ نہیں ملے گا جب کہ $O(H) = 6/O(A_4) = 12$ ہے۔

یہ بھی ایک قوی مثال ہے کہ لگرانج کا معکوس قضیہ صحیح نہیں ہوتا۔

لگرانج قضیے کے نتائج/اطلاقات (Consequences of Lagrange's Theorem)

قضیہ 10۔ اگر G ایک متناہی گروپ ہے اور اگر $a \in G$ تب $|a|/|G|$ یعنی a کا رتبہ G کے رتبے کو تقسیم کرتا ہے۔

ثبوت۔ دیا گیا ہے کہ G ایک متناہی گروپ ہے۔ فرض کرو کہ $O(G) = |G| = n$

فرض کرو کہ $a \in G$ اور $O(a) = |a| = m$ یعنی $a^m = e$

تب $H = \{a^1, a^2, \cdots, a^m = e\}$ گروپ G کا تحت گروپ ہو گا۔ اس لیے

$$O(H) = m$$

لگرانج کے قضیے کے مطابق $O(H)/O(G)$

$$\Rightarrow \quad m/n$$

یعنی $|a|/|G|$ یا $O(a)/O(G)$

قضیہ ثابت ہوا۔

قضیہ 11۔ اگر $(G,\cdot)$ ایک متناہی گروپ ہے جس کا رتبہ n ہے تب اگر $a \in G$ تب $a^n = e$ جہاں $e \in G$ اکائی ہے۔

ثبوت۔ دیا گیا ہے کہ $O(G) = n$ اور $a \in G$

فرض کرو کہ $|a| = d$ تب $d \leq n$ اور $a^d = e$

اگر $H = \{a^1, a^2, \cdots, a^d = e\}$ تحت گروپ ہو گا

$$O(H) = d$$

اور لگرانج کے قضیہ کے مطابق $O(H)/O(G)$ یعنی d/n

اس صورت میں $n = dq$ جہاں $q \in \mathbb{Z}^+$

اب

$$a^n = a^{dq} = (a^d)^q = e^q$$
$$\Rightarrow \quad a^n = e$$

قضیہ ثابت ہوا۔

نوٹ: قضیہ بالا کو یوں بھی لکھا جا سکتا ہے،

اگر $(G,\cdot)$ ایک متناہی گروپ ہے اور $a \in G$ تب $a^{|G|} = e$ ہو گا۔

وضاحت: قضیہ 2 کو ہم ضربی گروپ $G = \{1, \omega, \omega^2\}$ کے لیے پرکھیں گے۔ یہاں $O(G) = 3$۔

ہم دیکھتے ہیں کہ عناصر $1, \omega, \omega^2$ ہیں۔ اب

$$1^{O(G)} = 1^3 = 1 = e,$$
$$\omega^3 = 1$$

اور $(\omega^2)^3 = \omega^6 = \omega^3 \cdot \omega^3 = 1 \cdot 1 = 1$

لہٰذا G کے سبھی عناصر پر قضیہ واضح ہے۔

صریح نتیجہ (Corollary)

اگر ایک متناہی گروپ کا رتبہ مفرد صحیح عدد (Prime Number) ہو تو اس کا کوئی واجبی تحت گروپ نہیں ہو گا۔

ثبوت۔ فرض کرو کہ G ایک متناہی گروپ ہے جس کا رتبہ $O(G) = p$ ہے جب کہ p مفرد صحیح عدد ہے۔ تب اگر H گروپ G کا تحت گروپ ہو اور $O(H) = m$ ہے۔

تب لگرانج کے قضیے کے مطابق m/p تب p کے مفرد صحیح عدد ہونے کی وجہ سے $m = p$ یا $m = 1$ ہوگا۔
ان دونوں صورتوں میں غیر واجبی تحت گروپ ہوگا۔یعنی G کا کوئی واجبی تحت گروپ نہیں ہو سکتا۔

یہ ثابت ہوا۔

ترقیم(Notation):

$U(n)$ صحیح مثبت اعداد کا ایک سٹ ہے جو n سے چھوٹے اور n کے ہم مفرد ہوں، یعنی

$$U(n) = \{m \in \mathbb{Z}^+/(m,n) = 1\}$$

$(m,n) = 1$ سے مراد m اور n کا اعظم مشترک قاسم (G.C.D.) 1 ہے۔

مثلاً $U(10) = \{1,3,7,9\}$

$\because (1,10) = 1, (3,10) = 1, (7,10) = 1, (9,10) = 1$

مثال10۔ $H = \{1, 15\}$ کے تمام ہم سٹس $G = U(32)$ میں معلوم کرو۔

حل۔ ہمیں معلوم ہے کہ $G = U(32) = \{1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31\}$ بہ مقیاس 32 ضربی رشتے میں گروپ بناتا ہے۔اور دیا گیا ہے کہ $H = \{1, 15\}$ گروپ G کا تحت گروپ ہے۔

اب

$$1 \in G \Rightarrow 1H = \{1 \cdot 1, 1 \cdot 15\} = \{1, 15\} = H = 15H$$
$$3 \in G \Rightarrow 3H = \{3 \cdot 1, 3 \cdot 15\} = \{3, 13\} = 13H$$
$$5 \in G \Rightarrow 5H = \{5 \cdot 1, 5 \cdot 15\} = \{5, 11\} = 11H$$
$$7 \in G \Rightarrow 7H = \{7 \cdot 1, 7 \cdot 15\} = \{7, 9\} = 9H$$
$$17 \in G \Rightarrow 17H = \{17 \cdot 1, 17 \cdot 15\} = \{17, 31\} = 31H$$
$$19 \in G \Rightarrow 19H = \{19 \cdot 1, 19 \cdot 15\} = \{19, 29\} = 29H$$
$$21 \in G \Rightarrow 21H = \{21 \cdot 1, 21 \cdot 15\} = \{21, 27\} = 27H$$
$$23 \in G \Rightarrow 23H = \{23 \cdot 1, 23 \cdot 15\} = \{23, 25\} = 25H$$

H کا اشاریہ $=$ H کے مختلف ہم سٹس کی تعداد $= \frac{U(32)}{|H|}$

$$= \frac{16}{2}$$
$$= 8$$

اور ہم پورے 8 ہم سٹس بنا چکے ہیں۔

نوٹ: اگر H اور K کسی گروپ کے دو تحت گروپس ہوں اور $HK = \{hk/h \in H, k \in K\}$ تب

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

3.3 اکتسابی نتائج(Learning Outcomes)

اس اکائی میں ہم نے تحت گروپ سے ہم سٹس کس طرح بنائے جاتے ہیں، معلوم کر لیا۔ یہ بھی معلوم ہوا کہ ہم سٹس دائیں اور بائیں ہوتے ہیں اور ہر ہم سٹ میں عناصر کی تعداد مساوی ہوتی ہے۔ مختلف (دائیں یا بائیں) ہم سٹس کی تعداد کو تحت گروپ کا اشاریہ (Index) کہتے ہیں۔ یہ بھی معلوم ہوا کہ متوفق رشتہ معادل رشتہ ہوتا ہے۔ تحت گروپ کا اشاریہ گروپ کے رتبے کو تحت گروپ کے رتبے سے تقسیم کرنے پر حاصل ہوتا ہے یعنی $(G:H) = \frac{O(G)}{O(H)}$ جہاں G گروپ اور H اس کا تحت گروپ ہے۔ ایک قضیہ کو ہم نے ثابت کیا کہ کوئی دو دائیں یا بائیں ہم سٹس یا تو غیر مشترک ہوتے ہیں یا مساوی ہوتے ہیں۔ مزید یہ کہ دائیں اور بائیں ہم سٹس کے درمیان دور بطی (Bijection) تفاعل قائم ہو سکتا ہے۔ اور پھر قضیوں کے علاوہ ایک اہم نامور قضیہ لگرانج کا قضیہ بیان ہوا اور ثابت کیا گیا۔ اور اس کے نتائج کو اخذ کیا گیا۔ ان کے مثالوں کو پیش کیا گیا۔ اس ساتھ ہی چند مشقی سوالوں کو حل کیا گیا۔

3.4 کلیدی الفاظ (Key Words)

ہم سٹس، متوفق بہ مقیاس، معادل رشتہ، اشاریہ

3.5 نمونہ امتحانی سوالات (Model Examination Questions)

3.5.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. دائیں اور بائیں ہم سٹس کی تعریف کرو۔
2. معادلی رشتہ کیا ہوتا ہے؟

3.5.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. کسی تحت گروپ کے اشاریہ کی تعریف کیجیے اور گروپ $G = \{1, -1, i. -i\}$ بذریعہ ضرب اور تحت گروپ $H = \{1, -1\}$ ہو تب H کا اشاریہ معلوم کرو۔
2. گروپ $(\mathbb{Z}, +)$ کے لیے تمام منقسم ہم سٹس معلوم کیجیے جب کہ تحت گروپ $4\mathbb{Z}$ ہے۔
3. ثابت کرو کہ اگر G ایک متناہی گروپ ہے اور اگر $a \in G$ تب $|a|/|G|$

3.5.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. ہم سٹس کی تعریف کرو اور ثابت کرو کہ کوئی دو دائیں (بائیں) ہم سٹس یا تو غیر مشترک ہوں گے یا مماثل (مساوی) ہوں گے۔
2. لگرانج کے قضیے کو بیان اور ثابت کرو۔
3. اگر $H = \{0,3,6,9,12\}$ گروپ $(\mathbb{Z}_{15}, +_{15})$ کا تحت گروپ ہے، تب کے تمام بائیں ہم سٹس معلوم کرو اور H کا اشاریہ بھی معلوم کرو۔

4. اگر $(G,\cdot)$ ایک متناہی گروپ ہے جس کا رتبہ n ہے اور اگر $a \in G$ تب $a^n = e$، جہاں $e \in G$ اکائی ہے۔ ثابت کرو۔

3.6 مزید مطالعے کے لیے تجویز کردہ کتابیں (Suggested Books for further Readings)

1. I.N. Herstein: Topics in Algebra , Vikas Publishers
2. Surjeet Singh and Qazi Zameeruddin: Modern Algebra, Vikas Publishers
3. J.B. Fraleigh: A First course in Abstract Algebra

اکائی4۔ نارمل تحت گروپس اور خارج قسمت گروپس

(Normal Subgroups and Quotient Groups)

اکائی کے اجزا

4.0 تمہید(Introduction)

گروپ اور پھر اس کا تحت گروپ معلوم ہونے کے بعد ہم نے ہم سٹس کو بھی جان لیا۔ تحت گروپ پر ایک خاص شرط لگا کر اس کو نارمل تحت گروپ سے تعبیر کیا جاتا ہے۔ نارمل گروپ کے بعض خواص اور ان کا حاصل ضرب اور نارمل تحت گروپس کے درمیان تفاعل دو ربطی خاصیت ہونے کو پایا گیا ہے۔ کسی تحت گروپس کی مدد سے طبعی گراور گروپ کے مرکز حاصل کیے جا سکتے ہیں۔ نارمل تحت گروپ کے تمام دائیں (بائیں) ہم سٹس کا سٹ $\frac{G}{H}$ گروپ بنتا ہے، جسے خارج قسمت گروپ (Quotient Group) یا ضربی گروپ (Factor Group) کہتے ہیں جو آگے ہم مارفیت (Homomorphism) کے قضیے میں استعمال ہوتا ہے۔

اہم مسائل میں سے ایک جو صدیوں تک ریاضی دانوں کی توجہ کا مرکز بنا ہوا تھا، ایک کثیر رکنی مساوات کو جزروں کے ذریعہ حل کرنا تھا۔ دو درجی مساوات حل پزیر ہے آسانی کے ساتھ اور پھر سولہویں صدی عیسوی میں اطالوی ریاضی داں تارتالیہ (Tartalia, 1506-1557) اور کارڈن (Cardon, 1501-1576) نے کعبی مساوات (تیسرے درجے کی مساوات) کو حل کرنے کا طریقہ دریافت کیا۔ کارڈن کے شاگرد فیراری (Ferrari) نے 1545ء میں چار درجی مساوات (Biquadratic Equation) کو حل کرنے کا طریقہ پیش کیا۔ اس کے بعد تین صدیوں تک پانچویں درجے یا اس سے زیادہ درجہ کی مساوات کے حل کرنے کے متعلق کچھ بھی معلوم نہ ہو سکا۔ دو ذہین عبقری اطفال ابیل (Abel) اور گالوا (Galvi's) نے 1828 اور 1830 میں کسی مساوات کے حل اور اس کے ریشوں کے مبادلوں کے گروپ کے درمیان تعلقات کو پہچانا۔ اگر کسی مساوات کے ریشوں کے مبادلات کا گروپ ایک خاصیت دائیں اور بائیں ہم سٹس مساوای ہونے کی صورت میں گروپ کو خود حل پزیر کہتے ہیں۔ اور وہ مساواتیں جن کا متناظر گروپ حل پزیر ہے، خود حل پزیر ہوتی ہیں۔

نارمل گروپ ایسا گروپ ہے جو اس حل پزیری کی کسوٹی کے تعین کرنے میں نہایت اہم رول ادا کرتا ہے۔ زیر نظر اکائی کے موضوعات گروپ نظریات (Group Theory)، رنگ نظریات (Ring Theory) کے مطالعہ میں نہایت اہم کردار ادا کرتے ہیں۔

مزدوج جماعت (Conjugate Class) اور جماعتی مساوت (Class Equations) کا تعارف کیا جایے گا۔ اور یہ دیکھا جایے گا کہ گروپ کے عناصر میں مزدوج ہونے کا رشتہ معادلی رشتہ (Equivalence Relation) ہوتا ہے۔

4.1 مقاصد(Objectives)

اس اکائی کی تکمیل پر آپ کو اس قابل ہونا چاہیے کہ نارمل تحت گروپ کی تعریف کر سکیں اس شرط کو کسی تحت گروپ پر آزما سکیں۔ دیا ہوا تحت گروپ نارمل ہے یا نہیں پہچان سکیں۔ مثالیں دینے کے قابل ہو جائیں۔ نارمل تحت گروپ ہونے کے لیے بعض قضیے ثابت کر سکیں۔ خارج قسمت گروپ یا ضربی گروپ کی تعریف اس کے گروپ ہونے کی تصدیق کر سکیں۔ طبعی گر (Normalizer)

اور گروپ کے مرکز (Centre) کی تعریف کر سکیں اور یہ تصدیق کر سکیں کہ یہ نارمل تحت گروپ ہوتے ہیں۔ مزدجوج اور جماعتی مساوات کی تعریف کر سکیں۔

4.2 تعریفات اور حل شدہ قضیے/مشقیں (Definitions and Solved Theorems/Exercise)

نارمل تحت گروپ (Normal Subgroup)

تعریف: ایک گروپ G کے تحت گروپ H کو ہم نارمل تحت گروپ کہتے ہیں اگر $\forall x \in G$ اور $\forall h \in H$ کے لیے $xhx^{-1} \in H$

ترقیم (Notation): اگر گروپ G کا نارمل تحت گروپ ہے، تب اس کو ہم $H \lhd G$ سے ظاہر کریں گے۔

نوٹ:

1. اگر G ابیلین گروپ ہے تب تو اس کا ہر تحت گروپ نارمل ہو گا کیوں کہ

$\forall h \in H$ اور $\forall x \in G$

$$\begin{aligned} xhx^{-1} &= hxx^{-1} \\ &= he \\ &= h \in H \end{aligned}$$

2. G کے لیے غیر واجبی تحت گروپس (Improper Subgroups) $\{e\}$ اور G نارمل تحت گروپس ہوتے ہیں

$$\because \forall x \in G, xex^{-1} = xx^{-1} = e \in \{e\}$$

لہٰذا $\{e\}$ نارمل تحت گروپ ہے۔

اور G کے بارے میں $\forall x \in G$ اور $\forall h \in H$

$$xhx^{-1} \in G$$

چوں کہ سارے ہی عناصر G میں موجود ہیں، لہٰذا $G \lhd G$

3. کوئی بھی غیر ابیلین گروپ جس کا ہر تحت گروپ نارمل ہو، ہیملٹن (Hamilton) گروپ کہلاتا ہے۔
4. جس کسی غیر ابیلین گروپ کے کوئی واجبی نارمل تحت گروپ نہیں ہوتے اس کو سادہ (Simple) گروپ کہتے ہیں۔

قضیہ 1۔ کسی گروپ G کا تحت گروپ H نارمل ہو گا اگر اور صرف اگر $xHx^{-1} = H, \quad \forall x \in G$

ثبوت۔ فرض کرو کہ $\forall x \in G \Rightarrow xHx^{-1} = H$

تب ہمیں ثابت کرنا ہو گا کہ H نارمل تحت گروپ ہے۔

اب

$$\begin{aligned} & xHx^{-1} = H \\ \Rightarrow \quad & xHx^{-1} \subseteq H \\ \Rightarrow \quad & xhx^{-1} \in H, \forall h \in H \end{aligned}$$

لہٰذا H نارمل تحت گروپ ہے۔

بالعکس اگر فرض کریں کہ H ایک نارمل تحت گروپ ہے، تب ہمیں ثابت کرنا ہو گا کہ $xHx^{-1} = H, \quad \forall x \in G$

چوں کہ Hایک نارمل تحت گروپ ہے،اس لیے

$$\forall x \in G, \forall h \in H \implies xhx^{-1} \in H$$
$$\implies xHx^{-1} \subseteq H \qquad .....(1)$$

اسی طرح یہ بھی کیا جاسکتا ہے کہ

$$x^{-1}H(x^{-1})^{-1} \subseteq H \qquad [\because x^{-1} \in G]$$
$$\implies x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1}$$
$$\implies (xx^{-1})H(xx^{-1}) \subseteq xHx^{-1}$$
$$\implies eHe \subseteq xHx^{-1}$$
$$\implies H \subseteq xHx^{-1} \qquad .....(2)$$

مساوات(1)اور(2)کی مدد سے نتیجہ یہ نکلا کہ $xHx^{-1} = H$

قضیہ ثابت ہوا۔

قضیہ2۔ اگر H گروپ G کاایک تحت گروپ ہے،تب H نارمل تحت گروپ ہوگا اگراور صرف اگر H کا بایاں ہم سٹ اور دایاں ہم سٹ برابر ہوں۔

ثبوت۔ فرض کرو کہ Hنارمل تحت گروپ ہے،تب ہمیں ثابت کرنا ہوگا کہ $xH = Hx, \quad \forall x \in G$

چوں کہ Hنارمل تحت گروپ ہے،اس لیے

$$\forall x \in G \implies xHx^{-1} = H$$
$$\implies (xHx^{-1})x = Hx$$
$$\implies xH(x^{-1}x) = Hx$$
$$\implies xHe = Hx$$
$$\implies xH = Hx$$

اس کے بالعکس اگر بایاں اور دایاں ہم سٹ برابر لیے جائیں یعنی،

$$xH = Hx, \forall x \in G$$

تب ثابت کرنا ہوگا کہ Hنارمل تحت گروپ ہے۔

$$\because xH = Hx$$
$$x \in G \implies x^{-1} \in G$$
$$\implies xHx^{-1} = Hxx^{-1}$$
$$\implies xHx^{-1} = He = H$$
$$\implies xhx^{-1} \in H, \forall h \in H$$

چنانچہ Hنارمل تحت گروپ ہوا۔

قضیہ ثابت ہوا۔

قضیہ3۔ کسی گروپ G کا ایک تحت گروپ H ، نارمل تحت گروپ ہوگا اگراور صرف اگر H کے دو دائیں(بائیں) ہم سٹس کا حاصل ضرب پھر دایاں(بایاں) Hکا ہم سٹ ہوگا۔

ثبوت۔ فرض کرو کہ کسی گروپ G کا Hایک نارمل تحت گروپ ہے۔تب

$$\forall a, b \in G \Longrightarrow ab \in H$$

اور H کے تین دائیں ہم سٹس Ha, Hb, Hab ہیں۔تب

$$Ha \cdot Hb = H(aH)b$$
$$= H(Ha)b \qquad [Ha = aH \text{ چوں کہ } H \text{ نارمل ہے اس لیے}]$$
$$= HH(ab)$$
$$= Hab \qquad [\because H = HH \text{ چوں کہ } H \text{ تحت گروپ ہے}]$$

اس کے بالعکس اگر ہم فرض کریں کہ $Ha \cdot Hb = Hab$

تب ہمیں ثابت کرنا ہے کہ H ایک نارمل تحت گروپ ہوگا۔توجہ کرو $\forall x \in G$ اور $\forall h \in H$

$$xhx^{-1} = (ex)(hx^{-1})$$
$$\in Hx(Hx^{-1})$$
$$\in H(xx^{-1})$$
$$\in He$$
$$\in H$$

اس لیے H ایک نارمل تحت گروپ ہوا۔

اسی طرح یہ قضیہ بائیں ہم سٹس کے لیے بھی پورا اترتا ہے۔

چنانچہ قضیہ چابت ہوا۔

قضیہ 4۔ کسی دو نارمل تحت گروپس کا تقاطع (Intersection) بھی نارمل تحت گروپ ہوگا۔

یا

اگر N_1 اور N_2 کسی گروپ G کے دو نارمل تحت گروپس ہیں تب $N_1 \cap N_2$ بھی G کا ایک نارمل تحت گروپ ہوگا۔

ثبوت۔ فرض کرو کہ N_1 اور N_2 کسی گروپ G کے دو نارمل تحت گروپس ہیں۔

تب چوں کہ بنیادی طور پر N_1 اور N_2 تحت گروپس ضرور ہیں اس لیے ان کا تقاطع (Intersection) $N_1 \cap N_2$ تحت گروپ ضرور ہوگا۔

اب ہمیں یہ ثابت کرنا ہوگا کہ $N_1 \cap N_2$ نارمل بھی ہوگا۔ اس کے لیے اگر $n \in N_1 \cap N_2$ اور $x \in G$، تب $n \in N_1 \& n \in N_2$

اب چوں کہ N_1 اور N_2 نارمل تحت گروپس ہیں۔اس لیے

$$xnx^{-1} \in N_1$$

اور

$$xnx^{-1} \in N_2$$

چنانچہ

$$xnx^{-1} \in N_1 \cap N_2$$

لہٰذا ثابت ہوا کہ $N_1 \cap N_2$ نارمل تحت گروپ ہے۔

صریح نتیجہ (Corollary): کئی نارمل تحت گروپس کا تقاطع بھی نارمل تحت گروپس ہوگا۔

قضیہ 5۔ اگر G ایک گروپ ہے تب اس کا کوئی بھی نارمل تحت گروپ G کے غیر خالی تحت سٹ کے ساتھ تقلیبی

خاصیت(Commutative Property)پوری کرتا ہے۔

ثبوت: فرض کرو کہ N کسی گروپ G کا نارمل تحت گروپ ہے اور H گروپ G کا غیر خالی تحت سٹ ہے۔تب ہمیں ثابت کرنا ہے کہ

$$NH = HN$$

فرض کرو کہ $nh \in NH, n \in N \ \& \ h \in H$

چوں کہ N نارمل تحت گروپ ہے اس لیے

$$h^{-1}nh \in N \quad \& \quad hnh^{-1} \in N$$

جب کہ

$$h, h^{-1} \in H \quad \& \quad h, h^{-1} \in G, n \in N$$

غور کرو کہ $nh \in NH$ اور

$$\begin{aligned} nh &= hh^{-1}nh \\ &= h(h^{-1}nh) \\ &\in HN \qquad \because \ h^{-1}nh \in N \\ \Longrightarrow \quad NH &\subseteq HN \qquad \text{.....(1)} \end{aligned}$$

اسی طرح $hn \in HN$ اور

$$\begin{aligned} hn &= hnh^{-1}h \\ &= (hnh^{-1})h \\ &\in NH \qquad \because \ hnh^{-1} \in N \\ \Longrightarrow \quad HN &\subseteq NH \qquad \text{.....(2)} \end{aligned}$$

مساوات(1)اور(2)کی مدد سے معلوم ہوتا ہے کہ $NH = HN$

قضیہ ثابت ہوا۔

قضیہ6۔ ابیلین گروپ کا ہر تحت گروپ نارمل ہو گا۔

ثبوت۔ فرض کرو کہ G ایک ابیلین گروپ ہے اور H اس کا تحت گروپ ہے۔تب ہمیں ثابت کرنا ہے کہ H نارمل تحت گروپ ہو گا۔

فرض کرو کہ $x \in G$ اور $h \in H$ اور $e \in G$ اکائی ہے۔تب غور کرو کہ چوں کہ G ایک ابیلین گروپ ہے اس لیے

$$\begin{aligned} xhx^{-1} &= h(xx^{-1}) \\ &= he \\ &= h \in H \end{aligned}$$

چنانچہ

$$xhx^{-1} \in H, \forall x \in G \ \& \ \forall h \in H$$

لہٰذا ثابت ہوا کہ ابیلین گروپ کا ہر تحت گروپ نارمل ہو گا۔

مثال1۔ اگر G ایک گروپ ہے اور $N = \{x \in G \ / \ ax = xa, \forall a \in G\}$ تب ثابت کرو کہ N نارمل ہے۔

ثبوت۔ دیا گیا ہے کہ G ایک گروپ ہے اور

$$N = \{x \in G \ / \ ax = xa, \forall a \in G\}$$

پہلے ہم یہ ثابت کریں گے کہ N ایک تحت گروپ ہے۔ جس کے لیے ہم یہ ثابت کریں گے کہ اگر $x_1, x_2 \in N$ تب $x_1 x_2^{-1} \in N$

لہٰذا اگر $x_1, x_2 \in N$ تب $\forall a \in G$

$$ax_1 = x_1 a$$

اور

$$ax_2 = x_2 a$$

ہوگا۔

غور کرو کہ

$$\begin{aligned} & ax_2 = x_2 a \\ \Rightarrow \quad & x_2^{-1}(ax_2)x_2^{-1} = x_2^{-1}(x_2 a)x_2^{-1} \\ \Rightarrow \quad & (x_2^{-1}a)(x_2 x_2^{-1}) = (x_2^{-1}x_2)(ax_2^{-1}) \\ \Rightarrow \quad & (x_2^{-1}a)e = e(ax_2^{-1}) \\ \Rightarrow \quad & x_2^{-1}a = ax_2^{-1} \\ \Rightarrow \quad & x_2^{-1} \in N \end{aligned}$$

اب

$$\begin{aligned} (x_1 x_2^{-1})a &= x_1(x_2^{-1}a) \\ &= x_1(ax_2^{-1}) \\ &= (x_1 a)x_2^{-1} \\ &= (ax_1)x_2^{-1} \\ &= a(x_1 x_2^{-1}) \\ \Rightarrow \quad x_1 x_2^{-1} &\in N, \quad \forall x_1, x_2 \in N \end{aligned}$$

چنانچہ یہ ثابت ہوا کہ N ایک تحت گروپ ہے۔ اب یہ بتانے کے لیے کہ N نارمل ہے، توجہ کرو $x \in N$ اور $a \in G$ تب

$$\begin{aligned} axa^{-1} &= (ax)a^{-1} \\ &= (xa)a^{-1} \\ &= x(aa^{-1}) \\ &= xe \\ &= x \in N \end{aligned}$$

لہٰذا ثابت ہوا کہ N گروپ G کا نارمل تحت گروپ ہے۔

مثال 2۔ اگر H گروپ G کا تحت گروپ ہے اور $N(H) = \{g \in G / gHg^{-1} = H\}$ تب ثابت کرو کہ

(1) $N(H)$ گروپ G کا تحت گروپ ہے

(2) H نارمل تحت گروپ ہے $N(H)$ کا اور

(3) H گروپ G کا نارمل تحت گروپ ہوگا اگر اور صرف اگر $N(H) = G$

ثبوت۔ دیا گیا ہے کہ H گروپ G کا ایک تحت گروپ ہے اور $N(H) = \{g \in G / gHg^{-1} = H\}$

(1) $N(H)$ کو G کا تحت گروپ ثابت کرنے کے لیے

فرض کرو کہ $a, b \in N(H)$ تب

$$bHb^{-1} = H \quad \& \quad aHa^{-1} = H$$

اب

$$\begin{aligned} & bHb^{-1} = H \\ \Longrightarrow \quad & b^{-1}(bHb^{-1})b = b^{-1}Hb \\ \Longrightarrow \quad & (b^{-1}b)H(b^{-1}b) = b^{-1}Hb \\ \Longrightarrow \quad & eHe = b^{-1}Hb \\ \Longrightarrow \quad & H = b^{-1}Hb \\ \Longrightarrow \quad & b^{-1} \in N(H) \end{aligned}$$

تب غور کرو

$$\begin{aligned} (ab^{-1})H(ab^{-1})^{-1} &= ab^{-1}Hba^{-1} \\ &= a(b^{-1}Hb)a^{-1} \\ &= aHa^{-1} \\ &= H \\ \Longrightarrow \quad ab^{-1} &\in N(H) \end{aligned}$$

لہٰذا ثابت ہوا کہ $N(H)$ گروپ G کا تحت گروپ ہے۔

(2) یہ ثابت کرنے کے لیے کہ H تحت گروپ $N(H)$ کا نارمل تحت گروپ ہے فرض کرو کہ $h \in H$ تب

$$\begin{aligned} & hHh^{-1} = H \\ \Longrightarrow \quad & h \in N(H) \\ \Longrightarrow \quad & H \subseteq N(H) \end{aligned}$$

اور H تحت گروپ ہے $N(H)$ کا

اب H کو نارمل ثابت کرنے کے لیے فرض کرو کہ

$x \in N(H)$ تب

$$xHx^{-1} = H$$

اس سے یہ ثابت ہوا کہ H نارمل ہے۔

(3) یہ ثابت کرنے کے لیے کہ H گروپ G کا نارمل تحت گروپ ہے اگر اور صرف اگر $N(H) = G$

فرض کرو کہ H گروپ G کا نارمل تحت گروپ ہے، تب ہمیں ثابت کرنا ہوگا کہ $N(H) = G$

اب فرض کرو کہ $x \in G$ تب H کے نارمل ہونے کی وجہ سے

$$\begin{aligned} & xHx^{-1} = H \\ \Longrightarrow \quad & x \in N(H) \\ \Longrightarrow \quad & G \subseteq N(H) \end{aligned}$$

اور چوں کہ $N(H) \subseteq G$

$$\Longrightarrow \quad N(H) = G$$

بالعکس اگر $N(H) = G$ تو ہمیں ثابت کرنا ہوگا کہ H نارمل ہے G میں۔

فرض کرو کہ $x \in G$ تب $x \in N(H)$

تو پھر

$$xHx^{-1} = H$$

اس لیے H نارمل ہے۔ یہی ثابت کرنا تھا۔

مثال3۔ ثابت کرو کہ $SL(2,\mathbb{R}) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} / ad - bc = 1, a, b, c, d \in \mathbb{R}\right\}$ ایک نارمل تحت گروپ ہے گروپ $GL(2,\mathbb{R}) = \left\{\begin{bmatrix} p & q \\ r & s \end{bmatrix} / pq - rs \neq 0,\ p, q, r, s \in \mathbb{R}\right\}$ کے لیے۔

ثبوت۔ ہمیں معلوم ہے کہ $SL(2,\mathbb{R})$ ایک تحت گروپ ہے $GL(2,\mathbb{R})$ کا

اب اسے نارمل ثابت کرنا ہوگا

فرض کرو کہ $P \in SL(2,\mathbb{R})\ \&\ A \in GL(2,\mathbb{R})$ تب

$$det\, P = 1\ \&\ det\, A \neq 0$$

توجہ کرو کہ

$$\begin{aligned} det(APA^{-1}) &= det\, A\, det\, P\, (det\, A)^{-1} \\ &= det\, A \cdot 1 \cdot (det\, A)^{-1} \\ &= det\, A \cdot (det\, A)^{-1} \\ &= 1 \\ \Longrightarrow \qquad & APA^{-1} \in SL(2,\mathbb{R}) \end{aligned}$$

اس لیے $SL(2,\mathbb{R})$ نارمل ہے۔

ثابت ہوا۔

مثال4۔ اگر $H = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} / ad \neq 0, a, b, d \in \mathbb{R}\right\}$ ہو تو معلوم کرو کہ آیا H گروپ $GL(2,\mathbb{R})$ کا نارمل تحت گروپ ہے۔

حل۔ ہم جانتے ہیں کہ $GL(2,\mathbb{R}) = \left\{\begin{bmatrix} p & q \\ r & s \end{bmatrix} / pq - rs \neq 0,\ p, q, r, s \in \mathbb{R}\right\}$ ضربی گروپ ہے تب ظاہر ہے کہ $H = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} / ad \neq 0, a, b, d \in \mathbb{R}\right\}$ اس کا تحت سٹ ہوگا۔

اگر $a = 1 = d, b = 0$ لیے جائیں تب

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$$

یعنی اکائی موجود ہے، اس لیے $H \neq \phi$ اور $H \subseteq GL(2,\mathbb{R})$

اگر $A = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}\ \&\ B = \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \in H$ تب $a_1 d_1 \neq 0,\ a_2 d_2 \neq 0$

اب

$$\begin{aligned} B^{-1} &= \frac{adj\, B}{det\, B} \\ &= \frac{1}{a_2 d_2} \begin{bmatrix} d_2 & -b_2 \\ 0 & a_2 \end{bmatrix},\ a_2 d_2 \neq 0 \end{aligned}$$

تب غور کرو کہ

$$AB^{-1} = \frac{1}{a_2d_2}\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}\begin{bmatrix} d_2 & -b_2 \\ 0 & a_2 \end{bmatrix}$$
$$= \frac{1}{a_2d_2}\begin{bmatrix} a_1d_2 & -a_1b_2 + a_2b_1 \\ 0 & a_2d_1 \end{bmatrix} \in H$$

اس لیے H گروپ $GL(2,\mathbb{R})$ کا تحت گروپ ہے۔

اب نارمل ثابت کرنے کے لیے فرض کرو کہ $M = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL(2,\mathbb{R})$

تب بایاں ہم سٹ

$$MH = \left\{MN/N = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, ad \neq 0, a, b, d \in \mathbb{R}\right\}$$
$$= \left\{\begin{bmatrix} pa & pb + qd \\ ra & rb + sd \end{bmatrix}/pa(rb + sd) \neq 0, \quad p, q, r, s\ a, b, d \in \mathbb{R}\right\}$$

اور دایاں ہم سٹ

$$HM = \left\{NM/N = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, ad \neq 0, a, b, d \in \mathbb{R}\right\}$$
$$= \left\{\begin{bmatrix} ap + br & aq + bs \\ dr & ds \end{bmatrix}/(ap + br)ds \neq 0,\ p, q, r, s\ a, b, d \in \mathbb{R}\right\}$$

چوں کہ $MH \neq HM$ یعنی دایاں اور بایاں ہم سٹ برابر نہیں ہے۔

لہٰذا H نارمل تحت گروپ نہیں ہے۔

قضیہ 7۔ اگر M اور N دو نارمل تحت گروپس ہیں کسی گروپ G کے اور $M \cap N = \{e\}$ تب M ہر عنصر N کے ہر عنصر کے ساتھ تقلیبی خاصیت پوری کرتا ہے۔

ثبوت۔ دیا گیا ہے کہ M اور N کسی گروپ G کے دو نارمل تحت گروپس ہیں اور $M \cap N = \{e\}$

فرض کرو کہ $m \in M$ اور $n \in N$

تب ثابت کرنا ہے کہ $mn = nm$

اور یہ بھی ہوگا کہ $m^{-1} \in M$ اور $n^{-1} \in N$

اور $M \subseteq G, N \subseteq G$ ہونے کی وجہ سے $m, m^{-1}, n, n^{-1} \in G$

اب M نارمل ہونے کی وجہ سے ہم کہہ سکتے ہیں کہ $nmn^{-1} \in M$

اور پھر ثنائی خاصیت کی بنا پر

$$nmn^{-1}m^{-1} \in M \qquad \text{.....(1)}$$

اور N نارمل ہونے کی وجہ سے $mn^{-1}m^{-1} \in N, \quad \because n^{-1} \in N,\ m \in G$

اور پھر ثنائی خاصیت کی بنا پر

$$nmn^{-1}m^{-1} \in N \qquad \text{.....(2)}$$

مساوات (1) اور (2) کی مدد سے

$$
\begin{aligned}
& nmn^{-1}m^{-1} \in M \cap N = \{e\} \\
\Rightarrow \quad & nmn^{-1}m^{-1} = e \\
\Rightarrow \quad & nmn^{-1}m^{-1}m = em \\
\Rightarrow \quad & nmn^{-1}e = m \\
\Rightarrow \quad & nmn^{-1} = m \\
\Rightarrow \quad & nmn^{-1}n = mn \\
\Rightarrow \quad & nme = mn \\
\Rightarrow \quad & nm = mn
\end{aligned}
$$

قضیہ ثابت ہوا۔

قضیہ 8۔ اگر N اور H کسی گروپ G کے دو نارمل تحت گروپس ہیں تو NH بھی ایک نارمل تحت گروپ ہو گا۔

ثبوت۔ فرض کرو کہ $e \in G$ اکائی عنصر ہے تو پھر $e \in H, e \in N$

اور $NH = \{nh/n \in N, h \in H\}$

$NH \neq \phi \quad [\because e = e \cdot e \in NH]$

فرض کرو کہ $x, y \in NH$

تب فرض کرو کہ

$x = n_1h_1, n_1 \in N, h_1 \in H$

اور $y = n_2h_2, n_2 \in N, h_2 \in H$

اب غور کرو کہ

$$
\begin{aligned}
x^{-1}y &= (n_1h_1)^{-1}(n_2h_2) \\
&= \left(h_1{}^{-1}n_1{}^{-1}\right)(n_2h_2) \\
&= \left(h_1{}^{-1}n_1{}^{-1}n_2\right)(h_2) \\
&= h_1{}^{-1}(n_1{}^{-1}n_2)\left(h_1h_1{}^{-1}\right)h_2 \left[\because h_1h_1{}^{-1} = e\right] \\
&= \left\{h_1{}^{-1}(n_1{}^{-1}n_2)h_1\right\}\left(h_1{}^{-1}h_2\right) \in NH, [\because n_1{}^{-1}n_2 \in N]
\end{aligned}
$$

اور N نارمل ہے اور $h_1{}^{-1}h_2 \in H$

اس سے اخذ ہوتا ہے کہ NH ایک تحت گروپ ہے۔

اب ہم نارمل کی شرط دیکھتے ہیں

فرض کرو کہ $p \in NH \quad \& \quad g \in G$ جب کہ $p = nh$

اب

$$
\begin{aligned}
gpg^{-1} &= g(nh)g^{-1} \\
&= gn(g^{-1}g)hg^{-1} \\
&= (gng^{-1})(ghg^{-1}) \in NH
\end{aligned}
$$

چنانچہ یہ ثابت ہوا کہ NH نارمل تحت گروپ ہے۔

نوٹ: قضیہ بالا میں تحت گروپ ثابت کرنے کے لیے $xy^{-1} \in NH$ ثابت کرنے کی بجائے $x^{-1}y \in NH$ ثابت کیا گیا سہولت کی

خاطر جو کہ یوں بھی لیا جا سکتا ہے۔

قضیہ 9۔ اگر H کسی گروپ G میں تحت گروپ ہے اور $a \in G$ تب $aHa^{-1} = \{aha^{-1} / h \in H\}$ تحت گروپ ہو گا G کا۔

ثبوت۔ فرض کرو کہ $e \in G$ اکائی عنصر ہے، تب $e = aea^{-1} \in aHa^{-1}$

لہٰذا $aHa^{-1} \neq \phi$

فرض کرو کہ $x, y \in aHa^{-1}$

تب فرض کرو کہ

$$x = ah_1a^{-1} \ \& \ y = ah_2a^{-1}, \forall h_1, h_2 \in H$$

اب توجہ کرو کہ

$$\begin{aligned} xy^{-1} &= (ah_1a^{-1})(ah_2a^{-1})^{-1} \\ &= (ah_1a^{-1})\left(ah_2{}^{-1}a^{-1}\right) \\ &= (ah_1)(a^{-1}a)\left(h_2{}^{-1}a^{-1}\right) \\ &= (ah_1)(e)\left(h_2{}^{-1}a^{-1}\right) \\ &= a\left(h_1h_2{}^{-1}\right)a^{-1} \in aHa^{-1}, \left[\because h_1h_2{}^{-1} \in H\right] \end{aligned}$$

چنانچہ یہ ثابت ہوا کہ aHa^{-1} تحت گروپ ہے G کا۔

تبصرہ: aHa^{-1} کو H کا مزدوج تحت گروپ (Conjugate Subgroup) کہتے ہیں۔ عام طور پر $aHa^{-1} \neq H$ تاہم اگر $aHa^{-1} = H, \forall a \in G$ ہو جایے تب H نارمل ہوتا ہے یا خود زوجی (Self- Conjugate) یا غیر متغیر (Invariant) تحت گروپ ہوتا ہے۔

قضیہ 10۔ اگر G ایک گروپ ہے اور H اس کا تحت گروپ ہے جس کا اشاریہ 2 ہے $(Index = 2)$ تب نارمل تحت گروپ ہوتا ہے۔

ثبوت۔ دیا گیا ہے کہ H تحت گروپ ہے گروپ G کا

اور H کا اشاریہ 2 ہے

یعنی H کے دو ہی مختلف ہم سٹس ہوں گے دائیں یا بائیں۔ ہمیں ثابت کرنا ہے کہ H نارمل ہو گا۔

فرض کرو کہ $x \in G$

تب دو دائیں ہم سٹس H, Hx ہوں گے

اور دو بائیں ہم سٹس H, xH ہوں گے

اب ممکن یہ ہے کہ $x \in H$ ہو گا یا $x \notin H$ ہو گا۔

اگر $x \in H$ ہو، تب

$$xH = H = Hx$$

یعنی بائیں اور دائیں ہم سٹس مساوی ہیں

لہٰذا H نارمل تحت گروپ ہوگا

اور اگر $x \notin H$ ، تب

$$Hx \neq H \ \& \ xH = H$$

اور چوں کہ H کا اشاریہ 2 ہے اس لیے

$G = H \cup Hx = H \cup xH$ ہو جانا چاہیے

اس لیے

$$Hx = xH$$

لہٰذا پھر ثابت ہوتا ہے کہ H نارمل تحت گروپ ہے۔

چنانچہ قضیہ ثابت ہوا۔

خارج قسمت گروپ/ضربی گروپ(Quotient Group/Factor Group)

تعریف: اگر $(G,\cdot)$ گروپ ہے اور H اس کا نارمل تحت گروپ ہے تب H کے تمام ہم سٹس کا سٹ $\frac{G}{H} = \{Hx \ / \ x \in G\}$ جو کہ گروپ ہوتا ہے ہم سٹس کے ضرب کے ثنائی عمل کے تحت یعنی $Ha \cdot Hb = Hab, \forall Ha, Hb \in \frac{G}{H}$

$\frac{G}{H}$ خارج قسمت گروپ/مخروجی گروپ کہلاتا ہے۔

نوٹ: چوں کہ H نارمل تحت گروپ ہے اس لیے اس کے دائیں یا بائیں ہم سٹس میں فرق نہیں ہوتا ہے۔

لہٰذا $\frac{G}{H} = \{xH \ / \ x \in G\}$ بھی لیا جا سکتا ہے جہاں $aH \cdot bH = abH, \forall a, b \in G$

قضیہ 11۔ اگر G گروپ ہے اور H اس کا نارمل تحت گروپ ہے تب H کے تمام ہم سٹس کا سٹ $\frac{G}{H} = \{Hx \ / \ x \in G\}$ ہم سٹس کے ضرب کے ثنائی عمل کے تحت گروپ ہوتا ہے۔

ثبوت۔ دیا گیا ہے کہ G گروپ ہے اور H اس کا نارمل تحت گروپ ہے

اور $\frac{G}{H} = \{Hx \ / \ x \in G\}$

ہمیں ثابت کرنا ہے کہ $\frac{G}{H}$ گروپ ہوتا ہے ہم سٹس کے ضرب ثنائی عمل سے

1. **بند شی خاصیت**(Closure Property): فرض کرو کہ $Ha, Hb \in \frac{G}{H}, a, b \in G$

تب $HaHb = Hab \in \frac{G}{H}$ $[\because a, b \in G \implies ab \in G]$

لہٰذا بند شی خاصیت پوری ہوئی

2. **تلازمی خاصیت**(*Associative Property*): اگر $Ha, Hb, Hc \in \frac{G}{H}, a, b \in G$

تب

$$\begin{aligned} Ha(Hb \cdot Hc) &= Ha \cdot H(bc) \\ &= Ha(bc) \\ &= H(ab)c \end{aligned}$$

$$= Hab \cdot Hc$$
$$= (Ha \cdot Hb)Hc$$

تلازمی خاصیت بھی پوری ہوئی

3. **اکائی کا وجود**(Existence of Unity): چوں کہ G گروپ ہے۔فرض کرو کہ $e \in G$ اکائی ہے،تب $He \in \frac{G}{H}$ اس طرح سے کہ

$$HaHe = Hae = Ha, \forall Ha \in \frac{G}{H}$$

اس سے ثابت ہوا کہ $He \in \frac{G}{H}$ اس کی اکائی ہے۔

4. **معکوس کا وجود**(Existence of Inverse): G گروپ ہونے کی وجہ سے

$$\forall a \in G \Longrightarrow a^{-1} \in G$$

اس لیے

$$Ha, Ha^{-1} \in \frac{G}{H}$$

تب

$$Ha \cdot Ha^{-1} = Haa^{-1} = He$$
$$\Longrightarrow (Ha)^{-1} = Ha^{-1} \in \frac{G}{H}$$

اس سے معلوم ہوا کہ $\frac{G}{H}$ کے ہر عنصر Ha کا معکوس $\frac{G}{H}$ میں موجود ہے۔

چوں کہ گروپ کی تمام شرائط پر پوری ہوئیں۔ اس لیے ثابت ہوا کہ $\frac{G}{H}$ گروپ ہے۔

نوٹ: $O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)}$

قضیہ 12۔ ہر ابیلین گروپ کا خارج قسمت گروپ ابیلین ہوتا ہے۔

ثبوت۔ فرض کرو کہ G ابیلین گروپ ہے اور H اس کا تحت گروپ ہے۔تب H نارمل تحت گروپ ہوتا ہے، چوں کہ ابیلین گروپ کا ہر تحت گروپ نارمل ہوتا ہے۔

فرض کرو کہ $\frac{G}{H}$ خارج قسمت گروپ ہے

ہمیں ثابت کرنا ہے کہ $\frac{G}{H}$ ابیلین ہوگا

فرض کرو کہ $a, b \in G$ تب

$$Ha, Hb \in \frac{G}{H}$$

پھر

$$Ha \cdot Hb = Hab$$
$$= Hba \qquad [\because ab = ba, \forall a, b \in G]$$
$$= Hb \cdot Ha$$

لہٰذا ثابت ہوا کہ $\frac{G}{H}$ ابیلین ہے۔

نوٹ: اگر $(G,+)$ گروپ ہے اور H اس کا نارمل تحت گروپ ہے تب خارج قسمت گروپ $\frac{G}{H}=\{H+x\ /\ x\in G\}$ ہوگا اور یہاں ثنائی عمل اس طرح ہوگا

$$(H+a)+(H+b)=H+(a+b)$$

اس کی اکائی

$$H+e\in\frac{G}{H}$$

معمولی جمع کی صورت میں $0\in G$ ہوتا ہے چنانچہ $H+0=H\in\frac{G}{H}$ اکائی ہوتا ہے۔

تصدیق:

$$\begin{aligned}(H+a)+(H+0)&=H+(a+0)\\&=H+a\end{aligned}$$

اور معکوس $H+a\in\frac{G}{H}$ کے لیے

$$\begin{aligned}(H+a)+\{H+(-a)\}&=H+\{a+(-a)\}\\&=H+0\end{aligned}$$

یعنی $(H+a)^{-1}=H+(-a)$ ہوگا۔

مثال5۔ اگر $(\mathbb{Z},+)$ گروپ ہے اور $3\mathbb{Z}$ تحت گروپ ہے۔ $\frac{\mathbb{Z}}{3\mathbb{Z}}$ معلوم کرو۔

حل۔ تب $\mathbb{Z}$ ابیلین ہوتا ہے لہٰذا $3\mathbb{Z}$ نارمل تحت گروپ ہوگا۔

لہٰذا $\frac{G}{H}=\frac{\mathbb{Z}}{3\mathbb{Z}}=\{3\mathbb{Z},3\ \mathbb{Z}+1,3\mathbb{Z}+2\}$

چوں کہ

$$\begin{aligned}\mathbb{Z}&=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}\\3\mathbb{Z}&=\{\cdots,-6,-3,0,3,6,9,\cdots\}\\3\mathbb{Z}+1&=\{\cdots,-5,-2,1,4,7,10,\cdots\}\\3\mathbb{Z}+2&=\{\cdots,-4,-1,2,5,8,11,\cdots\}\\3\mathbb{Z}+3&=\{\cdots,-9,-6,-3,0,3,6,9,\cdots\}=3\mathbb{Z}\end{aligned}$$

اسی طرح

$$\begin{aligned}3\mathbb{Z}+4&=3\mathbb{Z}+1\\3\mathbb{Z}+5&=3\mathbb{Z}+2\\\vdots\quad&\quad\vdots\quad\quad\vdots\end{aligned}$$

اور یہ $\left(\frac{\mathbb{Z}}{3\mathbb{Z}},+\right)$ خارج قسمت گروپ ہوتا ہے جس کی شرائط حسب ذیل جدول سے تصدیق کی جاسکتی ہیں:

$+$	$3\mathbb{Z}$	$3\mathbb{Z}+1$	$3\mathbb{Z}+2$
$3\mathbb{Z}$	$3\mathbb{Z}$	$3\mathbb{Z}+1$	$3\mathbb{Z}+2$
$3\mathbb{Z}+1$	$3\mathbb{Z}+1$	$3\mathbb{Z}+2$	$3\mathbb{Z}$
$3\mathbb{Z}+2$	$3\mathbb{Z}+2$	$3\mathbb{Z}$	$3\mathbb{Z}+1$

جدول بند شی خاصیت کو صاف ظاہر کرتا ہے کہ ہر نتیجہ $3\mathbb{Z}$ کا عنصر ہے جس میں اکائی $3\mathbb{Z}$ ہے۔

اور

$3\mathbb{Z}$ کا معکوس $3\mathbb{Z}$ ہے

$(3\mathbb{Z}+1)$ کا معکوس $(3\mathbb{Z}+2)$ ہے

$(3\mathbb{Z}+2)$ کا معکوس $(3\mathbb{Z}+1)$ ہے

اور تلازمی خاصیت بھی پوری ہو گی۔

چوں کہ گروپ کی تمام شرائط پوری ہوتی ہیں۔اس لیے $\left(+,\frac{\mathbb{Z}}{3\mathbb{Z}}\right)$ خارج قسمت گروپ ہے۔

مثال6۔ اگر $G=\mathbb{Z}_{18}$ گروپ ہے بزریعہ جمع بہ مقیاس 18 اور $H=(6)=\{0,6,12\}$ تحت گروپ ہے۔تب $\frac{G}{H}$ معلوم کرو۔

حل۔ دیا گیا ہے کہ $G=\mathbb{Z}_{18}=\{0,1,2,3,\cdots,17\}+_{18}$

اور $H=(6)=\{0,6,12\}$

تب $O\left(\frac{G}{H}\right)=\frac{O(G)}{O(H)}=\frac{18}{3}=6$

اور 6 مختلف ہم سٹس درج ذیل ہوں گے:

$$\frac{G}{H}=\frac{\mathbb{Z}_{18}}{(6)}=\{H+0,H+1,H+2,H+3,H+4,H+5\}$$

باقی اور جو ہم سٹس $H+6, H+7$ وغیرہ بنیں گے وہ ان ہی میں سے کسی کسی کے مماسل ہوں گے

مثال7۔ اگر $G=U(32)=\{1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31\}$ اور $H=(16)=\{1,17\}$ تب خارج قسمت گروپ $\frac{G}{H}$ معلوم کرو۔

حل۔ $\frac{G}{H}$ کا رتبہ $O\left(\frac{G}{H}\right)=\frac{O(G)}{O(H)}=\frac{16}{2}=8$

اور یاد رہے کہ $U(32)$ گروپ بزریعہ ضرب ہوتا ہے بہ مقیاس 32

اس لیے $\frac{G}{H}=\{1H,3H,5H,7H,9H,11H,13H,15H\}$ عناصر ہوں گے۔

مثال8۔ ضربی گروپ $\frac{\mathbb{Z}_{60}}{(5)}$ کا رتبہ معلوم کرو۔

حل۔ ہمیں معلوم ہے کہ

$$\mathbb{Z}_{60}=\{0,1,2,3,\cdots,59\}$$

اور $|\mathbb{Z}_{60}|=60$

اور

$$(5)=\{0,5,10,15,20,25,30,35,40,45,50,55\}$$
$$|(5)|=12$$

$\frac{\mathbb{Z}_{60}}{(5)}$ کا رتبہ

$$O\left(\frac{\mathbb{Z}_{60}}{(5)}\right) = \frac{O(\mathbb{Z}_{60})}{O(5)} = \frac{60}{12} = 5$$

نارمل گر(Normalizer):

فرض کرو کہ G ایک گروپ ہے تب $a \in G$ کا نارمل گر(Normalizer) G کے وہ عناصر ہیں جو a سے تقلیب کرتے ہیں۔اس کو $N[a]$ سے تعبیر کرتے ہیں یعنی $N[a] = \{x \in G / xa = ax\}$

گروپ کا مرکز(Centre of a Group):

فرض کرو کہ G ایک گروپ ہے تب G کا مرکز G کے ان عناصر کا سٹ ہے جو G کے ہر عنصر سے تقلیب(Commutate) کرتے ہیں۔ اس کو $\mathbb{Z}(G)$ سے تعبیر کرتے ہیں یعنی $\mathbb{Z}(G) = \{x \in G / ax = xa, \forall a \in G\}$

قضیہ 13۔ کسی گروپ G کا مرکز نارمل تحت گروپ ہوتا ہے۔

ثبوت۔ اس کا ثبوت مثال 1 میں دیا گیا ہے۔

قضیہ 14۔ اگر G ایک گروپ ہے اور $a \in G$ تب a کا نارمل گر(Normalizer) $N[a]$ تحت گروپ ہوتا ہے G کا اور اگر $a \in \mathbb{Z}(G)$ (یعنی مرکز میں ہو) تب $N[a] = G$

ثبوت۔ فرض کرو کہ $e \in G$ اکائی ہے

ہمیں معلوم ہے کہ $N[a] = \{x \in G / xa = ax\}$ جہاں $a \in G$

اور $\mathbb{Z}(G) = \{x \in G / ax = xa, \forall a \in G\}$ یا $\mathbb{Z}(G) = \{a \in G / ax = xa, \forall x \in G\}$

چوں کہ $ae = ea$ ہوتا ہے،اس لیے $e \in N[a]$ چنانچہ $N[a] \neq \phi$

فرض کرو کہ $x, y \in N[a]$ تب $ay = ya$ اور $ax = xa$ ہوگا

تب غور کرو کہ

$$\begin{aligned} a(xy) = (ax)y = (xa)y &= x(ay) \\ &= x(ya) \\ &= (xy)a \end{aligned}$$

لہٰذا $xy \in N[a]$ .....(1)

اور پھر

$$\begin{aligned} & ax = xa \\ \Rightarrow\ & x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} \\ \Rightarrow\ & x^{-1}a(xx^{-1}) = (x^{-1}x)ax^{-1} \\ \Rightarrow\ & x^{-1}a(e) = (e)ax^{-1} \\ \Rightarrow\ & x^{-1}a = ax^{-1} \end{aligned}$$

لہٰذا $x^{-1} \in N[a]$ .....(2)

مساوات(1) اور(2) کی مدد سے یہ اخذ ہوتا ہے کہ $N[a]$ گروپ G کا تحت گروپ ہے۔

اب اگر $a \in \mathbb{Z}(G)$ تب ہر $x \in G$ کے لیے $ax = xa$ ہوگا۔

اس لیے $N[a] = G$

اس کے بالعکس اگر $a \in G$ اس طرح ہے کہ $N[a] = G$ ہے۔

تب $x \in G$ کے لیے $ax = xa$ تو پھر $a \in \mathbb{Z}(G)$

لہٰذا $N[a] = G$

قضیہ ثابت ہوا۔

تبصرہ: اگر G متناہی گروپ ہے اور $a \in \mathbb{Z}(G)$ تب $O(N[a]) = O(G)$ ہوگا۔

نوٹ:

$$\mathbb{Z}(G) = \bigcap_{a \in G} N[a]$$

مزدوج اور جماعتی مساوت(Conjugate and Class Equation):

فرض کرو کہ G ایک گروپ ہے اور $a \in G$ تب $b \in G$ کو a کا مزدوج کہا جاتا ہے اگر کسی $x \in G$ کے لیے $b = xax^{-1}$ ہو۔

قضیہ 15۔ ایک گروپ کے عناصر میں مزدوج ہونے کا رشتہ معادلی رشتہ ہوتا ہے۔

ثبوت۔ ہمیں معلوم ہے کہ کسی رشتہ کو معادل ہونے کے لیے تین شرائط پوری ہونی چاہیے:

(1) رجعی(Reflexive)

(2) تشاکل(Symmetric)

(3) انتقال پزیر(Transitive)

(1) چوں کہ $e \in G$ اکائی ہے تب $a = eae^{-1}$ صحیح ہے

اس لیے aRa یعنی رشتہ رجعی ہے

(2) فرض کرو کہ aRb تب کسی $x \in G$ کے لیے $b = xax^{-1}$ ہوگا

پھر چوں کہ $x^{-1} \in G$ اس لیے

$$\begin{aligned} x^{-1}bx &= x^{-1}(xax^{-1})x \\ &= (x^{-1}x)a(x^{-1}x) \\ &= eae \\ &= a \\ \Longrightarrow \quad & bRa \end{aligned}$$

لہٰذا رشتہ تشاکل ہے۔

(3) اگر فرض کریں کہ aRb اور bRc ہو تب

$\exists x \in G$ کہ $b = xax^{-1}$

اور $\exists y \in G$ کہ $c = yby^{-1}$ ہوگا

پھر

$$\begin{aligned} c &= yby^{-1} \\ &= y(xax^{-1})y^{-1} \\ &= (yx)a(x^{-1}y^{-1}) \\ &= (yx)a(yx)^{-1} \qquad [\because\ yx \in G] \\ \Rightarrow \quad & aRc \end{aligned}$$

یعنی رشتہ انتقال پزیر ہے۔

چوں کہ تینوں شرائط پوری ہوگئی۔اس لیے یہ ثابت ہوا کہ مزدوج ہونے کا رشتہ معادلی ہے۔

مزدوج جماعت(Conjugate Class):

اگر G ایک گروپ ہے اور $a \in G$ تب a کی مزدوج جماعت (Conjugate Class) G کے ایسے عناصر کا سٹ ہے جو a کے مزدوج ہیں اور اس کو یوں ظاہر کیا جاتا ہے

$$C[a] = \{xax^{-1} \ / \ x \in G\}$$

تبصرہ(Remark): یاد رہے کہ ایک سٹ پر کوئی معادلی رشتہ سٹ کو باہم غیر مشترک معادلی جماعتوں میں تقسیم کرتا ہے۔چنانچہ گروپ G بھی غیر مشترک معادلی جماعتوں میں منقسم ہو جاتا ہے اور پھر

$$O(G) = O\left(\bigcup_{a \in G} C[a]\right)$$

یعنی G متناہی ہو تو مزدوج جماعتوں میں عناصر کی تعداد کا مجموعہ G کے رتبہ کے برابر ہوگا۔

تبصرہ(Remark):اگر G ایک ابیلین گروپ ہے اور $a \in G$ تب $x \in G$ کے لیے $xax^{-1} = xx^{-1}a = ea = a$ یعنی a کا مزدوج صرف a ہی ہوتا ہے۔لہٰذا a کی مزدوج جماعت میں صرف a ہی شامل ہوتا ہے۔ لہٰذا $C[a] = [a]$

اس کا مطلب یہ ہے کہ ایک ابیلین گروپ میں ہر عنصر خود ایک جداگانہ مزدوج جماعت ہے۔

قضیہ 16۔ اگر G ایک متناہی گروپ ہے اور $a \in G$ تب a کی مزدوج جماعت $C[a]$ میں عناصر کی تعداد $\frac{O(G)}{O(N[a])}$ یعنی $N[a]$ کے اشاریہ کے برابر ہوگی۔ مزید براں

$$O(G) = \sum_{a \in G} C[a]$$

ثبوت۔ غور کرو نقش $f: C[a] \to \{gN[a] \ / \ g \in G\}$ جہاں $f(x) = g \cdot N[a]$ اور $x = gag^{-1}$

تو ہم دیکھتے ہیں کہ f خوش معرف ہے۔

اگر $x \in C[a]$ اس طرح سے ہو کہ $x = gag^{-1} = hah^{-1}$ تب

$$\begin{aligned} & h^{-1}(gag^{-1})g = h^{-1}(hah^{-1})g \\ \Rightarrow \quad & h^{-1}ga = ah^{-1}g \\ \Rightarrow \quad & h^{-1}g \in N[a] \end{aligned}$$

یعنی $h \in gN[a]$ اور $gN[a] = hN[a]$

اب یہ بتانے کے لیے کہ f ایک ایک ہے،

فرض کرو کہ $x, y \in C[a]$ اور اگر $f(x) = f(y)$ تب کسی $g, h \in G$ کے لیے

$x = gag^{-1}$ اور $y = hah^{-1}$

$$\begin{aligned} &\Rightarrow \quad gag^{-1} = hah^{-1} \\ &\Rightarrow \quad x = y \end{aligned}$$

چنانچہ f ایک ایک ہے۔

اور اب یہ بتانے کے لیے کہ f برتفاعل (Onto Function) ہے فرض کرو کہ $g \in G$ تب

$$\begin{aligned} &ag = ga \\ &\Rightarrow \quad (ag)g^{-1} = (ga)g^{-1} \\ &\Rightarrow \quad a = gag^{-1} \end{aligned}$$

یعنی $gag^{-1} \in C[a]$ لہٰذا $f(gag^{-1}) = gN[a]$ لہٰذا f برتفاعل ہے

چنانچہ $O(C[a]) = O(N[a])$

لہٰذا $N[a]$ کا G میں اشاریہ $= \frac{O(G)}{O(N[a])}$ یا $O(G) = \sum_{a \in G} C[a]$

قضیہ ثابت ہوا۔

جماعتی مساوات (Class Equation):

فرض کرو کہ G ایک متناہی گروپ ہے۔ مساوات $O(G) = O(\mathbb{Z}(G)) + \sum_a \frac{O(G)}{O(N[a])}$ جہاں جمع کا عمل ایک سے زائد عناصر رکھنے والی ممیّز مزدوج جماعتوں میں سے ہر ایک سے ایک عنصر کو لے کر کیا جاتا ہے۔ گروپ G کی جماعتی مساوات (Class Equation) کا نام دیا گیا ہے۔ گویا

$$O(G) = \mathrm{c} + n_1 + n_2 + \cdots + n_r$$

جہاں پر c مرکز کے عناصر کی تعداد اور $n_1, n_2, \cdots, n_r$ غیر واجبی مزدوج جماعتوں میں عناصر کی تعداد ہے۔

مثال 9۔ فرض کرو کہ p ایک مفرد صحیح عدد (Prime Number) ہے اور گروپ G کا رتبہ p^n ہے۔ تب $O(\mathbb{Z}(G)) \geq 2$ یعنی ایک مفرد عدد کا کسی قوت والے رتبے کا گروپ غیر واجبی (Non Trivial) مرکز رکھتا ہے۔

حل۔ فرض کرو کہ $a \in G$ اور چوں کہ $N[a]$ گروپ G کا تحت گروپ ہے اور لگرانج کے قضیہ کے مطابق $O(N[a])/O(G)$ اور $O(G) = p^n$ ہے اور فرض کرو کہ $O(N[a]) = p^m$ جہاں $m \leq n$ مثبت صحیح عدد ہے۔ اگر $a \in \mathbb{Z}(G)$ تب $m = n$ ہوگا چوں کہ اس صورت میں $N[a] = G$ بصورت دیگر $e \in \mathbb{Z}(G)$ لہٰذا $O(\mathbb{Z}(G)) \geq 1$ تب جماعتی مساوات $p^n = c + \sum \frac{p^n}{p^m}$ جب کہ c مرکز کے عناصر کی تعداد ہے۔ چوں کہ p تقسیم کرتا ہے p^n کو اور اسی طرح p^{n-m} کو بھی تقسیم کرتا ہے۔ اس لیے p کو c کو بھی تقسیم کرنا ہوگا۔ اس لیے $c \neq 1$ اور $c \neq 0$ ہوگا لہٰذا $c \geq 2$ اور p سے قابل تقسیم ہوگا

لہٰذا $\mathbb{Z}(G)$ غیر واجبی(Non Trivial) ہے۔

ثابت کیا گیا۔

مثال10۔ اگر p ایک مفرد صحیح عدد(Prime Number)ہے اور G ایک گروپ ہے جس کا رتبہ p^2 ہے۔تب ثابت کرو کہ G ابیلین گروپ ہے۔

حل۔ ہمیں معلوم ہے کہ $\mathbb{Z}(G)$ غیر واجبی(Non Trivial) ہے۔

نیز $\mathbb{Z}(G)$ گروپ G کا تحت گروپ ہے اور $O(G) = p^2$ لہٰذا $O(\mathbb{Z}(G)) = p$ یا $O(\mathbb{Z}(G)) = p^2$ ہوگا۔ لگرانج کے قضیہ کی مدد سے چوں کہ $O(\mathbb{Z}(G))/O(G)$

اگر ممکن ہو تو فرض کرو کہ $O(\mathbb{Z}(G)) = p$ اور چوں کہ $O(G) = p^2$ لہٰذا $a \in G$ ایسا موجود ہوگا کہ $a \notin \mathbb{Z}(G)$

اب $N[a]$ پر توجہ دیں

$N[a]$ تحت گروپ ہے گروپ G کا اور $\mathbb{Z}(G) \subseteq N[a]$

چوں کہ $a \in N[a]$

اس لیے $O(N[a]) > p$

چوں کہ $O(N[a])/O(G)$

$$\implies \quad O(N[a]) = p^2$$
$$\implies \quad N[a] = G$$

لیکن اس سے اخذ ہوتا ہے کہ $a \in \mathbb{Z}(G)$ جو کہ ہمارے مفروضے $a \notin \mathbb{Z}(G)$ کے برعکس ہے لہٰذا $O(\mathbb{Z}(G)) \neq p$ اس سے ماخوذ ہوا کہ $O(\mathbb{Z}(G)) = p^2$ اور $G = \mathbb{Z}(G)$ اور G ابیلین ہے۔

ثابت کیا گیا۔

4.3 اکتسابی نتائج(Learning Outcomes)

اس اکائی میں ہم نے نارمل تحت گروپ کا تعارف پایا۔ یہ معلوم ہوا کہ کسی ابیلین گروپ کے تمام تحت گروپس نارمل ہوتے ہیں۔ نارمل تحت گروپ کا تقاطع بھی نارمل ہوتا ہے۔ نارمل تحت گروپ ہونے اور نہ ہونے والی مثالیں سامنے آئیں۔ دائیں اور بائیں ہم سٹس کے درمیان دوربطی تفاعل بنایا جاسکتا ہے جب کہ تحت گروپ نارمل ہو۔ مرکز اور طبعی گر کی تعریفات سامنے آئیں۔ ان کے تحت قضیے ثابت کیے گیے جو کہ دلچسپ معلومات رہیں۔ خارج قسمت گروپ، نارمل تحت گروپ کے ہم سٹس کا گروپ ہوتا ہے۔ دیے ہوئے نارمل تحت گروپ کے لیے خارج قسمت گروپ تشکیل دیا گیا۔ مزدوج اور جماعتی مساوات کو ہم نے جانا اور ثابت کیا کہ مزدوج رشتہ معادلی رشتہ ہوتا ہے۔ مزدوج جماعت میں عناصر کی تعداد کے ضابطے کو اخذ کیا گیا اور ثابت کیا گیا۔ جماعتی مساوات سے متعلق مثالوں کو حل کیا گیا۔ اس اکائی سے

متعلق تمام تعریفات کے تحت کئی دلچسپ قضیوں کو بیان کیا گیا اور ثابت کیا گیا۔ جہاں ضرورت ہو تبصرہ بھی لکھا گیا۔

4.4 کلیدی الفاظ (Keywords)

نارمل تحت گروپ، تقاطع، مرکز، برتفاعل، خارج قسمت گروپ، مزدوج، جماعتی مساوات، معادلی رشتہ

4.5 نمونہ امتحانی سوالات (Model Examination Questions)

4.5.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. نارمل تحت گروپ کی تعریف کرو۔
2. خارج قسمت گروپ کی تعریف کرو۔

4.5.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. ثابت کرو کہ ابیلین گروپ کا ہر تحت گروپ نارمل ہوگا۔
2. ثابت کرو کہ کسی گروپ کے دو نارمل تحت گروپ کا تقاطع بھی نارمل ہوگا۔
3. اگر $H = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} / ad \neq 0, a, b, d \in \mathbb{R}\right\}$ ہو تو معلوم کرو کہ آیا H گروپ $GL(2, \mathbb{R})$ کا نارمل تحت گروپ ہے۔

4.5.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. نارمل تحت گروپ کی تعریف کرو اور ثابت کرو کہ اگر H گروپ G کا تحت گروپ ہے تب H نارمل ہوگا اگر اور صرف اگر $xH = Hx, \forall x \in G$
2. اگر G ایک گروپ ہے تب اس کا کوئی بھی نارمل تحت گروپ G کے غیر خالی تحت سٹ کے ساتھ تقلیبی خاصیت پوری کرتا ہے۔ ثابت کرو۔
3. اگر G ایک گروپ ہے اور H اس کا نارمل تحت گروپ ہے تب ثابت کرو کہ $\frac{G}{H} = \{Hx \ / \ x \in G\}$ ہم سٹس کے ضرب کے ثنائی عمل کے تحت گروپ ہوتا ہے۔
4. اگر G ایک گروپ ہے اور $a \in G$ تب ثابت کرو کہ a کا نارمل گر (*Normalizer*) $N[a]$ تحت گروپ ہوتا ہے G کا اور اگر $a \in \mathbb{Z}(G)$ تب $N[a] = G$

جاوابات:

4.5.2 مختصر جوابات کے حامل سوالات کے جوابات

1. قضیہ 6 کو ملاحظہ کیجیے۔
2. قضیہ 4 کو ملاحظہ کیجیے۔

3. مثال 4 کو ملاحظہ کیجیے۔

4.5.3 طویل جوابات کے حامل سوالات کے جوابات

1. قضیہ 2 کو ملاحظہ کیجیے۔
2. قضیہ 5 کو ملاحظہ کیجیے۔
3. قضیہ 11 کو ملاحظہ کیجیے۔
4. قضیہ 14 کو ملاحظہ کیجیے۔

4.6 مزید مطالعے کے لیے تجویز کردہ کتابیں(Suggested Books for Further Readings)

1. Text Book of Differential Equations, Khalil Ahmad, Real World Education Publishers, New Delhi
2. Ordinary and Partial Differential Equations- Rai Singhania, S.Chand & Company, New Delhi
3. A Text Book of B.Sc. (Mathematics), Volume –I , V. Venkateshwara Rao and others, S. Chand & Company New Delhi

اکائی 5۔ مبادلہ گروپس اور سائکلی گروپس

(Permutation Groups and Cyclic Groups)

اکائی کے اجزا

5.0 تمہید(Introduction)

گروپس کے بارے میں پچھلی اکائیوں میں ہم نے گروپ، ابیلین گروپ، تحت گروپ، ہم سٹس اور نارمل تحت گروپ کو اچھی طرح جان لیا ہے۔ اس اکائی میں ہم گروپ کی ایک خاص قسم کو دیکھیں گے جنھیں سائکلی گروپ کہتے ہیں، جن کے سارے عناصر ایک عنصر کی مدد سے حاصل کیے جاتے ہیں۔ یہ سائکلی گروپ ہمیشہ ابیلین گروپ ہوتے ہیں۔ لیکن ہر ابیلین گروپ سائکلی نہیں ہوتا۔ سائکلی گروپ کا تحت گروپ بھی سائکلی ہوتا ہے۔ لا متناہی سائکلی گروپ کے صرف دو مولد (Generators) ہوتے ہیں۔

مبادلہ گروپ ایک متناہی سٹ کا نقش ہوتا ہے جو ایک ایک اور بر ہوتا ہے۔ کسی متناہی سٹ کے اگر n عناصر ہوں تو $n!$ مبادلے ممکن ہوتے ہیں۔ ان تمام مبادلوں کا سٹ ضربی عمل کے ذریعہ گروپ بناتا ہے۔ مبادلوں کو سائکلی مبادلوں میں ظاہر کیا جا سکتا ہے اور ان کو جابدلی (Transposition) کے ضرب سے بھی ظاہر کیا جا سکتا ہے۔ مبادلوں کا معکوس بھی معلوم کیا جائے گا۔

5.1 مقاصد(Objectives)

اس اکائی کی تکمیل کے بعد آپ اس قابل ہو جائیں گے کہ سائکلی گروپ کیا ہوتا ہے ان کی کیا خصوصیات ہوتی ہیں اور ان کے تحت گروپ کی خصوصیات اور دیے گیے سائکلی گروپ مولدوں کو معلوم کر سکیں گے اس کے علاوہ مبادلہ گروپ کی تعریف کر سکیں گے اور مبادلہ گروپس کے درمیان ضربی عمل کا حاصل معلوم کر سکیں۔ کسی متناہی سٹ سے مبادلہ گروپ کو بنانے کے قابل ہو جائیں گے۔ سائکلی مبادلہ کی پہچان ہو جائے گی۔ دیے ہوے مبادلے کو سائکلی مبادلوں کے حاصل ضرب پر ظاہر کیا جا سکے گا۔ طاق اور جفت مبادلات کو پہچان سکیں گے۔

5.2 سائکلی گروپ(Cyclic Group)

تعریف: اگر $(G,\cdot)$ ایک گروپ ہے اور $a \in G$ اگر اس طرح سے کہ $G = \{a^n \,/\, n \in \mathbb{Z}\}$ تب G کو سائکلی گروپ کہتے ہیں اور a کو G کا مولد (Generator) کہتے ہیں۔ اسے اس طرح ظاہر کیا جاتا ہے $G =< a >= (a)$ یا $G = \{a\}$ اس طرح اگر $(G,+)$ گروپ ہے ہو تب $a \in G$ مولد ہو تو

$$G =< a >= (a) = \{na \,/\, n \in \mathbb{Z}\}$$

مثال 1۔ اگر گروپ $G = \{1,-1,i,-i\}$ ضربی لیا جایے تب ہم دیکھیں گے کہ آیا G سائکلی ہے یا نہیں اور اس کے مولد کون ہیں۔

$$1^1 = 1, 1^2 = 1, 1^3 = 1$$

$1 \in G$ اکائی ہونے کی وجہ سے اس کی کوئی بھی قوت اکائی ہی ہوتی ہے اس لیے '1' مولد نہیں ہے۔

$$(-1)^1 = -1, (-1)^2 = 1, (-1)^3 = -1$$

لہٰذا (-1) صرف دو ہی عناصر $\{1,-1\}$ کی تخلیق کر سکتا ہے۔ اس لیے (-1) مولد نہیں ہے۔

$$(i)^1 = i, (i)^2 = -1, (i)^3 = (i)^2 i = -i, (i)^4 = (i)^2(i)^2 = (-1)(-1) = 1$$

یعنی دیکھا یہ گیا ہے کہ i کی مختلف قوتوں کے ذریعہ G کے تمام عناصر تخلیق پا رہے ہیں۔ لہٰذا 'i' مولد ہے اور G سائکلی گروپ ہے۔

اسی طرح یہ بھی پایا گیا کہ $(-i)$ بھی G کی تخلیق کرتا ہے لہٰذا $(-i)$ بھی G کے تمام عناصر کے لیے مولد ہے۔اس سے ہم اس نتیجہ پر پہنچے کہ G ایک سائکلی گروپ ہے اور اس کے دو مولد $i, (-i)$ ہیں۔

یعنی $G =< -i > \& G =< i >$

مثال2۔ 1 کے جذرالمکعب (*Cube Root of Unity*) کا ضربی گروپ $G = \{1, \omega, \omega^2\}$ جہاں $\omega^3 = 1$ ہوتا ہے، سائکلی گروپ ہے جس کے مولد ω, ω^2 ہے۔یعنی $G =< \omega >$ اور $G =< \omega^2 >$

مثال3۔ $(\mathbb{Z}, +)$ گروپ ہوتا ہے جو کہ سائکلی گروپ ہے اور اس کے مولد $1, (-1)$ ہیں۔اس لیے $\mathbb{Z} =< 1 >$ اور $\mathbb{Z} =< -1 >$ کیوں کہ

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

اور

$$\begin{aligned}\mathbb{Z} &= \{n(1) \,/\, n \in \mathbb{Z}\} \\ &= \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}\end{aligned}$$

اور اسی طرح

$$\begin{aligned}\mathbb{Z} &= \{n(-1) \,/\, n \in \mathbb{Z}\} \\ &= \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}\end{aligned}$$

جب کہ اور کوئی مولد نہیں ہو سکتا۔ مثلاً 2 پر غور کریں تو یہ صرف جفت (Even) اعداد تخلیق کرے گا۔ کیوں کہ

$$\begin{aligned}< 2 > &= \{n(2) \,/\, n \in \mathbb{Z}\} \\ &= \{\cdots, -4, -2, 0, 2, 4, \cdots\}\end{aligned}$$

اسی طرح اور کوئی بھی صحیح عدد کے مکررات $\mathbb{Z}$ کو تخلیق نہیں دے سکتے۔

لہٰذا $(\mathbb{Z}, +)$ سائکلی گروپ ہے جس کے صرف دو مولد $1, (-1)$ ہیں۔

نوٹ:

1. متناہی سائکلی گروپ کے صرف دو ہی مولد ہوتے ہیں۔
2. اگر $a \in G$ مولد ہے تب a^{-1} بھی مولد ہوگا۔اسی طرح اگر $a \in G$ مولد نہیں ہے تب a^{-1} بھی مولد نہیں ہوگا۔
3. اگر $a \in G$ اور $O(G) = O(a)$ ہے تب a مولد ہوگا۔
4. اگر $a \in G$ اور اگر $O(G) = n$ اور $O(a) = m$ اور اگر $(m, n) = 1$ تب a مولد ہوگا۔
5. $G = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$ باعمل جمع سائکلی گروپ ہوتا ہے، چوں کہ یہ لا متناہی ہے اس کے دو ہی مولد ہوں گے۔ وہ دو مولد 2 اور (-2) ہوں گے۔

$$\begin{aligned}< 2 > &= \{2n \,/\, n \in \mathbb{Z}\} \\ &= \{\cdots, -4, -2, 0, 2, 4, \cdots\} \\ < -2 > &= \{-2n \,/\, n \in \mathbb{Z}\} \\ &= \{\cdots, -4, -2, 0, 2, 4, \cdots\}\end{aligned}$$

لہٰذا $G =< 2 > \& G =< -2 >$

6. $(\mathbb{Q}, +)$ گروپ ہوتا ہے لیکن سائکلی گروپ نہیں ہوتا۔

مثال4۔ ثابت کرو کہ گروپ $G = \{1, 2, 3, 4\}$ بہ عمل $\otimes_5$ سائکلی گروپ ہے اور اس کے تمام مولد معلوم کرو۔

حل۔ دیا گیا ہے کہ $G = \{1, 2, 3, 4\}$

1 اکائی ہونے کی وجہ سے مولد نہیں ہے۔

$$2^1 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 3$$

چوں کہ 2 کی مختلف قوتیں G کے تمام عناصر کی تخلیق کرتے ہیں اس لیے 2 مولد ہے اور G سائکلی گروپ ہے۔ اور اسی طرح

$$3^1 = 3, 3^2 = 1, 3^3 = 4, 3^4 = 2$$

لہٰذا 3 بھی ایک مولد ہے۔ اور پھر

$$4^1 = 4, 4^2 = 3, 4^3 = 2, 4^4 = 1$$

4 کی قوتیں صرف 1 اور 4 کو تخلیق دے پا رہی ہیں اس لیے 4 مولد نہیں ہے۔ لہٰذا یہ معلوم ہوا کہ $(G, \otimes_5)$ سائکلی گروپ ہے جس کے دو مولد 2 اور 3 ہیں۔

نوٹ: $3 = (2)^{-1}$ کیوں کہ $2 \otimes_5 3 = 1$ اس لیے 3 بھی مولد لیا جا سکتا تھا۔ تمام قوتوں کے امتحان کی ضرورت نہیں تھی۔

مثال5۔ اگر $G = \{a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$ بہ عمل ضرب گروپ ہے تو اس کے تمام مولد معلوم کرو۔

حل۔ ہمیں معلوم ہے کہ اگر $O(G) = n$ تب کسی بھی عنصر اور $a^n = e$ تب a مولد ہوتا ہے اور کوئی اور عنصر a^m مولد ہوگا اگر $(m, n) = 1$ یہاں (m, n) کے معنی G.C.D.(اعاد اعظم مشترک) ہے۔

چنانچہ $(1,8) = 1$ اس لیے a^1 مولد ہے۔

لہٰذا $(a)^{-1} = a^7$ بھی مولد ہے کیوں کہ $a^1 a^7 = a^8 = e$

$$(2,8) \neq 1$$

اس لیے a^2 مولد نہیں ہے۔

کیوں کہ $(a^2)^{-1} = a^6$ بھی مولد نہیں ہے۔

کیوں کہ $(3,8) = 1$ اس لیے a^3 مولد ہے۔

اور $(a^3)^{-1} = a^5$ بھی مولد ہے۔

چنانچہ معلوم ہوا کہ G سائکلی گروپ ہے اور اس کے تمام مولد حسب ذیل ہیں

$$a^1, a^3, a^5, a^7$$

مثال6۔ اگر $G = \{1,2, 3, 4, 5,6\}$ بہ عمل $\times_7$ ہے، تب ثابت کرو کہ G سائکلی گروپ ہے اور اس کے تمام مولد معلوم کرو۔

حل۔ 1 اکائی ہونے کی وجہ سے مولد نہیں ہوگا۔ اور

$$2^1 = 2, 2^2 = 4, 2^3 = 1, 2^4 = 2$$

مکررات (Repetitions) آنے شروع ہو گیے ہیں۔ اور کیوں کہ تمام عناصر تخلیق نہیں پا سکے اس لیے 2 مولد نہیں ہے۔

لہٰذا $4 = (2)^{-1}$ بھی مولد نہیں ہے کیوں کہ $2 \times_7 4 = 1$

اور

$$3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$$

G کے تمام عناصر 3 کی مختلف قوتوں پر تخلیق پاگئے ہیں اس لیے $G =< 3 >$

تو پھر $5 = (3)^{-1}$ بھی مولد ہے کیوں کہ $2 \times_7 5 = 1$

اس لیے $G =< 5 >$ اور $6^1 = 6, 6^2 = 1, 6^3 = 6, 6^4 = 1$

اس لیے 6 مولد نہیں ہے۔

لہٰذا $6 = (6)^{-1}$ بھی مولد نہیں ہے کیوں کہ $6 \times_7 6 = 1$

لہٰذا نتیجہ یہ ہوا کہ سائکلی گروپ ہے اور اس کے مولد 3 اور 5 ہیں۔

مثال 7۔ اگر $G = \{a^1, a^2, a^3, a^4 = e\}$ بہ عمل ضرب گروپ ہے تو اس کے تمام مولد معلوم کرو۔

حل۔ چوں کہ $a^4 = e$ اور $(1,4) = 1$ اس لیے a^1 مولد ہے۔

لہٰذا $a^3 = (a^1)^{-1}$ بھی مولد ہے کیوں کہ $a^1 a^3 = a^4 = e$

$$(2,4) \neq 1$$

اس لیے a^2 مولد نہیں ہے۔ لہٰذا $a^2 = (a^2)^{-1}$

اور $(3,4) = 1$ اس لیے a^3 مولد ہے۔ جو پہلے ہی معلوم ہو چکا۔

لہٰذا G کے تمام مولد a^1, a^3 ہیں۔

مثال 8۔ اگر گروپ G کا رتبہ 10 ہے تب اس کے تمام مولد معلوم کرو۔

حل۔ فرض کرو کہ $G = \{a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10} = e\}$ گروپ ہے۔ چوں کہ $a^{10} = e$

اور $(1,10) = 1$ اس لیے a^1 مولد ہے۔

لہٰذا $a^9 = (a^1)^{-1}$ بھی مولد ہے اور $(2,10) \neq 1$

اس لیے a^2 مولد نہیں ہے۔

لہٰذا $a^8 = (a^2)^{-1}$ بھی مولد نہیں ہے۔

کیوں کہ $(3,10) = 1$ اس لیے a^3 مولد ہے۔

لہٰذا $a^7 = (a^3)^{-1}$ بھی مولد ہے۔

اور $(4,10) \neq 1$

اس لیے a^4 مولد نہیں ہے۔

لہٰذا $a^6 = (a^4)^{-1}$ بھی مولد نہیں ہے۔

اور $(5,10) \neq 1$

اس لیے a^5 مولد نہیں ہے۔

لہٰذا $a^5 = (a^5)^{-1}$ بھی مولد نہیں ہے۔

چنانچہ معلوم ہوا کہ G سائکلی گروپ ہے اور اس کے تمام مولد حسب ذیل ہیں

$$a^1, a^3, a^7, a^9$$

قضیہ 1۔ ہر سائکلی گروپ ابیلین ہوتا ہے۔

ثبوت۔ فرض کرو کہ $(G,\cdot)$ سائکلی گروپ ہے، اس لیے

$$G = \{a^n \ / \ n \in \mathbb{Z}\}$$

اسے ابیلین ثابت کرنے کے لیے ہمیں ثابت کرنا ہوگا کہ G تقلیبی خاصیت کا حامل ہے۔

فرض کرو کہ $g_1, g_2 \in G$ تب فرض کرو کہ

$$g_1 = a^i, g_2 = a^j, \forall i, j \in \mathbb{Z}$$

تب

$$\begin{aligned} g_1 \cdot g_2 &= a^i \cdot a^j \\ &= a^{i+j} \\ &= a^{j+i} \qquad [\text{چوں کہ صحیح اعداد تقلیبی ہوتے ہیں}] \\ &= a^j \cdot a^i \\ &= g_2 \cdot g_1 \end{aligned}$$

یعنی تقلیبی خاصیت G پر پوری ہوئی۔ لہٰذا سائکلی گروپ ہے۔

چنانچہ ہر سائکلی گروپ ابیلین ہوتا ہے۔

نوٹ: اس قضیہ کا معکوس صحیح نہیں ہے (یعنی صحیح ہونا ضروری نہیں) مثلاً $(\mathbb{Q}, +)$ ابیلین گروپ ہوتا ہے مگر یہ سائکلی گروپ نہیں ہے۔

قضیہ 2۔ کسی سائکلی گروپ کا ہر تحت گروپ بھی سائکلی ہوتا ہے۔

ثبوت۔ فرض کرو کہ $(G,\cdot)$ سائکلی گروپ ہے

$$G = \{a^n \ / \ n \in \mathbb{Z}\} =< a >$$

اور فرض کرو کہ G کا تحت گروپ $(H,\cdot)$ ہے۔

اب یہ ثابت کرنا ہوگا کہ H سائکلی گروپ ہے۔

چوں کہ $H \subseteq G$ اس لیے H کا ہر عنصر $a^r \in H, \ \forall r \in \mathbb{Z}$ شکل پر ہوگا۔

فرض کرو کہ $a^d \in H$ جہاں $d \in \mathbb{Z}$ سب سے چھوٹا مثبت صحیح عدد ہے۔

اب ہم کوشش کریں گے کہ $H =< a^d >$ ثابت ہو جائے۔

یعنی a^d تحت گروپ H کا مولد ہو گا جس کی وجہ سے H سائکلی ہو جایے گا۔

اب فرض کرو کہ $a^m \in H$ جہاں $m \in \mathbb{Z}$

تب تقسیمی الخوارزم (Division Algorithm) سے دو یکتا صحیح اعداد $q, r \in \mathbb{Z}$

اس طرح موجود ہوں گے کہ

$$m = dq + r, \qquad 0 \leq r < d$$

تب

$$\begin{aligned} a^m &= a^{dq+r} \\ &= a^{dq} \cdot a^r \qquad \text{.....(1)} \end{aligned}$$

اب چوں کہ $a^d \in H$ اس لیے $(a^d)^q \in H$

یعنی $a^{dq} \in H$

چوں کہ H تحت گروپ ہے معکوسی خاصیت کی بنا پر، $a^{-dq} \in H$

تب بند شی خاصیت کی بنا پر

$$\begin{aligned} & a^m \cdot a^{-dq} \in H \\ \Longrightarrow \quad & a^{m-dq} \in H \\ \Longrightarrow \quad & a^r \in H \end{aligned}$$

یہ $r < d$ سے ممکن نہیں ہے کیوں کہ d سب سے چھوٹا مثبت صحیح عدد ہے کہ $a^d \in H$ لہٰذا صرف یہ ہی ہونا چاہیے کہ $r = 0$

مساوات (1) کی مدد سے

$$\begin{aligned} a^m &= a^{dq} \\ &= (a^d)^q \end{aligned}$$

معلوم ہوا کہ کوئی بھی عنصر $a^m \in H$ تخلیق پاتا ہے a^d کی کوئی قوت سے یعنی a^d مولد پایا گیا۔

چنانچہ $H =< a^d >$

چنانچہ ثابت ہوا کہ ایک سائکلی گروپ کا ہر تحت گروپ بھی سائکلی ہوتا ہے۔

نوٹ: مندرجہ بالا قضیہ کا معکوس صحیح ہونا ضروری نہیں ہے۔

مثلاً $(\mathbb{Z}, +)$ سائکلی گروپ ہے جو $(\mathbb{Q}, +)$ کا تحت گروپ ہے۔ مگر $(\mathbb{Q}, +)$ سائکلی گروپ نہیں ہوتا ہے۔

قضیہ 3۔ اگر G متناہی گروپ ہے جس کا رتبہ مفرد صحیح عدد ہے تب G سائکلی گروپ ہو گا۔

ثبوت۔ فرض کرو کہ $(G, \cdot)$ متناہی گروپ ہے

اور $O(G) = P$ جہاں $p \in \mathbb{Z}^+$ مفرد صحیح عدد ہے تب $p \geq 2$ ہو گا

فرض کرو کہ $e \in G$ اکائی ہے اور $a(\neq e) \in G$

فرض کرو کہ $H =< a >$ اور $O(H) \neq 1, a \neq e$

چوں کہ H گروپ G کا تحت گروپ ہوتا ہے اور لیگرانج کے قضیہ کے مطابق تحت گروپ کا رتبہ گروپ کے رتبے کو تقسیم کرتا ہے۔
لہٰذا $O(H)/O(G)$ اور چوں کہ $O(G) = p$ مفرد (Prime) ہے جس کے قاسم p اور 1 ہوتے ہیں۔ چوں کہ $O(H) \neq 1$ اس

لیے $O(H) = p$ ہوگا

$O(H) = p = O(G)$ تو پھر

اس لیے $H =< a >= G$

چنانچہ G سائکلی گروپ ہے۔

قضیہ ثابت ہوا۔

قضیہ 4۔ اگر G ایک سائکلی گروپ ہے اور $a \in G$ اس کا مولد ہے تب $a^{-1} \in G$ بھی مولد ہوگا۔

ثبوت۔ فرض کرو کہ $(G, \cdot)$ متناہی گروپ ہے۔

اگر $G = \{e\}$ ہو تب $e^{-1} = e$ تب قضیہ صحیح ہوگا

ورنہ اگر $O(G) > 1$ تب $\exists a \in G$ اور $a \neq e$

اور فرض کرو کہ a مولد ہے تب $G =< a >= \{a^n \ / \ n \in \mathbb{Z}\}$

چوں کہ $a \in G$ تب $a^{-1} \in G$ ہوگا، تب $a^n = (a^{-1})^{-n}, n \in \mathbb{Z}$

لہٰذا $G = \{(a^{-1})^{-n} \ / \ n \in \mathbb{Z}\} =< a^{-1} >$

اس لیے a^{-1} بھی مولد ہوا۔

قضیہ ثابت ہوا۔

قضیہ 5۔ ایک لامتناہی سائکلی گروپ کے ٹھیک دو مولد ہوتے ہیں (جو ایک دوسرے کے معکوس ہوتے ہیں)۔

ثبوت۔ فرض کرو کہ $G = \{a^n \ / \ n \in \mathbb{Z}\}$ لامتناہی گروپ ہے۔

یعنی G ایک سائکلی گروپ ہے جس کا مولد a ہے۔

فرض کرو کہ $a^m \in G$ بھی G کا مولد ہے۔

تب $a \in G$ کے لیے فرض کرو کہ $a = (a^m)^p, \ p \in G$

$$\begin{aligned} &\Rightarrow \quad a^{mp} = a \\ &\Rightarrow \quad a^{mp} \cdot a^{-1} = a \cdot a^{-1} \\ &\Rightarrow \quad a^{mp-1} = e \end{aligned}$$

تب اگر $mp - 1 > 0$

تب اگر فرض کرو کہ $mp - 1 = q$

تب $a^q = e$

تو پھر G متناہی ہو جایے گا۔ جو کہ نہیں ہے۔

اس لیے ضروری ہے کہ $mp - 1 = 0$

$$mp = 1$$
$$m = \pm 1 \ \& \ p = \pm 1$$

چنانچہ

$$a^m = a^{\pm 1}$$

یعنی a^{-1} اور a ٹھیک دو ہی G کے مولد ہوں گے۔

قضیہ ثابت ہوا۔

قضیہ 6۔ اگر کسی متناہی گروپ کا رتبہ n ہے اور اس میں کسی عنصر کا رتبہ بھی n ہے تو گروپ سائکلی ہو گا۔

ثبوت۔ فرض کرو کہ $(G,\cdot)$ متناہی گروپ ہے۔

اور $n = O(G)$ جہاں $n \in \mathbb{Z}^+$

اور فرض کرو کہ $a \in G$ اس طرح کہ $O(a) = n$ یعنی $a^n = e$

اب اگر G کا $H = \{a^r \ / \ r \in \mathbb{Z}\}$ سائکلی تحت گروپ ہے

تب چوں کہ $a^n = e$ اس لیے $O(H) = n$

معلوم ہوا کہ $O(H) = n = O(G)$

لہٰذا $G = H$ ہو جایے گا۔

چنانچہ $G =< a >$ سائکلی گروپ ہو گا۔

قضیہ ثابت ہوا۔

قضیہ 7۔ اگر G ایک سائکلی گروپ ہے جس کا مولد a ہے اور رتبہ n ہے۔ تب a^m سائکلی گروپ G کا مولد ہو گا اگر اور صرف اگر $(m,n) = 1$

ثبوت۔ فرض کرو کہ $G =< a >$ اور $O(a) = n$ یعنی $a^n = e$

تب G میں n عناصر ہوں گے۔

فرض کرو کہ $(m,n) = 1$

اور اگر $H =< a^m >$

تب ظاہر ہے

$$H \subseteq G \qquad .....(1)$$

اور a^m کی کوئی بھی قوت a کی کسی قوت کے برابر ہو گی۔ اب چوں کہ $(m,n)=1$ اس لیے $x,y \in \mathbb{Z}$ اس طرح سے کہ

$$mx+ny=1$$

ہو گا۔ تب

$$\begin{aligned} a=a^1 &= a^{mx+ny} \\ &= a^{mx}\cdot a^{ny} \\ &= a^{mx}\cdot (a^n)^y \\ &= a^{mx}\cdot e^y \\ &= a^{mx} \\ &= (a^m)^x \\ \Longrightarrow \quad & G \subseteq H \qquad \text{.....(2)} \end{aligned}$$

مساوات(1) اور(2) کی مدد سے

$$H=G=<a^m>$$

اس لیے ثابت ہوا کہ a^m مولد ہے۔

اس کے بالعکس فرض کرو کہ $G=<a^m>$ تب ثابت کرنا ہو گا کہ $(m,n)=1$

اگر فرض کر لیں کہ $(m,n)=d$ اور $d>1$ تب $\frac{m}{d}, \frac{n}{d}$ صحیح عدد ہوں گے، تب

$$\begin{aligned} (a^m)^{\frac{n}{d}} &= (a)^{\frac{mn}{d}} \\ &= (a^n)^{\frac{m}{d}} \\ &= (e)^{\frac{m}{d}} \\ &= e \end{aligned}$$

تب $\qquad |a^m|<n, \qquad \left[\because \frac{m}{d}<n\right]$

تب a^m مولد نہیں ہو سکے گا کیوں کہ $|a^m| \neq |G|=n$

اس لیے ہمارا مفروضہ کہ $(m,n)=d>1$ غلط ہے۔

اس لیے $d=1$ ہونا چاہیے یعنی $(m,n)=1$

قضیہ ثابت ہوا۔

آئیلر کا ٹوشینٹ تفاعل(Euler's Totient Function):

اگر $n \in \mathbb{Z}^+$ اور اگر $n={p_1}^{q_1}\cdot {p_2}^{q_2}\cdot {p_3}^{q_3}\cdots {p_m}^{q_m}$ جہاں $p_1,p_2,\cdots p_m$ اجزا ضربی مفرد اعداد ہیں۔

تب

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)$$

نوٹ: اگر n مفرد صحیح عدد ہے، تب اس کے کوئی اجزا ضربی نہیں ہوں گے۔ گویا $n=n'$

تب

$$\varphi(n) = n\left(1 - \frac{1}{n}\right)$$
$$= n\left(\frac{n-1}{n}\right)$$
$$= n - 1$$

ہو گا۔

نوٹ: ایک سائکلی گروپ جس کا رتبہ n ہے۔ اس کے $\varphi(n)$ مولد ہوتے ہیں۔

مثال9۔ $G = \{a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^8 = e\}$ ایک سائکلی گروپ ہے۔

حل۔ مثال 5 میں ہم نے دیکھا کہ اس کے 4 مولد ہیں $a^1, a^3, \ a^5, a^7$ اس کو ہم آئلر کے طریقے سے معلوم کریں گے کہ اس کے کتنے مولد ہوں گے۔

چوں کہ $O(G) = 8$ اس لیے $2^3 = 8$

اس لیے $\varphi(8) = 8 \cdot \left(1 - \frac{1}{2}\right)$

$= 8 \cdot \left(\frac{1}{2}\right) = 4$

یہاں یہ معلوم ہوا کہ گروپ جس کا رتبہ 8 ہے اس کے 4 مولد ہوں گے۔ اس کی تصدیق مثال 5 سے ہوتی ہے۔

مثال10۔ $G = \{1,2,3,4,5,6\}$ عمل $\otimes_7$ کے تحت ایک سائکلی گروپ ہے۔ اس کے کتنے مولد ہوں گے؟

حل۔ چوں کہ $O(G) = 6$ اس لیے $2^1 \cdot 3^1 = 6$

اس لیے $\varphi(6) = 6 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$

$= 6 \cdot \left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 2$

لہٰذا G کے 2 مولد ہیں جس کی تصدیق مثال 6 سے ہوتی ہے۔

مثال11۔ گروپس جن کے رتبے 5, 6,8,12, 15,60 ہیں ان کے مولدوں کی تعداد معلوم کرو۔

حل۔

a) اگر $|G| = 5$

چوں کہ 5 مفرد ہے۔ اس لیے

$\varphi(6) = 5 - 1 = 4$

یعنی گروپ جس کا رتبہ 5 ہے اس کے 4 مولد ہوں گے۔

b) اگر $|G| = 6$

چوں کہ $6 = 2^1 \cdot 3^1$ ہے۔ اس لیے مولد کی تعداد $\varphi(6)$ ہو گی۔

$\varphi(6) = 6 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$

$$= 6 \cdot \left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 2$$

یعنی گروپ جس کا رتبہ 6 ہے اس کے 2 مولد ہوں گے۔

(c) اگر $|G| = 8$

تب $8 = 2^3$ ہے۔اس لیے مولد کی تعداد

$$\varphi(8) = 8 \cdot \left(1 - \frac{1}{2}\right)$$
$$= 8 \cdot \left(\frac{1}{2}\right) = 4$$

یعنی گروپ جس کا رتبہ 8 ہے اس کے 4 مولد ہوں گے۔

(d) اگر $|G| = 12$

چوں کہ $12 = 2^2 \cdot 3^1$ ہے۔اس لیے مولد کی تعداد

$$\varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)$$
$$= 12 \cdot \left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 4$$

یعنی گروپ جس کا رتبہ 12 ہے اس کے 4 مولد ہوں گے۔

(e) اگر $|G| = 15$

چوں کہ $15 = 5^1 \cdot 3^1$ ہے۔اس لیے مولد کی تعداد

$$\varphi(15) = 15 \cdot \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$
$$= 15 \cdot \left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 8$$

یعنی گروپ جس کا رتبہ 15 ہے اس کے 8 مولد ہوں گے۔

(f) اگر $|G| = 60$

چوں کہ $60 = 2^2 \cdot 3^1 \cdot 5^1$ ہے۔اس لیے مولد کی تعداد

$$\varphi(60) = 60 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$
$$= 60 \cdot \left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 16$$

یعنی گروپ جس کا رتبہ 60 ہے اس کے 16 مولد ہوں گے۔

نوٹ: اگر G سائکلی گروپ ہے جس کا رتبہ n ہے تب G کے تحت سائکلی گروپ اور n کے اجزاضربی کے درمیان دوربطی تعلق ہوتا ہے۔

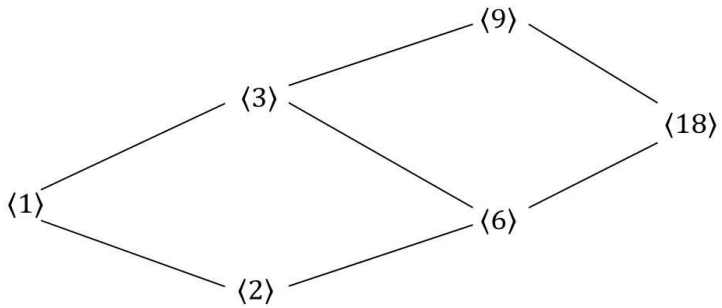
مثال12۔ گروپ $(\mathbb{Z}_{18}, +_{18})$ کے سارے تحت گروپس معلوم کرو۔اس کا لیاٹس خاکہ (Lattice Diagram) بھی بناؤ۔

حل- $\mathbb{Z}_{18}$ کے تحت گروپ وہ ہوتے ہیں جو 18 کے اجزاضربی سے تخلیق پاتے ہیں۔یعنی 18،9،6،3،2،1 سے تخلیق پاتے ہیں۔یہ

اس طرح ہوں گے

$$\langle 1\rangle = \{0,1,2,3,\cdots,17\}$$
$$\langle 2\rangle = \{0,2,4,6,8,10,12,14,16\}$$
$$\langle 3\rangle = \{0,3,6,9,12,15\}$$
$$\langle 6\rangle = \{0,6,12\}$$
$$\langle 9\rangle = \{0,9\}$$
$$\langle 18\rangle = \{0\}$$

یہاں ہم دیکھتے ہیں کہ $\langle 2\rangle$، $\langle 3\rangle$، $\langle 6\rangle$، $\langle 9\rangle$، $\langle 18\rangle$ سب $\langle 1\rangle$ کے تحت سٹس ہیں۔ $\langle 2\rangle$ میں $\langle 6\rangle$ اور $\langle 18\rangle$ تحت سٹس ہیں۔ $\langle 3\rangle$ میں $\langle 6\rangle$، $\langle 9\rangle$ اور $\langle 18\rangle$ موجود ہیں۔ اب ہم ان تحت سٹس کو ایسا ترتیب دیں گے کہ کون کس کے تحت آتا ہے اس کو لیٹس خاکہ (Lattice Diagram) کہتے ہیں۔



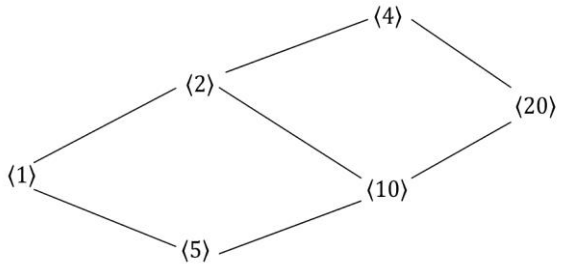
شکل 5.1۔ لیٹس خاکہ

مثال 13۔ گروپ $(\mathbb{Z}_{20}, +_{20})$ کے کتنے سائکلی تحت گروپس ہوں گے اور ان کے مولد کیا ہیں۔ اس کا لیاٹس خاکہ بھی بناؤ۔

حل۔ ہم جانتے ہیں کہ $\mathbb{Z}_{20} = \{0,1,2,3,\cdots,19\}$ گروپ ہے $+_{20}$ عمل سے۔ چوں کہ 20 کے اجزاضربی 1، 2، 4، 5، 10، 20 ہیں۔ لہٰذا یہ تمام مولد ہوں گے ان 6 سائکلی تحت گروپس کے اور ان کے ذریعے تخلیق پانے والے سائکلی تحت گروپس حسب ذیل ہوں گے۔

$$\langle 1\rangle = \{0,1,2,3,\cdots,19\}$$
$$\langle 2\rangle = \{0,2,4,6,8,10,12,14,16,18\}$$
$$\langle 4\rangle = \{0,4,8,12,16\}$$
$$\langle 5\rangle = \{0,5,10,15\}$$
$$\langle 10\rangle = \{0,10\}$$
$$\langle 20\rangle = \{0\}$$

اور ان کا لیٹس خاکہ (Lattice Diagram) یوں ہوگا۔



شکل 5.2۔ لیٹس خاکہ

مثال14۔ گروپ $(\mathbb{Z}_{30}, +_{30})$ کے تحت سائکلی گروپس جس کا مولد 25 ہے اس میں عناصر کی تعداد معلوم کرو۔

حل۔ ہم جانتے ہیں کہ $gcd(30,25) = 5$ اور $O(\langle 25\rangle) = \frac{30}{5} = 6$

اس لیے سائکلی تحت گروپ 25 سے تخلیق پانے والے 6 عناصر ہوں گے اور وہ تحت سائکلی گروپ یوں ہو گا۔

$$\langle 25\rangle = \{0,5,10,15,20,25\}$$

$\because 25 \cdot 1 = 25$

$25 \cdot 2 = 20$ وجہ سے $+_{30}$

$25 \cdot 3 = 15$ وجہ سے $+_{30}$

$25 \cdot 4 = 10$ وجہ سے $+_{30}$

$25 \cdot 5 = 5$ وجہ سے $+_{30}$

$25 \cdot 6 = 0$ وجہ سے $+_{30}$

$25 \cdot 7 = 25$ وجہ سے $+_{30}$

مثال15۔ گروپ $(\mathbb{Z}_{42}, +_{42})$ گروپ میں سائکلی تحت گروپ جس کا مولد 30 ہے اس کے عناصر کی تعداد معلوم کرو۔

حل۔ ہم جانتے ہیں کہ $gcd(42,30) = 6$

اور مولد 30 سے تخلیق پانے والے عناصر کی تعداد $O(\langle 30\rangle) = \frac{42}{6} = 7$ اور عناصر یہ ہوں گے

$$\langle 30\rangle = \{0,6,12,18,24,30,36\}$$

5.3 مبادلہ گروپ(Permutation Group)

تعریف: اگر S ایک غیر خالی سٹ ہے تب دور بطی تفاعل (1-1 and onto mapping) $f: S \to S$ کو S کا مبادلہ کہا جاتا ہے۔

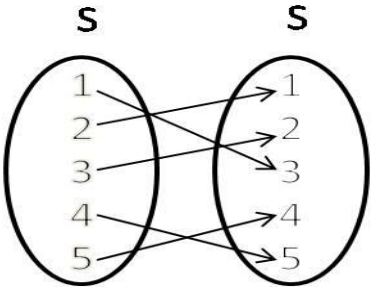
یا

ایک غیر خالی سٹ کا اسی پر دور بطی تفاعل کو مبادلہ کہا جاتا ہے۔

نوٹ:

1. اس نصاب میں S غیر خالی سٹ کو متناہی لیا جائے گا۔
2. **اگر** S میں n عناصر ہوں تو S پر مبادلہ درجہ n کہلائے گا (Permutation of degree n)۔

مثال1۔ اگر $S = \{1,2,3,4,5\}$ اور $f: S \to S$ اس طرح کہ



یہاں $f(1)=3, f(2)=1, f(3)=2, f(4)=5, f(5)=4$

اس کو مبادلہ یوں ظاہر کیا جاتا ہے

$$f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 1 & 2 & 5 & 4\end{pmatrix}$$

نوٹ:

1. $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}$ یعنی $f(x)=x, \forall x\in S$ اسے اکائی مبادلہ (Identity Permutation) کہتے ہیں۔
2. S میں اگر n عناصر ہوں تو $n!$ مبادلات ممکن ہیں۔
3. اگر f مبادلہ ہو تو f^{-1} دونوں صفوں کے مابین تبادلہ سے حاصل ہوتا ہے۔ جیسے $f=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 1 & 2 & 5 & 4\end{pmatrix}$ ہو تب

$$\begin{aligned}f^{-1}&=\begin{pmatrix}3 & 1 & 2 & 5 & 4\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}\\ &=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 5 & 4\end{pmatrix}\end{aligned}$$

نقائش کی ترکیب (Composition of Mapping): اگر $f:S\to S$ اور $g:S\to S$ دو نقائش ہیں، تب gof یوں ہوگا

$$(gof)(x)=g(f(x))$$

یا یوں سمجھیں اگر $f=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ f(1) & f(2) & f(3) & \cdots & f(n)\end{pmatrix}$ اور $g=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ g(1) & g(2) & g(3) & \cdots & g(n)\end{pmatrix}$

تب

$$\begin{aligned}gof&=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ g(1) & g(2) & g(3) & \cdots & g(n)\end{pmatrix}\circ\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ f(1) & f(2) & f(3) & \cdots & f(n)\end{pmatrix}\\ &=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ g(f(1)) & g(f(2)) & g(f(3)) & \cdots & g(f(n))\end{pmatrix}\end{aligned}$$

یاد رہے کہ gof بھی S ہی کا ایک مبادلہ ہوگا اور عمل ایک شائی عمل ہوگا۔

نوٹ: gof کو عام طور پر ضرب سے ظاہر کرتے ہیں یعنی $gof=gf$

مثال 2۔ اگر $S=\{1,2,3\}$

چوں کہ 3 عناصر ہیں اس لیے جملہ مبادلات ضربیہ 3 یعنی $3!$ ہوں گے یعنی

$$3!=3\cdot 2\cdot 1=6$$

وہ مان لیں کہ

$$f_1=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$$
$$f_2=\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$
$$f_3=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$$
$$f_4=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$$
$$f_5=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$$
$$f_6=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

ان6 کے علاوہ مبادلات ممکن نہیں ہیں۔ غور کریں کہ f_1 اکائی مبادلہ ہے۔

اب دیکھیں ترکیب

$$f_2 f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ f_2(f_3(1)) & f_2(f_3(2)) & f_2(f_3(3)) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ f_2(2) & f_2(1) & f_2(3) \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

اس کو یوں آسانی سے لکھا جا سکتا ہے

$$f_2 f_3 = \begin{pmatrix} 1_{\downarrow} & 2_{\downarrow} & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1_{\downarrow} & 2_{\downarrow} & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

یہاں ہم نے دیکھا کہ دائیں جانب کی قوس میں $2 \to 1$ اور پھر بائیں قوس میں $3 \to 2$ لہٰذا نتیجتاً $2 \to 1$

پھر 2 کے بارے میں پہلی قوس میں $1 \to 2$ اور پھر دائیں قوس میں $1 \to 1$ لہٰذا نتیجتاً $2 \to 1$

اسی طرح پہلی قوس میں 3 کا عکس 3 اور اس عکس 3 کا پہلی قوس میں عکس 2 ہے اس لیے 3 کا آخری عکس 2 لیا جائے گا۔

نوٹ کیجیے کہ $f_2 f_3 = f_5$ بنا ہے۔

نوٹ: اوپر والی مثال میں اگر $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ مبادلات کا سٹ درجہ 3 پر ایک غیر تقلیبی گروپ بنتا ہے مبادلات کے ضربی عمل پر۔

ثبوت: ان تمام مبادلات کا ترکیبی جدول جس کو کیلے جدول (Caylay Table) بھی کہتے ہیں یوں بنتا ہے

.	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

غور کرنے سے معلوم ہوا کہ تمام ضرب پر حاصل ہونے والے مبادلات S_3 کے ممبر عناصر ہیں۔ اس لیے بند شی خاصیت (Closure Property) پوری ہوئی۔

اور اگر دیکھا جائے کہ $f_2(f_3 f_4) = (f_2 f_3) f_4$

$$f_2 f_2 = f_5 f_4$$
$$f_1 = f_1$$

یعنی تلازمی خاصیت (Associative Property) پوری ہوئی۔

اور نمایاں ہے کہ f_1 اکائی ہے چوں کہ f_1 کسی سے ضربی ترکیب پر دوسرے کو فرق نہیں کرتا ہے جیسے $f_1 f_4 = f_4$

اس لیے S_3 میں اکائی موجود ہے۔

اور ہم دیکھتے ہیں کہ $f_1^{-1} = f_1,\ f_2^{-1} = f_2,\ f_3^{-1} = f_3,\ f_4^{-1} = f_5,\ f_5^{-1} = f_4,\ f_6^{-1} = f_6$

چوں کہ گروپ کے چاروں خصوصیات پوری ہوتی ہیں اس لیے S_3 گروپ ہوا۔

اب چوں کہ $f_4 f_6 = f_2$

اور $f_6 f_4 = f_3$

گویا $f_4 f_6 \neq f_6 f_4$

لہاذا تقلیبی خاصیت پوری نہیں ہوئی۔

اس لیے S_3 غیر تقلیبی گروپ بنتا ہے۔

نوٹ: یاد رکھیں کہ مبادلات کا گروپ غیر تقلیبی ہوتا ہے۔ جب کہ اس میں 2 سے زیادہ عناصر ہوں اور

$$O(S_3) = 3!$$

مبادلات کا رتبہ (Order of a Permutation):

اگر $f \in S_n$ اس طرح کہ $f^m = I$ جہاں $m \in \mathbb{Z}^+$ کمترین مثبت صحیح عدد ہے تب f کا رتبہ m ہوگا $O(f) = m$، I اکائی مبادلہ ہے۔

مثال 1۔

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

تب

$$f^2 = ff = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$f^3 = f^2 f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{I(Identity)}$$

لہٰذا f کا رتبہ 3 ہے۔ یعنی $O(f) = 3$

مثال 2۔ اگر $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}, f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$ تب حسب ذیل معلوم کرو

(i fg (ii gf (iii $(fg)^{-1}$ (iv $g^{-1}f^{-1}$ (v f^2

حل۔

(i

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$$

(ii

$$gf = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 1 & 3 & 5 & 4\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 3 & 2 & 1 & 5\end{pmatrix}$$
$$= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 3 & 1 & 2 & 4\end{pmatrix}$$

نوٹ: $fg \neq gf$

(iii i) کے مطابق $fg = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 4 & 2 & 5 & 1\end{pmatrix}$ اس لیے

$$(fg)^{-1} = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 4 & 2 & 5 & 1\end{pmatrix}^{-1}$$
$$= \begin{pmatrix}3 & 4 & 2 & 5 & 1\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}$$
$$= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 3 & 1 & 2 & 4\end{pmatrix}$$

(iv

$$g^{-1}f^{-1} = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 1 & 3 & 5 & 4\end{pmatrix}^{-1}\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 3 & 2 & 1 & 5\end{pmatrix}^{-1}$$
$$= \begin{pmatrix}2 & 1 & 3 & 5 & 4\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}\begin{pmatrix}4 & 3 & 2 & 1 & 5\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}$$
$$= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 1 & 3 & 5 & 4\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 3 & 2 & 1 & 5\end{pmatrix}$$
$$= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 3 & 1 & 2 & 4\end{pmatrix}$$

نوٹ: $(fg)^{-1} = g^{-1}f^{-1}$

(v

$$f^2 = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 3 & 2 & 1 & 5\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 3 & 2 & 1 & 5\end{pmatrix}$$
$$= \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}$$

نوٹ: $f^2 = I$ چنانچہ $O(f) = 2$ ہے۔

سائکلی مبادلہ(Cyclic Permutation):

فرض کرو کہ $S = \{a_1, a_2, \cdots, a_n\}$ ایک متناہی سٹ ہے اور $f: S \to S$ ایک مبادلہ ہے

$$f = \begin{pmatrix}a_1 & a_2 & a_3 & \cdots & a_k & a_{k+1} & \cdots & a_n\\ a_2 & a_3 & a_4 & \cdots & a_1 & a_{k+1} & \cdots & a_n\end{pmatrix}$$

غور کرو کہ $f(a_1) = a_2, f(a_2) = a_3, \cdots, f(a_k) = a_1$ اور $f(a_{k+1}) = a_{k+1}$، $f(a_{k+2}) = a_{k+2}$ اور $f(a_n) = a_n$

یعنی ہر عنصر اس کے مقدم پر نقش ہوتا ہے اور a_k واپس پہلے عنصر a_1 پر نقش ہوتا ہے اور باقی اپنے آپ پر نقش ہیں۔

اسے ہم یوں ظاہر کرتے ہیں

$$f = (a_1 a_2 \cdots a_k)(a_{k+1})\cdots(a_n)$$
$$= (a_1 a_2 \cdots a_k) \quad \text{یا}$$

یہ ایک سائکلی مبادلہ ہے جس کا طول k ہے اور n علامات (Symbols) پر ہے۔

نوٹ1: اپنے آپ پر نقش ہونے والے عناصر کو ظاہر نہیں کیا جاتا ہے۔

نوٹ2: سائکلی کی ترتیب بدلے بغیر f کو مختلف طریقوں سے لکھا جا سکتا ہے۔

مثلاً $f = (a_3\ a_4\ \cdots a_k\ a_1\ a_2)$ یا $f = (a_2\ a_3\ \cdots a_k\ a_1)$ وغیرہ۔

نوٹ3: کسی مبادلہ کو غیر مشترک سائکلی مبادلات کے ضرب کے طور پر لکھا جا سکتا ہے

مثلاً $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 2 & 5 & 4 & 6 & 7 \end{pmatrix}$ تب $f = (1\ \ 3\ \ 2)(4\ \ 5)(6)(7)$ یا $f = (1\ \ 3\ \ 2)(4\ \ 5)$

نوٹ4: دو طول والی سائکل کو جابدل (Transposition) کہتے ہیں۔

نوٹ5: ہر سائکل کو جابدل (Transposition) کے حاصل ضرب کے طور پر ظاہر کیا جا سکتا ہے

مثلاً $f = (1\ \ 3\ \ 2\ \ 5)(4\ \ 6\ \ 7)$

$= (1\ \ 5)(1\ \ 2)(1\ \ 3)(4\ \ 7)(4\ \ 6)$

نوٹ6: اگر کسی مبادلہ کو غیر مشترک سائکلس میں ظاہر کرنے کے بعد جابدل میں رقم کرنے پر اگر وہ طاق تعداد میں ہوں تو مبادلہ طاق کہلاتا ہے اور اگر جابدل کی تعداد جفت ہو تو جفت مبادلہ کہلاتا ہے۔

مثلاً نوٹ 5 کی مثال میں جابدل کی تعداد 5 ہے لہٰذا f طاق مبادلہ ہے۔ جب کہ اگر

$f = (1\ \ 3\ \ 2\ \ 6)(4\ \ 5)$

تب $= (1\ \ 6)(1\ \ 2)(1\ \ 3)(4\ \ 5)$

یہاں 4 جابدل ہیں لہٰذا f جفت مبادلہ ہے۔

نوٹ7: سائکلی مبادلہ کا معکوس عناصر کی الٹی ترتیب لکھنے سے حاصل ہوتا ہے۔

مثلاً $f = (1\ \ 2\ \ 4\ \ 5\ \ 6)$

تب $f^{-1} = (6\ \ 5\ \ 4\ \ 2\ \ 1)$

اور اس لیے اگر

$$f = (a_1\ \ a_2\ \ a_3\ \ \cdots\ \ a_k)$$
$$\Longrightarrow f^{-1} = (a_k\ \ a_{k-1}\ \ a_{k-2}\ \ \cdots\ \ a_1)$$

مثال3۔ $f = (2\ \ 3\ \ 4\ \ 5)(6\ \ 7\ \ 8)$

$$\Longrightarrow\ f^{-1} = (6\ \ 7\ \ 8)^{-1}(2\ \ 3\ \ 4\ \ 5)^{-1}$$
$$\Longrightarrow\ f^{-1} = (8\ \ 7\ \ 6)(5\ \ 4\ \ 3\ \ 2)$$

مثال4۔ $f = (1\ \ 3\ \ 6)(1\ \ 3\ \ 5\ \ 7)(6\ \ 7)(1\ \ 2\ \ 3\ \ 4)$ کو غیر مشترک سائکلوں کے حاصل ضرب پر ظاہر کرو۔ اس کا معکوس معلوم کرو اور یہ بھی معلوم کرو کہ آیا f طاق ہے۔

حل۔ مان لو کہ $f = (1\ \ 3\ \ 6)(1\ \ 3\ \ 5\ \ 7)(6\ \ 7)(1\ \ 2\ \ 3\ \ 4)$

چوں کہ علامات 1 تا 7 استعمال ہوئی ہیں، اس لیے ہر سائکل 7 علامات پر لکھی جائے گی۔

لہٰذا

$$f = \left[\begin{pmatrix}1&2&3&4&5&6&7\\3&2&6&4&5&1&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\3&2&5&4&7&6&1\end{pmatrix}\right]$$
$$\left[\begin{pmatrix}1&2&3&4&5&6&7\\1&2&3&4&5&7&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\2&3&4&1&5&6&7\end{pmatrix}\right]$$
$$= \begin{pmatrix}1&2&3&4&5&6&7\\6&2&5&4&7&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\2&3&4&1&5&7&6\end{pmatrix}$$

دائیں جانب سے دو، دو مبادلوں کا حاصل ضرب لیا گیا۔ پھر ان دو مبادلوں کا حاصل ضرب

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

تب اس کے غیر مشترک سائکلس یہ ہیں $= (1\quad 2\quad 5\quad 7)(3\quad 4\quad 6)$

اور

$$f^{-1} = [(1\quad 2\quad 5\quad 7)(3\quad 4\quad 6)]^{-1}$$
$$\Longrightarrow f^{-1} = (3\quad 4\quad 6)^{-1}(1\quad 2\quad 5\quad 7)^{-1}$$
$$\Longrightarrow f^{-1} = (6\quad 7\quad 3)(7\quad 5\quad 2\quad 1)$$

اور یہ دیکھنے کے لیے کہ آیا f طاق مبادلہ ہے جب کہ حاصل شدہ

$$f = (1\quad 2\quad 5\quad 7)(3\quad 4\quad 6)$$
$$= (1\quad 7)(1\quad 5)(1\quad 2)(3\quad 6)(3\quad 4)$$

یہ 5 جابدل کا حاصل ضرب ہے۔ لہٰذا f ایک طاق مبادلہ ہے۔

مثال 5۔ $(9\quad 8\quad 7\quad 6\quad 1)(4\quad 5\quad 6)(1\quad 2\quad 3)$ کو غیر مشترک سائکلوں کے حاصل ضرب پر ظاہر کرو۔ اس کا معکوس معلوم کرو اور یہ بھی معلوم کرو کہ کیا یہ جفت مبادلہ ہے۔

حل۔ فرض کرو کہ $f = (1\quad 2\quad 3)(4\quad 5\quad 6)(1\quad 6\quad 7\quad 8\quad 9)$

چوں کہ 9 علامات ہیں اس لیے ہر سائکل 9 علامات پر لکھی جائے گی۔ اب

$$f = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&1&4&5&6&7&8&9\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\1&2&3&5&6&4&7&8&9\end{pmatrix}$$
$$\begin{pmatrix}1&2&3&4&5&6&7&8&9\\6&2&3&4&5&7&8&9&1\end{pmatrix}$$
$$= \begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&1&4&5&6&7&8&9\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&2&3&5&6&7&8&9&1\end{pmatrix}$$
$$= \begin{pmatrix}1&2&3&4&5&6&7&8&9\\4&3&1&5&6&7&8&9&2\end{pmatrix}$$
$$= (1\quad 4\quad 5\quad 6\quad 7\quad 8\quad 9\quad 2\quad 3)$$
$$\Longrightarrow f^{-1} = (3\quad 2\quad 9\quad 8\quad 7\quad 6\quad 5\quad 4\quad 1)$$

اور چوں کہ

$$f = (1\quad 4\quad 5\quad 6\quad 7\quad 8\quad 9\quad 2\quad 3)$$
$$= (1\quad 3)(1\quad 2)(1\quad 9)(1\quad 8)(1\quad 7)(1\quad 6)(1\quad 5)(1\quad 4)$$

یہ 8 جفت جابدل ہیں اس لیے f ایک جفت مبادلہ ہے۔

قضیہ 8۔ اگر $S = \{a_1, a_2, \cdots, a_n\}$ n حروف/علامات پر سٹ ہے اور S_n مبادلہ گروپ ہے تب اس میں ٹھیک نصف مبادلے جفت اور

نصف طاق ہوتے ہیں۔یعنی منجملہ $n!$، $\frac{n!}{2}$ جفت اور $\frac{n!}{2}$ طاق ہوتے ہیں۔

ثبوت۔ ہم جانتے ہیں کہ $O(S_n) = n!$

فرض کرو کہ $S = \{e_1, e_2, \cdots, e_p, o_1, o_2, \cdots, o_q\}$، جہاں $e_i's$ جفت مبادلے اور $o_i's$ طاق مبادلے ہیں اور $p + q = n!$

اب اگر $t \in S_n$ ایک جابدل ہے تب $te_1, te_2, \cdots, te_p$ طاق مبادلے ہوں گے۔

چنانچہ $p \leq q$ پہلے سے طے ہے کہ q طاق مبادلے ہیں۔۔۔۔۔۔۔۔۔۔(1)

اور $to_1, to_2, \cdots, to_q$ جفت مبادلے ہوں گے۔

چنانچہ $q \leq p$ کیوں کہ طے ہے کہ p جفت مبادلے ہیں۔۔۔۔۔۔۔۔۔۔(2)

(1) اور (2) کی مدد سے یہ اخذ ہوتا ہے $p = q$

تو پھر $p + q = n!$

سے اخذ ہوتا ہے کہ $p = \frac{n!}{2}$ اور $q = \frac{n!}{2}$

یعنی مبادلہ گروپ S_n میں ٹھیک نصف جفت اور نصف طاق مبادلے پائے جاتے ہیں۔

قضیہ ثابت ہوا۔

قضیہ 9۔ کوئی دو مشترک سائکلی مبادلے باہم متقلب (Commutative) ہوتے ہیں۔

ثبوت۔ فرض کرو کہ $S = \{a_1, a_2, \cdots, a_n\}$

فرض کرو کہ $f = (x_1\ x_2\ \cdots\ x_k)$ اور $g = (y_1\ y_2\ \cdots\ y_l)$

دو مشترک سائکلی مبادلے ہیں S پر۔

اب ہم کو ثابت کرنا ہے کہ $fg = gf$ ہوگا۔

فرض کرو کہ $x \in S$ تب (i) $x \in f$ یا (ii) $x \in g$ (iii) $x \notin f, x \notin g$

صورت(i): فرض کرو کہ $x \in f$

$$\Rightarrow x \in \{x_1, x_2, \cdots, x_k\}$$

اس لیے $f(x) \in \{x_1, x_2, \cdots, x_k\}$

غیر مشترک مبادلے ہونے کی وجہ سے

$$f \cap g = \{x_1\ x_2\ \cdots\ x_k\} \cap \{y_1\ y_2\ \cdots\ y_l\} = \emptyset$$

اس لیے $x, f(x) \notin \{y_1\ y_2\ \cdots\ y_l\}$

$$g(x) = x\ \&\ g\big(f(x)\big) = f(x)$$

تب $(gf)(x) = g\big(f(x)\big) = f(x)$

اور $(fg)(x) = f\big(g(x)\big) = f(x)$

$$\Rightarrow fg(x) = gf(x), \quad \forall x \in S$$

صورت(ii): فرض کرو کہ $x \in g$

$$\Rightarrow x \in \{y_1, y_2, \cdots, y_l\}$$

اس لیے $g(x) \in \{y_1, y_2, \cdots, y_l\}$

$$x, g(x) \notin \{x_1, x_2, \cdots, x_k\}$$

$$f(x) = x \;\&\; f\big(g(x)\big) = g(x)$$

تب $(gf)(x) = g\big(f(x)\big) = g(x)$

اور $(fg)(x) = f\big(g(x)\big) = g(x)$

$$\Rightarrow fg(x) = gf(x), \quad \forall x \in S$$

صورت(iii): فرض کرو کہ

$$x \notin \{x_1, x_2, \cdots, x_k\} \;\&\; x \notin \{y_1, y_2, \cdots, y_l\}$$

اس لیے $f(x) = x \;\&\; g(x) = x$

$$x \notin \{x_1, x_2, \cdots, x_k\}$$

اب $(gf)(x) = g\big(f(x)\big) = g(x) = x$

اور $(fg)(x) = f\big(g(x)\big) = f(x) = x$

$$\Rightarrow fg(x) = gf(x), \quad \forall x \in S$$

تینوں صورتوں میں قضیہ صحیح ثابت ہوا۔

قضیہ10۔ کسی بھی مبادلہ کو غیر مشترک سائکلوں کے حاصل ضرب کے بطور ظاہر کیا جاسکتا ہے۔اس سے قطع نظر کہ سائکلوں کی ترتیب کچھ ہو۔

ثبوت۔ فرض کرو کہ $f \in S_n$ ایک غیر اکائی مبادلہ ہے اور $a_1 \in S$

توجہ کریں $f = \sigma_1\sigma_2 \cdots \sigma_n$

چوں کہ f متناہی ہے یہ سب عناصر مختلف نہیں ہو سکتے ہیں۔فرض کرو کہ $f^r(a_1) = a_1$

تب مرتب n–گانہ(n-Tuple)

$$\sigma_1 = \big(a_1 \;\; f(a_1) \cdots f^{r-1}(a_1)\big)$$

r طول کی ایک سائکل ہے۔ اگر $b_1 \in S$ اور $b_1 \notin \sigma_1$ ہو، تو $b_1 \;\; f(b_1) \;\; f^2(b_1) \cdots$ پر توجہ کریں۔ یہ سبھی عناصر ممیز نہیں ہو سکتے اس لیے مان لیں کہ $\sigma_2 = \big(b_1 \;\; f(b_1) \;\; f^2(b_1) \cdots \;\; f^{r-1}(b_1)\big)$ ایک اور سائکل ہے جس کا طول s ہے، چوں کہ s متناہی ہے۔اس عمل کا ہم اعادہ کر سکتے ہیں یہاں تک کہ s کے تمام عناصر خالی ہو جائیں۔مزید براں سائکلیں غیر مشترک ہونے کے سبب جس ترتیب میں ان کو رقم کیا جاتا ہے وہ اہمیت کے حامل نہیں۔

یہ دیکھنے کے لیے کہ یہ نمائندگی یکتا ہے، مان لیں کہ $f = \sigma_1\sigma_2 \cdots \sigma_n = \rho_1\rho_2 \cdots \rho_m$ جہاں پر یہ سب ایک سے زیادہ طول رکھنے

والی سائکلیں ہیں۔

فرض کرو کہ $a_i \in \sigma_i$ تب $a_i \in s$ اس لیے a_i کا کسی ایک سائکل ρ_i میں شامل ہونا لازم ہے۔ مان لیں کہ $a_i \in \rho_j$ چوں کہ کوئی دو سائکلیں یا تو غیر مشترک ہوتی ہیں یا مماثل، اس لیے مان لو کہ $\sigma_i = \rho_j$ لہٰذا ہر σ_i کسی نہ کسی ρ_j کے برابر ہوتا ہے۔ چنانچہ f کی نمائندگی یکتا ہوگی۔

قضیہ ثابت ہوا۔

نوٹ:

1۔ دو جفت مبادلوں کا حاصل ضرب پھر سے جفت مبادلہ ہوتا ہے۔

2۔ دو طاق مبادلوں کا حاصل ضرب جفت مبادلہ ہوتا ہے۔

3۔ اکائی مبادلہ جفت ہوتا ہے۔

قضیہ 11۔ $S_n (n \geq 2)$ کے جفت مبادلوں کا سٹ A_n رتبہ $\frac{1}{2}(n!)$ کا تحت گروپ ہوتا ہے۔ جفت مبادلوں کے اس گروپ کو متبادل گروپ (Alternating Group) کہتے ہیں۔

ثبوت۔ نقائش کی ترکیب اجزائی (ضرب) کا عمل ثنائی عمل ہوتا ہے لہٰذا بند شی خاصیت پوری ہوئی چوں کہ دو جفت مبادلوں کا حاصل ضرب جفت ہوتا ہے۔

نقائش کی تلازمیت ظاہر ہے پوری ہوگی۔

اکائی مبادلہ چوں کہ جفت ہوتا ہے اس لیے A_n میں موجود ہوگا۔

چوں کہ f^{-1} صرف لکھنے کی ترتیب الٹی کرنے سے حاصل ہوتا ہے اس لیے پھر سے جفت مبادلہ A_n میں موجود ہوگا۔

چوں کہ گروپ کی تمام شرائط پوری ہوئیں۔ اس لیے A_n گروپ ہے۔ اور $O(A_n) = \frac{1}{2}(n!)$

نوٹ

1۔ طاق مبادلوں کا سٹ گروپ نہیں ہوتا ہے اس لیے کہ دو طاق مبادلوں کا حاصل ضرب جفت ہوتا ہے۔ لہٰذا بند شی خاصیت پوری نہیں ہوئی۔

2۔ A_n متبادل گروپ (Alternating Group) گروپ S_n کا تحت گروپ ہوتا ہے۔

5.4 اکتسابی نتائج (Learning Outcomes)

اس اکائی میں سائکلی گروپ کو پہچانا اور یہ بھی معلوم ہوا کہ ہر سائکلی گروپ ابیلین ہوتا ہے جب کہ معکوس صحیح ہونا ضروری نہیں اور ہر سائکلی گروپ کا تحت گروپ بھی سائکلی ہوتا ہے۔ سائکلی گروپ کے مولد کو معلوم کیا گیا۔ سائکلی گروپ کے تحت گروپ کی تعداد اور مولد کی تعداد کو معلوم کیا گیا۔ مبادلہ گروپ کی تعریف اور مثال دیکھی گئیں۔ کسی بھی متناہی سٹ کے تمام مبادلات کا سٹ ضربی گروپ بنانا

ہے۔ کسی بھی مبادلہ کو غیر مشترک سائکلی مبادلات کے حاصل ضرب کے بطور رقم کیا جاسکتا ہے۔ مبادلات طاق اور جفت ہوتے ہیں۔ مبادلہ گروپ میں نصف یعنی $\frac{1}{2}(n!)$ جفت اور نصف طاق ہوتے ہیں۔ جفت مبادلے بھی گروپ بناتے ہیں جسے متبادل گروپ کہتے ہیں۔

5.5 کلیدی الفاظ (Keywords)

مبادلہ، سائکلی گروپ، متبادل گروپ، جفت، طاق، غیر مشترک، مولد

5.6 نمونہ امتحانی سوالات (Model Examination Questions)

5.6.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. متبادل گروپ کی تعریف کیجیے۔

5.6.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. گروپ $(\mathbb{Z}_{36}, +_{36})$ کا لیٹس کا خاکہ بناؤ۔
2. اس گروپ کے تمام مولد معلوم کرو جس کا رتبہ 10 ہے۔
3. سائکلی گروپ $(\{4,8,12,16\}, \times_{20})$ کے تمام مولد معلوم کرو۔
4. گروپ $(\mathbb{Z}_{20}, +_{20})$ کے کتنے سائکلی تحت گروپس ہوں گے ان کے مولد کیا ہیں۔ اس کا لیاٹس خاکہ بھی بناو۔
5. گروپ $(\mathbb{Z}_{12}, +_{12})$ کا لیٹس کا خاکہ بناؤ۔
6. گروپ $(\mathbb{Z}_{17}, +_{17})$ کے تمام تحت گروپس کے رتبے معلوم کرو۔
7. گروپ $(\mathbb{Z}_{60}, +_{60})$ کے تحت سائکلی گروپ جس کا مولد 30 ہے اس کا رتبہ معلوم کرو۔
8. اگر سائکلی گروپ ہیں جن کے رتبے بالترتیب 6،8 اور 20 ہیں۔ ان کے تمام مولد معلوم کرو۔
9. $(4\ \ 5)(1\ \ 2\ \ 3)(1\ \ 2\ \ 3\ \ 4\ \ 5)$ کو غیر مشترک سائکلوں کے حاصل ضرب کی شکل میں لکھو۔ اس کا معکوس معلوم کرو اور ثابت کرو کہ یہ طاق مبادلہ ہے۔ (اشارہ: پہلے درجے میں پہلے دو کا حاصل ضرب معلوم کرلو اور تیسرا ویسا ہی رکھو۔ پھر حاصل ضرب سے تیسرے کا حاصل ضرب معلوم کرلو۔)
10. اگر $S = \{a_1, a_2, \cdots, a_n\}$ تب مبادلہ گروپ S_n میں ثابت کرو کہ نصف جفت اور نصف طاق مبادلات ہوں گے۔
11. سائکلی گروپ $G = \{a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$ کے تمام مولد معلوم کرو۔

5.6.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. سائکلی گروپ کی تعریف کرو اور ثابت کرو کہ ہر سائکلی گروپ ابیلین ہوتا ہے۔
2. ثابت کرو کہ سائکلی گروپ کا ہر تحت گروپ سائکلی ہوتا ہے۔

3. اگر $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ تو

$i.$ fg $ii.$ gf $iii.$ $(fg)^{-1}$ $iv.$ $g^{-1}f^{-1}$ $v.$ f^2

کو معلوم کرو۔

4. $f = (1\ \ 3\ \ 6)(1\ \ 3\ \ 5\ \ 7)(6\ \ 7)(1\ \ 2\ \ 3\ \ 4)$ کو غیر مشترک سائکلوں کے حاصل ضرب پر ظاہر کرو۔اس کا معکوس معلوم کرواور یہ معلوم کرو کہ آیا یہ طاق مبادلہ ہے۔

5.7 مزید مطالعے کے لیے تجویز کردہ کتابیں(Suggested Books for Further Readings)

1. Text Book of Differential Equations, Khalil Ahmad, Real World Education Publishers, New Delhi
2. Ordinary and Partial Differential Equations- Rai Singhania, S.Chand & Company, New Delhi
3. A Text Book of B.Sc. (Mathematics), Volume –I , V. Venkateshwara Rao and others, S. Chand & Company New Delhi

اکائی6۔ گروپس کی ہم مارفیت

(Homomorphism of Groups)

اکائی کے اجزا

6.0 تمہید (Introduction)

ہم مارفیت کا نظریہ دو گروپوں کے درمیان رشتہ کو تشکیل دیتا ہے۔ بلکہ اُسکے درمیان معادلی رشتہ کو تشکیل دیتا ہے۔ ہم جانتے ہیں کہ اکائی کے جذر المکعب $\{1, w, w^2\}$ ضربی گروپ بناتے ہیں اور $\{0,1,2\}$ بہ مقیاس جمع پر گروپ بناتے ہیں۔ ان دو گروپوں کے درمیان ایک نقش f اگر ہم یوں تشکیل دیں کہ $f(1=w^0)=0$ $f(w^1)=1$ $f(w^2)=2$ تب ہم دیکھتے ہیں کہ ایک ایک اور بر نقش ہے لیکن ہم $f(1.w), f(1.w^1)=$ اور $f(w.w^2)$ اُنکے عکسوں $0+1,0+2,1+2$ کے متعلق کیا کہہ سکتے ہیں؟ یہ نظریات مزید دلچسپی کا باعث ہیں اور تحقیقات کے نئے ابواب کا نقیب ہے۔ اس سے متعلق قضیے اور مشقیں اس اکائی میں زیر بحث رہیں گی۔

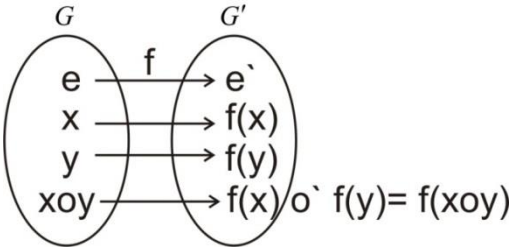
6.1 مقاصد (Objectives)

اس اکائی کے مطالعہ، تکمیل کے بعد آپ اس قابل ہو جائیں گے کہ دو گروپس کے بیچ ہم مارفیت کب ہوتی ہے۔ اور اسکا کرنل کیا ہوتا ہے۔ کرنل کی خصوصیات کیا ہیں۔ ہم مارفیت اگر برہو اور ایک ایک ہو یا دونوں ہوں تو انکے نام میں کیا خصوصیت جمع ہوتی ہے۔ ہم مارفیت سے متعلق قضیے اور دیئے ہوئے دو گروپس کے بیچ ہم مارفیت ممکن ہے یا نہیں جان لیں گے۔

6.2 تعریفات اور حل شدہ مشقیں (Definitions and Solved Examples)

گروپ ہم مارفیت (Group Homomorphism)

تعریف: فرض کرو کہ (G,O) اور (G',O') دو گروپ ہیں اور $f, G \to G'$ ایک نقش ہے۔ یہ ہم مارفیت (Homomorphism) کہلاتا ہے۔ اگر $f(xoy) = f(x)O'f(y) \forall x, y \in G$ اسکو نقش میں یوں ظاہر کیا جاسکتا ہے۔



نوٹ: (1) ہم مارفیت میں ہمیشہ G کی اکائی کا عکس G' کی اکائی ہوتا ہے۔

(2) اگر $f(x) = e' \forall\ x\ G$ تب f ہم مارفیت ہوتا ہے۔

چوں کہ $x_1, x_2 \in G \Rightarrow f(x_1.\ x_2) = e'$

$= e'e'$

$= f(x_1)f(x_2)$

لہذا f ہم مارفیت ہے۔

اور اس کو کمترین ہم مارفیت (Least Homomorphism) کہتے ہیں۔

(3)عام طور پر قضیوں میں $(G,\bullet)$ اور $(G',\bullet)$ لیا جاتا ہے۔

تعریف(2): ہم مارفیت کا عکس(Image of Homomorphism)

اگر $f:G\to G'$ ہم مارفیت ہے تب f کا عکس یا(Range of f)یوں ہوتا ہے۔ $f(G)=I_m(f)=\{f(x)/x\in G\}$

اور یاد رہے کہ $f(G)\subseteq G'$

تعریف(3) : جو ہم مارفیت ایک ایک ہوتا ہے اُسے وحید مارفیت(Monomorphism)کہتے ہیں۔

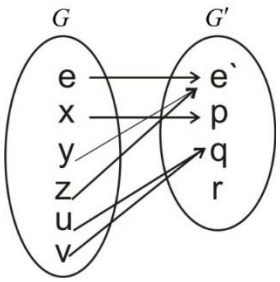
تعریف(4): جو ہم مارفیت بر ہوتا ہے۔اُسے بر مارفیت(Epimorphism)کہتے ہیں۔

تعریف(5): جو ہم مارفیت ایک ایک اور بر دونوں ہو تو اُسے یک مارفیت(Isomorphism)کہتے ہیں۔

تعریف(6): اگر $f:G\to G$ یعنی خود ہم مارفیت ہو تو اسے خود مارفیت(Automorphism)کہتے ہیں۔

تعریف(7): ہم مارفیت کا کرنل(Kernel of a Homomorphism) اگر $f:G\to G'$ ایک ہم مارفیت ہے تب G کے اُن تمام عناصر کا سیٹ جو G' کی اکائی پر نقش ہوتے ہیں f کا کرنل(Kernel of f) کہلاتا ہے۔یعنی

$Ker\ f=\{x\in G/\ f(x)=e'\}$ جہاں $e'\in G'$ اکائی ہے۔مثلاً



تب $Ker\ f=\{e,y,z\}$

نوٹ: $Ker\ f\neq\phi$ کیوں کہ $f(e)=e'$ ہمیشہ ہوتا ہے۔اس لیے کم از کم $e\in Ker\ f$

مثال1۔ $(R,\bullet)$ اور $(R^+,\bullet)$ دو گروپ ہیں اور نقش $f:R\to R^+$ اس طرح کہ $f(x)=a^x\ \forall\ x\in R$ اور $a>0,\neq 1$

تب f ہم مارفیت ہوتا ہے۔

توجہ کریں $\therefore x,y\in R \qquad x+y\in R$

تب $f(x)=a^x$

اور $f(y)=a^y$

اور پھر $f(x+y)=a^{x+y}$

$=a^x.\ a^y$

$=f(x)\,f(y)$

چنانچہ ثابت ہوا کہ f ہم مارفیت ہے۔

اس کے کرنل کے لیے اگر $f(x)=1$ یہاں $1\in R^+$ اکائی ہے۔

$$\Rightarrow a^x = 1$$
$$\Rightarrow x = 0$$
$$\Rightarrow \ker f = \{0\}$$

مثال2۔ اگر $(\mathbb{Z},+)$ ایک گروپ ہے اور $G'=\{1,-1\}$ ضربی گروپ ہے۔تب نقش $f:\mathbb{Z}\to G'$ اس طرح کہ

$$f(n)=\begin{cases}1, & \text{اگر } n \text{ ہے جفت}\\ -1, & \text{اگر } n \text{ ہے طاق}\end{cases}$$

تب f ہم مارفیت ہوتا ہے اور اسکا کرنل بھی معلوم کریں۔

حل۔ فرض کرو کہ $x_1, x_2 \in \mathbb{Z}$ جفت ہیں اور $y_1, y_2 \in \mathbb{Z}$ طاق ہیں۔

صورت(i) دو جفت عناصر کے درمیان ہم مارفیت کا امتحان کریں گا۔

$\because x_1, x_2 \in Z$ دونوں جفت ہیں اس لیے $x_1+x_2\in\mathbb{Z}$ بھی جفت ہوں گے۔

اور $$f(x_1+x_2)=f(x_1).f(x_2)$$

$$\Rightarrow 1=1.1$$

$$\Rightarrow 1=1$$

شرط صحیح ہوئی۔

صورت:(ii) ایک جفت اور ایک طاق عنصر کے درمیان $x_1, y_1\in\mathbb{Z}$ جہاں x_1 جفت اور y_1 طاق ہے تب x_1+y_1 طاق ہوگا۔تب

$$f(x_1+y_1)=f(x_1).f(y_1)$$
$$\Rightarrow -1=1.(-1)$$

$$-1=-1$$

شرط صحیح ہوئی۔

صورت(iii) دونوں عناصر طاق ہوں۔تب اگر $y_1, y_2\in\mathbb{Z}$ دونوں طاق ہیں تب y_1+y_2 جفت ہوگا۔

تب $$f(y_1+y_2)=f(y_1).f(y_2)$$
$$\Rightarrow 1=(-1).(-1)$$

$$1=1$$

شرط یہاں بھی صحیح ہوئی۔

چنانچہ ہم مارفیت کی شرط ہر صورت پوری ہوئی اس لیے f ایک ہم مارفیت ہے۔

اب f کا کرنل معلوم کرنے کے لیے فرض کرو کہ $f(x)=1$ ، جہاں $'1'$,G' کی اکائی ہے۔

ہم جانتے ہیں کہ ہر جفت $x\in\mathbb{Z}$ کے لیے عکس '1' ہے۔اسلیے کرنل میں سارے جفت معہ '0' کرنل میں موجود ہوں گے۔

6.3 قضیے اور حل شدہ مشقیں (Theorems and Solved Examples)

قضیہ 1۔ اگر $f:G\to G'$ ہم مارفیت ہے اور اگر $a\in G$ اور $|a|$ متناہی ہے۔ تب $|f(a)|$ تقسیم کرتا ہے $|a|$ کو

ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(\overline{G},\bullet)$ دو گروپ ہیں اور $f:G\to G'$ ہم مارفیت ہے۔

اور $a\in G$ اور $|a|=n$ یعنی $x^n=e$، جہاں $e\in G$ اکائی ہے۔

تب $f(a)\in\overline{G}$

اور چوں کہ $f(e)=e'$ جہاں $e'\in\overline{G}$ اکائی ہے۔

غور کرو کہ
$$e'=f(e)=f(a^n)$$
$$=[f(a)]^n$$
$$\Rightarrow |f(a)|=n$$

تب یہ بات صاف ہے کہ $|f(a)|$ تقسیم کرتا ہے $|a|$ کو کیوں کہ دونوں بھی n ہیں۔

قضیہ ثابت ہوا۔

قضیہ 2۔ اگر $f:G\to G'$ ایک ہم مارفیت ہے تب $\ker f$ تحت گروپ ہوتا ہے۔G گروپ کا۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(G',\bullet)$ دو گروپ ہیں اور $e\in G$، $e'\in G'$ اُنکے اکائی ہیں۔

ہم جانتے ہیں کہ $Ker\ f=\{x\in G/\ f(x)=e'\}$

ہمیں ثابت کرنا ہے کہ $Ker\ f$ تحت گروپ ہے G کا۔ یہ تو ظاہر ہے کہ $Ker\ f\subseteq G$ اور $Ker\ f\neq\phi$ کیوں کہ $f(e)=e'$

اسلیے $e\in Ker\ f$

اب مان لو کہ $x,y\in Ker\ f$

تب $f(x)=e'\ f(y)=e'$

اور چوں کہ $x,y\in Ker\ f\Rightarrow x,y\in G$

$$\Rightarrow xy^{-1}\in G$$

تب توجہ کرو کہ $f(xy^{-1})=f(x)\,f(y^{-1})$ ہم مارفیت کی وجہ

$$=e^1[f(y)]^{-1}$$
$$=e^1.(e^1)^{-1}$$
$$=e^1.e^1$$
$$=e^1$$
$$f(xy^{-1})=f(x)\,f(y^{-1})$$

اس سے ثابت ہوا کہ $Ker\ f$ تحت گروپ ہے G کا۔ قضیہ ثابت ہوا۔

قضیہ 3۔ اگر f ایک ہم مارفیت ہے۔ G گروپ سے G' گروپ پر تب $Ker\ f$ نارمل تحت گروپ ہوتا ہے G کا

ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(G',\bullet)$ دو گروپ ہیں اور $e \in G$ اور $e' \in G'$ دونوں کی اکائیاں ہیں۔ اور $f : G \to G'$ ہم مارفیت ہے۔ ہم جانتے ہیں کہ $\ker f = \{x \in G / f(x) = e'\}$ ہے۔ ہمیں ثابت کرنا ہے کہ $\ker f$ نارمل تحت گروپ ہوتا ہے G کا۔ ہم ثابت کریں گے کہ $\ker f$ تحت گروپ ہے G کا پھر نارمل کی شرط دیکھیں گے۔

یہ تو ظاہر ہے کہ $Ker\ f \subseteq G$

اور $Ker\ f \neq \phi$ چوں کہ $f(e) = e'$ اس لیے $e \in Ker\ f$

اب مان لو کہ $x, y \in Ker\ f$

تب $f(x) = e'\ f(y) = e'$

اور چوں کہ $x, y \in G$

$$\Rightarrow xy^{-1} \in G$$

اب غور کرو ہم مارفیت کی وجہ

$$\begin{aligned} f(xy^{-1}) &= f(x)\, f(y^{-1}) \\ &= e'\left[f(y)\right]^{-1} \\ &= e'.(e')^{-1} \\ &= e'.e' \\ &= e' \end{aligned}$$

$$\Rightarrow xy^{-1} Ker\ f \qquad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

یہاں ثابت ہوا کہ $Ker\ f$ تحت گروپ ہے G کا۔ اب نارمل کی شرط دیکھیں۔

مان لو کہ $g \in G$ اور $x \in Ker\ f$

تب غور کرو کہ

$$\begin{aligned} f(g\,x\,g^{-1}) &= f(g)\, f(x)\, f(g^{-1}) \\ &= f(g) e' \left[f(g)\right]^{-1} \\ &= f(g)\left[f(g)\right]^{-1} \\ &= e' \end{aligned}$$

$$\Rightarrow g\,x\,g^{-1} \in Ker\ f\ \ \forall x \in Ker\ f\ \ \&\ \forall g \in G$$

یہاں معلوم ہوا کہ $Ker\ f$ نارمل تحت گروپ ہے G کا۔

لہذا قضیہ ثابت ہوا۔

قضیہ 4۔ اگر f ہم مارفیت ہے G سے G' پر تب $f(a) = f(b)$ اگر اور صرف اگر $a \ker f = b \ker f$

ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(G',\bullet)$ دو گروپ ہیں اور $e\in G$ اور $e'\in G'$ ان کی اکائیاں ہیں اور $f:G\to G'$ ہم مارفیت ہے۔

ہم جانتے ہیں کہ $Ker\ f=\{x\in G/\ f(x)=e'\}$

اگر $a,b\in G$ تب $a\ker f=b\ker f$ دو ہم سٹس ہوں گے $\ker f$ کے G میں اب اگر $f(a)=f(b)$

$$[f(a)]^{-1}\in G\ \because\Leftrightarrow [f(a)]^{-1}f(a)=[f(a)]^{-1}f(b)$$
$$\Leftrightarrow e'=f(a^{-1})f(b)$$
$$\Leftrightarrow e'=f(a^{-1}b)$$
$$\Leftrightarrow a^{-1}b\in \ker f$$
$$\Leftrightarrow a\ker f=b\ker f$$

چنانچہ قضیہ ثابت ہوا۔

قضیہ 5۔ اگر $\phi:G\to\bar{G}$ ہم مارفیت ہے اور $g\in G$ اگر $\phi(g)=g'$ تب
$\phi^{-1}(g')=\{x\in G/\phi(x)=g'\}=g.\ker\phi$

ثبوت۔ دیا گیا ہے کہ $\phi:G\to\bar{G}$ ہم مارفیت ہے۔

اور ہم جانتے ہیں کہ $\ker\phi=\{x\in G/\phi(x)=e'\}$ اور یہ G کا تحت گروپ ہے۔

فرض کرو کہ $\phi(g)=g'\qquad g'\in\bar{G}$

تب $\phi^{-1}(g')=\{x\in G/\phi(x)=g'\}$

تب یہ ثابت کرنے کے لیے کہ $\phi^{-1}(g')=g.\ker\phi$

فرض کرو کہ $x\in\phi^{-1}(g')=\phi(x)=g'=\phi(g)$

$$\Rightarrow x\ker\phi=g\ker\phi$$
$$\Rightarrow x\in x\ker\phi=g\ker\phi$$
$$\Rightarrow\phi^{-1}(g')\subseteq g\ker\phi\ \ldots\ldots\ldots\ldots(1)$$

اور فرض کرو کہ $g(x)\in g\ker\phi$

$$\Rightarrow y\in\ker\phi\Rightarrow\phi(y)=e^1$$

تب غور کرو کہ $\phi(gy)=\phi(g)\phi(y)$

$$=g'.e'$$
$$=g'$$
$$\Rightarrow gy=\phi^{-1}(g')$$
$$\Rightarrow gy\in\phi^{-1}(g')$$
$$\Rightarrow g\ker\phi\subseteq\phi^{-1}(g^1).....(1)$$

(1)اور(2)کی مدد سے

$$\phi^{-1}(g') = g\ker\phi$$

قضیہ ثابت ہوا۔

قضیہ 6۔ اگر $\phi : G \to \overline{G}$ ہم مارفیت ہے اور اگر $|\ker\phi| = n$ تب نقش ϕ ایک $n-to-1$ نقش ہوتا ہے G سے $\phi(G)$ پر

ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(G',\bullet)$ دو گروپ ہیں۔ $e \in G$ اور $e' \in \overline{G}$ اکائیاں ہیں۔

تب ہم جانتے ہیں کہ $Ker\,\phi = \{x \in G / \phi(x) = e'\}$ یہ G کا تحت گروپ ہوتا ہے۔

فرض کرو کہ $|\ker\phi| = n$

تب $g\ker\phi = \phi^{-1}(g^1)$

فرض کرو کہ $g = e \in G,\quad g^1 = e^1 \in \overline{G}$

$$\Rightarrow e\ker\phi = \phi^{-1}(e^1)$$

$$\Rightarrow \ker\phi = \phi^{-1}(e^1)$$

تب $|\ker\phi| = |\phi^{-1}(e^1)|$

اور چوں کہ $|\ker\phi| = n$

اس لیے ϕ $n-to-1$ بر نقش ہو گا۔

قضیہ ثابت ہوا۔

قضیہ 7۔ اگر $f : G \to G'$ گروپوں کی ہم مارفیت ہے اور $e \in G$ اور $e' \in G'$ اُنکی اکائیاں ہیں تب

$(i) f(e) = e' \qquad (ii) f(x^{-1}) = [f(x)]^{-1} \forall x \in G$

ثبوت۔ (i) غور کرو $f(ee) = f(e)$

$\Rightarrow f(e)\,f(e) = f(e)$ ہم مارفیت کی وجہ سے

$\Rightarrow f(e)\,f(e) = e^1\,f(e)$ تنسیخ کے کلیہ کی وجہ سے

$\Rightarrow f(e) = e^1$

(ii) فرض کرو کہ $x \in G \Rightarrow x^{-1} \in G$

اور $xx^{-1} = e$

تب غور کرو $f(xx^{-1}) = f(x)\,f(x^{-1})$

$$\Rightarrow f(e) = f(x)\,f(x^{-1})$$

$$\Rightarrow e^1 = f(x)\,f(x^{-1})$$

$$\Rightarrow [f(x)]^{-1} = f(x^{-1})$$

قضیہ ثابت ہوا۔

قضیہ 8۔ اگر $(G,\bullet)$ اور $(G',\bullet)$ دو گروپ ہیں اور $f: G \to G'$ ہم مارفیت ہے تب $f(G)$ تحت گروپ ہوگا G' کا۔

ثبوت۔ دیا گیا ہے $f: G \to G'$ کہ ہم مارفیت ہے۔

اور $f(G) = \{ f(a) / a \in G \}$

$\Rightarrow f(G) \subseteq G'$

تب ہمیں ثابت کرنا ہے کہ $f(G)$ تحت گروپ ہوگا G^1 کا۔

فرض کرو کہ $a', b' \in f(G)$

تب $a, b \in G \ni$ اس طرح کہ $f(a) = a' \ f(b) = b'$

اب غور کرو کہ $a'(b')^{-1} = f(a)\big(f(b)\big)^{-1}$

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

ہم مارفیت کی وجہ سے

$\because ab^{-1} \in G \Rightarrow a'(b')^{-1} \in f(G)$

چنانہ $f(G)$ تحت گروپ ہو، G' کا۔

قضیہ ثابت ہوا۔

قضیہ 9۔ ابیلین گروپ کا ہم مارفی عکس بھی ابیلین ہوتا ہے۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ ابیلین گروپ ہے۔ اور ایک اور $(G',\bullet)$ گروپ ہے۔

اور $f: G \to G'$ ہم مارفیت ہے۔

دیا گیا ہے کہ G ابیلین ہے اور ثابت کرنا ہے کہ $f(G)$ ابیلین ہوگا۔

اگر $a', b' \in f(G)$ تب $a, b \in G \ni$ اس طرح کہ $f(a) = a' \ f(b) = b'$

یاد رہے کہ $ab = ba$ [$\because G$ ابیلین ہے۔]

غور کرو $a^1b^1 = f(a)\, f(b)$

ہم مارفیت کی وجہ

$= f(ab)$

$= f(ba) \qquad ab = ba \because$

$= f(b)\, f(a)$

$= b'a'$

چوں کہ تقلیبی خاصیت پوری ہوئی اس لیے $f(G)$ ابیلین ہے۔

قضیہ ثابت ہوا۔

قضیہ 10۔ سائکلی گروپ کا ہم مارفی عکس بھی سائکلی ہوگا۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ سائکلی گروپ ہے۔اور $f:G\to f(G)$ ہم مارفیت اور $G=\{a^n/n\in Z\}=\langle a\rangle$

تب G کا عکس $f(G)=\{f(a)/a\in G\}$

ہمیں ثابت کرنا ہوگا کہ $f(G)$ سائکلی ہے۔

ہم جانتے ہیں کہ $a\in G\Rightarrow f(a)\in f(G)$

اگر $b\in G$ تب $b=a^m\ m\in Z$ چوں کہ $G=\langle a\rangle$

اور $f(b)\in f(G)$ تب

$$\begin{aligned} f(b) &= f(a^m)\\ &= f(a.a.....m\ times)\\ &= f(a)\,f(a).....m\ times\\ &= [f(a)]^m \end{aligned}$$

معلوم ہوا کہ کوئی بھی عنصر $f(b)\in f(G)$ کو $f(a)$ کی کوئی قوت کے طور پر ظاہر کیا جاسکتا ہے۔

لہٰذا $f(a)$ مولد ہوا ہم مارفی عکس $f(G)$ کا چنانچہ ہم مارفی عکس $f(G)$ سائکلی ہے۔

قضیہ ثابت ہوا۔

قضیہ 11۔ اگر $f:G\to G'$ ایک گروپ ہم مارفیت ہے e اور e' اکائیاں ہیں G اور G' کی تب f ایک ایک نقش ہوگا اگر اور صرف اگر $\ker f=\{e\}$

ثبوت۔ فرض کرو کہ f ایک ایک ہے۔تب ثابت کرنا ہوگا کہ $\ker f=\{e\}$

ہم جانتے ہیں کہ $\ker f=\{x\in G/f(x)=e'\}$

تب چوں کہ ہمیشہ $f(e)=e'$

$$\Rightarrow e\in\ker f$$

یعنی $\ker f=\phi$

اب مان لیں کہ $a\in\ker f$

تب $f(a)=e'$

تو پھر $f(a)=e'=f(e)$

اور چوں کہ f ایک ایک ہے

اس لیے $a=e$

لہٰذا $\ker f=\{e\}$

اس کے بالعکس فرض کرو کہ $\ker f=\{e\}$

تب ہمیں ثابت کرنا ہوگا کہ f ایک ایک ہے۔

فرض کرو کہ $a,b \in G$

اور $f(a) = f(b)$

$$\Rightarrow f(a)\left[f(b)\right]^{-1} = f(b)\left[f(b)\right]^{-1}$$
$$f(a)f(b^{-1}) = e'$$
$$\Rightarrow \quad f(ab^{-1}) = e'$$
$$\Rightarrow \quad ab^{-1} \in \ker f = \{e\}$$
$$\Rightarrow \quad ab^{-1} = e$$
$$\Rightarrow \quad (ab^{-1})b = eb$$
$$\Rightarrow \quad a(b^{-1}b) = b$$
$$\Rightarrow \quad ae = b$$
$$\Rightarrow \quad a = b$$

چنانچہ f ایک ایک نقش ہے۔

قضیہ ثابت ہوا۔

قضیہ 12۔ اگر H نارمل تحت گروپ ہے G کا تب نقش $f : G \to \frac{G}{H}$ جو $f(a) = aH$ سے معرف ہے، ہم مارفیت ہوتا ہے۔ اس کو فطری ہم مارفیت (Natural Homomorphism) یا (Canonical Homomorphism) کہتے ہیں اور $\ker f = H$ ہوگا۔

ثبوت۔ دیا گیا ہے $f : G \to \frac{G}{H}$ اور $f(a) = aH$ $\forall a \in G$

فرض کرو کہ $a,b \in G$ تب $ab \in G$

تب غور کرو کہ $f(ab) = abH$
$$= aH.bH$$
$$= f(a)\,f(b)$$

اس سے ثابت ہوا کہ f ہم مارفیت ہے۔

اور $\ker f = \{a \in G / f(a) = H\}$

کیوں کہ $\frac{G}{H}$ کی اکائی $eH = H$ ہے۔

چوں کہ اگر $f(a) = aH = H$ $a \in \ker f$

$$\Rightarrow a \in H$$

اس لیے $\ker f = \{a \in G / a \in H\} = H$

قضیہ ثابت ہوا۔

قضیہ 13۔ اگر G ایسا گروپ ہے کہ $\frac{G}{Z(G)}$ سائکلی ہے تو G ابیلین ہوگا۔ یہاں پر $Z(G)$، G کا مرکز ہے۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ گروپ ہے۔

اور G کا مرکز $Z(G)=\{x\in G / gx=xg\forall g\in G\}$

تب ہم جانتے ہیں کہ $Z(G)$ نارمل تحت گروپ ہے G کا۔

اور $\dfrac{G}{Z(G)}=\{gZ(G)/\forall g\in Z(G)\}$

فرض کرو کہ $\dfrac{G}{Z(G)}=\langle gZ(G)\rangle$ سائکلی گروپ ہے۔

تب ہمیں ثابت کرنا ہے کہ G ابیلین ہو گا۔

فرض کرو کہ $a,b\in G$

تب $aZ(G)=(gZ(G))^i \quad i\in Z$

$=g^iZ(G)$

مان لیں $x\in Z(G)$ $\Rightarrow a=g^i.x$

اسی طرح $bZ(G)=(gZ(G))^j \quad j\in Z$

$=g^j.Z(G)$

مان لیں $b=g^j.y \quad y\in Z(G)$

اب غور کرو $ab=g^{i+j}xy$

$\because i,j\in Z \quad \therefore i+j=j+i$ اور مرکز کے عناصر بھی تقلیبی صفت پوری کرتے ہیں۔اس لیے

$ab=g^{j+i}yx$

$=ba$

لہذا $\forall\ a,b\in G$ تقلیب کی صفت پوری ہوئی۔

اسلیے G ابیلین ہے۔

قضیہ ثابت ہوا۔

مثال 1۔ اگر $f:Z_{30}\to Z_{30}$ ہم مارفیت ہے اور $\ker f=\{0,10,20\}$ اور $f(23)=9$ تب 9 کا معکوس سیٹ معلوم کرو۔

حل۔ دیا گیا ہے کہ $f:Z_{30}\to Z_{30}$ ہم مارفیت ہے۔

اور $\ker f=\{0,10,20\}$

اور $f(23)=9$

$\Rightarrow f^{-1}(9)=23+\ker f$

$=23+\{0,10,20\}$

$=\{23,33,43\}$

$= \{23, 3, 13\}$ بہ مقیاس $+_{30}$ کی وجہ

$= \{3, 13, 23\}$

مثال 2۔ اگر $(G, \bullet)$ غیر صفر حقیقی اعداد کا گروپ ہے اور $f : G \to G$ اس طرح سے کہ $f(x) = x^2, \forall x \in G$ تب ثابت کرو کہ f ہم مارفیت ہے اور اسکا کرنل بھی معلوم کرو۔

حل۔ دیا گیا ہے کہ $f : G \to G$

$$f(x) = x^2 \forall x \in G$$

فرض کرو کہ $a, b \in G \Rightarrow ab \in G$

تب $f(a) = a^2 \quad f(b) = b^2 \quad f(ab) = (ab)^2$

غور کرو $f(ab) = (ab)^2$

$= a^2 b^2$

$= f(a) f(b)$

یہاں معلوم ہوا کہ f ہم مارفیت ہے۔ اب اسکا کرنل معلوم کرنے کے لیے ہم جانتے ہیں کہ $1 \in G$ اکائی ہے۔

اسلیے $\ker f = \{x \in G / f(x) = 1\}$

$f(x) = 1 \therefore$

$\Rightarrow x^2 = 1$

$\Rightarrow x = \pm 1$

اس لیے کرنل $\ker f = \{1, -1\}$

مثال 3۔ اگر $(Z, +)$ اور $G = (\{1, -1, i, -i\}, \bullet)$ دو گروپ ہیں اور نقش $f : Z \to G$ اس طرح سے کہ $f(n) = i^n \quad n \in Z$ تب ثابت کرو کہ f ہم مارفیت ہے اور اس کا کرنل بھی معلوم کر۔

حل۔ دیا گیا ہے۔ $f : Z \to G$

$$f(n) = i^n \quad n \in Z$$

اور ظاہر ہے کہ اسکی $1 \in G$ اکائی ہے۔

اگر $a, b \in Z$ تب $a + b \in Z$

غور کرو $f(a + b) = i^{a+b}$

$= i^a . i^b$

$= f(a) f(b)$

چنانچہ f ہم مارفیت ہوا۔

اب کرنل معلوم کرنے کے لیے

ہم دیکھتے ہیں کہ $f(1)=i^1=i,\ f(2)=i^2=-1$

$f(3)=i^3=-i,\ f(4)=i^4=1$

$f(5)=i^5=i,\ f(6)=i^6=-1$

لہذا f برتفاعل ہےاور ہر چار عناصر بعد مکرر عکس پائے جاتے ہیں۔

جیسے $i^4=1=i^8=i^{12}.....$

لہذا $\ker f=\{n\in Z\ /\ f(n)=1\}$

$i^{4n}=1$

اس لیے $f(4n)=1$

$\therefore \ker f=\{4n/n\in Z\}$

مثال4۔ اگر $(Z,+)$ صحیح اعداد کا گروپ ہے اور نقش $f:Z\to Z$ ہے جہاں $f(x)=Zx\quad \forall x\in Z$ تب ثابت کرو کہ f ہم مارفیت ہےاُسکا کرنل معلوم کرواور معلوم کرو کہ آیا f برہم مارفیت ہے۔

حل۔ دیا گیاہے کہ $f:Z\to Z$ اور $f(x)=Zx,\ \forall x\in Z$

اگر $a,b\in Z$ تب $a+b\in Z$

غور کرو $f(a+b)=2(a+b)=2a+2b$

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

اس لیے f ہم مارفیت ہے۔

اور چوں کہ $0\in Z$ اکائی ہو گی۔

اس لیے کرنل کے لیے اگر $f(x)=2x=0$

$\Rightarrow x=0$

لہذا $\ker f=\{0\}$

چوں کہ $2x$ عکس ہمیشہ جفت ہوتا ہے اس لیے سارے طاق اعداد دوسرے گروپ یعنی (Codomain) میں چھوٹے ہوئے ہوں گے۔اس لیے f برہم مارفیت نہیں ہے۔

مثال5۔ اگر $f:C_0\to C_0$ جہاں $f(Z)=Z^n$ اور $Z\in C_0$ اور n ایک مستقل (Constant) مثبت صحیح عدد ہے تو ثابت کرو کہ f برہم مارفیت ہےاور اسکا کرنل بھی معلوم کرو۔

حل۔ ہم جانتے ہیں $(C_0,\bullet)$ گروپ ہوتا ہے۔

اور دیا گیاہے کہ $f:C_0\to C_0$

$f(Z)=Z^n\quad Z\in C_0$ اور n مقرر (Constant) مثبت صحیح عدد ہے۔

فرض کرو کہ $Z_1, Z_2 \in C_0$ تب $Z_1, Z_2 \in C_0$ (بند شی خاصیت کی بناء)

تب $f(Z_2) = Z_2^{\,n}$ $f(Z_1) = Z_1^{\,n}$ اور $f(Z_1 Z_2) = (Z_1 Z_2)^n$

غور کرو $f(Z_1 Z_2) = (Z_1 Z_2)^n$

$$= Z_1^{\,n} . Z_2^{\,n}$$
$$= f(Z_1) f(Z_2)$$

چنانچہ f ہم مارفیت ہے۔

اور اگر $f(Z_1) = f(Z_2)$

$$\Rightarrow Z_1^{\,n} = Z_2^{\,n}$$
$$\Rightarrow Z_1 = Z_2$$

یہاں f ایک ایک ہوا چوں کہ $f : C_0 \to C_0$ ایک ایک ہے اسلیے بر نقش ہے۔ لہذا f برہم مارفیت ہے۔

کرنل کے لیے فرض کرو کہ $f(Z) = Z^n = 1$

لہٰذا Z کے جذر۔n $\left(n^{th}\ roots\right)$ کرنل ہو گا۔

اس لیے $\ker f = \left\{ e^{2\pi i/n} / r = 0,1,2,.....(n-1) \right\}$

مثال 6۔ 6 یا 6 سے کم رتبہ رکھنے والے تمام گروپس کی درجہ بندی کرو۔

حل۔ (i) اگر $o(G) = 1$ تب $G = \{e\}$ معمولی گروپ ہے۔

(ii) اگر $o(G) = 2$ تب یہ ایک مفرد عدد ہے اور ہر مفرد عدد کے رتبہ کا گروپ سائکلی ہوتا ہے۔ نتیجتاً ابیلین ہوتا ہے چوں کہ ہر سائکلی ابیلین ہوتا ہے۔ چوں کہ ایک ہی رتبہ کے دو سائکلی گروپ ہم مارفی ہوتے ہیں اس لیے اگر $G = \left(\{1,-1\}, \bullet\right)$ گروپ ہو تب کسی دوسرے دو رتبہ والے گروپ سے ہم مارف ہوتا ہے۔

(iii) اگر $o(G) = 3$ تب یہ ایک مفرد ہونے کی بناء سائکلی اور نتیجتاً ابیلین ہوتا ہے۔ چنانچہ اگر $G = \left(\{1, w, w^2\}, \bullet\right)$ گروپ ہو تب کسی دوسرے 3 رتبہ والے گروپ سے ہم مارف ہوتا ہے۔

(iv) اگر $o(G) = 4 = 2^2$ تب $o(G) = 4 = 2^2$ اور ہم جانتے ہیں کہ اگر p مفرد عدد ہے تب p^2 رتبہ والا گروپ ابیلین ہوتا ہے لہذا G ابیلین گروپ ہو گا۔

لیکن یہاں دو امکانات ہیں۔

فرض کرو کہ $a \in G$ اور $o(a) = 2$ یا $o(a) = 4$ یہ اس لیے کہ چوں کہ $o(a)$ تقسیم کرتا ہے $o(G)$ کو۔

اگر $o(a) = 2$ تو اکائی عنصر اور a ، G کے پورے عناصر کی تکمیل نہیں کرتے۔

فرض کرو کہ $b \in G$ اور $b \neq a$

اگر $o(a)=4$ تب G میں عناصر کی تعداد چار سے زیادہ ہوگی۔ چوں کہ G گروپ ہے یہ اخذ ہوتا ہے کہ $a.b \in G$ مزید یہ کہ $o(ab)=2$

اس طرح سے $G=\{e,a,b,ab\}$ جو کہ کلائین کا 4 گروپ ہے۔ یہ ابیلین ہوتا ہے۔ اور دو عناصر a اور b سے تخلیق پاتا ہے۔ G سائکلی نہیں کیوں کہ کوئی واحد عنصر سارے گروپ کی تخلیق نہیں کرتا۔

اگر $o(b)=4$ تب G سائکلی اور نتیجتاً ابیلین ہوتا ہے۔ چوں کہ ایک ہی رتبہ رکھنے والے دو سائکلی گروپس یک مارفی ہوتے ہیں اس لیے $G=(\{1,-1,i,-i\},\bullet)$ رتبہ 4 والے ہر سائکلی گروپ سے ہم صارف ہوتا ہے۔

(v) اگر $o(G)=5$ تو چوں کہ 5 ایک مفرد عدد ہے اس لیے یہ سائکلی اور نتیجتاً ابیلین ہوتا ہے۔ اور کسی بھی 5 رتبہ والے گروپ کے ہم مارف ہوتا ہے۔

(vi) اگر $o(G)=6$ تب دو امکانات ہیں۔

یا تو G ایک چھٹے رتبہ کا عنصر رکھتا ہے یا G چھٹے رتبہ کا عنصر نہیں رکھتا۔ اگر G میں کوئی چھٹے رتبہ کا عنصر موجود ہے تو یہ سائکلی ہوگا اور نتیجتاً ابیلین ہوگا۔ اگر G میں کوئی چھٹے رتبہ کا عنصر موجود نہیں ہے تو اس میں 2 اور 3 رتبہ والے عناصر موجود ہوں گے۔ اس صورت میں $G = S_3$ اور غیر ابیلین ہوگا۔

مثال 7۔ اگر $(R,+)$ اور $(R^+,\bullet)$ دو گروپس ہیں تب نقش $f:R^+ \to R$ معرف بہ $f(x)=\log_{10} x, \forall x \in R^+$ تب ثابت کرو کہ f ہم مارفیت ہے اور اس کا کرنل بھی معلوم کرو۔

حل۔ دیا گیا ہے کہ $f:R^+ \to R$

$$f(x)=\log_{10} x \qquad \forall x \in R^+ \text{ اور}$$

فرض کرو کہ $a,b \in R^+ \Rightarrow ab \in R^+$ تب $f(a)=\log_{10} a,\quad f(b)=\log_{10} b,\quad f(ab)=\log_{10} ab$

غور کرو کہ
$$\begin{aligned} f(ab) &= \log_{10} ab \\ &= \log_{10} a + \log_{10} b \\ &= f(a)+f(b) \end{aligned}$$

لہٰذا f ہم مارفیت ہوا۔

اب کرنل معلوم کرنے کے لیے

چوں کہ $(R,+)$ میں '0' اکائی ہے۔

اسلیے $\ker f = \{x \in R^+ / f(x)=0\}$

$$\begin{aligned} f(x) &= \log_{10} x = 0 \qquad \therefore \\ &\Rightarrow x = 1 \end{aligned}$$

اس لیے $\ker f = \{1\}$

مثال 8۔ اگر $(R_0, \bullet)$ گروپ ہے غیر صفر حقیقی اعداد کا اور $f : R_0 \to R_0$ اس طرح سے کہ $\forall x \in R_0 \quad f(x) = |x|$ تب ثابت کرو کہ f ہم مارفی ہے اور اسکا کرنل بھی معلوم کرو۔

حل۔ دیا گیا ہے کہ $f : R_0 \to R_0$

جہاں $\forall x \in R_0 \quad f(x) = |x|$

فرض کرو کہ $a, b \in R_0 \Rightarrow ab \in R_0$

تب $f(a) = |a| \quad f(b) = |b| \quad f(ab) = |ab|$

غور کرو $f(ab) = |ab|$

$$= |a|\,|b|$$

$$= f(a)\, f(b)$$

یہاں ثابت ہوا کہ f ہم مارفی ہے۔

اب f کے کرنل کے لیے

چوں کہ $(R_0, \bullet)$ میں '1' اکائی ہے۔

اس لیے $\ker f = \{x \in R_0 \,/\, f(x) = 1\}$

تب $f(x) = |x| = 1$

$$\Rightarrow x = \pm 1$$

اس لیے $\ker f = \{1, -1\}$

مثال 9۔ اگر $\phi : GL(2, R) \to (R_0, \bullet)$ معرف بہ $\phi(A) = \det A$ ہو $\forall A \in GL(2, R)$ تب ثابت کرو کہ ϕ ہم مارف ہے اور اس کا کرنل بھی معلوم کرو۔

حل۔ فرض کرو کہ $A, B \in GL(2, R)$ تب $AB \in GL(2, R)$

اور $\phi(A) = |A| \quad \phi(B) = |B| \quad \phi(AB) = |AB|$

غور کرو کہ $\phi(AB) = \det(AB) = |AB|$

$$= |A|\,|B|$$

$$= \phi(A)\ \phi(B)$$

لہذا ϕ ہم مارف ہوا۔

اور اب کرنل کے لیے ہمیں معلوم ہے کہ $(R_0, \bullet)$ میں اکائی '1' ہے۔

اس لیے $\ker \phi = \{A \in GL(2, R) \,/\, \phi(A) = 1\}$

$$\phi(A) = |A| = 1 \qquad \therefore$$
$$\Rightarrow A \in SL(2,R)$$

لہذا $\ker \phi = SL(2,R)$

نوٹ: $SL(2,R)$، (Special Linear Group) ہے جہاں 2×2 رتبہ کے حقیقی اعداد ماترس جنکا $\det = 1$ ہوتا ہے۔

مثال 10۔ ثابت کرو کہ نقش $f:(R,+)\to GL(2,R)$ اس طرح کہ $\forall\, x \in R$ $f(x) = \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix}$ ہم مارفیت ہے اور اسکا کرنل معلوم کرو۔

حل:۔ دیا گیا ہے کہ $f:(R,+)\to GL(2,R)$

اور $\qquad f(x) = \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix} \forall\, x \in R$

فرض کرو کہ $x, y \in R$

تب $x+y \in R$ بند شی خاصیت کی بناء

تب غور کرو کہ $\qquad f(x) = \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix}$

$$f(y) = \begin{bmatrix} \cos y & \sin y \\ -\sin y & \cos y \end{bmatrix} \;\&\; f(x+y) = \begin{bmatrix} \cos(x+y) & \sin(x+y) \\ -\sin(x+y) & \cos(x+y) \end{bmatrix}$$

$$f(x).f(y) = \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix}.\begin{bmatrix} \cos y & \sin y \\ -\sin y & \cos y \end{bmatrix}$$
$$= \begin{bmatrix} \cos x\cos y - \sin x\sin y & \cos x\sin y + \sin x\cos y \\ -\sin x\cos y - \cos x\sin y & -\sin x\sin y + \cos x\cos y \end{bmatrix}$$
$$= \begin{bmatrix} \cos(x+y) & \sin(x+y) \\ -\sin(x+y) & \cos(x+y) \end{bmatrix}$$
$$= f(x+y)$$

f ہم مارفیت ہے۔

اب کرنل معلوم کرنے کے لیے ہم جانتے ہیں $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2,R)$ اکائی ہے۔

اگر $\qquad f(x) = \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$\Rightarrow \cos x = 1 \qquad \sin x = 0$$
$$\Rightarrow x = 2n\pi \;\; n \in Z$$
$$\therefore \ker f = \{2n\pi / n \in Z\}$$

6.4 کلیدی الفاظ (Keywords)

ہم مارفیت، نقش، وحید مارفیت، دور بطی، یک مارفیت، کرنل، عکس، سالگلی

6.5 اکتسابی نتائج(Learning Outcomes)

گروپوں کے درمیان ایک خاص نقش کو ہم مارفیت کہتے ہیں۔ یہ نقش ایک ایک ہو تو وحید مارفیت اور بر ہو تو برمارفیت اور دونوں ہوں (دور بطی) تب اسے یک مارفیت کہتے ہیں۔ کرنل اُن عناصر کا سیٹ ہے پہلے گروپ سے جو دوسرے گروپ کے اکائی پر نقش ہوتے ہیں۔ ہم مارفیت کا کرنل پہلے گروپ کا نارمل تحت گروپ ہوتا ہے۔ ایپلین گروپ کا ہم مارفی عکس بھی ایپلین ہوتا ہے۔ ہم مارفیت میں ہمیشہ دونوں گروپوں کی اکائیاں نقش ہوتی ہیں۔ سائکلی گروپ کا ہم مارفی عکس بھی سائکلی ہوتا ہے۔ نقش $f : G \to \frac{G}{H}$ جہاں $f(a) = aH$ فطری ہم مارفیت کہلاتا ہے۔ ہم مارفیت کو ثابت کرنے اور کرنل معلوم کرنے کی چند مشقیں حل کی گئیں۔

6.6 نمونہا متحانی سوالات(Model Examination Questions)

6.6.1 معروضی جوابات کے حامل سوالات(Objective Answer Type Questions)

1. ہم مارفیت کی تعریف کیجیے۔
2. کرنل کی تعریف کرو۔
3. یک مارفیت کی تعریف کیجیے۔

6.6.2 مختصر جوابات کے حامل سوالات(Short Answer Type Questions)

1. اگر $f: G \to G'$ گروپوں کی ہم مارفیت ہے اور $e \in G$ اور $e' \in G'$ ان کی اکائیاں ہیں تب ثابت کرو کہ
   (a $f(e) = e'$
   (b $f(x^{-1}) = [f(x)]^{-1}, \forall x \in G$
2. اگر $(G,\cdot)$ اور $(G',\cdot)$ دو گرپس ہیں اور $f: G \to G'$ ہم مارفیت ہے تب ثابت کرو کہ $f(G)$، G' کا تحت گروپ ہوگا۔
3. اگر $(G,\cdot)$ غیر صفر حقیقی اعداد کا گروپ ہے اور $f: G \to G$ اس طرح سے ہے کہ $f(x) = x^2, \forall x \in G$ تب ثابت کرو کہ f ہم مارفیت ہے اور اس کا کرنل بھی معلوم کرو۔
4. اگر $(R^+,\cdot)$ اور $(R,+)$ دو گروپس ہیں تب نقش $f: R^+ \to R$ معرف بہ $f(x) = \log_{10} x, \forall x \in R^+$ تب ثابت کرو کہ f ہم مارفیت ہے اور اس کا کرنل بھی معلوم کرو۔

6.6.3 طویل جوابات کے حامل سوالات(Long Answer Type Questions)

1. ثابت کرو کہ کرنل نارمل تحت گروپ ہوتا ہے۔
2. ثابت کرو کہ ایپلین گروپ کا ہم مارفی عکس بھی ایپلین ہوتا ہے۔
3. ثابت کرو کہ سائکلی گروپ کا ہم مارفی عکس بھی ایپلین ہوتا ہے۔
4. اگر $f: G \to G'$ ہم مارفیت ہے اور e اور e' اکائیاں ہیں تب ثابت کرو کہ ایک ایک نقش ہوگا اگر اور صرف اگر $kerf = \{e\}$ ہے۔

6.7 مزید مطالعے کے لیے تجویز کردہ کتابیں(Suggested Books for Further Readings)

1. Text Book of Differential Equations, Khalil Ahmad, Real World Education Publishers, New Delhi
2. Ordinary and Partial Differential Equations- RaiSinghania, S.Chand& Company, New Delhi
3. A Text Book of B.Sc. (Mathematics), Volume –I , V. VenkateshwaraRao and others, S. Chand & Company New Delhi

اکائی 7۔ گروپس کی یک مارفیت

(Isomorphism of Groups)

اکائی کے اجزا

7.0 تمہید(Introduction)

پچھلی اکائی میں دو گروپوں کے درمیان نقش ہم مارفیت کب کہلاتا ہے، ہم نے جانا۔اس کے متعلق قضیے زیر بحث رہے گی جسکو یک مارفیت سے تعبیر کرتے ہیں۔ ہم مارفیت کا بنیادی قضیہ بیان اور ثابت ہوگا۔ کیلے(Caylay)کا قضیہ (Permutation Group)پر یک مارفیت ثابت کرے گا۔ یک مارفیت سے متعلق قضیوں کی تعداد اور مشقیں اس قدر ہیں کہ اسکو ایک علٰحدہ اکائی بنانا مناسب ہوا۔

7.1 مقاصد(Objectives)

اس اکائی کی تکمیل کے بعد آپ اس قابل ہو جائیں گے کہ دیا ہوا نقش یک مارفی ہے یا نہیں جانچ کر سکیں گے۔ یک مارفیت کے متعلق قضیے، ثابت کر سکیں گے۔ ہم مارفیت کا بٹادی قطیہ بیان اور ثابت کر سکیں گے۔ کیلے(Caylay)کا قضیہ بیان اور ثابت کر سکیں گے اور ان کے متعلق مشقوں کو حل کر پائیں گے۔

7.2 تعریفات اور مثالیں(Definitions and Examples)

یک مارفیت(Isomorphism): فرض کرو کہ $(G,0)$اور $(G',0')$دو گروپ ہیں اور $f:G\to G'$ جو دو ربطی یعنی ایک ایک اور بر(1-1 & onto)ہم مارفیت ہے۔تب f یک مارفیت کہلاتا ہے۔ یا

$f:G\to G'$ یک مارفیت کہلاتا ہے، اگر تین شرطیں پوری ہوں۔

(1) $f(a,b)=f(a)0f(b)\forall a,b\in G$ (ہم مارفیت)

(2) f ایک ایک ہو (1-1)

(3) f بر تفاعل ہو (onto)

نوٹ:۔(1) $f:G\to G'$ یک مارفیت ہو تو یوں ظاہر کیا جاتا ہے۔ $G\cong G'$

(2)اگر ہم مارفیت ہو تو یوں ظاہر کیا جاتا ہے۔ $G\simeq G'$

مثال1۔ اگر $(R,+)$اور $(R^+,\bullet)$ دو گروپ ہوں تب $\varphi:R\to R^+$

معرف بہ $\varphi(x)=2^x$ $\forall x\in R$ یک مارفیت ہوتا ہے۔

فرض کرو کہ $x,y\in R\Rightarrow x+y\in R$

تب
$$\varphi(x+y)=2^{(x+y)}$$
$$=2^x.2^y$$
$$=\varphi(x).\varphi(y) \quad \text{--------(1)}$$

اور اگر
$$\varphi(x)=\varphi(y)$$
$$\Rightarrow \quad 2^x=2^y$$
$$\Rightarrow \quad x=y$$

$\Rightarrow$ ہے $1.1\ \varphi$ ---------(2)

اور کسی بھی $a \in R^+$ کے لیے $log_2 a \in R$

اس طرح سے کہ $\varphi(log_2 a) = 2^{log_2 a} = a$

(3) لہٰذا φ برنقش ہے۔

(1) (2) اور (3) کی مدد سے ثابت ہوا کہ ϕ یک مارفیت ہے۔

مثال2۔ اگر $G = \{..... -3,-2,-1,0,1,2,3,.....\}$ اور $m \in \mathbb{Z}$

$G' = \{.....-2m, -m, , 0, m, 1m, 2m, 3m.....\}$ دو جمع کے عمل سے گروپ ہیں۔

تب نقش $f: G \to G'$ جہاں $f(a) = ma,\ \forall a \in G$

یک مارفیت ہوتا ہے۔

فرض کرو کہ $a,b \in G,$ تب $a+b \in G$

غور کرو $f(a+b) = m(a+b)$

$= ma + mb$

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

$\Rightarrow$ f ہم مارفیت ہے۔ ----------(1)

اور اگر $f(a) = f(b)$

$ma = mb$

$\Rightarrow a = b$

$\Rightarrow$ f ایک ایک ہے --------(2)

کسی بھی $a \in G$ کے لیے $m\,a \in G'$

اس طرح کہ $f(a) = ma$

$\Rightarrow$ f برنقش ہے۔ --------(3)

(1)،(2) اور (3) کے ذریعہ ثابت ہوا کہ f یک مارفیت ہے۔

مثال3۔ اگر $(R,+)$ اور $(R^+, \bullet)$ دو گروپ ہیں اور $f : R^+ \to R$ اس طرح کہ

$f(x) = log_{10} x,\ \forall x \in R^+$ تب f یک مارفیت ہے۔

فرض کرو کہ $x,y \in R^+ \Rightarrow xy \in R^+$

غور کرو $f(xy) = log_{10} xy$

$= log_{10} x + log_{10} y$

$= f(x) + f(y)$

$\Rightarrow$ f ہم مارفیت ہے۔ ----------(1)

اور اگر $f(x) = f(y)$

$\Rightarrow \log_{10} x = \log_{10} y$

$\Rightarrow x = y$

$\Rightarrow$ f ایک ایک ہے۔ .....(2)

اگر $a \in R$ تب $10^a \in R^+$

اس طرح کہ $f(10^a) = log_{10}^{10^a} = a$

چنانچہ $\Rightarrow$ f برنقش ہے۔ .....(3)

(1)،(2)اور(3)سے معلوم ہوا کہ f ایک ایک برہم مارفیت ہے۔

چنانچہ f یک مارفیت ہوا۔

مثال4۔ کوئی بھی لامتناہی سائکلی گروپ $\mathbb{Z}$ پر یک مارف ہوتا ہے۔

فرض کرو کہ $G = \langle a \rangle = \{a^n / n \in \mathbb{Z}\}$ لامتناہی سائکلی گروپ ہے۔

اور فرض کرو کہ $\varphi: G \to \mathbb{Z}$

معرف بہ $\varphi(a^n) = n \quad n \in \mathbb{Z}$

فرض کرو کہ $a^m, a^n \in G \Rightarrow a^m . a^n \in G$

غور کرو $\varphi(a^m . a^n) = \varphi(a^{m+n})$

$= m + a$

$= \varphi(a^m) + \varphi(a^n)$

یہاں معلوم ہوا کہ ϕ ہم مارفیت ہے ـــــــــــ(1)

اور اگر $\varphi(a^m) = \varphi(a^n)$

$\Rightarrow \quad m = n$

$\Rightarrow \quad a^m = a^n$

یہاں معلوم ہوا کہ φ ایک ایک ہے ـــــــــــ(2)

اور کسی $n \in \mathbb{Z}$ کے لیے $a^n \in G$

اس طرح کہ $\varphi(a^n) = n$

یہاں معلوم ہوا کہ φ برنقش ہے ـــــــــــ(3)

(1)،(2)اور(3)سے معلوم ہوا کہ φ یک مارفیت ہے۔

یعنی کوئی بھی لامتناہی سائکلی گروپ $\mathbb{Z}$ پر یک مارف ہوتا ہے۔

7.3 حل شدہ قضیے اور مشقیں (Solved Theorems and Examples)

قضیہ1۔ اگر $(G, \bullet)$ اور $(G', \bullet)$ دو گروپ ہوں اور $\varphi: G \to G'$ یک مارفیت ہے۔ تب

$\varphi(a^n) = [\varphi(a)]^n, \forall a \in G, \ \forall n \in \mathbb{Z}$

ثبوت۔ دیا گیا ہے کہ $\varphi: G \to G'$ یک مارفیت ہے اور ثابت کرنا ہے کہ $\varphi(a^n) = [\varphi(a)]^n, \forall a \in G,\ \forall n \in \mathbb{Z}$

پہلی صورت: $n \in \mathbb{Z}^+$

اس کو ہم ریاضیاتی استقرا (Mathematical Induction) سے ثابت کریں گے

$n = 1$ کے لیے

$$L.H.S = \varphi(a^1) = \varphi(a)$$
$$= [\varphi(a)]^1 = R.H.S$$

لہٰذا $n = 1$ کے لیے یہ صحیح ہے۔

فرض کرو کہ $n = k$ کے لیے بھی یہ صحیح ہے۔

یعنی $\varphi(a^k) = [\varphi(a)]^k$

اب $n = k+1$ کے لیے

$$\begin{aligned}\varphi(a^{k+1}) &= \varphi(a^k.a)\\ &= [\varphi(a^k).\varphi(a)]\\ &= [\varphi(a)]^k.[\varphi(a)]\\ &= [\varphi(a)]^{k+1}\end{aligned}$$

چنانچہ مساوات $n = k+1$ کے لیے بھی صحیح ہوئی۔

لہٰذا ریاضیاتی استقرا کی رو سے مساوات $\varphi(a^n) = [\varphi(a)]^n, \forall a \in G\ \&\ \forall n \in \mathbb{Z}^+$ صحیح ہے۔

دوسری صورت: اگر $n \in \mathbb{Z}^-$

تب $m = -n$ مثبت جمع عدد ہو گا یعنی $m \in \mathbb{Z}^+$

تب $\varphi(a^m) = [\varphi(a)]^m$

$$\Rightarrow \varphi(a^{-n}) = [\varphi(a)]^{-n}$$

لہٰذا یہاں مساوات $n \in \mathbb{Z}^-$ کے لیے بھی صحیح ہے۔

تیسری صورت: $n = 0 \in \mathbb{Z}$ تب

$$\varphi(a^0) = \varphi(e) = e' = [\varphi(a)]^0$$

مساوات صحیح ہے۔ لہٰذا ہر صورت میں قضیہ ثابت ہوا۔

قضیہ 2۔ اگر $(G,\bullet)$ اور $(G',\bullet)$ دو گروپ ہیں اور $f: G \to G'$ یک مارفیت ہو تب $\forall a, b \in G$ متقلب ہوں گے اگر اور صرف اگر $f(a), f(b)$ متقلب ہوں۔

ثبوت۔ دیا گیا ہے کہ $f: (G,\bullet) \to f: (G',\bullet)$ یک مارفیت ہے

فرض کرو کہ $a, b \in G$

اور $ab = ba$

تب ثابت کرنا ہے کہ $f(a), f(b) = f(b)f(a)$

غور کرو $f(a)f(b) = f(ab)$

$ab = ba \because$ $= f(ba)$

$= f(b)f(a)$

چنانچہ $f(a), f(b)$ متقلب ہوئے۔

اس کے بالعکس فرض کرو کہ $f(a) \cdot f(b) = f(b) \cdot f(a)$

اب ثابت کرنا ہے کہ $ab = ba$

غور کرو کہ $f(a)f(b) = f(b)f(a)$

$f(ab) = f(ba)$

$\Rightarrow ab = ba$ $\because f$ ایک ایک ہے۔

لہٰذا $a, b \in G$ متقلب ہوئے۔ قضیہ ثابت ہوا۔

قضیہ 3۔ اگر $\varphi: G \to \overline{G}$ یک مارفیت ہے تب $G = \langle a \rangle$ اگر اور صرف اگر $\overline{G} = \langle \varphi(a) \rangle$

ثبوت۔ فرض کرو کہ $(G, \bullet)$ اور $(\overline{G}, \bullet)$ دو گروپ ہیں۔

اور $\varphi: G \to \overline{G}$ یک مارفیت ہے

فرض کرو کہ $G = \langle a \rangle = \{a^n / n \in Z\}$ سائکلی گروپ ہے۔

ثابت کرنا ہوگا کہ $\overline{G} = \langle \varphi(a) \rangle$ سائکلی گروپ ہے۔

کسی $a \in G$ کے لیے $\varphi(a) \in \overline{G}$

تب $a^n \in G$ چوں کہ G سائکلی ہے۔

تب $\varphi(a^n) \in \overline{G}$

$\Rightarrow \varphi(a^n) = [\varphi(a)]^n, \forall n \in \mathbb{Z}$

$\Rightarrow \quad \overline{G} = \langle \varphi(a) \rangle$

$\overline{G}$ سائکلی گروپ ہے۔

اس کے بالعکس فرض کرو کہ $\overline{G} = \langle \varphi(a) \rangle$ سائکلی ہے۔

تب ثابت کرنا ہوگا کہ G سائکلی ہے۔

غور کرو $\forall a \in G \Rightarrow \varphi(a) \in \overline{G}$

تب $[\varphi(a)]^n \in \overline{G}$ چوں کہ $\overline{G}$ سائکلی ہے

$\Rightarrow \varphi(a^n) \in \overline{G}$ $\quad \because [\varphi(a)]^n = \varphi(a^n)$

$\Rightarrow a^n \in G$

$\Rightarrow G = \langle a \rangle$

لہٰذا G سائکلی گروپ ہوا۔

قضیہ ثابت ہوا۔

قضیہ 4۔ اگر $\varphi : G \to \overline{G}$ یک مارفیت ہے تب $\forall a \in G, |a| = |\varphi(a)|$ یعنی $a \in G$ کے لیے a' کا رتبہ اور $\varphi(a)$ کا رتبہ مساوی ہوں گے۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(\overline{G},\bullet)$ دو گروپ ہیں۔

اور $\varphi : G \to \overline{G}$ یک مارفیت ہے

فرض کرو کہ $a \in G$ اور $|a| = n, n \in \mathbb{Z}$.....(A)

تب ہمیں ثابت کرنا ہوگا کہ $|\varphi(a)| = n$

چوں کہ a کا رتبہ n ہے اس لیے $a^n = e$ جہاں $e \in G$ اکائی ہے۔

$$\varphi(a)^n = \varphi(e) \because$$
$$\Rightarrow \varphi(a.a.a.....n, times) = e'$$
$$\Rightarrow \varphi(a)\varphi(a)..... ...n\ times = e'$$
$$\Rightarrow [\varphi(a)]^n = e'$$

$\varphi(a)$ کا رتبہ $\Rightarrow |\varphi(a)| \le n$ .....(1)

اگر ممکن ہو کہ $|\varphi(a)| = m$ اور $m < n$.....(B)

تب $[\varphi(a)]^m = e'$

$$\Rightarrow \varphi(a^m) = \varphi(e)$$

$\because \Rightarrow a^m = e$ φ 1-1 ہے یک مارفیت کی بنا۔

$$\Rightarrow |a| = m < n$$

یہ (A) کی تردید کرتا ہے کیونکہ $|a| = n$ ہے۔

لہٰذا (B) ممکن نہیں ہے لہٰذا $|\varphi(a)| = n$ ہوگا۔ چنانچہ $|a| = |\varphi(a)|$ ثابت ہوا۔

قضیہ ثابت ہوا۔

قضیہ 5۔ اگر $\varphi : G \to \overline{G}$ یک مارفیت ہے اور G متناہی ہے تب G اور $\overline{G}$ مساوی رتبہ رکھنے والے عناصر کی تعداد بھی مساوی ہو گی۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(\overline{G},\bullet)$ دو گروپ ہیں۔

اور $\varphi : G \to \overline{G}$ یک مارفیت ہے۔

دیا گیا ہے کہ G متناہی گروپ ہے۔

فرض کرو کہ $|G| = n$

تب فرض کرو کہ $a \in G$

تب $|a| = n$ ہو گا۔

$\Rightarrow a^n = e = 1$ (اکائی)

تب $\varphi : G \to \overline{G}$ چوں کہ 1-1 اور بر ہو گا یک مارفیت کی بنا۔

$$\Rightarrow 1 = \varphi(1)$$
$$= \varphi(a^n)$$
$$= [\varphi(a)]^n$$

چنانچہ G اور $\overline{G}$ میں عناصر کی تعداد مساوی ہو گی جن کے رتبے n ہیں۔

گویا یہ ثابت ہو گیا کہ G اور $\overline{G}$ میں مساوی رتبہ رکھنے والے عناصر کی تعداد بھی مساوی ہو گی۔

قضیہ ثابت ہوا۔

قضیہ 6۔ اگر $\varphi : G \to \overline{G}$ یک مارفیت ہے تب $\varphi^{-1} : \overline{G} \to G$ یک مارفیت ہو گا۔

ثبوت۔ فرض کرو کہ $(G, \bullet)$ اور $(\overline{G}, \bullet)$ دو گروپ ہیں۔

اور $\varphi : G \to \overline{G}$ یک مارفیت ہے۔

تب ثابت کرنا ہے کہ $\varphi^{-1} : \overline{G} \to G$ یک مارفیت ہو گا۔

ہم جانتے ہیں $\varphi(G) = \{\varphi(a) \in \overline{G} / a \in G\}$

مان لیں کہ $a \in G$

تب $b \in \overline{G}$ اس طرح کہ $b = \varphi(a)$

تب $\varphi^{-1}(\overline{G}) = \{\varphi^{-1}(b) / b \in \overline{G}\}$

$$\Rightarrow a = \varphi^{-1}(b) \in \varphi^{-1}(\overline{G}) = G$$

اب چوں کہ ϕ 1-1 ہو گا یک مارفیت کی بنا۔

$\therefore$ غور کرو کہ $\Rightarrow \varphi^{-1}(b_1) = \varphi^{-1}(b_2)$

$$\Rightarrow \varphi(\varphi^{-1}(b_1)) = \varphi(\varphi^{-1}(b_2))$$
$$\Rightarrow b_1 = b_2$$

لہٰذا 1-1 ہوا۔ .....(1)

اور $\forall g \in G \Rightarrow \varphi(g) \in \varphi(G) = \overline{G}$

$$g' \in \overline{G} \Rightarrow \varphi^{-1}(\varphi(g)) = \varphi^{-1}(g')$$
$$\Rightarrow \quad \varphi(g) = g'$$
$$\Rightarrow \quad g = \varphi^{-1}(g')$$

لہٰذا φ^{-1} برنقش ہوا۔ .....(2)

اب فرض کرو کہ $x', y' \in \overline{G} = \varphi(G)$

تب مان لو کہ $x' = \varphi(x)$ اور $y' = \varphi(y)$ جب کہ $x, y \in G$

$\Rightarrow \varphi^{-1}(x') = x \ \& \varphi^{-1}(y') = y$ چوں کہ φ^{-1} 1-1 ہے۔

تب $\Rightarrow \varphi^{-1}(x', y') = \varphi^{-1}[\varphi(x)\varphi(y)]$

$= \varphi^{-1}[\varphi(xy)]$ چوں کہ φ یک مارفیت ہے۔

$= xy$

$= \varphi^{-1}(x')\varphi^{-1}(y')$ .....(3)

φ^{-1} ہم مارفیت ثابت ہوا۔

(1)،(2)اور(3) سے معلوم ہوا کہ φ^{-1} 1-1 برا اور ہم مارفیت ہے۔

اس لیے φ^{-1} یک مارفیت ہے۔

قضیہ ثابت ہوا۔

قضیہ 7۔ اگر $\varphi : G \to \overline{G}$ یک مارفیت ہے تب G ابیلین ہوگا اور صرف اگر G ابیلین ہو۔

ثبوت۔ فرض کرو کہ $(G, \bullet)$ اور $(\overline{G}, \bullet)$ دو گروپ ہیں۔

اور $\varphi : G \to \overline{G}$ یک مارفیت ہے۔

فرض کرو کہ G ابیلین ہے تب ثابت کرنا ہوگا کہ $\overline{G}$ ابیلین ہوگا۔

فرض کرو کہ $a', b' \in \overline{G}$

تب $\exists a, b \in G$ اس طرح سے کہ $a' = f(a), b' = f(b)$

غور کرو $a'b' = \varphi(a)\varphi(b)$

$= \varphi(ab)$ $\because \varphi$ یک مارفیت ہے۔

$= \varphi(ba)$ $\because G$ ابیلین ہے۔

$= \varphi(b)\varphi(a)$

$= b'a'$

یہاں ثابت ہوا کہ $\overline{G}$ ابیلین ہے۔

اس کے بالعکس فرض کرو کہ $\overline{G}$ ابیلین ہے تب ہمیں ثابت کرنا ہوگا کہ G ابیلین ہے۔

فرض کرو کہ $a, b \in G$

تب مان لو کہ $\varphi(a) = a', \varphi(b) = b'$ ، جہاں $a, b \in \overline{G}$ اور $a'b' = b'a'$

تب $a = \varphi^{-1}(a'), \ b = \varphi^{-1}(b')$ چوں کہ φ 1-1 ہے یک مارفیت کی بنا پر

تب غور کرو کہ $ab = \varphi^{-1}(a')\varphi^{-1}(b')$

چوں کہ φ^{-1} بھی یک مارفیت ہوتا ہے۔ $\varphi^{-1} = (a'b')$

$\because \overline{G}$ ابیلین ہے $= \varphi^{-1}(b'a')$

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

$\Rightarrow ab = ba \ \forall \ a,b \in G$

چنانچہ G ابیلین گروپ ہوا۔

قضیہ ثابت ہوا۔

قضیہ 8۔ اگر $\varphi : G \to \overline{G}$ یک مارفیت ہے اور اگر k تحت گروپ ہے G کا تب $\varphi(k)$ تحت گروپ ہوگا $\overline{G}$ کا۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(\overline{G},\bullet)$ دو گروپ ہیں۔

اور $\varphi : G \to \overline{G}$ یک مارفیت ہے۔

اور k تحت گروپ ہے G کا

تب $\varphi(k) = \{\varphi(x)/a \in k\}$

ہمیں ثابت کرنا ہے کہ $\varphi(k)$ تحت گروپ ہوگا $\overline{G}$ کا۔

تب $a \in G \Rightarrow \varphi(e) = e' \in \overline{G}$ چوں کہ $\varphi(k) \neq \varphi$

غور کرو $\varphi(x_1), \varphi(x_2) \in \varphi(k)$

تب $x_1, x_2 \in k$

تب توجہ کرو $\varphi(x_1), \left[\varphi(x_2)\right]^{-1} = \varphi(x_1)\varphi(x_2^{-1})$

$= \varphi(x_1 \cdot x_2^{-1})$

اب چوں کہ $x_1 \cdot x_2^{-1} \in k$ تحت گروپ ہونے کی وجہ سے

اس لیے $\varphi(x_1)[\varphi(x_2)]^{-1} \in \varphi(k)$

اس لیے $\varphi(k)$ تحت گروپ ہوا $\overline{G}$ کا۔

قضیہ ثابت ہوا۔

قضیہ 9۔ اگر $\varphi : G \to \overline{G}$ یک مارفیت ہے تب $\varphi(\mathbb{Z}(G)) = \mathbb{Z}(\bar{G})$ یعنی G کے مرکز کا عکس $\overline{G}$ کے مرکز کے برابر ہوگا۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(\overline{G},\bullet)$ دو گروپ ہیں۔

اور $\varphi : G \to \overline{G}$ یک مارفیت ہے۔

ہم جانتے ہیں گروپ کا مرکز $\mathbb{Z}(G) = \{a \in G/ax = xa \ \ \forall x \in G\}$

اسی طرح $\mathbb{Z}(\bar{G}) = \{a' \in \bar{G}/a'x' = x'a' \ \ \forall x' \in \bar{G}\}$

اب غور کرو $\forall\ \varphi(a) \in \varphi(\mathbb{Z}(G))$

$\Leftrightarrow \quad a \in \mathbb{Z}(G)$

$\Leftrightarrow \quad ax = xa,\ \forall\ x \in G$

$\Leftrightarrow \quad \varphi(ax) = \varphi(xa)$

$\Leftrightarrow \quad \varphi(a)\varphi(x) = \varphi(x)\ \varphi(a)$

$\Leftrightarrow \quad a'x' = x'a'\ , \varphi(a) = a'\ \varphi(x) = x'$

$\Leftrightarrow \quad a' \in\ \mathbb{Z}(\bar{G})$

چنانچہ $\varphi(Z(G)) = Z(\overline{G})$

قضیہ ثابت ہوا۔

قضیہ 10۔ کوئی بھی متناہی سائکلی گروپ جس کا رتبہ 'n' ہے یک مارف ہوتا ہے۔$(\mathbb{Z}_n, +_n)$ یہ یعنی جمع کے تحت بہ مقیاس n صحیح اعداد کے گروپ پر۔

ثبوت۔ فرض کرو کہ $G = \{a, a^2, a^3, \ldots\ldots a^n = e\}$ سائکلی گروپ ہے۔

اور $|G| = n$

اور $\mathbb{Z}_n = \{0,1,2,\ldots\ldots\ldots\ldots (n-1)\}, +_n$ گروپ ہے۔

فرض کرو کہ $\mathbb{Z}_n = \{0,1,2,\ldots\ldots\ldots\ldots (n-1)\}, +_n$

جہاں $f(a^m) = m\ \forall\ a^m \in G$

$a^0 = a^n = e\ \ \because$

$\therefore f(e) = f(a^0) = 0 \in \mathbb{Z}_n$

اگر $a^i, a^j \in G$

تب $f(a^i) = f(a^j)$

$\Rightarrow i = j$

$\Rightarrow a^i = a^j$

لہٰذا f 1- 1 ہے۔.....(1)

اور اگر $k \in \mathbb{Z}_n$ تب $a^k \in G$

اس طرح سے کہ $f(a^k) = k$

لہٰذا f بر نقش ہے۔.....(2)

اب اگر $a^i, a^j \in G$ تب $a^i . a^j = a^{i+j} \in G$

تقسیمی الگورتھم (Division Algorithm) کے مدد سے $q, r \in \mathbb{Z}_n$ جہاں $\exists\ 0 \le r < n$ ، $i + j = nq + r$ ہوگا۔

تب $a^{i+j} = a^{nq+r}$

$$= a^{nq}.a^{r}$$
$$= \left(a^{n}\right)^{q}.a^{r}$$
$$= e^{q}.a^{r}$$
$$= e.a^{r} = a^{r}$$
$$\Rightarrow \quad f\left(a^{i+j}\right) = f\left(a^{r}\right) = r$$
$$i.e. f\left(a^{i}.a^{j}\right) = f\left(a^{r+j}\right) = r$$
$$\Rightarrow \quad \left(a^{i}.a^{j}\right) = i + j = r$$
$$= f\left(a^{i}\right) + f\left(a^{j}\right) = r$$

f ہم مارف ہے۔.....(3)

(1)،(2)اور(3)سے معلوم ہوا کہ f 1-1اور بر مارف ہے۔

اس لیے f یک مارفیت ہے۔ قضیہ ثابت ہوا۔

ہم مارفیت کا اساسی قضیہ(Fundamental Theorem of Homomorphism of Groups)

قضیہ 11۔ اگر $f : G \xrightarrow{\text{on to}} G'$ برہم مارفیت ہے جس کا کرنل K ہے تب $\frac{G}{K} \cong G'$

یا

کسی بھی گروپ G کا ہم مارف عکس کے G کسی خارج قسمت گروپ پر یک مارف ہوتا ہے۔

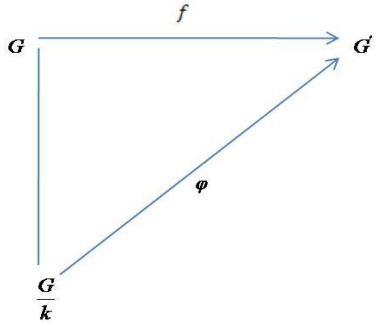
ثبوت۔ فرض کرو کہ $(G,\bullet)$ اور $(G',\bullet)$ دو گروپ ہیں۔

اور $f : G \xrightarrow{\text{on to}} G'$ برہم مارفیت ہے۔

ہمیں ثابت کرنا ہے کہ G' کسی کے G خارج قسمت گروپ سے یک مارف ہوتا ہے۔

فرض کرو کہ $Ker\ f = K$ جہاں $Ker\ f = K = \{r \in G / f(r) = e'\}$

تب G, K کا نارمل تحت گروپ ہوگا۔



شکل 7.1

اور $\frac{G}{K}$ ایک خارج قسمت گروپ ہے جہاں $\frac{G}{K} = \{Ka / a \in G\}$

اب ہم ثابت کریں گے کہ $\frac{G}{K} \cong G'$

اس کے لیے فرض کرو کہ $\varphi: \frac{G}{K} \to G'$ جہاں $\varphi(Ka) = f(a),\ \forall Ka \in \frac{G}{K}$

اب یہ ثابت کرنا ہو گا کہ φ 1-1 اور برہم مارفیت ہے۔

پہلے ہم یہ ثابت کریں گے کہ

(i) φ صحیح معرف ہے۔(well defined)

فرض کرو کہ $\mathrm{K}a, Kb \in \frac{G}{K}$

اور $Ka = Kb$

$$\begin{aligned}
&\Rightarrow && ab^{-1} \in K \\
&\Rightarrow && f(ab^{-1}) = e' \\
&\Rightarrow && f(a)f(b^{-1}) = e' \\
&\Rightarrow && f(a)[f(b)]^{-1} = e' \\
&\Rightarrow && f(a)[f(b)]^{-1}f(b) = e'f(b) \\
&\Rightarrow && f(a)e' = f(b) \\
&\Rightarrow && f(a) = f(b) \\
&\Rightarrow && \varphi(Ka) = \varphi(b)
\end{aligned}$$

لہٰذا φ صحیح معرف ہے۔

(ii) یہ ثابت کرنے کے لیے φ 1-1 ہے۔

فرض کرو کہ $\varphi(Ka) = \varphi(Kb)$

$$\begin{aligned}
&\Rightarrow && f(a) = f(b) \\
&\Rightarrow && f(a)f(b)^{-1} = f(b)[f(b)]^{-1} \\
&\Rightarrow && f(a)f(b^{-1}) = e' \\
&\Rightarrow && f(ab^{-1}) = e' \\
&\Rightarrow && ab^{-1} \in K \\
&\Rightarrow && Ka = Kb
\end{aligned}$$

لہٰذا φ 1-1 ہے۔

(iii) یہ ثابت کرنے کے لیے کہ φ بر نقش ہے۔

اگر $\exists\ x \in G$ تب $y \in G'$

اس طرح کہ $f(x) = y$ ہو گا۔

اور پھر $\varphi(Kx) = f(x) = y$ جہاں $Kx \in \frac{G}{K}$

لہٰذا φ بر نقش ہے۔

(iv) یہ ثابت کرنے کے لیے کہ φ ہم مارفیت ہے۔

فرض کرو کہ $Ka, Kb \in \frac{G}{K}$

غور کرو $\varphi(Ka.Kb) = \varphi(Kab)$ $\because$ K نارمل تحت گروپ ہے۔

$= f(ab)$

$= f(a)f(b)$ $\because$ f ہم مارفیت ہے۔

$= \varphi(Ka)\varphi(Kb)$

چنانچہ φ ہم مارفیت ہے۔

چنانچہ φ 1-1اور برہم مارفیت ہے گویا φ یک مارفیت ہے۔

لہٰذا ثابت ہوا کہ $\frac{G}{K} \cong G'$

قضیہ ثابت ہوا۔

قضیہ 12۔کیلے کا قضیہ(Cayley's Theorem)

ہر متناہی گروپ یک مارف ہوتا ہے ایک مبادلہ گروپ پر

ثبوت۔ فرض کرو کہ $(G,\bullet)$ ایک متناہی گروپ ہے۔

اگر $a \in G$ تب $ax \in G' \ \forall x \in G$ ہوگا۔

اب توجہ کرو۔ $f_a: G \to G$

جہاں کہ $f_a(x) = ax, \forall x \in G$

تب اگر $x,y \in G$ تب $ax,ay \in G$

اور اگر $x = y$

$\Rightarrow \quad f_a(x) = f_a(y)$

لہٰذا fa صحیح معرف ہے(well defined)۔

اور اگر $f_a(x) = f_a(y)$ لیا جائے۔

تب $ax = ay$

$\Rightarrow x = y$

لہٰذا f 1-1 ہوا۔

اور fa بر نقش ہوگا۔اس لیے کہ اگر $x \in G$ تب $a^{-1}x \in G$

اس طرح سے کہ $f_a(xa^{-1}) = a(a^{-1}x)$

$= \left(xa^{-1}\right)x$

$= ex = x$

لہٰذا f_a 1-1 بر نقش ہے۔

چوں کہ fa ایک تا ایک اور بر نقش ہوا 'G' پر لہٰذا f_a ایک مبادلہ ہے۔ G پر اب دوسرے مرحلہ میں ہم $G' = \{f_a / a \in G\}$ تمام مبادلات جو G پر بن سکتے ہیں اُسکا سیٹ بناتے ہیں اور ثابت کریں گے کہ یہ مبادلہ گروپ ہے۔جس کے لیے گروپ کے 4 مطلوبہ شرائط کو جانچا جائے گا۔

(i)بند شی خاصیت: اگر $a,b \in G$ تب $ab \in G$

اور $f_a, f_b \in G'$

غور کرو $x \in G$ کے لیے $(f_a f_b)(x) = f_a(f_b(x))$

$$= f_a(bx)$$
$$= a(bx)$$
$$= (ab)(x)$$
$$= f_{ab}(x)$$

اور چوں کہ $f_a, f_b \in G'$ لہٰذا بند شی خاصیت پوری ہو گی۔

(ii)تلازمی خاصیت: $a,b,c \in G$ کے لیے $f_a, f_b, f_c \in G'$

تب $((f_a, f_b)f_c)(x) = (f_{ab})(f_c(x))$

$$= f_{(ab)c}(x)$$
$$= f_{a(bc)}(x)$$
$$= (f_a(f_{bc}))f(x)$$
$$= (f_a(f_b f_c))(x)$$

لہٰذا تلازمی خاصیت پوری ہوئی۔

(iii)اکائی کا وجود: اگر $e \in G$ اکائی ہو تب $f_e \in G'$

اس طرح کہ $f_a f_e = f_{ae} = f_a$

اور $f_e f_a = f_{ea} = f_a$

لہٰذا $f_e \in G'$ اکائی ہے۔

(iv)معکوس کا وجود ہے: ہم جانتے ہیں اگر $a \in G$ تب $a^{-1} \in G$ چوں کہ G گروپ ہے۔

لہٰذا $f_a, f_{a^{-1}} \in G'$

جو کہ $f_a f_{a^{-1}} = f_{aa^{-1}} = f_e$

چنانچہ معلوم ہوا کہ کسی بھی $f_a \in G'$ کے لیے $(f_a)^{-1} = f_{a^{-1}} \in G'$ لہٰذا گروپ کے سارے یعنی چاروں شرائط پورے ہونے کی بنا G ایک مبادلہ گروپ ہوا۔

اب آخر میں ہمیں ثابت کرنا ہو گا کہ G اور G' کے بیچ یک مارفیت ہے۔

فرض کرو کہ $\varphi : G \to G'$ جہاں $\varphi(a) = fa$ $a \in G$

اب ہمیں ثابت کرنا ہے کہ φ 1-1 اور برہم مارفیت ہے۔

φ 1-1 ہو گا اس لیے کہ

اگر $a,b \in G$ $\varphi(a) = \varphi(b)$

$\Rightarrow$ $f_a = f_b$

$\Rightarrow$ $f_a(x) = f_b(x)$ $\forall\ x \in G$

$$\Rightarrow \quad ax = bx$$
$$\Rightarrow \quad a = b$$

لہٰذا φ 1-1 ہے۔

اور φ برنقش ہوگا اس لیے کہ

اگر $fa \in G'$ تب $a \in G$ اس طرح سے کہ $\varphi(a) = fa$ ہوگا۔

لہٰذا ϕ برنقش ہے۔

اور پھر ϕ ہم مارف دیکھنے کے لیے

غور کرو $a,b \in G \Rightarrow ab \in G$

اور پھر
$$\varphi(ab) = fab$$
$$= fa\ fb$$
$$= \varphi(a)\varphi(b)$$

لہٰذا ϕ ہم مارف ہوا۔

چوں کہ ϕ 1-1 اور برہم مارف ہے لہٰذا ϕ یک مارف ہے یعنی $G \cong G'$

قضیہ ثابت ہوا۔

نوٹ(1):۔ مندرجہ بالا قضیہ کو یوں بھی بیان کیا جاسکتا ہے۔

ہر گروپ ایک مبادلہ گروپ کے تحت کا ہم مارفی ہوتا ہے۔

نوٹ(2):۔ کیلے کا قضیہ لامتناہی گروپ کے لیے بھی صحیح ہوتا ہے۔

نوٹ(3):۔ کیلے کے قضیہ کو یوں بھی بیان کیا جاسکتا ہے۔

کوئی بھی 'n' رتبہ والا گروپ مبادلہ گروپ S_n پر یک مارف ہوتا ہے۔

مثال 1۔ ضربی گروپ $G = \{1, w, w^2\}$ کے لیے باقاعدہ مبادلہ گروپ جس پر یک مارف ہو معلوم کرو۔

حل۔ دیا گیا ہے کہ $G = \{1, w, w^2\}$ ضربی گروپ ہے۔

G ہر یک مارف ہونے والا باقاعدہ مبادلہ گروپ معلوم کرنے کے لیے ہم کیلے کا قضیہ استعمال کریں گے۔

لہٰذا $fa: G \to G'$

$$a \in G, \quad fa(x) = ax \quad \forall x \in G$$

تب باقاعدہ مبادلہ گروپ $G' = \{f_1, f_w, f_{w^2}\}$ ہوگا۔

جہاں

$$f_1=\begin{pmatrix}1 & w & w^2\\ 1.1 & 1.w & 1.w^2\end{pmatrix}=\begin{pmatrix}1 & w & w^2\\ 1 & w & w^2\end{pmatrix}$$

$$f_w=\begin{pmatrix}1 & w & w^2\\ w.1 & w.w & w.w^2\end{pmatrix}=\begin{pmatrix}1 & w & w^2\\ w & w^2 & 1\end{pmatrix}$$

$$f_{w^2}=\begin{pmatrix}1 & w & w^2\\ w^2.1 & w^2.w & w^2.w^2\end{pmatrix}=\begin{pmatrix}1 & w & w^2\\ w^2 & 1 & w\end{pmatrix}$$

مثال2۔ ضربی گروپ $G=\{1,-1,i,-i\}$ کے لیے یک مارف ہونے والا باقاعدہ مبادلہ گروپ معلوم کرو۔

حل۔ دیا گیا ہے کہ $G=\{1,-1,i,-i\}$ ضربی گروپ ہے۔

G سے یک مارف ہونے والا باقاعدہ مبادلہ گروپ معلوم کرنے کے لیے ہم کیلے کے قضیہ سے مدد لیں گے۔

لہٰذا $fa: G\to G$

جہاں $a\in G,\ fa(x)=ax\ \ \forall x\in G$

تب باقاعدہ متبادلہ گروپ $G'=\{f_1, f_{-1}, f_i, f_{-i}\}$ ہو گا۔

جہاں

$$f_1=\begin{pmatrix}1 & -1 & i & -i\\ 1.1 & 1.(-1) & 1.i & 1.(-i)\end{pmatrix}=\begin{pmatrix}1 & -1 & i & -i\\ 1 & -1 & i & -i\end{pmatrix}$$

$$f_{-1}=\begin{pmatrix}1 & -1 & i & -i\\ -1.1 & -1.(-1) & -1.i & -1.(-i)\end{pmatrix}=\begin{pmatrix}1 & -1 & i & -i\\ -1 & 1 & -i & i\end{pmatrix}$$

$$f_i=\begin{pmatrix}1 & -1 & i & -i\\ i.1 & i.(-1) & i.i & i.(-i)\end{pmatrix}=\begin{pmatrix}1 & -1 & i & -i\\ i & -i & -1 & 1\end{pmatrix}$$

$$f_{-i}=\begin{pmatrix}1 & -1 & i & -i\\ -i.1 & -i.(-1) & -i.(i) & -i.(-i)\end{pmatrix}=\begin{pmatrix}1 & -1 & i & -i\\ -i & i & 1 & -1\end{pmatrix}$$

مثال3۔ ضربی گروپ $U(12)$ کے لیے اس سے یک مارف ہونے والا مبادلہ گروپ $\overline{U(12)}$ معلوم کرو۔

حل۔ ہم جانتے ہیں۔ $U(12)=\{1,5,7,11\}$ 12 سے ہم مفرد ہونے والے صحیح اعداد کا سٹ ہے جو ضربی گروپ ہوتا ہے۔

اس سے یک مارف ہونے والا $\overline{U(12)}$ مبادلہ گروپ کیلے (Caylay) کے قضیے کے مطابق

$$fa: U(12)\to U(12)$$
$$a\in U(12),\ fa(x)=ax\ \ \forall x\in U(12)$$

اور مبادلہ گروپ $\overline{U(12)}=\{f_1, f_5, f_7, f_{11}\}$ ہو گا۔

جہاں

$$f_1 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 1.1 & 1.5 & 1.7 & 1.11 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{pmatrix}$$

$$f_5 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5.1 & 5.5 & 5.7 & 5.11 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{pmatrix}$$

$$f_7 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7.1 & 7.5 & 7.7 & 7.11 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{pmatrix}$$

$$f_{11} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11.1 & 11.5 & 11.7 & 11.11 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{pmatrix}$$

مثال4۔ بتلاؤ کہ ایک ہی درجہ (رتبہ) کے دو سائکلی گروپ یک مارفی ہوتے ہیں۔

حل۔ صورت(i): اگر G_1 اور G_2 دو n رتبہ والے سائکلی گروپ ہیں (متناہی گروپ) تب فرض کرو کہ

$$G_1 = \{a, a^2, a^3, \cdots, a^n = e\}$$

اور

$$G_2 = \{b, b^2, b^3, \cdots, b^n = e\}$$

اور اگر $f: G_1 \to G_2$ معرف بہ $f(a^p) = b^p, 1 \le p \le n$ اور $a^p \in G_1, b^p \in G_2$

تب اگر $f(a^p) = f(a^q)$

تب $b^p = b^q$

$\Rightarrow p = q$

$\Rightarrow a^p = a^q$

لہٰذا f 1-1 ہے۔

اور چوں کہ $f: G_1 \to G_2$ جو 1-1 ہے اور دونوں کے درجے برابر ہیں اس لیے f ضرور بر نقش ہوگا۔

اور غور کرو (i) $a^p, a^q \in G_1, 1 < p+q \le n$

تب

$$f\left(a^p \cdot a^q\right) = f\left(a^{p+q}\right)$$
$$= b^{p+q}$$
$$= b^p \cdot b^q$$
$$= f\left(a^p\right) f\left(b^q\right)$$

f ہم مارفیت ہے۔

صورت(ii): $a^p, a^q \in G_1, p+q > n$

تب $p+q = n+v \ \ 1 \le r \le n$ ہوگا۔

پھر $f\left(a^p, a^q\right) = f\left(a^{p+q}\right)$

$$= f\left(a^{n+r}\right)$$
$$= f\left(a^{n}.a^{r}\right)$$
$$= f\left(e.a^{r}\right)$$
$$= f\left(a^{r}\right)$$
$$= b^{r}$$
$$= b^{p+q-n}$$
$$= b^{p+q}.b^{-n}$$
$$= b^{p+q}.\left(b^{n}\right)^{-1}$$
$$= b^{p+q}.e^{-1}$$
$$= b^{p+q}e$$
$$= b^{p+q}$$
$$= b^{p}.b^{q}$$
$$= f\left(a^{p}\right)f\left(a^{q}\right)$$

اس صورت میں بھی f ہم مارف ہے۔

چوں کہ f1-1 برہم مارف ہے اس لیے f یک مارف ہے۔یعنی $G_1 \cong G_2$

صورت(2)اگر G_1 اور G_2 لامتناہی سائکلی گروپ ہیں۔

تب ہم جانتے ہیں کہ کوئی بھی لامتنانی ہی سائکلی گروپ $(\mathbb{Z},+)$ سے یک مارف ہوتا ہے۔لہٰذا قضیہ دونوں صورتوں میں ثابت ہوا۔

مثال5۔ اگر $G=\{0,1,2,3\}$ بہ مقیاس جمع 4 گروپ ہے اور $G'=\{1,2,3,4\}$ بہ مقیاس ضرب 5 گروپ ہے تب ثابت کرو کہ $f:G\to G'$ یک مارفیت ہے۔

حل۔ دونوں گروپ کے کیلے جدول یوں ہوں گے۔

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

اکائی = 0

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
1	4	3	2	1

اکائی = 1

اور

$1^{-1}=1$ $\qquad$ $0^{-1}=0$

$2^{-1}=3$ $\qquad$ $1^{-1}=3$

$3^{-1}=2$ $\qquad$ $2^{-1}=2$

$4^{-1}=4$ $\qquad$ $3^{-1}=1$

ہم جانتے ہیں $f(e)=e^1$ $\qquad$ یعنی $f(0)=1$ ہوگا۔

اور $\qquad f(a^{-1})=[f(a)]^{-1}, \forall a\in G$

اور اگر $\qquad f(1)=2, f(2)=4, f(3)=2$

تب $\qquad \because 3^{-1}=1 \quad f(1)=f(3^{-1})$

$$=[f(3)]^{-1}$$
$$=3^{-1}$$
$$=2$$

اور $\qquad \because 2^{-1}=2 \quad f(2)=f(2^{-1})$

$$=[f(2)]^{-1}$$
$$=4^{-1}$$
$$=4$$

اور $\qquad \because 1^{-1}=3 \quad f(3)=f(1^{-1})=[f(1)]^{-1}=2^{-1}=3$

اب غور کرو $\qquad f(0+_4 2)=f(2)=4=1\times_5 4=f(0)\times_5 f(2)$

یا $\qquad f(2+_4 3)=f(1)=2$

اور $\qquad f(2)\times_5 f(3)=4\times_5 3=2$

لہٰذا $\qquad f(2+_4 3)=f(2)\times_5 f(3)$

اس لیے $\qquad \forall a,b\in G \Rightarrow f(a+_4 b)=f(a)\times_5 f(b)$

f ہم مارف ہوا۔اور چوں کہ f 1-1 ظاہر ہے اور دونوں کے رتبے برابر ہونے کی وجہ بر تفاعل ہے۔لہٰذا f 1-1 اور بر ہم مارف ہونے کی وجہ سے یک مارف ہے۔

مثال6۔ اگر G_1,G_2,G_3 تین گروپ ہیں اور اگر $f:G_1\to G_2$ اور $g:G_2\to G_3$ دو یک مارفیت ہیں تو ثابت کرو کہ $gof:G_1\to G_3$ بھی یک مارفیت ہے۔

حل۔ دیا گیا ہے کہ $f:G_1\to G_2$ یک مارفیت ہے لہذا یہ 1-1 اور بر ہم مارفیت ہیں۔

اور $\qquad g:G_2\to G_3$ یک مارفیت ہے۔لہٰذا یہ 1-1 اور بر ہم مارفیت ہے۔

لہٰذا $\qquad gof:G_1\to G_3$ بھی 1-1 اور بر نقش ضرور ہوگا۔

اب اسے یک مارفیت ثابت کرنے کے لیے ہمیں صرف ہم مارفیت ثابت کرنا ہوگا۔

فرض کرو کہ $a,b \in G$

تب غو کرو $(gof)(ab) = g(f(ab))$

$= g(f(a)f(b))$ $\because$ f ہم مارفیت ہے۔

$= g(f(a))g(f(b))$ $\because$ g ہم مارفیت ہے۔

$= [(gof)(a)][(gof)(b)]$

لہٰذا gof ہم مارفیت ہوا جو 1-1 پر بھی ہے۔

اس لیے gof یک مارفیت ہے۔

7.4 اکتسابی نتائج (Learning Outcomes)

ہم مارفیت جو ایک ایک اور بر ہو یک مارفیت کہلاتی ہے۔ $f: G \to G'$ یک مارفیت ہو تو اگر G ابیلین ہو تو $f(G)$ بھی ابیلین ہوتا ہے۔ اور اگر G سائکلی ہو تو $f(G)$ بھی سائکلی ہوتا ہے۔ یہ بھی قضیہ سامنے آیا کہ $|a| = |f(a)|$ ہوگا کسی بھی $a \in G$ کے لیے $f^{-1}: G' \to G$ بھی یک مارفیت ہوتا ہے۔ اگر k تحت گروپ ہے G کا تب $f(k)$ تحت گروپ ہوگا G' کا کسی بھی گروپ G کا ہم مارف عکس G کے کسی خارج قسمت گروپ سے یک مارف ہوتا ہے۔ یہ بھی مارفیت کا اساسی یا بنیادی قضیہ کہلاتا ہے۔ ہر گروپ یک مارف ہوتا ہے۔ ایک مبادلہ گروپ پر۔ اسکو کیلے کا قضیہ کہا جاتا ہے۔ چند مشقی سوالات کو بھی زیر بحث لایا گیا ہے۔

7.5 کلیدی الفاظ (Keywords)

ہم مارفیت، یک مارفیت، مبادلہ گروپ

7.6 نمونہ امتحانی سوالات (Model Examination Questions)

7.6.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. یک مارفیت کی تعریف کرو۔
2. کیلے کا قضیہ بیان کرو۔

7.6.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. اگر $f: G \to G'$ یک مارفیت ہے تب ثابت کرو کہ $\forall a,b \in G$ متقلب ہوں گے۔ اگر اور صرف اگر $f(a), f(b)$ متقلب ہوں گے۔
2. بتلاؤ کہ ایک ہی درجہ کے دو سائکلی گروپ یک مارفی ہوتے ہیں۔
3. ضربی گروپ $G = \{1,-1,i,-i\}$ کے لیے یک مارف ہونے والا باقاعدہ مبادلہ گروپ معلوم کرو۔

4. اگر $G = \{0,1,2,3\}$ یہ میقاس جمع 4 گروپ ہے اور $G' = \{1,2,3,4\}$ یہ مقیاس ضرب 5 گروپ ہے تب ثابت کرو کہ $f : G \to G'$ یک مارفیت ہے۔

7.6.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. ہم مارفیت کا اساسی (بنیادی) قضیہ بیان اور ثابت کرو۔
2. کیلے کا قضیہ بیان اور ثابت کرو۔
3. اگر $\varphi : G \to \overline{G}$ یک مارفیت ہے تب ثابت کرو کہ $\varphi(\mathbb{Z}(G)) = \mathbb{Z}(\overline{G})$
4. اگر $\varphi : G \to \overline{G}$ یک مارفیت ہے تب ثابت کرو کہ $\forall a \in G \Rightarrow |a| = |\varphi(a)|$

7.7 مزید مطالعے کے لیے تجویز کردہ کتابیں (Suggested Books for Further Reading)

1. Text Book of Differential Equations, Khalil Ahmad, Real World Education Publishers, New Delhi
2. Ordinary and Partial Differential Equations- RaiSinghania, S.Chand& Company, New Delhi
3. A Text Book of B.Sc. (Mathematics), Volume –I , V. VenkateshwaraRao and others, S. Chand & Company New Delhi

اکائی 8۔ گروپس کی خودمارفیت
(Automorphism of Groups)

اکائی کے اجزا

8.0 تمہید(Introduction)

پچھلی دو اکائیوں میں دو گروپوں کے درمیان ایک نقش پر بحث زیر مطالعہ رہا۔ ہم مارفیت میں ایک شرط کے پورا ہونے پر اُسے ہم مارفیت کہا گیا اور یک مارفیت میں اُس شرط پر دو اور شرطیں ایک ایک اور بڑھا کر کے اُسے یک مارفیت کیا گیا۔ اس اکائی میں ان ہی تین شرطوں کو نقش پر پرکھا جائے گا لیکن دو مختلف گروپوں کی بجائے دامنہ اور ہم دامنہ دونوں گروپ ایک ہی گروپ ہوگا۔ اندرونی خودمارفیت اور بیرونی خودمارفیت کا تعارف بھی پیش کیا جائے گا۔ ان کے متعلق قضیے اور چند مشقیں بھی حل کی جائیں گی۔

8.1 مقاصد(Objectives)

اس اکائی کی تکمیل کے بعد آپ کو اس قابل ہونا چاہیے کہ خودمارفیت کیا ہے۔ یک مارفیت سے اس میں کیا مناسبت ہے۔ اندرونی خودمارفیت (Inner Automorphism) کسے کہتے ہیں معلوم ہونا چاہیے۔ بیرونی خود مارفیت (Outer Automorphism) کسے کہتے ہیں معلوم ہونا چاہیے۔ دیے ہوئے نقش کی خودمارفیت کی جانچ کرنے کی صلاحیت پیدا ہونا چاہیے۔

8.2 تعریفات اور مثالیں(Definitions and Examples)

8.2.1 خودمارفیت (Automorphism)

اگر G ایک گروپ ہے اور $f : G \to G$ نقش یک مارفیت ہے تب f کو یک مارفیت کہتے ہیں۔ یا

اگر $(G,\bullet)$ گروپ ہے تب نقش $f : G \to G$ کو خودمارفیت کہتے ہیں اگر تین شرطیں پوری ہوں۔

(1) $f(a,b) = f(a)\,f(b) \forall a,b \in G$ یعنی ہم مارفیت ہو۔

(2) f ایک ایک ہو (1-1)

(3) f بر ہو۔

مثال 1۔(1) نقش: $\phi: \mathbb{C} \to \mathbb{C}$ معرف بہ $\varphi(a+bi) = a-bi$، $\forall a+bi \in \mathbb{C}$، $a, b \in R$ خودمارفیت ہوتا ہے۔ جہاں $(\mathbb{C}, +)$ کا ملتف اعداد (Complex Number) کا گروپ ہے۔

ہم جانتے ہیں کہ $\mathbb{C} = \{a + \text{bi}/a,\text{b} \in \text{R}\}$ ملتف اعداد کا سٹ اور $(\mathbb{C}, +)$ گروپ ہوتا ہے۔

دیا گیا ہے کہ $\varphi(a+bi) = a-bi$

فرض کرو کہ $a_1 + b_1 i, a_2 + b_2 i \in \mathbb{C}$

تب $\varphi(a_1 + b_1 i) = a_1 - b_1 i$

اور $\varphi(a_2 + b_2 i) = a_2 - b_2 i$

غور کرو $\varphi[(a_1 + b_1 i) + (a_2 + b_2 i)] = \varphi[(a_1 + a_2) + (b_1 + b_2) i]$

$$= (a_1 + a_2) - (b_1 + b_2)i$$
$$= (a_1 - b_1 i) + (a_2 - b_2 i)$$
$$= \varphi(a_1 + b_1 i) + \varphi(a_2 + b_2 i) \quad \text{.....(1)}$$

φ ہم مار فیت ہوا۔

اور اگر $\varphi(a_1 + b_1 i) = \varphi(a_2 + b_2 i)$

$$\Rightarrow a_1 + b_1 i = a_2 + b_2 i$$
$$\Rightarrow a_1 = a_2 \ \& \ b_1 = b_2$$
$$\Rightarrow a_1 + b_1 i = a_2 + b_2 i$$

φ 1-1 ہے۔ $\Rightarrow$ .....(2)

اب اگر کسی بھی $a + bi \in C$

کے لیے $a + (-b)i \in C$ ہوتا ہے۔

اس طرح سے کہ $\phi(a + (-b)i) = a - (-b)i$

$$= a + bi$$

لہٰذا φ بر(onto) ہے۔ .....(3)

(1)،(2)اور(3) کی مدد سے معلوم ہوا کہ φ خود مار فیت ہے۔

مثال2۔ اگر $\mathbb{R}^2 = \{(a,b)/a,b \in \mathbb{R}\}$ تب $\phi : R^2 \to R^2$ جب کہ $\phi(a,b) = (b,a)$ اور گروپ $(\mathbb{R}^2, +)$ ہو تب ϕ خود مار فیت ہے۔

حل۔ فرض کرو کہ $(a_1,b_1),(a_2,b_2) \in R^2$

تب $\phi(a_1,b_1) = (b_1,a_1)$

اور $\phi(a_2,b_2) = (b_2,a_2)$

غور کرو $\phi[(a_1,b_1) + (a_2,b_2)] = \phi[(a_1 + a_2, b_1 + b_2)]$
$$= (b_1 + b_2, a_1 + a_2)$$
$$= (b_1,a_1) + (b_2,a_2)$$
$$= \phi(a_1,b_1) + \phi(a_2,b_2)$$

ϕ ہم مار فیت ہے۔ $\Rightarrow$ .....(1)

اور اگر $\phi(a_1,b_1) = \phi(a_2,b_2)$
$$\Rightarrow (b_1,a_1) = (b_2,a_2)$$
$$\Rightarrow b_1 = b_2 \ \& \ a_1 = a_2$$
$$\Rightarrow (a_1,b_1) = (a_2,b_2)$$

ϕ 1-1 ہے۔ $\Rightarrow$ .....(2)

اور کسی بھی $(a,b) \in R^2$ کے لیے $(b,a) \in R^2$

جہاں $\phi(a,b) = (b,a)$

چنانچہ ϕ بر(onto)ہوا۔ .....(3)

(1)،(2)اور(3)کی بنا پر ϕ خودمارفیت ثابت ہوا۔

مثال3۔ نقش $f: \mathbb{Z} \to \mathbb{Z}$ جو کہ $f(x) = -x, \forall x \in \mathbb{Z}$ اور $\mathbb{Z}$ صحیح اعداد کا جمعی گروپ ہے تب f خودمارفیت ہے۔

حل۔ جیسا کہ دیا گیا ہے کہ $(\mathbb{Z}, +)$ گروپ ہے۔

اور $f: \mathbb{Z} \to \mathbb{Z}$

$$f(x) = -x \ , \forall x \in \mathbb{Z}$$

غور کرو اگر $x, y \in \mathbb{Z}$ تو پھر $x + y \in \mathbb{Z}$

تب $f(x) = -x$ اور $f(y) = -y$

اور
$$\begin{aligned} f(x+y) &= -(x+y) \\ &= -x - y \\ &= (-x) + (-y) \\ &= f(x) + f(y) \end{aligned}$$

f ہم مارفیت ہے۔ .....(1) $\Rightarrow$

اور اگر
$$\begin{aligned} f(x) &= f(y) \\ \Rightarrow -x &= -y \\ \Rightarrow x &= y \end{aligned}$$

f ایک ایک(1-1)ہے۔ .....(2) $\Rightarrow$

اور اگر $x \in \mathbb{Z}$ جب کہ $\mathbb{Z}$ ہم دامنہ(Codomain)ہے۔ تب $-x \in \mathbb{Z}$

اس طرح سے کہ $f(-x) = -(-x)$

$$f(-x) = x$$

f بر(onto)ہے۔ .....(3) $\Rightarrow$

(1)،(2)اور(3)کی بنا پر یہ نتیجہ اخذ کرتے ہیں کہ f خودمارفیت ہے۔

8.2.2 اندرون اور بیرون خودمارفیت(Inner Automorphism and Outer Automorphism)

فرض کرو کہ $(G, \bullet)$ ایک گروپ ہے اور اگر $fa: G \to G$ معرف بہ $fa(x) = a^{-1}xa \ \forall x \in C$ اور کسی متعین $a \in G$ کے لیے خودمارفیت ہو تو fa کو اندرون خودمارفیت کہتے ہیں G کا۔

نوٹ۔ $fa(x) = ax\ a^{-1} \ \forall x \in C$ بھی لیا جاسکتا ہے۔

نوٹ۔ جو خودمارفیت اندرون نہیں ہوتا وہ بیرونی خودمارفیت کہلاتا ہے۔

مثال4۔ کسی بھی ابیلین گروپ کا اندرون خودمارفیت اکائی نقش ہی ہوتا ہے۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ ابیلین گروپ ہے۔

اور $a \in G \quad fa: G \to G$ متعین عنصر ہے۔

تب خودمارفیت کی وجہ سے

$$\forall x \in C \Rightarrow fa(x) = a^{-1}xa$$

$$= a^{-1}xa \qquad \because C \text{ ابیلین ہے۔ } ax = xa \text{ ہوگا۔} \therefore$$
$$= ex$$
$$= x$$

fa اکائی نقش ہے۔ $\Rightarrow$

اس سے ثابت ہوا کہ اکائی نقش ہی اندرون خودمارفیت ہوتا ہے۔

8.2.3 خودمارفی گروپ(Group of Automorphism)

اگر $(G,\bullet)$ گروپ ہے تب G ہر ممکن تمام خودمارفتیں ایک گروپ بناتی ہیں۔ یہ عمل ترکیب نقش ہے۔ اُس گروپ کو خودمارفی گروپ Group of Automorphism of G) کا G) کہتے ہیں۔ جیسے Aut(G) سے ظاہر کرتے ہیں۔

یعنی $Aut(G) = A(G)\{\varphi / \phi \text{ is Aut of } G\}$

8.2.4 اندرونی خودمارفیت کا گروپ(Group of Inner Automorhism)

اگر G ایک گروپ ہے تب G پر تمام اندرون خود مارفتیں ایک گروپ بنتے ہیں جسکو اندرونی خود مارفیت گروپ کہتے ہیں۔ جسے Inn(G) سے ظاہر کیا جاتا ہے۔

یعنی $Inn(G) = \{\phi_e, \phi_a, \phi_b \ldots\ldots\ldots\ldots\}$

جہاں ϕ_e اکائی ہوتا ہے اور دوسرے اور خودمارفتیں ہیں۔

8.3 حل شدہ قضیے اور مشقیں(Solved Theorems and Examples)

قضیہ 1۔ کسی گروپ G پر تمام خودمارفیتوں کا سٹ بہ عمل ترکیب نقش گروپ ہوتا ہے جسے خودمارفی گروپ کہتے ہیں اور $Aut(G)$ سے ظاہر کرتے ہیں۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ گروپ سے اور $A(G) = \{\phi: \phi \text{ is an Automorphism of } G\}$

تب $\phi : G \to G$ خودمارفیت یعنی 1-1 اور بر(onto) ہم مارفیت ہے۔

فرض کرو کہ '0' عمل ترکیب نقش ہے کوئی بھی دو نقشوں کے بیچ۔

اب ہم $A(G)$ بر گروپ کی خاصیتیں جانچ کریں گے۔

(1) بندشی خاصیت: فرض کرو کہ $\phi, \Psi \in A(G)$

تب چوں کہ ϕ, Ψ خودمارفیتیں ہیں اس لیے 1-1 اور بر ہیں۔ لہٰذا $\phi o \Psi$ بھی 1-1 اور بر ہوگا۔

فرض کرو کہ $a,b \in G$ تب $a,b \in (G)$

غور کرو $\phi o \Psi(ab) = \Psi(\phi(ab))$

$= \Psi(\phi(a)\phi(b))$ $\because \phi$ خودمارفیت ہے۔

$= \Psi(\phi(a))\Psi(\phi(b))$ $\because \Psi$ خودمارفیت ہے۔

$= (\Psi o \phi)(a)(\Psi o \phi)(b)$

لہٰذا $\Psi o \phi$ بھی ہم مارفیت اور 1-1 اور بر ہے۔ اس لیے $\Psi o \phi$ خودمارفیت ہیں۔

$\Rightarrow \Psi o \phi \in A(G)$

بند شی خاصیت پوری ہوئی۔

(2) چوں کہ عمل ترکیب نقش تلازمی ہوتا ہے۔

لہٰذا $A(G)$ بر تلازمی خاصیت پوری ہوتی ہے۔

(3) اکائی کا وجود۔ چوں کہ $I : G \to G$ اکائی نقش موجود ہوتا ہے۔

جو $\phi e : G \to G$ ہوتا ہے۔

$\phi e(x) = e^{-1}xe \quad \forall x \in G$

$= x$

اور $\phi o I = \phi = I o \phi$ ہوگا۔ لہٰذا $A(G)$ میں اکائی موجود ہے۔

(4) معکوس کا وجود۔ اگر $\phi \in A(G)$ تب ϕ 1-1 اور بر ہونے کی بنا

ϕ^{-1} بھی 1-1 اور بر ہوگا۔ اور ہم مارفیت بھی ہوگا۔ گویا خودمارفیت ہوگا۔

تب $\phi^{-1} \in A(G)$

اور $\phi\ \phi^{-1} = \phi\ \phi^{-1} = I$

لہٰذا معلوم ہوا کہ ہر $\phi \in A(G)$ کے لیے اس کا معکوس $A(G)$ میں موجود ہے۔

چوں کہ گروپ کے چاروں مطلوبہ خاصیتیں پوری ہوئیں۔

اس لیے $(A(G), o)$ گروپ ہو 1-1 سے $Aut(G)$ سے ظاہر کرتے ہیں۔

قضیہ ثابت ہوا۔

قضیہ 2۔ کسی گروپ کے تمام اندرونی خودمارفیتیوں کا سٹ گروپ ہوتا ہے۔ بہ عمل ترکیب نقش ہے۔

ثبوت۔ فرض کرو کہ $(G, \bullet)$ گروپ ہے۔

تب $Inn(G) = \{\phi / \phi(x) = a\,x\,a^{-1} \ \forall\ x \in G\}$

جہاں $\phi a : G \to G$ خود مارفیت

اب ہمیں $Inn(G)$ ہر گروپ کی خاصیتیں جانچنا ہو گا۔

(1) بند شی خاصیت:۔ فرض کرو کہ $\phi_a, \phi_b \in Inn(G)$

تب $\forall x \in G \text{ ، } \phi_a(x) = a\,x\,a^{-1}$ اور $\phi_b(x) = b\,x\,b^{-1}$

غور کرو $(\phi_b o \phi_a)(x) = \phi_b(\phi_a(x))$

$$= \phi_b(a\,x\,a^{-1})$$
$$= b(a\,x\,a^{-1})b^{-1}$$
$$= (ba)\,x\,(a^{-1}b^{-1})$$
$$= (ba)\,x\,(ba)^{-1} \in Inn(G)$$

لہٰذا بند شی خاصیت پوری ہوئی۔

(2) تلازمی خاصیت:۔ اگر $\phi_a, \phi_b, \phi_c \in Inn(G)$

تب غور کرو $[(\phi_a o \phi_b) o \phi_c](x) = (\phi_a o \phi_b)[\phi_c(x)]$

$$= \phi_a[\phi_b(\phi_c(x))]$$
$$= [(ab)c]\,x\,[(ab)c]^{-1}$$
$$= [a(bc)]\,x\,[a(bc)]^{-1} \quad a,b,c \in G \text{ :·} \text{ متلازم ہوتے ہیں۔}$$
$$= [\phi_a o (\phi_b o \phi_c)](x)$$

چنانچہ $Inn(G)$ تلازمی خاصیت پوری کرتا ہے۔

(3) وجود اکائی:۔ $e \in G$:· G کی اکائی ہے۔

تب $\phi_e \in Inn(G)$

$$\Rightarrow \phi_e(x) = e\,x\,e^{-1}$$
$$= x = I(a)$$

اس لیے $(\phi_e o \phi_a)(x) = \phi_e(\phi_a(x))$

$$= \phi_e(a\,x\,a^{-1}) = a\,x\,a^{-1}$$
$$= \phi_a(x)$$

اس لیے $\phi_e o \phi_a = \phi_e = \phi_e o \phi_b$

$\phi_e \in Inn(G)$:· اکائی ہے۔

(4) معکوس کا وجود:۔ جب $a \in G$ تب $a^{-1} \in G$

تو پھر $\phi_a \in Inn(G)$ اور $\phi_{e^{-1}} \in Inn(G)$

تب غور کرو $(\phi_a o \phi_{a^{-1}})(x) = \phi_a(\phi_{a^{-1}}(x))$

$$= \left(aa^{-1}\right) x \left(aa^{-1}\right)^{-1} = e\,x\,e^{-1} = \phi_e(x)$$

اس طرح $\phi_a o \phi_{a^{-1}} = \phi_a(x)$

لہٰذا $(\phi_a)^{-1} = \phi_{a^{-1}} \in Inn(G)$

چنانچہ $(Inn(G), 0)$ ہر گروپ کی تمام خاصیتیں پوری ہوئیں۔

اس لیے $Inn(G)$ گروپ ہوا۔

قضیہ ثابت ہوا۔

قضیہ 3۔ اگر $(G, \bullet)$ یک گروپ ہے اور $a \in G$ ایک متعین عنصر ہے تب نقش $f_a : G \to G$ معرف بہ

$f_a(x) = a^{-1}x\,a \quad \forall\ x \in G$ خودمارفیت ہوتا ہے۔

ثبوت۔ دیا ہوا ہے کہ $(G, \bullet)$ گروپ ہے۔

اور $f_a : G \to G$ $\quad a \in G, a \in G$ $\quad f_a(x) = a^{-1}x\,a \quad \forall\ x \in Ga$ تب ہمیں ثابت کرنا ہے کہ f_a خودمارفیت ہے۔

جس کے لیے ذیل کی 3 شرطیں پوری ہونا گا۔

(1) f_a ہم مارفیت ہونا چاہیے۔

فرض کرو کہ $x, y \in G \Rightarrow xy \in G$

تب غور کرو $f_a(xy) = a^{-1}(xy)a$

$$= a^{-1}x\left(a\,a^{-1}\right)ya$$

$$= \left(a^{-1}xa\right)\left(a^{-1}ya\right)$$

$$= f_a(x)\, f_a(y)$$

لہٰذا f_a ہم مارفیت ہوا۔

(2) f_a 1-1 ہونا چاہیے۔

فرض کرو کہ $x, y \in G$

اور فرض کرو کہ $f_a(x) = f_a(y)$

$\Rightarrow a^{-1}xa = a^{-1}ya$

$\Rightarrow x = y$ تنسیخ کے کلیات کی بنا

$\Rightarrow$ f_a 1-1 ہے۔

(3) f_a بر(onto) ہونا چاہیے۔

فرض کرو کہ (ہم دامنہ میں) $y \in G$

تب $a \in G$ کے لیے $a^{-1} \in G$

اور(دامنہ میں) $a\,y\,a^{-1} \in G$

اس طرح سے کہ $f_a\left(a\,y\,a^{-1}\right) = a^{-1}\left(a\,y\,a^{-1}\right)a$

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

$$= y$$

$\Rightarrow$ f_a بر(onto)ہے۔

چوں کہ f_a 1-1 اور بر(onto)ہم مارفیت ہے۔

اس لیے f_a خودمارفیت ثابت ہوا۔

قضیہ ثابت ہوا۔

قضیہ 4۔ کسی بھی مثبت صحیح عدد $'n'$ کے لیے $Aut\left(\mathbb{Z}_n\right)$ یک مارف ہوتا ہے۔ $U\left(n\right)$ سے۔

ثبوت۔ فرض کرو کہ $n \in \mathbb{Z}^+$

ہم جانتے ہیں کہ $Aut\left(\mathbb{Z}_n\right)$ اور $U\left(n\right)$ ضربی گروپ ہوتے ہیں۔

فرض کرو کہ $T : Aut\left(\mathbb{Z}_n\right) \to U\left(n\right)$

جہاں $T\left(\alpha\right) = \alpha\left(1\right)$

اور $\alpha\left(k\right) = k\alpha\left(1\right)\ \forall\ k \in \mathbb{Z}_n$

اگر $\alpha, \beta \in Aut \in \left(\mathbb{Z}_n\right)$

$$\Rightarrow \alpha\left(1\right) = \beta\left(1\right)$$

$$\Rightarrow \alpha\left(k\right) = k\alpha\left(1\right) = k\beta\left(1\right) = \beta\left(k\right)$$

$$\Rightarrow \alpha\left(k\right) = \beta\left(k\right)\ \forall\ k \in \mathbb{Z}_n$$

$$\therefore T\left(\alpha\right) = T\left(\beta\right)$$

$$\Rightarrow \alpha\left(1\right) = \beta\left(1\right)$$

$$\Rightarrow \alpha = \beta$$

T 1 -1 ہے۔ $\Rightarrow$ .....(1)

اور فرض کرو کہ $r \in U\left(n\right)$

اور $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ اس طرح سے کہ $\alpha\left(s\right) = sr\left(mod\ n\right)\ \forall s \in \mathbb{Z}_n$

تب α خودمارفیت ہے $\mathbb{Z}_n$ پر۔

$$\therefore T\left(\alpha\right) = \alpha\left(1\right) = r$$

لہٰذا T بر(onto)ہوا.....(2)

اور فرض کرو کہ $\alpha, \beta \in Aut\left(\mathbb{Z}_n\right)$

تب غور کرو $T(\alpha\beta)=(\alpha\beta)(1)$

$$\begin{aligned}&=\alpha(\beta(1))\\&=\alpha(1+1+.....+1)(\beta(1)times)\\&=\alpha(1)+\alpha(1)+.....+\alpha(1)(\beta(1)times)\\&=\alpha(1).\beta(1)\\&=T(\alpha).T(\beta)\end{aligned}$$

لہٰذا T ہم ماریفیت ہے۔.....(3)

(1)،(2)اور(3) کی مدد سے معلوم ہوا کہ T یک ماریفیت ہے۔

لہٰذا $Aut(\mathbb{Z}_n)\cong U(n)$

قضیہ ثابت ہوا۔

قضیہ 5۔ اگر G ایک گروپ ہے تب $Inn(G)$ تحت گروپ ہوگا۔ $Aut(G)$ کا اور $\frac{G}{k(G)}\cong Inn(G)$ جہاں $k(G)$ کرنل ہے۔ (یا)

اگر G ایک گروپ ہے تب $Inn(G)$ نارمل تحت گروپ ہوگا۔ $Aut(G)$ کا اور $\frac{G}{k(G)}\cong Inn(G)$ جہاں $k(G)$ کرنل ہے۔

ثبوت۔ فرض کرو کہ $\phi: G\to Inn(G)$

جہاں $\phi(g)=I_g,\ g\in G$

تب اگر $g,h\in G$

تب کسی بھی $x\in G$ کے لیے

$$\begin{aligned}I_{gh}(x)&=gh\ x\ (gh)^{-1}\\&=gh\ xh^{-1}g^{-1}\\&=g(hxh^{-1})g^{-1}\\&=I_gI_h(x)\end{aligned}$$

اس لیے $\phi(gh)=I_{gh}=I_gI_h=\phi(g)\phi(h)$

$\Rightarrow$ ϕ ہم ماریفیت ہے۔

اور چوں کہ $\phi(G)=Inn(G)$

اور $Inn(G)\subseteq Aut(G)$

اس لیے $Inn(G)$ تحت گروپ ہونا ہے $Aut(G)$ کا

اور $ker\,\phi=k(G)=\{g\in G/\ I_g(x)=x,\forall x\in G\}$

$$= \{ g \in G / \; g\, x\, g^{-1} = x \;\; \forall x \in G \}$$

اس لیے ہم مارفت کے اساسی بنیادی قضیہ سے معلوم ہوتا ہے کہ

$$\frac{G}{k(G)} \cong Inn(G)$$

اور اگر $\sigma \in Aut(G)$ اور $g \in G$ تب $\forall\, x \in G, \sigma I_g \;\; \sigma^{-1} = I_{\sigma g}\, x$

اس لیے $Inn(G)$ نارمل تحت گروپ ہوا۔ $Aut(G)$ کا۔

نوٹ:۔ یادرہے کہ $\frac{Aut(G)}{Inn(G)}$ G کا بیرون خود مارفیت گروپ کہلاتا ہے۔

قضیہ 6۔ اگر $(\mathbb{C}, +)$ مختلف اعداد (ComplexNumbers) کا جمعی گروپ ہے اور نقش $\phi: \mathbb{C} \to \mathbb{C}$ اس طرح ہے کہ $\phi(Z) = p(Z) \;\; \forall \;\; Z \in \mathbb{C}$ اور p ایک غیر صفر مختلف عدد ہے۔ تب ثابت کرو کہ ϕ خود مارفیت ہے۔

حل۔ دیا گیا ہے کہ $(\mathbb{C}, +)$ مختلف اعداد کا جمعی گروپ ہے۔

اور $\phi: \mathbb{C} \to \mathbb{C}$

جہاں $\phi(Z) = p(Z) \;\; \forall \;\; Z \in \mathbb{C}$

اور $p(\neq, o) \in \mathbb{C}$

فرض کرو کہ $Z_1, Z_2 \in \mathbb{C}$

تب $Z_1 + Z_2 \in \mathbb{C}$

اور $\phi(Z_1) = pZ_1, \quad \phi(Z_2) = pZ_2$

غور کرو $\phi(Z_1 + Z_2) = p(Z_1 + Z_2)$

$\Rightarrow \quad pZ_1 = pZ_2$

$\Rightarrow \quad \phi(Z_1) = \phi(Z_2)$

ϕ ہم مارفیت ہے۔ $\Rightarrow$ .....(1)

اگر $\phi(\mathbb{Z}_1) = \phi(Z_2)$

$\Rightarrow pZ_1 = pZ_2$

$\Rightarrow \quad Z_1 = Z_2$

ϕ 1-1 ہے۔ $\Rightarrow$ .....(2)

اور اگر $Z' \in \mathbb{C}$ (Codomain) تب $\frac{Z}{P} \in \mathbb{C}$ کیوں کہ $P \neq 0$

اس طرح سے کہ $\phi\left(\frac{Z'}{P}\right) = p\left(\frac{Z'}{P}\right)$

لہٰذا ϕ بر (onto) نقش ہوا۔ $\Rightarrow$ .....(3)

(1)، (2) اور (3) کی مدد سے معوم ہوا کہ ϕ خود مارفیت (Automorphism) ہے۔

قضیہ 7۔ اگر G ایک گروپ ہے تب نقش $\varphi : G \to G$ جو کہ معرف بہ یوں ہے۔ $\forall a \in G \quad \phi(a) = a^{-1}$ تو ثابت کرو کہ ϕ خودمارفیت ہوگا اگر اور صرف اگر G ابیلین ہے۔

ثبوت۔ فرض کرو کہ $(G, \bullet)$ گروپ ہے۔

اور دیا گیا ہے کہ $\varphi : G \to G$

اس طرح سے کہ $\phi(a) = a^{-1} \quad \forall a \in G$

(1) فرض کرو کہ ϕ خودمارفیت ہے۔

تب ہمیں ثابت کرنا ہے کہ G ابیلین ہوگا۔

فرض کرو کہ $x, y \in G$ تب $xy \in G$ ہوگا۔

غور کرو $\phi(xy) = (xy)^{-1}$ جیسا کہ ϕ کی تعریف ہے۔

$= y^{-1}x^{-1}$

$= \phi(y)\phi(x)$

$= \phi(xy)$ چوں کہ ہم مارفیت ہے۔

$\Rightarrow xy = yx$

$\Rightarrow$ G ابیلین ہے۔

(2) اس کے برعکس اگر کو G ابیلین مان لیا جائے۔

تب ہمیں ثابت کرنا ہے کہ ϕ خودمارفیت ہے۔

اب اگر $x, y \in G$ تب $xy = yx$ ہوگا۔

اور اگر $\phi(x) = \phi(y)$

$\Rightarrow x^{-1} = y^{-1}$

$\Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1}$

$\Rightarrow x = y$

چنانچہ ϕ 1-1 ہوا۔.....(1)

اور اگر $x \in G$ (Codomain) تب $x^{-1} \in G$ (Domain)

اس طرح سے کہ $\phi(x^{-1}) = (x^{-1})^{-1}$

$= x$

ϕ بر (onto) ہے۔.....(2)

اور اگر $x, y \in G \Rightarrow xy \in G$

غور کرو کہ $\phi(xy) = (xy)^{-1}$

$$= y^{-1}x^{-1}$$
$$= x^{-1}y^{-1}$$

$\because G$ ایبلین ہے۔

$$= \phi(x)\phi(y)$$

لہٰذا ϕ ہم مارفیت ہے۔ .....(3)

(1)،(2)اور(3) کی بنا پر معلوم ہوا کہ ϕ خود مارفیت ہے۔

قضیہ 8۔ اگر $(R^+, \bullet)$ گروپ ہے اور $f : R^+ \to R^+$ معرف بہ $f(x) = x^2, \forall x \in R^+$ تب ثابت کرو کہ f خود مارفیت ہے۔

حل۔ دیا گیا ہے $(R^+, \bullet)$ کہ گروپ ہے۔

اور $f : R^+ \to R^+$

جہاں $f(x) = x^2, \forall x \in R^+$

ہمیں ثابت کرنا ہے کہ f خود مارفیت ہے۔

یعنی f 1-1 اور برہم مارفیت ہوگا۔

(1) فرض کرو کہ $x_1, x_2 \in R^+$

اور اگر $f(x_1) = f(x_2)$

$$\Rightarrow x_1^2 = x_2^2$$
$$\Rightarrow x_1 = x_2$$

f 1-1 ہے۔ .....(1)

(2) اگر $y \in R^+$ (Codomain)

(3) $\sqrt{y} \in R^+$ (Domain)

اس طرح سے کہ $f(\sqrt{y}) = (\sqrt{y})^2$

چنانچہ f بر(onto) ہوا .....(2)

(3) فرض کرو کہ $x_1, x_2 \in R^+$ تب $x_1x_2 \in R^+$

غور کرو کہ $f(x_1x_2) = (x_1x_2)^2$

$$= x_1^2 x_2^2$$
$$= f(x_1)(x_2)$$

چنانچہ f ہم مارفیت ہے .....(3)

(1)،(2)اور(3) سے ثابت ہوا کہ f خود مارفیت ہے۔

مثال 5۔ اگر H تحت گروپ ہے گروپ G کا، تب اگر $\phi : G \to G$ خود مارفیت ہے اور $\phi(H) = \{\phi(h) / h \in H\}$ تب ثابت کرو کہ $\phi(H)$ ایک تحت گروپ ہوگا G کا۔

حل۔ دیا گیا کہ H تحت گروپ ہے گروپ $(G, \bullet)$ کا

اور $\phi : G \to G$ خود مارفیت ہے۔

اور یہ کہ $\phi(H) = \{\phi(h) / h \in H\}$

ہمیں ثابت کرنا ہے کہ $\phi(H)$ ایک تحت گروپ ہوگا گرو G کا۔

غور کرو اگر $a, b \in H$ تب $ab^{-1} \in H$ چوں کہ H تحت گروپ ہے۔

اور $\phi(a), \phi(b), \phi(ab^{-1}) \in H$ ہوگا۔

تب $\phi(ab^{-1}) = \phi(a)\phi(b^{-1})$ $\because \phi$ خود مارفیت ہے۔

$= \phi(a)[\phi(b)]^{-1} \in \phi(H)$

$\Rightarrow$ تحت $\phi(H)$ گروپ ہوا G کا

لہٰذا ثابت کیا گیا۔

مثال 6۔ ثابت کرو کہ 4 رتبہ والا سائکلی گروپ پر خود مارفی گروپ (Group of Automorphism) کا رتبہ 2 ہوگا۔

یا

ثابت کرو کہ اگر $G = \{a, a^2, a^3, a^4 = e\}$ تب $O(Aut(G)) = 2$

حل۔ فرض کرو کہ $G = \{a, a^2, a^3, a^4 = e\}$ سائکلی گروپ ہے۔

جہاں $O(G) = 4$ ہے۔

یہ ظاہر ہے کہ $O(a) = 4 \because a^4 = e$

$O(a^2) = 2 \because (a^2)^2 = a^4 = e$

$O(a^3) = 4 \because (a^3)^4 = (a^4)^3 = e^3 = e$

$\& O(a^4) = 1 \because (a^4)^1 = e^1 = e$

اور چوں کہ خود مارفیت یک مارفیت ہوتا ہے۔

اور یک مارفیت میں کسی بھی عنصر کا رتبہ اور اس کے عکس کا رتبہ برابر ہوتے ہیں۔ اس لیے خود مارفیت جو G پر بنائے جا سکتے ہیں۔ وہ I اور f ہو سکتے ہیں، جو کہ یوں معرف ہوں گے۔

$I(e) = e \quad I(a) = a \quad I(a^2) = a^2 \quad I(a^3) = a^3$

اور $f(e) = e \quad f(a) = a^3 \quad f(a^2) = a^2 \quad f(a^3) = a^2$

چنانچہ $Aut(G)=\{I,f\}$ گروپ ہوگا بہ عمل ترکیب نقش۔

تب $O(Aut(G))=2$

قضیہ ثابت ہوا۔

مثال 7 ۔ گروپ $(\mathbb{Z}_{10},+_{10})$ کے لیے $Aut(\mathbb{Z}_{10})$ معلوم کرو اور اس کے لیے یک مارف ہونے والا $U(10)$ بھی معلوم کرو۔

حل۔ ہم جانتے ہیں کہ $\mathbb{Z}_{10}=\{0,1,2,3,4,5,6,7,8,9\}$

یہ گروپ ہوگا بہ عمل $+_{10}$

$$|0|=1 \qquad \because 1.0=0$$

یہاں (اکائی) $|1|=10 \qquad \because 10\cdot 1=0$

$$|2|=5 \qquad \because 5\cdot 2=0$$
$$|3|=10 \qquad \because 10\cdot 3=0$$
$$|4|=5 \qquad \because 5\cdot 4=0$$
$$|5|=2 \qquad \because 2\cdot 5=0$$
$$|6|=5 \qquad \because 5\cdot 6=0$$
$$|7|=5 \qquad \because 10\cdot 7=0$$
$$|8|=5 \qquad \because 5\cdot 8=0$$
$$|9|=5 \qquad \because 10\cdot 9=0$$

ہم دیکھتے ہیں کہ رتبہ 10 رکھنے والے عناصر (جو کہ $\mathbb{Z}_{10}$ کا بھی رتبہ ہے) یہ ہیں 1,3,7,9

ہم جانتے ہیں کہ اگر ϕ یک مارفیت ہے تب

$$|a|=|\phi(a)|$$

لہٰذا جو یک مارفتیں ممکن ہوں گی وہ $\alpha_9,\alpha_7,\alpha_3,\alpha_1$ ہوں گی۔

یہ خود مارفتیں ہوں گی دیکھنے کے لیے

ظاہر ہے کہ α_1 اکائی ہے۔

اور $\alpha_3(x)=3x \ \forall x\in\mathbb{Z}_{10}$

اور چوں کہ $x\equiv y\pmod{10}$

$$\Rightarrow 3x=3y\pmod{10}$$

لہٰذا α_3 خوش معرف ہے

مزید یہ کہ $\alpha_3(a^{-1})=(\alpha_3(a))^{-1}, \ \forall a\in\mathbb{Z}_{10}$

اس لیے α_2 1-1 ہے۔

اور چوں کہ $\alpha_3(1)=3$ جہاں $\mathbb{Z}_{10}=\langle 3\rangle$

اس لیے α_3 بر(onto)ہے۔

اب ہم مارفیت کی جانچ کے لیے $\alpha_3(a+b)=3(a+b)$, $\forall a,b\in\mathbb{Z}_{10}$

غور کرو $=3a+3b$

$=\alpha_3(a)+\alpha_3(b)$

لہٰذا α_3 1-1اور برہم مارفیت ہوا۔

گویا α_3 خودمارفیت ہوا $\mathbb{Z}_{10}$ پر۔

اسی طرح ہم دیکھ سکتے ہیں کہ α_7,α_9 بھی خودمارفتیں ہونگے۔

لہٰذا $Aut(\mathbb{Z}_{10})=\{\alpha_1,\alpha_3,\alpha_7,\alpha_9\}$ ہوگا۔

اور ہم جانتے ہیں کہ $U(10)=\{1,3,7,9\}$

10سے کم اور10سے ہم مفرد ہونے والے صحیح اعداد کا سٹ ہے۔

اور یہ گروپ ہوتا ہے بہ مقیاس ضرب10ان کے Caylay گروپ حسب ذیل ہوں گے۔

$U(10)$

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$Aut(\mathbb{Z}_{10})$

0	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

یہاں $\phi: Aut(\mathbb{Z}_{10})\to U(10)$

معرف بہ $\phi(\alpha_a)=a \quad \forall a\in U(10)$

خودمارفیت ہوتا ہے یعنی $Aut(\mathbb{Z}_{10})\cong U(10)$

نوٹ۔ قضیہ4کے مطابق $Aut(\mathbb{Z}_n)\cong U(n)$ ثابت ہوتا ہے۔

مثال8۔ اگر $(R^+,\bullet)$ گروپ ہے تب ثابت کرو کہ نقش ϕ خودمارفیت ہوگا۔جو کہ $\phi: R^+\to R^+$ معرف بہ $\phi(x)=\sqrt{x}\ \forall\ x\in R^+$ ہے۔

حل۔ دیا گیا ہے کہ $(R^+,\bullet)$ مثبت صحیح اعداد کا ضربی گروپ ہے۔

اور نقش $\phi: R^+\to R^+$

$\phi(x) = \sqrt{x} \ \forall \ x \in R^+$ ہے۔

تب ہمیں ثابت کرنا ہے کہ ϕ خود مارفیت ہے۔

جس کے لیے ϕ 1-1 اور برہم مارفیت بتلانا ہو گا۔

غور کرو کہ اگر $x_1, x_2 \in R^+$ (Domain)

اور اگر $\phi(x_1) = \phi(x_2)$ ہو تب

$\sqrt{x_1} = \sqrt{x_2}$ تعریف کے مطابق

$\Rightarrow x_1 = x_2$

ϕ 1-1 ہے۔ $\Rightarrow$ ..... (1)

اور اگر $y \in R^+$ (Codomain) تب $y^2 \in R^+$ (Domain)

اس طرح سے کہ $\phi(y^2) = \sqrt{y^2} = y$

لہٰذا ϕ بر (onto) ہوا .....(2)

اور اگر $x_1, x_2 \in R^+ \Rightarrow x_1 x_2 \in R^+$ بند شی خاصیت کی بنا۔

تب $\phi(x_1 x_2) = \sqrt{x_1 x_2}$ تعریف کے مطابق

$= \sqrt{x_1}\sqrt{x_2}$

$= \phi(x_1)\phi(x_2)$

لہٰذا ϕ ہم مارفیت ہوا ہے۔ .....(3)

نتائج (1)، (2) اور (3) کی بنا پر ہمیں معلوم ہوا کہ ϕ خود مارفیت ہے۔

قضیہ ثابت کیا گیا۔

مثال 9۔ ثابت کرو کہ $\phi : U(16) \to U(16)$ نقش معرف بہ $\phi(x) = x^3 \ \forall \ x \in U(16)$ خود مارفیت ہوتا ہے۔

حل۔ ہم جانتے ہیں کہ ہو $U(16) = \{1,3,5,7,9,11,13,15\}$ گا۔

جو کہ 16 سے کم اور 6 سے ہم مفرد مثبت صحیح اعداد کا سٹ ہے۔

غور کرو $1^3 = 1 \quad 3^3 = 11 \ (mod\ 16)$

$5^3 = 13 \quad 7^3 = 7 \quad 9^3 = 9$

$11^3 = 3 \quad 13^3 = 5 \quad 15^3 = 15$

جیسا کہ تعریف میں دیا گیا کہ $\phi(x) = x^3 \ \forall \ x \in U(16)$

لہٰذا

$$\phi(1) = 1^3 = 1$$
$$\phi(3) = 3^3 = 11$$
$$\phi(5) = 5^3 = 13$$
$$\phi(7) = 7^3 = 7$$
$$\phi(9) = 9^3 = 9$$
$$\phi(11) = 11^3 = 3$$
$$\phi(13) = 13^3 = 5$$
$$\phi(15) = 15^3 = 15$$

عناصر اوران کے معکوس پر غور کرنے سے معلوم ہوتا ہے کہ ϕ 1-1 اور بر ہے۔ پھر بھی نقش کی تعریف کے مطابق 1-1 اور بر ہم مارفیت کی جانچ کریں گے۔

غور کرو اگر (Domain) $x_1, x_2 \in U(10)$

اور اگر $\phi(x_1) = \phi(x_2)$

$$\Rightarrow x_1^3 = x_2^3$$
$$\Rightarrow x_1 = x_2$$

ϕ 1-1 ہے۔ $\Rightarrow$ .....(1)

اور اگر (Codomain) $y \in U(10)$ تب (Domain) $y^{1/3} \in U(10)$

$$\phi\left(y^{1/3}\right) = \left(y^{1/3}\right)^3 = y$$

لہٰذا ϕ بر (onto) ہوا۔ $\Rightarrow$ .....(2)

اور غور کرو کہ اگر $x_1, x_2 \in U(10)$ تب $x_1 x_2 \in U(10)$

اور $\phi(x_1 x_2) = (x_1 x_2)^3$

$$= x_1^3 . x_2^3$$
$$= \phi(x_1)\phi(x_2)$$

لہٰذا ϕ ہم مارفیت ہوا۔ $\Rightarrow$ .....(3)

(1)، (2) اور (3) کی بنیاد پر ϕ 1-1 اور بر ہم مارفیت ہوا۔ گویا ϕ خود مارفیت ہوا۔

ہم کسی دو عناصر پر جانچ بھی کریں گے۔

$$9,13 \in U(16) \Rightarrow \phi(9) = 9, \phi(13) = 5 \pmod{16}$$

اور $\phi(9 \cdot 13) = \phi(9)\phi(13)$

$$\Rightarrow \phi(5) = 9 \cdot 5 \pmod{16}$$
$$\Rightarrow 13 = 13$$

مارفیت ثابت ہوا۔

مثال10۔ اگر $R^n = \{(a_1, a_2 \ldots\ldots\ldots a_n) / a_i's \in R\}$ تب ثابت کرو کہ نقش

$\phi : (a_1, a_2 \ldots\ldots\ldots a_n) \to (-a_{11}, -a_2 \ldots\ldots\ldots -a_n)$ خود مارفیت ہوگا جب کہ $(R^n, +)$ گروپ ہے۔

حل۔ دیا گیا ہے کہ $R^n = \{(a_1, a_2 \ldots\ldots\ldots a_n) / a_i's \in R\}$

اور $(R^n, +)$ گروپ ہے۔ اور پھر $\phi : R^+ \to R^+$

جو کہ یوں معرف ہے۔ $\phi : (a_1, a_2 \ldots\ldots\ldots a_n) = (-a_1, -a_2 \ldots\ldots\ldots -a_n)$

ہمیں ثابت کرنا ہے کہ ϕ خود مارفیت ہے۔

جس کے لیے 1-1 اور برہم مارفیت ثابت کرنا ہوگا۔

غور کرو اگر $(a_1, a_2 \ldots\ldots\ldots a_n), (b_1, b_2 \ldots\ldots\ldots b_n) \in R^n$

اور اگر $\phi(a_1, a_2 \ldots\ldots\ldots a_n) = \phi(b_1, b_2 \ldots\ldots\ldots b_n)$

$\Rightarrow (a_1, a_2 \ldots\ldots\ldots a_n) = (b_1, b_2 \ldots\ldots\ldots b_n)$

$\Rightarrow a_1 = b_1,\ a_2 = b_2, \ldots\ldots\ldots, a_n = b_n$

تب $(a_1, a_2 \ldots\ldots\ldots a_n) = (b_1, b_2 \ldots\ldots\ldots b_n)$

ϕ 1-1 ہے۔ ..... (1)

اور اگر (codomain) $(x_1, x_2 \ldots\ldots\ldots x_n) \in R^n$

تب (Domain) $(-x_1, -x_2 \ldots\ldots\ldots -x_n) \in R^n$

اس طرح سے کہ $\phi(-x_1, -x_2 \ldots\ldots\ldots -x_n) = (-(-x_1), -(-x_2) \ldots\ldots\ldots -(-x_n))$

$= (x_1, x_2 \ldots\ldots\ldots x_n)$

لہٰذا ϕ بر (Onto) ہوا ..... (2)

اور آخر میں اگر $(a_1, a_2 \ldots\ldots\ldots a_n), (b_1, b_2 \ldots\ldots\ldots b_n) \in R^n$

تب غور کرو $\phi[(a_1, a_2 \ldots\ldots\ldots a_n) + (b_1, b_2 \ldots\ldots\ldots b_n)] = [a_1 + b_1, a_2 + b_2 \ldots\ldots\ldots a_n + b_n]$

$= (-(a_1 + b_1), -(a_2 + b_2), \ldots\ldots\ldots -(a_n + b_n))$

$= (-a_1 - b_1, -a_2 - b_2, \ldots\ldots\ldots -a_n - b_n)$

$= (-(a_1 + b_1), -(a_2 + b_2), \ldots\ldots\ldots -(a_n + b_n))$

$= (-a_1, -a_2 \ldots\ldots\ldots -a_n) + (-b_1, -b_2 \ldots\ldots\ldots -b_n)$

$= \phi(a_1, a_2 \ldots\ldots\ldots a_n) + \phi(b_1, b_2 \ldots\ldots\ldots b_n)$

لہٰذا ϕ ہم مارفیت ہوا۔ ..... (3)

(1)، (2) اور (3) کی وجہ سے یہ نتیجہ نکلا کہ ϕ خود مارفیت ہے۔

ثابت کیا گیا۔

مثال 11۔ کسی بھی گروپ G کے لیے $\frac{G}{Z(G)} \cong Inn(G)$ جہاں $Z(G)$، G کا مرکز ہے اور $Inn(G)$ اندرون خودمارفیت ہے G کا۔

ثبوت۔ فرض کرو کہ $(G,\bullet)$ گروپ ہے۔

اور مرکز کے معنی $Z(G) = \{a \in G / ax = xa,\ \forall\ x \in G\}$

اور ہم جانتے ہیں کہ یہ نارمل تحت گروپ ہوتا ہے G گروپ کا

تب خارج قسمت گروپ $\frac{G}{Z(G)} = \{gZ(G)/g \in G\}$

یعنی مرکز کے ہم سٹیں کا گروپ ہے۔

اور $Inn(G) = \{\phi \in G / \phi(x) = g\,x\,g^{-1}, \forall\ x \in G\}$

فرض کرو کہ $T: \frac{G}{Z(G)} \to Inn(G)$

جہاں $T(gZ(G)) = \phi_g,\ \forall\ g \in G$

اب اگر $g \in (G) = hZ(G)\ \forall\ g,h \in G$

$\Leftrightarrow \quad h^{-1}g \in Z(G)$

$\Leftrightarrow \quad (h^{-1}g)x = x(h^{-1}g) \forall\ x \in G$

$\Leftrightarrow \quad h(h^{-1}gx)g^{1} = h(xh^{-1}g)g^{-1}$

$\Leftrightarrow \quad g\,x\,g^{-1} = h\,x\,h^{-1}$

$\Leftrightarrow \quad \phi_g(x) = \phi_h(x)$

$\Leftrightarrow \quad \phi_g = \phi_h$

یہاں معلوم ہوا کہ ϕ خوش معرف بھی ہے اور 1-1 بھی ہے۔(1)

فرض کرو کہ $\exists g \in G$ تب $\phi_g \in Inn(G)$

اس طرح سے کہ $\phi_g(x) = g\,x\,g^{-1}, \forall\ x \in G$

لہٰذا $T(g\ Z(G)) = \phi_g$

اس لیے T بر(onto) ہوا۔ .....(2)

اب غور کرو کہ

$T(g\ Z(G).h\ Z(G)) = T((gh)Z(G))$

$= \phi_{gh} = \phi_g\phi_h$ $\quad \therefore \phi$ خودمارفیت ہے۔

$= T(g\ Z(G)).T(h\ Z(G))$

لہٰذا T ہم مارفیت ہوا۔ .....(3)

(1)،(2) اور (3) کے مطابق T یک مارفیت ہوا۔

یعنی $\frac{G}{Z(G)} \cong Inn(G)$ ثابت ہوا۔

8.4 اکتسابی نتائج(Learning Outcomes)

خود مارفیت دراصل یک مارفیت ہے جو کہ ایک گروپ G سے خود G پر نقش ہوتا ہے۔ کسی گروپ G پر تمام خود مارفتوں کا سٹ بہ عمل ترکیب نقش گروپ ہوتا ہے۔ جسے گروپ خود مارفیت(Group Automorhism) کہتے ہیں اور $Aut(G)$ سے ظاہر کیا جاتا ہے۔ خود مارفیت $\phi_a : G \to G$ جہاں $\phi_a(x) = a\ x\ a^{-1}, \forall\ x \in G, a \in G$ اندرونی خود مارفیت (Inner Automorphism) کہلاتا ہے۔ اور ان تمام کاسٹ بھی گروپ ہوتا ہے۔ بہ عمل ترکیب نقش جسے گروپ اندرون خود مارفیت (Inner Group Automorphism) کہتے ہیں۔ اسے $Inn(G)$ سے ظاہر کیا جاتا ہے۔ $Inn(G)$ نارمل تحت گروپ ہوتا ہے۔ $Aut(G)$ گروپ کا یہ بھی دیکھایا گیا کہ $\frac{G}{Ker(G)} \cong Inn(G)$ اور بھی قضیے اور مشقیں اکائی سے متعلق زیر بحث ہیں۔ جو اندرون خود مارفیت نہیں ہے۔ اُسے بیرون خود مارفیت(Outer Automorphism) کہتے ہیں۔

8.5 کلیدی الفاظ(Keywords)

خود مارفیت، اندرون خود مارفیت، بیرون خود مارفیت

8.6 نمونہ امتحانی سوالات(Model Examination Questions)

8.6.1 معروضی جوابات کے حامل سوالات(Objective Answer Type Questions)

1. خود مارفیت کی تعریف کیجیے۔
2. اندرون خود مارفیت کی تعریف کرو۔
3. بیرون خود مارفیت کی تعریف کرو۔

8.6.2 مختصر جوابات کے حامل سوالات(Short Answer Type Questions)

1. اگر G ایک گروپ ہے تب نقش $\phi : G \to G$ جو کہ معرف بہ یول ہے۔ $\phi(a) = a^{-1}\ \forall\ a \in G$ تو ثابت کرو کہ ϕ خود مارفت ہوگا اور صرف اگر G ابیلین ہو۔
2. اگر $(R^+, \bullet)$ ایک گروپ ہے اور $f : R^+ \to R^+$ معرف بہ $f : R^+ \to R^+$ تب ثابت کرو کہ $f(x) = x^2\ \forall x \in$ f خود مارفیت ہے۔
3. ثابت کرو کہ اگر $G = \{a, a^2, a^3, a^4, = e\}$ ضربی گروپ ہے تب $O(Auto(G)) = 2$
4. گروپ $(\mathbb{Z}_{10}, +_{10})$ کے لیے $Aut(\mathbb{Z}_{10})$ معلوم کرو اور اس کے لیے یک مارف ہونے والا بھی $U(10)$ معلوم کرو۔

8.6.3 طویل جوابات کے حامل سوالات(Long Answer Type Questions)

1. کسی گروپ G پر تمام خود مارفتیوں کا سٹ بہ عمل ترکیب نقش گروپ ہوتا ہے۔ ثابت کیجیے۔

2. اندرون خودمارفیت کی تعریف کرتے ہوئے ثابت کرو کہ $Inn(G)$ بہ عمل ترکیب نقش گروپ ہوتا ہے۔
3. کسی بھی مثبت صحیح عدد n کے لیے ثابت کرو کہ $Aut(\mathbb{Z}_n)$ یک مارف ہوتا ہے۔ $U(n)$ سے
4. اگر G گروپ ہے تب ثابت کرو کہ $Inn(G)$ نارمل تحت گروپ ہوگا $Aut(G)$ کا اور $\frac{G}{K(G)} \cong Inn(G)$ جہاں $K(G)$ کرنل ہے۔

8.7 مزید مطالعے کے لیے تجویز کردہ کتابیں(Suggested Books for Further Readings)

1. Text Book of Differential Equations, Khalil Ahmad, Real World Education Publishers, New Delhi
2. Ordinary and Partial Differential Equations- RaiSinghania, S.Chand& Company, New Delhi
3. A Text Book of B.Sc. (Mathematics), Volume –I , V. VenkateshwaraRao and others, S. Chand & Company New Delhi

اکائی 9۔ رنگ اور تحت رنگ

(Ring and Subring)

اکائی کے اجزا

9.0 تمہید(Introduction)

بلاک 1 اور بلاک 2 میں ہم نے ایک ثنائی عمل رکھنے والے الجبرائی نظام پر بحث کی تھی جو مختلف گروپوں پر مشتمل تھی۔اس بلاک 3 اور بلاک 4 میں ہم دو ثنائی عمل والے الجبرائی نظاموں پر بحث کریں گے۔مثلاً $(\mathbb{Z},+,\bullet)$ یعنی صحیح اعداد کا سٹ اور اس کے ساتھ دو ثنائی عمل جمع اور ضرب ہیں۔اگر $(\mathbb{Z},+)$ تقلیبی گروپ ہو اور $(\mathbb{Z},\bullet)$ نصف گروپ ہو اور عمل ضرب پر جمع تقسیمی (Distributive) خاصیت دائیں اور بائیں رکھتا ہو تو $(\mathbb{Z},+,\bullet)$ کو رنگ کہا جاتا ہے۔ رنگ کے نظریات ریاضیات اور کمپیوٹر گرافکس کے دیگر شعبوں میں مسائل کی تحقیق میں اہم رول ادا کرتے ہیں۔

9.1 مقاصد(Objectives)

اس اکائی کی تکمیل کے بعد آپ اس قابل ہو جائیں گے کہ رنگ کی تعریف کریں مثالیں دیں اور دیئے ہوئے سٹ کو دیئے ہوئے دو مثالی اعمال کے تحت رنگ ہو گا یا نہیں آزما سکیں گے۔اسی طرح دیا ہوا تحت سٹ تحت رنگ کب ہو گا معلوم ہو جائے گا اور دیئے ہوئے تحت سٹ کو تحت رنگ ہونے کے لیے کیا ضروری کافی شرائط ہیں معلوم ہو جائے گا۔

9.2 رنگ(Ring)

تعریف:

ایک سٹ R مع دو ثنائی اعمال '+' اور '•' رنگ کہلاتا ہے اگر مندرجہ ذیل اصول متعارفہ کی تکمیل کرتا ہے۔

$R_1 : (R,+)$ ابیلین گروپ ہے۔

R_{11} : بند شی خاصیت(Closure Axiom):۔ $\forall\ a,b \in R \Rightarrow a+b \in R$

R_{12} : تلازمی خاصیت(Associative Axiom):۔ $\forall\ a,b,c \in R \Rightarrow a+(b+c)=(a+b)+c$

R_{13} : اکائی خاصیت(Identity Axiom):۔ $0 \in R$ اس طرح سے کہ $0+a=a+0=0$

$\forall a \in R$

R_{14} : معکوسی خاصیت(Inverse Axiom):۔

$\forall\ a \in R \exists -a \in R\ s.t. a+(-a)=(-a)+a=0$

R_{15} : تقلیبی خاصیت(Commutative Axiom):۔ $\forall a,b \in R \Rightarrow a+b=b+a$

$R_2 : (R,\bullet)$ نصف گروپ ہے۔

R_{21} : بند شی خاصیت(Closure Axiom):۔ $\forall\ a,b \in R \Rightarrow a.b \in R$

R_{22} : تلازمی خاصیت(Associative Axiom):۔ $\forall\ a,b,c\ R \Rightarrow a.(b.c)=(a.b).c$

R_3 : ضرب کا عمل جمع کے عمل پر تقسیمی ہے (Distributive Law):۔

R_{31} : بائیں تقسیمی خاصیت(Left Distributive Law):۔ $\forall\ a,b,c \in R \Rightarrow a.(b+c) = a.b + a.c$

R_{32} :دائیں تقسیمی خاصیت(Right Distributive Law):۔ $\forall\ a,b,c \in R \Rightarrow (b+c).a = b.a + c.a$

نوٹ(1):۔اگر کوئی رنگ بلحاظ ضرب تقلیبی خاصیت کی تکمیل کرتا ہے تو اسے تقلیبی رنگ کہتے ہیں۔یعنی

$$\forall\ a,b \in R \Rightarrow a.b = b.a$$

نوٹ(2):۔اگر کوئی رنگ بلحاظ اکائی خاصیت کی تکمیل کرتا ہے۔یعنی $1 \in R$ تب اسے رنگ اکائی یا اکائی رکھنے والا رنگ کہتے ہیں۔

نوٹ(3):۔رنگ میں کم از کم ایک عنصر موجود ہوگا جو کہ $\{0\}$ ہوگا۔

نوٹ(4):۔اکائی بلحاظ جمع جو '0' سے تعبیر کیا گیا رنگ کا صفر کہلاتا ہے۔

نوٹ(5):۔ $a.b$ کو ab سے بھی ظاہر کیا جاتا ہے۔

نوٹ(6):رنگ معہ اکائی '1' میں کم از کم دو عناصر $\{0,1\}$ ہوں گے۔

تعریف: بولین رنگ(Boolean Ring) اگر $(R,+,\bullet)$ ایک رنگ ہے جس میں $\forall a \in R \Rightarrow a^2 = a$ تب اسے بولین رنگ(Boolean Ring) کہا جاتا ہے۔

مثال: بولین رنگ ہے جہاں شائی معہ عمال $\oplus_2$ اور $\oplus_2$ ہیں۔کیونکہ $0^2 = 0$ اور $1^2 = 1$

نوٹ(7) $R = \{0\}$ رنگ ہوتا ہے اور اسے صفر رنگ(Zero ring) یا Null Ring کہتے ہیں۔

یونٹ (unit)

اگر $(R,+,\bullet)$ ایک رنگ ہے اور $a \in R$ کے لیے 'a' کا ضربی معکوس R میں موجود ہو تو 'a' R میں واحد کہلاتا ہے۔

مثال۔ $R = \{0,1,2,3,4\}$ تب $(R,\oplus_5,\otimes_5)$ رنگ ہوتا ہے اور اس میں '0' کے علاوہ باقی تمام عناصر کے ضربی معکوس موجود ہیں لہٰذا $1,2,3,4$ رنگ R کے واحد ہیں۔

وضاحت:۔ضربی معکوس

$$1^{-1} = 1$$
$$2^{-1} = 3$$
$$3^{-1} = 2$$
$$4^{-1} = 4 \in R$$

حل شدہ مشقیں:۔

مثال 1۔ثابت کرو کہ تمام جفت صحیح اعداد کا سٹ معہ صفر ایک تقلیبی رنگ ہوگا بغیر اکائی کے اور جب کہ ثنائی اعمال '+' اور '.' ہیں۔

حل۔فرض کرو کہ $R = \{2x / x \in \mathbb{Z}\}$

تب $R = \{.....-4,-2,0,2,4,6.....\}$

تب ہمیں $(R,+,\bullet)$ ہر رنگ کی تمام اصول معارضہ کی آزمائش کرتا ہوگا۔

$R_1 : (R,+)$ تقلیبی گروپ ہونا چاہیے۔

R_{11} : بند شی خاصیت(Closure Axiom):اگر $2m, 2n \in R$ جہاں $m, n \in \mathbb{Z}$

تب $2m+2n = 2(m+n)$

$\in R \quad m+n \in \mathbb{Z}$

لہٰذا بند شی خاصیت کی تکمیل ہوئی۔

R_{12} : تلازمی خاصیت(Associative Axiom):۔اگر $2m, 2n, 2p \in R$ تب

$(2m+2n)+2p = 2m+(2n+2p)$ ہوگا اس لیے کہ

صحیح اعداد تلازمی خاصیت پوری کرتے ہیں۔

R_{13} :اکائی خاصیت(Identity Axiom):۔چوں کہ $0 \in R$ اکائی ہے بہ عمل جمع اس لیے اکائی خاصیت کی تکمیل پوری ہوئی۔

R_{14} : معکوسی خاصیت(Inverse Axiom):۔چوں کہ $\forall\ 2x \in R \Rightarrow -2x \in R$

اس طرح سے کہ $2x+(-2x) = 0$ اس لیے معکوسی خاصیت پوری ہوئی۔

R_{15} : تقلیبی خاصیت(Commutative Axiom):۔

اگر $2m, 2n \in R$

تب $2m+2n = 2(m+n)$

$= 2(m+n)$

$= 2m+2n$

لہٰذا تقلیبی خاصیت کی تکمیل ہوئی۔

یہاں تک یہ ثابت ہوا کہ $(R,+)$ ایک تقلیبی گروپ ہے۔

$R_2 : (R,\bullet)$ ایک نصف گروپ ہونا چاہیے۔

R_{21} : بند شی خاصیت(Closure Axiom) :

اگر $2m, 2n \in R$ تب $2m.2n = 2(2mn) \in R$

لہٰذا کسی دو جفت اعداد کا حاصل ضرب پھر جفت ہی ہوتا ہے۔اس لیے بند شی خاصیت پوری ہوئی ہے۔

R_{22} : تلازمی خاصیت(Associative Axiom):۔اگر $2m, 2n, 2p \in R$

تب $(2m.2n).2p = 8mnp$

$= 2m.(2n.2p)$

لہٰذا تلازمی خاصیت پوری ہوئی۔ یہاں یہ ثابت ہوا کہ $(R,\bullet)$ ایک نصف گروپ ہے۔

R_3 : تقسیمی خاصیتیں پوری ہونا چاہیے(Distributive Law must be prove)

R_{31} : بائیں تقسیمی خاصیت(Left Distributive Law)اگر $2m, 2n, 2p \in R$

تب $2m.(2n+2p)=2m.2n+2m.2p$ اور

R_{32} : دائیں تقسیمی خاصیت(Right Distributive Law):۔اگر $2m,2n\in R$

تب $(2n+2p).2m=2m.2n+2p.2m$

ظاہر ہے کہ پورے ہوں گے۔

چوں کہ رنگ کے سارے اصول معارضہ کی تکمیل $(R,+,\bullet)$ پر ہو گی۔اس لیے تمام جفت صحیح اعداد کا سٹ صفر رنگ ہوتا ہے۔اب چوں کہ R & 1 چوں کہ '1' طاق عدد ہے۔

اور $\forall\ 2m,2n\in R$

بر $2m.2n=4mn$

$=4mn$

$=2m.2n$

لہٰذا عمل ضرب پر تقلیبی خاصیت پوری ہوتی ہے۔

لہٰذا معلوم ہوا کہ تمام جفت اعداد صحیح کا سٹ معہ صفر ایک تقلیبی رنگ ہوتا ہے۔بغیر اکائی کے۔ثابت ہوا۔

مثال2۔ ثابت کرو کہ صحیح عدد یہ مقیاس کا سٹ یہ مقیاس جمع اور یہ مقیاس ضرب کے تحت اکائی کے ساتھ تقلیبی رنگ ہوتا ہے۔

حل۔ دیا گیا سٹ فرض کرو کہ $R=\{0,1,2,3,4,5\}=6$ ہے۔

ہمیں ثابت کرنا ہے کہ $(R,\oplus_6,\otimes_6)$ تقلیبی رنگ معہ اکائی ہو گا۔

کیلے کے جدول حسب ذیل ہوں گے۔

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\otimes_6$	0	1	2	3	4	3
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

R_3 : $(R,\otimes_6)$ تقلیبی گروپ ہونا چاہیے۔

R_{11} : بند شی خاصیت(Closure Axiom):کیلے کے جدول سے ظاہر ہے کہ کسی بھی دو عناصر کا جمع بہ مقیاس کا سٹ R کا ہی عنصر ہو گا لہٰذا بند شی خاصیت پوری ہوئی۔

R_{12} : تلازمی خاصیت(Associative Axiom):۔ $\forall\ a,b,c\in R\Rightarrow(a\oplus b)\in c=a\oplus(b\oplus c)$

مثلاً $(2\oplus_6 3)\oplus_6 5=2\oplus_6(3\oplus_6 5)$

$\Rightarrow 5\oplus_6 5=2\oplus_6 2$

$\Rightarrow 4=4$

لہٰذا تلازمی خاصیت R پر صادق ہے۔

R_{13} :اکائی خاصیت(Identity Axiom):۔ کیلے جدول سے ظاہر ہے کہ $0 \in R$ اکائی بہ عمل $\oplus_6$ ہے۔

R_{14} : معکوسی خاصیت(Inverse Axiom):۔ $\forall\ a \in R \exists b \in R\ s.t. a \oplus_6 b$

کیلے جدول سے ظاہر ہے کہ

$$0^{-1} = 0, 1^{-1} = 5, 2^{-1} = 4, 3^{-1} = 3, 4^{-1} = 2, 5^{-1} = 1 \in R$$

لہٰذا ہر عنصر کا معکوس R میں موجود ہے۔

R_{15} : تقلیبی خاصیت(Commutative Axiom): $\forall a, b \in R \Rightarrow a \oplus b = b \oplus a$

ہم دیکھتے ہیں کہ مثال کے طور پر

$$2 \oplus_6 5 = 5 \oplus_6 2$$
$$1 = 1$$

اس طرح سارے عناصر پر یہ خاصیت پوری ہوتی ہے۔

یہاں معلوم ہوا کہ $(R, \oplus_6)$ ایک تقلیبی گروپ ہے۔

R_2 : $(R, \otimes_6)$ نصف گروپ ہونا چاہیے معہ اکائی اور تقلیبی خاصیت۔

R_{21} :بند شی خاصیت(Closure Axiom) :

کیلے کے جدول بہ مقیاس ضرب 6 سے ظاہر ہے کہ R پر یہ خاصیت مادق ہے۔

R_{22} : تلازمی خاصیت(Associative Axiom):۔

$\forall a, b, c \in R \Rightarrow a \otimes_6 (b \otimes_6 c) = (a \otimes_6 b) \otimes_6 c$ اگر

مثال دیکھیں: $2 \otimes_6 (3 \otimes_6 4) = (2 \otimes_6 3) \otimes_6 4$

$$\Rightarrow 2 \otimes_6 0 = 0 \otimes_6 4$$
$$0 = 0$$

R_{23} :اکائی خاصیت(Identity Axiom):۔ کیلے جدول سے ظاہر ہے کہ $1 \in R$ اکائی ہے۔

چوں کہ $\forall a \in R \Rightarrow 1 \otimes_6 a = a \otimes_6 1 = a$

R_{25} :اکائی خاصیت(Identity Axiom):۔ کیلے جدول سے ظاہر ہے کہ $1 \in R$ اکائی ہے۔

چوں کہ $\forall a \in R \Rightarrow 1 \otimes_6 a = a \otimes_6 1 = a$

R_{15} : تقلیبی خاصیت(Commutative Axiom):۔

$$\forall a, b \in R \Rightarrow a \otimes_6 b = b \otimes_6 a$$

مثال دیکھیں $2 \otimes_6 5 = 5 \otimes_6 2$

$$4 = 4$$

لہٰذا تقلیبی خاصیت پوری ہوتی ہے۔

R_3 : تقسیمی خاصیتیں پور ہونی چاہیے۔

R_{31} : بائیں تقسیمی خاصیت:۔ $\forall a,b,c \in R$

$$\Rightarrow a \otimes_6 (b \oplus_6 c) = (a \otimes_6 b) \oplus_6 (a \otimes_6 c)$$

مثال:۔ $$\Rightarrow 2 \otimes_6 (3 \oplus_6 4) = (2 \otimes_6 3) \oplus_6 (2 \otimes_6 4)$$

$$\Rightarrow 2 \otimes_6 1 = 0 \oplus_6 2$$

$$2 = 2$$

خاصیت پوری ہوئی۔

R_{32} :دائیں تقسیمی خاصیت:۔ $\forall a,b,c \in R$

$$\Rightarrow (b \oplus_6 c) \otimes_6 a = (b \otimes_6 a) \oplus_6 (c \otimes_6 a)$$

مثال $$\Rightarrow (3 \oplus_6 4) \otimes_6 5 = 3 \otimes_6 5 \oplus_6 4 \otimes_6 5$$

$$\Rightarrow 1 \otimes_6 5 = 3 \oplus_6 2$$

$$5 = 5$$

خاصیت پوری ہوئی۔

اس کے ساتھ ہی یہ ثابت ہوتا ہے کہ $(R, \oplus_6, \otimes_6)$ ایک تقلیبی رنگ معہ اکائی ہوتا ہے۔

مثال 3۔ ثابت کرو کہ $R = \{0,2,4,6,8\} \bmod 10$ تب $(R, \oplus_{10}, \otimes_{10})$ رنگ ہوگا اور اسکا اکائی بہ عمل ضرب بہ مقیاس 10 بھی معلوم کرو۔

حل۔ دیا گیا ہے کہ $R = \{0,2,4,6,8\} \bmod 10$

کیلے کے جدول حسب ذیل ہوں گے۔

$\oplus_{10}$	0	2	4	0	8
0	0	2	4	6	8
2	0	4	6	8	0
6	4	6	8	0	2
7	6	8	0	2	4
8	8	0	2	4	6

$\otimes_{10}$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

اب ہم رنگ ہونے کی شرائط کی آزمائش کریں گے۔

R_1 : $(R_1, \oplus_{10})$ ایک تقلیبی گروپ ہونا چاہیے۔

R_{11} :بندشی خاصیت(Closure Axiom) :

$$\forall a,b \in R \Rightarrow a \oplus_{10} b \in R$$

ہم دیکھتے ہیں کہ جدول سے ظاہر ہے کہ $(R_1, \oplus_{10})$ بند ہے۔

R_{22} : تلازمی خاصیت(Associative Axiom):۔

$$\forall a,b,c \in R \Rightarrow a \oplus_{10} (b \oplus_{10} c) = (a \oplus_{10} b) \oplus_{10} c$$

مثال:۔ $$2 \oplus_{10} (6 \oplus_{10} 8) = (2 \oplus_{10} 6) \oplus_{10} 8$$
$$2 \oplus_{10} 4 = 8 \oplus_{10} 8$$
$$6 = 6$$

لہٰذا خاصیت پوری ہوئی۔

R_{13} :اکائی خاصیت(Identity Axiom):۔ جدول بہ مقیاس جمع 10 سے ظاہر ہے کہ $0 \in R$ اکائی ہے۔

چوں کہ $\forall a \in R \Rightarrow a \oplus_{10} 0 = 0 \oplus_{10} a = a$

R_{14} : معکوسی خاصیت(Inverse Axiom):۔

$$\forall\ a \in R \exists b \in R\ s.t. a \oplus_{10} b = 0$$

ہم دیکھتے ہیں کہ

$$0^1 = 0, 2^1 = 8, 4^1 = 6, 6^1 = 4, 8^1 = 2 \in R$$

R_{15} : تقلیبی خاصیت(Commutative Axiom):۔

$$\forall a,b \in R \Rightarrow a \oplus_{10} b = b \oplus_{10} a$$

مثال:۔

$$6 \oplus_{10} 2 = 2 \oplus_{10} 6$$
$$8 = 8$$

سارے ہی عناصر پر یہ خاصیت پوری اترتی ہے۔ یہاں معلوم ہوا کہ $(R, \oplus_{10})$ ایک تقلیبی گروپ ہے۔

R_1 : $(R, \oplus_{10})$ نصف گروپ ہونا چاہیے۔

R_{21} : بند شی خاصیت(Closure Axiom) :

$$\forall a,b \in R \Rightarrow a \otimes_{10} b \in R$$

جدول سے ظاہر ہے کہ $(R, \otimes_{10})$ بند ہے۔

R_{22} : تلازمی خاصیت(Associative Axiom):۔

$$\forall a,b,c \in R \Rightarrow a \otimes_{10} (b \otimes_{10} c) = (a \otimes_{10} b) \otimes_{10} c$$

مثال:۔ $$4 \otimes_{10} (6 \otimes_{10} 8) = (4 \otimes_{10} 6) \otimes_{10} 8$$
$$4 \otimes_{10} 6 = 4 \otimes_{10} 8$$
$$2 = 2$$

سارے ہی عناصر پر یہ خاصیت پوری ہو گی۔

لہٰذا $(R,\otimes_{10})$ نصف گروپ ہوا۔

R_3 : تقسیمی خاصیتیں:۔

R_{31} : بائیں تقسیمی خاصیت(Left Distributive Law)

$$\forall\ a,b,c\in R\Rightarrow a\otimes_{10}(b\oplus_{10}c)=(a\otimes_{10}b)\oplus_{10}(a\otimes_{10}c)$$

مثال:۔
$$4\otimes_{10}(2\oplus_{10}6)=(4\otimes_{10}2)\oplus_{10}(4\otimes_{10}6)$$
$$4\otimes_{10}8=8\oplus_{10}4$$
$$2=2$$

R_{32} :دائیں تقسیمی خاصیت(Right Distributive Law):۔

$$\forall\ a,b,c\in R\Rightarrow(b\oplus_{10}c)\otimes_{10}a=(b\otimes_{10}a)\oplus_{10}(c\otimes_{10}a)$$
$$e.g.(4\oplus_{10}6)\otimes_{10}2=(4\otimes_{10}2)\oplus_{10}(6\otimes_{10}2)$$
$$0\otimes_{10}2=8\oplus_{10}2$$
$$0=0$$

لہٰذا تقسیمی خاصیتیں پوری ہوئیں۔

یہاں یہ نتیجہ نکلا کہ $(R,\oplus_{10},\otimes_{10})$ ایک رنگ ہے۔

ہم دیکھتے ہیں کہ یہ مقیاس ضرب ہے۔

$$\forall a\in R\Rightarrow a\otimes_{10}6=a=6\otimes_{10}a$$

لہٰذا $6\in R$ اس رنگ کی اکائی ہے۔

مثال4۔ جانچ کرو کہ آیا سٹ $R=\{a\sqrt{2}\ /\ a\in Q\}$ ہو تب بہ عمل جمع وضرب رنگ ہو گا یا نہیں۔

حل۔ دیا گیا ہے کہ $R=\{a\sqrt{2}\ /\ a\in Q\}$

ہم پہلے بند شی خاصیتیں بہ عمل جمع اور ضرب دیکھیں گے۔

بہ عمل جمع $\forall\ a\sqrt{2},b\sqrt{2}\in R\Rightarrow a\sqrt{2}+b\sqrt{2}=(a+b)\sqrt{2},a+b\in Q$

لہٰذا بند شی خاصیت صحیح ہوتی ہے۔

جب کہ بہ عمل ضرب $\forall\ a\sqrt{2},b\sqrt{2}\in R$

$$a\sqrt{2}.b\sqrt{2}=ab.2$$
$$=ab\sqrt{2}.\sqrt{2}=\left(a(b)\sqrt{2}\right)\sqrt{2}$$

یا
$$=\left(a\sqrt{2}(b)\right)\sqrt{2}$$

ہر دو صورتوں میں یا تو $b\sqrt{2}\notin Q$

یا پھر $a\sqrt{2}\notin Q$

اس لیے بند شی خاصیت پوری نہیں ہوتی۔

جو کہ R بہ عمل ضرب نصف رنگ ہونا ہوتا ہے، رنگ ہونے کے لیے۔

لہٰذا $R = \{a\sqrt{2} / a \in Q\}$ رنگ نہیں ہوگا۔

مثال 5۔ ثابت کرو کہ ملتف اعداد کا سٹ (Complex Number set) بہ عمل جمع و ضرب ایک تقلیبی رنگ معہ اکائی ہوتا ہے۔

حل۔ فرض کرو کہ $\mathbb{C} = \{a+bi / a,b \in R\}$

تب مطلوبہ خاصیتیں بہ عمل جمع اور ضرب آزمائیں گے۔

$R_1 : (\mathbb{C},+)$ تقلیبی گروپ ہونا چاہیے۔

R_{11} : بند شی خاصیت:۔ غور کرو اگر $a_1+b_1i, a_2+b_2i \in \mathbb{C}$

تب $(a_1+b_1i)+(a_2+b_2i) = (a_1+a_2)+(b_1+b_2)i \in \mathbb{C} \because a_1+a_2, b_1+b_2 \in R$

لہٰذا $\mathbb{C}$ بہ عمل جمع بند ہے۔

R_{12} تلازمی خاصیت:۔ توجہ کرو

$$\begin{aligned}(a_1+b_1i)+\{(a_2+b_2i)+(a_3+b_3i)\} &= (a_1+b_1i)\{(a_2+a_3)+(b_2+b_3)i\}\\ &= \{a_1(a_2+a_3)\}+\{b_1+(b_2+b_3)\}i\\ &= \{(a_1+a_2)+a_3\}+\{(b_1+b_2)+b_3\}i\\ &= \{(a_1+a_2)+(b_1+b_2)i\}+(a_3+b_3)i\\ &= \{(a_1+b_1i)+((a_2+b_2i))\}+(a_3+b_3i)\end{aligned}$$

معلوم ہوا تلازمی خاصیت پوری ہوتی ہے۔

R_{13} : اکائی خاصیت: چوں کہ $a=b=0 \in R$

اس لیے $0+0i=0 \in \mathbb{C}$

اس طرح سے کہ $\forall a+bi \in \mathbb{C} \Rightarrow (a+bi)+0 = a+bi$

اس لیے اکائی بہ عمل جمع موجود ہے۔

R_{14} : معکوسی خاصیت: غور کرو کہ $\forall a+bi \in \mathbb{C} \Rightarrow -a(-b)i+ \in \mathbb{C}$

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

لہٰذا ہر ملتف عدد کا جمعی معکوس $\mathbb{C}$ میں موجود ہے۔

R_{15} : تقلیبی خاصیت: غور کرو کہ $(a_1+b_1i)+(a_2+b_2i) = (a_1+a_2)+(b_1+b_2)i$

$= (a_2+a_1)+(b_2+b_1)i$ $\because$ حقیقی اعداد تقلیبی ہوتے ہیں۔

$$= (a_2 + b_2 i) + (a_1 + b_1 i)$$

لہٰذا $(\mathbb{C}, +)$ تقلیبی گروپ ہوا۔

$R_2 : (\mathbb{C}, \bullet)$ نصف گروپ معہ اکائی و تقلیبی صفت ہونا چاہیے۔

R_{21} : بند شی خاصیت :۔ اگر $(a_1 + b_1 i) + (a_2 + b_2 i) \in \mathbb{C}$

تب $(a_1 + b_1 i).(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i \in \mathbb{C} \quad \because (a_1 a_2 - b_1 b_2), (a_1 b_2 + b_1 a_2) \in R$

لہٰذا بند شی خاصیت پوری ہوئی۔

R_{22} تلازمی خاصیت :۔ ہم جانتے ہیں کہ ملتف اعداد تلازمی خاصیت پوری کرتے ہیں۔

یعنی $(a_1 + b_1 i).\{(a_2 + b_2 i).(a_3 + b_3 i)\} = \{(a_1 + b_1 i).(a_2 + b_2 i)\}.(a_3 + b_3 i)$

R_{23} : اکائی خاصیت :۔ توجہ کرو۔ $a = 1, b = 0 \in R$

تو پھر $a + bi = 1 + 0i = 1 \in \mathbb{C}$

اس طرح سے کہ $\forall (a + bi) \in \mathbb{C}$

$(a + bi).1 = a + bi = 1.(a + bi)$

لہٰذا $1 \in \mathbb{C}$ ضربی اکائی ہے۔

R_{25} : تقلیبی خاصیت :۔ غور کرو اگر $(a_1 + b_1 i), (a_2 + b_2 i) \in \mathbb{C}$

تب $(a_1 + b_1 i).(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2) i$

$\because = (a_2 + b_2 i) + (a_1 + b_1 i)$ $(a_1 a_2 - b_1 b_2), (a_1 b_2 + b_1 a_2)$ حقیقی اعداد متلازم ہوتے ہیں۔

لہٰذا تقلیبی خاصیت بہ عمل ضرب پوری ہوئی۔

R_3 : تقلیبی خاصیتیں: ہم جانتے ہیں کہ ملتف اعداد تقسیمی خاصیتیں پوری کرتے ہیں۔

یعنی $(a_1 + b_1 i).\{(a_2 + b_2 i).(a_3 + b_3 i)\} = (a_1 + b_1 i).(a_2 + b_2 i).(a_3 + b_3 i)$

اور $\{(a_2 + b_2 i) + (a_3 + b_3 i)\}.(a_1 + b_1 i) = (a_2 + b_2 i).(a_1 + b_1 i) + (a_3 + b_3 i).(a_1 + b_1 i)$

یہاں ثابت ہوا کہ $(\mathbb{C}, +, \bullet)$ ایک تقلیبی رنگ مع اکائی ہوتا ہے۔

مثال 6۔ اگر $R = \{a + b\sqrt{2} / a, b \in Q\}$ تب ثابت کرو کہ $(R, +, \bullet)$ ایک تقلیبی رنگ مع اکائی ہوگا۔

حل۔ دیا گیا ہے کہ $R = \{a + b\sqrt{2} / a, b \in Q\}$ مطلوبہ خاصتیوں کی آزمائش ذیل میں کی جائے گی۔

$R_1 : (R, +)$ تقلیبی گروپ ہونا چاہیے۔

R_{11} بند شی خاصیت: اگر $(a_1 + b_1\sqrt{2}), (a_2 + b_2\sqrt{2}) \in R$

تب $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in R$

چوں کہ $(a_1+a_2),(b_1+b_2)\in Q$

R_{12} تلازمی خاصیت: غور کرو

$$\begin{aligned}\left(a_1+b_1\sqrt{2}\right)+\left\{\left(a_2+b_2\sqrt{2}\right)+\left(a_3+b_3\sqrt{2}\right)\right\}&=\left(a_1+b_1\sqrt{2}\right)+\left\{(a_2+a_3)+(b_2+b_3)\sqrt{2}\right\}\\&=\left\{a_1+(a_2+a_3)\right\}+\left\{b_1+(b_2+b_3)\right\}\sqrt{2}\\&=\left\{(a_1+a_2)+a_3\right\}+\left\{(b_1+b_2)+b_3\right\}\sqrt{2}\\&=\left\{(a_1+a_2)+(b_1+b_2)\sqrt{2}\right\}+(a_3+b_3)\sqrt{2}\\&=\left\{\left(a_1+b_1\sqrt{2}\right)+\left(a_2+b_2\sqrt{2}\right)\right\}+\left(a_3+b_3\sqrt{2}\right)\end{aligned}$$

تلازمی خاصیت پوری ہوئی۔

R_{13} اکائی خاصیت: اگر $a=0,b=0\in Q$

تب $a+b\sqrt{2}=0+0\sqrt{2}\in R$

یعنی $0\in R$ جمعی اکائی موجود ہے۔

R_{14} معکوس خاصیت: ہم دیکھتے ہیں کہ $\forall\left(a+b\sqrt{2}\right)\in R\,\exists\left(-a+(-b)\sqrt{2}\right)\in R$

$s.t.\left(a+b\sqrt{2}\right)+\left(-a+(-b)\sqrt{2}\right)=0$

لہٰذا معکوسی خاصیت پوری ہوئی۔

R_{15} تقلیبی خاصیت: غور کرو $\left(a_1+b_1\sqrt{2}\right)+\left(a_2+b_2\sqrt{2}\right)=(a_1+a_2)+(b_1+b_2)\sqrt{2}$

$$\begin{aligned}&=(a_2+a_1)+(b_2+b_1)\sqrt{2}\\&=\left(a_2+b_2\sqrt{2}\right)+\left(a_1+b_1\sqrt{2}\right)\end{aligned}$$

یہاں معلوم ہوا کہ $(R,+)$ ایک تقلیبی گروپ ہے۔

R_2: $(R,\bullet)$ ایک نصف گروپ ہوا اور اکائی و تقلیبی خاصیتوں کے ساتھ

R_{21} بند شی خاصیت: اگر $\left(a_1+b_1\sqrt{2}\right),\left(a_2+b_2\sqrt{2}\right)\in R$

تب $\left(a_1+b_1\sqrt{2}\right).\left(a_2+b_2\sqrt{2}\right)=(a_1a_2+2b_1b_2)+(a_1b_2+b_1a_2)\sqrt{2}\in R$

R_{22} تلازمی خاصیت: دیکھا جا سکتا ہے کہ

$$\left(a_1+b_1\sqrt{2}\right)\left\{\left(a_2+b_2\sqrt{2}\right).\left(a_3+b_3\sqrt{2}\right)\right\}=\left\{\left(a_1+b_1\sqrt{2}\right).\left(a_2+b_2\sqrt{2}\right)\right\}.\left(a_3+b_3\sqrt{2}\right)$$

R_{23} اکائی خاصیت: اگر $a=1,b=0\in Q$

تب $a+b\sqrt{2}=1+0\sqrt{2}=1\in R$

یعنی R میں اکائی بہ عمل ضرب موجود ہے۔

R_{25} تقلیبی خاصیت: غور کرو کہ $\left(a_1+b_1\sqrt{2}\right).\left(a_2+b_2\sqrt{2}\right)=(a_1a_2+2b_1b_2)+(a_1b_2+b_1a_2)\sqrt{2}$

$$= (a_2 a_1 + 2b_2 b_1) + (a_2 b_2 + b_2 a_1)\sqrt{2}$$
$$= \left(a_2 + b_2\sqrt{2}\right).\left(a_1 + b_1\sqrt{2}\right)$$

R_3 تقسیمی خاصیتیں: بہ ذریعہ اعمال جمع وضرب دیکھا جاسکتا ہے کہ

$$\left(a_1 + b_1\sqrt{2}\right).\left\{\left(a_2 + b_2\sqrt{2}\right) + \left(a_3 + b_3\sqrt{2}\right)\right\} = \left(a_1 + b_1\sqrt{2}\right).\left(a_2 + b_2\sqrt{2}\right) + \left(a_1 + b_1\sqrt{2}\right)\left(a_3 + b_3\sqrt{2}\right)$$

$$\left\{\left(a_2 + b_2\sqrt{2}\right) + \left(a_3 + b_3\sqrt{2}\right)\right\}\left(a_1 + b_1\sqrt{2}\right) = \left(a_2 + b_2\sqrt{2}\right).\left(a_1 + b_1\sqrt{2}\right) + \left(a_3 + b_3\sqrt{2}\right)\left(a_1 + b_1\sqrt{2}\right)$$

اور

لہٰذا ثابت ہوا کہ $(R, +, \bullet)$ ایک تقلیبی رنگ معہ اکائی ہے۔

مثال 7۔ اگر $M_1 = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} / \, a,b,c,d \in R\right\}$ تب ثابت کرو کہ یہ سٹ ماترسوس کے جمع اور ضرب کے تحت ایک غیر تقلیبی رنگ مع اکائی ہوتا ہے۔

حل۔ دیا گیا ہے $M_1 = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} / \, a,b,c,d \in R\right\}$ کہ جہاں R حقیقی اعداد کا سٹ ہے۔

مطلوبہ خاصیتوں کی جانچ ذیل میں کریں گے۔

$R_1 : (M_1, +)$ ایک تقلیبی گروپ ہونا چاہیے۔

R_{11} بند شی خاصیت: غور کرو اگر $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in M_2$

تب $$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix} \in M_2$$

$$a_1 + a_2, b_1 + b_2, c_1 + c_2, d_1 + d_2 \in R$$

R_{12} تلازمی خاصیت: توجہ کرو

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \left\{\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} + \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}\right\} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 + a_3 & b_2 + b_3 \\ c_2 + c_3 & d_2 + d_3 \end{pmatrix}$$
$$= \begin{pmatrix} a_1 + (a_2 + a_3) & b_1 + (b_2 + b_3) \\ c_1 + (c_2 + c_3) & d_1 + (d_2 + d_3) \end{pmatrix}$$
$$= \begin{pmatrix} (a_1 + a_2) + a_3 & (b_1 + b_2) + b_3 \\ (c_1 + c_2) + c_3 & (d_1 + d_2) + d_3 \end{pmatrix}$$
$$= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix} + \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$$
$$= \left\{\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}\right\} + \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$$

خاصیت پوری ہوئی۔

R_{13} اکائی خاصیت: اگر $a = b = c = d = 0 \in R$

$$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\in M_2$$ تب

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

لہٰذا $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\in M_2$ جمع اکائی ہے۔

R_{14} معکوس خاصیت: غور کرو $\forall\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in M_2\ \exists\begin{pmatrix}-a & -b\\ -c & -d\end{pmatrix}\in M_2$

$$s.t.\begin{pmatrix}a & b\\ c & d\end{pmatrix}+\begin{pmatrix}-a & -b\\ -c & -d\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$

یعنی M_2 کے برماتر س کا جمعی معکوس M_2 میں موجود ہے۔

R_{15} تقلیبی خاصیت:

$$\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}+\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}=\begin{pmatrix}a_1+a_2 & b_1+b_2\\ c_1+c_2 & d_1+d_2\end{pmatrix}$$

$$=\begin{pmatrix}a_1+a_2 & b_1+b_2\\ c_1+c_2 & d_1+d_2\end{pmatrix}=\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}+\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}$$

خاصیت پوری ہوئی۔

$R_2:(M_2,\bullet)$ نصف گروپ ہونا چاہیے۔

R_{21}: بند شی خاصیت: اگر $\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix},\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}\in R$

تب $$\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}+\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}=\begin{pmatrix}a_1a_2+b_1c_2 & a_1b_2+b_1d_2\\ c_1c_2+d_1c_2 & c_1d_2+d_1d_2\end{pmatrix}\in M_2$$

R_{22}: تلازمی خاصیت: ہم جانتے ہیں کہ مانرس تلازمی ہوتے ہیں۔

یعنی $A.(B.C)=(A.B).C$

R_3 تقسیمی خاصیتیں:

بائیں تقسیمی خاصیت پر غور کریں۔

$$\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}.\left\{\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}+\begin{pmatrix}a_3 & b_3\\ c_3 & d_3\end{pmatrix}\right\}=\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}.\begin{pmatrix}a_1+a_3 & b_2+b_3\\ c_2+c_3 & d_2+d_3\end{pmatrix}$$

$$=\begin{pmatrix}a_1(a_2+a_3)+b_1(c_2+c_3) & a_1(b_2+b_3)+b_1(d_2+d_3)\\ c_1(a_2+a_3)+d_1(c_2+c_3) & c_1(b_2+d_3)+d_1(d_1+d_3)\end{pmatrix}$$

$$=\begin{pmatrix}a_1a_2+a_1a_3+b_1c_2+b_1c_3 & a_1b_1+a_1b_3+b_1d_1+b_1d_3\\ c_1a_2+c_1a_3+d_1c_2+d_1c_3 & c_1b_2+c_1b_3+d_1d_2+d_1d_3\end{pmatrix}\to(1)$$

اور

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\cdot\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}+\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\cdot\begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}=\begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{pmatrix}+\begin{pmatrix} a_1a_3+b_1c_3 & a_1b_3+b_1d_3 \\ c_1a_3+d_1c_3 & c_1b_3+d_1d_3 \end{pmatrix}$$

$$=\begin{pmatrix} a_1a_2+b_1c_2+a_1a_3+b_1c_3 & a_1b_2+b_1d_2+a_1b_3+b_1d_3 \\ c_1a_2+d_1c_2+c_1a_3+d_1c_3 & c_1b_2+d_1d_2+c_1b_3+d_1d_3 \end{pmatrix}\rightarrow(2)$$

(1) اور(2)سے بائیں تقسیمی خاصیت بھی پوری ہوتی ہے۔

لہٰذا $(M_2,+,\bullet)$ ایک رنگ ثابت ہوا۔

اب چوں کہ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\in M_2$ اس طرح سے کہ

اس لیے ضربی اکائی موجود ہے لہٰذا رنگ مع اکائی ہوا۔

اور ماتر س بلحاظ ضرب عمل تقلیبی نہیں ہوتے۔

کیوں کہ $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}=\begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{pmatrix}$

اور $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}=\begin{pmatrix} a_2a_1+b_2c_1 & a_2b_1+b_2d_1 \\ c_2a_1+d_2c_1 & c_2b_1+d_2d_1 \end{pmatrix}$

ظاہر ہے $AB\neq BA$

لہٰذا نتیجہ یہ نکلا کہ $(M_2,+,\bullet)$ غیر تقلیبی رنگ مع اکائی ہے۔

مثال8۔ اگر $S=\{f\ /\ f:R\rightarrow R$، $f\}$ مسلسل ہے یعنی مسلسل حقیقی قدر رکھنے والے تفاعل کا سٹ ہے اور انکے درمیان جمع اور ضرب یوں معرف ہیں کہ

$$(f+g)(\gamma)=f(x)+g(\gamma)$$

$$(fog)(x)=f(x).g(x)$$

تب ثابت کرو کہ $(S,+,0)$ ایک تقلیبی رنگ مع اکائی ہوگا۔

حل۔ دیا گیا سٹ اور شائی اعمال کی روشنی میں مطلوبہ خاصیتیں جانچی جائیں گے۔

R_1: $(S,+)$ ایک تقلیبی گروپ ہونا چاہیے۔

R_{11}: بند شی خاصیت، دیے ہوئے تعریف کے مطابق یہ خاصیت صادق ہے۔

R_{12}: تلازمی خاصیت: غور کرو

$$\begin{aligned}(f+(g+h))(x)&=f(x)+(g+h)(x)\\&=f(x)+\{g(x)+h(x)\}\\&=\{f(x)+g(x)\}+h(x)\\&=(f+g)x+h(x)=((f+g)+h)x\end{aligned}$$

خاصیت پوری ہوتی ہے۔

R_{13} :اکائی خاصیت: صفر تفاعل $\forall x \in R, \quad f(x) = 0$ جمعی اکائی ہے۔

R_{14} :معکوس خاصیت: $\forall f(x) \in S \; \exists \quad f(x) \in S$ جمعی اکائی ہے۔

$$s.t.\, f(x) + \big(-f(x)\big) = 0$$

R_{15} :تقلیبی خاصیت: $(f+g)(x) = f(x) + g(x)$ جمعی اکائی ہے۔

$$= g(x) + f(x)$$
$$= (g+f)(x)$$

R_2 : $(S, \bullet)$ نصف گروپ مع اکائی و تقلیبی خاصیت ہونا چاہیے۔

R_{21} :بند شی خاصیت:۔دی ہوئی تعریف $(fog)(x) = f(x).g(x) \in S$ کے مطابق

R_{22} :تلازمی خاصیت:۔ غور کرو $\big(fo(goh)\big)(x) = f(x)(goh)(x)$

$$= f(x).\big(g(x).h(x)\big)$$
$$= \big(f(x)g(x).h(x)\big)$$
$$= (fog)x.h(x)$$
$$= \big((fog)oh\big)(x)$$

چنانچہ تلازمی خاصیت پوری ہوتی ہے۔

R_{23} :اکائی خاصیت: غور کرو کہ $\forall x \in R, \quad f(x) = 1$ تفاعل میں اکائی ہوتا ہے کیونکہ

$$(fog)(x) = f(x)g(x)$$
$$= 1.g(x)$$
$$= g(x)$$

اور

$$(gof)(x) = g(x)\, f(x)$$
$$= g(x).g$$
$$= g(x)$$

R_{25} :تقلیبی خاصیت: توجہ کرو $f, g \in s$ تب

$$(fog)(x) = f(x)g(x)$$
$$= g(x)\, f(x)$$
$$= (gof)(x)$$

خاصیت صادق ہے۔

R_3 :تقسیمی خاصیت: غور کرو $\big(fo(g+h)\big)x = f(x).(g+h)(x)$ تب

$$= f(x)\big[g(x) + h(x)\big]$$
$$= f(x).g(x) + f(x).h(x)$$
$$= (fog)(x) + (foh)(x)$$

اس طرح $\left((g+h)of\right)x=(gof)(x)+(hof)(x)$

صحیح ہو گا۔

چوں کہ $(S,+,0)$ پر رنگ کے تمام صفات پورے ہوئے اور مزید بہ عمل '0' اکائی اور تقلیبی صفات بھی پورے ہوئے اس لیے دیا گیا سٹ تقلیبی رنگ مع اکائی ہے۔

مثال 9۔ صحیح اعداد کا سٹ $\mathbb{Z}$ جس پر دو ثنائی اعمال اس طرح معرف ہیں۔

$$a\oplus b=a+b-1$$

اور $a\otimes b=a+b-ab$

تب ثابت کرو کہ $(\mathbb{Z},\oplus,\otimes)$ اکائی کے ساتھ تقلیبی رنگ ہو گا۔

حل۔ مطلوبہ صفات پر ذیل میں بحث کی جائے گی۔

$R_1:(\mathbb{Z},\oplus)$ تقلیبی گروپ ہونا چاہیے۔

R_{11}: بند شی خاصیت: تعریف کے مطابق $\forall a,b\in\mathbb{Z}\Rightarrow a\oplus b=a+b-1\in\mathbb{Z}$

R_{12}: تلازمی خاصیت: غور کرو $a\oplus(b\oplus c)=a\oplus(b+c-1)$

$=a+(b+c-1)-1$

$=a+b+c-2$

اور $(a\oplus b)\oplus c=(a+b-1)\oplus c$

$=(a+b-1)+c-1=a+b+c-2$

یعنی $a\oplus(b\oplus c)=(a\oplus b)\oplus c$ ثابت ہوا۔

R_{13}: اکائی خاصیت:۔ $\forall a\in\mathbb{Z}\,\exists e\in\mathbb{Z}\ s.t.$

$a\oplus e=a$

$\Rightarrow a+e-1=a$

$e=1\in\mathbb{Z}$ بہ عمل $\oplus$ اکائی ہے۔

R_{14}: معکوس خاصیت:۔ $\forall a\in\mathbb{Z}\,\exists b\in\mathbb{Z}\ s.t.\ a\oplus b=1$

$\Rightarrow a+b-1=1$

$\Rightarrow b=(2-a)=\in\mathbb{Z}$

یعنی بہ عمل $\oplus$ $a^{-1}=(2-a)\in\mathbb{Z}$

R_{15}: تقلیبی خاصیت:۔ غور کرو $a\oplus b=a+b-1$

$=b+a-1$ $\therefore$ صحیح اعداد تقلیبی ہوتے ہیں۔

$=b\oplus a$

$R_2:(\mathbb{Z},\otimes)$ نصف گروپ مع اکائی و تقلیبی خاصیت ہوتا ہو گا۔

R_{21} بند شی خاصیت:۔ جیسا کہ معرف بہ ہے کہ $\forall a,b \in \mathbb{Z} \Rightarrow a \otimes b = a+b-ab \in \mathbb{Z}$

R_{22} : تلازمی خاصیت: غور کرو $a \otimes (b \otimes c) = a \otimes (b+c-bc)$

$$= a+b+c-bc-a(b+c.bc)$$
$$= a+b+c-bc-ab-ac+abc$$

اور $(a \otimes b) \otimes c = (a+b-ab) \otimes c$

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

لہٰذا $a \otimes (b \otimes c) = (a \otimes b) \otimes c$

ثابت ہوا۔

R_{23} :اکائی خاصیت: $\forall a \in \mathbb{Z}\ \exists e \in \mathbb{Z}$

$$s.t\ a \otimes e = a$$
$$\Rightarrow a+e-ae = a$$
$$\Rightarrow e(1-a) = a$$
$$\Rightarrow e = 0 \in \mathbb{Z}$$

یعنی بہ $0 \in \mathbb{Z}$ عمل $\otimes$ اکائی ہے۔

R_{25} : تقلیبی خاصیت:۔ غور کرو $\forall a,b \in \mathbb{Z}, \quad a \otimes b = a+b-ab$

$= b+a-ba$ [چوں کہ صحیح اعداد تقلیبی ہوتے ہیں۔]

$= b \otimes a$ [بہ عمل جمع وضرب]

R_3 : تقسیمی خاصیتیں:۔ غور کرو۔ $a \otimes (b \otimes c) = a \otimes (a+c-1)$

$$= a+(b+c-1)-a(b+c-1) = a+b+c-1-ab-ac+a$$
$$= 2a+b+c-ab-ac-1$$

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

$$= a+b-ab+a+c-ac-1$$
$$= 2a+b+c-ab-ac-1$$

معلوم ہوا کہ بائیں تقسیمی کلیہ پورا ہوتا ہے۔

اسی طرح دائیں تقسیمی کلیہ بھی پورا ہوتا ہے۔

چنانچہ ثابت ہوا کہ $(\mathbb{Z}, \oplus, \otimes)$ رنگ معہ اکائی و تقلیبی ہے۔

9.3 تحت رنگ (Subring)

تعریف:۔ اگر $(R,+,\bullet)$ ایک رنگ ہے اور s اُسکا ایک غیر خالی سٹ ہے تب s تحت رنگ کہلاتا ہے R کا اگر $(s,+,\bullet)$ بھی رنگ ہوتا ہے یعنی $(s,+,\bullet)$ بھی رنگ کی تمام خاصیتیوں کو پورا کرتا ہے۔

مثال(1):۔ ہم جانتے ہیں کہ $(z,+,\bullet)$ رنگ ہوتا ہے۔اور $2z \subset Z$

اور ہم نے دیکھا کہ $(2z,+,\bullet)$ بھی رنگ ہوتا ہے اس لیے $2z$ تحت رنگ ہے۔

مثال(2): اگر $M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} / a,b,c,d \in R \right\}$ تب $(M_2,+,\bullet)$ رنگ ہوتا ہے اور

$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} / a,b,c,d \in R \right\}$ یہاں $S \subset < M_2$ اور بھی رنگ کے تمام خاصیتیں پوری کرتا ہے لہٰذا S تحت رنگ ہے M_2 کا۔

مثال(3): مرکب اعداد/ملتف اعداد کا سٹ $\mathbb{C} = \{a + bi / a,b \in R\}$ رنگ ہوتا ہے۔ بہ اعمال جمع وضرب اور گاسین مجمع اعداد کا سٹ (Gaussian Integers) تحت ہوتا ہے $C = \{a + bi / a,b \in \mathbb{Z}\}$ کا۔

قضیے:۔

قضیہ 1۔ اگر S ایک غیر خالی تحت سٹ ہے رنگ $(R,+,\bullet)$ کا تب S تحت رنگ ہوگا، R کا اگر اور صرف اگر

$\forall a,b \in S \Rightarrow a-b \in S$ (i)

$\forall a,b \in S \Rightarrow a.b \in S$ (ii)

ثبوت۔ فرض کرو کہ S ، R کا تحت رنگ ہے۔

تب $\forall b \in S \Rightarrow -b \in S$ معکوس بہ عمل جمع کی وجہ

تو پھر $\forall a,b \in S \Rightarrow a+(-b) \in S$ بہ عمل جمع بند شی خاصیت کی بنا پر

$\Rightarrow a-b \in S$

اور $\forall a,b \in S \Rightarrow a.b \in S$ بہ عمل ضرب بند شی خاصیت کی بنا پر

چنانچہ ضروری شرائط پوری ہوئیں۔

اس کے بالعکس فرض کرو کہ دیا گیا ہے

$\forall a,b \in S \Rightarrow a-b \in S$ (i)

$\forall a,b \in S \Rightarrow a.b \in S$ (ii)

تب ہمیں ثابت کرنا ہے کہ یہ دو شرطیں کافی ہیں تحت رنگ ہونے کے لیے

دیا گیا ہے کہ $\forall a,b \in S \Rightarrow a-b \in S$

اگر $a = b$

تب $a.a = 0 \in S$ اکائی بہ عمل جمع موجود ہے۔

اگر $a=0$

تب $0-b=-b\in S$ یعنی جمعی معکوس پر عنصر کا S میں موجود ہے۔

تب $a-(-b)=a+b\in S$ یعنی بند شی خاصیت بہ عمل پوری ہوتی ہے اور تلازمیت اور تقلیبیت S تحت سٹ رنگ R کا ہونے کی وجہ موروثی طور پر پوری ہوتی ہے۔

لہٰذا $(S,+)$ تقلیبی گروپ ہوا۔ .....(1)

اور دیا گیا ہے $\forall a,b\in S\Rightarrow a.b\in S$ کہ بند شی خاصیت ہے۔

اور تلازمیت موروثی طور پر پوری ہو گی۔

اس لیے $(S,\bullet)$ نصف گروپ ہوا۔ .....(2)

تقسیمی کلیئے بھی ضرور پورے ہوں گے موروثی طور پر

یعنی $\forall a,b,c\in S$

$$\Rightarrow a.(a+c)=a.b+a.c$$

اور $(b+c)a=b.a+c.a$ .....(3)

(1)،(2)اور(3) کی بنا پر S تحت رنگ ہوا R رنگ بھی کا۔

لہٰذا قضیہ ثابت ہوا۔

قضیہ 2۔ کوئی دو تحت رنگوں کا تقاطع تحت رنگ ہوتا ہے۔

یا

اگر S_1 اور S_2 دو تحت رنگ میں رنگ کے تب $S_1\cap S_2$ بھی R کا تحت رنگ ہو گا۔

ثبوت۔ فرض کرو کہ S_1 اور S_2 دو تحت رنگ ہیں رنگ ہوئے۔

تب ہمیں ثابت کرنا ہے کہ $S_1\cap S_2$ بھی تحت رنگ ہو گا۔

$S_1\cap S_2\neq 0$ چوں کہ $0\in S_1\cap S_2$ اس لیے کہ جمعی اکائی دونوں تحت رنگ میں ہوتی ہے۔

فرض کرو کہ $a,b\in S_1\cap S_2$

$$\Rightarrow a,b\in S_1 \qquad a,b\in S_2$$

تب S_1 تحت رنگ ہونے کی بنا $a-b\in S_1$ اور $ab\in S_1$

اسی طرح S_2 تحت رنگ ہونے کی بنا $a-b\in S_2$ اور $ab\in S_2$

$$\Rightarrow a.b\in S_1\cap S_2$$

اور $ab\in S_1\cap S_2$

لہٰذا $S_1\cap S_2$ تحت رنگ ہوتا ہے۔ قضیہ ثابت ہوا۔

نتیجہ سریح(Corollary)

اگر $S_1, S_2 ..... S_n$ تحت رنگ ہیں رنگ R کے تب $\bigwedge_{i=1}^{n} Si$ بھی تحت رنگ ہوگا۔

ثبوت:۔اوپر قضیہ میں ثابت کیا گیا کہ کسی دو تحت رنگ کا تقاطع تحت ہوتا ہے۔یعنی $S_1 \cap S_2$ تحت رنگ ہوگا۔

تو پھر $(S_1 / S_2) \cap S_3$ بھی تحت رنگ ہوگا۔

اسی طرح $(S_1 \cap S_2 \cap S_3) \cap S_n$ بھی تحت رنگ ہوگا۔

لہٰذا $\bigwedge_{i=1}^{n} Si = S_1 \cap S_2 \cap S_3 ..... S_n$ بھی تحت رنگ ہوگا۔

قضیہ 3۔اگر S_1, S_2 دو تحت رنگ ہیں ایک رنگ R کے تب $S_1 \cup S_2$ تحت رنگ ہوگا اور صرف اگر ایک دوسرے میں شامل ہو یعنی

$S_1 \subset S_2$ یا $S_2 \subset S_1$

کسی دو تحت رنگوں کا اجماع تحت رنگ ہوگا اگر اور صرف اگر کوئی ایک دوسرے میں شامل ہو۔

ثبوت۔فرض کرو کہ S_1, S_2 دو تحت رنگ ہیں رنگ R کے

اور فرض کرو کہ $S_1 \subset S_2$

تب $S_1 \cup S_2 = S_2$

چوں کہ S_2 تحت رنگ ہے اس لیے $S_1 \cup S_2$ بھی تحت رنگ ہوگا۔

یہاں ضروری شرط پوری ہوئی۔

معکوساً فرض کرو کہ $S_1 \cup S_2$ تحت رنگ ہے۔

تب ہمیں ثابت کرنا ہوگا کہ یا تو $S_1 \subset S_2$ یا پھر $S_2 \subset S_1$ ہوگا۔

اگر ممکن ہو تو فرض کریں کہ $S_1 \not\subset S_2$ اور $S_2 \not\subset S_1$

تو پھر $\exists a \in S_1 \;\&\; a \notin S_2$ .....(1)

$\exists b \in S_2 \;\&\; b \notin S_1$ .....(2)

مگر $a, b \in S_1 \cup S_2$

تو پھر $a+b \in S_1 \cup S_2$ چوں کہ $S_1 \cup S_2$ تحت رنگ ہے لہٰذا بند شی ہے۔

ممکنات یہ ہوں گی۔ $a+b \in S_1$ یا $a+b \in S_2$ یا $a+b \in S_1 \cap S_2$

صورت(1):۔ $a+b \in S_1$

چوں کہ $a \in S_1$ اس لیے $-a \in S_1$

تب $-a+(a+b) \in S_1$

$\Rightarrow b \in S_1$ یہ(2) کی تردید کرتا ہے۔

لہٰذا یہ صورت صحیح نہیں ہے یعنی $a+b \notin S_1$

صورت(2) $a+b \in S_2$

چوں کہ $b \in S_2$ اس لیے $-b \in S_2$

تب $a+b+(-b) \in S_2$

$\Rightarrow a \in S_2$ یہ (1) کی تردید کرتا ہے۔

لہٰذا یہ صورت بھی صحیح نہیں ہے یعنی $a+b \notin S_2$

پھر ظاہر ہے کہ $a+b \in S_1 \cap S_2$

چنانچہ $a+b \notin S_1 \cup S_2$ یہ تردید کرتا ہے کہ $S_1 \cup S_2$ تحت رنگ ہے۔

اس لیے مفروضہ $S_1 \not\subset S_2$ اور $S_2 \not\subset S_1$ غلط ہے۔

اس لیے ہونا یہ چاہیے کہ یا تو $S_1 \subset S_2$ یا $S_2 \subset S_1$

قضیہ ثابت ہوا۔

مثال 1۔ثابت کرو کہ $S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} / a,b,c,d \in R \right\}$ تحت رنگ ہوگا تمام 2×2 حقیقی مانرسوں کے رنگ کا۔

حل۔فرض کرو کہ $M_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} / a,b,c,d \in R \right\}$ اور $(M_2, +, \bullet)$ رنگ ہے۔

ظاہر ہے $S \subset M_2$ اور $S \neq 0$

غور کرو $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \in S$

تب $A-B = \begin{bmatrix} a_1-a_2 & b_1-b_2 \\ 0 & c_1-c_2 \end{bmatrix} \in S$ .....(1)

اور $A.B = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} . \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$

$= \begin{bmatrix} a_1a_2 & a_1b_2+b_1c_2 \\ 0 & c_1c_2 \end{bmatrix} \in S$ .....(2)

(1)اور(2)سے ظاہر ہے کہ S تحت رنگ ہے M_2 رنگ کا۔

ثابت ہوا۔

مثال 2۔اگر $(R, +, \bullet)$ ایک رنگ ہے اور $C(R) = \{x \in R / xa = ax \ \forall a \in R\}$ تب ثابت کرو کہ $C(R)$ تحت رنگ ہوگا R کا۔

حل۔دیا گیا ہے کہ $C(R) = \{x \in R / xa = ax \ \forall a \in R\}$

$0a = a0 \ \forall a \in R \because$

$0 \in C(R) \therefore$ یعنی $C(R) \neq 0$

فرض کرو کہ $x, y \in C(R)$

تب $\forall a \in R \qquad xa = ax$ اور $ya = ay$

غور کرو $a(x-y) = ax - ay$

$= xa - ya$

$= (x-y)a$

$\to x - y \in C(R) \qquad \ldots\ldots\ldots\ldots (1)$

اور $a(xy) = (ax)y$

$= (xa)y = x(ay)$

$= x(ya)$

$= (xy)a$

$\to xy \in C(R) \qquad \ldots\ldots\ldots\ldots (2)$

(1)اور(2)سے ظاہر ہے کہ $C(R)$ تحت رنگ ہے۔ثابت کیا گیا۔

مثال3۔ ثابت کرو کہ ایک رنگ R تقلیبی ہوگا اگر اور صرف اگر $\forall a, b \in R$

$\Rightarrow (a+b)^2 = a^2 + 2ab + b^2$

حل۔ فرض کرو کہ R تقلیبی ہے۔

تب $(a+b)^2 = (a+b)(a+b)$

$= a^2 + ab + ba + b^2$

$= a^2 + ab + ba + b^2 \quad \because ab = ba$

$= a^2 + 2ab + b^2$

اس کے برعکس اگر $\forall a, b \in R \Rightarrow (a+b)^2 = a^2 + 2ab + b^2$

تب ہمیں ثابت کرنا ہے کہ $ab = ba$

غور کرو $(a+b)^2 = (a+b).(a+b)$

$= a^2 + ab + ba + b^2$

اور $= a^2 + 2ab + b^2$ دیا گیا ہے۔

لہٰذا $ab + ba = 2ab$

یہ ممکن ہے جب کہ $ab = ba$

لہٰذا R تقلیبی ہوا۔

ثابت ہوا۔

9.4 اکتسابی نتائج(Learning Outcomes)

اس اکائی میں ہم نے رنگ اور تحت رنگ کے کئی مثالوں کی جانکاری حاصل کی اور ان کے متعلق بہت سے نظریات کے بارے میں معلومات حاصل ہو گئی ہو گی۔

9.5 کلیدی الفاظ(Keywords)

رنگ، تحت رنگ، بولین رنگ

9.6 نمونہ امتحانی سوالات(Model Examination Questions)

9.6.1 معروضی جوابات کے حامل سوالات(Objective Answer Type Questions)

1. کسی رنگ کے یونٹ کی تعریف کرو۔
2. بولین رنگ کی مثال دو۔
3. رنگ $R=\{0,2,4,6,8\} \bmod 10$ کی اکائی(Unity) ---------ہے۔

A. 2 B. 4 C. 6 D. 8

4. رنگ $(\mathbb{Z},+,\cdot)$ کے یونٹس ہیں

A. 2 B. 4 C. 6 D. 8

9.6.2 مختصر جوابات کے حامل سوالات(Short Answer Type Questions)

1. ثابت کرو کہ ملتف اعداد کا سٹ بہ عمل جمع وضرب رنگ ہوتا ہے۔
2. تحت رنگ کی تعریف کرو اور ثابت کرو کہ کوئی دو تحت رنگوں کا تقاطع تحت رنگ ہوتا ہے۔
3. رنگ $Z_{14}=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13\}$ کے تمام یونٹس معلوم کرو۔
4. ثابت کرو کہ تمام جفت صحیح اعداد کا سٹ معہ صفر ایک تقلیبی رنگ بغیر اکائی ہوتا ہے بہ اعمال جمع وضرب۔
5. اگر $(R,+,\bullet)$ ایک رنگ ہو اور $C(R)=\{x\in R / xa=ax\ \forall a\in R\}$ تب ثابت کرو کہ $C(R)$ تحت رنگ ہو گا R کا۔
6. ثابت کرو کہ ایک رنگ تقلیبی ہو گا اگر اور صرف اگر $\forall a,b\in R \Rightarrow (a+b)^2=a^2+2ab+b^2$
7. جانچ کرو کہ آیا سٹ $R=\{a\sqrt{2} / a\in Q\}$ بہ عمل جمع وضرب رنگ ہو گا یا نہیں۔

9.6.3 طویل جوابات کے حامل سوالات(Long Answer Type Questions)

1. ثابت کرو کہ $R=\{0,1,2,3,4\} \bmod 5$ رنگ ہو گا بہ اعمال $\oplus_5$ اور $\otimes_5$
2. ثابت کرو کہ $(R,\oplus_{10},\otimes_{10})$ رنگ ہو گا جب کہ $R=\{0,2,4,6,8\} \bmod 10$ ہے۔

3. اگر $M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in R \right\}$ تب ثابت کرو کہ $(M_2, +, \bullet)$ رنگ ہو گا۔

4. اگر ایک غیر خالی تحت سٹ ہے رنگ $(R, +, \bullet)$ کا تب تحت رنگ ہو گا۔

اگر اور صرف اگر $\forall a,b \in S \Rightarrow a-b \in S$ (i)

$\forall a,b \in S \Rightarrow a.b \in S$ (ii)

5. ثابت کرو کہ دو تحت رنگوں کا اجماع تحت رنگ ہو گا اگر اور صرف اگر وہ ایک دوسرے کے تحت سٹ ہوں۔

6. ثابت کرو کہ حقیقی 2×2 ماترسوں کا سٹ $S = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} / a,b,c \in R \right\}$ بہ لحاظ ماترسوں کے جمع اور ضرب کے رنگ ہو گا۔

9.7 مزید مطالعے کے لیے تجویز کردہ کتابیں (Suggested Books for Further Readings)

(1) Surjeet Singh and QaziZameeruddin : Modern Algebra, Vikas Publishing house Pvt. Ltd.

(2) I.N Hevstein, Topic in Algebera, Vikas Publishers

اکائی10۔ انٹگرل دامنے اور میدان
(Integral Domains & Fields)

اکائی کے اجزا

10.0 تمہید(Introduction)

الجبرائی نظام ایک سٹ اور دو ثنائی عمل پر پچھلی اکائی میں بحث کی گئی جسے رنگ کہا گیا۔ یہ عمل ضرب معکوس کو بالکل نظر انداز کیا گیا اور کیلے کے جدول میں دو غیر صفر عناصر کا حاصل ضرب صفر ہونے کو بھی نظر انداز کیا گیا۔ اس اکائی میں خصوصاً ان دو خصوصیات کو بحث میں لا کر رنگ کا نام تبدیل کریں گے۔ انٹگرل دامنہ اور میدان سے۔ پھر ان کے درمیان بننے والے قضیوں کو ثابت کریں گے اور مشقیں بھی حل کی جائیں گی۔

10.1 مقاصد(Objectives)

اس کائی کی تکمیل کے بعد آپ اس قابل ہو جائیں گے کہ صفر کے قاسم(Zero Divisors) کون ہوتے ہیں اور ان کے سٹ میں رہتے ہوئے کیا خصوصیات پیدا ہوتے ہیں۔ انٹگرل دامنہ کی تعریف کر سکیں گے اور میدان کی تعریف کر سکیں اور میدان کی تعریف کر سکیں گے اور ان کے درمیان رشتہ جوڑ سکیں گے۔

10.2 تعریفات(Definitions)

صفر کا قاسم(Zero Divisor): اگر $(R,+,\bullet)$ ایک رنگ ہے اور اگر $a \in R\,(a \neq 0)$ اور $\exists b \neq 0 \in R$ تب اگر $a \cdot b = 0$ تب $'a'$ کو صفر کا بایاں قاسم کہتے ہیں۔ اسی طرح $b \cdot a = 0$ تب $'a'$ کو صفر کا دایاں قاسم کہتے ہیں۔

جو صفر کا بایاں اور دایاں قاسم ہوتا ہے اُسے صفر کا قاسم(Zero Divisors) کہتے ہیں۔

نوٹ۔ ایک تقلیبی رنگ میں ہر بایاں صفر قاسم دایاں صفر قاسم بھی ہوتا ہے۔

مثال 1۔ $R = \{1,2,3,4,5\}\ mod\ 6$ رنگ ہوتا ہے بہ مقیاس 6 جمع و ضرب کے اور ہم دیکھتے ہیں کہ

$$2 \otimes_6 3 = 0 = 3 \otimes_6 2$$

$$3 \otimes_6 4 = 0 = 4 \otimes_6 3$$

لہٰذا $2,3,4$ اس رنگ میں صفر کے قاسم ہیں۔

مثال 2۔ $R = \{0,1,2,3,4\}\ mod\ 5$ رنگ ہوتا ہے بہ مقیاس 5 جمع و ضرب کے اور اس رنگ میں کوئی صفر کے قاسم موجود نہیں ہیں۔

نوٹ(1):۔ جو سٹ بہ مقیاس مفرد عدد ہو اُس میں صفر کے قاسم نہیں ہوتے۔

نوٹ(2):۔ اگر $(\mathbb{Z}_m, \oplus_n, \otimes_n)$ رنگ ہے اور n غیر مفرد صحیح عدد ہے تب $1 < m < n$ اور اگر $(m,n) \neq 1$ یعنی m,n کا $g.c.d$ $'1'$ نہیں ہے تب $'m'$ صفر کا قاسم ہے جیسے مثال (1) میں

چوں کہ $(6,2) = 2 \neq 1$ اس لیے 2 صفر کا قاسم ہے۔

$(6,3) = 3 \neq 1$ اسے لیے 3 صفر کا قاسم ہے۔

$(6,4) = 4 \neq 1$ اس لیے 4 صفر کا قاسم ہے۔

اور $(6,5) = 1$ اس لیے 5 صفر کا قاسم نہیں ہے۔

مثال 3۔ $M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in R \right\}$ بہ عمل جمع وضرب ماترس رنگ ہوتا ہے۔

اور چوں کہ $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

اس لیے $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ دونوں صفر کے قاسم ہیں۔

لہٰذا ماترس کے سٹ میں بھی صفر قاسم پائے جاتے ہیں۔

انتگرل دامنہ (Integral Domain): ایک تقلیبی رنگ معہ اکائی جس میں صفر کے قاسم موجود نہ ہوں انتگرل دامنہ کہلاتا ہے۔

مفصل تعریف:۔ $(D,+,\bullet)$ انتگرل دامنہ کہلاتا ہے۔ اگر درج ذیل خصوصیات پوری ہوتی ہوں۔

$I_1 : (D,+)$ ایک تقلیبی رنگ ہے

I_{11} **: بند شی خاصیت:۔** $\forall a,b \in D \Rightarrow a+b \in D$

I_{12} **: تلازمی خاصیت:۔** $\forall a,b,c \in D \Rightarrow a+(b+c) = (a+b)+c$

I_{13} **: اکائی خاصیت:۔** $0 \in D$

I_{14} **: معکوس خاصیت:۔** $\forall a \in D \Rightarrow \exists b \in D s.t. a+b = 0$

I_{15} **: تقلیبی خاصیت:۔** $\forall a,b \in D \Rightarrow a+b = b+a$

$I_2 : (D,\bullet)$ نصف گروپ معہ اکائی و تقلیبی خاصیت ہو۔

I_{21} **: بند شی خاصیت:۔** $\forall a,b \in D \Rightarrow a \,.\, b \in D$

I_{22} **: اکائی خاصیت:۔** $\forall a,b,c \in D \Rightarrow a.(b.c) = (a.b).c$

I_{23} **: تلازمی خاصیت:۔** $, \in D$

I_{24} **: تقلیبی خاصیت:۔** $\forall a,b \in D \Rightarrow a.b = b.a$

I_3 **: تقسیمی کلیات پورے ہوں۔**

I_{31} **: بایاں تقسیمی کلیہ:۔** $\forall a,b,c \in D \Rightarrow a \,.(b+c) = a.b + a.c$

I_{32} **: دایاں تقسیمی کلیہ:۔** $\forall a,b,c \in D \Rightarrow (b+c).a = b.a + c.c$

$I_4 : D$ میں صفر کے قاسم موجود نہ ہوں۔

یعنی اگر $a,b \in D$ اور اگر $a.b = 0$ تب یا تو $a \neq 0$ یا $b = 0$ ہونا ہوگا۔

نوٹ:۔ انٹگرل دامنہ میں رنگ پر اضافہ درج ذیل خاصیتیں ہیں:

i) (I_{23}) اکائی خاصیت بہ عمل ضرب

ii) (I_{24}) تقلیبی خاصیت بہ عمل ضرب

iii) $D(I_4)$ میں صفر کے قاسم موجود نہ ہوں۔

تقسیمی رنگ (Division Ring / Skew Field): ایک رنگ $(R,+,\bullet)$ کو تقسیمی رنگ کہتے ہیں اگر $(R_0,\bullet)$ ایک گروپ بنتا ہے۔

نوٹ:۔ ایک رنگ پر مندرجہ ذیل خصوصیات اضافہ ہونے پر تقسیمی رنگ کہلاتا ہے:

i) اکائی خاصیت بہ عمل ضرب

ii) معکوس خاصیت بہ عمل ضرب (غیر صفر عناصر پر)

میدان (Field): ایک انٹگرل دامنہ کو میدان کہتے ہیں اگر اُسکے ہر غیر صفر عنصر کا ضربی معکوس موجود ہوں۔

یا

ایک تقلیبی تقسیمی رنگ کو میدان کہتے ہیں۔ یا

$(F,+,\bullet)$ میدان کہلاتا ہے اگر

i) $(F,+)$ ابیلین گروپ ہے۔

ii) $(F,\bullet)$ غیر صفر عناصر، ابیلین گروپ بناتے ہیں۔

تقسیمی کلیات پورے ہوتے ہوں۔

مفصل تعریف:۔

$(F,+,\bullet)$ ایک میدان ہوتا ہے اگر درج ذیل خصوصیات پوری ہوتی ہوں۔

F_1 : $(F,+)$ **ابیلین گروپ ہو۔**

F_{11} : **بند شی خاصیت:۔** $\forall a,b\in F \Rightarrow a+b\in F$

F_{12} : **تلازمی خاصیت:۔** $\forall a,b,c\in F \Rightarrow a+(b+c)=(a+b)+c$

F_{13} : **اکائی خاصیت:۔** $0\in F$

F_{14} : **معکوس خاصیت:۔** $\forall a\in F \Rightarrow \exists b\in F\ s.t.\ a+b=0$

F_{15} : **تقلیبی خاصیت:۔** $\forall a,b\in F \Rightarrow a+b=b+a$

F_2 : $(F,\bullet)$ ابیلین گروپ ہو غیر صفر عناصر کے لیے۔

F_{11} **:بند شی خاصیت:۔** $\forall a,b \in F \Rightarrow a.b \in F$

F_{12} **:تلازمی خاصیت:۔** $\forall a,b,c \in F \Rightarrow a.(b.c) = (a.b).c$

F_{13} **:اکائی خاصیت:۔** $1 \in F$

F_{14} **:معکوس خاصیت:۔** $\forall a \neq 0 \in F \quad \exists b \in F \; s.t. a.b = 1$

F_{15} **:تقلیبی خاصیت:۔** $\forall a,b \in F \Rightarrow a.b = b.a$

F_3 : تقسیمی کلیات پورے ہوتے ہوں $\forall a,b,c \in F \Rightarrow a\ .(b+c) = a.b + a.c$

اور $(b+c).a = b.a + c.a$

نوٹ(1): ایک رنگ پر درج ذیل خصوصیات اضافہ ہونے سے وہ میدان ہوتا ہے:

i) اکائی خصوصیت بہ عمل ضرب

ii) معکوس خصوصیات بہ عمل ضرب غیر صفر عناصر کے لیے

iii) تقلیبی خاصیت بہ عمل

نوٹ(2): کسی بھی انتگرل دامنہ میں کم از کم دو عناصر موجود ہوں گے '0' اور '1' یعنی اکائیاں بہ عمل جمع و ضرب

نوٹ(3): کسی بھی میدان میں بھی کم از کم دو عناصر '0' اور '1' موجود ہونا ہوگا۔

10.3 حل شدہ قضیے (Solved Theorems)

قضیہ 1۔ کسی رنگ $(R,+,\bullet)$ میں صفر کے قاسم شامل نہیں رہتے اگر اور صرف اگر بلحاظ ضرب R میں تنسیخی کلیے صادق ہیں۔

ثبوت۔ فرض کرو کہ R میں صفر کے قاسم شامل نہیں ہیں۔

تب ہمیں ثابت کرنا ہے کہ تنسیخی کلیئے صادق ہیں۔

اگر $a,b,c \in R$ اور $a \neq 0$

تب $ab = bc$

$\Rightarrow \quad b - c = 0 \quad \because a \neq 0$

$\Rightarrow \quad b = c$

اسی طرح $ba = ca$

$\Rightarrow \quad ba - ca = 0$

$\Rightarrow \quad (b-c)a = 0$

$\Rightarrow \quad b - c = 0 \quad \because a \neq 0$

$\Rightarrow \quad b = c$

لہٰذا تنسیخی کلیے بایاں اور دایاں ثابت/صادق ہوا۔

معکوساً فرض کرو کہ تنسیخی کلیے صادق ہیں۔

ہمیں ثابت کرنا ہے کہ R میں صفر کے قاسم شامل نہیں ہیں۔

اگر ممکن ہو فرض کرو کہ $a,b \in R$

اور $a \neq 0, b \neq 0$ اور $ab = 0$

$$\Rightarrow ab = a0$$

$$\Rightarrow b = 0 \qquad \text{تنسیخی کلیہ کی وجہ}$$

یہ بہ عمل نتیجہ ہے چوں کہ فرض کیا گیا تھا کہ $b \neq 0$

اس لیے ممکناً فرض کیا گیا مفروضہ $ab = 0$ اور $a \neq 0, b \neq 0$ ممکن نہیں ہے۔

لہٰذا $ab = 0$ اُسی وقت ہوگا جب کہ یا تو $a = 0$ یا $b = 0$

لہٰذا R میں صفر کے قاسم موجود نہیں ہیں۔

قضیہ ثابت ہوا۔

قضیہ 2۔ کسی بھی انتگرل دامنہ میں تنسیخی کلیئے صادق ہوتے ہیں۔

ثبوت:۔ فرض کرو کہ D ایک انتگرل دامنہ ہے۔

فرض کرو کہ $a,b,c \in D$ اور $a \neq 0$

اور فرض کرو کہ $ab = ac$

$$\Rightarrow ab.ac = 0$$

$$\Rightarrow a(b.c) = 0$$

$(\because D$ انتگرل دامنہ ہے$) \quad \because a \neq 0 \Rightarrow b.c = 0$

لہٰذا تنسیخی کلیہ صادق ہے (بایاں)

اسی طرح اگر $ba = ca$

$$\Rightarrow ba - ca = 0$$

$$\Rightarrow (b-c)a = 0$$

$$\Rightarrow b - c = 0 \quad \because a \neq 0$$

$$\Rightarrow b = c$$

لہٰذا دایاں تنسیخی کلیہ بھی صادق ہے۔

قیضہ ثابت ہوا۔

قضیہ 3۔ کسی بھی میدان میں صفر کے قاسم شامل نہیں ہوتے۔

ثبوت۔ فرض کرو کہ $(F,+,\bullet)$ ایک میدان ہے۔

اگر $a,b \in F$ اور $a \neq 0$

تب F میدان ہونے کی وجہ سے $a^{-1} \in F$ (چوں کہ میدان میں ہر غیر صفر عنصر کا ضربی معکوس موجود ہوتا ہے۔)

تب $a^{-1}a = 1$

اگر $ab = 0$

تب $$a^{-1}(ab) = a^{-1}0$$
$$\Rightarrow (a^{-1}a)b = 0$$
$$\Rightarrow 1b = 0$$
$$\Rightarrow b = 0$$

لہٰذا معلوم ہوا کہ اگر $ab = 0$ اور $a \neq 0$ تب لازماً $b = 0$

اس سے ثابت ہوا کہ میدان F میں صفر کے قاسم موجود نہیں ہیں۔

قضیہ 4۔ ہر میدان ایک انتگرل دامنہ ہے۔

ثبوت۔ فرض کرو کہ $(F,+,\bullet)$ ایک میدان ہے۔

تب F ایک تقلیبی رنگ معہ اکائی اور ہر غیر صفر عنصر کا ضربی معکوس رکھتا ہوگا۔ اب F کو انتگرل دامنہ ثابت کرنے کے لیے صرف یہ کافی ہوگا کہ یہ ثابت کریں کہ F میں صفر کے قاسم شامل نہیں ہے۔

فرض کرو کہ $a,b \in F$ اور $a \neq 0$ تب $a^{-1} \in F$ اس طرح سے کہ $a^{-1}a = 1$

فرض کرو کہ $ab = 0$

تب $$a^{-1}(ab) = a^{-1}0$$
$$\Rightarrow (a^{-1}a)b = 0$$
$$\Rightarrow 1b = 0$$
$$\Rightarrow b = 0$$

لہٰذا معلوم ہوا کہ اگر $ab = 0$ اور $a \neq 0$ تب لازماً $b = 0$

اس سے معلوم ہوا کہ F میں صفر کے قاسم موجود نہیں ہیں۔

لہٰذا ایک F انتگرل دامنہ ہے۔

قضیہ ثابت ہوا۔

نوٹ۔ قضیہ بالا کا معکوس صحیح نہیں ہوتا۔

مثلاً $(Z,+,\bullet)$ انتگرل دامنہ ہے۔

جس میں صفر کے قاسم موجود نہیں ہیں کیوں کہ اگر $a,b \in Z$ اور $a \neq 0$

تب اگر $ab = 0 \Leftarrow b = 0$ لازماً

لیکن Z میدابن نہیں ہے چوں کہ $(Z, \{0\}, \bullet)$ گروپ میں ہوتا اس لیے صحیح عدد کا ضربی معکوس صحیح ہونا ضروری نہیں جیسے

$$2^{-1} = \frac{1}{2} \notin Z$$

لہٰذا $(Z, +, \bullet)$ انتگرل دامنہ ہے لیکن میدان نہیں ہے۔

قضیہ 5۔ ہر متناہی انتگرل دامنہ میدان ہوتا ہے۔

ثبوت۔ فرض کرو کہ $(D, +, \bullet)$ ایک متناہی انتگرل دامنہ ہے۔

فرض کرو کہ $D = \{0, 1, a_1, a_2 .....a_n\}$ سارے ممیّز عناصر ہیں۔

فرض کرو کہ $A = \{1, a_1, a_2 .....a_n\}$ یعنی D کے غیر صفر عناصر ہیں۔

اگر ہم ثابت کرتے ہیں کہ D ہر غیر عنصر کا ضربی معکوس میں موجود ہے تب D میدان ہو جائے گا۔

اگر $a_i \in A$ لہٰذا $a_i \neq 0$

تب $B = a_i A = \{a_i / a_i a_1, a_i a_2 .....a_i a_n\}$

B میں سارے ممیّز عناصر ہوں گے ورنہ اگر $a_i a_j = a_i a_k$

$$\Rightarrow a_j = a_k$$

D کی تعریف کا تردید کرتا ہے۔

اور B کے سارے عناصر غیر صفر ہیں کیوں کہ یہ انتگرل دامنہ کے عناصر ہیں جو کہ صفر ہیں۔ جن کا حاصل ضرب غیر صفر ہی ہوگا کیوں کہ اس میں عنصر کے قاسم موجود نہیں ہوتے۔

لہٰذا میں بھی غیر صفر کے عناصر موجود ہیں جیسا کہ میں ہیں۔ (کسی دوسری ترتیب میں) لہٰذا $A = B$

اور چوں کہ $1 \in A$

$$\Rightarrow 1 \in B$$

تو پھر $a_i a_j = 1$ کسی $1 \leq j \leq n$ کے لیے

$$\Rightarrow a_i^{-1} = a_j \in D$$

یعنی D کے ہر غیر صفر عنصر 'a_i' کا ضربی معکوس D میں موجود ہے۔ لہٰذا D ایک میدان ہوا۔

قضیہ ثابت ہوا۔

قضیہ 6۔ اگر 'p' ایک مفرد عدد ہو تو Zp ایک میدان ہوگا۔

ثبوت۔ ہم جانتے ہیں کہ $Zp = \{0, 1, 2, ...(p-1)\}$ جس میں p عناصر ہیں اور $(Zp, \oplus, \odot)$ رنگ ہوتا ہے۔

چوں کہ ہم جانتے ہیں کہ ایک متناہی انتگرل دامنہ میدان ہوتا ہے۔اس لیے یہ ثابت کرنا کافی ہے کہ ہر ایک انتگرل دامنہ ہے۔ جسکے لیے یہ ثابت کرنا ہو گا کہ

(1) Zp معہ اکائی ضربی ہے۔

(2) Zp تقلیبی بہ عمل ضرب ہے۔

(3) Zp میں صفر کے قاسم شامل نہیں ہیں۔

اب دیکھتے ہیں(1)صاف ظاہر ہے کہ لہٰذا اک $1 \in Zp$ ائی ضربی موجود ہے۔

$\forall a, b \in Zp$ (2)

$a \odot b = b \odot a$ صادق ہے اس لیے کہ صحیح اعداد تقلیبی ہوتے ہیں۔

اور(3)اگر $a, b \in Zp$

اور اگر $a \odot b = 0 \pmod p$

$\because p \Rightarrow p/ab \Rightarrow p/a$ یا p/b مفرد ہے۔

لیکن ایسا نہیں ہو سکتا چوں کہ $1 < a < p$ اور $1 < b < p$

لہٰذا یا تو یا ہوتا ہو گا۔

جس سے معلوم ہوا کہ Zp میں صفر کے قاسم شامل نہیں ہیں۔

لہٰذا درج بالا تینوں شرائط پورے ہونے کی بنا Zp ایک متناہی انتگرل دامنہ ہے۔تو پھر Zp ایک میدان ہوا۔

قضیہ ثابت ہوا۔

قضیہ 7۔ اگر $(Z_n, +, \bullet)$ ایک میدان ہے تب n مفرد عدد ہو گا۔

ثبوت۔ دیا گیا ہے کہ $(Z_n, +, \bullet)$ ایک میدان ہے۔

$Z_n = \{0, 1, 2, 3, \ldots\ldots\ldots (n-1)\} \bmod n$

ثابت کرنا ہے کہ n مفرد(Prime)عدد ہو گا۔

اگر مان لیا جائے کہ n مفرد عدد نہیں ہے تب فرض کریں کہ n, m کا قاسم ہے۔

تب $1 < q < n$ $s.t.$ $\exists q \in Z$ اور $mq = n$ ہو گا۔

$\Rightarrow mq = 0 \pmod n$

چوں کہ Z_n ایک میدان ہے اس لیے اس میں صفر کے قاسم موجود نہیں ہیں۔اس لیے $mq = 0 \pmod n$ تا تو یا $q = 0 \pmod n$ ہونا ہو گا۔

تب یاتو $m=n$ یا $n=q$ ہونا ہوگا۔

$\because m$ قاسم ہے n کا $\Rightarrow m=n$ یا $m=1$

جس سے یہ ثابت ہوتا ہے کہ n ایک مفرد عدد ہی ہوگا۔

کسی رنگ کا ممیّز:(Characteristic of a Ring)

تعریف: فرض کرو کہ $(R,+,\bullet)$ ایک رنگ ہے اور $n\in Z^+$ اقل ترین مثبت صحیح عدد ہو اس طرح سے کہ $\forall a\in R\Rightarrow na=0$ تب $'n'$ کو رنگ R کا ممیّز کہتے ہیں۔ اگر اس طرح کا کوئی صحیح عدد ممکن نہ ہو تب R کو صفر ممیّز رکھنے والا کہا جاتا ہے۔

مثال1۔ $Z_n=\{0,1,2,3,4\}\bmod 5$

$\because 5.0=0$ $\quad 10.0=0$

$5.1=0(\bmod 5)$ $\quad 10.1=0(\bmod 5)$

$5.2=0\ (\bmod 5)$ $\quad 10.2=0$

$5.3=0\ (\bmod 5)$ $\quad 10.3=0$

$5.4=0\ (\bmod 5)$ $\quad 10.4=0$

لیکن 5 اقل ترین مثبت صحیح عدد ہے جو کہ شرط کو پوری کرتا ہے۔

اس لیے $Cha(Z_5)=5$

مثال2۔ $(Z,+,\bullet)$ رنگ ہے۔ یہاں کوئی مثبت عدد نہیں ملے گا جو ں کہ شرط پوری کر سکے $n.a=0\ \forall a\in Z$ ممکن نہیں ہے۔

اس لیے $Cha(Z)=0$

قضیہ8۔ ایک انتگرل دامنہ کا ممیّز صفر ہوتا ہے یا ایک مفرد عدد۔

ثبوت۔ فرض کرو کہ D ایک انتگرل دامنہ ہے۔

اور مان لین کہ D کا ممیّز صفر نہیں ہے۔

تب فرض کرو کہ $Cha(D)=m$ جہاں m اقل ترین صحیح عدد ہے۔

اس طرح سے کہ $ma=0\ \forall a\in D$

اگر ہم فرض کریں کہ m مفرد عدد نہیں ہے تب $1<a<m, 1<b<m$ $\quad \exists a,b\in Z^+$

اس طرح سے کہ $m=ab$

ہم جانتے ہیں کہ $1\in D$

تب غور کرو $m.1=ab.1=(a.1)(b.1)=0$ $\quad$ کیوں کہ $Cha(D)=m$

اور چوں کہ D انتگرل دامنہ ہے اس میں صفر کے قاسم شامل نہیں ہوتے۔

اس لیے $a.1=0$ یا $ba=0$ جب کہ $1<a<m, 1<b<m$

لیکن یہ نہیں ہونا چاہئے اس لیے کہ m اقل ترین مثبت صحیح عدد ہوگا $m.1=0$ ہونے کے لیے کیوں کہ $Cha(D)=m$

لہٰذا مفروضہ کہ m مفرد نہیں ہے غلط ہے۔

اس لیے m کو مفرد عدد ہی ہونا چاہئے۔

لہٰذا ثابت ہوا کہ کسی بھی انٹگرل دامنہ کا ممیّز یا تو صفر ہوتا ہے ورنہ مفرد عدد ہوتا ہے۔

قضیہ ثابت ہوا۔

نوٹ (1) چوں کہ میدان انٹگرل دامنہ ہوتا ہے اس لیے ہر میدان کا ممیّز بھی صفر یا مفرد عدد ہوی ہوتا ہے۔

(2) تقسیمی رنگ کا ممیّز بھی صفر یا مفرد عدد ہی ہوتا ہے۔

(3) Zp رنگ جہاں p مفرد عدد ہے کا ممیّز p ہوتا ہے۔

10.4 حل شدہ مشقیں (Solved Examples)

مثال 1:۔ ثابت کرو کہ $\mathbb{Z}_5=\{0,1,2,3,4\} \bmod 5$ ایک انٹگرل دامنہ ہے۔

حل:۔ دیا گیا ہے کہ $\mathbb{Z}_5=\{0,1,2,3,4\} \bmod 5$

ہمیں ثابت کرنا ہے کہ یہ $(\mathbb{Z}_5,\oplus_5,\otimes_5)$ ایک انٹگرل دامنہ ہوگا۔

کیلے کے جدول دونوں اسطرح ہوں گے۔

$\oplus_5$	0	1	2	3	3
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4.	0	1	2
4	4	0	1	2	3

$\otimes_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

I_1 : $(\mathbb{Z}_5,\oplus_5)$ تقلیبی گروپ ہونا چاہئے۔

I_{11} **: بند شی خاصیت:۔** $\forall a,b\in\mathbb{Z}_5 \Rightarrow a\oplus_5 b\in\mathbb{Z}_5$

جدول بہ عمل $\oplus_5$ دیکھنے سے معلوم ہوتا ہے کہ $\mathbb{Z}_5$ بہ عمل جمع بہ مقیاس 5 بند ہے کیوں کہ کسی بھی $\mathbb{Z}_5$ کے دو عناصر کا حاصل جمع پھر سے $\mathbb{Z}_5$ کا ہے ممبر ہے۔

I_{12} **: تلازمی خاصیت:۔** $\forall a,b,c\in\mathbb{Z}_5 \Rightarrow a\oplus_5(b\oplus_5 c)=(a\oplus_5 b)\oplus_5 c$

مثلاً: $2\oplus_5(3\oplus_5 4)=(2\oplus_5 3)\oplus_5 4$

$$2\oplus_5 2=0\oplus_5 4$$

$$4=4$$

خاصیت صادق ہے۔

I_{13} **:اکائی خاصیت:۔** ہم دیکھتے ہیں کہ $0 \in \mathbb{Z}_5$ اس طرح ہے کہ $0 \oplus a = a \oplus 0 = a$

$\forall a \in \mathbb{Z}_5$ اس لیے '0' بہ عمل مقیاس 5 اکائی ہے۔

I_{14} **:معکوس خاصیت:۔** $\forall\ a \in \mathbb{Z}_5\ \exists b \in \mathbb{Z}_5\ s.t.\ a \oplus b = 0$

ہم دیکھتے ہیں کہ

$$0^{-1} = 0$$
$$1^{-1} = 4$$
$$2^{-1} = 3$$
$$3^{-1} = 2$$
$$4^{-1} = 1 \in \mathbb{Z}_5$$

لہٰذا معکوس خاصیت پوری ہوئی۔

I_{15} **: تقلیبی خاصیت:۔** $\forall\ a,b \in \mathbb{Z}_5 \Rightarrow a \oplus_5 b = b \oplus_5 a$

جدول سے ظاہر ہے کہ

$$3 \oplus_5 4 = 4 \oplus_5 3$$
$$2 = 2$$

سارے ہی عناصر کے لیے یہ خاصیت صادق ہے۔

I_2 : $(\mathbb{Z}_5, \otimes_5)$ نصف گروپ معہ اکائی و تقلیبی ہونا چاہئے۔

I_{21} **:بند شی خاصیت:۔** $\forall a,b \in \mathbb{Z}_5 \Rightarrow a \otimes_5 b \in \mathbb{Z}_5$

جدول بہ عمل $\otimes_5$ سے ظاہر ہے کہ کسی بھی دو عناصر کا حاصل ضرب پھر سے Z_5 کا ممبر ہے لہٰذا $\mathbb{Z}_5$ بہ عمل $\otimes_5$ بند ہے۔

I_{22} **: تلازمی خاصیت:۔** $\forall a,b,c \in \mathbb{Z}_5 \Rightarrow a \otimes_5 (b \otimes_5 c) = (a \otimes_5 b) \otimes_5 c$

مثلاً: $1 \otimes_5 (2 \otimes_5 4) = (1 \otimes_5 2) \otimes_5 4$

$$\Rightarrow 1 \otimes_5 3 = 2 \otimes_5 4$$
$$3 = 3$$

یہ خاصیت سارے ہی عناصر پہ پوری اترتی ہے۔

I_{23} **:اکائی خاصیت:۔** $\forall a \in \mathbb{Z}_5, 1 \in \mathbb{Z}_5\ \ s.t.\ \ a \otimes_5 1 = 1 \otimes_5 a = a$

لہٰذا $1 \in \mathbb{Z}_5$ اکائی ہے بہ عمل $\otimes_5$

I_{24} **: تقلیبی خاصیت:۔** $\forall\ a,b \in \mathbb{Z}_5 \Rightarrow a \otimes_5 b = b \otimes_5 a$

مثلاً: $3 \otimes_5 4 = 4 \otimes_5 3$

$$2 = 2$$

جدول میں دیکھا جاسکتا ہے کہ سارے عناصر یہ خاصیت پورا کرتے ہیں۔

I_3 : **تقسیمی کلیے صادق ہونا چاہیے۔**

$$\forall\, a,b,c \in \mathbb{Z}_5 \Rightarrow a \otimes_5 (b \oplus_5 c) = (a \otimes_5 b) \oplus_5 (a \otimes_5 c)$$

$$e.g.\ 2 \otimes_5 (3 \oplus 4) = (2 \otimes_5 3) \oplus_5 (2 \otimes_5 4)$$

$$\Rightarrow \qquad 2 \otimes_5 2 = 1 \oplus_5 3$$

$$4 = 4$$

اور

$$(b \oplus_5 c) \otimes_5 a = (b \otimes_5 a) \oplus_5 (c \otimes_5 a)$$

$$e.g. (2 \oplus_5 3) \otimes_5 4 = (2 \otimes_5 4) \oplus_5 (3 \otimes_5 4)$$

$$0 \otimes_5 4 = 3 \oplus_5 2$$

$$0 = 0$$

لہٰذا دونوں بایاں اور دایاں تقسیمی کلیے صادق ہیں۔

I_4 : $\mathbb{Z}_5$ میں صفر کے قاسم شامل نہ ہوں۔

جدول بہ عمل $\otimes_5$ سے ظاہر ہے کہ

جہاں بھی $a \otimes_5 b = 0$ تب یا تو $a = 0$ یا $b = 0$

لہٰذا $\mathbb{Z}_5$ میں صفر کے قاسم موجود نہیں ہیں۔

چوں کہ انتگرل دامنہ کے تمام خاصیتیں پوری ہوئی اس لیے $(\mathbb{Z}_5, \oplus_5, \otimes_5)$ انتگرل دامنہ ہے۔

مثال 2 ۔آزمائش کرو کہ آیا $\mathbb{Z}_6 = \{0,1,2,3,4,5\} \bmod 6$ بہ عمل جمع وضرب بہ مقیاس 6 ایک انتگرل دامنہ ہے؟

حل۔دیا گیا ہے کہ $\mathbb{Z}_6 = \{0,1,2,3,4,5\} \bmod 6$

یہ دیکھنے کے لیے کہ آیا یہ انتگرل دامنہ ہے۔ غور کیجئے کیلے جدول پر

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\otimes_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

جدول بہ عمل ضرب بہ مقیاس 6 میں ہم دیکھتے ہیں کہ دو غیر صفر عناصر کا حاصل ضرب صفر ہو رہا ہے۔

جیسے $2 \otimes_6 3 = 0 = 3 \otimes_6 2$

$$3 \otimes_6 4 = 0 = 4 \otimes_6 3$$

لہٰذا $\mathbb{Z}_6$ میں صفر کے قاسم موجود ہیں۔

اور انتگرل دامنہ کے لیے ضروری ہے کہ وہ صفر کے قاسم نہ رکھتا ہو۔

اس لیے $\mathbb{Z}_6$ انتگرل دامنہ نہیں ہے۔

نوٹ:۔ $\mathbb{Z}_6$ انتگرل دامنہ نہیں ہونے کی وجہ سے میدان ہونے کا سوال پیدا نہیں ہوتا۔

مثال 3۔ ثابت کرو کہ $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\} \bmod 7$ بہ عمل جمع وضرب بہ مقیاس 7 ایک میدان ہوتا ہے۔

حل۔ دیا گیا ہے کہ $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\} \bmod 7$

کیلے کے جدول بہ عمل جمع وضرب بہ مقیاس 7 یوں ہوں گے۔

$\oplus_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4.	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\otimes_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$(\mathbb{Z}_7, \oplus_7) = F_1$ تقلیبی گروپ ہونا ہو گا۔

F_{11} **: بند شی خاصیت:۔** $\forall a,b \in \mathbb{Z}_7 \Rightarrow a \oplus_7 b \in \mathbb{Z}_7$

کیلے کے جدول بہ عمل جمع یہ مقیاس 7 سے واضح ہے کہ Z_7 بند ہے۔

F_{12} **: تلازمی خاصیت:۔** $\forall a,b,c \in \mathbb{Z}_7 \Rightarrow a \oplus_7 (b \oplus_7 c) = (a \oplus_7 b) \oplus_7 c$

مثلاً دیکھتے ہیں کہ $3 \oplus_7 (4 \oplus_7 5) = (3 \oplus_7 4) \oplus_7 5$

$$\Rightarrow 3 \oplus_7 2 = 0 \oplus_7 5$$

$$5 = 5$$

لہٰذا خاصیت صادق ہے۔

F_{13} **: اکائی خاصیت:۔** ہم دیکھتے ہیں کہ $0 \in \mathbb{Z}_7$

جہاں $\forall a \in \mathbb{Z}_7 \Rightarrow a \oplus_7 0 = 0 = 0 \oplus_7 a = a$

اس لیے $0 \in \mathbb{Z}_7$ اکائی ہے۔

F_{14} : **معکوس خاصیت:۔** $\forall a \in \mathbb{Z}_7 \exists \;\; b \in \mathbb{Z}_7 \; s.t. \; a \oplus_7 b = 0$

ہم دیکھتے ہیں کہ

$$0^{-1} = 0, 1^{-1} = 6, 2^{-1} = 5, 3^{-1} = 4, 4^{-1} = 3, 5^{-1} = 2, 6^{-1} = 1 \quad \in \mathbb{Z}_7$$

یعنی تمامع ناصر کے معکوس موجود ہیں۔

F_{15} : **تقلیبی خاصیت:۔** $\forall a, b \in \mathbb{Z}_7 \;\Rightarrow\; a \oplus_7 b = b \oplus_7 a$

جدول سے ظاہر ہے یہ خاصیت صادق ہے۔

F_2 : غیر عناصر کے لیے یعنی $\left(\mathbb{Z}_7 - \{0\}, \otimes_7\right)$ تقلیبی گروپ ہونا ہوگا۔

F_{21} : **بند شی خاصیت:۔** $\forall a, b \in \mathbb{Z}_7 \Rightarrow a \otimes_7 b \in \mathbb{Z}_7$

جدول بہ عمل $\otimes_7$ سے ظاہر ہے کہ Z_7 بند ہے۔

F_{22} : **تلازمی خاصیت:۔** $\forall a, b, c \in \mathbb{Z}_7 \Rightarrow a \otimes_7 \left(b \otimes_7 c\right) = \left(a \otimes_7 b\right) \otimes_7 c$

مثلاً دیکھتے ہیں کہ $4 \otimes_7 \left(5 \otimes_7 6\right) = \left(4 \otimes_7 5\right) \otimes_7 6$

$$\Rightarrow 4 \otimes_7 2 = 6 \otimes_7 5$$
$$1 = 1$$

لہٰذا خاصیت صادق ہے۔

F_{23} : **اکائی خاصیت:۔** ہم دیکھتے ہیں کہ $1 \in \mathbb{Z}_7$

اس طرح سے کہ $\forall a \in \mathbb{Z}_7 \Rightarrow a \otimes_7 1 = 1 \otimes_7 a = a$

F_{24} : **معکوس خاصیت:۔** $\forall a \in \mathbb{Z}_7 \exists \;\; b \in \mathbb{Z}_7 \; s.t. \; a \otimes_7 b = 1 \quad \left(a \neq 0\right)$

ہم دیکھتے ہیں کہ

$$1^{-1} = 1, 2^{-1} = 4, 3^{-1} = 5, 4^{-1} = 2, 5^{-1} = 3, 6^{-1} = 6 \quad \in \mathbb{Z}_7$$

یعنی ہر غیر صفر عنصر ضربی معکوس $\mathbb{Z}_7$ میں رکھتا ہے۔

F_{25} : **تقلیبی خاصیت:۔** $\forall a, b \in \mathbb{Z}_7 \;\Rightarrow\; a \otimes_7 b = b \otimes_7 a$

جدول سے ظاہر ہے یہ خاصیت صادق ہے۔

F_3 : **تقسیمی کلیہ صادق ہوتا ہوگا۔**

$$\forall a, b, c \in \mathbb{Z}_7 \Rightarrow a \otimes_7 \left(b \oplus_7 c\right) = \left(a \otimes_7 b\right) \oplus_7 \left(a \otimes_7 c\right)$$

اور $\left(b \oplus_7 c\right) \otimes_7 a = \left(b \otimes_7 a\right) \oplus_7 \left(c \otimes_7 a\right)$

مثلاً $2 \otimes_7 \left(4 \oplus_7 5\right) = \left(2 \otimes_7 4\right) \oplus_7 \left(2 \otimes_7 5\right)$

$$\Rightarrow 2 \otimes_7 2 = 1 \oplus_7 3$$
$$4 = 4$$

اس طرح $(4 \oplus_7 5) \otimes_7 2 = (4 \otimes_7 2) \oplus_7 (5 \otimes_7 2)$

$$\Rightarrow 2 \otimes_7 2 = 1 \oplus_7 3$$
$$4 = 4$$

کیوں کہ تمام میدان کے لیے لازم تمام شرائط کی تکمیل ہوئی اس لیے $(\mathbb{Z}_7, \oplus_7, \otimes_7)$ ایک میدان ہے ثابت ہوا۔

مثال 4۔ ثابت کرو کہ تمام گاسین صحیح اعداد (Gaussian Integers) کا سٹ ایک انٹگرل دامنہ ہوتا ہے بہ عمل جمع و ضرب جانچو کہ آیا یہ میدان بھی ہوتا ہے۔

حل۔ ہم جانتے ہیں کہ گاسین صحیح اعداد کا سٹ یہ ہوگا۔ $G = \{a + bi / a, b \in \mathbb{Z}\}$

ہم انٹگرل دامنہ کے خاصیتیں آزمائیں گے۔

$I_1 : (G, +)$ تقلیبی گروپ ہونا چاہیے۔

I_{11} **بند شی خاصیت:** غور کرو اگر $(a_1 + b_1 i)(a_2 + b_2 i) \in G$

تب $(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i \in G$

I_{12} **تلازمی خاصیت:** توجہ کرو

$$\begin{aligned}(a_1 + b_1 i) + \{(a_2 + b_2 i) + (a_3 + b_3 i)\} &= (a_1 + b_1 i) + \{(a_2 + a_3) + (b_2 + b_3) i\} \\ &= \{a_1 + (a_2 + a_3)\} + \{b_1 + (b_2 + b_3)\} i \\ &= \{(a_1 + a_2) + a_3\} + \{(b_1 + b_2) + b_3\} i \\ &= \{(a_1 + a_2) + (b_1 + b_2) i\} + (a_3 + b_3 i) \\ &= \{(a_1 + b_1 i) + (a_2 + b_3 i)\} + (a_3 + b_3 i)\end{aligned}$$

خاصیت صادق ہے۔

I_{13} **: اکائی خاصیت:** اگر $a = b = 0 \in \mathbb{Z}$ تب $0 + 0i \in G$

اس طرح سے کہ $(0 + 0i) + (a + bi) = (a + bi) + (0 + 0i) = a + bi$

لہٰذا اکائی موجود ہے۔

I_{14} **: معکوس خاصیت:** اگر $a + bi \in G$ تب $(-a + (-b) i) \in G$

جہاں $(a + bi) + (-a + (-b) i) = 0$

لہٰذا $(a + bi)^{-1} = -a - bi \in G$ بہ عمل جمع

I_{15} **: تقلیبی خاصیت:** غور کرو $(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i$

$$= (a_2 + a_1) + (b_2 + b_1)i$$
$$= (a_2 + b_2 i) + (a_1 + b_1 i)$$

لہٰذا خاصیت صادق ہے۔

$I_2 : (G, \bullet)$ نصف گروپ مع اکائی و تقلیبی ہونا چاہئے۔

I_{21} **بند شی خاصیت:** اگر $(a_1 + b_1 i), (a_2 + b_2 i) \in G$

$(a_1 + b_1 i).(a_2 + b_2 i) = (a_1 a_2 + b_1 b_2) + (a_1 b_2 + b_2 a_2)i \in G$ تب $\because (a_1 a_2 - b_1 b_2), (a_1 b_1 + b_1 a_2) \in \mathbb{Z}$

I_{23} **اکائی خاصیت:** غور کرو $a = 1,\ b = 0 \in \mathbb{Z}$ تب $1 + 0i = 1 \in G$

اور $(a + bi).1 = 1.(a + bi) = a + bi$

لہٰذا $1 \in G$ اکائی بہ عمل ضرب موجود ہے۔

I_{24} **تقلیبی خاصیت** : توجہ کرو $(a_1 + b_1 i).(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i$

$$= (a_2 a_1 - b_2 b_1) + (a_2 b_1 + b_2 a_1)i$$
$$= (a_2 + b_2 i).(a_1 + b_1 i)$$

خاصیت صادق ہے۔

I_3 : **تقسیمی کلیات صادق ہونا چاہیے۔**

ہم جانتے ہیں کہ ملتف اعداد تقسیمی ہوتے ہیں۔

یعنی $(a_1 + b_1 i)\{(a_2 + b_2 i) + (a_3 + b_3 i)\} = (a_1 + b_1 i).(a_2 + b_2 i) + (a_1 + b_1 i).(a_3 + b_3 i)$

اور $\{(a_2 + b_2 i) + (a_3 + b_3 i)\}.(a_1 + b_1 i) = (a_2 + b_2 i) + (a_1 + b_1 i) + (a_3 + b_3 i).(a_1 + b_1 i)$

I_4 : G **میں صفر کے قاسم شامل نہ ہوں۔**

غور کرو اگر $(a_1 + b_1 i), (a_2 + b_2 i) \in G$

اور اگر $a_1 + b_1 i \neq 0$

اور اگر $(a_1 + b_1 i).(a_2 + b_2 i) = 0$

$$\Rightarrow (a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i = 0$$
$$\Rightarrow a_1a_2 - b_1b_2 = 0, \quad a_1b_2 + b_1a_2 = 0$$
$$\Rightarrow \frac{a_1}{b_1} = \frac{b_2}{a_2}, \qquad \frac{a_1}{b_1} = -\frac{a_2}{b_2}$$
$$\Rightarrow \frac{b_2}{a_2} = -\frac{a_2}{b_2}$$
$$\Rightarrow {b_2}^2 = -{a_2}^2$$
$$\Rightarrow {a_2}^2 + {b_2}^2 = 0$$

تب لازماً $a_2 = 0\ ,\ b_2 = 0$ کیوں کہ ${a_2}^2$ اور ${b_2}^2$ مثبت یا صفر ہی ہو سکتے ہیں۔ اور دو مثبت اعداد کا حاصل جمع صفر نہیں ہو سکتا۔ لہٰذا

$a_2 + b_2 i = 0$ لازماً

لہٰذا انتگرل دامنہ کے سارے خاصیتیں پورے ہوئے۔

لہٰذا $(G, +, \bullet)$ انتگرل دامنہ ہے۔

G میدان ہونے کے لیے اس کے لیے ہر غیر صفر عنصر کا ضربی معکوس G میں موجود ہونا چاہیے۔

فرض کرو کہ $(a+bi).\ x = 1$

$$\Rightarrow x = \frac{1}{a+bi}$$
$$= \frac{a-bi}{(a+bi)(a-bi)}$$
$$= \frac{a-bi}{a^2+b^2}$$
$$= \left\{\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i\right\} \notin G$$

کیوں کہ $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \notin \mathbb{Z}$

لہٰذا معکوسی خاصیت پوری نہیں ہو پائی۔

اس لیے $(G, +, \bullet)$ یعنی گاسین صحیح اعداد کا سٹ انتگرل دامنہ تو ہو گا لیکن میدان نہیں ہے۔

نوٹ:۔ تمام ملتف اعداد کا سٹ $G = \{a+bi / a, b \in R\}$ انتگرل دامنہ اور میدان دونوں ہوتا ہے کیوں کہ

$$(a+bi)^{-1} = \left\{\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i\right\} \in G$$

اس لیے کہ $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in R$ جہاں $a^2 + b^2 \neq 0$ چوں کہ غیر صفر عناصر کے لیے ہی دیکھا جائے گا۔

مثال 5۔ ثابت کرو کہ سٹ $Q\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} / a, b \in Q\right\}$ بہ عمل جمع و ضرب انتگرل دامنہ اور میدان بھی ہوتا ہے۔

حل۔ حل دیا گیا ہے کہ $Q\left[\sqrt{2}\right]=\left\{a+b\sqrt{2}/\,a,b\in Q\right\}$

انتگرل دامنہ کے خاصیتیں آزمائے جائیں گے۔

$I_1:\left(Q\left[\sqrt{2}\right],+\right)$ تقلیبی گروپ ہونا چاہیے۔

I_{11}: **بند شی خاصیت:۔** اگر $\left(a_1+b_1\sqrt{2}\right)\left(a_2+b_2\sqrt{2}\right)\in Q\left[\sqrt{2}\right]$

تب $\left(a_1+b_1\sqrt{2}\right)+\left(a_2+b_2\sqrt{2}\right)=\left(a_1+a_2\right)+\left(b_1+b_2\right)\sqrt{2}\in Q\left[\sqrt{2}\right]$

معلوم ہوا کہ $Q\left[\sqrt{2}\right]$ بند ہے۔

I_{12}: **تلازمی خاصیت:۔** غور کرو

$$\begin{aligned}\left(a_1+b_1\sqrt{2}\right)+\left\{\left(a_2+b_2\sqrt{2}\right)+\left(a_3+b_3\sqrt{2}\right)\right\}&=\left(a_1+b_1\sqrt{2}\right)+\left\{\left(a_2+a_3\right)+\left(b_2+b_3\right)\sqrt{2}\right\}\\&=\left\{a_1\left(a_2+a_3\right)\right\}+\left\{b_1\left(b_2+b_3\right)\right\}\sqrt{2}\\&=\left\{\left(a_1+a_2\right)+a_3\right\}+\left\{\left(b_1+b_2\right)+b_3\right\}\sqrt{2}\\&=\left\{\left(a_1+a_2\right)+\left(b_1+b_2\right)\sqrt{2}\right\}+\left(a_3+b_3\sqrt{2}\right)\\&=\left\{\left(a_1+b_1\sqrt{2}\right)+\left(a_2+b_2\sqrt{2}\right)\right\}+\left(a_3+b_3\sqrt{2}\right)\end{aligned}$$

خاصیت صادق ہے۔

I_{13}: **اکائی خاصیت:۔** غور کرو $a=b=0\in Q$

اور $a=b=0\in Q\left(Q+0\sqrt{2}\right)\in Q\left[\sqrt{2}\right]$

جب کہ $\left(0+a\sqrt{2}\right)+\left(a+b\sqrt{2}\right)=\left(a+b\sqrt{2}\right)+\left(0+a\sqrt{2}\right)=a+b\sqrt{2}$

$\therefore\ 0+a\sqrt{2}=0\in Q\left[\sqrt{2}\right]$ اکائی ہے۔

I_{14}: **معکوس خاصیت:۔** توجہ کرو $\forall a+b\sqrt{2}\in Q\left[\sqrt{2}\right]\ \exists\left(-a+\left(-b\right)\sqrt{2}\right)\in Q\left[\sqrt{2}\right]$

$$s.t.\ \left(a+b\sqrt{2}\right)+\left(-a-b\sqrt{2}\right)=0$$

لہٰذا ہر عنصر کا معکوس موجود ہے۔

I_{15}: **تقلیبی خاصیت:۔** توجہ کرو $\left(a_1+b_1\sqrt{2}\right)+\left(a_2+b_2\sqrt{2}\right)=\left(a_1+a_2\right)+\left(b_1+b_2\right)\sqrt{2}$

$$\begin{aligned}&=\left(a_2+a_1\right)+\left(b_2+b_1\right)\sqrt{2}\\&=\left(a_2+b_2\sqrt{2}\right)+\left(a_1+b_1\sqrt{2}\right)\end{aligned}$$

خاصیت صادق ہے۔

$I_2:\left(Q\left[\sqrt{2}\right],\bullet\right)$ تقلیبی گروپ مع اکائی و تقلیبی ہونا چاہئے۔

I_{21}: **بند شی خاصیت:۔** غور کرو اگر $a_1+b_1\sqrt{2}, a_2+b_2\sqrt{2}\in Q\left[\sqrt{2}\right]$

تب $\left(a_1+b_1\sqrt{2}\right).\left(a_2+b_2\sqrt{2}\right)=\left(a_1a_2+b_1b_2\right)+\left(a_1b_1+b_1a_2\right)\sqrt{2}\in Q\left[\sqrt{2}\right]$

لہٰذا $Q\left[\sqrt{2}\right]$ بہ عمل بند ہے۔

I_{22}: **تلازمی خاصیت:۔** غور کرو

$$\left(a_1+b_1\sqrt{2}\right).\left\{\left(a_2+b_2\sqrt{2}\right).\left(a_3+b_3\sqrt{2}\right)\right\}=\left\{\left(a_1+b_1\sqrt{2}\right).\left(a_2+b_2\sqrt{2}\right)\right\}.\left(a_3+b_3\sqrt{2}\right)$$

صادق ہو گی چوں کہ حقیقی اعداد تلازمی ہوتے ہیں۔

I_{23}: **اکائی خاصیت:۔** توجہہ کرو $a=1,\ b=0\in Q$

تب $1+0\sqrt{2}=1\in Q\left[\sqrt{2}\right]$

لہٰذا اکائی موجود ہے۔

I_{24}: **تقلیبی خاصیت:۔** غور کرو $\left(a_1+b_1\sqrt{2}\right).\left(a_2+b_2\sqrt{2}\right)=\left(a_1a_2+2b_1b_2\right)+\left(a_1b_1+b_1a_2\right)\sqrt{2}$

$$=\left(a_2a_1+2b_2b_1\right)+\left(a_2b_1+2b_2a_1\right)\sqrt{2}$$
$$=\left(a_2+b_2\sqrt{2}\right).\left(a_1+b_1\sqrt{2}\right)$$

خاصیت صادق ہے۔

I_3: **تقسیمی کلیے صادق ہونا چاہئے۔**

چوں کہ ہر حال نہ عناصر حقیقی اعداد ہیں اس لیے دونوں کلیے صادق ہوں گے۔

یعنی $\left(a_1+b_1\sqrt{2}\right)\left\{\left(a_2+b_2\sqrt{2}\right)+\left(a_3+b_3\sqrt{2}\right)\right\}=\left(a_1+b_1\sqrt{2}\right).\left(a_2+b_2\sqrt{2}\right)+\left(a_1+b_1\sqrt{2}\right).\left(a_3+b_3\sqrt{2}\right)$

اور $\left\{\left(a_2+b_2\sqrt{2}\right)+\left(a_3+b_3\sqrt{2}\right)\right\}.\left(a_1+b_1\sqrt{2}\right)=\left(a_2+b_2\sqrt{2}\right).\left(a_1+b_1\sqrt{2}\right)+\left(a_3+b_3\sqrt{2}\right)\left(a_1+b_1\sqrt{2}\right).$

I_3: $Q\left[\sqrt{2}\right]$ **میں صفر کے قاسم موجود نہ ہونا چاہیے۔**

فرض کرو کہ $\left(a_1+b_1\sqrt{2}\right),\left(a_2+b_2\sqrt{2}\right)\in Q\left[\sqrt{2}\right]$

جہاں $a_1+b_1\sqrt{2}\neq 0$

اور اگر $\left(a_1+b_1\sqrt{2}\right).\left(a_2+b_2\sqrt{2}\right)=0$

$$\Rightarrow\left(a_1a_2+2b_1b_2\right)+\left(a_1b_2+b_1a_2\right)\sqrt{2}=0$$

$$\Rightarrow a_1a_2+2b_1b_2=0 \text{ اور } a_1b_2+b_1a_2=0$$

$$\Rightarrow \frac{a_1}{b_1} = \frac{-2b_2}{a_2} \quad \& \quad \frac{a_1}{b_1} = \frac{-a_2}{b_2}$$

$$\Rightarrow \frac{-2b_2}{a_2} = \frac{-a_2}{b_2}$$

$$\Rightarrow \quad {b_2}^2 = {a_2}^2$$

$$\Rightarrow \quad \frac{a_2}{b_2} = \sqrt{2}$$

یہ ناممکن ہے چوں کہ $a_2, b_2 \in Q$

چنانچہ ضروری ہے کہ $a_2 = 0,\ b_2 = 0$

یعنی $a_2 + b_2\sqrt{2} = 0$

یعنی دو عناصر کا حاصل ضرب اگر صفر ہوتا ہو تو ایک صفر ہونا ضروری ہوا۔

لہٰذا معلوم ہوا کہ $Q\left[\sqrt{2}\right]$ میں صفر کے قاسم شامل نہیں ہیں۔

چوں کہ انتگرل دامنہ کے تمام شرائط پورے ہوئے اس لیے $Q\left[\sqrt{2}\right]$ بہ عمل جمع و ضرب ایک انتگرل دامنہ ہے۔

مثال 6۔ ثابت کرو کہ $\left(Q\left[\sqrt{2}\right], +, \bullet\right)$ انتگرل دامنہ میدان بھی ہوتا ہے۔

حل۔ ہم جانتے ہیں کہ ایک انتگرل دامنہ میدان ہونے کے لیے صرف یہ ثابت کرنا ہوگا کہ انتگرل دامنہ کا ہر غیر صفر عنصر اپنا ضربی معکوس اسی سٹ میں رکھتا ہے۔

لہٰذا فرض کرو کہ $Q\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \,/\, a, b \in Q\right\}$

اور فرض کرو کہ $\left(a + b\sqrt{2}\right).x = 1$ جہاں $a = b \neq 0$

$$x = \frac{1}{a + b\sqrt{2}}$$

$$x = \frac{1}{a + b\sqrt{2}} \times \frac{a - b\sqrt{2}}{a - b\sqrt{2}}$$

$$= \left\{\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}\right\} \in Q\left[\sqrt{2}\right]$$

$$\left[\because \frac{a}{a^2 - 2b^2}, \frac{-b}{a^2 - 2b^2} \in Q\right]$$

چنانچہ معلوم ہوا کہ کے $Q\left[\sqrt{2}\right]$ ہر غیر صفر عنصر کا ضربی معکوس $Q\left[\sqrt{2}\right]$ میں موجود ہے۔

لہٰذا $\left(Q\left[\sqrt{2}\right], +, \bullet\right)$ ایک میدان ہوتا ہے۔

مثال 7۔ $M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in R \right\}$ بہ عمل ماترس کی جمع وضرب جو کہ رنگ ہوتا ہے کیا یہ انتگرل دامنہ اور میدان بھی ہوتا ہے۔

حل۔ دیا گیا ہے $(M_2, +, \bullet)$ کہ رنگ ہے۔

یہ انتگرل دامنہ اور میدان ہونے کے لیے ہم جانتے ہیں کہ ایک رنگ انتگرل دامنہ ہونے کے لیے مزید مندرجہ ذیل 3 شرائط پوری ہونا ہوتا ہے۔

(1) اکائی بہ عمل ضربی موجود ہو۔ جو کہ $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_2$ موجود ہے۔

(2) بہ عمل ضرب تقلیبی ہو۔ نہ نہیں ہو گا۔

اس لیے کہ $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \neq \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$

$$\begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix} \neq \begin{bmatrix} a_2a_1 + b_2c_1 & a_2b_1 + b_2d_1 \\ c_2a_1 + d_2c_1 & c_2b_1 + d_2d_1 \end{bmatrix}$$

شرط پوری نہیں ہو پائی۔

(3) M_2 میں صفر کا قاسم شامل نہ ہو۔

M_2 میں صفر کے قاسم موجود ہوتے ہیں جیسا کہ

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

یعنی دو غیر صفر عناصر کا حاصل ضرب صفر ہو رہا ہے۔

یہ شرط بھی پوری نہیں ہو پائی۔

لہٰذا M_2 انتگرل دامنہ نہیں ہو گا۔

نوٹ:۔ اگر کوئی سٹ انتگرل دامنہ نہیں ہوتا ہے تو اُس کے میدان ہونے کا سوال ہی پیدا نہیں ہوتا۔

لہٰذا $(M_2, +, \bullet)$ میدان نہیں ہوتا۔

مثال 8۔ اگر R ایک غیر صفر رنگ ہے جس میں $a^2 = a \ \forall a \in R$ تب ثابت کرو کہ $cha(R) = 2$

یا

ثابت کرو کہ ایک بولین رنگ کا ممیّز 2 ہوتا ہے۔

حل۔ چوں کہ دیا گیا ہے۔ بولین رنگ کی وجہ سے

$$a^2 = a \ \forall a \in R$$

$$\Rightarrow \quad (a+a)^2 = a+b$$
$$\Rightarrow \quad (a+a).(a+a) = a+a$$
$$\Rightarrow \quad a(a+a)+a(a+a) = a+a$$
$$\Rightarrow (a^2+a^2)+(a^2+a^2) = a+a$$
$$\Rightarrow \quad (a+a)+(a+a) = a+a$$
$$\Rightarrow \quad 2a = 0 \quad \forall a \in R$$

لہٰذا $cha(R) = 2$ ثابت ہوا۔

10.5 اکتسابی نتائج (Learning Outcomes)

اس اکائی میں آپ نے صفر کے قاسم کی تعریف اور اس کے متعلق چند مثالوں کے بارے میں جان لیا ہو گا نیز انٹگرل دامنہ اور میدان کے کئی مثال اور نظریات کو سمجھ گئے ہوں گے۔

10.6 کلیدی الفاظ (Keywords)

انٹگرل دامنہ، میدان

10.7 نمونہ امتحانی سوالات (Model Examination Questions)

10.7.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. $\mathbb{R} = \{0,1,2,3,4,5\}, +_6, \times_6$ کے صفر کے قاسم کتنے ہیں؟

A. 1 B. 2 C. 3 D. 4

2. اگر $(\mathbb{R}, +, \cdot)$ کی ممیز (Characteristic) 2 ہو تو $a + a = 0, \forall a \in \mathbb{R}$ ہو گا۔ (صحیح/غلط)

3. ذیل کا کون سا الجبرائی اسٹرکچر میدان نہیں ہے؟

A. $(\mathbb{Z}, +, \cdot)$ B. $(\mathbb{Q}, +, \cdot)$ C. $(\mathbb{R}, +, \cdot)$ D. $(\mathbb{C}, +, \cdot)$

10.7.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. میدان کی تعریف کرو اور ثابت کرو کہ ہر میدان انٹگرل دامنہ ہوتا ہے۔
2. ثابت کرو کہ ایک انٹگرل دامنہ کا ممیّز (Characteristics) صفر ہوتا ہے یا مفرد عدد۔
3. اگر $cha(R) = 2$ تب ثابت کرو کہ

$$(a+b)^2 = a^2+b^2 = (a-b)^2 \ \forall a,b \in R \quad (i)$$
$$(a+b)^3 = a^3+b^3 \ \ \forall a,b \in R, \ cha(R) = 3 \ (ii)$$

4. $\mathbb{Z}_4$ اور $\mathbb{Z}_5$ کے تمام واحدے معلوم کرو۔

5. اگر R ایک غیر صفر رنگ ہے جس میں $\forall a \in R \quad a^2 = a$ تب ثابت کرو کہ $cha(R) = 2$

6. سٹ $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0)(0,1)(1,0)(1,1)\}$ میں صفر کے قاسم معلوم کرو۔

7. $\mathbb{Z}_6$ کے واحدے معلوم کرو۔

10.7.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. انتگرل دامنہ کی تعریف کرو اور ثابت کرو کہ $(\mathbb{Z}_5, +, \bullet)$ انتگرل دامنہ ہے۔

2. ثابت کرو کہ $(\mathbb{C}, +, \bullet)$ میدان ہوتا ہے۔

3. ثابت کرو کہ گوسین صحیح اعداد کا سٹ انتگرل دامنہ ہوتا ہے لیکن میدان نہیں۔

4. ثابت کرو کہ ایک متناہی انتگرل دامنہ میدان ہوتا ہے۔

5. اگر $M_2 \left\{ \begin{bmatrix} x & y \\ y & x \end{bmatrix} / x, y \in C \right\}$ تب ثابت کرو کہ $(M_2, +, \bullet)$ تقسیمی رنگ یا Skew Field ہوتا ہے۔

10.8 مزید مطالعے کے لیے تجویز کردہ کتابیں (Suggested Books for Further Reading)

1. Surjeet Singh K QaziZameeruddin, Modern Algebra Vikas Publishing House Pvt. Ltd.
2. I.N. Hestien: Topics in Algebra, Vikas Publishers.
3. A text Book of R.Sc. Mathematics (Abstract Algebra) V.VenkateshwavaRao& 5 others, S. Chand & Co Ltd.

اکائی 11۔ آئڈیال اور خارج قسمت رنگ

(Ideals and Quotient Ring)

اکائی کے اجزا

11.0 تمہید(Introduction)

آئڈیال ایک مخصوص قسم کا تحت رنگ ہے اور اس کو رنگ سے وہی نسبت حاصل ہے جو ایک نارمل گروپ کو گروپ سے ہے۔ جرمن ریاضی داں Ernst Kummer (1810-1893) نے صحیح اعداد کے رنگ میں آئڈیال کا تصور استعمال کیا۔ رنگ ہم مارفیت میں ہم مارفیت کا کرنل آئڈیال ہوتا ہے۔ رنگ کے نظریات میں آئڈیال مرکزی حیثیت کا حامل ہے۔ آئڈیال میں بھی خصوصیت پائی جاتی ہے۔ جنھیں Maximal Ideal, Principal Ideal, Prime Ideal مخصوص صفات رکھنے کی بنا پر نامزد کیا گیا ہے۔ ان کے متعلقہ کلیات اور قضیے بحث میں لائے جائیں گے۔

11.1 مقاصد(Objectives)

اس اکائی کی تکمیل پر آپ کو اس قابل ہو جانا چاہیے کہ دائیں اور بائیں آئڈیال اور آئڈیال کی تعریف کر سکیں۔ اس کی مثالیں دے سکیں۔ تین مخصوص آئڈیال کو پہچان سکیں۔ ان کے قضیات اور نتائج کو ثابت کر سکیں۔ خارج قسمت رنگ کی تعریف کر سکیں اس کے خواص اور متعلقہ قضیوں کو ثابت کر سکیں۔

11.2 تعریفات(Definitions)

دایاں آئڈیال(Right Ideals):۔ اگر R ایک رنگ ہے اور $\cup \subset R$ تب $\cup$ دایاں آئڈیال کہلاتا ہے۔ اگر

(1) $\forall a,b \in \cup \Rightarrow a-b \in \cup$ یا $(\cup,+)$ گروپ ہے۔

اور (2) $\forall a \in \cup \ \ \& \ \forall r \in R \Rightarrow ar \in \cup$

بایاں آئڈیال(Left Ideals):۔ اگر R ایک رنگ ہے اور $\cup \subset R$ تب $\cup$ بایاں آئڈیال کہلاتا ہے۔ اگر

(1) $\forall a,b \in \cup \Rightarrow a-b \in \cup$ یا $(\cup,+)$ گروپ ہے۔

اور (2) $\forall a \in \cup \ \ \& \ \forall r \in R \Rightarrow ra \in \cup$

آئڈیال(Ideals):۔ اگر R ایک رنگ ہے اور $\cup \subset R$ تب $\cup$ آئڈیال کہلاتا ہے۔ اگر دو جانبی آئڈیال یعنی دایاں اور بایاں آئڈیال ہے۔

بہ الفاظ دیگر

ایک غیر خالی سیٹ $\cup$ کسی رنگ R کا آئڈیال ہوگا اگر

(1) $\forall a,b \in \cup \Rightarrow a-b \in \cup$ یا $(\cup,+)$ گروپ ہے۔

اور (2) $\forall a \in \cup \ \ \& \ \forall r \in R \Rightarrow ar,\ ra \in \cup$

نوٹ:۔ (1) رنگ R اگر تقلیبی ہے تب دایاں اور بایاں آئڈیال مختلف نہیں ہوتے۔

(2) رنگ کا ہر آئڈیال تحت رنگ ہوگا لیکن معکوس صحیح ہونا ضروری نہیں۔

مثال1 ۔ صحیح اعداد کا رنگ Z تحت رنگ ہوتا ہے ناطق اعداد کے رنگ Q کا لیکن Z آئڈیال نہیں ہوتا Q کا اس لیے کہ

$$5 \in Z,\ \frac{1}{2} \in Q$$

اور $$5.\frac{1}{2} = \frac{5}{2} \notin Z$$

لہٰذا Z ریدیال نہیں ہو سکتا Q کا

(3) کسی بھی رنگ R میں ہمیشہ آئڈیال ہوتا ہے اور R بھی آئڈیال ہوتا ہے R کے لیے۔ $\{0\}$ اور R دونوں غیر واجبی (Trivial) آئڈیال کہلاتے ہیں کے R لیے۔

(4) $\{0\}$ کو صفر آئڈیال یا Null Ideal کہتے ہیں۔

اور R کو اکائی آئڈیال یا Unit Ideal کہتے ہیں۔

(5) غیر واجبی ایدال $\{0\}$ اور R کے علاوہ آئڈیال واجبی ایدال Non-Trivial یا Proper آئڈیال کہلاتے ہیں۔

مثال2 ۔ فرض کرو کہ R تمام صحیح اعداد کا رنگ ہے اور $\cup$ تمام جفت صحیح اعداد معہ صفر رنگ ہے۔ ظاہر ہے کہ $\cup$ تحت رنگ ہے کا

اور $$\forall a \in \cup \ \ \& \ \forall r \in R$$

$$a.r = r.a \in \cup$$

چوں کہ کوئی جفت عدد کو کسی صحیح عدد سے ضرب دینے سے جفت عدد حاصل ہوتا ہے۔ لہٰذا $\cup$ آئڈیال ہے R کا۔

مثال3 ۔ اگر $Z[x]$ کثیر رکنی رنگ ہے جس کے عددی سر صحیح اعداد ہیں اور $I = \langle x, 2 \rangle$ کثیر رکنی رنگ ہے جس کے عددی سر صحیح جفت اعداد ہیں تب I آئڈیال ہوگا۔ $Z[x]$

مثال4۔ اگر $M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / \ a,b,c,d \in 2Z \right\}$ رنگ اور

$L_2 = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / \ a,b \in Z \right\}$ تب M_2, L_2 کا بایاں آئڈیال ہے اور دایاں آئڈیال نہیں ہے۔

مشاہدہ کریں $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2$ اور $\begin{bmatrix} p & 0 \\ q & 0 \end{bmatrix} \in L_2$

تب $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & 0 \\ q & 0 \end{bmatrix} = \begin{bmatrix} ap+bq & 0 \\ cp+dq & 0 \end{bmatrix} \in L_2$ لہٰذا بایاں آئڈیال ہے۔

اور $\begin{bmatrix} p & 0 \\ q & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} pa & pb \\ qa & qb \end{bmatrix} \notin L_2$ لہٰذا دایاں آئڈیال نہیں ہے۔

مثال5 ۔ $(Z_{12}, \oplus_{12}, \otimes_{12})$ ایک تقلیبی رنگ ہے۔ اس کے واجبی (Proper) آئڈیال درج ذیل ہیں۔

$$Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$$
$$I_1 = \{0,2,4,6,8,10\}$$
$$I_2 = \{0,3,6,9\}$$
$$I_3 = \{0,4,8\}$$
$$I_4 = \{0,6\}$$

غیر واجبی آئڈیال $\{0\}$ اور Z_{12} خود ہوں گے۔

اصل آئڈیال(Principal Ideal)

اگر R ایک تقلیبی رنگ معہ اکائی ہے اور $a \in R$ تب $\cup = \{ra / r \in R\}$ جو کہ a کے افعاف کا سیٹ کہلاتا ہے۔ a سے تخلیق شدہ اصل آئڈیال(Principal Ideal) کہلاتا ہے۔ $\cup = \langle a \rangle$ ظاہر کیا جاسکتا ہے۔

نوٹ۔ ایسا رنگ جس کا ہر آئڈیال اصل آئڈیال ہو تو اُس رنگ کو اصل آئڈیال رنگ(Principal Ideal Ring) کہتے ہیں۔

مثال(5) میں Z_{12} اصل آئڈیال رنگ ہے۔ چوں کہ اس کے تمام آئڈیال اصل آئڈیال ہیں جو درج ذیل ہیں۔

$$Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\} = \langle 1 \rangle$$
$$I_1 = \{0,2,4,6,8,10\} = \langle 2 \rangle$$
$$I_2 = \{0,3,6,9\} = \langle 3 \rangle$$
$$I_3 = \{0,4,8\} = \langle 4 \rangle$$
$$I_4 = \{0,6\} = \langle 6 \rangle$$
$$\{0\} = \langle 0 \rangle$$

Z_{12} اور $\{0\}$ غیر واجبی آئڈیال بھی اصل آئڈیال ہیں۔

اور I_1, I_2, I_3, I_4 بھی اصل ایدیال ہیں جو کہ واجبی آئڈیال ہیں۔

مفرد آئڈیال(Prime Ideal)

اگر R ایک تقلیبی رنگ ہے تب ایک آئڈیال $\cup \subset R$ مفرد آئڈیال(Prime Ideal) کہلاتا ہے اگر

$$a,b \in R \;\&\; ab \in \cup \Rightarrow a \in \cup \; or \; b \in \cup$$

مثال۔ انتگرال دامنہ R میں صفر آئڈیال $\{0\}$ مفرد آئڈیال ہوتا ہے۔ اس لیے کہ اگر $a,b \in R$ اور اگر $a,b \in \{0\}$ تب $ab = 0$ تب $b = 0$ یا $a = 0$ چوں کہ انتگرال دامنہ میں صفر کے قاسم موجود نہیں ہوتے۔

لہٰذا $\{0\}$ مفرد آئڈیال ہوگا انتگرال دامنہ R کا۔

عظیمی آئڈیال(Maximal Ideal)

ایک رنگ R کے آئڈیال M کو عظیمی(Maximal) آئڈیال کہتے ہیں۔ اگر $M \neq R$ اور اگر کسی آئڈیال I کے لیے $M \subseteq I \subseteq R$ ہو تو $I = M$ ہو یا $I = R$ بہ الفاظ دیگر

ایک رنگ R کے آئڈیل M کو عظیمی (Maximal) آئڈیل کہتے ہیں۔ اگر $M \neq R$ اور M ہر محیط کوئی اور آئڈیل کا وجود نہ ہو۔

مثال۔ مثال (5) میں رنگ $Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$ ہے۔

Z_{12} اور $\{0\}$ غیر واجبی آئڈیل ہے۔

اور $I_1 = \{0,2,4,6,8,10\}$

$I_2 = \{0,3,6,9\}$

$I_3 = \{0,4,8\}$

$I_4 = \{0,6\}$

واجبی آئڈیل ہیں۔

ان میں I_1 عظیمی آئڈیل ہے۔ اور I_2 بھی عظیمی آئڈیل ہے کیوں کہ ان کو محیط کیے ہوئے کوئی اور آئڈیل کا وجود نہیں ہے۔ جب کہ I_3 عظیمی آئڈیل نہیں ہے چوں کہ ان عناصر کو رکھتے ہوئے I_1 آئڈیل وجود ہیں۔ اسی طرح I_4 عظیمی آئڈیل نہیں ہے چوں کہ اس پر محیط I_2 اور I_1 آئڈیل موجود ہیں۔

خارج قسمت رنگ (Quotient Ring or Factor Ring)

تعریف:۔ اگر U ایک آئڈیل ہے رنگ R کا تب سیٹ $\{x+U / x \in R\} = \frac{R}{U}$ ایک رنگ ہوتا ہے جو کہ خارج قسمت رنگ کہلاتا ہے۔

جس کے اعمال جمع و ضرب یوں معرف ہیں۔ $(a+U)+(b+U)=(a+b)+U \quad \forall a,b \in R$

$$\& \ (a+U).(b+U) = ab+U \ \forall a,b \in R$$

نوٹ (1):۔ R رنگ ہونے کی بناء پہ عمل جمع تقلیبی ہے۔ اس لیے $x+U = U+x$ ہو گا۔

اس صورت میں $\forall a,b \in R \ (U+a)+(U+b) = U+(a+b)$

$$\& \ (U+a).(U+b) = U+ab \quad \forall a,b \in R$$

نوٹ (2):۔ $\frac{R}{U}$ خارج قسمت رنگ کا صفر $U+0$ یا $0+U$ یعنی ہو گا۔ اور اسکی اکائی $U+1$ یا $1+U$ ہو گا۔

نوٹ (3):۔ $a+U$ کو $\bar{a}$ یا $[a]$ سے بھی ظاہر کیا جاتا ہے۔

ایسی صورت میں $[a]+[b]=[a+b]$ اور $[a].[b]=[ab]$ سے ظاہر کیا جائے گا۔

نوٹ (4):۔ اگر $(a+b)=(b+U)$ تب $a-b \in U$

نوٹ (5):۔ اگر $a+U=U$ تب $a \in U$

11.3 حل شدہ قضیے (Solved Theorems)

قضیہ 1۔ کسی U ایک آئڈیل ہے اور رنگ معہ اکائی R کا اور اگر $1 \in U$ تب $U = R$ ہو گا۔

ثبوت۔ $\cup$، R کا آئڈیال ہونے کی وجہ سے $\cup \subset R$ ..... (1)

چوں کہ $1 \in \cup$

اس لیے $\forall\ x \in R\ \&\ 1 \in \cup \Rightarrow x.1 \in \cup$ ($\cup$ آئڈیال ہونے کی وجہ)

$$i.e. \quad x \in \cup$$

تب (1) اور (2) کی بنا پر معلوم ہوا کہ $\cup = R$

قضیہ ثابت ہوا۔

قضیہ 2۔ کسی بھی میدان (Field) کے واجبی آئڈیال (Proper/Non-Trivial) نہیں ہوتے۔

(یا)

کسی بھی میدان F کے صفر دو آئڈیال $\{0\}$ اور F ہی ہوں گے۔

ثبوت۔ فرض کرو کہ U آئڈیال ہے ایک F میدان کا۔

اور اگر $\cup \neq \{0\}$ تب ہمیں ثابت کرنا ہوگا کہ $\cup = F$ ہی ہوگا۔ ظاہر ہے $\cup \subset F$ چوں کہ $\cup$ آئڈیال ہے F کا۔

اگر $a \in \cup$ اور $a \neq 0$ تب $a^{-1} \in F$

اور $\cup$ پھر آئڈیال ہونے کی وجہ $aa^{-1} \in \cup$

$$\Rightarrow 1 \in \cup$$

تب $\forall\ x \in F$

$x.1 \in \cup$ آئڈیال ہونے کی وجہ سے

$$\Rightarrow x \in \cup$$
$$\Rightarrow F \subset \cup$$

اور $\cup \subset F$ ہوتا ہی ہے۔

$$\Rightarrow \cup = F$$

اس سے معلوم ہوا کہ یا تو $\cup = \{0\}$ ہوگا یا $\cup = F$ ہی ہوگا۔

قضیہ ثابت ہوا۔

قضیہ 3۔ اگر R ایک تقلیبی رنگ ہے اور $a \in R$ تب $Ra = \{ra / r \in R\}$ آئڈیال ہوگا R کا۔

ثبوت۔ دیا گیا ہے کہ $Ra = \{ra / r \in R$ اور $a \in R$

چوں کہ $0 \in R$

$0a = 0 \in Ra \therefore$ لہٰذا $Ra \neq Q$

اور $Ra \subset R$

فرض کرو کہ $x, y \in Ra$

اور مان لیں کہ اور $x = r_2 a \quad r_1\ r_2 \in R$ اور $y = r_2 a$

تب F میدان ہونے کی وجہ سے $a^{-1} \in F$ (چوں کہ میدان میں ہر غیر صفر عنصر کا ضربی معکوس موجود ہوتا ہے۔)

تب $x - y = r_1 a - r_2 a$

$= (r_1 - r_2) a \in Ra \quad \because (r_1 - r_2) \in R$ .....(1)

اور اگر $x \in Ra$ اور $r \in R$

تب $x.r = (r_1 a) r$

$= r_1 (a r)$

$\because R$ تقلیبی رنگ ہے۔ $= r_1 (ra)$

$= (r_1 r) a \in Ra \qquad \therefore r_1 r \in R$

اور $x.r = r.x \in Ra$ چوں کہ R تقلیبی ہے۔ .....(2)

(1) اور (2) کی بناء Ra آئڈیال ہوا رنگ R کا قضیہ ثابت ہوا۔

نوٹ:۔ R تقلیبی ہونے کی وجہ سے $Ra = aR = \{ra / r \in R\}$ بھی آئڈیال ہو گا۔

قضیہ 4۔ ایک تقلیبی رنگ معہ اکائی ایک میدان ہوتا ہے اگر اس کے کوئی واجبی آئڈیال نہ ہوا۔

ثبوت۔ فرض کرو کہ R ایک تقلیبی رنگ معہ اکائی ہے۔

اور R کے کوئی واجبی آئڈیال نہیں ہیں یعنی اسکے صرف دو غیر واجبی آئڈیال $\{0\}$ اور R ہی ہیں۔

ثابت کرنا ہے کہ R ایک میدان ہو گا۔

جس کے لیے یہ ثابت کرنا ہو گا کہ R کے ہر غیر صفر عنصر کا ضربی معکوس R میں موجود ہو گا۔ فرض کرو کہ $a \neq 0 \in R$

ہم جانتے ہیں $ab0 \in R$ $aR = \{ar / r \in R\}$ کہ آئڈیال ہوتا ہے کا چوں کہ $a \neq 0$ اس لیے $aR \neq \{0\}$ لہٰذا $aR = R$ ہی ہوتا ہو گا۔ (چوں کہ اس کے دو ہی غیر واجبی آئڈیال ہیں۔)

چوں کہ $1 \in R$ اس لیے $1 \in aR$

تب $\exists b \neq 0 \in Q$

$s.t. ab = 1 \in R$

$\Rightarrow a^{-1} = b \in R$

معلوم ہوا کہ کوئی بھی $a \neq 0 \in R$ کا ضربی معکوس R میں موجود ہے۔ لہٰذا R ایک میدان ہوا۔ قضیہ ثابت ہوا۔

قضیہ 5۔ کسی رنگ R کے کوئی بھی دو آئڈیال کا تقاطع (Intervention) R کا آئڈیال ہو گا۔

ثبوت۔ فرض کرو کہ R رنگ ہے اور U_1, U_2 اس کے دو آئڈیال ہیں۔

چوں کہ $0 \in R$ اس لیے $0 \in U_1,\ 0 \in U_2$ سارے ممیّز عناصر ہیں۔

لہٰذا $0 \in U_1 \cap U_2$

$\Rightarrow U_1 \cap U_2 \neq 0$

مان لیں کہ $a, b \in U_1 \cap U_2$

تب $a, b \in U_1,\ a, b \in U_2$

$\because U_1$ اور U_2 دونوں آئڈیال ہیں۔ $\Rightarrow a-b \in U_1 \quad \& \ a-b \in U_2$

$$(1).....\Rightarrow a-b \in U_1 \cap U_2$$

اور $r \in R$ کے لیے

$ar, ra \in U_1$

اور $ar, ra \in U_2$ چوں کہ U_1 اور U_2 آئڈیال ہیں۔

$$(2)..... \Rightarrow ar, ra \in U_1 \cap U_2$$

(1) اور (2) کی بناء معلوم ہوا کہ $U_1 \cap U_2$ ایدال ہے R کا۔ قضیہ ثابت ہوا۔

نتیجہ صریح:۔ اگر $U_1, U_2, ...U_n$ آئڈیال ہوں رنگ R کے تب $\bigcap_{i=1}^{n} U_i$ بھی R کا آئڈیال ہو گا۔ اس لیے جب دو آئڈیال کا تقاطع $U_1 \cap U_2$ آئڈیال ہے تب $(U_1 \cap U_2) \cap U_3$ بھی آئڈیال ہو گا۔ پھر $(U_1 \cap U_2 U_3) \cap U_4$ بھی آئڈیال ہو گا۔

اس طرح $\bigcap_{i=1}^{n} U$ آئڈیال ہو گا۔

قضیہ 6۔ اگر U_1 اور U_2 دو آئڈیال ہیں رنگ R کے تب $U_1 \cup U_2$ بھی R کا آئڈیال ہو گا اگر اور صرف اگر $U_1 \subset U_2$ یا $U_2 \subset U_1$ ہو یعنی ایک دوسرے میں ضم ہو۔

ثبوت۔ دیا گیا ہے کہ U_1 اور U_2 دو رنگ R کے آئڈیال ہیں۔

فرض کرو کہ ایک دوسرے میں ضم ہے یعنی $U_1 \subset U_2$

تب ہمیں ثابت کرنا ہو گا کہ $U_1 \cup U_2$ آئڈیال ہو گا۔

چوں کہ $U_1 \subset U_2$ اس لیے $U_1 \cup U_2 = U_2$

اب چوں کہ U_2 آئڈیال ہے اس لیے $U_1 \cup U_2$ بھی آئڈیال ہو گیا۔

اس کے بالعکس فرض کرو کہ $U_1 \cup U_2$ آئڈیال ہے رنگ کا .....(1)

تب ہمیں ثابت کرنا ہو گا کہ یا تو $U_1 \subset U_2$ یا $U_2 \subset U_1$ ہونا چاہئے۔

لیکن اگر امکاناً مان لیا جائے کہ $U_1 \not\subset U_2$ اور $U_2 \not\subset U_1$

تب $\exists a \in U_1 \ \& \ a \notin U_2$ .....(2)

اور $\exists b \in U_2 \ \& \ b \notin U_1$ .....(2)

اور لازماً $a, b \in U_1 \cup U_2$

تب $U_1 \cup U_2$ آئڈیال ہونے کی بناء $a+b \in U_1 \cup U_2$ چوں کہ آئڈیال '+' کے تحت کا تحت گروپ ہوتا ہے۔

لہٰذا $a+b \in U_1 \cup U_2$ یا $a+b \in U_2$ یا $a+b \in U_1$

صورت(1) $a+b \in U_1$ تب چوں کہ $a \in U_1$

تب $-a \in U_1$ (تحت گروپ ہونے کی وجہ سے معکوسی خاصیت کی بناء)

تب $-a+(a+b) \in U_1$

$\Rightarrow b \in U_1$

یہ(3) کی تردید کرتا ہے۔

لہٰذا $a+b \notin U_1$

صورت(2):۔ $a+b \in U_2$ تب چوں کہ $b \in U_2$

اس لیے $-b \in U_2$

تب $(a+b)+(-b)+ \in U_2$

$\Rightarrow a \in U_2$

یہ(2) کی تردید کرتا ہے۔

لہٰذا $a+b \notin U_2$

تب صورت(3) $a+b \in U_1 \cap U_2$ کا سوال ہی نہیں پیدا ہوتا۔

تب نتیجہ یہ ہو گا کہ $a+b \in U_1 \cup U_2$ اور یہ(1) کی تردید کرتا ہے۔اس نتیجہ پر اس لیے پہنچے کہ امکان $U_2 \not\subset U_1$ اور $U_1 \not\subset U_2$ کو مانا گیا

لہٰذا یہ مفروضہ غلط ہے۔

لہٰذا ہونا یہ ہو گا کہ یا تو $U_2 \subset U_1$ یا $U_1 \subset U_2$ یعنی ایک دوسرے میں ضم ہونا چاہئے قضیہ ثابت ہوا۔

قضیہ 7۔ کوئی بھی میدان اصل آئڈیال رنگ ہوتا ہے۔

ثبوت۔ فرض کرو کہ $(F,+,\bullet)$ ایک میدان ہے۔تب ہم جانتے ہیں کہ F کے صرف دو ہی آئڈیال $\langle 0\rangle$ اور $\langle 1\rangle$ ہوتے ہیں۔اور یہ دونوں آئڈیال چوں کہ اصل آئڈیال ہیں۔اس لیے F اصل آئڈیال رنگ ہوگا۔قضیہ ثابت ہوا۔

قضیہ 8۔ صحیح اعداد کا رنگ $(Z,+,\bullet)$ اصل آئڈیال رنگ ہوتا ہے۔(یا) صحیح اعداد کا رنگ Z کا ہر آئڈیال اصل آئڈیال ہوتا ہے۔

ثبوت۔ فرض کرو کہ U کا آئڈیال ہے Z کا۔

تب اگر $U=\{0\}$ تب $U=\langle 0\rangle$ اصل آئڈیال ہے۔

اور اگر $U\neq\{0\}$ تب $\exists a\,t\,U\ \&\ a+0$

تب U آئڈیال ہونے کی بناء $-a\in U$

تب چوں کہ $U\subset Z$

اس لیے a اور $-a$ میں کوئی ایک مثبت صحیح عدد ہوگا۔

لہٰذا $U^+\neq\phi$

تب U^+ میں کی Well Ordering Principle کی بنا U^+ میں کم ترین صحیح عدد ہوگا۔فرض کرو کہ $b\in U^+$ کم ترین صحیح عدد ہے۔اب ہم کوشش کریں گے کہ $U=\langle b\rangle$ اصل آئڈیال ہو جائے گا۔

فرض کرو کہ $x\in U$

تب چوں کہ $b\neq 0$ اس لیے $\exists\ q,r\in Z$

اس طرح سے کہ $x=bq+r \quad 0\leq r<b$

اب چوں کہ $q\in Z\ \&\ b\in U$ اور U آئڈیال ہے Z کا

اس لیے $bq\in U$

اور چوں کہ $x\in U$

اس لیے $x-bq\in U$ آئڈیال کی وجہ

یعنی $r\in U$

اب چوں کہ $0\leq r<b$ اور $b\in U^+$ کم ترین ممبر ہے۔

اس لیے لازماً $r=0$ ہوگا۔

چنانچہ $x-bq=r=0$

$$\Rightarrow x=bq$$

لہٰذا کوئی بھی عنصر $x\in U$ b کا اضعاف ہوگا۔

لہٰذا $U = \{bq / q \in Z\}$

$\Rightarrow U = \langle b \rangle$

یعنی U اصل آئڈیال ہوا۔ گویا Z کا ہر آئڈیال اصل ہے۔ اس لیے اصل آئڈیال رنگ ہے۔ قضیہ ثابت ہوا۔

قضیہ 9۔ اگر U ایک آئڈیال ہے رنگ R کا تب سیٹ $\forall a,b \in U \quad \frac{R}{U} = \{x+U / x \in R\}$ معرف بہ اعمال جمع و ضرب

$$(a+U)+(b+U) = a+b+U$$

$$(a+U).(b+U) = ab+U$$

جہاں $\forall a+U, b+U \in \frac{R}{U}$

ایک رنگ ہوتا ہے۔

ثبوت۔ چوں کہ $(R,+)$ ایک تقلیبی گروپ ہوتا ہے اسلیے $\left(\frac{R}{U},+\right)$ بھی تقلیبی ہو گا۔

$\left(\frac{R}{U},+,\bullet\right)$ کو رنگ ثابت کرنے کے لیے ہمیں ثابت کرنا ہو گا کہ

(1) ہم سیٹیں بہ عمل ضرب خوش معرف ہے۔

(2) عمل ضرب تلازمی ہے۔

(3) تقسی می کلیے صادق ہیں۔

لہٰذا (1) فرض کرو کہ $a+U = a_1+U$ اور $b+U = b_1+U$

تب $a = a_1+U_1$ اور $b = b_1+U_2$ جہاں $U_1, U_2 \in U$

تب $$ab = (a_1+U_1)(b_1+U_2)$$

$$= a_1b_1 + a_1U_2 + U_1b_1 + U_1U_2$$

چوں کہ U آئڈیال ہے اس لیے $a_1U_2, U_1b_2, U_1U_2 \in U$

$$\therefore ab - a_1b_1 \in U$$

$$\Rightarrow ab+U = a_1b_1+U$$

$$\Rightarrow (a+U).(b+U) = (a_1+U).(b_1+U)$$

اس لیے ثابت ہوا کہ ہم سیٹیں کا ضرب خوش معرف ہے۔

اور (2) فرض کرو کہ $a+U, b+U, c+U \in \frac{R}{U}$

تب $$\left[(a+U).(b+U)\right].(c+U) = (ab+U).(c+U)$$

$$= (ab)c + U$$
$$= a(bc) + U \quad \because a, b, c \in R[Ring]$$
$$= (a+U).(bc+U)$$
$$= (a+U).[(b+U)(c+U)]$$

لہٰذا عمل ضرب تلازمی ہے۔

(3) تقسیمی کلیات کے لیے دیکھیں

$$= (a+U).[(b+U)(c+U)] = (a+U).[(b+c)+U]$$
$$= a.(b+c)+U$$
$$= (ab+ac)+U$$
$$= (ab+U).(ac+U)$$
$$= (a+U).(b+U)+(a+U).(c+U)$$

بایاں تقسیمی کلیہ صادق ہوا۔

اسی طرح دایاں تقسیمی کلیہ بھی صادق ہوتا ہے۔

سارے شرائط پورے ہوئے اس لیے $\left(\frac{R}{U}, +, \bullet\right)$ رنگ ہوا۔ قضیہ ثابت ہوا۔

قضیہ 10۔ اگر $\frac{R}{U}$ خارج قسمت رنگ ہے تب

(1) اگر R تقلیبی ہے تب $\frac{R}{U}$ بھی تقلیبی ہوگا۔

(2) اگر R معہ اکائی ہے تب $\frac{R}{U}$ بھی معہ اکائی ہوگا۔

ثبوت۔ (1) چوں کہ R تقلیبی ہے اس لیے $\forall a, b \in R \quad ab = ba$

اور $a+U, b+U \in \frac{R}{U}$

تب
$$(a+U).(b+U) = ab+U$$
$$= ba+U$$
$$= (b+U).(a+U)$$

لہٰذا $\frac{R}{U}$ تقلیبی ہے۔

(2) چوں کہ R معہ اکائی ہے اس لیے $1 \in R$ اس طرح سے کہ $\forall a \in R \quad 1.a = a.1 = a$

فرض کرو کہ $a+U \in \frac{R}{U}$ اور $1+U \in \frac{R}{U}$ جہاں $a, 1 \in R$

تب دیکھیں کہ $(a+U).(1+U) = a.1+U$
$= a+U$

اسی طرح $(1+U).(a+U) = 1a+U$
$= a+U$

لہٰذا $1+U \in \frac{R}{U}$ اکائی ہے۔ قضیہ ثابت ہوا۔

قضیہ 11۔ اگر R تقلیبی رنگ ہے اور $U \neq R$ آئڈیال ہے تب مفرد آئڈیال ہوگا۔ اگر صرف اگر $\frac{R}{U}$ انتگرال دامنہ ہو۔

ثبوت۔ فرض کرو کہ U مفرد آئڈیال تقلیبی رنگ کا۔

تب ہمیں ثابت کرنا ہے کہ $\frac{R}{U}$ انتگرال دامنہ ہے۔

جس کے لیے یہ ثابت کرنا ہوگا کہ $\frac{R}{U}$ میں صفر کے قاسم موجود ہیں۔

فرض کرو کہ $a+U, b+U \in \frac{R}{U}$ اور $a+U$ صفر ہے $\frac{R}{U}$ میں

اور اگر $(a+U).(b+U) = 0+U$

تب $ab+U = 0+U = U$

$\Rightarrow ab \in U$

تب چوں کہ U مفرد آئڈیال ہے اس لیے یا تو $a \in U$ ہوگا یا پھر $b \in U$

تب $a+U = U$ یا $b+U = U$

یعنی $a+U$ یا $b+U$ صفر ہے۔

اس سے ثابت ہوا کہ $\frac{R}{U}$ میں کوئی دو غیر صفر عناصر کا حاصل ضرب صفر نہیں ہو سکتا۔ اس لیے $\frac{R}{U}$ میں صفر کے قاسم موجود نہیں ہیں۔

اس کے برعکس اگر مان لیا جائے کہ $\frac{R}{U}$ انتگرال دامنہ ہے تب ہمیں ثابت کرنا ہے کہ U مفرد آئڈیال ہے۔

اگر $a,b \in U$ تب $ab \in U$

تب $ab+U = U$

$\Rightarrow (a+U).(b+U) = U = 0+U$

$\Rightarrow a+U = U$

یا $b+U = U$ چوں کہ $\frac{R}{U}$ انتگرال دامنہ ہے جس میں صفر کے قاسم نہیں ہوتے

$\Rightarrow a \in U$ یا $b \in U$

لہٰذا U مفرد آئڈیال ہوا۔ قضیہ ثابت ہوا۔

قضیہ 12۔ صحیح اعداد کے رنگ Z میں کسی بھی مفرد عدد سے تخلیق پایا ہوا آئدیال عظیمی ہوتا ہے۔

ثبوت۔ فرض کرو کہ p ایک مفرد عدد ہے۔

تب $M = \langle p \rangle = \{ pn / n \in Z \}$ سے p تخلیق پایا ہوا آئدیال ہے۔

ہمیں ثابت کرنا ہے کہ M عظیمی آئدیال ہے۔ اگر ممکن ہو تو ہم فرض کریں گے کہ U آئدیال ہے اور $M \subset U \subset Z$ چوں کہ Z کا بر آئدیال مفرد ہوتا ہے۔

اس لیے فرض کرو کہ $U = \langle q \rangle$ جہاں q عدد ہے۔

$$\Rightarrow \langle p \rangle \subset \langle q \rangle \subset Z$$
$$\Rightarrow p \in \langle q \rangle$$
$$\Rightarrow p = qm \qquad m \in Z$$

چوں کہ p مفرد عدد ہے اس لیے $m = 1$ ہی ہو سکتا ہے۔

لہٰذا $p = q$

$$\Rightarrow \langle p \rangle = \langle q \rangle = M = U$$

یا $q = 1$ ہو تب $\langle q \rangle = Z = U$

لہٰذا ثابت ہوا کہ M عظیمی آئدیال ہے۔ قضیہ ثابت ہوا۔

نوٹ:۔ مرکب (غیر مفرد) عدد سے تخلیق پایا ہوا آئدیال عظیمی نہیں ہوگا۔

مثلاً:۔ $M = \langle 8 \rangle \{ \ldots\ldots\ldots\ldots -24, -16, -8, 0, 8, 16, 24 \ldots\ldots\ldots\ldots \}$

جب کہ $U = \langle 4 \rangle \{ \ldots\ldots\ldots\ldots -24, -20, -16, -12, -8, -4, 0, 4, 8 \ldots\ldots\ldots\ldots \}$

ہم دیکھتے ہیں کہ $M \subset U \subset Z$

چوں کہ $\langle 8 \rangle \subset \langle 4 \rangle \subset Z$

قضیہ 13۔ اگر M عظیمی آئدیال ہے صحیح اعداد کے رنگ Z کا تب M کسی مفرد عدد سے تخلیق پایا ہوا ہوگا۔

ثبوت:۔ فرض کرو کہ $M = \langle n \rangle \; n \in Z$ عظیمی آئدیال ہے Z کا تب ہمیں ثابت کرنا ہے کہ n مفرد عدد ہے۔ اگر ممکن سمجھا جائے تو n مفرد نہیں ہے۔

تب $n = ab$ جہاں a, b مفرد ہیں۔

تب $U = \langle a \rangle$ آئدیال ہوگا Z کا۔

اور $M \subset U \subset Z$

اب چوں کہ M عظیمی آئدیال ہے اس لیے $U = Z$ یا $M = U$ ہونا چاہئے۔

صورت(1)اگر $U = Z$

تب $U = \langle a \rangle = Z = \langle 1 \rangle$

$\Rightarrow a = 1$

تب $n = ab$

$\Rightarrow = 1.b$

$n = b$ مفرد عدد ہے۔

صورت(2):۔اگر $M = U$

تب $U = \langle a \rangle = M$

$\Rightarrow a \in M \Rightarrow a \in \langle n \rangle$

$\Rightarrow a = r\,n \;\; r \in Z$

$\therefore n = ab = (rn)b$

$= n(rb)$

$\Rightarrow r\,b = 1$

$\Rightarrow r = 1 \;\; \& \;\; b = 1$

$\therefore n = a(1) = a$ مفرد عدد ہے۔

لہٰذا ہر دو صورتوں میں n مفرد عدد ہی پایا گیا۔

لہٰذا $M = \langle n \rangle$ عظیمی آئڈیال مفرد عدد سے ہی تخلیق پایا ہے۔قضیہ ثابت ہوا۔

نوٹ:۔رنگ Z میں ہر آئڈیال جو مفرد عدد سے تخلیق پایا عظیمی ہو گا۔

قضیہ 14۔ایک تقلیبی رنگ معہ اکائی R کا آئڈیال U عظیمی ہو گا اگر اور صرف اگر خارج قسمت رنگ $\frac{R}{U}$ میدان ہو۔

ثبوت۔ دیا گیا ہے کہ R تقلیبی رنگ معہ اکائی ہے۔

اور U آئڈیال ہے R کا

تب $\frac{R}{U} = \{x + U / x \in R\}$ بھی تقلیبی رنگ معہ اکائی ہو گا۔ہم جانتے ہیں کہ $0 \in R$

اور $0 + U = U \in \frac{R}{U}$ صفر عنصر ہے $\frac{R}{U}$ کا۔

اور اگر $a + U = U$ ($\frac{R}{U}$ کا صفر عنصر)

$\Leftrightarrow a \in U$

فرض کرو کہ U عظیمی آئڈیال ہے R کا تب ہمیں ثابت کرنا ہو گا کہ $\frac{R}{U}$ میدان ہے۔ جس کے لیے یہ ثابت کرنا ہو گا کہ $\frac{R}{U}$ کے ہر غیر صفر عنصر کا ضربی معکوس $\frac{R}{U}$ میں موجود ہیں۔

فرض کرو کہ $x+U \in \frac{R}{U}$ غیر صفر عنصر ہے یعنی $x \notin U$

اگر $\langle x \rangle$ اصل آئڈیال ہے R کا تب $\langle x \rangle + U$ بھی R کا آئڈیال ہو گا۔

$$\because x \notin U \Rightarrow U \subset \langle x \rangle + U$$

اس لیے $U \subset \langle x \rangle + U \subseteq R$ اور U جیسا کہ فرض کیا گیا عظیمی آئڈیال ہے۔

$$\Rightarrow \langle x \rangle + U = R = \langle 1 \rangle$$

$$\Rightarrow \exists\ a \in U\ \&\ \alpha \in R\ s.t.\ a + x\alpha = 1$$

$$\therefore 1+U = (a + x\alpha) + U$$

$$= (a+U) + (x\alpha + U)$$

$$= U + (x\alpha + U) \qquad \because a \in U$$

$$= (0+U) + (x\alpha + U)$$

$$= (0 + x\alpha) + U$$

$$= x\alpha + U = (x+U)(\alpha + U)$$

یعنی کسی بھی غیر صفر عنصر $x+U \in \frac{R}{U}$ کے لیے ضربی معکوس $\alpha + U \in \frac{R}{U}$ موجود ہے۔ لہٰذا $\frac{R}{U}$ میدان ہوا۔

اس کے برعکس فرض کرو کہ $\frac{R}{U}$ میدان ہے تب ہمیں ثابت کرنا ہے کہ U عظیمی آئڈیال ہو گا۔ فرض کرو کہ U^1 بھی ایک آئڈیال ہے۔ R کا اس طرح کہ $U \subset U^1$ اور $U \neq U^1$

تب ہم ثابت کریں گے کہ $U^1 = R$ ہو گا۔ جس سے ثابت ہو گا کہ U عظیمی آئڈیال ہے۔

چوں کہ $U \subset U^1$ اور $U \neq U^1$ اس لیے

$$\exists\ \alpha U^1\ \&\ \alpha \notin U$$

$$U + \alpha \neq U \Rightarrow \text{یعنی غیر صفر عنصر ہے } \frac{R}{U} \text{ میں}$$

چوں کہ $\frac{R}{U}$ میدان ہے اسلیے ہر غیر صفر عنصر کا ضربی معکوس اُس میں موجود ہو گا۔

فرض کرو کہ $(\alpha + U)^{-1} = x + U \in \frac{R}{U}$

تب $(\alpha + U)(x+U) = 1 + U$

$$\Rightarrow \alpha x + U = 1 + U$$

$$\Rightarrow 1 - \alpha x \in U \subset U^1$$

$$\because x \in R \ \& \ \alpha \in U^1 \Rightarrow \alpha x \in U^1 \left[Ideal\right]$$

تب $\alpha x + \in U^1 \left(1 - \alpha x\right) \in U^1$

$$\Rightarrow 1 \in U^1$$

تب آئڈیال $U^1 = \langle 1 \rangle = R$

لہٰذا U عظیمی آئڈیال ہے۔ قضیہ ثابت ہوا۔

11.4 حل شدہ مثالیں (Solved Examples)

مثال 1۔ ثابت کرو کہ تحت $U = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} / \ a, b \in Z \right\}$ تحت رنگ ہوگا لیکن آئڈیال نہیں 2×2 ماترس کے رنگ کے لیے جس کے عناصر صحیح اعداد ہیں۔

حل۔ فرض کرو کہ $M = \left\{ \begin{bmatrix} a & c \\ d & b \end{bmatrix} / \ a, b, c, d \in Z \right\}$ رنگ ہے۔

جس کے لیے $U = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} / \ a, b \in Z \right\}$ تحت سیٹ ہے۔

ہم جانتے ہیں کہ ایک غیر خالی تحت سیٹ S کے کسی رنگ R کے لیے تحت رنگ ہونے کے لیے یہ کافی ہوگا کہ

$$\forall a, b \in S \Rightarrow a - b \in S \ (1)$$

$$\forall a, b \in S \Rightarrow ab \in S \ (2)$$

اس لیے فرض کرو کہ $\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}, \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \in U$

تب $\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & 0 \\ 0 & b_1 - b_2 \end{bmatrix} \in U$

پہلی شرط پوری ہوئی۔

اور $\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} . \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 + 0 & 0 + 0 \\ 0 + 0 & 0 + b_1 b_2 \end{bmatrix}$

$$\begin{bmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{bmatrix} \in U$$

دوسری شرط بھی پوری ہوئی۔ لہٰذا U تحت رنگ ہوا M کا۔

آئڈیال ہونے کی آزمائش یوں کریں گے۔

فرض کرو کہ $B=\begin{bmatrix} a_2 & c_2 \\ d_2 & b_2 \end{bmatrix} \in M$ اور $A=\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} \in U$

تب $$AB=\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}\begin{bmatrix} a_2 & c_2 \\ d_2 & b_2 \end{bmatrix}$$

$$=\begin{bmatrix} a_1a_2+0 & a_1c_2+0 \\ 0+b_1d_2 & 0+b_1b_2 \end{bmatrix} \notin U$$

لہٰذا U دایاں آئڈیال نہیں ہوا۔

اسی طرح $$BA=\begin{bmatrix} a_2 & c_2 \\ d_2 & b_2 \end{bmatrix}\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}$$

$$=\begin{bmatrix} a_2a_1+0 & 0+c_2b_1 \\ d_2a_1+0 & 0+b_2b_1 \end{bmatrix} \notin U$$

لہٰذا U بایاں آئڈیال بھی نہیں ہو سکا۔

اس لیے ثابت ہوا کہ U تحت رنگ ہے M کا لیکن آئڈیال نہیں ہے۔

مثال 2۔ ثابت کرو کہ $U=\left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a,b \in Z\right\}$ بایاں آئڈیال ہے لیکن دایاں آئڈیال نہیں ہے۔ 2×2 ماترسوں کے رنگ جس کے عناصر صحیح اعداد ہیں کے لیے۔

حل۔ فرض کرو کہ $M=\left\{\begin{bmatrix} a & c \\ b & d \end{bmatrix} / a,b,c,d \in Z\right\}$ رنگ ہے۔

اور $U=\left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a,b \in Z\right\}$ تحت سیٹ ہے۔

فرض کرو کہ $\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix},\begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} \in U$

تب $$\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}-\begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}=\begin{bmatrix} a_1-a_2 & 0 \\ b_1-b_2 & 0 \end{bmatrix} \in U$$

آئڈیال کی پہلی شرط پوری ہوئی۔

اور فرض کرو کہ $B=\begin{bmatrix} a & c \\ b & d \end{bmatrix} \in M$ اور $A=\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \in U$

تب غور کرو $$AB=\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}\begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

$$=\begin{bmatrix} a_1a & a_1c \\ b_1a & b_1c \end{bmatrix} \notin U$$

لہٰذا U دایاں آئڈیال نہیں ہے۔

$$BA = \begin{bmatrix} a & c \\ b & d \end{bmatrix}\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \qquad \text{اور}$$

$$= \begin{bmatrix} aa_1 + cb_1 & 0 \\ ba_1 + db_1 & 0 \end{bmatrix} \notin U$$

لہٰذا U بایاں آئڈیال ہے۔ثابت ہوا۔

مثال 3۔ ثابت کرو کہ تحت سیٹ $U = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / \, a,b \in Z \right\}$ رنگ $(M,+,\bullet)$ 2×2 ماتر سوں کا جس کے عناصر صحیح اعداد سے تخلیق پائے ہوں کے لیے دایاں آئڈیال ہے لیکن بایاں نہیں۔

حل: دیا گیا ہے کہ $M = \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} / \, a,b,c,d \in Z \right\}$ رنگ ہے۔

اور $U = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / \, a,b \in Z \right\}$ تحت سیٹ ہے۔

ثابت کرنا ہے کہ دایاں آئڈیال ہے لیکن بایاں نہیں رنگ کے لیے

فرض کرو کہ $A = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix},\ B = \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} \in U$

تب $A - B = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & 0 \end{bmatrix} \in U$

لہٰذا آئڈیال ہونے کی پہلی شرط پوری ہوئی۔

اور فرض کرو کہ $R = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$

تب غور کرو $AR = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$$= \begin{bmatrix} a_1a + b_1c & a_1b + b_1d \\ 0 & 0 \end{bmatrix} \in U$$

لہٰذا U دایاں آئڈیال ہوا M کے لیے

اور $RA = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}$

$$= \begin{bmatrix} aa_1 & ab_1 \\ ca_1 & db_1 \end{bmatrix} \in \notin U$$

لہٰذا U بایاں آئڈیال نہیں ہے۔ثابت ہوا۔

مثال 4۔ کیا منطقی اعداد کا سیٹ آئڈیال ہو گا حقیقی اعداد کے رنگ $(R,+,\bullet)$ کے لیے۔

حل:۔ دیا گیا ہے۔ کہ رنگ $(R,+,\bullet)$ حقیقی اعداد کا سیٹ ہے۔

اور Q منطقی اعداد کا سیٹ ہے۔

ظاہر ہے $Q=\left\{{}^{p}\!/\!_{q} / q\neq 0, p,q\in Z\right\}$ اور $Q\subset R$ ہوتا ہے۔

غور کرو کہ $x\in Q$ اور $r\in R$ ہو

تب $xr\notin Q$ کیوں کہ r حقیقی ہونے کی بناء غیر منطقی بھی ہو گا۔

تب xr غیر منطقی ہو گا جو Q میں موجود نہیں ہو گا۔

لہٰذا Q آئڈیال نہیں ہو گا R کے لیے۔

مثال 5۔ کوئی مثال پیش کرو جو تحت رنگ ہوتا ہے لیکن آئڈیال نہیں۔

حل۔ فرض کرو کہ رنگ $(R,+,\bullet)$ حقیقی اعداد کا رنگ ہے۔

اور $Q=\left\{{}^{p}\!/\!_{q} / q\neq 0, p,q\in Z\right\}$ منطقی اعداد کا سیٹ ہے۔

ظاہر $Q\subset R$ ہے

چوں کہ $(Q,+,\bullet)$ رنگ ہوتا ہے۔

اس لیے Q تحت رنگ ہو گا R کا

اور غور کرو کہ $\frac{2}{5}\in Q$ اور $\sqrt{2}\in R$

تب $\frac{2}{5}\sqrt{2}\notin Q$

لہٰذا Q آئڈیال نہیں ہو سکتا۔

لہٰذا Q مطلوبہ بہ مثال کے لیے کافی ہے۔

مثال 6۔ اگر U_1 اور U_2 دو آئڈیال ہیں رنگ کے تب ثابت کرو کہ $U_1+U_2=\{x+y / x\in U_1, y\in U_2\}$ بھی R کا آئڈیال ہو گا۔

حل۔ فرض کرو کہ $0\in R$ صفر عنصر ہے۔

تب چوں کہ $0\in U_1$ اور $0\in U_2$ اس لیے $0+0=0\in U_1+U_2$

لہٰذا U_1+U_2 غیر خالی تحت سیٹ ہے R کا

فرض کرو کہ $a,b\in U_1+U_2$ اور $r\in R$

تب فرض کرو کہ $a=x_1+y_1 \quad x_1\in U_1,\ y_1\in U_2$

$b=x_2+y_2 \quad x_2\in U_1,\ y_2\in U_2$

تب $a-b=(x_1+y_1)-(x_2+y_2)$

$$= (x_1 - y_1) + (x_2 - y_2) \quad x_2 - x_1, y_1 - y_2 \in U_2$$

$$\Rightarrow a - b \in U_1 + U_2$$

لہٰذا آئڈیال کی پہلی شرط پوری ہوئی $U_1 + U_2$ پر .....(1)

اور $ar = (x_1 + y_1)r$

$= x_1 r + y_1 r \qquad x_1 r \in U_1$ (U_1 آئڈیال ہونے کی بناء)

$y_1 r \in U_2$ اور (U_2 آئڈیال ہونے کی بناء)

$\Rightarrow a r \in U_1 + U_2$ .....(2)

اور اسی طرح $ra = r(x_1 + y_1)$

$= r x_1 + r y_1 \qquad r x_1 \in U_1$ (U_1 آئڈیال ہونے کی بناء)

$r y_1 \in U_2$ (U_2 آئڈیال ہونے کی بناء)

$\Rightarrow r a \in U_1 + U_2$ .....(3)

(1)(2)اور(3) کی بنیاد پر $U_1 + U_2$ آئڈیال ہے R کا۔ ثابت ہوا۔

مثال 7۔ اگر m متعینہ صحیح عدد ہو تب ثابت کرو کہ $U = \{mx / x \in Z\}$ آئڈیال ہوگا صحیح اعداد کے رنگ کا۔

حل۔ دیا گیا ہے $(Z, +, \bullet)$ رنگ ہے۔

اور $m \in Z$, $U = \{mx / x \in Z\}$ تحت سیٹ ہوگا Z کا۔

اگر $m_1 x, m_2 x \in U$ جہاں اور $x_1, x_2 \in Z$ متعینہ $x \in Z$

تب $mx_1 - mx_2 = m(x_1 - x_2) \in U$

اس لیے کہ $x_1 - x_2 \in Z$

لہٰذا آئڈیال کی پہلی شرط پوری ہوئی U پر .....(1)

اور اگر $r \in Z$

تب $(mx)r = m(xr) \in U$

چوں کہ $x, r \in Z$ اسلیے $xr \in Z$

لہٰذا U دایاں آئڈیال ہوا۔ .....(2)

اور $r(mx) = (rm)x$

$= (mr)x$ $\because Z$ تقلیبی ہوتا ہے۔

$$= m(rx)$$

$$\Rightarrow r\,x \in Z \quad r, x \in Z \because$$

لہٰذا U بایاں آئڈیال ہوا۔ .....(3)

(1)،(2)اور(3)کی بنیاد پر Z, U کا آئڈیال ثابت ہوا۔

مثال8۔ ذیل کے رنگوں کے عظیمی آئڈیال معلوم کرو۔

(1) Z_n (2) Z_{10} (3) Z_{12}

حل۔ (1)ہم جانتے ہیں کہ $Z_n = \{0,1,2,.....(n-1)\} \bmod n$

پہلی صورت:۔ اگر n مفرد عدد ہے تب Z_n کے کوئی غیر معمولی آئڈیال نہیں ہوں گے۔یعنی اس کے صرف دو آئڈیال $\{0\}$ اور Z_n ہوں گے۔

لہٰذا اس کے کوئی عظیمی آئڈیال نہیں ہوں گے۔

دوسری صورت:۔ اگر n مفرد عدد نہیں ہے۔تب Z_n کے غیر معمولی آئڈیال بھی ہوں گے۔اگر n کا قاسم ہے۔تب ان میں $\langle p \rangle$ تخلیق پائے ہوئے آئڈیال عظیمی آئڈیال ہوں گے اگر p مفرد ہے۔اور اگر p غیر مفرد ہے تب $\langle p \rangle$ آئڈیال عظیمی نہیں ہوں گے۔

(2) Z_{10}

$$Z_{10} = \{0,1,2,3,4,5,6,7,8,9\} \bmod 10$$

10 کے قاسم $\{1,2,5,10\}$ ہیں۔

لہٰذا تمام آئڈیال

$$\langle 1 \rangle = Z_{10}$$
$$\langle 2 \rangle = \{0,2,4,6,8\}$$
$$\langle 5 \rangle = \{0,5\}$$
$$\langle 10 \rangle = \{0\}$$

ہوں گے۔

ان میں $\langle 1 \rangle$ اور $\langle 10 \rangle$ معمولی آئڈیال ہیں جو عظیمی نہیں ہو سکتے۔اور باقی میں جو مفرد عدد سے تخلیق پائے ہیں وہ عظیمی ہوں گے۔لہٰذا $\langle 2 \rangle$ اور $\langle 5 \rangle$ دونوں عظیمی آئڈیال ہیں۔

(3) Z_{12}

$$Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$$

12 کے قاسم $\{1,2,3,4,6,12\}$ ہیں۔

لہٰذا تمام آئڈیال ممکنہ حسب ذیل ہیں۔

$$\langle 1\rangle = \{0,1,2,3,4,5,6,7,8,9,10,11\} = Z_{12}$$
$$\langle 2\rangle = \{0,2,4,6,8,10\}$$
$$\langle 3\rangle = \{0,3,6,9\}$$
$$\langle 4\rangle = \{0,4,8\}$$
$$\langle 6\rangle = \{0,8\}$$
$$\langle 12\rangle = \{0\}$$

اور $\langle 1\rangle$ معمولی $\langle 12\rangle$ آئڈیال ہیں جو عظیمی نہیں ہو سکتے۔

باقی میں جو مفرد عدد سے تخلیق شدہ ہیں وہ عظیمی ہوں گے۔

لہٰذا $\langle 2\rangle$ اور $\langle 3\rangle$ عظیمی آئڈیال ہیں Z_{12} کے۔

مثال 9۔ دیا گیا ہے کہ $M = \{0,4\}$ عظیمی آئڈیال ہے رنگ $R = \{0,2,4,6\}$ کے لیے ثابت کرو کہ M مفرد آئڈیال نہیں ہے۔

$\mod 8$ کے تحت

حل۔ رنگ $R = \{0,2,4,6\}$ ہے۔

اور $M = \{0,4\}$ عظیمی آئڈیال ہے۔

ہم دیکھتے ہیں کہ $2.6 = 12$

$$= 4 \pmod 8$$

$4 \in M$ مگر نہ ہی $2 \in M$ اور نا ہی $6 \in M$

لہٰذا M مفرد آئڈیال نہیں ہے۔ ثابت ہوا۔

11.5 اکتسابی نتائج (Learning Outcomes)

اس اکائی میں طلبا دایاں، بایاں آئڈیال اور آئڈیال کی تعریفات اور ان کی مثالوں کو سمجھ گئے ہوں گے۔ نیز طلبا ان آئڈیال کے نظریات اور خارج قسمت رنگ کے متعلق مسائل اور نظریات سے واقف ہو گئے ہوں گے۔

11.6 کلیدی الفاظ (Keywords)

خارج قسمت رنگ، اصل ایدیال، مفرد ایدیال، عظیمی ایدیال، واجبی ایدیال، میدان

11.7 نمونہ امتحانی سوالات (Model Examination Questions)

11.7.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. خارج قسمت رنگ کی تعریف کرو۔

2. اصل آئڈیل، مفرد آئڈیل اور عظیمی آئڈیل کی تعریف کرو۔

11.7.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. ثابت کرو کہ کسی بھی میدان کے واجبی آئڈیل نہیں ہوتے۔
2. ثابت کرو کہ اگر U ایک آئڈیل ہے رنگ معہ اکائی R کا اور اگر $1 \in U$ تب $U = R$ ہوگا۔
3. اگر $\frac{R}{U}$ خارج قسمت رنگ ہے تب ثابت کرو کہ
   a) اگر R تقلیبی ہے تب بھی $\frac{R}{U}$ تقلیبی ہوگا۔
   b) اگر R معہ اکائی ہے تب $\frac{R}{U}$ بھی معہ اکائی ہوگا۔
4. ثابت کرو کہ تحت سیٹ $U = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} / a,b \in Z \right\}$ 2×2 ماترس صحیح اعداد کے لیے تحت رنگ ہوگا لیکن آئڈیل نہیں ہو سکتا۔
5. ثابت کرو کہ $U = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a,b \in Z \right\}$ بایاں آئڈیل ہے لیکن دایاں نہیں 2×2 ماترسوں کے رنگ کے لیے جس کے عناصر صحیح اعداد ہیں۔
6. ذیل کے رنگوں کے عظیمی آئڈیل معلوم کرو۔
   (a) Z_n (b) Z_{12}

11.7.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. آئڈیل کی تعریف کرو اور ثابت کرو کہ کسی دو آئڈیل کا تقاطع بھی آئڈیل ہوتا ہے۔
2. ثابت کرو کہ اگر U_1 اور U_2 دو آئڈیل ہیں رنگ R کے تب ان کا اجماع $(U_1 \cup U_2)$ بھی آئڈیل ہوگا۔ اگر اور صرف اگر $U_1 \subset U_2$ یا $U_2 \subset U_1$ ہو۔
3. ثابت کرو کہ کوئی بھی میدان اصل آئڈیل رنگ ہوتا ہے۔
4. ثابت کرو کہ صحیح اعداد کا رنگ $(Z, +, \bullet)$ اصل آئڈیل رنگ ہوتا ہے۔
5. ثابت کرو کہ R اگر تقلیبی رنگ ہے اور $U \neq R$ آئڈیل ہے تب U مفرد آئڈیل ہوگا۔ اگر اور صرف اگر $\frac{R}{U}$ انتگرال دامنہ ہو۔
6. ثابت کرو کہ ایک تقلیبی رنگ مع اکائی R کا آئڈیل ع U ظیمی ہوگا اگر اور صرف اگر خارج قسمت رنگ $\frac{R}{U}$ میدان ہو۔
7. اگر R ایک تقلیبی رنگ ہے اور $a \in R$ تب ثابت کرو $Ra = \{ra / r \in R\}$ آئڈیل ہوگا۔

11.8 مزید مطالعے کے لیے تجویز کردہ کتابیں(Suggested Books for Further Reading)

1. Surjeet Singh and Qazi Zameeruddin, Modern Algebra Vikas Publishing House Pvt. Ltd.
2. I.N. Hestien: Topics in Algebra, Vikas Publishers.
3. A Text Book of B.Sc. Mathematics (Abstract Algebra) V.Venkateshwava Rao & 5 others, S. Chand & Co Ltd.
4. J.B. Fralengh : A First Convse in Abstract Algebra

اکائی 12۔ رنگوں کی ہم مارفیت، کرنل اور یک مارفیت

(Homomorphism of Rings, Kernel and Isomorphism)

اکائی کے اجزا

12.0 تمہید (Introduction)

دو رنگوں کے درمیان باہمی ربط (جس طرح دو گروپوں میں کیا گیا) ہم مارفیت کو معرف کیا جاتا ہے۔ چوں کہ رنگ میں دو شائی اعمال ہوتے ہیں۔ اس لیے ہم مارفیت ہونے کی دو شرطیں ہوں گی۔ کرنل ہم مارفیت کا ایدیال ہوتا ہے۔ ہم مارفیت کے علاوہ یک مارفیت بھی دیکھی جائے گی۔ ہم مارفیت کا بنیادی قضیہ اور متعلقہ قضیے زیر بحث رہیں گے۔

12.1 مقاصد (Objectives)

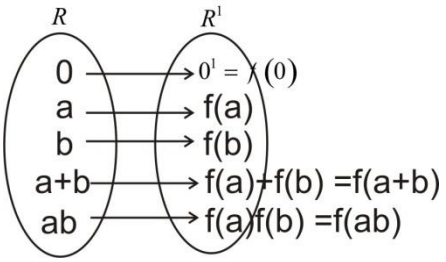
اس اکائی کے ختم پر طالب علم رنگوں کی ہم مارفیت، یک مارفیت، اپی مارفیت، مونو مارفیت کی تعریف کر پائیں گے۔ کرنل کیا ہوتا ہے اور ہم مارفیت کی مثالیں دینے کے قابل ہونگے۔ متعلقہ قضیئے اور مشقیں حل کرنے کے قابل ہو جائیں گے۔

12.2 تعریفات (Definitions)

ہم مارفیت: اگر R اور R^1 دو رنگ ہیں اور $\phi : R \to R^1$ ہم مارفیت کہلاتا ہے۔ اگر

$$(i)\ \phi(a+b) = \phi(a) + \phi(b)\ \forall a,b \in R$$
$$(ii)\ \phi(ab) = \phi(a).\ \phi(b)\ \forall a,b \in R$$

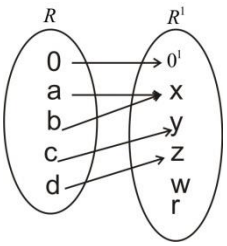
یعنی



نوٹ:۔ $0 \in R$ اور $0^1 \in R^1$ دونوں رنگوں میں صفر عناصر ہیں۔ ہم مارفیت میں '0' کا عکس ''0'' ہوتا ہے۔

ہم مارفک عکس:۔ اگر $\phi : R \to R^1$ ہم مارفیت ہے تب ہم مارفک عکس کا یہ ہوگا۔ $\phi(R) = \overline{R} = \{\phi(x) / x \in R\}$

مثلاً:۔



تب ہم مارفک عکس یہ ہوگا۔ $\phi(R)=\overline{R}=\{0^1,x,y,z\}$

w,r کسی کا عکس نہ ہونے کی وجہ شامل نہیں ہو سکے۔

نوٹ:۔ $\phi(R)=\overline{R}\subset R^1$ کبھی خالی نہیں ہوگا کیوں کہ کم از کم $0^1\in R^1$ عکس ضرور ہوگا۔'0'کا۔

اپی مارفیت/برمارفیت(Epimorphism)

اگر R اور R^1 دو رنگ ہیں اور نقش $\phi:R\to R^1$ ہم مارفیت جو کہ بر(onto) بھی ہے تب اس ہم مارفیت کو اپی مارفیت یا برمارفیت کہتے ہیں۔

نوٹ: Onto Homomorphism کی صورت میں $\overline{R}=Q(R)=R^1$

وحید مارفیت(Monomorphism):

اگر R اور R^1 دو رنگ ہیں اور نقش $\phi:R\to R^1$ ہم مارفیت ہے جو ایک ایک (1-1) بھی ہے تب اسکو وحید مارفیت کہتے ہیں۔

یک مارفیت(Isomorphism):

اگر R اور R^1 دو رنگ ہیں اور نقش $\phi:R\to R^1$ ایک ایک اور بر ہم مارفیت ہے تب اس کو یک مارفیت یا ایک ایک مارفیت(Isomorphism) کہتے ہیں۔

خود مارفیت(Automorphism):

اگر $(R,+,\bullet)$ ایک رنگ ہے اور نقش $\phi:R\to R$ ایک ایک اور بر ہم مافیت ہے تب یہ خود مارفیت(Automorphism) کہلاتا ہے۔

ترقیم(Notation):

اگر R اور R^1 کے بیچ ہم مارفیت ہے تب اسے $R\simeq R^1$ سے ظاہر کرتے ہیں اور اگر یک مارفیت ہے تب $R\cong R^1$ سے ظاہر کرتے ہیں۔

نوٹ1: اگر U رنگ R کا ایدیال ہے تب $\frac{R}{U}=\{x+U/x\in R\}$ بھی رنگ ہوتا ہے ہم سیٹس کے جمع وضرب کے تحت

نوٹ2: اگر U رنگ R کا ایدیال ہے تب $\frac{R}{U}=\{x+U/x\in R\}$ اور $\phi:R\to\frac{R}{U}$ اس طرح کہ $\phi(x)=x+U,\ \forall x\in R$ تب ϕ فطری ہم مارفیت کہلاتا ہے۔ R بر $\frac{R}{U}$ پر

نوٹ3: اگر R اور R^1 دو رنگ ہیں اور نقش $\phi: R \to R^1$ اس طرح سے کہ $\phi(x) = 0^1 \ \forall \ x \in R$ تب صفر ہم مارفیت (Identity Homomorphism) کہلاتا ہے۔

12.3 حل شدہ قضیے (Solved Theorems)

قضیہ 1۔ اگر R اور R^1 دو رنگ ہیں اور $\phi: R \to R^1$ ہم مارفیت ہے تب

$$(i)\phi(0) = 0^1 \quad (ii)\phi(-a) = -\phi(a) \forall \ a \in R \quad (iii)\phi(a-b) = \phi(a) - \phi(b) \forall \ a,b \in R$$

ثبوت۔ (i) $0 + R \Rightarrow 0 + 0 = 0$

$$\therefore \phi(0+0) = \phi(0)$$

(جمعی اکائی) $\Rightarrow \phi(0) + \phi(0) = \phi(0) + 0^1 \quad 0^1 \in R^1$

$\Rightarrow \phi(0) = 0^1$ تنسیخی کلیہ کی بناء

(ii) اگر $a \in R$ تب $-a \in R$ چوں کہ وہ جمعی معکوس ہے۔

تب $a + (-a) = 0$

$$\Rightarrow \phi(a + (-a)) = \phi(0)$$

$\phi(a) + \phi(-a) = 0^1$ ہم مارفیت کی بناء

$$\Rightarrow \phi(-a) = -\phi(a)$$

(iii) اگر $a,b \ x \in R$

تب $\phi(a-b) = \phi(a + (-b))$

$$= \phi(a) + \phi(-b)$$

$= \phi(a) - \phi(b)$ چوں کہ $\phi(-b) = \phi(b)$

قضیہ ثابت ہوا۔

نوٹ:۔ ہم مارفیت میں $\phi(0) = 0^1$ ہوگا لیکن $\phi(1) = 1^1$ ہونا ضروری نہیں ہاں اگر R اور R^1 انتگرال دامنہ ہیں تب $\phi(1) = 1^1$ ہوگا۔

قضیہ 2۔ اگر $Q: R \to R^1$ ہم مارفیت ہے تب $r \in R$ اور $n \in Z^+$ کے لیے

$\phi(nr) = n\phi(r), \ \phi(r^n) = [\phi(r)]^n$، ہوگا۔

ثبوت۔ دیا گیا ہے کہ $Q: R \to R^1$ ہم مارفیت ہے۔

تب $r \in R$ اور $n \in Z^+$ کے لیے

$$n.r \in R$$

$$\phi(n.r) = \phi(r + r + ...n\,times)$$ تب

$$= \phi(r) + \phi(r) + ...n\,times$$
$$= n\phi(r)$$

$$\phi(r^n) = \phi(r.r.r.....n\,times)$$ اور

$$= \phi(r).\phi(r) + ...n\,times$$
$$= [\phi(r)]^n$$

قضیہ ثابت ہوا۔

قضیہ 3۔ اگر $\phi: R \to R^1$ ہم مارفیت ہے اور S تحت رنگ ہے R کا تب $\phi(S) = \{\phi(x) / x \in S\}$ تحت رنگ ہوگا R^1 کا۔

ثبوت۔ دیا گیا ہے کہ R اور R^1

اور S تحت رنگ ہے کا R

اور $\phi: R \to R^1$ ہم مارفیت ہے۔

ثابت کرنا ہے کہ $\phi(S) = \{\phi(x) / x \in S\}$ تحت رنگ ہوگا۔ R^1

چوں کہ $0 \in R$ اسلیے $0 \in S$

$$\phi(0) = 0^1 \in \phi(S)$$ تب

لہذا $\phi(S) \neq \phi$ اور $\phi(S) \subseteq R^1$

$$\forall\, \phi(x), \phi(y) \in \phi(S)$$ اس لیے

$$\Rightarrow \exists\, x, y \subset S$$
$$\Rightarrow x - y \in S,\ x.y \in S$$
$$\Rightarrow \phi(x-y) \in \phi(S)\ \&\ \phi(x.y) \in \phi(S)$$

$$\phi(x-y) = \phi(x + (-y))$$ اور

$$\phi(x-y)=\phi\big(x+(-y)\big)$$
$$=\phi(x)+\phi(-y)$$
$$=\phi(x)-\phi(-y)\in\phi(S) \quad \text{.....(1)}$$

مزید $=\phi(x.y)=\phi(x).\phi(y)\in\phi(S)$ .....(2)

(1)اور(2)سے ثابت ہوتا ہے کہ $\phi(S)$ تحت رنگ ہے R^1 کا۔قضیہ ثابت ہوا۔

قضیہ 4۔ اگر $\phi: R\xrightarrow{onto} R^1$ ہم مارفیت ہے اور اگر S ایدیال ہے R کا تب $\phi(S)$ ایدیال ہوگا R^1 کا۔

ثبوت۔ دیا گیا ہے کہ $\phi: R\to R^1$ ہم مارفیت ہے۔

لہذا R اور R^1 رنگس ہیں۔

اور دیا گیا ہے کہ S ایدیال ہے R کا

ثابت کرنا ہے کہ ایدیال ہوگا R^1 کا۔

اینج سیٹ $\phi(S)=\{\phi(x)/\ x\in S\}$ تحت سیٹ ہوگا R^1 کا۔

اور $0\in R\Rightarrow 0\in S$

اور $\phi(0)=0^1\in\phi(S)$

چنانچہ $\phi(S)\neq\phi$

اور $\phi(S)\subseteq R^1$

$$\forall\phi(x),\phi(y)\in\phi(S)\Rightarrow\exists x,y\in S$$
$$\Rightarrow x-y\in S \ \ \&\ \ x.y\in S$$
$$\Rightarrow\phi(x-y)\in\phi(S)$$

تب
$$\Rightarrow\phi(x-y)=\phi\big(x+(-y)\big)$$
$$=\phi(x)+\phi(-y)$$
$$=\phi(x)-\phi(y)\in\phi(S) \quad \text{.....(1)}$$

فرض کرو کہ $r\in R$ اور $x\in S$

تب $rx, xr\in S$

اب اگر $r^1 \in R^1$ اور $x^1 \in \phi(S)$

تب $r^1 = \phi(r)\ r \in S$ اور $x^1 = \phi(x)\ x \in S$

غور کرو $r^1.x^1 = \phi(r).\phi(x)$

$$(2)..... = \phi(rx) \in \phi(s)$$

اسی طرح $x^1 r^1 = \phi(x).\phi(r)$

$$(3)..... = \phi(xr) \in \phi(S)$$

(1)،(2)اور(3)سے ثابت ہوا کہ $\phi(S)$ ایدیال ہے R^1 کا۔ قضیہ ثابت ہوا۔

قضیہ 5۔ اگر $\phi : R \to R^1$ ہم مارفیت ہے تب

(i) R رنگ کا ہم مارفک عکس رنگ ہوگا یعنی $\phi(R)$ رنگ ہوگا۔

(ii) تقلیبی رنگ R کا ہم مارفک عکس $\phi(R)$ تقلیبی رنگ ہوگا۔

ثبوت۔ (i) دیا گیا ہے کہ $\phi : R \to R^1$ ہم مارفیت ہے۔

R اور R^1 رنگس ہیں۔

R کا ہم مارفک عکس $\overline{R} = \phi(R) = \{\phi(x) \in R^1 / x \in R\}$

یہ ثابت کرنے کے لیے $\overline{R}$ رنگ ہے یہ ثابت کرنا کافی ہوگا کہ $\overline{R}$ تحت رنگ ہے R^1 کا

چوں کہ $0 \in R$ اسلیے $\phi(0) = 0^1 \in \overline{R} \subset R^1$

چوں کہ $0 \in R$ اس لیے $0 \in U_1,\ \ 0 \in U_2$ سارے ممیّز عناصر ہیں۔

$$\overline{R} \neq \phi \therefore$$

فرض کرو کہ $a^1, b^1 \phi(R) = \overline{R}$

تب $\exists a, b \in \phi$

$$s.t.\ \phi(a) = a^1\ \&\ \phi(b) = b^1$$
$$\because a, b \in R \Rightarrow a - b,\ ab \in R$$
$$\Rightarrow \phi(a-b), \phi(ab) \in \phi(R)$$

اب $a^1 - b^1 = \phi(a) - \phi(b)$

$$(1) \quad \ldots\ldots\ldots\ldots\ldots = \phi(a-b) \in \phi(R)$$

اور $a^1 . b^1 = \phi(a)\phi(b)$

$$(2)\ldots\ldots\ldots\ldots\ldots = \phi(ab) \in \phi(R)$$

(1)اور(2)سے ثابت ہے کہ تحت ر $\overline{R} = \phi(R)$ R^1 نگ ہے کا۔یعنی $\overline{R} = \phi(R)$ خود بھی رنگ ہے ثابت ہوا۔

(ii)دیا گیا ہے کہ R تقلیبی رنگ ہے۔

ثابت کرنا ہے کہ $\overline{R} = \phi(R)$ بھی تقلیبی رنگ ہوگا۔

رنگ ہونا(i)میں ثابت ہو چکا۔

تقلیبی خاصیت کو آزمایا جاتا ہے۔

دیا گیا ہے کہ $\forall a, b \in R$

$$\Rightarrow ab = ba$$

فرض کرو $\phi(b) = b^1, b^1 \in \overline{R}$ & $\phi(a) = a^1, a^1 \in \overline{R}$

تب $a^1 . b^1 = \phi(a)\phi(b)$

$$= \phi(ab)$$

$$= \phi(ba) \qquad \because R \text{ تقلیبی ہے۔}$$

$$= a^1\ b^1 \qquad \forall a^1\ b^1 \in \overline{R}$$

چنانچہ ثابت ہوا کہ اگر R تقلیبی رنگ ہے تب ہم مارفک عکس $\overline{R} = \phi(R)$ بھی تقلیبی رنگ ہوتا ہے۔

قضیہ ثابت ہوا۔

قضیہ 6۔ اگر نقش $\phi : R \to R^1$ یک مارفیت ہے تب

(i) R^1 انگرال دامنہ ہوگا R انگرال دامنہ ہو۔

(ii) R^1 میدان ہوگا اگر R میدان ہو۔

ثبوت۔ (i)**چوں کہ** $\phi(0) = 0^1$ جہاں '0' اور "0^1" بالترتیب اور کے صفر ہیں۔ R اور R^1 یک مارفیت کی بناء ϕ 1-1 ہوگا۔

اس لیے $0 \in R$ صرف ایک عنصر ہوگا جس کا عکس 0^1 ہوگا۔

فرض کرو کہ $a^1 \neq 0^1, b^1 \neq 0^1$ اور $a^1, b^1 \in R^1$

تب $\exists a, b \in R$ اور $a \neq 0 \quad b \neq 0$

اس طرح سے کہ $\phi(a) = a^1 \ , \ \phi(b) = b^1$

چوں کہ R انگرال دامنہ ہے اس لیے $ab \neq 0$ چوں کہ $a \neq 0 \quad b \neq 0$ ہے۔

$$\Rightarrow \phi(ab) = \phi(0)$$
$$\Rightarrow \phi(a)\phi(b) \neq 0^1$$
$$\Rightarrow a^1 b^1 \neq 0^1$$

یہاں نتیجہ نکلا کہ $a \neq 0 \ , \ b \neq 0$ ہونے پر $a^1 b^1 \neq 0^1$

چنانچہ R^1 میں صفر کے قاسم موجود نہیں ہے۔

R انگرال دامنہ ہونے کی وجہ سے اس میں اکائی موجود ہو گی $1 \in R$۔

تب $\phi(1) \in R^1$ فرض کرو کہ $\phi(1) = 1^1$

تب $$a^1.1^1 = \phi(a).\phi(1)$$
$$= \phi(a.1)$$
$$= a^1$$

یہاں معلوم ہوا کہ $1^1 \in R^1$ اکائی ہے۔ چنانچہ ثابت ہوا کہ R^1 انگرال دامنہ ہے۔

(ii) دیا گیا ہے R میدان ہو گا۔

R میدان ہونے کی وجہ سے

(1) R تقلیبی ہے بہ عمل ضرب

(2) R میں اکائی موجود ہے یعنی $1 \in R$

(3) R کے ہر غیر صفر عنصر کا ضربی معکوس R میں موجود ہے۔

ہم جانتے ہیں کہ R تقلیبی ہونے پر R^1 بھی تقلیبی ہوتا ہے۔ اور اگر $1 \in R$ تب $1^1 \in R^1$ ضربی اکائی موجود ہوتا ہے۔

اب صرف یہ ثابت کرنا کافی ہو گا کہ R^1 کے ہر غیر صفر عنصر کا ضربی معکوس R^1 میں موجود ہو گا۔ تب ثابت ہو جائے گا کہ R^1 بھی میدان ہے۔

فرض کرو کہ $a^1 \neq 0^1 \in R^1$

تب $\phi(a) = a^1 \neq 0^1$ اس طرح سے کہ $\exists\ a \in R$

$$\Rightarrow a \neq 0$$

تب $a^{-1} \in R$

تب $aa^{-1} = 1 = a^{-1}a$

$$\therefore \phi\left(aa^{-1}\right) = \phi(1) = \phi\left(a^{-1}a\right)$$
$$\Rightarrow \phi(a)\phi\left(a^{-1}\right) = 1^1 = \phi\left(a^{-1}\right)\phi(a)$$
$$\Rightarrow \left[\phi(a)\right]^{-1} = \phi\left(a^{-1}\right) \in R^1$$

ثابت ہوا کہ R^1 کے ہر غیر صفر عنصر کا ضربی معکوس R^1 میں موجود ہے۔ نتیجہ یہ نکلا کہ R^1 بھی میدان ہے۔

قضیہ ثابت ہوا۔

قضیہ 7۔ اگر $\phi : R \to R^1$ ہم مارفیت ہے اور اگر U^1 ایدیال ہے R^1 کا تب ایدیال ہوگا R کا۔

ثبوت۔ دیا گیا ہے کہ $\phi : R \to R^1$ ہم مارفیت ہے رنگ R سے رنگ R^1 پر اور $U^1 \subset R^1$ ایدیال ہے۔

ثابت کرنا ہے کہ $\phi\left(U^1\right) \subset R$ ایدیال ہوگا۔

فرض کرو کہ $U = \phi^{-1}(U) = \left\{x \in R / \phi(x) \in U^1\right\}$

$$\because \phi(0) = 0^1 \in U^1 \Rightarrow \phi^{-1}\left(U^1\right) = U \neq \phi \ \ \& \ U \subset R$$

فرض کرو کہ $a, b \in U$

$$\Rightarrow \phi(a), \phi(b) \in U^1$$

دیا گیا ہے کہ U^1 ایدیال ہے

$$\Rightarrow \phi(a), \phi(b) \in U^1$$

$$\Rightarrow \phi(a-b) \in U^1 \Rightarrow a - b\phi^{-1}\left(U^1\right) = U \qquad \text{(1).....}$$

اور اگر $a \in U,\ r \in U$

تب $\phi(a) \in U^1, \phi(r) \in R^1$

اور چوں کہ U^1 ایدیال ہے اس لیے $\phi(a)\ \phi(r) \in U^1$

اور $\phi(r)\ \phi(a) \in U^1$

$$(2)\ldots\ldots\ldots\ldots\qquad \Rightarrow \phi(ar)\,\phi(ra)\in U^1 \Rightarrow ar, ra\in U=\phi^{-1}\left(U^1\right)$$

(1)اور(2)سے ظاہر ہوتا ہے کہ $\phi^{-1}\left(U^1\right)$ ایدیال ہے رنگ R میں۔ قضیہ ثابت ہوا۔

رنگ ہم مارفیت کا کرنل(Kernel of Homomorphism Ring)

اگر R اور R^1 رنگ ہیں اور نقش $\phi: R\to R^1$ ہم مارفیت ہے تب سیٹ $K=\ker\phi=I(\phi)\left\{x\in R/\phi(x)=0^1\right\}$ کو ϕ کا کرنل کہا جاتا ہے۔

نوٹ:

1. $\ker\phi=\phi^{-1}\left(0^1\right)\subset R$
2. چوں کہ ہر ہم مارفیت میں $\phi(x)=0^1$ ہوتا ہے اس لیے کم از کم $0^1\in\ker\phi$ اس لیے $\phi\neq\ker\phi$ ہو گا۔
3. صفر ہم مارفیت میں چوں کہ $\phi(x)=0^1\ \forall\ x\in R$ ہوتا ہے اس لیے $\ker\phi\neq R$ ہو گا۔
4. اکائی ہم مارفیت میں چوں کہ $\phi(x)=x\forall\ x\in R$

یہی ہوتا ہے۔ $\Rightarrow\phi(0)=0^1$

$$\therefore \ker\phi=\{0\}$$

5. یک مارفیت میں نقش 1-1 ہونے کے بناء صرف $\phi(0)=0^1$ ہوتا ہے۔

$$\therefore \ker\phi=\{0\}$$

یہی ہوتا ہے۔

قضیہ 8۔ اگر $\phi: R\to R^1$ ہم مارفیت ہے تب $\ker\phi$ ایدیال ہو گا رنگ R کا۔

ثبوت۔ فرض کرو کہ $0\in R$ اور $0^1\in R^1$ رنگس کے صفر ہیں۔

ہم جانتے ہیں کہ کرنل $K=\ker\phi=\left\{x\in R/\phi(x)=0^1\right\}$

چوں کہ ہم مارفیت ϕ میں $\phi(0)=0^1\Rightarrow 0\in R$

$$\Rightarrow K\neq\phi$$

اور $K\subset R$

فرض کرو کہ $a,b\in K$

تب $f(a)=0^1, f(b)=0^1$

تب $\phi(a-b)=\phi(a)-\phi(b)$

$=0^1-0^1$

$=0^1$

$\Rightarrow a-b\in K$ .....(1)

اور اگر $r\in R$

تب $\phi(ar)=\phi(a)\phi(r)$

$=0^1\phi(r)$

$=0^1$

$\Rightarrow ar\in K$ .....(2)

اور $\phi(ra)=\phi(r)\phi(a)$

$=\phi(r)0^1$

$=0^1$

$\Rightarrow ra\in K$ .....(3)

(1)،(2)اور(3)سے معلوم ہوا کہ کرنل K ایدیال ہے رنگ R میں۔قضیہ ثابت ہوا۔

قضیہ 9۔ اگر R دو R^1 رنگ ہیں اور نقش $\phi: R\to R^1$ ہم مارفیت ہے تب ϕ 1-1 ہوگا یا یک مارفیت ہوگا اگر صرف اگر

$\ker\phi=\{0\}$

ثبوت۔ دیا گیا ہے $\phi: R\to R^1$ کہ ہم مارفیت ہے۔

ہم جانتے ہیں کہ $K=\ker\phi=\{x\in R/\phi(x)=0^1\}$

فرض کرو کہ ϕ نقش 1-1 ہے۔

تب ہمیں ثابت کرنا ہے کہ $\ker\phi=\{0\}$

فرض کرو کہ $a\in\ker\phi$

تب $\phi(a)=0^1$

چوں کہ $\phi(0)=0^1$

$\Rightarrow \phi(a) = \phi(0) \Rightarrow a = 0$ ϕ نقش 1-1 ہونے کے بناءپر

ثابت ہوا کہ صفر $\phi(0) = 0^1$

لہذا $\ker \phi = \{0\}$

اس کے بالعکس فرض کرو کہ $\ker \phi = \{0\}$

تب ہمیں ثابت کرنا ہوگا کہ ϕ 1-1 ہوگا۔

فرض کرو کہ $a, b \in R$

اور $\phi(a) = \phi(b)$

$$\Rightarrow \phi(a) - \phi(b) = 0^1$$
$$\Rightarrow (a - b) = 0^1$$
$$\Rightarrow a - b \in \ker \phi = \{0\}$$
$$\Rightarrow a - b = 0$$
$$\Rightarrow a = b$$

تب ثابت ہوا کہ ϕ 1-1 ہے۔ قضیہ ثابت ہوا۔

رنگ ہم مارفیت کا اساسی قضیہ (Fundamental Theorem of Ring Homomorphism)

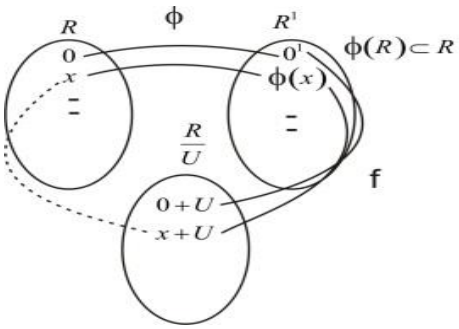
قضیہ 10۔ اگر اور R دو R^1 رنگ ہیں اور نقش $\phi : R \to R^1$ ہم مارفیت ہے اور $\ker \phi = U$ تب $\phi(R)$ (یعنی R کا ہم مارفی عکس) یک مارفی ہوتا ہے $\frac{R}{U}$ پر۔

ثبوت۔ دیا گیا ہے کہ $\phi : R \to R^1$ ہم مارفیت ہے۔

اور R, U کا ایدیال ہے

اور $\frac{R}{U} = \{x + U / x \in R\}$ خارج قسمت رنگ ہے۔

ثابت کرنا ہے کہ $\frac{R}{U} \cong \phi(R)$



کسی بھی $\phi(x) \in \phi(R)$

کی صورت میں $x \in R$

فرض کرو کہ $f : \frac{R}{U} = \phi(R)$

اس طرح سے کہ $f(x+U) = \phi(x) \ \forall \ x+U \in \frac{R}{U}$

تب اگر $a+U_1 b+U \in \frac{R}{U}$

اور اگر $a+U = b+U$

$$\Leftrightarrow a-b \in U$$

$\Leftrightarrow \phi(a-b) = 0^1$ چوں کہ کرنل ہے۔

$$\Leftrightarrow \phi(a-b) = 0^1$$
$$\Leftrightarrow \phi(a) - \phi(b) = 0^1 = \phi(0)$$
$$\Leftrightarrow \phi(ab) = \phi(b)$$
$$\Leftrightarrow f(a+U) = f(b+U)$$

اس سے ثابت ہوا کہ f خوش معرف ہے اور 1-1 بھی ہے۔

اب یہ ثابت کریں گے کہ f برتفاعل ہے۔

فرض کرو کہ $y \in \phi(R)$ تب $\exists\ x \in R$

تب چوں کہ $\phi(x) = y \ x \in R$

اور $x+U \in \frac{R}{U}$

اس طرح $y = \phi(x) = f(x+U)$

چنانچہ ہر $y \in \phi(R)$ کے لیے $x+U \in \frac{R}{U}$ اس طرح سے کہ $f(x+U)=y$

لہذا f برتفاعل ہے۔

اب آخر میں یہ ثابت کریں گے کہ f ہم مارفیت ہے۔

فرض کرو کہ $a+U_1 b+U \in \frac{R}{U}$ تب $a,b \in R$

پھر
$$f\left[(a+U)+(b+U)\right] = f\left((a+b)+U\right)$$
$$= \phi(a+b)$$
$$= \phi(a)+\phi(b)$$
$$= f(a+U)+f(b+U)$$

اور
$$f\left[(a+U).(b+U)\right] = f(ab+U)$$
$$= \phi(ab)$$
$$= \phi(a).\phi(b)$$
$$= f(a+U).f(b+U)$$

ثابت ہوا کہ f ہم مارفیت ہے۔

چوں کہ $f:\frac{R}{U}=\phi(R)$ 1-1 اور برہم مارفیت ہے۔

اس لیے f یک مارفیت ہے۔

یعنی $\frac{R}{U} \cong \phi(R)$

قضیہ ثابت ہوا۔

نوٹ:

1. رنگ کے ہم مارفی اساسی قضیہ کو یوں بھی بیان کیا جاسکتا ہے۔ کوئی بھی رنگ R کا ہم مارفی عکس یک مارفی ہوتا ہے R کے کسی خارج قسمت رنگ پر۔
2. اگر $\phi: R \xrightarrow{onto} R^1$ ہم مارفیت ہے اور U ایدیال ہے رنگ R کا تب $\frac{R}{U} \cong R^1$ چوں کہ اس صورت میں $R^1=\phi(R)$ (onto کی وجہ سے)

قضیہ 11۔ اگر U رنگ R کا ایدیال ہے تب $\frac{R}{U}$ رنگ R کا ہم مارفی عکس ہوتا ہے۔ (یا)

ہر خارج قسمت رنگ اُسکے رنگ کا ہم مارفی عکس ہوتا ہے۔

ثبوت۔ ہم جانتے ہیں کہ اگر R رنگ ہے اور U اُسکا ایدیال ہے تب

$\frac{R}{U} = \{x+U / x \in R\}$ خارج قسمت رنگ ہے۔

ثابت کرنا ہے کہ $R \simeq \frac{R}{U}$

فرض کرو کہ $\phi : R \to \frac{R}{U}$ جہاں $\phi(a) = a+U \quad \forall a \in R$

اگر $a, b \in R$

اور $a = b$

$$\Rightarrow a+U = b+U$$
$$\Rightarrow \phi(a) = \phi(a)$$

معلوم ہوا کہ ϕ خوش معرف ہے۔

اور
$$\phi(a+b) = (a+b)+U$$
$$= (a+U)+(b+U)$$
$$= \phi(a)+\phi(b)$$

اور
$$\phi(ab) = ab+U$$
$$= (a+U)+(b+U)$$
$$= \phi(a).\phi(b)$$

چوں کہ ϕ ہم مارفک ہے۔

اب اگر $x+U \in \frac{R}{U}$ تب $x \in R$ اسطرح سے کہ $\phi(x) = x+U$ معلوم ہوا کہ ϕ بر نقش ہے۔

چنانچہ ثابت ہوا کہ $\phi : R \xrightarrow{onto} \frac{R}{U}$ برمارفیت ہے۔

قضیہ ثابت ہوا۔

نوٹ:

1. $\ker \phi = \{x \in R / \phi(x) = 0+U\}$

$$= U$$

چنانچہ یادرہے کہ رنگ R کا ہر ایدیال کرنال ہوتا ہے R کے خارج قسمت کا۔

2. $\phi : R \to \frac{R}{U}$ کو فطری ہم مارفیت کہتے ہیں۔(Canonical or Natural Homomorphism)

قضیہ 12۔ اگر R رنگ ہے اور اسکا اکائی '1' ہے تب نقش $\phi : Z \to R$ معرف بہ $\phi(n) = n.1$ ہم مارفیت ہوگا۔

ثبوت۔ دیا گیا ہے کہ R رنگ ہے اور $1 \in R$ اکائی ہے۔

اور $\phi : Z \to R$

$$\phi(n) = n.1 \quad \forall n \in Z$$

تب اگر $m, n \in Z$

$$\Rightarrow \phi(m) = m.1$$
$$\phi(n) = n.1$$

تب $m+n \in Z$ اور $mn \in Z$

اور $$\phi(m+n) = (m+n).1$$

$$= m.1 + n.1$$

$$= \phi(m) + \phi(n) \qquad \text{.....(1)}$$

اور $$\phi(mn) = (mn).1$$

$$= (m.1).(n.1)$$

$$= \phi(m)\,\phi(n) \qquad \text{.....(2)}$$

(1) اور (2) سے ثابت ہوا کہ ϕ ہم مارفیت ہے۔ قضیہ ثابت ہوا۔

12.4 حل شدہ مشقیں (Solved Examples)

مثال 1۔ اگر R ایک تقلیبی رنگ ہے جسکا ممیّز $\{Cha(R) = 2\}$ 2 ہے تب نقش $\phi : R \to R$ معرف بہ $\phi(x) = x^2 \quad \forall x \in R$ ہم مارفیت ہوگا ثابت کرو۔

حل۔ دیا گیا ہے کہ R ایک تقلیبی رنگ ہے۔ اور $Cha(R) = 2$

$$\Rightarrow 2x = 0 \quad \forall x \in R$$

فرض کرو کہ $\phi : R \to R$ اور $\phi(x) = x^2 \ \forall x \in R$

تب اگر $x, y \in R$

$$\Rightarrow \phi(x) = x^2 \quad \phi(y) = y^2$$
$$\therefore x + y \in R \Rightarrow \phi(x+y) = (x+y)^2$$
$$= x^2 + 2xy + y^2$$
$$= x^2 + 0 + y^2 \quad \because cha(R) = 2$$
$$= x^2 + y^2$$
$$= \phi(x) + \phi(y) \quad \text{.....(1)}$$

اور چوں کہ $x, y \in R$

$$\Rightarrow \phi(xy) = (xy)^2$$
$$= x^2 y^2$$
$$= \phi(x)\phi(y) \quad \text{.....(2)}$$

(1)اور(2)سے معلوم ہوا کہ ϕ ہم ماریفیت ہے۔ چنانچہ ثابت ہوا۔

مثال2۔ اگر $Z(\sqrt{2}) = \{m + n\sqrt{2} / m, n \in Z\}$ رنگ ہے بہ عمل جمع و ضرب تب ثابت کرو کہ $\phi : Z(\sqrt{2}) \to Z(\sqrt{2})$ خود ماریفیت ہوگا معرف بہ $\phi(m + n\sqrt{2}) = m - n\sqrt{2} - \quad \forall m + n\sqrt{2} \in Z(\sqrt{2})$

کرنل بھی معلوم کرو۔

حل۔ دیا گیا ہے کہ $\phi(m + n\sqrt{2}) = m - n\sqrt{2}, \forall m + n\sqrt{2} \in Z(\sqrt{2})$

فرض کرو کہ $a = m_1 + n_1\sqrt{2}, \quad b = m_2 + n_2\sqrt{2} \in Z\sqrt{2}$

تب $a + b = (m_1 + m_2) + (n_1 + n_2)\sqrt{2}$

اور $a.b = (m_1 m_2 + 2n_1 n_2) + (m_1 n_2 + m_2 n_1)\sqrt{2}$

تب $\phi(a+b) = (m_1 + m_2) - (n_1 + n_2)\sqrt{2}$

اور $= (m_1 + n_1\sqrt{2}) - (m_2 + n_2\sqrt{2})$

$$= \phi(a) + \phi(b) \quad \text{.....(1)}$$

$$\phi(ab) = (m_1 m_2 + 2n_1 n_2) - (m_1 n_2 + m_2 n_1)\sqrt{2}$$

$$= \left(m_1 - n_1\sqrt{2}\right)\left(m_2 - n_2\sqrt{2}\right)$$

$$= \phi(a)\phi(b) \qquad \text{.....(2)}$$

ہم مارفیت ثابت ہوا۔

اب اگر $\phi(a) = \phi(b)$

$$\Rightarrow m_1 - n_1\sqrt{2} = m_2 - n_2\sqrt{2}$$
$$\Rightarrow m_1 = m_2 \ \& \ n_1 = n_2$$
$$\Rightarrow m_1 + n_1\sqrt{2} = m_2 + n_2\sqrt{2}$$
$$\Rightarrow a = b$$

معلوم ہوا کہ ϕ 1-1 ہے۔ .....(3)

اور اگر $y = m + n\sqrt{2} \in Z\left(\sqrt{2}\right)$ جو کہ Codomain میں ہے۔

تب $\exists\ x = m - n\sqrt{2} \in Z\left(\sqrt{2}\right)$ جو کہ Domain میں ہے۔

اس طرح کہ $\phi(x) = \phi\left(m - n\sqrt{2}\right)$

$$= \phi\left(m + (-n)\sqrt{2}\right)$$
$$= m - (-n)\sqrt{2}$$
$$= m + n\sqrt{2} = y$$

چنانچہ ϕ بر(onto) ہے۔ .....(4)

چوں کہ ϕ 1-1 اور برہم مارفیت ہے۔اس لیے ϕ یک مارفیت ہے۔

اور دونوں رنگ $Z\left(\sqrt{2}\right)$ ہی ہونے کی بناء خود مارفیت ہے۔ثابت ہوا۔

کرنل معلوم کرنے کے لیے

فرض کرو کہ $\phi\left(m + n\sqrt{2}\right) = 0$

$$\Rightarrow m - n\sqrt{2}$$
$$\Rightarrow m = 0 \ \& \ n = 0$$

لہذا صرف $\phi(0) = 0$ ہو گا۔

اس طرح کرنل کا سیٹ $\ker\phi = \{0\}$ ہو گا۔

مثال3۔اگر ملتف اعداد (Complex Number) کا رنگ ہے اور $M_2(R)$ 2×2 حقیقی اعداد والی ماترس کا رنگ ہے تب ثابت کرو کہ $\phi: C \to M_2(R)$ معرف بہ $\forall a+ib \in C$ $\phi(a+ib)=\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ وحیدمارفیت (1-1 Homomorphism) ہوتا ہے اس کا کرنل بھی معلوم کرو۔

حل۔ اگر $Z_1, Z_1 \in C$ اور $Z_1 = x_1 + iy_1$ $Z_2 = x_2 + iy_2$ جبکہ $x_1, y_1, x_2, y_2 \in R$

تب $$\phi(Z_1) = \phi(x_1 + iy_1)$$

$$= \begin{bmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{bmatrix}$$

اور $\phi(Z_2) = \phi(x_2 + iy_2) = \begin{bmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{bmatrix}$

تب $$\phi(Z_1 + Z_2) = \phi\left[(x_1 + iy_1) + (x_2 + iy_2)\right]$$

$$= \phi\left[(x_1 + x_2) + i(y_1 + y_2)\right]$$

$$= \begin{bmatrix} x_1 + x_2 & y_1 + y_2 \\ -(y_1 + y_2) & x_1 + x_2 \end{bmatrix}$$

$$= \begin{bmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{bmatrix} + \begin{bmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{bmatrix}$$

$$= \phi(Z_1) + \phi(Z_2) \quad \text{.....(1)}$$

اور $$\phi(Z_1.Z_2) = \phi\left[(x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1)\right]$$

$$= \begin{bmatrix} x_1x_2 - y_1y_2 & x_1y_2 + x_2y_1 \\ -(x_1y_2 + x_2y_1) & x_1x_2 - y_1y_2 \end{bmatrix}$$

$$= \begin{bmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{bmatrix}\begin{bmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{bmatrix}$$

$$= \phi(Z_1).\phi(Z_2) \quad \text{.....(2)}$$

(1) اور (2) سے ظاہر ہے کہ ϕ ہم مارفیت ہے۔

(2) اب مان لو اگر $\phi(Z_1) = \phi(Z_2)$

$$\Rightarrow \begin{bmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{bmatrix} = \begin{bmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{bmatrix}$$

$$\Rightarrow x_1 = x_2 \quad \text{اور} \quad y_1 = y_2$$

$$\text{لہذا} \quad x_1 + iy_1 = x_2 + iy_2$$

$$\Rightarrow Z_1 = Z_2 \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

چنانچہ ϕ 1-1 ہوا۔

اب (1) (2) اور (3) کی بناء ϕ وحید ہم مارفیت ہوا۔

اب اسکا کرنل معلوم کرنے کے لیے

$$\text{اگر} \quad \phi(Z_1) = \phi(x_1 + iy_1) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\text{یعنی} \quad \begin{bmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

تب $x_1 = 0$ اور $y_1 = 0$ ہی ہونا ہے۔

لہذا $Z_1 = 0 + i0 \in C$ ہوا۔

یعنی $\ker \phi = \{0\}$

مثال 4۔ اگر R صحیح اعداد کا رنگ ہے اور R^1 جفت صحیح اعداد کا رنگ ہے اور عمل ضرب $a \forall b = \frac{ab}{2} \ \forall a, b \in R^1$ ، $\phi : R \to R^1$

اس طرح کہ $\phi(x) = 2x \forall x \in R$ تب ثابت کرو کہ ϕ یک مارفیت ہے۔

حل۔ دیا گیا ہے کہ R صحیح اعداد کا رنگ ہے۔ اور $R^1 = \{2n / n \in Z\}$

اور اس کا عمل ضرب یوں ہے $a \forall b = \frac{ab}{2} \ \forall a, b \in R^1$

اور $\phi : R \to R^1$

جہاں $\phi(x) = 2x \forall x \in R$

فرض کرو کہ $x_1, x_2 \in R$

تب $\phi(x_1) = 2x_1, \quad \phi(x_2) = 2x_2$

اور $\phi(x_1 + x_2) = 2(x_1 + x_2)$

$= 2x_1 + 2x_2$

اور $= \phi(x_1) + \phi(x_2)$ .....(1)

اور $\phi(x_1.x_2) = 2(x_1 . x_2)$

$= \frac{2x_1 . 2x_2}{2}$

اور $= 2x_1 \times 2x_2$

$= \phi(x_1) \times \phi(x_2)$ .....(2)

اور اگر $\phi(x_1) = \phi(x_2)$

$\Rightarrow 2x_1 = 2x_2$

$\Rightarrow x_1 = x_2$

$\Rightarrow$ ϕ 1-1 ہے۔ .....(3)

اور اگر $b \in R^1$ تب b جفت صحیح عدد ہونے کی بناء $a \in R$ اس طرح سے کہ $b = 2a$

اور $\phi(a) = 2a = b$

لہذا بر ϕ نقش (onto) ہوا۔ .....(4)

(1) (2) (3) اور (4) کی بنا ϕ یک مارفیت ہوا۔

مثال 5۔ اگر R حقیقی اعداد کا رنگ ہے اور $\phi : R \to R$ جہاں $\phi(x) = 2x \forall x \in R$ تب کیا ϕ ہم مارفیت ہو گا؟

حل۔ دیا گیا ہے کہ R حقیقی اعداد کا رنگ ہے بہ عمل جمع و ضرب اور نقش ہے۔ $\phi : R \to R$

جہاں $\phi(x) = 2x \forall x \in R$ ہم مارفیت کی شرائط آزمائیں۔

فرض کرو کہ $x_1, x_2 \in R$

تب $\phi(x_1) = 2x_1$ اور $\phi(x_2) = 2x_2$

اور $\phi(x_1 + x_2) = 2(x_1 + x_2)$

$= 2x_1 + 2x_2$

$= \phi(x_1) + \phi(x_2)$

پہلی شرط صادق ہے۔

دوسری شرط $\phi(x_1x_2) = 2(x_1x_2)$

$= 2x_1.x_2$

$\neq 2x_1.2x_2$

یعنی $\neq \phi(x_1) + \phi(x_2)$

دوسری شرط پوری نہیں ہوئی۔ لہذا ϕ ہم ماریفیت نہیں ہے۔

مثال 6۔ اگر $R = \{a + ib / a, b \in Z\}$ گاسین صحیح اعداد کا رنگ ہے اور Z صحیح اعداد کا رنگ ہے تب معلوم کرو کہ کیا $\phi : R \to Z$ معرف بہ $\phi(a + ib) = a$ ہم ماریفیت ہو گا؟

حل۔ دیا گیا ہے کہ گاسین صحیح اعداد کا رنگ $R = \{a + ib / a, b \in Z\}$ ہے۔

اور Z صحیح اعداد کا رنگ ہے۔

اور نقش $\phi : R \to Z$

معرف بہ $\phi(a + ib) = a \ \forall a + ib \in R$ ہے۔

ہم ماریفیت کی پہلی شرط کی آزمائش

فرض کرو کہ $a_1 + ib_1 \ , \ a_2 + ib_2 \in R$ تب $\phi(a_1 + ib_1) = a_1 \ ، \phi(a_{12} + ib_2) = a_2$

تب $\phi\left[(a_1 + ib_1) + (a_2 + ib_2)\right] = \phi\left[(a_1 + a_2) + i(b_1 + b_2)\right]$

$= (a_1 + a_2) = a_1 + a_2$

$= (a_1 + ib_1) + (a_2 + ib_2)$ .....(1)

پہلی شرط پوری ہوئی۔

دوسری شرط کی آزمائش۔

$$\phi\left[(a_1 + ib_1).(a_2 + ib_2)\right] = \phi\left[(a_1a_2 - b_1 + b_2) + i(a_1b_2 + b_1a_2)\right]$$
$$= a_1a_2 - b_1b_2$$
$$\neq a_1a_2$$
$$\neq \phi(a_1 + ib_1).\ \phi(a_2 + ib_2)$$

یعنی دوسری شرط پوری نہیں ہوئی۔ .....(2)

لہذا ϕ ہم مارفیت نہیں ہے۔

مثال 7۔ کیا رنگ $2Z$ یک مارفک ہے رنگ $3Z$ سے؟

حل۔ فرض کرو کہ $\phi: 2Z \to 3Z$

بہ معرف $\phi(2x) = 3x \ \forall x \in Z$

$$2Z = \{2x / x \in Z\}$$

اور $$3Z = \{3x / x \in Z\}$$

تب اگر $x_1, x_2 \in Z$

تب $\phi(2x_1) = 3x_1$ اور $\phi(2x_2) = 3x_2$

غور کرو $\phi(2x_1 + 2x_2) = \phi(2(x_1 + x_2))$

$$= 3(x_1 + x_2)$$
$$= 3x_1 + 3x_2$$
$$= \phi(2x_1) + \phi(2x_2)$$

ہم مارفیت کی پہلی شرط یوں دیکھیں۔

$$\phi(2x_1.2x_2) = \phi(2(x_1.x_2))$$
$$= 3(2x_1 2x_2)$$
$$\neq 3x_1.3x_2$$

یعنی $\neq \phi(2x_1).\phi(2x_2)$

دوسری شرط پوری نہیں ہوئی۔ لہذا ϕ ہم مارفیت نہیں ہے۔ تو پھر یک مارفیت ہونے کا سوال ہی پیدا نہیں ہوتا۔

مثال 8۔ ثابت کرو کہ نقش $\phi: M_2(Z) \to Z$ معرف بہ $\forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(Z)$ $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a$ رنگ ہم مارفیت نہیں ہے۔

حل۔ فرض کرو کہ $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in M_2(Z)$

تب $$\phi\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\right) = a_1$$

اور $\phi\left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) = a_2$ ہو گا۔

$$= a_1 + a_2$$

$$= \phi\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\right) + \phi\left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right)$$

ہم مارفیت کی پہلی شرط پوری ہوئی۔

اب دوسری شرط کی آزمائش کریں۔

$$\phi\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}.\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}\right)$$

$$= a_1a_2 + b_1c_2$$

$$\neq a_1a_2$$

یعنی $\neq \phi\left(\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}\right).\phi\left(\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}\right)$

دوسری شرط پوری نہیں ہوئی۔

لہذا ϕ ہم مارفیت نہیں ہے۔

مثال 9۔ ثابت کرو کہ نقش $\phi : Z[i] \to Z[i]$ معرف بہ $\forall\ m - in \in Z[i],\ m, n \in Z$ $\phi(m + in) = m - in$ گاسین صحیح اعداد رنگس پر خود مارفیت ہے۔

حل۔ ہم جانتے ہیں کہ $Z[i] = \{m + in / m, n \in Z\}$ گاسین صحیح اعداد کا رنگ ہے۔

فرض کرو کہ $m_1 + in_1, m_2 + in_2 \in Z[i]$

تب $\phi(m_1 + in_1) = m_1 - in_1$ اور $\phi(m_2 + in_2) = m_2 - in_2$

پھر $\phi\left[(m_1 + in_1) + (m_2 + in_2)\right] = \phi\left[(m_1 + m_2) + i(n_1 + n_2)\right]$

$$= (m_1 + m_2) - i(n_1 + n_2)$$

$$= (m_1 + in_1) + (m_2 + in_2)$$

$$= \phi(m_1 + in_1) + \phi(m_2 + in_2) \quad \text{.....(1)}$$

ہم مارفیت کی پہلی شرط پوری ہوئی۔

اور $\phi\left[(m_1+in_1).(m_2+in_2)\right]=\phi\left[(m_1m_2-n_1n_2)+i(m_1n_2+n_1m_2)\right]$

$$=(m_1m_2-n_1n_2)-i(m_1n_2+n_1m_2)$$
$$=(m_1-in_1)(m_2-in_2)$$

$$=\phi\left[(m_1+in_1)\right]\phi\left[(m_2+in_2)\right] \quad \text{.....(2)}$$

ہم مارفیت کی دوسری شرط بھی پوری ہوئی۔ لہذا ϕ ہم مارفیت ہوا۔

اوراب غور کریں اگر $\phi(m_1+in_1)=\phi(m_2+in_2)$

$$\Rightarrow m_1-in_1=m_2-in_2$$
$$\Rightarrow m_1=m_2 \quad \& \quad n_1=n_2$$

لہذا $m_1+in_1=m_2+in_2$

چنانچہ ϕ ایک ایک (1-1) ہوا۔

اور اگر $a+ib\in Z[i]$ ہو جو ہم دامنہ میں ہے۔

تب $\exists\ a-ib\in Z[i]$

اس طرح کہ $\phi(a-ib)=\phi\left(a+i(-b)\right)$

$$=a-i(-b)$$
$$=a+ib$$

لہذا ϕ بر (onto) ہوا۔

چوں کہ ϕ 1-1 اور برہم مارفیت ہے $Z[i]$ سے خود $Z[i]$ پر اسلیے ϕ خود مارفیت ثابت ہوا۔

مثال 10۔ ثابت کرو کہ ایک رنگ ہم مارفیت میں آیڈ مپوٹنٹ عنصر کا عکس بھی آیڈ مپوٹنٹ ہوتا ہے۔

حل:۔ فرض کرو کہ R ایک رنگ ہے اور R^1 دوسرا رنگ ہے۔

اور فرض کرو کہ $\phi: R\to R^1$ ہم مارفیت ہے۔

اگر 'a' آیڈ مپوٹنٹ عنصر ہے تب $a=a^2$ ہو گا۔ (Idempotent)

فرض کرو کہ $a\in R$ تب $\phi(a)\in R^1$

غور کرو $\left[\phi(a)\right]^2=\phi(a).\phi(a)$

$$= a.a$$
$$= a^2$$
$$= a$$
$$= \phi(a)$$

چنانچہ بھی آیڈ مپوٹنٹ (Idempotent) عنصر پایا گیا۔

12.5 اکتسابی نتائج (Learning Outcomes)

اس اکائی میں طلبا نے رنگ ہم مارفیت اس کے کرنل اور یک مارفیت کی تعریفات، چند مثالیں ان سے متعلق نظریات کے بارے میں جانکاری حاصل کی ہو گی۔

12.6 کلیدی الفاظ (Keywords)

برمارفیت، وحید مارفیت، یک مارفیت، خود مارفیت، ترقیم، ہم مارفیت، مارفک عکس، رنگ ہم مارفیت

12.7 نمونہ امتحانی سوالات (Model Examination Questions)

12.7.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. رنگ کے ہم مارفیت کی ایک مثال دو۔
2. رنگ کی ہم مارفی عکس رنگ ہوتی ہے۔ (صحیح/غلط)
3. ذیل کا کون سا الجبرائک اسٹرکچر رنگ نہیں ہو گا

A $(\mathbb{R}, +, .)$ B $(\mathbb{Q}, +, .)$ C $(\mathbb{Z}, +, .)$ D $(\mathbb{N}, +, .)$

12.7.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. ثابت کرو کہ اگر $\phi : R \xrightarrow{onto} R^1$ ہم مارفیت ہے اور اگر S ایدیال ہے تب $\phi(S)$ ایدیال ہو گا R^1 کا۔
2. ثابت کرو کہ ہر خارج قسمت رنگ اُسکے رنگ کا ہم مارفی عکس ہوتا ہے۔
3. اگر R ایک تقلیبی رنگ ہے جس کا ممیّز 2 ہے۔ تب نقش $\phi : R \to R$ معرف بہ $\forall x \in R \quad \phi(x) = x^2$ ہم مارفیت ہو گا۔ ثابت کرو۔
4. اگر R صحیح اعداد کا رنگ ہے اور R^1 جفت صحیح اعداد کا رنگ ہے اور عمل ضرب $a \times b = \frac{ab}{2} \quad \forall a, b \in R^1$

$\phi : R \to R^1$ جہاں $\forall x \in R \quad \phi(x) = 2x$ تب ثابت کرو کہ ϕ یک مارفیت ہے۔

5. کیا رنگ $2Z$ یک مارفک ہے رنگ $3Z$ سے۔

6. ثابت کرو کہ ایک رنگ ہم مارفیت میں آیڈ مپوٹنٹ (Idempotent) عنصر کا عکس بھی آیڈ مپوٹنٹ ہوتا ہے۔

12.7.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. اگر $\phi: R \to R^1$ ہم مارفیت ہے تب ثابت کرو۔

$$(i)\ \phi(0)=0 \quad (ii)\phi(-a)=-\phi(a) \quad (iii)\phi(a-b)=\phi(a)-\phi(b) \quad \forall a,b \in R$$

2. اگر $\phi: R \to R^1$ ہم مارفیت ہے تب ثابت کرو کہ

(i) R رنگ کا ہم مارفک عکس رنگ ہوگا یعنی $\phi(R)$ رنگ ہوگا۔

(ii) تقلیبی رنگ R کا ہم مارفک عکس $\phi(R)$ بھی تقلیبی رنگ ہوگا۔

3. اگر نقش $\phi: R \to R^1$ یک مارفیت ہے تب ثابت کرو کہ

(i) R^1 انگرال دامنہ ہوگا اگر R انگرال دامنہ ہو۔

(ii) R^1 میدان ہوگا اگر R میدان ہو۔

4. رنگ ہم مارفیت کا کرنل کی تعریف کرو اور ثابت کرو کہ اگر $\phi: R \to R^1$ ہم مارفیت ہے تب $\ker\phi$ ایدیال ہوگا رنگ R کا۔

5. اگر R اور R^1 دو رنگ ہیں اور نقش $\phi: R \to R^1$ ہم مارفیت ہے تب ϕ 1-1 ہوگا۔ یا یک مارفیت ہوگا اگر اور صرف اگر $\ker\phi=\{0\}$۔ ثابت کرو۔

6. رنگ ہم مارفیت کا اساسی قضیہ بیان اور ثابت کرو۔

7. ثابت کرو کہ نقش $\phi: Z[i] \to Z[i]$ معرف بہ $\phi(m+in)=m-in \ \forall\ m+in \in Z[i]$ گاسین صحیح اعداد رنگ پر خود مارفیت ہے۔

8. اگر C ملتف اعداد (Complex Numbers) کا رنگ ہے اور $M_2(R)$ 2×2 حقیقی اعداد والی ماترس کا رنگ ہے تب ثابت کرو کہ $\phi: C \to M_2(R)$ معرف بہ $\phi(a+ib)=\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\ \forall a+ib \in C$ وحید مارفیت ہوتا ہے۔ اسکا کرنل بھی معلوم کرو۔

12.8 مزید مطالعے کے لیے تجویز کردہ کتابیں (Suggested Books for Further Reading)

1. I.N. Hestien: Topics in Algebra, Vikas Publishers.
2. A Text Book of B.Sc. Mathematics (Abstract Algebra) V.VenkateshwavaRao& 5 others, S. Chand & Co Ltd.
3. Surjeet Singh ٔQaziZameeruddin, Modern Algebra Vikas Publishing House Pvt. Ltd.

اکائی 13۔ کثیر رکنی رنگ

(Polynomial Rings)

اکائی کے اجزا

13.0 تمہید(Introduction)

پچھلے درجوں میں آپ نے غیر متعین متغیر میں صحیح، ناطق اور حقیقی ضریب کے ساتھ کثیر رکنی عبارات کے بارے میں پڑھا ہوگا جیسے $8x^3 - 3x^2 - 3x + 1,\ y^2 - 2y + 5$ وغیرہ متعین متغیر t، y اور x میں کثیر رکنی ہیں۔ اس اکائی میں ہم کسی رنگ (Ring) اور پھر کسی میدان (Field) پر کثیر رکنی رنگ کے بارے تفصیل کے ساتھ پڑھیں گے نیز بہت سے قضیوں کو ثابت اور مثالوں کو حل کریں گے۔

13.1 مقاصد(Objectives)

اس اکائی کے مکمل ہونے کے بعد آپ اس قابل ہو جائیں گے کہ:

1. کثیر رکنی رنگ کی بنیادی جانکاری سے متعرف ہو سکیں۔
2. کسی رنگ اور میدان پر کثیر رکنی رنگ کو سمجھ سکیں۔
3. کثیر رکنی رنگ سے وابستہ قضیوں کو بیان اور ثابت کر سکیں۔

13.2 کثیر رکنی رنگ(Polynomial Ring)

13.2.1 بنیادی معلومات(Basic Information)

رنگ پر کثیر رکنی(Polynomial over Ring)

فرض کرو کہ R کوئی رنگ ہے۔ رنگ R پر کثیر رکنی سے مراد متعین متغیر (Indeterminate Variable) x میں ایسی عبارت ہے جو درجہ ذیل شکل میں ہو

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$$

جہاں $a_0, a_1, a_2, \cdots$ رنگ R کے عناصر (Elements) ہیں اور ان میں سے متناہی تعداد $a_i, i \in \mathbb{Z}^+$ (Finite Number) صفر کے مساوی ہیں۔ $a_0, a_1x, a_2x^2, \cdots$ کثیر رکنی کے ارکان (*Terms*) ہیں۔ پہلا عنصر a_0 کثیر رکنی کا مستقل عنصر کہلاتا ہے۔ اگر m سب سے بڑا غیر منفی صحیح عدد (Non-negative Integer) اس طرح سے وجود رکھتا ہو کہ $a_m \neq 0$، تب a_mx^m کو کثیر رکنی کا اولی رکن اور a_m کو کثیر رکنی کا اولی ضریب (Leading Coefficient) کہتے ہیں۔ اگر کثیر رکنی کا اولی ضریب $a_m = 1$ ہو تب اس کثیر رکنی کو وہدی کثیر رکنی (Monic Polynomial) کہتے ہیں۔ اگر تمام $a_0, a_1, a_2, \cdots$ صفر ہوں تب کثیر رکنی کو زیرو کثیر رکنی (Zero Polynomial) کہتے ہے۔ یعنی

$$O(x) = 0 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^n + \cdots$$

فرض کرو کہ $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$ کسی اختیاری رنگ R پر ایک کثیر رکنی ہے۔ تب f درجہ n کا کثیر رکنی کہلایے گا اگر اور صرف اگر $a_n \neq 0$ اور $a_m = 0, \forall m > n$

اگر $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$ اور $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m + \cdots$

رنگ R پر دو کثیر رکنی ہیں اور اگر $m = n$ اور $a_i = b_i, \forall i \in \mathbb{Z}^+$ تب $f(x)$ اور $g(x)$ مساوی ہوں گے۔ یعنی $f(x) = g(x)$

ان کے لیے جمع کا عمل درجہ ذیل طریقہ پر ہوتا ہے

$$\begin{aligned} f(x) + g(x) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_k + b_k)x^k + \cdots \\ &= c_0 + c_1x + c_3x^2 + \cdots + c_kx^k + \cdots \end{aligned}$$

جہاں $c_k = a_k + b_k, \forall k \in \mathbb{Z}^+$

اور ضرب کا عمل

$$\begin{aligned} f(x)g(x) &= (a_0 + a_1x + a_2x^2 + \cdots)(b_0 + b_1x + b_2x^2 + \cdots) \\ &= a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_0b_2 + a_1b_1)x^2 + \cdots \\ &= d_0 + d_1x + d_3x^2 + \cdots \end{aligned}$$

جہاں $d_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_1b_{k-1} + a_0b_k, \forall k \in \mathbb{Z}^+$

مثلاً اگر $f(x) = -4x^3 + 3x^2 + 5x + 2$ اور $g(x) = 5x^4 - x^3 + 4x + 3$ تب

$$\begin{aligned} f(x) + g(x) &= (2 + 3)x^0 + (5 + 4)x^1 + (3 + 0)x^2 + (-4 - 1)x^3 + (0 + 5)x^4 \\ &= 5x^0 + 9x^1 + 3x^2 - 5x^3 + 5x^4 \end{aligned}$$

اور

$$\begin{aligned} f(x)g(x) &= (-4x^3 + 3x^2 + 5x + 2)(5x^4 - x^3 + 4x + 3) \\ &= 6 + (15 + 8)x + (9 + 20)x^2 + (-4 - 1)x^3 + (-12 + 12 - 2)x^4 \\ &\quad +(25 - 3)x^5 + (15 + 4)x^6 - 20x^7 \\ &= 6 + 23x + 29x^2 - 2x^3 - 11x^4 + 22x^5 + 19x^6 - 20x^7 \end{aligned}$$

رنگ پر کثیر رکنی رنگ (Ring Polynomial over Ring)

فرض کرو کہ R ایک اختیاری رنگ ہے اور x ایک متعین متغیر ہے۔ تب تمام کثیر رکنیوں کا سٹ

$$\mathrm{R}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n / a_i \in R, i \in \mathbb{Z}^+\}$$

رنگ پر کثیر رکنی وں کا سٹ کہلاتا ہے۔

فرض کرو کہ R پر تمام کثیر رکنیوں کا سٹ $\mathrm{R}[x]$ ہے۔ تب $\mathrm{R}[x]$ ایک غیر خالی سٹ ہے اور مندرجہ بالا ذکر کیے گئے جمع اور ضرب کے عمل سے $\mathrm{R}[x]$ ایک رنگ بنے گا جسے ہم کثیر رکنیوں کا رنگ کہتے ہیں۔ ساتھ ہی ہم جانتے ہیں کہ زیرو کثیر رکنی $O(x) \in \mathrm{R}[x]$ جمع کے عمل کے تحت اکائی ہے۔

کسی کثیر رکنی $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$ کا جمع کے عمل کے تحت معکوس

$-f(x) = -a_0 - a_1x - a_2x^2 + \cdots + (-a_n)x^n + \cdots$ ایک کثیر رکنی ہوگا۔ اسی طرح چوں کہ $1 \in \mathrm{R}$ اکائی ہے، تب کثیر رکنی $I(x) = 1 + 0x + 0x^2 + \cdots + 0x^n + \cdots \in \mathrm{R}[x]$ ایک اکائی ہوگی۔ اگر ہم رنگ کی جگہ کسی میدان (Field) کو لیں تب کثیر رکنی کا میدان کے متناظر (Corresponding) رنگ $\mathrm{F}[x]$ حاصل ہوتا ہے۔

فرض کرو کہ رنگ R پر کثیر رکنی رنگ R[x] ہے اور $f: R \to \mathrm{R}[x]$ اس طرح سے ہے کہ $f(a) = a + 0x + 0x^2 + \cdots$ جس سے صاف ظاہر ہوتا ہے کہ f ایک تا ایک ہم ماریفت (One-One Homomorphism) رکھتا ہے۔ ساتھ ہی

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

اور

$$f(ab) = f(a)f(b)$$

اس لیے R کثیر رکنی رنگ R[x] کے کسی تحت رنگ پر یک ماریفت (Isomorphism) رکھتا ہے۔ اس لیے ہم R کو R[x] کا تحت رنگ بھی کہہ سکتے ہیں۔ اس سے ہمیں درجہ ذیل قضیہ ثابت کرنا آسان ہو جاتا ہے۔

قضیہ 1۔ فرض کرو کہ R[x] کسی رنگ R پر کثیر رکنی رنگ ہے، تب ثابت کرو کہ R تقلیبی ہوگا اگر اور صرف اگر R[x] تقلیبی ہو۔

ثبوت۔ اگر R[x] تقلیبی ہے تب اس کا کوئی بھی تحت رنگ بھی تقلیبی ہوگا۔ اب چوں کہ ہم جانتے ہیں کہ R کثیر رکنی رنگ R[x] کے تحت رنگ کے یکمار فی ہوتا ہے۔ اس لیے یہ تقلیبی ہوگا۔

اس کے برعکس فرض کرو کہ R تقلیبی ہے اور

$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$ اور $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m + \cdots$

کثیر رکنی رنگ R[x] کے دو عناصر ہیں، تب

$$\begin{aligned} f(x)g(x) &= (a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots)(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m + \cdots) \\ &= a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_0b_2 + a_1b_1)x^2 + \cdots \\ &= b_0a_0 + (b_0a_1 + b_1a_0)x + (b_0a_2 + b_2a_0 + b_1a_1)x^2 + \cdots \\ &= (b_0 + b_1x + b_2x^2 + \cdots + b_mx^m + \cdots)(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots) \\ &= g(x)f(x) \end{aligned}$$

اس لیے یہ ثابت ہوا کہ R[x] تقلیبی ہے۔

قضیہ 2۔ فرض کرو کہ R[x] کسی رنگ R پر کثیر رکنیوں کا سٹ ہے، تب ثابت کرو کہ R[x] بالحاظ کثیر رکنیوں کے جمع اور ضرب پر ایک رنگ ہوتا ہے۔

ثبوت۔

G_1: ثنائی موضوع (Closure axiom): فرض کرو کہ $f(x)$ اور $g(x)$ کثیر رکنی رنگ R[x] کے دو عناصر ہیں، ہمیں معلوم ہے کہ دو کثیر رکنیوں کا ضرب اور جمع سے حاصل بھی ایک کثیر رکنی ہوتا ہے اس لیے $f(x) + g(x) \in \mathrm{R}[x]$ اور $f(x)g(x) \in \mathrm{R}[x]$ جس سے ہم کہہ سکتے ہیں کہ R[x] کثیر رکنیوں کے جمع اور ضرب کے عمل کے تحت ثنائی موضوع کی تکمیل کرتا ہے۔

G_2: تلازمتی موضوع (Associative axiom): فرض کرو کہ کثیر رکنی رنگ R[x] کے تین عناصر

$f(x) = a_0 + a_1x + a_2x^2 + \cdots$, $g(x) = b_0 + b_1x + b_2x^2 + \cdots$ اور $h(x) = c_0 + c_1x + c_2x^2 + \cdots$ ہیں، تب جمع کے عمل کے لیے تلازمیت

$$\begin{aligned}\big(f(x)+g(x)\big)+h(x) &= (a_0+b_0)+c_0+(a_1+b_1)x+c_1x+(a_2+b_2)x^2+c_2x^2+\cdots\\ &= [(a_0+b_0)+c_0]+[(a_1+b_1)+c_1]x+[(a_2+b_2)+c_2]x^2+\cdots\\ &= [a_0+(b_0+c_0)]+[a_1+(b_1+c_1)]x+[a_2+(b_2+c_2)]x^2+\cdots\\ &= a_0+(b_0+c_0)+a_1x+(b_1+c_1)x+a_2x^2+(b_2+c_2)x^2+\cdots\\ &= f(x)+\big(g(x)+h(x)\big)\end{aligned}$$

اب ضرب کے عمل کے لیے تلازمیت کی جانچ کرتے ہیں

$$\begin{aligned}[f(x)g(x)]h(x) &= [(a_0+a_1x+a_2x^2+\cdots)(b_0+b_1x+b_2x^2+\cdots)](c_0+c_1x+c_2x^2+\cdots)\\ &= [a_0b_0+(a_1b_0+a_0b_1)x+(a_2b_0+a_0b_2+a_1b_1)x^2+\cdots](c_0+c_1x+c_2x^2+\cdots)\\ &= (d_0+d_1x+d_2x^2+\cdots+d_lx^l+\cdots)(c_0+c_1x+c_2x^2+\cdots+c_mx^m+\cdots)\end{aligned}$$

جہاں $d_l=\sum_{l=n+k}a_nb_k$

$$\begin{aligned}[f(x)g(x)]h(x) &= e_0+e_1x+e_2x^2+\cdots+e_ix^i+\cdots\\ &= \sum_{l+m=i}d_lc_m=\sum_{l+m=i}\left(\sum_{n+k=l}a_nb_k\right)c_m=\sum_{m+n+k=i}a_nb_kc_m\end{aligned}$$

اسی طرح ہم ثابت کر سکتے ہیں کہ

$$f(x)[g(x)h(x)]=\sum_{m+n+k=i}a_nb_kc_m$$

G_3: جمعی اکائی کا وجود(Existence of Additive Identity): فرض کرو کہ $O(x)=0+0x+0x^2+\cdots$ کثیر رکنی رنگ $R[x]$ کا ایک عنصر ہے، تب

$$\begin{aligned}f(x)+O(x) &= (a_0+a_1x+a_2x^2+\cdots)+(0+0x+0x^2+\cdots)\\ &= (a_0+0)+(a_1+0)x+(a_2+0)x^2+\cdots\\ &= a_0+a_1x+a_2x^2+\cdots\\ &= f(x)\end{aligned}$$

اس لیے صفر کثیر رکنی جمعی اکائی ہے۔

G_4: جمعی معکوس کا وجود(Existence of Additive Inverse): فرض کرو کہ $f(x)=a_0+a_1x+a_2x^2+\cdots$ کثیر رکنی رنگ $R[x]$ کا ایک عنصر ہے اور تب $-f(x)=-a_0-a_1x-a_2x^2-\cdots$ بھی اسکا ایک عنصر ہو گا، تب

$$\begin{aligned}-f(x)+f(x) &= (-a_0-a_1x-a_2x^2-\cdots)+(a_0+a_1x+a_2x^2+\cdots)\\ &= (-a_0+a_0)+(-a_1+a_1)x+(-a_2+a_2)x^2+\cdots\\ &= 0+0x+0x^2+\cdots\\ &= O(x)\in R[x]\end{aligned}$$

اس سے ہم کہہ سکتے ہیں کہ $R[x]$ کا ہر ایک عنصر اپنا ایک معکوس رکھتا ہے۔

بالحاظ جمع ضرب کی تقسیم پزیری(Distributivity of Multiplication with Respect to Addition)

ہم جانتے ہیں کہ

$$
\begin{aligned}
f(x)[g(x)+h(x)] &= (a_0+a_1x+a_2x^2+\cdots)[(b_0+b_1x+b_2x^2+\cdots)+(c_0+c_1x+c_2x^2+\cdots)] \\
&= (a_0+a_1x+a_2x^2+\cdots)[(b_0+c_0)+(b_1+c_1)x+\cdots+(b_n+c_n)x^n+\cdots] \\
&= [a_0(b_0+c_0)]+[a_0(b_1+c_1)+a_1(b_0+c_0)]x+\cdots \\
&= [(a_0b_0+a_0c_0)]+[(a_0b_1+a_0c_1)x+(a_1b_0+a_1c_0)x]+\cdots \\
&= [a_0b_0+(a_0b_1+a_1b_0)x+\cdots]+[a_0c_0+(a_0c_1+a_1c_0)x+\cdots] \\
&= f(x)g(x)+f(x)h(x)
\end{aligned}
$$

اسی طرح

$$
\begin{aligned}
[f(x)+g(x)]h(x) &= [(a_0+a_1x+a_2x^2+\cdots)+(b_0+b_1x+b_2x^2+\cdots)](c_0+c_1x+c_2x^2+\cdots) \\
&= [(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+c_2x^2+\cdots](c_0+c_1x+c_2x^2+\cdots) \\
&= [(a_0+b_0)c_0+[(a_1+b_1)c_0+(a_0+b_0)c_1]x+\cdots] \\
&= [(a_0c_0+b_0c_0)]+[(a_1c_0+b_1c_0)x+(a_0c_1+b_0c_1)x]+\cdots \\
&= [a_0c_0+(a_1c_0+a_0c_1)x+\cdots]+[b_0c_0+(b_1c_0+b_0c_1)x+\cdots] \\
&= f(x)h(x)+g(x)h(x)
\end{aligned}
$$

تقلیبی خاصیت(Commutative Properties): فرض کرو کہ کثیر رکنی رنگ $\mathrm{R}[x]$ کے دو عناصر

$f(x)=a_0+a_1x+a_2x^2+\cdots \quad , g(x)=b_0+b_1x+b_2x^2+\cdots$ ہیں، تب جمع کے عمل کے لیے

$$
\begin{aligned}
f(x)+g(x) &= (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+\cdots+(a_k+b_k)x^k+\cdots \\
&= (b_0+a_0)+(b_1+a_1)x+(b_2+a_2)x^2+\cdots+(b_k+a_k)x^k+\cdots \\
&= g(x)+f(x)
\end{aligned}
$$

جس سے تقلیبی خاصیت پوری ہوئی۔

اب چوں رنگ کی تمام خصوصیات کو کثیر رکنیوں کا سٹ مطمئن کرتا ہے اس لیے ثابت ہوا کہ $\mathrm{R}[x]$ بالحاظ کثیر رکنیوں کے جمع اور ضرب پر ایک رنگ ہے۔

قضیہ 3۔ اگر R کوئی اختیاری رنگ ہے اور R^I کثیر رکنی رنگ $\mathrm{R}[x]$ میں مستقل کثیر رکنیوں کا سٹ ہے۔ تب ثابت کرو کہ R^I رنگ R پر یک مارفیت رکھتا ہے۔

ثبوت۔ دیا ہے کہ R^I کثیر رکنی رنگ $\mathrm{R}[x]$ میں مستقل کثیر رکنیوں کا سٹ ہے۔ اس لیے فرض کرو کہ $\mathrm{R}^I = a+0x+0x^2+\cdots$ اس طرح کہ $a \in R$

اب فرض کرو کہ نقش(Map) $f: R \to \mathrm{R}^I$ اس طرح سے متعرف ہے کہ

$$f(a)=a+0x+0x^2+\cdots, \forall a \in R$$

اب چوں کہ $f(a)=f(b)$ اس لیے

$$
\begin{aligned}
a+0x+0x^2+\cdots &= b+0x+0x^2+\cdots \\
\Rightarrow \quad a &= b
\end{aligned}
$$

اس لیے f ایک تا ایک ہے۔ ساتھ ہی ظاہر ہے کہ f بر(Onto) تفاعل بھی ہوگا۔ اب

$$f(a+b) = (a+b) + 0x + 0x^2 + \cdots$$
$$= (a + 0x + 0x^2 + \cdots) + (b + 0x + 0x^2 + \cdots)$$
$$= f(a) + f(b)$$

اور

$$f(ab) = (ab) + 0x + 0x^2 + \cdots$$
$$= (a + 0x + 0x^2 + \cdots)(b + 0x + 0x^2 + \cdots)$$
$$= f(a)f(b)$$

اس لیے f یک مارفیت(Isomorphism) رکھتا ہے۔اس طرح $R \cong \mathrm{R}^I$

قضیہ(Theorem)4: اگر $\mathrm{R}[x]$ کسی رنگ R پر کثیر رکنی رنگ ہو اور فرض کرو کہ اس کی دو غیر صفری کثیر رکنیاں

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m, a_m \neq 0$$

اور $$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n, b_n \neq 0$$

ہیں،تب ثابت کرو:

a) اگر $f(x) + g(x) \neq 0$ تب $deg[f(x) + g(x)] \leq max(m,n)$

b) اگر $f(x)g(x) \neq 0$ تب $deg[f(x)g(x)] \leq m + n$

c) اگر R ایک انتگرل دامنہ ہو تو $deg[f(x)g(x)] = m + n$

d) R ایک انتگرل دامنہ ہوگا اگر اور صرف اگر $\mathrm{R}[x]$ انتگرل دامنہ ہو۔

e) اگر F ایک میدان ہے تو $F[x]$ میدان نہیں ہوگا۔

ثبوت۔ (a) دیے گیے کثیر رکنیوں سے ہمیں حاصل ہے

$$\deg f(x) = m, \deg g(x) = n$$

ساتھ ہی اگر $f(x) + g(x) \neq 0$ تب ہمارے سامنے تین صورتیں پیش آتی ہیں۔

پہلی صورت میں اگر $m \neq n$ تب $deg[f(x) + g(x)] = max(m,n)$

دوسری صورت میں اگر $m = n$ اور $a_m + b_n \neq 0$ تب $deg[f(x) + g(x)] = m$

تیسری صورت میں اگر $m = n$ اور $a_m + b_n = 0$ تب $deg[f(x) + g(x)] < max(m,n)$

اس لیے ثابت ہوا کہ $deg[f(x) + g(x)] \leq max(m,n)$

(b) فرض کرو کہ $f(x)g(x) \neq 0$ اور

$$f(x)g(x) = (a_0 + a_1x + a_2x^2 + \cdots + a_mx^m + \cdots)(b_0 + b_1x + b_2x^2 + \cdots + b_nx^n + \cdots)$$
$$= a_0b_0 + (a_1b_0 + a_0b_1)x + (a_2b_0 + a_0b_2 + a_1b_1)x^2 + \cdots + a_mb_nx^{m+n}$$

اس سے ہم کہہ سکتے ہیں کہ $f(x)g(x)$ کا درجہ(Degree) یکتا ہوگا۔

اگر $a_mb_n \neq 0$،تب

$$deg[f(x)g(x)] = m + n$$

اور اگر $a_m b_n = 0$، تب

$$deg[f(x)g(x)] < m + n$$

اس طرح ثابت ہوا کہ $deg[f(x)g(x)] \leq m + n$

(c) فرض کرو کہ R ایک انتگرل دامنہ ہے اور $R[x]$ کے دو غیر صفری کثیر رکنی $f(x)$ اور $g(x)$ ہیں۔ اب چوں کہ $a_m \neq 0$ اور $b_n \neq 0$ اس لیے

$$deg[f(x)g(x)] = m + n$$

(d) اگر $R[x]$ انتگرل دامنہ ہو اور کیوں کہ R کثیر رکنی رنگ $R[x]$ کے کسی تحت رنگ کے ساتھ یک مارفیت رکھتا ہے، اس لیے R بھی انتگرل دامنہ ہو گا۔

اس کے بالعکس فرض کرو کہ R ایک انتگرل دامنہ ہے۔ اب مان لو کہ $f(x)$ اور $g(x)$ کثیر رکنی رنگ کے دو غیر صفری عناصر اس طرح سے ہیں کہ

$$f(x)g(x) = 0$$

اب چوں کہ $a_0 \neq 0$ اور $b_0 \neq 0$ اس لیے جس سے $a_0 b_0 \neq 0$ اس لیے $f(x)$ اور $g(x)$ مستقل کثیر رکنی نہیں ہو سکتے۔ اب ہم کہہ سکتے ہیں کہ

$$f(x)g(x) \neq 0$$

چوں کہ $f(x)$ اور $g(x)$ میں سے کم از کم ایک مستقل کثیر رکنی ہے، اس لیے

$$deg[f(x)g(x)] \geq 1$$

اب R کے انتگرل دامنہ ہونے کی وجہ سے

$$deg[f(x)g(x)] = m + n \geq 1$$

جس سے تضاد ظاہر ہوتا ہے چوں کہ اس سے $f(x)g(x) = 0$ جب کہ $a_i b_i \neq 0, i > 0$

یہ تبھی ممکن ہے جب $f(x) = 0$ یا $g(x) = 0$ اس لیے $R[x]$ ایک انتگرل دامنہ ہے۔

(e) یہ ثابت کرنے کے لیے کہ $F[x]$ میدان نہیں ہے ہمیں ثابت کرنا ہو گا کہ $F[x]$ میں ایک غیر صفری عنصر وجود رکھتا ہے جس کا کوئی ضربی معکوس نہیں ہے۔ فرض کرو کہ $f(x) \in F[x]$ اس طرح سے ہے کہ

$$degf(x) > 0$$

چوں کہ

$$f(x)O(x) = O(x) \neq I(x)$$

جہاں $I(x) = 1 + 0x + 0x^2 + \cdots$

اس لیے $f(x)$ کا معکوس $O(x)$ نہیں ہو سکتا ہے۔

اب فرض کرو کہ $g(x)$ کوئی غیر صفری کثیر رکنی ہے۔ F کے میدان ہونے وجہ سے ہمیں حاصل ہے

$$deg[f(x)g(x)] = m + n > 0 \qquad [\because m > 0 \ \& \ n \geq 0]$$

اس لیے $F[x]$ کے اکائی عنصر کا درجہ صفر ہے۔اس لیے $I(x) \in F[x]$ کے لیے

$$f(x)g(x) \neq I(x)$$

اس سے ہم کہہ سکتے ہیں کہ $f(x)$ کا ضربی معکوس وجود نہیں رکھتا ہے۔اس لیے $F[x]$ میدان نہیں ہے۔

نوٹ: صفر کثیر رکنی کو چھوڑ کر سبھی مستقل کثیر رکنیوں کا معکوس حاصل کیا جاسکتا ہے۔

تعریف: فرض کرو کہ R ایک انتگرل دامنہ ہے۔تب R پر n متغیرات $x_1, x_2, \cdots, x_n$ میں کثیر رکنیوں کا رنگ درجہ ذیل طریقہ سے متعرف ہوتا ہے

$$R_1 = R[x_1]$$
$$R_2 = R_1[x_2]$$
$$R_3 = R_2[x_3]$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$R_n = R_{n-1}[x_n]$$

تب R_n کو R پر متغیرات $x_1, x_2, \cdots, x_n$ میں کثیر رکنیوں کا رنگ کہتے ہیں اور اس کو $R_n = R[x_1, x_2, \cdots, x_n]$ سے ظاہر کرتے ہیں۔

قضیہ 5۔ اگر R ایک انتگرل دامنہ ہو، تو $R[x_1, x_2, \cdots, x_n]$ بھی انتگرل دامنہ ہوگا۔

ثبوت۔ دیا ہے کہ R ایک انتگرل دامنہ ہے تب $R_1 = R[x_1]$ بھی انتگرل دامنہ ہوگا۔اسی طرح سے چوں کہ اب R_1 ایک انتگرل دامنہ ہے، تب $R_2 = R_1\left[x_1, x_2\right]$ بھی انتگرل دامنہ ہوگا۔اور پھر اسی طرح ظاہر ہے کہ $R_3 = R_2[x_1, x_2, x_3]$، $R_4 = R_3[x_1, x_2, x_3, x_4]$، .....، $R_n = R_{n-1}[x_1, x_2, \cdots, x_n]$ کو بھی انتگرل دامنہ ثابت کر سکتے ہیں۔

اس لیے ثابت ہوا کہ اگر R ایک انتگرل دامنہ ہو، تو $R[x_1, x_2, \cdots, x_n]$ بھی انتگرل دامنہ ہوگا۔

قضیہ 6۔ اگر F ایک میدان ہو، تو $F[x_1, x_2, \cdots, x_n]$ ایک انتگرل دامنہ ہوتا ہے۔

ثبوت۔ فرض کرو کہ اگر F ایک میدان ہے تب $F_1 = F[x_1]$ بھی انتگرل دامنہ ہوگا۔اسی طرح سے چوں کہ اب F_1 ایک انتگرل دامنہ ہے، تب $F_2 = F_1\left[x_1, x_2\right]$ بھی انتگرل دامنہ ہوگا۔ اسی طرح $F_3 = F_2[x_1, x_2, x_3]$، $F_4 = F_3[x_1, x_2, x_3, x_4]$، .....، $F_n = F_{n-1}[x_1, x_2, \cdots, x_n]$ کو بھی من درجہ بالا طرز پر انتگرل دامنہ ثابت کر سکتے ہیں۔

اس لیے ثابت ہوا کہ اگر F ایک میدان ہے، تو $F[x_1, x_2, \cdots, x_n]$ ایک انتگرل دامنہ ہوگا۔

تعریف۔ انتگرل دامنہ کے ذریعہ بنے کوشینٹ میدان کو $x_1, x_2, \cdots, x_n$ میں F پر ریشنل تفاعلات کا میدان کہتے ہیں۔اس کو $F[x_1, x_2, \cdots, x_n]$ سے ظاہر کرتے ہیں۔یہ میدان الجبرائک جیومتری میں اہم کردار ادا کرتا ہے۔

تعریف۔اگر $f, g \in F[x]$ دو کثیر رکنی ہیں، تب f اور g کو تلازمی کہتے ہیں اگر $f(x) = cg(x)$ جب کہ c میدان F کا ایک غیر صفری عنصر ہے۔

تعریف۔ $F[x]$ کے اس عنصر کو اکائی کہا جاتا ہے جس کا کوئی ضربی معکوس وجود رکھتا ہو۔

تعریف۔ اگر $f \in F[x]$ تب f ہمیشہ اپنی تلازمیت کے ذریعے تقسیم پزیر ہے۔ ساتھ ہی $F[x]$ سبھی اکائیوں سے بھی تقسیم پزیر ہوگا۔ یہ سبھی تقسیم کرنے والے غیر واجب قاسم (Improper Divisor) کہلاتے ہیں۔ان کے علاوہ f کے دوسرے قاسموں کو واجب قاسم (Proper Divisor) کہتے ہیں، اگر یہ وجود رکھتے ہوں۔

تعریف۔ فرض کرو کہ F کوئی میدان ہے اور $p, q \in F[x]$ دو کثیر رکنی ہیں، تب p اور q کا اعظم مشترک قاسم (Greatest Common Divisor) ایک غیر صفری کثیر رکنی d ہے اس طرح سے کہ $d|p$ اور $d|q$ ساتھ ہی p اور q کا کوئی بھی قاسم، d کا بھی قاسم ہو۔ اعظم مشترک قاسم کو ہم (p, q) سے ظاہر کرتے ہیں۔

تعریف۔ $p, q \in F[x]$ دو کثیر رکنی کو اضافی مفرد (Relatively Prime) کہا جاتا ہے اگر ان کا اعظم مشترک قاسم (GCD) $F[x]$ کی اکائی ہو۔

قضیہ 6۔ فرض کرو کہ میدان F پر کثیر رکنی دامنہ $F[x]$ کے دو غیر صفری کثیر رکنی p اور q ہیں، تب $F[x]$ میں یکتا طور پر دو کثیر رکنی d اور r اس طرح وجود رکھتے ہیں کہ

$$p(x) = d(x)q(x) + r(x)$$

جب کہ یا تو $r(x) = 0$ یا $\deg r(x) < \deg q(x)$

ثبوت۔ فرض کرو کہ $\deg p(x) = l$، $\deg q(x) = m$ اور $\deg r(x) = n$

اب اگر $l < m$ یا اگر $p(x) = 0$ تب چوں کہ

$$p(x) = 0 \cdot q(x) + r(x) \Rightarrow p(x) = r(x)$$

اس لیے

$$p(x) = 0 \cdot q(x) + p(x)$$

اب فرض کرو کہ $l \geq m$ اس صورت میں ہم ریاضیاتی استقرا کی مدد سے یہ ثابت کریں گے۔

13.3 اکتسابی نتائج (Learning Outcomes)

اس اکائی کو پڑھنے کے بعد آپ نے رنگ اور میدان پر کثیر رکنی رنگ کی تعریف اور ان سے وابستہ مختلف قضیوں کو ثابت کرنا سیکھا ہوگا۔

13.4 کلیدی الفاظ (Keywords)

غیر متعین متغیر، عبارت، کثیر رکنی، میدان، رنگ، اولی ضریب

13.5 نمونہ امتحانی سوالات(Model Examination Questions)

13.5.1 معروضی جوابات کے حامل سوالات(Objective Answer Type Questions)

1. کسی رنگ پر کثیر رکنی رنگ کی تعریف کیجیے۔
2. کسی میدان پر کثیر رکنی رنگ کی تعریف کیجیے۔
3. دو کثیر رکنیوں کی جمع حاصل کرنے کے لیے ہمیں ان کے یکساں قوتوں کے ضریبوں کو جوڑنا چاہیے۔ *(T/F)*
4. صفر کثیر رکنی کا درجہ کیا ہوتا ہے؟
5. مستقل کثیر رکنی کا درجہ n ہوتا۔ *(T/F)*
6. صفر کثیر رکنی کو چھوڑ کر سبھی مستقل کثیر رکنیوں کا معکوس حاصل کیا جا سکتا ہے۔ *(T/F)*
7. کثیر رکنی کا اولی ضریب کسے کہتے ہیں؟

13.5.2 مختصر جوابات کے حامل سوالات(Short Answer Type Questions)

1. اگر F ایک میدان ہو، تو $F[x_1, x_2, \cdots, x_n]$ ایک انتگرل دامنہ ہوتا ہے۔
2. فرض کرو کہ میدان F پر کثیر رکنی دامنہ $F[x]$ کے دو غیر صفری کثیر رکنی p اور q ہیں، تب $F[x]$ میں یکتا طور پر دو کثیر رکنی d اور r اس طرح وجود رکھتے ہیں کہ

$$p(x) = d(x)q(x) + r(x)$$

جب کہ یا تو $r(x) = 0$ یا $\deg r(x) < \deg q(x)$

13.5.3 طویل جوابات کے حامل سوالات(Long Answer Type Questions)

1. اگر $\mathrm{R}[x]$ کسی رنگ R پر کثیر رکنی رنگ ہو اور فرض کرو کہ اس کی دو غیر صفری کثیر رکنیاں

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m, a_m \neq 0$$

اور $$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n, b_n \neq 0$$

ہیں، تب ثابت کرو:

a) اگر $f(x) + g(x) \neq 0$ تب $deg[f(x) + g(x)] \leq max(m, n)$

b) اگر $f(x)g(x) \neq 0$ تب $deg[f(x)g(x)] \leq m + n$

c) اگر R ایک انتگرل دامنہ ہو تو $deg[f(x)g(x)] = m + n$

d) R ایک انتگرل دامنہ ہوگا اگر اور صرف اگر $\mathrm{R}[x]$ انتگرل دامنہ ہو۔

e) اگر F ایک میدان ہے تو $F[x]$ میدان نہیں ہوگا۔

2. اگر R کوئی اختیاری رنگ ہے اور R^I کثیر رکنی رنگ $R[x]$ میں مستقل کثیر رکنیوں کا سٹ ہے۔ تب ثابت کرو کہ R^I رنگ R پر یک مارفیت رکھتا ہے۔

3. فرض کرو کہ $R[x]$ کسی رنگ R پر کثیر رکنیوں کا سٹ ہے، تب ثابت کرو کہ $R[x]$ بالحاظ کثیر رکنیوں کے جمع اور ضرب پر ایک رنگ ہوتا ہے۔

جوابات:

13.5.1 معروضی سوالات کے جوابات

3. T

5. F

6. T

13.6 مزید مطالعے کے لیے تجویز کردہ کتابیں (Suggested Books for Further Readings)

1. I.N. Hestien: Topics in Algebra, Vikas Publishers.
2. A Text Book of B.Sc. Mathematics (Abstract Algebra) V. Venkateshwava Rao & 5 others, S. Chand & Co Ltd.
3. Surjeet Singh Qazi Zameeruddin, Modern Algebra Vikas Publishing House Pvt. Ltd.

اکائی14۔ گوسی صحیح اعداد کا رنگ

(Ring of Gaussian Integers)

اکائی کے اجزا

14.0 تمہید (Introduction)

پچھلی اکائی میں ہم نے کثیر رکنی رنگ کی بنیادی معلومات کے ساتھ رنگ (Ring) اور پھر کسی میدان (Field) پر کثیر رکنی رنگ کے بارے تفصیل کے ساتھ پڑھا نیز بہت سے قضیوں کو ثابت اور مثالوں کو حل کرنا سیکھ گئے ہوں گے۔ اس اکائی میں کثیر رکنی رنگ سے متعلق ایک مسئلہ پر تفصیلی بحث کریں گے جو گوسی صحیح اعداد کی رنگ کے نام سے جانی جاتی ہے۔

14.1 مقاصد (Objectives)

اس اکائی کے مکمل طور پر پڑھنے کے بعد آپ اس قابل ہو جائیں گے کہ :

- گوسی صحیح اعداد کی بنیادی جانکاری سے متعرف ہو کر چند مثالوں کو حل کر سکیں۔
- گوسی صحیح اعداد کی رنگ کو سمجھ سکیں اور اس سے وابستہ قضیوں کو بیان اور ثابت کر سکیں۔

14.2 گوسی صحیح اعداد کی رنگ (Ring of Gaussian Integers)

ایسے ملتف اعداد (Complex Numbers) جن کے حقیقی اور خیالی حصّے دونوں صحیح اعداد ہوں، گوسی صحیح اعداد کہلاتا ہے۔ یہ ملتف اعداد کے معمولی جمع اور ضرب کے عمل کے ساتھ ایک انتگرل دامنہ بناتا ہے۔ اس کو علامت $\mathbb{Z}[i]$ سے ظاہر کرتے ہیں۔ یہ دو درجی صحیح اعداد کے تقلیبی رنگ کی ایک خاص صورت ہے۔

تعریف: گوسی اعداد ایک سٹ ہے جو درجہ ذیل شکل میں ہوتا ہے

$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$$

جہاں $i^2 = -1$ ہوتا ہے۔

گوسی صحیح اعداد ملتف مستوی میں کسی مربع لیٹس کے نقاط ہوتے ہیں۔

اب فرض کرو کہ $a + ib , c + id \in \mathbb{Z}[i],\ \forall a, b, c, d \in \mathbb{Z}$ ہیں۔ تب جمع کے عمل کے تحت

$$(a + ib) + (c + id) = (a + c) + i(b + d) \in \mathbb{Z}[i]$$

اور اسی طرح ضرب کے عمل کے ساتھ

$$(a + ib)(c + id) = (ac - bd) + i(bc + ad) \in \mathbb{Z}[i]$$

اس سے ہم کہہ سکتے ہیں کہ گوسی صحیح اعداد کا سٹ $\mathbb{Z}[i]$ جمع اور ضرب کے عمل کے تحت بند شی خاصیت کو مطمئن کرتا ہے۔ اور اسی وجہ سے $\mathbb{Z}[i]$ ایک رنگ ہے۔

گوسی صحیح اعداد $a + ib$ کا ذوج (Conjugate) $a - ib$ ہوتا ہے جو کہ پھر ایک گوسی صحیح اعداد ہے۔ اس کی نارم (Norm) گوسی صحیح اعداد اور اس کے ذوج کے حاصل ضرب کے مساوی ہوتی ہے۔ جیسے

$$\begin{aligned} N(a + ib) &= (a + ib)(a - ib) \\ &= a^2 - (ib)^2 \end{aligned}$$

$$= a^2 + b^2$$

دوسرے الفاظ میں کسی گوسی صحیح عدد کی نارم اس کی مطلق قدر کے مساوی ہوتی ہے جو کہ ایک غیر صفری صحیح عدد ہوتا ہے۔

تعریف: کسی گوسی صحیح عدد کے رنگ کی یونٹ یا اکائی (ایسا گوسی صحیح عدد جس کا ضربی معکوس بھی گوسی عدد ہو) ایک گوسی صحیح عدد ہوتی ہے جس کی نارم 1 ہو، جیسے $1, -1, i$ اور $-i$

فرض کرو کہ $h = x + iy$ اور $k = u + iv$ ایک جوڑا گوسی صحیح اعداد ہیں تب

$$\begin{aligned} N(hk) &= N[(x + iy)(u + iv)] \\ &= N[(xu - vy) + i(uy + xv)] \\ &= (xu - vy)^2 + (uy + xv)^2 \\ &= (x^2u^2 - 2xyuv + v^2y^2) + (u^2y^2 + 2xyuv + x^2v^2) \\ &= x^2(u^2 + v^2) + y^2(u^2 + v^2) \\ &= (x^2 + y^2)(u^2 + v^2) \\ &= N(h)N(k) \end{aligned}$$

گوسی مفرد (Gaussian Prime): فرض کرو کہ p کوئی غیر صفری گوسی صحیح عدد اس طرح سے ہے کہ $N(p) \geq 2$ جب کہ p ایک اکائی نہیں ہے۔ تب p گوسی مفرد ہو گا اگر

$$p \mid xy \Rightarrow p \mid x \text{ یا } p \mid y$$

غیر تحویل پذیر (Irreducible): فرض کرو کہ p کوئی غیر صفری گوسی صحیح عدد اس طرح سے ہے کہ $N(p) \geq 2$ جب کہ p ایک اکائی نہیں ہے۔ تب p گوسی غیر تحویل پذیر ہو گا اگر

$$p = xy \Longleftarrow x \text{ یا } y \text{ اکائی ہو۔}$$

اضافی مفرد (Relatively Prime): فرض کرو کہ $\mathbb{Z}[i]$ اکائی عنصر 1 کے ساتھ ایک انتگرل دامنہ ہے۔ تب $x, y \in \mathbb{Z}[i]$ کو اضافی مفرد اعداد کہتے ہیں اگر ان کا اعظم مشترک قاسم 1 ہو۔ یعنی

$$gcd(x, y) = 1$$

قضیہ: ثابت کرو کہ $\mathbb{Z}[i]$ ایک انتگرل دامنہ ہوتا ہے۔

ثبوت: ہم جانتے ہیں کہ ہر ایک انتگرل دامنہ بغیر صفر قاسم کے ایک تقلیبی رنگ ہوتا ہے۔ اور ہم یہ بھی جانتے ہیں کہ $\mathbb{Z}[i]$ ایک اکائی عنصر کے ساتھ تقلیبی رنگ ہے۔ اس لیے یہاں ہمیں صرف یہ ثابت کرنا ہے کہ یہ بغیر صفر قاسم کے ایک تقلیبی رنگ ہے۔

مان لو کہ $(x + iy).(u + iv) = 0 \in \mathbb{Z}[i]$

تب یا تو $x + iy = 0$ یا $u + iv = 0$ ہونا چاہیے۔

مان لو کہ $x + iy \neq 0 \Longrightarrow x^2 + y^2 \neq 0$ تب $u + iv = 0$ اس لیے $(x + iy).(u + iv) = 0$

یعنی $x^2 + y^2 \neq 0$

اس لیے

$$(xu - yv) + i(xv + yu) = 0 = 0 + i0$$
$$\Rightarrow \quad xu - yv = 0, xv + yu = 0$$
$$\Rightarrow \quad u = 0, v = 0$$

یعنی $u + iv = 0$ حاصل ہوتا ہے۔

اس لیے اگر $(x + iy).(u + iv) = 0$ ہو جب کہ $x + iy \neq 0$ تب $u + iv = 0$ ہو گا۔

اسی طرح اگر $(x + iy).(u + iv) = 0 \in \mathbb{Z}[i]$ ہو جب کہ $u + iv \neq 0$ تب $x + iy = 0$ ہو گا یعنی $(x + iy).(u + iv) = 0$ تب $(x + iy)$، $(u + iv)$ میں سے کوئی ایک صفر ہو گا۔

اس طرح $\mathbb{Z}[i]$ بغیر صفر قاسم کے ایک تقلیبی رنگ ہے۔

اس لیے $\mathbb{Z}[i]$ ایک انتگرل دامنہ ہوتا ہے۔

قضیہ ثابت ہوا۔

یوکلیڈین رنگ یا یوکلیڈین دامنہ (Euclidean Ring or Euclidean Domain):

فرض کرو کہ $\mathbb{Z}[i]$ کوئی انتگرال دامنہ ہے۔ اگر $\mathbb{Z}[i]$ کے ہر ایک غیر صفری عنصر x کے لیے ہم ایک مثبت صحیح عدد $d(x)$ کو تفویض (Assign) کرتے ہیں جو درجہ ذیل خصوصیات کو مطمئن کرتا ہے

1) ہر ایک $x \neq 0$ کے لیے $d(x)$ ایک مثبت صحیح عدد ہے۔

2) سبھی $x, y \neq 0$ کے لیے $d(xy) \geq d(x)$

3) کسی $x, y \in R$ اور $y \neq 0$ کے لیے $q, r \in R$ اس طرح سے کہ
$$x = qy + r$$
جہاں $r = 0$ یا $d(y) > d(r)$

قضیہ: گوسی صحیح اعداد کا سٹ ایک اقلیدسی رنگ (Euclidean Ring) ہوتا ہے۔

ثبوت: اس قضیہ کو ثابت کرنے کے لیے ہم ثابت کریں گے کہ

دیے گئے $x, y \in \mathbb{Z}[i]$ کے لیے $q, r \in \mathbb{Z}[i]$ اس طرح وجود رکھتے ہیں کہ $y = xq + r$ جہاں $r = 0$ یا $d(r) < d(x)$

یہاں ہم سب سے پہلے مان لیتے ہیں کہ $y = a + bi \in \mathbb{Z}[i]$ ایک اختیاری ہے اور x کوئی مثبت صحیح عدد n ہے۔

صحیح عدد کے رنگ کے لیے حاصل کر سکتے ہیں $a = sn + s_1$ اور $b = tn + t_1$ جہاں s_1 اور t_1 جو $|t_1| \leq \frac{1}{2}n$ اور $|s_1| \leq \frac{1}{2}n$ کو مطمئن کرتا ہے۔

فرض کرو کہ $r = s_1 + t_1 i$ اور $q = s + ti$ تب

$$\begin{aligned} y = a + bi &= (sn + s_1) + (tn + t_1)i \\ &= (s + ti)n + (s_1 + t_1 i) \\ &= qn + r \end{aligned}$$

چوں کہ $d(r) = d(s_1 + t_1 i) = {s_1}^2 + {t_1}^2 \leq \frac{1}{4}n^2 + \frac{1}{4}n^2 < n^2 = d(n)$

اس کیس میں ہم نے دکھایا کہ

$$y = qn + r$$

جب کہ $d(r) < d(n)$ یا $r = 0$

اس لیے تقسیمی الگورتھم ثابت ہوتی ہے

پھر سے مان لو کہ $y, x \neq 0 \in \mathbb{Z}[i]$ اور پہلے کی طرح $y = y\bar{x}$ اور $n = x\bar{x}$ لیتے ہیں جہاں $\bar{x}$ گوسی صحیح عدد x کا ذوج (Conjugate) ہے۔ من درجہ بالا ثابت کردہ رزلٹ سے $q, r \in \mathbb{Z}[i]$ کے لیے، چوں کہ $x \neq 0$ ایک مثبت صحیح عدد ہے اس لیے $d(\bar{x})$ ایک مثبت صحیح عدد ہوگا۔ تب

$$\begin{aligned} y\bar{x} &= q(x\bar{x}) + r \\ d(r) &< d(n) \\ \Rightarrow \quad d\big(y\bar{x} - q(x\bar{x})\big) &< d(x\bar{x}) \\ \Rightarrow \quad d(y - qx)d(\bar{x}) &< d(x)d(\bar{x}) \\ \Rightarrow \quad d(y - qx) &< d(x) \end{aligned}$$

اس لیے

$$y = qx + r$$

جہاں $y - qx = r$ اس لیے $r = 0$ یا $d(r) = d(y - qx) < d(x)$

اس سے ثابت ہوا کہ $\mathbb{Z}[i]$ ایک اقلیدسی رنگ ہے۔

نوٹ: اکائی عنصر کے ساتھ $\mathbb{Z}[i]$ ایک تقلیبی رنگ ہے۔ یہ فیلڈ نہیں ہوتا ہے کیوں کہ $\mathbb{Z}[i]$ میں $1 - i$ کا ضربی معکوس وجود نہیں رکھتا یعنی

$$(1 - i)^{-1} = \frac{1}{1 - i} = \frac{(1 + i)}{(1 + i).(1 - i)} = \frac{1}{2} + \frac{i}{2} \notin Z[i]$$

تقسیم پذیری (Divisibility):

فرض کرو کہ $x, y \in \mathbb{Z}[i]$ تب ہم یہ کہیں کہ y کو x تقسیم کرتا ہے $\Leftrightarrow$ تب q اس طرح وجود رکھتا ہے کہ $y = qx$

مثال 1۔ جانچ کرو کہ x کو y تقسیم کرتا ہے یا نہیں؟

i. $y = 3 + 5i, x = 11 - 8i$

ii. $y = 2 - 3i, x = 4 + 7i$

iii. $y = 3 - 39i, x = 3 - 5i$

iv. $y = 3 - 5i, x = 3 - 39i$

حل۔

i. چوں کہ

$$\frac{11 - 8i}{3 + 5i} = \frac{11 - 8i}{3 + 5i} \times \frac{3 - 5i}{3 - 5i}$$

$$= \frac{(11-8i)(3-5i)}{34}$$
$$= \frac{33-79i-40}{34}$$
$$= \frac{-7-79i}{34}$$
$$\Rightarrow (3+5i) \nmid (11-8i)$$

اس لیے x کو y تقسیم نہیں کرتا ہے۔

ii. چوں کہ

$$\frac{4+7i}{2-3i} = \frac{4+7i}{2-3i} \times \frac{2+3i}{2+3i}$$
$$= \frac{(4+7i)(2+3i)}{13}$$
$$= \frac{8+26i-21}{13}$$
$$= \frac{-13+26i}{13}$$
$$= -1+2i$$
$$\Rightarrow (2-3i) \ / \ (4+7i)$$

اس لیے x کو y تقسیم کرتا ہے۔

iii. چوں کہ

$$\frac{3-5i}{3-39i} = \frac{3-5i}{3-39i} \times \frac{3+39i}{3+39i}$$
$$= \frac{(3-5i)(3+39i)}{1530}$$
$$= \frac{9+102i+195}{1530}$$
$$= \frac{204+102i}{1530}$$
$$= \frac{2+i}{15}$$
$$\Rightarrow (3-39i) \nmid (3-5i)$$

اس لیے x کو y تقسیم نہیں کرتا ہے۔

iv. چوں کہ

$$\frac{3-39i}{3-5i} = \frac{3-39i}{3-5i} \times \frac{3+5i}{3+5i}$$
$$= \frac{(3-39i)(3+5i)}{34}$$
$$= \frac{9-102i+195}{34}$$

$$= \frac{204 - 102i}{34}$$
$$= 6 - 3i$$
$$\Rightarrow (3 - 5i) \ / \ (3 - 39i)$$

اس لیے x کو y تقسیم کرتا ہے۔

تقسیمی الگورتھم (Division algorithm):

فرض کرو کہ $x, y \in \mathbb{Z}[i]$ جب کہ $y \neq 0$ تب $\mathbb{Z}[i]$ میں q, r اس طرح وجود رکھتے ہیں کہ

$$x = yq + r$$

اور

$$N(r) < N(y)$$

ثبوت۔ چوں کہ $N\left(\frac{r}{y}\right) = \frac{N(r)}{N(y)}$، اب ہمیں r اس طرح سے حاصل کرنا ہے کہ $N\left(\frac{r}{y}\right) < 1$

چوں کہ $N(h) < |h|^2$ ہوتا ہے، اس لیے

$$\frac{r}{y} = \frac{x}{y} - q$$

اس سے ہم q کی قدر $\frac{x}{y}$ کی دوری 1 کے درمیان ہی حاصل کر سکتے ہیں۔ جیسا کہ ہم جانتے ہیں کہ گوسی صحیح اعداد ملتف مستوی میں یکساں جگہ کے لیٹس کو تشکیل دیتے ہیں اس لیے اب فرض کرو کہ q اس طرح سے ہے کہ

$$r = x - qy$$

جب کہ

$$N(r) = N(x - qy) = N\left(\frac{x}{y} - q\right)N(y) < N(y)$$

مثال 2۔ اگر $x = 4 + 5i$ اور $y = 3$ تب $\frac{x}{y} = \frac{4+5i}{3}$ چار گوسی صحیح اعداد کی اکائی دوری کے اندر ہے۔ یہاں $N(y) = 9$ اور ہم تقسیمی الگورتھم کو چار طریقوں سے ظاہر کر سکتے ہیں۔

$$4 + 5i = 3(1 + 2i) + (1 - i) \quad N(r) = 2$$
$$= 3(2 + 2i) + (-2 - i) \quad N(r) = 5$$
$$= 3(1 + i) + (1 + 2i) \quad N(r) = 5$$
$$= 3(2 + i) + (-2 + 2i) \quad N(r) = 8$$

مثال 3۔ اگر $x = 2 + 7i$ اور $y = 1 + 2i$ تب $\frac{x}{y} = \frac{2+7i}{1+2i} = \frac{2+7i}{1+2i} \times \frac{1-2i}{1-2i} = \frac{16+3i}{5}$

اب

$$x = yq + r$$

اس لیے

$$N(r) = N(1) = 1 < 5 = N(y)$$
$$\Rightarrow \quad N(r) = N(y)$$

ان کے علاوہ دو اور گوسی صحیح اعداد $\frac{x}{y}$ کی اکائی دوری کے قریب ہی وجود رکھتے ہیں۔ جو کہ اس طرح ہیں:

$$2 + 7i = (1 + 2i)3 + (-1 + i) \qquad N(r) = 2$$

$$= (1+2i)(4+i) - 2i \qquad N(r) = 4$$

اعظم مشترک قاسم(Greatest Common Divisor)

اعظم مشترک قاسم اور یکلڈ الگورتھم کی تفصیلی وضاحت دوسرے اعداد کی طرح ہی کی جاسکتی ہے۔

تعریف: دیا ہے $a, b \in \mathbb{Z}[i]$ اور فرض کرو کہ $S = \{ka + \lambda b : k, \lambda \in \mathbb{Z}[i]\}$ ان سبھی غیر صفری عناصر کا سٹ ہے جن کی نارم قلیل ہو۔ تب a اور b کا اعظم مشترک قاسم d سٹ S کا ایک عنصر ہے۔ ہم علامت $d = gcd(a, b)$ کا استعمال a اور b کے اعظم مشترک قاسم کے لیے کریں گے۔

مثال کے لیے اگر ہم $b = 2 + i$ اور $a = i$ کو لیں تو ہم دیکھتے ہیں کہ

$$1 = (2+i)(1+i) - 3i \in S$$

چوں کہ ایسا کوئی عنصر 1 کو چھوڑ کر وجود نہیں رکھتا ہے جس کی نارم کم تر ہو، اس لیے دیے گئے a اور b کا اعظم مشترک قاسم 1 ہو گا۔

اعظم مشترک قاسم کی چند خصوصیات:

فرض کرو کہ a اور b کا اعظم مشترک قاسم d ہے، تب

1) مشترکہ قاسم(Common Divisor): d دونوں a اور b کو تقسیم کرتا ہے۔
2) عظیمیت(Maximality): a اور b کے ہر مشترکہ قاسم d کو تقسیم کرتا ہے اور ان سبھی میں d کی نارم اعظم ہو گی۔
3) $S = \{\mu d : \mu \in \mathbb{Z}[i]\}$ خاص طور پر $\pm d$ اور $\pm di$ اعظم مشترک قاسم ہیں۔

یکلڈ الگورتھم(Euclid's Algorithm):

فرض کرو کہ $x, y \in \mathbb{Z}[i]$ دو غیر صفری عناصر ہیں۔ تقسیمی قضیہ کو بار بار لاگو کرتے ہوئے، x, y سے شروع کرتے ہیں اور پھر اس حاصل قاسم اور باقی(Remainder) کو بالترتیب مقسوم(Dividend) اور قاسم(Divisor) کے طور پر ایک مساوات میں رکھتے ہیں بشرط یہ کہ باقی صفر نہ ہو اور اسی طرح آخری غیر صفر باقی x, y کے سبھی مشترکہ قاسموں سے تقسیم پذیر ہے اور اس لیے یہ x, y کا سب سے بڑا مشترکہ قاسم ہے۔ ریاضیاتی طور پر اسے درجہ ذیل طریقہ سے ظاہر کرتے ہیں

$$a = bc_1 + r_1$$

$$b = r_1c_2 + r_2$$

$$r_1 = r_2c_3 + r_3$$

$$\vdots \quad \vdots \quad \vdots$$

چوں کہ اس قضیہ کو صحیح اعداد کے لیے ثابت کیا جا چکا ہے اس لیے یہاں ہم اس کو ثابت نہیں کریں گے۔

مثال4۔ $i + 4$ اور 3 کا اعظم مشترک قاسم حاصل کرو۔

حل۔ فرض کرو کہ $x = 4 + i$ اور $y = 3$ اب

کسر $\frac{x}{y} = \frac{4+i}{3}$ کی قدر، گوسی صحیح اعداد $1, 2, 1 + i, 2 + i$ کی اکائی دوری کے درمیان ہے۔ اس لیے

$$4 + i = 1 \cdot 3 + (1 + i), \qquad N(r) = 2 < 9 = N(y)$$

$$3 = (1 - i)(1 + i) + 1 \qquad N(r) = 1$$

اب اعظم مشترک قاسم حاصل کرنے کے لیے الٹی سمت میں

$$gcd(4 + i, 3) = 1 = 3 - (1 - i)(1 + i) = 3 - (1 - i) \qquad \text{.....(1)}$$

اس کے ساتھ ساتھ

$$4 + i = 2 \cdot 3 + (i - 2) \qquad N(r) = 5$$

$$3 = (-1 - i)(i - 2) + (-i) \qquad N(r) = 1$$

مساوات (1) میں $-i$ سے ضرب دے کر حاصل ہے

$$\begin{aligned} gcd(4 + i, 3) = -i &= 3 + (1 + i)(i - 2) \\ &= 3 + (1 + i)(4 + i - 2 \cdot 3) \\ &= (-1 - 2i) \cdot 3 + (1 + i)(4 + i) \end{aligned}$$

مثال 5۔ $x = 7 + 17\,i$ اور $y = 8 - 14\,i$ کا اعظم مشترک قاسم حاصل کیجیے۔

حل۔ سب سے پہلے تقسیمی الگورتھم لگاتے ہیں

$$\begin{aligned} \frac{x}{y} &= \frac{7 + 17\,i}{8 - 14\,i} \\ &= \frac{7 + 17\,i}{8 - 14\,i} \times \frac{8 + 14\,i}{8 + 14\,i} \\ &= \frac{56 + 136i + 98i - 238}{64 + 196} \\ &= \frac{26(-7 + 9i)}{260} \\ &= \frac{-7 + 9i}{10} \end{aligned}$$

اس لیے ہم $y = -1 + i$ کو منتخب کرتے ہیں

$$\Rightarrow 7 + 17i = (-1 + i)(8 - 14i) + 1 - 5i$$

ایک بار پھر تقسیمی الگورتھم کا استعمال کرنے پر

$$\frac{8 - 14i}{1 - 5i} = \frac{8 - 14i}{1 - 5i} \times \frac{1 + 5i}{1 + 5i}$$

$$= \frac{(8 - 14i)(1 + 5i)}{26}$$

$$= 3 + i \quad \text{.....(1)}$$

$$\Rightarrow gcd(7 + 17i, 8 - 14i) = 1 - 5i$$

مساوات(1) سے ہم حاصل کرتے ہیں

$$8 - 14i = (3 + i)(1 - 5i)$$

$$\Rightarrow 7 + 17i = \frac{(-7 + 9i)(8 - 14i)}{10}$$

$$= \frac{\{(-7 + 9i)(3 + i)\}(1 - 5i)}{10}$$

$$= \frac{(-30 + 20i)(1 - 5i)}{10}$$

$$= (-3 + 2i)(1 - 5i)$$

$$\Rightarrow gcd(7 + 17i, 8 - 14i) = 1 - 5i$$

14.3 اکتسابی نتائج (Learning Outcomes)

اس اکائی کو مکمل کرنے پر آپ نے:

- تقسیم پذیر گوسی صحیح اعداد کے بارے میں پڑھا۔
- تقسیم پذیر گوسی صحیح اعداد پر چند مثالوں کو حل کیا۔
- یکلڈ الگورتھم کے بیان کو سمجھا۔

14.4 کلیدی الفاظ (Keywords)

گوسی صحیح اعداد، تقسیم پذیری، عظیمیت، یکلڈ الگورتھم، اقلیدسی دامنہ، اقلیدسی رنگ

14.5 نمونہ امتحانی سوالات(Model Examination Questions)

14.5.1 معروضی جوابات کے حامل سوالات(Objective Answer Type Questions)

1. گوسی صحیح اعداد کی تعریف کرو۔
2. گوسی صحیح اعداد کی تقسیم پذیری سے آپ کیا سمجھتے ہو۔
3. $y = 3 - 5i$ کو $x = 3 - 39i$ تقسیم کرتا ہے۔ *(T/F)*
4. گوسی مفرد(Gaussian prime)کی تعریف کرو۔
5. اضافی مفرد کی تعریف کرو۔

14.5.2 مختصر جوابات کے حامل سوالات(Short Answer Type Questions)

جانچ کرو کہ x کو y تقسیم کرتا ہے یا نہیں؟

1. $y = 1 + 3i, x = 7 + i$
2. $y = 1 + 3i, x = 4 + i$
3. ثابت کرو کہ $N(xy) = N(x)N(y), \forall x, y \in \mathbb{Z}[i]$
4. یکلڈ الگورتھم کو بیان کرو۔
5. گوسی صحیح اعداد q, r حاصل کرو جو $x = yq + r$ کو مطمئن کرتے ہوں جب کہ $N(r) \leq \frac{1}{2}N(y)$
6. $y = 2i, x = 3 + i$ کے لیے اعظم مشترک قاسم حاصل کرو۔
7. $y = 3 + 5i, x = 11 - 8i$ کے لیے اعظم مشترک قاسم حاصل کرو۔

14.5.3 طویل جوابات کے حامل سوالات(Long Answer Type Questions)

1. ثابت کرو کہ $\mathbb{Z}[i]$ ایک انتگرل دامنہ ہوتا ہے۔
2. ثابت کرو کہ گوسی صحیح اعداد کا سٹ ایک اقلیدسی رنگ ہوتا ہے۔

14.6 مزید مطالعے کے لیے تجویز کردہ کتابیں(Suggested Books for Further Readings)

1. Basic Abstract Algebra 2nd Edition by P.B. Bhattacharya, S.K. Jain and S.R. Nagpaul, Cambridge University Press-
2. Topics in Abstract Algebra 2nd Edition by M.K. Sen, ShamikGhosh and MukhoPadhyay University Press.
3. Topics in Algebra, 2nd Edition by I. N. Herstein, Wiley India Pvt. Ltd, New Delhi.

اکائی 15۔ پریمیٹو کثیر رکنیاں اور ان کی خصوصیات

(Primitive Polynomials and their Properties)

اکائی کے اجزا

15.0 تمہید (Introduction)

اس اکائی میں طلبا پریمیٹو کثیر رکنی اور اس سے متعلق کئی مثالیں اور چند نظریات کے بارے میں جانکاری حاصل کریں گے۔

15.1 مقاصد (Objectives)

اس اکائی کے مکمل ہونے پر آپ سب اس قابل ہو جائیں گے کہ:

1. پریمیٹو کثیر رکنی اور دوسری کثیر رکنیوں میں فرق کر سکیں۔
2. پریمیٹو کثیر رکنی کے مسائل حل کر سکیں اور
3. پریمیٹو کثیر رکنیوں کے نظریات کی مدد سے کچھ مسائل حل کر سکیں۔

15.2 پریمیٹو کثیر رکنی (Primitive Polynomial)

15.2.1 پریمیٹو کثیر رکنیوں کی چند مثالیں اور نظریات

(Examples of Primitive Polynomials and Theorems)

تعریف: ایک کثیر رکنی $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$ پریمیٹو کثیر رکنی کہلاتی ہے اگر

$$g.c.d.(a_0, a_1, a_2, \cdots, a_n) = 1$$

ہو، جہاں $g.c.d.$ اعظم مشترک قاسم ہے۔

مثال۔ $f(x) = 2 + 3x + 4x^2$ ایک پریمیٹو کثیر رکنی ہے، چوں کہ $g.c.d.(2,3,4) = 1$ ہے۔

تعریف: کثیر رکنی کا کنٹینٹ اگر $f(x)$ (Content of a Polynomial)، $R[x]$ کی غیر صفر کثیر رکنی ہے، تب $f(x)$ کا سروں (Coefficients) کی gcd کو $f(x)$ کا کنٹینٹ (Content) کہتے ہیں اور اسے $c(f(x))$ یا $c(f)$ سے ظاہر کرتے ہیں۔

مثال۔ بتلاؤ کہ $f(x) = 2x^2 + 3x + 1$ اور $g(x) = x^2 + 2$ کا حاصل ضرب ایک پریمٹیو کیثر رکنی ہے۔

حل۔ دیا گیا ہے کہ $f(x) = 2x^2 + 3x + 1$ اور $g(x) = x^2 + 2$

$$\begin{aligned} \therefore f(x).g(x) &= (2x^2 + 3x + 1)(x^2 + 2) \\ &= 2x^4 + 4x^2 + 3x^3 + 6x + x^2 + 2 \\ &= 2x^4 + 3x^3 + 5x^2 + 6x + 2 \end{aligned}$$

اور $f(x).g(x)$ کا کنٹینٹ (content)

$$c(fg) = g.c.d\,(2,3,5,6,2) = 1$$

$\Leftarrow f(x).g(x)$ پریمٹیو کیثر رکنی ہے۔

مثال۔ فرض کرو کہ $f(x) = 3 + 6x + 9x^3 \in \mathbb{Z}[x]$ ہے۔

تب $c(f)=g.c.d(3,6,9)=3$ ایک غیر صیفر کثیر رکنی $f(x)\in R[x]$ پریمٹیو کثیر رکنی (Primitive Polynomial) کہلاتی ہے اگر $c(f)=1$ ہو۔

مونک کثیر رکنی(Monic Polynomial)

ایک کثیر رکنی $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n\in\mathbb{Z}[x]$ مونک(monic) کثیر رکنی کہلاتی ہے اگر $a_n=1$ ہو۔

نوٹ: تمام مونک کثیر رکنیاں پریمیٹو ہوں گے۔ مثلاً $f(x)=2+4x+6x^2+x^3$ ایک مونک کثیر رکنی ہے اور چوں کہ $g.c.d.(2,4,6,1)=1$ اس لیے $f(x)$ پریمیٹو کثیر رکنی بھی ہوگا۔اس کا معکوس درست نہیں ہے اس کو ہم ذیل کی مثال سے جان سکتے ہیں۔

مثال۔ $g(x)=2x+3x^2+4x^3$ پریمیٹو ہے لیکن مونک نہیں ہے(چوں کہ $a_2=4\neq 1$)

غیر تحویل پذیر کثیر رکنی(Irreducible Polynomial):

تعریف: ایک کثیر رکنی $f(x)\in F[x]$ جس کی ڈگری 1 سے بڑھ کر ہے F پر غیر تحویل پذیر کہلاتی ہے اگر

$$f(x)=g(x)\cdot h(x)$$

ہو، جہاں $g(x),h(x)\in F[x]$ ہو۔

$$\Longrightarrow \qquad g(x) \text{ یا } h(x)\in F$$

یعنی $deg(g(x))=0$ یا $deg(h(x))=0$ ہوگا ($g(x)$ یا $h(x)$ سے کوئی ایک F میں مستقل ہے)۔

مثال 1۔ $f(x)=x^2-3\in\mathbb{Q}[x]$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے اور $\mathbb{R}$ میں تحویل پذیر ہے چوں کہ

$$x^2-3=(x-\sqrt{3})(x+\sqrt{3})$$

اور $x\pm\sqrt{3}\in\mathbb{R}[x]$ ہے۔

نظریہ: $R[x]$ کے دو پریمیٹو کثیر رکنیوں کا حاصل ضرب بھی پریمیٹو کثیر رکنی ہوگا(R ایک UFD ہے)

ثبوت۔ فرض کرو کہ $R[x]$ میں

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$$

اور

$$g(x)=b_0+b_1x+b_2x^2+\cdots+b_mx^m$$

جہاں $a_n\neq 0$، $b_m\neq 0$ ہیں۔

اگر $n=0$ ہو، تب $f(x)=a_0\neq 0$، $\mathbb{R}$ کی یونٹ ہے اور $g.c.d.(f(x)g(x))=g.c.d.(g(x))=1$

اس لیے $f(x)g(x)$ بھی پریمیٹو کثیر رکنی ہے۔

اسی طرح اگر $m=0$ ہو تب بھی $f(x)g(x)$ پریمیٹو ہوگا۔

فرض کرو کہ $m,n\geq 1$ ہیں۔ ہمیں بتلانا ہے کہ $g.c.d.(f(x)g(x))=1$ ہوگا۔

تب ہم $f(x)g(x)$ کو پریمیٹو کہہ سکتے ہیں۔

فرض کرو کہ P، ($f(x)g(x)$ کے سروں) $g.c.d.$ کا ایک جزضربی(Factor) ہے چوں کہ $f(x)$ پریمیٹو ہے P، $a_j(j = 0,1,2,\cdots,n)$ کو تقسیم نہیں کر سکتا ہے۔ فرض کرو کہ a_j ، $f(x)$ کا پہلا سر ہے جو P سے ناقابِل تقسیم ہے اور اسی طرح فرض کرو کہ b_k ، $g(x)$ کا پہلا سر ہے جو P سے تقسیم نہیں ہو سکتا ہے۔

ہمیں معلوم ہے کہ

$$f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n + \cdots + c_{m+n}x^{m+n}$$

جہاں $c_n = a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \cdots + a_nb_0, \forall n = 0,1,2,\cdots,m+n, c_0 = a_0b_0$ ہیں۔

حاصل ضرب $f(x)g(x)$ میں x^{j+k} کا سر

$$c_{j+k} = a_0b_{j+k} + a_1b_{j+k-1} + a_2b_{j+k-2} + \cdots + a_{j-1}b_{k+1} + a_jb_k + a_{j+1}b_{k-1} + \cdots + a_{j+k}b_0$$

جس طرح سے j اور k لیے گئے ہیں اس حساب سے $P/a_s, \forall s < j$ اور $P/b_r, \forall r < k$

$$P/a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \cdots + a_{j+k}b_0$$

اور $P/a_0b_{j+k} + a_1b_{j+k-1} + \cdots + a_{j-1}b_{k+1}$

چوں کہ

$$P/a_jb_k \Longrightarrow P/g.c.d.(\text{سر کے } f(x)g(x))$$

اس لیے P/b_k یا P/a_j

جو کہ a_j اور b_k کی تعریف کے خلاف ہے۔ اس لیے ($f(x)g(x)$ کے سروں) $g.c.d.$ ایک مفرد عدد تقسیم نہیں کر سکتا ہے۔ اس لیے

$$g.c.d.\Big(\text{سروں کے } f(x)g(x)\Big) = 1$$

اس لیے $f(x)g(x)$ پریمیٹو کثیر رکنی ہے۔

مثال2۔ $f(x) = 2 + 3x + 4x^2, g(x) = 5x + 7 \in \mathbb{Z}[x]$ دو پریمیٹو کثیر رکنیاں ہیں اور ان کا حاصل ضرب

$$f(x)g(x) = 14 + 31x + 43x^2 + 20x^3$$

بھی پریمیٹو ہے اس لیے کہ $g.c.d.(14,31,43,20) = 1$

مثال3۔ $f(x) = 3 + 4x + 7x^2, g(x) = 8 + 7x^2 + 9x^3 \in \mathbb{Z}[x]$ یہاں $g.c.d.(3,4,7) = 1$ اور $g.c.d.(8,7,9) = 1$

اس لیے $f(x)g(x)$ دونوں پریمیٹو کثیر رکنیاں ہیں اور

$$f(x)g(x) = (3 + 4x + 7x^2)(8 + 7x^2 + 9x^3) = 24 + 32x + 77x^2 + 55x^3 + 85x^4 + 63x^5$$

یہاں $g.c.d.(24,32,77,55,85,63) = 1$

اس لیے $f(x)g(x)$ پریمیٹو کثیر رکنی ہے۔

نتیجے(Results):

1. فرض کرو کہ F ایک فیلڈ ہے تب $f(x) \in F[x]$، F پر تحویل پذیر ہوگا اگر $f(x)$ کا F میں ایک ریشہ (Root) α ہو یعنی $f(\alpha) = 0$ ہو۔

2. $f(x) \in F[x]$، F پر تحویل پذیر ہوگا $\iff$ $f(x)$ کا ایک ریشہ α، F میں ہو (2 یا $deg(f(x)) = 3$ ہے)۔

گاؤس لیما (Gauss Lemma)

فرض کرو کہ $f(x) \in \mathbb{Z}[x]$ ایک پریمیٹو کثیر رکنی ہے تب $f(x)$، $\mathbb{Q}$ پر تحویل پذیر ہوگا $\iff$ $f(x)$ تحویل پذیر ہے $\mathbb{Z}$ پر۔

ثبوت۔ دیا گیا ہے کہ $f(x) \in \mathbb{Z}[x]$ ایک پریمیٹو کثیر رکنی ہے۔

فرض کرو کہ $f(x)$، $\mathbb{Q}$ پر تحویل پذیر ہے۔

ہمیں بتلانا ہے کہ $f(x)$، $\mathbb{Z}$ پر بھی تحویل پذیر ہوگا۔

چوں کہ $f(x)$، $\mathbb{Q}$ پر تحویل پذیر ہے۔ $g(x), h(x) \in \mathbb{Q}[x]$

اس طرح وجود رکھتے ہیں کہ $f(x) = g(x).h(x)$

اور $deg(g(x)).deg(h(x)) > 0$ ہے۔

فرض کرو کہ

$$g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$$

اور $$h(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$$

جہاں $a_j's, b_j's \in \mathbb{Q}$ ہیں۔

ہم $f(x)$ کو ذیل کی شکل میں ظاہر کر سکتے ہیں

$$f(x) = g(x).h(x) = \frac{a}{b}u_1(x).u_2(x), \qquad a, b \in \mathbb{Z}$$

اور $u_1(x), u_2(x) \in \mathbb{Z}[x]$ پریمیٹو کثیر رکنی ہیں۔ اس لیے

$$bf(x) = au_1(x).u_2(x) \qquad \text{.....(1)}$$

چوں کہ $u_1(x), u_2(x)$ پریمیٹو ہیں اور $f(x)$ پریمیٹو ہے۔ اگر دونوں جانب $g.c.d$ لیں تو حاصل ہوگا

$$b \times 1 = \pm a \cdot 1$$
$$\therefore b = \pm a$$
$$\pm af(x) = au_1(x).u_2(x)$$
$$f(x) = \pm u_1(x).u_2(x)$$

جہاں $u_1(x), u_2(x) \in \mathbb{Z}[x]$ ہے۔ اس لیے $f(x)$، $\mathbb{Z}$ پر تحویل پذیر ہے۔

معکوس (Converse): چوں کہ $\mathbb{Z} \subseteq \mathbb{Q}$ اور $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$

تمام کثیر رکنیاں جو $\mathbb{Z}$ میں تحویل پذیر ہیں $\mathbb{Q}$ میں بھی تحویل پذیر ہوں گی۔

کورولری (Corollary): اگر ایک پریمیٹو کثیر رکنی $f(x) \in \mathbb{Z}[x]$ کا ریشہ $\mathbb{Q}$ میں ہو تب $f(x)$ کا ریشہ $\mathbb{Z}$ میں ہی ہے۔

ثبوت۔ فرض کرو کہ α پریمیٹو کثیر رکنی $f(x)$ کا ایک ریشہ $\mathbb{Q}$ میں ہے۔ تب

$$f(x) = (x - \alpha)g(x)$$

اگر $deg(f(x)) = n$ ہو تب $deg(g(x)) = n-1$ ہے یہاں $\alpha \in \mathbb{Q}$ اور $g(x) \in \mathbb{Q}[x]$ ہے۔

اس لیے $f(x)$ ، $\mathbb{Q}$ پر تحویل پذیر ہے۔

چوں کہ $f(x)$ پریمیٹو ہے، گاوس لیما کی مدد سے $\mathbb{Z}$ پر $f(x)$ تحویل پذیر ہے۔ اس لیے

$$\beta \in \mathbb{Z} \ni f(x) = (x-\beta)h(x)$$

اور $h(x) \in \mathbb{Z}[x]$ ہے۔

نوٹ: ایک کثیر رکنی $f(x) \in \mathbb{Z}[x]$ ، $\mathbb{Z}$ پر تحویل پذیر ہے اگر $f(x)$ کا ایک ریشہ $\mathbb{Z}$ میں ہو۔ ہر غیر تحویل پذیر کثیر رکنی $\mathbb{Z}$ پر پریمیٹو کثیر رکنی ہے۔

نتیجہ 1۔ فرض کرو $f(x), g(x)$ ، $\mathbb{Z}[x]$ کے دو پریمٹیو کثیر رکنیاں ہیں۔ اگر $c_1 \neq 0,\ c_2 \neq 0 \in \mathbb{Z}$ اس طرح ہیں کہ $c_1 f(x) = c_2 g(x)$ تب $c_1 = \pm c_2$ اور $f(x) = \pm g(x)$ ہوں گے۔

ثبوت: فرض کرو کہ $(a_n \neq 0)$ $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ تب $g.c.d(a_0, a_1, \ldots a_n) = 1$ اور $t_0, t_1, \ldots t_n \in \mathbb{Z}$ اس طرح ہیں کہ $t_0 a_0 + t_1 a_1 + \ldots + t_n a_n = 1$ چونکہ $c_1 f(x) = c_2 g(x)$

$$c_2 / (t_0\, c_1 a_0 + t_1 c_1 a_1 + \ldots + t_n c_1 a_n) \text{ اس طرح } c_2 \,/\, c_1 a_0, c_1 a_1, \ldots c_1 a_n$$
$$\Rightarrow c_2 / c_1 (t_0\, a_0 + t_1 a_1 + \ldots + t_n a_n) = c_1$$

اسی طرح c_1 / c_2

$$\therefore c_1 / c_2 \ \&\ \ c_2 / c_1 \ \Rightarrow c_1 = \pm c_2$$
$$\Rightarrow f(x) = \pm g(x)$$

نوٹ:(1) کوئی بھی غیر صیفر کثیر رکنی $f(x)$ کو ایک غیر صیفر اسکیلار (Scalar) اور ایک پریمٹیو کثیر رکنی کے حاصل ضرب میں لکھا جا سکتا ہے چوں کہ $\dfrac{f(x)}{c(f)}$ پریمٹیو ہے اور $c(f)$ ایک غیر صیفر اسکیلر ہے۔

(2) ہر غیر تحویل پزیر (Irreducible) کثیر رکنی پریمٹیو کثیر رکنی ہے۔

نتیجہ 2۔ فرض کرو $f(x) \in \mathbb{Z}[x]$ اور $(n > 0)$ $\deg(f(x)) = n$ فرض کرو کہ $f(x)$ ، $\mathbb{Z}[x]$ کے درجہ $'r'$ اور $'s'$ والے کثیر رکنیوں کا حاصل ضرب نہیں ہے۔ $(0 < r < n,\ 0 < s < n,\ \ r + s = n)$ تب $f(x)$ ، $Q[x]$ کے درجہ $'r'$ اور $'s'$ والے کثیر رکنیوں کا بھی حاصل ضرب نہیں ہو سکتا۔

ثبوت: دیا گیا ہے کہ $f(x) \in \mathbb{Z}[x]$ اور $\deg(f(x)) = n$ یہ بھی دیا گیا ہے کہ $\mathbb{Z}[x]$ کے درجہ $'r'$ اور $'s'$ کے دو کثیر رکنیوں کا حاصل ضرب $f(x)$ نہیں ہو سکتا ہے۔

ہمیں بتلانا ہے کہ $f(x) \neq g(x).h(x)$

جہاں $g(x), h(x) \in Q[x]$ درجہ $'r'$ اور $'s'$ والے کثیر رکنیوں ہیں۔

$$\Rightarrow f(x)=c_0 f_0(x),\quad g(x)=\frac{c_1}{d_1}g_0(x)$$

اور $h(x)=\frac{c_2}{d_2}h_0(x)$ ہوں گے جہاں $f_0(x)\,,g_0(x)\,,\ h_0(x)$ کے $\mathbb{Z}[x]$ Primitive کثیر رکنیوں

ہیں اور $c_0\ ,c_1,\ c_2,\ d_1,\ d_2\in\mathbb{Z}$

تب $c_0 f_0(x)=\frac{c_1}{d_1}g_0(x)\ .\frac{c_2}{d_2}h_0(x)$

$$\Rightarrow c_0 d_1 d_2 f_0(x)=c_1 c_2 g_0(x)\ h_0(x)$$

گاوس لیما کی مدد سے ہمیں معلوم ہے کہ $g_0(x)\ h_0(x)$ Primitive ہے اور اوپر دے گیے نتیجہ سے

$c_0 d_1 d_2=\pm c_1 c_2$ ہوگا۔

$$\Rightarrow f_0(x)=g_0(x)\ h_0(x)$$

جہاں $g_0(x)\ h_0(x)\in\mathbb{Z}[x]$ درجہ $'r'$ اور $'s'$ والے کثیر رکنیاں ہیں۔

$$\Rightarrow f(x)=c_0 f_0(x)=c_0 g_0(x)h_0(x)$$

جو کہ صحیح نہیں ہے اس لیے $f(x)$ کو $Q[x]$ کے درجہ $'r'$ اور $'s'$ والے کثیر رکنیوں کے حاصل ضرب میں نہیں لکھا جا سکتا ہے۔

مثال 5۔ $f(x)=8x^3+4x+1\in\mathbb{Z}[x]$ ایک پریمٹیو کثیر رکنی ہے اور $g(x)=8x^3+4x+2\in\mathbb{Z}[x]$ کا پریمٹیو کیشر رکنی نہیں ہے چوں کہ

$$c(f)=g.c.d(8,4,1)=1$$

اور $$c(g)=g.c.d(8,4,2)=2$$

چوں کہ

$$g(x)=2\left(4x^3+2x+1\right)=2g_1(x)$$

جہاں $g_1(x)=4x^3+2x+1$ پریمٹیو کثیر رکنی ہے اس لیے یہ ممکن ہے کہ

$$g(x)=2g_1(x)$$

اور $g_1(x)$ پریمٹیو کثیر رکنی ہے۔

نظریہ۔ اگر $f(x)\in R[x]$ ایک غیر صفر کثیر رکنی ہے جہاں R ایک UFD ہے تب $f(x)=df_1(x)$ ہوگا، جہاں $f_1(x)$ پریمٹیو کثیر رکنی اور $d=c(f)$

ثبوت۔ فرض کرو کہ $f(x)=a_0+a_1x+\ldots+a_nx^n$ ہے اور فرض کرو کہ

$$c(f)=d=g.c.d.(a_0,a_1,\ldots,a_n)$$

تب $d/a_i\ \forall i$

$$\Rightarrow\quad a_i=du_i$$
$$f(x)=du_0+du_1x+du_2x^2+\ldots+du_nx^n$$

$$= d(u_0 + u_1x + u_2x^2 + \ldots + u_nx^n)$$
$$= df_1(x)$$

اور $f_1(x)$ ایک پریمٹیو کثیر رکنی ہے۔

نظریہ۔ اگر $f(x).g(x)$، $R[x]$ کی ایک پریمٹیو کثیر رکنی ہے، R ایک UFD تب $f(x)$، $g(x)$ بھی پریمٹیو کثیر رکنیاں ہوں گے۔

ثبوت۔ دیا گیا ہے کہ $f(x).g(x) \in R[x]$ ایک پریمٹیو کثیر رکنی ہے اور R ایک UFD ہے، تب $c\big(f(x).g(x)\big)$ ایک یونٹ (Unit) ہے۔

$\Longleftarrow$ ایک $k \in R$ اس طرح ہوگا کہ $c(f.g).k = 1$

$$\Rightarrow \quad c(f)c(g).k = 1$$
$$\Rightarrow \quad c(f)(c(g).k) = 1$$

$\Longleftarrow$ $c(f)$ ایک یونٹ (Unit) ہے۔

$\Longleftarrow$ f ایک پریمٹیو کثیر رکنی ہوگا۔

اسی طرح اگر یونٹ $\Longleftarrow$ g ایک پریمٹیو کثیر رکنی ہے۔

اس طرح اگر $f(x).g(x)$ ایک پریمٹیو کثیر رکنی ہو تب $g(x)$ اور $f(x)$ بھی پریمٹیو کثیر رکنیاں ہوں گے۔

نتیجے (Results):

1. اگر R ایک UFD ہے تب ہر $f(x) \in R[x]$، $R[x]$ کا غیر تحویل پذیر عنصر ہوگا $\Longleftrightarrow$ f، R کا غیر تحویل پذیر عنصر یا $R[x]$ کی غیر تحویل پذیر پریمٹیو کثیر رکنی ہے۔
2. اگر R ایک UFD ہے اور $p(x) \in R[x]$ ایک پریمٹیو کثیر رکنی ہے تب $p(x)$ کو یکتا طور پر $R[x]$ کے غیر تحویل پذیر عناصر کے حاصل ضرب میں لکھا جا سکتا ہے۔

نظریہ۔ اگر R ایک UFD ہے تب $R[x]$ بھی UFD ہوگا۔

ثبوت۔ دیا گیا ہے کہ R ایک UFD ہے۔ فرض کرو کہ $f(x) \neq 0 \in R[x]$ یونٹ نہیں ہے اور $f(x) = df'(x)$ جہاں $d = c(f)$ اور $f'(x)$ ایک پریمٹیو کثیر رکنی ہے۔

اوپر دیے گئے نتیجہ کی مدد سے

$$f'(x) = f_1(x) \cdot f_2(x) \cdots f_k(x)$$

یکتا طور پر $R[x]$ کے غیر تحویل پذیر عناصر کے حاصل ضرب میں لکھ سکتے ہیں۔

چوں کہ $d \in R$ اور R ایک UFD ہے، d یونٹ ہوگا یا $d = d_1d_2 \cdots d_r$ جہاں ہر d_i، R کا غیر تحویل پذیر عنصر ہے۔

اگر d یونٹ ہو تب $f(x) = df'(x)$

$$f(x) = df_1(x) \cdot f_2(x) \cdots f_k(x)$$
$$= \big(df_1(x)\big) \cdot f_2(x) \cdots f_k(x)$$

اور $df_1, f_2, \cdots, f_k$، $R[x]$ کے غیر تحویل پذیر عناصر ہیں۔

اگر d یونٹ نہیں ہے تب $d = d_1 d_2 \cdots d_r$ اور چوں کہ ہر d_i، R کا غیر تحویل پذیر عنصر ہے۔ ہر d_i، $R[x]$ کا بھی غیر تحویل پذیر عنصر ہوگا۔ اس طرح $f(x) = d_1 d_2 \cdots d_r f_1 f_2 \cdots f_k$ ہوگا جس سے اس نظریہ کا ثبوت مکمل ہوگا۔

15.3 اکتسابی نتائج (Learning Outcomes)

اس اکائی کو پڑھنے کے بعد آپ نے پریمیٹو کثیر رکنی، ان کی چند مثالوں کے بارے میں جانکاری حاصل کی ہوگی۔ نیز اس سے متعلق نظریات کو جان کر چند مسائل حل کیے ہوں گے۔

15.4 کلیدی الفاظ (Keywords)

کثیر رکنی، پریمیٹو کثیر رکنی، گاوس لیما، ریشہ

15.5 نمونہ امتحانی سوالات (Model Examination Questions)

15.5.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. پریمیٹو کثیر رکنی کی ایک مثال دو۔
2. ہر مونک کثیر رکنی پریمیٹو کثیر رکنی ہوگی۔ (T/F)
3. ذیل کی کون سی کثیر رکنی پریمیٹو ہے؟

(A) $2 + 4x + 8x^2$ (B) $2 + 5x + 7x^2$ (C) $2x + 8x^3$ (D) ان میں سے کوئی بھی نہیں

4. $6 + 2x + 8x^2 + 12x^3$، $\mathbb{Q}[x]$ میں پریمیٹو کثیر رکنی ہے۔ (T/F)
5. $x^2 + 2x + 1 \in \mathbb{Z}[x]$ پریمیٹو ہے لیکن $\mathbb{Z}$ میں غیر تحویل پذیر ہے۔ (T/F)

15.5.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. ایک مثال کے ذریعے بتلاو کہ دو پریمیٹو کثیر رکنیوں کا حاصل ضرب بھی پریمیٹو کثیر رکنی ہوگا۔
2. پریمیٹو کثیر رکنی کی تعریف کرو۔ اس کی دو مثالیں دو۔
3. بتلاو کہ ہر مونک کثیر رکنی پریمیٹو ہوتی ہے اور اس کا معکوس درست نہیں ہے۔
4. ذیل میں سے کون سی کثیر رکنیاں پریمٹیو ہیں:

i. $5x^3 - 5x + 10$

ii. $x^4 - 3x^2 + 9$

iii. $2x^5 - 5x^4 + 5$

15.5.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. ثابت کرو کہ دو پریمیٹو کثیر رکنیوں کا حاصل ضرب بھی پریمیٹو کثیر رکنی ہے۔

2. گاوس لیما کو بیان اور ثابت کرو۔

جوابات:

15.5.1 معروضی سوالات کے جوابات

2. T

3. *B*)

4. *F*

5. *F*

15.6 مزید مطالعے کے لیے تجویز کردہ کتابیں (Suggested Books for Further Readings)

1. Basic Abstract Algebra 2nd Edition by P.B. Bhattacharya, S.K. Jain and S.R. Nagpaul, Cambridge University Press-
2. Topics in Abstract Algebra 2nd Edition by M.K. Sen, Shamik Ghosh and Mukho Padhyay University Press.
3. Topics in Algebra, 2nd Edition by I. N. Herstein, Wiley India Pvt. Ltd, New Delhi

اکائی16۔ آئزن اسٹین کی کسوٹی اور غیر تحویل پذیر کثیر رکنیاں

(Eisensteins Criteria and Irreducible Polynomials)

اکائی کے اجزا

16.0 تمہید(Introduction)

اس اکائی میں طلبا $\mathbb{Z}$ ،$\mathbb{Q}$،$\mathbb{R}$ اور کسی بھی میدان پر تحویل اور غیر تحویل پذیر کثیر رکنیوں کے بارے میں معلومات حاصل کریں گے اور ان سے متعلق کئی مسئلوں کو حل کریں گے۔ اس اکائی میں طلبا آئزین اسٹین کی کسوٹی کے نظریے کو ثابت کر کے اس کی مدد سے کئی مسائل کو $\mathbb{Q}$ پر تحویل پذیر ہونے کا ثبوت دیں گے۔

16.1 مقاصد(Objectives)

اس اکائی کے مکمل ہونے پر آپ اس قابل ہو جائیں گے کہ کسی بھی میدان پر کون سی کثیر رکنی تحویل پذیر اور کون سی غیر تحویل پذیر ہو سکتی ہے، کی جانکاری حاصل کر لیں گے۔ آئزین اسٹین کسوٹی کی مدد سے کثیر رکنیوں کو $\mathbb{Q}$ پر غیر تحویل پذیر ہے بتلا سکیں گے۔

16.2 تحویل پذیر اور غیر تحویل پذیر کثیر رکنیاں(Reducible and Non-reducible Polynomials)

تحویل پذیر کثیر رکنی: ایک کثیر رکنی $f(x) \in \mathbb{Z}[x]$ تحویل پذیر کہلاتی ہے اگر دو کثیر رکنیاں $g(x), h(x) \in F[x]$ اس طرح ہوں کہ

$$f(x) = g(x) \cdot h(x)$$

اور $deg\big(g(x), h(x)\big) > 0$ ہو۔

غیر تحویل پذیر کثیر رکنی: ایک کثیر رکنی $f(x) \in \mathbb{Z}[x]$ غیر تحویل پذیر کہلاتی ہے اگر $deg\big(f(x)\big) > 1$ ہو اور اگر

$$f(x) = g(x) \cdot h(x)$$

جہاں $g(x), h(x) \in F[x]$

یعنی $g(x)$ یا $h(x)$ میں سے کوئی ایک مستقل ہے۔

مثال۔ $f(x) = x^2 - 2 \in \mathbb{Q}[x]$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے، چوں کہ $x^2 - 2 = \big(x - \sqrt{2}\big)\big(x + \sqrt{2}\big)$ اور $\pm\sqrt{2} \notin \mathbb{Q}$ ہے، نیز $x^2 - 2$، $\mathbb{R}[x]$ پر تحویل پذیر ہوگا اس لیے کہ $x - \sqrt{2}, x + \sqrt{2} \in \mathbb{R}[x]$

مثال۔ $f(x) = x^2 + 5 \in \mathbb{R}[x]$، $\mathbb{R}$ پر غیر تحویل پذیر ہے اور چوں کہ $x^2 + 5 = \big(x - \sqrt{5}i\big)\big(x + \sqrt{5}i\big)$ ہے اور $x^2 + 5$، $\mathbb{C}$ پر تحویل پذیر ہے۔

نوٹ: $p(x) \in F[x]$، F پر غیر تحویل پذیر ہوگا $\Leftrightarrow$ $\langle p(x) \rangle$، $F[x]$ میں غطی ایدیال ہے $\Leftrightarrow$ $\frac{F[x]}{\langle p(x) \rangle}$ ایک فیلڈ ہے۔

نظریہ: اگر $f(x) \in F[x]$، F میں ایک ریشہ α ہو تب $f(x)$، F پر تحویل پذیر ہوگا

ثبوت۔ دیا گیا ہے کہ $f(x) \in F[x]$ اور $\alpha \in F$، $f(x)$ کا ریشہ ہے۔ اس لیے

$$f(\alpha) = 0$$

مان لو کہ $g(x) = x - \alpha$ ہے۔

تب تقسیمی الگورتھم کی مدد سے $g(x) = x - \alpha \neq 0$، $f(x)$ کے لیے $q(x), r(x) \in F[x]$ اس طرح وجود رکھتے ہیں کہ

$$f(x) = q(x)g(x) + r(x)$$

جہاں $r(x) = 0$ ہوگا یا $deg\big(r(x)\big) > deg\big(g(x)\big) = 1$ ہے

اس لیے

$$\begin{aligned} & x = \alpha \\ \Rightarrow\ & f(\alpha) = q(\alpha)g(\alpha - \alpha) + r(\alpha) \\ \Rightarrow\ & 0 = 0 + r(\alpha) = r \\ & r = 0 \qquad \left[\because deg\big(r(x)\big) < 1 \text{ یا } deg\big(r(x)\big) = 0\right] \end{aligned}$$

$$deg\big(g(x)\big) = deg(x - \alpha) = 1 \text{ اور } f(x) = q(x)g(x) \qquad \Leftarrow$$

اس لیے $f(x)$، F پر تحویل پذیر ہے۔

نظریہ: اگر $deg\big(g(x)\big) = 3$ یا 2 ہو تب $f(x) \in F[x]$، F پر تحویل پذیر ہوگا $\Leftrightarrow$ $f(x)$ کا ایک ریشہ α، F میں ہو۔

ثبوت۔ اس نظریہ کا معکوس کا ثبوت اوپر دیے گئے نظریہ کا ثبوت ہے۔

فرض کرو کہ $f(x) \in F[x]$ اور $deg\big(g(x)\big) = 3$ یا 2 ہے اور $f(x)$، F پر تحویل پذیر ہے۔

$$f(x) = f_1(x) \cdot f_2(x) \text{ اور } deg\big(f_1(x), f_2(x)\big) \geq 1 \text{ ہے۔} \qquad \Leftarrow$$

اگر ہم فرض کرتے ہیں کہ $deg\big(g(x)\big) = 3$ تب

$$\begin{aligned} & f(x) = f_1(x) \cdot f_2(x) \\ \Rightarrow\ & deg\big(f_1(x)\big) = 2, deg\big(f_2(x)\big) = 1 \end{aligned}$$

یعنی $f_1(x)$ یا $f_2(x)$ میں سے کوئی ایک درجہ 1 کا ہے۔ مان لو کہ $f_1(x) = ax + b$ ہے، جہاں $a, b \in F$ اور $a \neq 0$ ہے۔

$$\Rightarrow \qquad f(x) = (ax + b) \cdot f_2(x) \qquad \ldots\ldots(*)$$

$$ax + b = 0 \Rightarrow x = -a^{-1}b \in F$$

اس طرح $\alpha = -a^{-1}b \in F$ ہوگا اور $a\alpha + b = 0$

$$\Rightarrow \qquad f(\alpha) = (a\alpha + b) \cdot f_2(\alpha) = 0$$

$f(x)$ کا F میں ایک ریشہ α، وجود رکھتا ہے۔

نظریہ: فرض کرو کہ $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$ ایک مونک کثیر رکنی ہے۔ اگر $f(x)$ کا ایک ریشہ $\alpha \in \mathbb{Q}$، ہو تب $\alpha \in \mathbb{Z}$ ہوگا اور ${}^{\alpha}/_{a_0}$ (α، a_0 کو تقسیم کرتا ہے)۔

ثبوت۔ دیا گیا ہے کہ $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$ ہے اور $f(x)$ کا ایک ریشہ $\alpha \in \mathbb{Q}$، ہے۔

ہمیں بتلانا ہے کہ

(i) $\alpha \in \mathbb{Z}$ اور

(ii) ${}^{\alpha}/_{a_0}$

فرض کرو کہ $\alpha = \frac{r}{s} \in \mathbb{Q}$ ہے اور $g.c.d.(r,s) = 1$

(چوں کہ $f(x)$ کا ایک ریشہ α ہے) $\quad f(\alpha) = 0$

$$\Rightarrow \quad a_0 + a_1\left(\frac{r}{s}\right) + a_2\left(\frac{r}{s}\right)^2 + \cdots + a_{n-1}\left(\frac{r}{s}\right)^{n-1} = -\left(\frac{r}{s}\right)^n$$

$$\Rightarrow \quad a_0 + a_1\frac{r}{s} + a_2\frac{r^2}{s^2} + \cdots + a_{n-1}\frac{r^{n-1}}{s^{n-1}} = -\left(\frac{r^n}{s^n}\right)$$

$$\Rightarrow \quad a_0 s^{n-1} + a_1 r s^{n-2} + a_2 r^2 s^{n-3} + \cdots + a_{n-1}r^{n-1} = -\left(\frac{r^n}{s}\right) \quad \ldots\ldots(*)$$

(*) کی بائیں قدر صحیح عدد ہے۔اس لیے

$$-\frac{r^n}{s} \in \mathbb{Z} \Rightarrow s = \pm 1$$

$s = 1$ لیتے ہیں،اس لیے

$$a_0 + a_1\frac{r}{1} + a_2\frac{r^2}{1^2} + \cdots + a_{n-1}\frac{r^{n-1}}{1^{n-1}} = \pm r^n$$

$\alpha = \pm r \Leftarrow$ ، $\alpha = \pm r \in \mathbb{Z}$ اور $f(x)$ کا ایک ریشہ ہے

نیز $\pm r^n$ ہے $a_0 = -a_1 r - a_2 r^2 - \cdots - a_{n-1}r^{n-1}$

$$\Rightarrow \quad \pm r/a_0$$

$$\therefore \quad \alpha/a_0$$

اس طرح ہر مونک کثیر رکنی $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$ کا ایک ریشہ $\alpha \in \mathbb{Z}$، ہو گا اور α/a_0

مثال۔بتلاو کہ $f(x) = x^3 - x - 1 \in \mathbb{Q}[x]$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔

حل۔دیا گیا ہے کہ $f(x) = x^3 - x - 1 \in \mathbb{Q}[x]$

$$= 1 \cdot x^3 + +0 \cdot x^2 + (-1)x + (-1)$$

یہ بات واضح ہے کہ $f(x)$ ایک مونک کثیر رکنی ہے۔

فرض کرو کہ $f(x)$، $\mathbb{Q}$ پر تحویل پذیر ہے۔ تب ایک ریشہ $\alpha \in \mathbb{Q}$ اس طرح ہو گا کہ

$$f(\alpha) = \alpha^3 - \alpha - 1 = 0$$

چوں کہ $f(x)$ مونک ہے۔اوپر دیے گئے نظریہ کی مدد سے اگر $f(x)$ کا ایک ریشہ $\alpha \in \mathbb{Q}$ ہو تب $\alpha \in \mathbb{Z}$ ہو گا اور $\alpha/a_0 = -1$

اس لیے $\alpha = \pm 1$

اور $f(1) \neq 0$، $f(-1) \neq 0$

یہ صحیح نہیں ہے۔اس لیے ہمارا یہ مان لینا کہ $f(x)$ تحویل پذیر کثیر رکنی ہے غلط ثابت ہوا۔اس لیے $f(x)$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔

16.3 آئزن اسٹین کی کسوٹی(Eisenstein's Criteria)

بیان(Statement): فرض کرو کہ $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x]$
اور $n \geq 1$ اگر ایک مفرد صحیح عدد 'P' ، اس طرح ہو کہ

$$P^2 \nmid a_0 \text{ اور } P \nmid a_n, P/a_0, a_1, a_2, \cdots, a_{n-1}$$

(P ، $a_0, a_1, a_2, \cdots, a_{n-1}$ کو تقسیم کرتا ہے، اور P ، a_n کو اور P^2، a_0 کو تقسیم نہیں کرتا ہے)

تب $f(x)$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔

ثبوت۔ دیا گیا ہے کہ $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n \in \mathbb{Z}[x]$ اور 'P' ، ایک مفرد صحیح عدد اس طرح ہے کہ

$$P^2 \nmid a_0 \text{ اور } P \nmid a_n, P/a_0, a_1, a_2, \cdots, a_{n-1}$$

ہمیں بتلانا ہے کہ $\mathbb{Q}$ پر $f(x)$ غیر تحویل پذیر ہو گا۔

(*).....فرض کرو کہ $f(x)$، $\mathbb{Q}$ پر تحویل پذیر ہے۔

اس لیے

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m + \cdots + a_nx^n$$
$$= (b_0 + b_1x + b_2x^2 + \cdots + b_rx^r)(c_0 + c_1x + c_2x^2 + \cdots + c_sx^s)$$

گاؤس لیما کی مدد سے ہم مان لیں کہ $b_i's, c_j's \in \mathbb{Z}[x]$، $a_k \in \mathbb{Z}[x]$ اور $r, s < n$ اس طرح ہیں کہ $r + s = n$ ہو۔

$$\Longrightarrow \quad a_0 = b_0c_0, \qquad a_n = b_rc_s,$$

دیا گیا ہے کہ $P/a_0 = b_0c_0$ اور $P^2 \nmid a_0 = b_0c_0$

اس سے دو باتیں ممکن ہیں:

P/b_0 اور $P \nmid c_0$ یا P/c_0 اور $P \nmid b_0$

فرض کرو کہ P/c_0 اور $P \nmid b_0$ ہے۔

چوں کہ $P \nmid a_n = b_rc_s \Longleftarrow P \nmid b_r$ اور $P \nmid c_s$ ہے ہو گا۔

مان لو کہ c_m پہلا سر ہے $c_0 + c_1x + c_2x^2 + \cdots + c_sx^s$ کا کہ $P \nmid c_m$

ہمیں معلوم ہے کہ $a_m = b_0c_m + b_1c_{m-1} + b_2c_{m-2} + \cdots + b_mc_0$ ہے۔

چوں کہ $P \nmid b_0$ اور $P \nmid c_m$ ہے $P \nmid a_m$ ہو گا۔

$$\Longrightarrow m = n$$

اور $n = m \leq s < n$ ہو گا جو کہ غلط ہے۔

یہ اس لیے ہوا کہ ہم (*) میں $f(x)$، کو تحویل پذیر مانے تھے۔

اس لیے $\mathbb{Q}$ پر $f(x)$ غیر تحویل پذیر ہے۔

مثال1۔ بتلاؤ کہ $f(x) = x^2 - 2 \in \mathbb{Z}[x]$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔

حل۔ دیا گیا ہے

$$f(x) = x^2 - 2 \in \mathbb{Z}[x]$$
$$= -2 + 0 \cdot x + 1 \cdot x^2$$

اور $a_0 = -2, a_1 = 0, a_2 = 1$ ہیں۔

ایک مفرد صحیح عدد $P = 2$ اس طرح وجود رکھتا ہے کہ

$P = 2/a_0 = -2, a_1 = 0, P = 2 \nmid a_2 = 1$ اور $P^2 = 4 \nmid a_0 = -2$

اس لیے آئزین اسٹین کسوٹی کی مدد سے ہم کہہ سکتے ہیں کہ $f(x) = x^2 - 2 \in \mathbb{Z}[x]$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔

مثال2۔ بتلاؤ کہ $f(x) = x^3 - 5x + 10 \in \mathbb{Z}[x]$، $\mathbb{Q}$ پر غیر تحویل پذیر ہوگا۔

حل۔ دیا گیا ہے کہ $f(x) = x^3 - 5x + 10 \in \mathbb{Z}[x]$ ہے۔

$$= 10 - 5 \cdot x + 0 \cdot x^2 + 1 \cdot x^3$$

اور اس میں $a_0 = 10, a_1 = -5, a_2 = 0, a_3 = 1$ ہیں۔

ایک مفرد صحیح عدد $P = 5$ اس طرح ہے کہ

$P = 5/a_0 = 10, a_1 = -5, a_2 = 0,$ اور $P = 5 \nmid a_3 = 1$

اور $P^2 = 25 \nmid a_0 = 10$ تب آئزین اسٹین کسوٹی کی مدد سے ہم کہہ سکتے ہیں کہ $f(x) = x^3 - 5x + 10 \in \mathbb{Z}[x]$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔

مسئلہ1۔ بتلاؤ کہ ذیل کی کثیر رکنیاں غیر تحویل پذیر ہوں گی:

i. $f(x) = 5x^4 + 4x^3 - 6x^2 - 14x + 2 \in \mathbb{Z}[x]$، $\mathbb{Z}$ پر

ii. $g(x) = 2x^4 + 6x^3 - 9x^2 + 15 \in \mathbb{Z}[x]$، $\mathbb{Z}$ پر

iii. $h(x) = 10x^3 - 7x + 14 \in \mathbb{Z}[x]$، $\mathbb{Q}$ پر

iv. $p(x) = x^4 + 2x + 2 \in \mathbb{Z}[x]$، $\mathbb{Q}$ پر

v. $q(x) = 2x^5 - 5x^4 + 5 \in \mathbb{Z}[x]$، $\mathbb{Q}$ پر

حل۔

i. دیا گیا ہے کہ $f(x) = 5x^4 + 4x^3 - 6x^2 - 14x + 2 \in \mathbb{Z}[x]$ ہے،

یہاں $a_0 = 2, a_1 = -14, a_2 = -6, a_3 = 4, a_4 = 5$ ہیں۔

ایک مفرد صحیح عدد $P = 2$ اس طرح ہے کہ

$P = 2/a_0, a_1, a_2, a_3$ اور $P = 2 \nmid a_4 = 5, P^2 = 2^2 = 4 \nmid a_0 = 2$

اس لیے آئزین اسٹین کسوٹی کی مدد سے $f(x)$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔ چوں کہ پریمیٹو کثیر رکنی ہے، اس لیے گاؤس لیما کی مدد سے ہم کہہ سکتے ہیں $f(x)$، $\mathbb{Z}$ پر غیر تحویل پذیر ہے۔

ii. دیا گیا ہے کہ $g(x) = 2x^4 + 6x^3 - 9x^2 + 15 \in \mathbb{Z}[x]$ ہے،

یہاں $a_0 = 15, a_1 = 0, a_2 = -9, a_3 = 6, a_4 = 2$ ہیں۔

ایک مفرد صحیح عدد $P = 3$ اس طرح وجود رکھتا ہے کہ

$P = 3 \nmid 2, P^2 = 3^2 = 9 \nmid 15$ اور $P = 3/15, 0, -9, 6$

$g(x)$ کے لیے $P = 3$ سے آئزین اسٹین کسوٹی کی پوری ہوتی ہے اس لیے $g(x)$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔ چوں کہ $g(x)$ پریمیٹو ہے، اس لیے گاؤس لیما کی مدد سے ہم کہہ سکتے ہیں $g(x)$، $\mathbb{Z}$ پر بھی غیر تحویل پذیر ہوگا۔

iii. دیا گیا ہے کہ $h(x) = 10x^3 - 7x + 14$ ہے،

$$= 14 - 7 \cdot x + 0 \cdot x^2 + 10 \cdot x^3$$

یہاں $a_0 = 14, a_1 = -7, a_2 = 0, a_3 = 10$ ہیں۔

$P = 7$ ایک ایسا مفرد صحیح عدد ہے کہ

$P = 7 \nmid a_3 = 10, P^2 = 7^2 = 49 \nmid 14$ اور $P = 7/14, -7, 0$

اس طرح آئزین اسٹین کسوٹی کے شرائط پوری ہوتی ہیں اور $h(x)$، $\mathbb{Q}$ پر غیر تحویل پذیر ہوگا۔

iv. دیا گیا ہے کہ $p(x) = x^4 + 2x + 2 \in \mathbb{Z}[x]$ ہے،

$$= 2 + 2 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 + 1 \cdot x^4$$

یہاں $a_0 = 2, a_1 = 2, a_2 = 0, a_3 = 0, a_4 = 1$ ہیں۔

مفرد صحیح عدد $P = 2$ اس طرح وجود رکھتا ہے کہ

$P = 2 \nmid a_4 = 1, P^2 = 2^2 = 4 \nmid a_0 = 2$ اور $P = 2/a_0, a_1, a_2, a_3$

تب آئزین اسٹین کسوٹی کی مدد سے $p(x)$، $\mathbb{Q}$ پر غیر تحویل پذیر ہوگا۔

v. دی گئی کثیر رکنی ہے

$$q(x) = 2x^5 - 5x^4 + 5 \in \mathbb{Z}[x]$$
$$= 5 + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 - 5 \cdot x^4 + 2 \cdot x^5$$

یہاں $a_0 = 5, a_1 = 0, a_2 = 0, a_3 = 0, a_4 = -5, a_5 = 2$ ہیں۔

ایک مفرد صحیح عدد $P = 5$ اس طرح ہے کہ

$P = 5 \nmid a_5 = 2, P^2 = 5^2 = 25 \nmid a_0 = 5$ اور $P = 5/5,0,0,0,-5$

اس طرح آئزین اسٹین کسوٹی کی تمام شرائط پوری ہوئیں اور $q(x) = 2x^5 - 5x^4 + 5$، $\mathbb{Q}$ پر غیر تحویل پذیر ہوگا۔

مسئلہ 2۔ بتلاؤ کہ $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_7[x]$، $\mathbb{Z}_7$ پر غیر تحویل پذیر ہے۔

حل۔ دیا گیا ہے کہ

$$f(x) = x^3 + 3x + 2$$

اور $deg\big(f(x)\big) = 3$ ہے۔

ہمیں معلوم ہے کہ اگر $f(x) \in F[x]$ کا درجہ 2 یا 3 ہو تو $f(x)$، F میں تحویل پذیر ہوگا $\Leftrightarrow$ $f(x)$ کا ایک ریشہ α، F میں ہوگا۔

یہاں
$$F = \mathbb{Z}_7$$
$$= \{0,1,2,3,4,5,6\}$$

اس لیے

$$f(0) = 0^3 + 3 \cdot 0 + 2 = 2 \neq 0$$
$$f(1) = 1^3 + 3 \cdot 1 + 2 = 6 \neq 0$$
$$f(2) = 2^3 + 3 \cdot 2 + 2 = 16 \neq 0$$
$$f(3) = 3^3 + 3 \cdot 3 + 2 = 38 \neq 0$$
$$f(4) = 4^3 + 3 \cdot 4 + 2 = 78 \neq 0$$
$$f(5) = 5^3 + 3 \cdot 5 + 2 = 142 \neq 0$$
$$f(6) = 6^3 + 3 \cdot 6 + 2 = 236 \neq 0$$

اس طرح کا کوئی بھی ریشہ م $\mathbb{Z}_7$ یں نہیں ہے۔اس لیے $f(x) = x^3 + 3x + 2 \in \mathbb{Z}_7$، $\mathbb{Z}_7$ پر غیر تحویل پذیر ہے۔

مسئلہ 3۔ بتلاؤ کہ $f(x) = x^3 - x - 1 \in \mathbb{Q}[x]$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔

حل۔ دیا گیا ہے کہ

$$f(x) = x^3 - x - 1 \in \mathbb{Q}[x]$$
$$= -1 - 1 \cdot x + 0 \cdot x^2 + 1 \cdot x^3$$

یہ واضح ہے کہ $f(x)$ ایک مونک کثیر رکنی ہے۔

(*).....فرض کرو کہ $f(x)$، $\mathbb{Q}$ پر تحویل پذیر ہے۔

اس لیے $\exists \alpha \in \mathbb{Q}$ اور $f(\alpha) = \alpha^3 - \alpha - 1 = 0$ ہوگا۔

چوں کہ $f(x)$ مونک ہے اگر $\alpha \in \mathbb{Q}$، $f(x)$ کا ایک ریشہ ہو تب ایک معروف نظریہ کی مدد سے حاصل ہے $\alpha \in \mathbb{Z}$ اور
$$\alpha/a_0 = -1$$
$$\Rightarrow \alpha = \pm 1$$

$f(-1) = (-1)^3 + 1 - 1 = -1 \neq 0$ اور $f(1) = 1^3 - 1 - 1 = -1 \neq 0$ کے لیے $f(x)$

اس لیے α ، $f(x)$ کا ریشہ نہیں ہے۔

یہ غلط بیان ہے اسی لیے ہمارا مفروضہ $f(x)$ کو $\mathbb{Q}$ پر تحویل پذیر ماننا غلط ہے۔

اس لیے $f(x) = x^3 - x - 1 \in \mathbb{Q}[x]$، $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔

مسئلہ 3۔ اگر p ایک مفرد صحیح عدد ہے اور $\varphi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ ہو تب بتلاؤ کہ $\varphi_p(x)$، $\mathbb{Q}$ پر غیر تحویل پذیر ہوگا۔

حل۔ دیا گیا ہے کہ $\varphi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ اور p ایک مفرد صحیح عدد ہے، تب

$$g(x) = \varphi_p(x+1) = \frac{(x+1)^{p-1}}{(x+1)-1}$$

$$= \frac{1}{x}\left[x^{p-1} + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x\right]$$
$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1}$$
$$= \binom{p}{p-1} + \binom{p}{p-2}x + \binom{p}{p-3}x^2 + \cdots + \binom{p}{2}x^{p-3} + \binom{p}{1}x^{p-2} + x^{p-1}$$
$$= p + \frac{p(p-1)}{2!}x + \frac{p(p-1)(p-2)}{3!}x^2 + \cdots + px^{p-2} + x^{p-1}$$

اس کے تمام سروں کو تقسیم کرتا ہے، $P \nmid p, P^2 \nmid 1$

تب آئزین اسٹین کی کسوٹی سے یہ واضح ہے کہ $\varphi_p(x)$، $\mathbb{Q}$ پر غیر تحویل پذیر ہوگا۔

16.5 اکتسابی نتائج (Learning Outcomes)

اس اکائی کو مکمل کرنے پر آپ نے تحویل پذیر اور غیر تحویل پذیر کثیر رکنیوں میں فرق جانا ہے اور آئزین اسٹین کی کسوٹی کی مدد سے کئی کثیر رکنیوں کو غیر تحویل پذیر بتلایا ہوگا۔

16.6 کلیدی الفاظ (Keywords)

تحویل پذیر کثیر رکنی، غیر تحویل پذیر کثیر رکنی، آئزین اسٹین کی کسوٹی

16.7 نمونہ امتحانی سوالات (Model Examination Questions)

16.7.1 معروضی جوابات کے حامل سوالات (Objective Answer Type Questions)

1. $f(x) = x^2 - 5$ تحویل پذیر ہے

A) $\mathbb{Z}$ پر B) $\mathbb{Q}$ پر C) $\mathbb{R}$ پر D) ان میں سے کوئی بھی نہیں

2. $1 + x + x^2 + x^3 + x^4$، $\mathbb{Q}$ پر تحویل پذیر ہے۔ (*T/F*)

3. ایک مفرد صحیح عدد p کے لیے $f(x) = x^n - p$ ہمیشہ $\mathbb{Q}$ پر غیر تحویل پذیر ہے۔ (*T/F*)

4. $f(x) = x^2 + 2x + 1$ تحویل پذیر ہے

A) مونک B) پریمیٹو C) دونوں D) ان میں سے کوئی بھی نہیں

5. اگر α، $f(x) \in F[x]$ کا ریشہ ہو تب _____ $= f(\alpha)$ ہے۔

16.7.2 مختصر جوابات کے حامل سوالات (Short Answer Type Questions)

1. بتلاؤ کہ $f(x) = x^2 + 8x - 2$، $\mathbb{Q}$ پر غیر تحویل پذیر ہوگا۔
2. ذیل کی کثیر رکنیوں کی $\mathbb{Q}$ پر غیر تحویل پذیری کی جانچ کرو:
   a) $8x^3 + 6x^2 - 9x + 24$
   b) $x^4 + 9x + 3$

3. بتلاؤ کہ $x^4 + 8 \in \mathbb{Q}[x]$، $\mathbb{Q}$ پر تحویل پذیر ہے۔

16.7.3 طویل جوابات کے حامل سوالات (Long Answer Type Questions)

1. گاؤس لیما کو بیان اور ثابت کرو۔
2. آئزین اسٹین کی کسوٹی کو بیان اور ثابت کرو۔

جوابات:

16.7.1 معروضی سوالات کے جوابات

2. F
3. T
4. C

16.8 مزید مطالعے کے لیے تجویز کردہ کتابیں (Suggested Books for Further Readings)

1. Basic Abstract Algebra 2nd Edition by P.B. Bhattacharya, S.K. Jain and S.R. Nagpaul, Cambridge University Press-
2. Topics in Abstract Algebra 2nd Edition by M.K. Sen, Shamik Ghosh and Mukho Padhyay University Press.
3. Topics in Algebra, 2nd Edition by I. N. Herstein, Wiley India Pvt. Ltd, New Delhi

نمونہ امتحانی پرچہ

ریاضیات (الجبرا)

BSMM301CCT

ہدایات:

یہ پرچہ سوالات تین حصوں پر مشتمل ہے: حصہ اول، حصہ دوم اور حصہ سوم۔ ہر جواب کے لیے لفظوں کی تعداد اشارتن ہے۔ تمام حصوں سے سوالوں کا جواب دینا لازمی ہے۔

1۔ حصہ اول میں 10 لازمی سوالات ہیں جو کہ معروضی سوالات / خالی جگہ پر کرنا / مختصر جواب والے سوالات ہیں۔ ہر سوال کا جواب لازمی ہے۔ ہر سوال کے لیے 1 نمبر مختص ہے۔ $10 \times 1 = 10$

2۔ حصہ دوم میں آٹھ سوالات ہیں۔ اس میں سے طالب علم کو کوئی پانچ سوالات کے جواب دینے ہیں۔ ہر سوال کا جواب تقریبن 200 لفظوں پر مشتمل ہے۔ ہر سوال کے لیے 6 نمبرات مختص ہیں۔ $5 \times 6 = 30$

3۔ حصہ سوم میں پانچ سوالات ہیں۔ اس میں سے طالب علم کو کوئی تین سوالات کے جواب دینے ہیں۔ ہر سوال کا جواب تقریبن 500 لفظوں پر مشتمل ہے۔ ہر سوال کے لیے 10 نمبرات مختص ہیں۔ $3 \times 10 = 30$

حصہ اول

(i) گروپ کی تعریف کیجیے۔

(ii) ہم سٹس کی ایک مثال دیجیے۔

(iii) خارج قسمت گروپ کی تعریف کرو۔

(iv) مبادلہ گروپ کی تعریف کرو۔

(v) گروپ کے ہم مارفیت سے آپ کیا سمجھتے ہو؟

(vi) گرپ کی یک مارفیت کی تعریف کرو۔

(vii) رنگ کی ایک مثال دیجیے۔

(viii) کثیر رکنی رنگ کی تعریف کیجیے۔

(ix) گاؤسین صحیح اعداد کے رنگ کی تعریف کیجیے۔

(x) پریمٹو کثیر رکنی کیا ہوتی ہے؟

حصہ دوم

2. بتلاؤ کہ سٹ $\{\ldots -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$ جہاں $\left(m \in \mathbb{Z}^+\right)$ ہے ایک تقلیبی گروپ ہے۔

3. Factor Group $\frac{\mathbb{Z}_{60}}{\langle 5 \rangle}$ کا رتبہ (Order) معلوم کرو۔

4. $\mathbb{Z}_{36}$ کے تحت گروپ $H = \langle 9 \rangle$ کے تمام بائیں ہم سٹس معلوم کرو۔

5. ذیل کے کون سے مبادلے جفت یا طاق ہیں۔

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

6. فرض کرو کہ $G = \left(\mathbb{R}^+, .\right)$ اور $G' = \left(\mathbb{R}^+, +\right)$ اگر $\varnothing : G \to G'$ کی تعریف اس طرح ہے کہ $\varnothing(x) = \log_{10}^x$ تب بتلاؤ کہ $\varnothing$ یک مافیت ہے

7. متناہی سائکل گروپ G جو 'a' سے generated ہے اور اگر $o(a) = n$ ہو $\mathbb{Z}_n$ سے isomorphic ہوگا۔

8. $\mathbb{Z}_{14}$ کے سارے یونٹس (Units) معلوم کرو۔

9. بتلاؤ کہ $\mathbb{R} = \{0, 2, 4, 6\}$ $+_8$ $\times_8$ ایک رنگ ہے۔

حصہ سوم

10. ثابت کرو کہ $S_1 = \{0, 3\}$ اور $S_2 = \{0, 2, 4\}$، $(\mathbb{Z}_6, +_6, \times_6)$ کے تحت رنگس ہیں۔

11. اگر R ایک تقلیبی رنگ ہے جس کا Characteristic 2 ہے $\phi : R \to R$ جس کی تعریف $\phi(x) = x^2$ ہو ایک ہم مارفیت ہے۔

12. $x^4 + 4 \in \mathbb{Z}_5[x]$ کے فیاکٹرس (factors) معلوم کرو۔

ثابت کرو کہ $f(x) = 2x^4 + 6x^3 - 9x^2 + 15$، Q پر غیر تحویل پذیر ہے۔

13. بتلاؤ کہ ذیل کی کثیر رکنیاں $f(x) = 6 + 18x^8 + 12x^9 + 9x^{10} + 4x^{13}$ اور $g(x) = 12 + 30x^4 + 12x^5 + 5x^7$، Q پر غیر تحویل پذیر ہوں گے۔

14. بتلاؤ کہ رنگ $\left(R = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \;/\; a, b, c, d \in \mathbb{Z}\right\}, .\right)$ کا سٹ $B = \left\{\begin{bmatrix} p & q \\ 0 & 0 \end{bmatrix} \;/\; p, q \in \mathbb{Z}\right\}$، R کا دایاں ایدیال (right ideal) ہے لیکن بایاں ایدیال (left ideal) نہیں ہے۔

لیب مینول

الجبرا

تصدیق نامہ

تصدیق کی جاتی ہے کہ بیایس سی (تیسرا سمسٹر) الجبرا کے تجرباتی حصہ کے کام کا یہ اصلی ریکارڈ ہے جسے

نے مولانا آزاد نیشنل اردو یونیورسٹی کے اسٹڈی سینٹر _____ میں تعلیمی سال

_____ کے دوران تیار کیا۔

تاریخ

دستخط کونسلر

فہرست

بلاک۔ 5 گروپ تھیوری

پانچواں بلاک اکائی 17 سے 20 پر مشتمل ہے۔ جس میں گروپ سے متعلق تعریفات اور مسائل ہیں۔ اکائی – 17 میں گروپ کے بنیادی خصوصیات، چند مثالیں اور تحت گروپ کے مسائل دیے گئے ہیں۔ اکائی – 18 میں کوسٹ، نارمل تحت گروپ اور کوشینٹ گروپ کے تجرباتی مسائل پیش کیے گئے ہیں۔ باقی دو اکائیوں میں مبادلہ گروپ، سائکلی گروپ، ہم مارفیت اور یک مارفیت کے تجرباتی مسائل دیے گئے ہیں۔

اکائی 17۔ گروپس–بنیادی خصوصیات اور تحت گروپ

(Groups-Basic Properties and Subgroup)

Objective 17.0

اس اکائی میں طلبا کی مسئلہ حل صلاحیت کو بہتر بنانے کے لیے گروپس اور تحت گروپ کے مسائل پیش کیے گئے ہیں۔

17.1 :اس حصے میں گروپس اور تحت گروپس کے مختلف مسائل کو حل کرنے سے پہلے گروپ اور تحت گروپ کی بنیادی معلومات دی گئی ہیں۔

یوکلڈس کا تقسیم کاالگارتھم (Euclids Division Algorithm)

اگر $a, b \neq 0 \in \mathbb{Z}$ ہو تب یکتا صحیح اعداد $q, r \in \mathbb{Z}$ اس طرح وجود رکھتے ہیں کہ $a = bq + r$ اور $0 \leq r < |b|$۔

نوٹ: اگر a اور b مثبت ہوں تب $a = bq + r$ اور $0 \leq r < b$ ہوگا۔

اگر $r = 0$ ہو تب $a = bq$ ہوگا اور 'b' کو a کا ڈوائزر (divisor) کہتے ہیں اور b / a سے ظاہر کرتے ہیں۔

اگر $r \neq 0$ ہو تب $b \nmid a$ (a، b کا ڈوائزر نہیں ہوگا)۔

اعظم ترین مشترک ڈوائزر (Greatest CommonDivisor)

اگر $a, b \in \mathbb{Z}$ اور $d \in \mathbb{Z}$ اس طرح ہے کہ d / a اور d / b تب d کو a اور b کا common divisor کہتے ہیں۔

اگر a, b کا c کوئی common divisor ہو تب اور c / d بھی ہو تب، d کو a اور b کا Greatest Common Divisor کہتے ہیں۔

مثال: فرض کرو کہ $a = 18$ اور $b = 24$ تب a اور b کے common divisor ہیں۔ 2, 3, 6 یہاں 2, 3/6

g.c.d. (18, 24) = 6

اگر $g.c.d\ (a,b) = 1$ ہو تب a اور b کو ایک دوسرے کا co-prime صحیح اعداد یا relatively prime integers کہتے ہیں۔

کانگروینس (Congruence) ماڈیولر ارتھمیاٹک:

فرض کرو کہ m ایک مقررہ مثبت صحیح عدد ہے اور $a,b \in \mathbb{Z}$ تب 'a' کو b سے congruent mod m کہتے ہیں۔ اگر $m/a-b$ اسے $a \equiv b \pmod m$ سے ظاہر کرتے ہیں۔

نوٹ: (i) $b \equiv a \pmod m \ \Leftrightarrow \ a \equiv b \pmod m$

(ii) $a \equiv b \pmod m$ اور $c \equiv d \pmod m$

$$\Rightarrow a+c \equiv b+d \pmod m$$

اور $$ac \equiv bd \pmod m$$

آئیلر ϕ-تفاعل (Euler ϕ - Function):

اگر $n \in \mathbb{Z}^+$ تب $n(>1)$ کا آئیلر ϕ-تفاعل جسے $\phi(n)$ سے ظاہر کرتے ہیں کی تعریف اس طرح کی گئی ہے۔

"وہ عدد ہے جتنے کے n سے چھوٹے مثبت صحیح اعداد $\phi(n) = n$ سے relatively prime ہونگے"۔

نوٹ: $\phi(1) = 1$

مثال: $\phi(10) = 4$

ثنائی عمل (Binary Operation): ہم جانتے ہیں کہ arithmetic میں چار بنیادی آپریشنس $(+)$ (Operations)، $(-)$، $(\times)$ اور $(\div)$ ہیں۔ ان کی مدد سے بہت سے Operations کی تعریف کر سکتے ہیں، جسے ہم '$*$'، '$\circ$'، '$\oplus$' وغیرہ سے ظاہر کرتے ہیں۔

تعریف ثنائی عمل (Binary Operation): ایک عمل '$*$' کسی غیر خالی سٹ S پر ثنائی عمل کہلاتا ہے اگر $*: S \times S \to S$ ہو۔ یعنی $\forall a,b \in S \ \ a*b \in S$ ہو۔

مثالیں: (i) طبعی اعداد کے سٹ N پر '$+$' ایک ثنائی عمل ہے۔ چونکہ $\forall a,b \in \mathbb{N} \ \ a+b \in \mathbb{N}$ ہے۔

(ii) ضرب '$\times$' بھی N پر ثنائی عمل ہوگا۔

(iii) '$-$' N پر ثنائی عمل نہیں ہے۔ چونکہ $\begin{pmatrix} \because \ for\, 1,2 \in \mathbb{N} \\ 1-2=-1 \notin \mathbb{N} \end{pmatrix}$

تعریف: گروپ: ایک غیر خالی سٹ G ثنائی عمل '$*$' کے حوالے سے گروپ کہلاتا ہے اگر

(i) $a*b \in G \ \ \forall a,b \in G$ بند شی کلیہ (Closure Law)

(ii) $(a*b)*c = a*(b*c) \ \ \forall a,b \in G$ تلازمی (Associative Law)

اکائی کا وجود (iii) ایک $e \in G$ اس طرح وجود رکھتا ہے کہ

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

(یہاں 'e' کو G کی اکائی کہتے ہیں)

(iv) ہر $a\in G$ کے لیے ایک $b\in G$ ایسا ہوگا کہ معکوس کا وجود

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

اور b کو a کا معکوس کہتے ہیں اور اسے a^{-1} سے ظاہر کرتے ہیں۔

ان چار اصولوں کے علاوہ اگر $a*b=b*a \quad \forall a,b\in G$ ہو تب $(G,*)$ کو abelian گروپ یا تقلیبی گروپ کہتے ہیں۔

مثال: $(\mathbb{Z},+)$ ایک تقلیبی گروپ۔

نوٹ: 1) گروپ کا اکائی عنصر یکتا ہوتا ہے۔

2) $a\in G$ کے لیے a^{-1} بھی یکتا ہوتا ہے۔

مثال: بتلاؤ کہ $G=\{\ldots -6,-4,-2,0,2,4,6,\ldots\}$، $\{2n / n\in\mathbb{Z}\}=$ جمع '+' کے عمل سے ایک لامتناہی ابیلین گروپ ہوگا۔

حل: دیا گیا ہے کہ $G=\{2n / n\in\mathbb{Z}\}=\{\ldots -6,-4,-2,0,2,4,6,\ldots\}$

(i) بند شی کلیہ: فرض کرو کہ $x=2n_1, y=2n_2\in G$ ہیں جہاں $n_1,n_2\in\mathbb{Z}$۔

$$\therefore x+y=2n_1+2n_2=2(n_2+n_1)=2n_3\in G(\because n_3=n_1+n_2\in\mathbb{Z})$$

$$\therefore x+y\in G\forall x,y\in G$$

$\Leftarrow G$ بلحاظ '+' بند ہے۔

(ii) تلازمی کلیہ: فرض کرو کہ $x=2n_1, y=2n_2, z=2n_3\in G$

$$\Rightarrow (x+y)+z=(2n_1+2n_2)+2n_3$$

$$=2(n_1+n_2)+2n_3$$

$$=2\left[(n_1+n_2)+2n_3\right]$$

$$=2\left[n_1+(n_2+2n_3)\right]$$

$$=2n_1+2(n_2+n_3)$$

$$=x+(y+z)$$

$$\therefore (x+y)+z=x+(y+z)\forall x,y,z\in G$$

(iii) اکائی کا وجود: $0\in G$ اس طرح ہے کہ ہر $x=2n\in G$ کے لیے $x+o=o+x=x$ ہے۔

$\Leftarrow$ 'o' G کی اکائی ہے۔

(iv) معکوس کا وجود : ہر $x = 2n \in G$ کے لیے $-x = 2(-n) \in G$ اس طرح وجود رکھتا ہے کہ

$$x + (-x) = (-x) + x = 0$$

$\Leftarrow$ $-x = 2(-n)$، $x = 2n \in G$ کا معکوس ہے۔

نیز $\forall x = 2n_1, y = 2n_2 \in G$ کے لیے $x + y = y + x$ ہوگا۔اس لیے $(G, +)$ ایک تقلیبی گروپ ہے۔

متناہی گروپس کے لیے کامپوزشن کا ٹیبل طریقہ(Composition Table Method)

اگر $S = \{a_1, a_2, a_3 ..... a_n\}$ ایک متناہی سٹ اور 'o' اس پر ایک ثنائی عمل ہے تب S کے عناصر سے اسی کے عنصر کا حاصل ضرب لے کر ذیل سا ایک ٹیبل بناتے ہیں جسے Composition Table کہتے ہیں۔

(عمل کا جدول)

o	a_1	a_2	..	...	...	a_n
a_1	$a_1 o a_1$	$a_1 o a_2$				$a_1 o a_n$
a_2	$a_2 o a_1$	$a_2 o a_2$				$a_2 o a_n$
..	...	...	...	...	...	
...	...	...	...	...	...	
...	...	...	...	...	...	
a_n	$a_n o a_1$	$a_n o a_2$				$a_n o a_n$

بند شی کلیہ: اگر جدول کے تمام حاصل ضرب عناصر S میں ہی ہوں تو ہم S کو بلحاظ 'o' بند کہتے ہیں۔

تلازمی کلیہ: اس کو ہم $\forall a, b, c \in S$ کے لیے $(a o b) o c = a o (b o c)$ جانچ کے پورا کرتے ہیں۔

اکائی کا وجود: اگر ٹاپ رو (Top Row) کسی بھی رو کے برابر ہو جس پر a_i $(1 \le i \le n)$ $a_i = e$ ہو تو S کی اکائی ہو گی۔

معکوس کا وجود: عملی جدول سے اگر $a_i \in e$ $\Rightarrow a_j = a_i$ ہو تب $a_i o a_j = e$ ہو گا۔ $a_i^{-1} = a_j$

نیز سارے متعلقہ روس اور اکالمس برابر ہوں تب 'o' تقلیبی ہو گا اور (S, o) کو تقلیبی گروپ کہا جائے گا۔

تعریف: تحت گروپ(Subgroup)

گروپ $(G, \bullet)$ کا تحت سٹ H، G کا تحت گروپ کہلاتا ہے اگر $(H, \bullet)$ خود میں ایک گروپ ہو۔اسے ہم $H < G$ سے ظاہر کرتے ہیں۔

نوٹ: (1) گروپ کی identity 'e' تمام تحت گروپ کی بھی identity ہوگی۔

(2) اگر H گروپ $(G,\bullet)$ کا تحت گروپ ہو تب

$$HH = H$$

$$H^{-1} = H$$

اور $HH^{-1} \subseteq H$ ہوگا۔

(3) ہر گروپ $(G \neq \{e\},\bullet)$ کے ہمیشہ دو تحت گروپس ہونگے جو $H = \{e\}$ اور $H = G$ ہیں۔

مثال: گروپ $G = \{1,-1,i,-i\}$ کے لیے $H = \{1\}$ اور $H = \{1,-1\}$ دو تحت گروپس ہیں۔

نظریات:

(1) **تحت گروپ کی ضروری اور کافی شرط**

(Necessary and Sufficient Condition for Subgroup)

گروپ G کا ایک غیر خالی سٹ H، G کا تحت گروپ ہوگا $\Leftrightarrow HH^{-1} \subseteq H$ (یعنی $ab^{-1} \in H \forall a,b \in H$)

(2) ایک متناہی سٹ H، گروپ G کا تحت گروپ ہوگا $\Leftrightarrow a.b \in H \forall a,b \in H$

(3) اگر H_1 اور H_2 گروپ $(G,\bullet)$ کے دو تحت گروپ ہیں تب $H_1 \cap H_2$ بھی G کی تحت گروپ ہے۔

نمونہ تجرباتی سوال

فرض کرو کہ $GL(2,\mathbb{R})$ ، 2×2 ماترس $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ کا سٹ ہے جہاں $a,b,c,d \in \mathbb{R}$ اور $ad - bc \neq 0$ ہیں۔ثابت کرو کہ بلحاظ ماترس کے ضرب کے $GL(2,\mathbb{R})$ ایک گروپ ہوگا۔

مقصد (Aim) : $(GL(2,\mathbb{R}), .)$ کو گروپ بتانا ہے۔

طرز عمل (Procedure) :

دئے گیئے سٹ $GL(2,\mathbb{R})$ کی پہچان کرنا اور بلحاظ ماترس کے ضرب کے گروپ کے چاروں کلّیوں کی جانچ کرنا۔

دیا گیا سٹ ہے $GL(2,\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \ / \ a,b,c,d \in \mathbb{R}, ad - bc \neq 0 \right\}$

فرض کرو کہ $B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$, $C = \begin{pmatrix} a_3 & b_2 \\ c_3 & d_3 \end{pmatrix} \in GL(2,\mathbb{R})$ جہاں $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$,

$a_1,b_1,c_1,d_1,a_2,b_2,c_2,d_2,a_3,b_3,c_3,d_3 \in \mathbb{R}$ ہیں۔

(i) بند شی کلّیہ (Closure law)

$$\forall \ A,B \in GL(2,\mathbb{R}) \quad ، \quad \det(A) = a_1d_1 - b_1c_1 \neq 0 \ ,$$
$$\det(B) = a_2d_2 - b_2c_2 \neq 0$$

$$AB=\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}$$

$$=\begin{pmatrix}a_1a_2+b_1c_2 & a_1b_2+b_1d_2\\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2\end{pmatrix}$$

اور ہمیں معلوم ہے کہ

$$\det(AB)=\det A.\det B\neq 0$$

$$\therefore\ A.B\in GL(2,\mathbb{R})$$

(ii) تلازمی کلّیہ (Associative law)

فرض کرو کہ $A=\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}$, $B=\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}$, $C=\begin{pmatrix}a_3 & b_2\\ c_3 & d_3\end{pmatrix}\in GL(2,\mathbb{R})$ ہیں۔

تب $(AB).C=\left[\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}\right].\begin{pmatrix}a_3 & b_2\\ c_3 & d_3\end{pmatrix}$

$$=\begin{pmatrix}a_1a_2+b_1c_2 & a_1b_2+b_1d_2\\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2\end{pmatrix}.\begin{pmatrix}a_3 & b_2\\ c_3 & d_3\end{pmatrix}$$

$$=\begin{pmatrix}a_1a_2a_3+b_1c_2a_3+a_1b_2c_3+b_1d_2c_3 & a_1a_2b_3+b_1c_2b_3+a_1b_2d_3+b_1d_1d_3\\ c_1a_2a_3+d_1c_2a_3+c_1b_2c_3+d_1d_2c_3 & c_1a_2b_3+d_1c_2b_3+c_1b_2d_3+d_1d_2d_3\end{pmatrix}\quad \text{--- (I)}$$

اسی طرح $A.(BC)=\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}.\left[\begin{pmatrix}a_2 & b_2\\ c_2 & d_2\end{pmatrix}\begin{pmatrix}a_3 & b_2\\ c_3 & d_3\end{pmatrix}\right]$

$$=\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}\begin{pmatrix}a_2a_3+b_2c_3 & a_2b_3+b_2d_3\\ c_2a_3+d_2c_3 & c_2b_3+d_2d_3\end{pmatrix}$$

$$=\begin{pmatrix}a_1a_2a_3+b_1b_2c_3+b_1c_2a_3+b_1d_2c_3 & a_1a_2b_3+a_1b_2d_3+b_1c_2b_3+b_1d_2d_3\\ c_1a_2a_3+c_1b_2c_3+d_1c_2a_3+d_1d_2c_3 & c_1a_2b_3+c_1b_2d_3+d_1c_2b_3+d_1d_2d_3\end{pmatrix}\quad \text{--- (II)}$$

$$\text{(I), (II)}\Rightarrow A.(B.C)=(A.B).C$$

اور

$$\det\left(A.(B.C)\right)=\det A.\det(BC)$$

$$=\det A.\left(\det B.\det C\right)$$

$$=\left[\det(A).\det(B)\right]\det C$$

$$= \det(AB).\det C$$

$$= \det\left[(AB).C\right]$$

$$(AB)C = A(BC) \quad \forall A,B,C,D \in GL(2,\mathbb{R}) \Leftarrow$$

$\Leftarrow$ "." تلازمی کلّیہ کو پورا کرتا ہے۔

(iii) اکائی کا وجود (Existence of Identity)

اگر ہم $a = d = 1$ اور $b = c = 0$ لیں تب $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R})$ اس طرح وجود رکھتا ہے کہ

$$\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{R})$$

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

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

تب $\forall A \in GL(2,\mathbb{R})$ ، $AI = IA = A$ ہو گا

$$\det(IA) = \det I.\det A = 1.\det A$$

اور $\det(AI) = \det A.\det I = \det A.1$

$$\therefore \det(AI) = \det(IA) \neq 0$$

$\Leftarrow$ $GL(2,\mathbb{R}), I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ کی اکائی ہے۔

(iv) معکوس کا وجود (Existence of inverse)

فرض کرو کہ $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{R})$ جہاں $\det(A) = ad - bc \neq 0$ ہے۔

$$B = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in GL(2,\mathbb{R})$$

اس طرح ہے کہ $A.B = \frac{1}{ad-bc}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$$A.B = \frac{1}{ad-bc}\begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

اور اسی طرح $BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ہو گا۔

$$\therefore AB = BA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \in GL(2,\mathbb{R})$$

اور $\det(AB) = \det A \det B$

$$\det(AB) = \det A \det\left(A^{-1}\right)$$

$$= \det A \det\left(A\right)^{-1} = \det I \neq 0$$

اس طرح ہر $GL\left(2,\mathbb{R}\right) \in A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ کا ایک $B = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ معکوس $GL\left(2,\mathbb{R}\right)$ میں وجود رکھتا ہے۔

$\Leftarrow (G, .)$ ایک گروپ ہے۔

17.2 عملی مسائل

17.2.1 عملی مسئلہ : بتلاؤ کہ سٹ $\mathrm{m}\mathbb{Z} = \{\ldots -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$ جہاں $\left(\mathrm{m} \in \mathbb{Z}^{+}\right)$ ہے ایک تقلیبی گروپ ہے۔

17.2.2 عملی مسئلہ: بتلاؤ کہ $G = \{2n / n \in \mathbb{Z}\}$ عمل ـــــــــ سے ایک ابیلین گروپ ہو گا۔

17.2.3 عملی مسئلہ :ثابت کرو کہ $(\mathbb{Z}, \oplus)$ ایک تقلیبی گروپ ہو گا۔ دیا گیا ہے کہ

$$a \oplus b = a + b + 1 \; \forall a, b \in \mathbb{Z}$$

17.2.4 عملی مسئلہ: بتلاؤ کہ $G=\{a+b\sqrt{2}/a,b\in\mathbb{Q}\}$ عمل '$+$' سے ایک تقلیبی گروپ ہوگا۔

17.2.5 عملی مسئلہ :ثابت کرو کہ $G = \{x / x \in \mathbb{Q}^+\}$ عمل 'o' کے تحت جس کی تعریف ہے
$aob = \frac{ab}{3} \forall a_1 b \in G$ ایک تقلیبی گروپ ہو گا۔

17.2.6 **عملی مسئلہ :ثابت کرو کہ** $G = \{0,1,2,...6\}$ $+_7$ **ایک ابیلین گروپ ہے۔**

17.2.7 عملی مسئلہ: بتلاؤ کہ $G = \{(a,b) / a,b \in \mathbb{R}, a \neq 0\}$ عمل 'o' کے تحت جس کی تعریف ہے

$(a,b)o(c,d) = (ac, bc+d)$ ایک غیر تقلیبی رنگ ہے۔ نیز بتلاؤ کہ $H = \{(1,b) / b \in \mathbb{R}\}$ اس کا تحت گروپ ہے۔

17.2.8 عملی مسئلہ: بتلاؤ کہ (i) $H_1 = \{0,2,4\}$

اور (ii) $H_2 = \{0,3\}$

$(\mathbb{Z}_6 +_6)$ کے تحت گروپس ہیں۔ کیا $H_1 \cup H_2$ تحت گروپ ہے؟ وضاحت کرو۔

اکائی18۔ ہم سٹس–نارمل تحت گروپس اور خارج قسمت گروپس

(Cosets – Normal Subgroups and Quotient Groups)

18.0 مقصد

اس اکائی میں طلباء ہم سٹس، نارمل تحت گروپس اور خارج قسمت گروپس کے کئی مسائل کے بارے میں جانکاری حاصل کرکے انہیں حل کریں گے۔

18.1 تعارف

فرض کرو کہ $(G,\bullet)$ ایک گروپ ہے اور H اسکا تحت گروپ $a \in G$ کے لیے سٹ $aH = \{ah / h \in H\}$ کو G میں H کا بایاں ہم سٹ کہیں گے اور $Ha = \{ha / h \in H\}$ کو G میں H کا دایاں ہم سٹ کہیں گے۔ واضح ہے کہ $aH, Ha \subseteq G$ اگر G کا عمل '$+$' ہو تب $a + H = \{a + h / h \in H\}$ اور $H + a = \{h + a / h \in H\}$، H کے G میں بایاں اور دایاں ہم سٹس ہیں۔

نوٹ: اگر H، G کا تحت گروپ ہے اور $a, b \in G$ تب $a(bH) = (ab)H$ اور $|aH|$، $|Ha|$ اس عدد کو ظاہر کرتے ہیں جتنے کے aH اور Ha میں عناصر ہوں۔

مثال: گروپ $(\mathbb{Z}, +)$ کی $H = \{3n / n \in \mathbb{Z}\} = \{\ldots -9, -6, -3, 0, 3, 6, 9\}$ ایک تحت گروپ ہے اور اس کے ہم سٹس ہیں۔

$$H + 0 = H$$
$$H + 1 = \{\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\}$$
$$H + 2 = \{\ldots -7, -4, -1, 2, 5, 8, 11, \ldots\}$$
$$H + 3 = \{\ldots -6, -3, 0, 3, 6, 9, \ldots\} = H$$
$$H + 4 = \{\ldots -5, -2, 1, 4, 7, 10, \ldots\} = H + 1$$
$$H + 5 = \{\ldots -4, -1, 2, 5, 8, 11, \ldots\} = H + 2$$
$$H + 6 = H + 3 = H$$

اسی طرح $H = H + 6 = H + 9 = H + 12 \ldots\ldots$ ہیں اور $H + 0$، $H + 1$، $H + 2$ ہی H کے مختلف ہم سٹس ہیں۔

مثال : $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\} = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ مبادلوں کے ضرب (Product of Permutations) سے ایک گروپ ہے۔ اور $H = \{(1), (1\,3)\}$، S_3 کا تحت گروپ اور ذیل کے سٹس S_3 میں H کے left cosets ہیں۔

$$(1).H = \{(1)(1), (1)(1,3)\} = \{(1), (1,3)\} = H \text{ کے لیے } (1) \in G$$
$$(1\,2)H = \{(1\,2)(1), (1\,2)(13)\} = \{(1\,2), (1,3\,2)\}$$

$$(1\,3)H = \{(1\,3)(1),(1\,3)(13)\} = \{(1\,3)\}$$

$$(2\,3)H = \{(2\,3)(1),(2\,3)(13)\} = \{(2\,3),(1,2\,3)\}$$

$$(1\,2\,3)H = (2\,3)H$$

$$(1\,3\,2)H = (1\,2)H$$

تحت گروپ کے خصوصیات

(1) اگر H، گروپ G کا تحت گروپ ہو تب $h \in G$ کے لیے $Hh = hH = H$ ہو گا۔

(2) $Ha = Hb \Leftrightarrow ab^{-1} \in H$

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

(3) اگر H، گروپ G کا تحت گروپ ہے تب H کے تمام بائیں ہم سٹس اور H کے تمام دائیں ہم سٹس کے درمیان ایک bijection ہو گا۔

(4) اگر G ایک متناہی گروپ اور H اس کا تحت گروپ ہو تب $|G : H| = \frac{|G|}{|H|}$ وہ عدد ہے جتنے کہ H کے G میں ہم سٹس ہیں۔

Lagrange کا نظریہ:

متناہی گروپ G کے ہر تحت گروپ کا رتبہ G کے رتبہ کو تقسیم کرتا ہے۔

تعریف: گروپ $(G,\bullet)$ کا ایک تحت گروپ H نارمل (Normal) کہلاتا ہے۔

$$xhx^{-1} \in H \ \forall x \in G \forall h \in H \quad \Leftrightarrow$$

$$x^{-1}hx \in H \ \forall x \in G \forall h \in H \quad \text{یا}$$

$$Hx = xH \ \forall x \in G \quad \text{یا}$$

$$\forall x \in G \quad xHx^{-1} = H \quad \text{یا}$$

نظریات:

(1) ایک تحت گروپ H، گروپ G کا نارمل تحت گروپ ہے $\Leftrightarrow$ H کے دو دائیں ہم سٹس کا حاصل ضرب بھی دایاں ہم سٹ ہو گا۔

(2) تقلیبی گروپ کا ہر تحت گروپ نارمل ہے۔

(3) گروپ $(G,\bullet)$ کا ایسا تحت گروپ H جس کا index 2 ہو نارمل ہو گا۔

(4) دو نارمل تحت گروپس کا تقاطع (intersection) بھی نارمل ہو گا۔

خارج قسمت گروپ یا فیاکٹر گروپ(Quotient Group / Factor Group)

اگر H گروپ G کا ایک نارمل تحت گروپ ہو تب سٹ $G/H=\{Ha/a\in G\}$ تمام دائیں ہم سٹس کا سٹ بلحاظ $(Ha)(Hb)=Hab\ \forall Ha,Hb\in G/H$ ایک گروپ ہو گا جسے ہم خارج قسمت گروپ یا Factor Group کہتے ہیں۔ اس گروپ میں $He=H$ ، G/H کی اکائی ہے۔

رزلٹ ہیں :

(1)اگر گروپ G متناہی ہے اور H نارمل تحت گروپ تب $|G/H|=\frac{|G|}{|H|}$ ہو گا۔

(2)ابیلیس گروپ کا خارج قسمت گروپ بھی ابیلیس ہو گا۔

18.2 عملی مسائل

18.2.1 عملی مسئلہ : $U(32)=\{1,3,5,7,6,11,13,15,19,21,23,25,27,29,31\}$ گروپ کے تحت گروپ $H=\{1,15\}$ کے تمام ہم سٹس معلوم کرو۔

18.2.2 عملی مسئلہ: (i) عملی مسائل: اگر $H = \{1,11\}$، $U(30)$ کا تحت گروپ ہو تب $\frac{|U(30)|}{|H|}$ معلوم کرو۔

(ii) Factor Group $\frac{\mathbb{Z}_{60}}{\langle 5 \rangle}$ کا رتبہ (Order) معلوم کرو۔

18.2.3 عملی مسئلہ: کیا $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \ / \ a,b,d \in \mathbb{R}, ad \neq 0 \right\}$، $GL(2, \mathbb{R})$ کا نارمل تحت گروپ ہے؟

18.2.4 عملی مسئلہ: $\mathbb{Z}_{36}$ کے تحت گروپ $H = \langle 18 \rangle$ کے تمام ہم سٹس معلوم کرو۔

18.2.5 عملی مسئلہ: تحت گروپ $\left(H = \{0,3,6,9,12\} \ +_{15}\right)$ کے لیے گروپ $(\mathbb{Z}_{15}, +_{15})$ میں تمام بائیں ہم سٹس معلوم کرو۔ نیز $\mathbb{Z}_{15}$ میں اس تحت گروپس H کا index معلوم کرو۔

18.2.6 عملی مسئلہ: $\mathbb{Z}_{36}$ کے تحت گروپ $H = \langle 9 \rangle$ کے تمام بائیں ہم سٹس معلوم کرو۔

اکائی19۔مبادلہ گروپس اور سائکلی گروپس

(Permutation Groups and Cyclic Groups)

19.0 مقصد

اس اکائی میں طلباء مبادلوں کے اور سائکلی گروپ کے مسائل کو حل کریں گے۔

19.1 تعارف

ایک مبادلہ ایک سٹ S پر ایسا نقش ہے $f:S\to S$ جو $1-1$ اور بر ہے۔

مثال: $f:\mathbb{R}\to\mathbb{R}$ جس کی تعریف $f(x)=x+1$ ہو $\mathbb{R}$ پر ایک مبادلہ(Permutation)ہے۔

اگر $S=\{a_1,a_2,a_3,...a_n\}$ تب ایک نقش $f:S\to S$ جو $1-1$ اور بر ہو درجہ n والا مبادلہ کہلاتا ہے۔ اور اسے $f=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ b_1 & b_2 & \dots & b_n\end{pmatrix}$ سے ظاہر کرتے ہیں جہاں $b_1,b_2,...b_n\in S$ اور $b_1=f(a_1)\ b_2=f(a_2)$ ۔۔۔۔۔۔۔۔$b_n=f(a_n)$ ہیں۔ $S=\{a_1,a_2,a_3,...a_n\}$ پر دو مبادلے f,g مساوی ہونگے اگر $f(a)=g(a)\quad\forall a\in S$ ہو۔

اگر $f=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ b_1 & b_2 & \dots & b_n\end{pmatrix}$ اور $g=\begin{pmatrix}b_1 & b_2 & \dots & b_n\\ c_1 & c_2 & \dots & c_n\end{pmatrix}$ کوئی دو مبادلے $S=\{a_1,a_2,a_3,...a_n\}$ پر ہوں تب ان کا ضرب اس طرح دیا جاتا ہے۔ $gof=gf=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ c_1 & c_2 & \dots & c_n\end{pmatrix}$ ۔

یہاں $\forall i=1,2,3,...\text{n}\quad gf=gof(a_i)=\text{g}(f(a_i))$ ہے۔اور سٹ $S_n=\{f/f:S\to S\}$ ایک گروپ بنے گا دیے گئے ضرب کے تحت۔ نیز $|S_n|=n!$ اور $I=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ a_1 & a_2 & \dots & a_n\end{pmatrix}$، S_n کی اکائی ہے۔ اس گروپ کو مبادلہ گروپ یا سمٹرک گروپ کہتے ہیں۔

مثال: اگر $S=\{1,2,3\}$ ہو تب

$$S_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$$ ہے اور $|S_3|=3!=6$

اگر $f=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ b_1 & b_2 & \dots & b_n\end{pmatrix}\in S_n$ ہو تب $f^{-1}=\begin{pmatrix}b_1 & b_2 & \dots & b_n\\ a_1 & a_2 & \dots & a_n\end{pmatrix}$ ہو گا۔

سائکلی مبادلہ(Cyclic Permutation)

فرض کرو کہ $S=\{a_1,a_2,a_3,...a_n\}$ ہے اور $f=\begin{pmatrix} a_1 & a_2 & a_3 & . & . & a_k & a_{k+1} & . & . & a_n \\ a_2 & a_3 & a_4 & . & . & a_1 & a_{k+1} & . & . & a_n \end{pmatrix}$، S پر ایک Permutation ہے۔

یہاں $f(a_1)=a_2\ f(a_2)=a_3$------ $f(a_k)=a_1\ f(a_{k+1})=a_{k+1}\ f(a_n)=a_n$

اس قسم کے مبادلے کو k طول والا سائکل مبادلہ یا $k-Cycle$ کہتے ہیں۔اسے $(a_1,a_2,a_3,...a_k)$ سے ظاہر کرتے ہیں۔ $2-cycle$ کو ٹرانسپوزشن(Transposition) کہتے ہیں۔

نوٹ: ہر مبادلے کو مختلف cycles کے حاصل ضرب میں ظاہر کر سکتے ہیں اور ہر Cycle کو transposition کے حاصل ضرب میں اس طرح لکھ سکتے ہیں۔

$$(a_1a_2....a_n)=(a_1\ a_n)(a_1\ a_{n-1})(a_1\ a_{n-2})....(a_1\ a_2)$$

مثال: $S=\{1,2,3,4,5,6,7,8,9\}$ پر $f=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 1 & 4 & 3 & 2 & 5 & 7 & 8 & 9 \end{pmatrix}$ ایک مبادلہ ہے جو

$f=(1\ \ 6\ \ 5\ \ 2)(3\ \ 4)(7)(8\ \ 9)$ کے برابر ہے۔ $=(1\ \ 2)(1\ \ 5)(1\ \ 6)(3\ \ 4)(8\ \ 9)$ کے برابر ہے۔

(چوں کہ (7) اکائی ہے)

تعریف(جفت اور طاق مبادلیں)

تعریف: سائکل گروپ(Cycle Group):ایک گروپ $(G,.)$ سائکلی کہلاتا ہے اگر ایک عنصر $a\in G$ اس طرح وجود رکھتا ہے کہ ہر $x\in G$ کے لیے $n\in\mathbb{Z}\ \ x=a^n$ ہوگا۔اس 'a' کو سائکلی گروپ G کا generator کہتے ہیں اور G کو $G=\langle a\rangle$ سے ظاہر کرتے ہیں۔

مثال: گروپ $G=\{1,-1,i,-i\}=\langle i\rangle=\langle -i\rangle$ اس گروپ کے i اور $-i$ دو جنریٹرس ہیں۔

سائکلی گروپس کی چند خصوصیات

(1) ہر سائکل گروپ ابیلین گروپ ہے۔

(2) اگر سائکلی گروپ G کا 'a' generator ہو تب a^{-1} بھی G کا generator ہوگا۔

(3) سائکلی گروپ کا ہر تحت گروپ سائکلی ہے۔

(4) اگر G ایک متناہی گروپ ہے $|G|=n$ اور اگر $a\in G$ اس طرح ہو کہ $(o(a)=n)$ تب G سائکلی گروپ ہوگا۔

(5) اگر $G=\langle a\rangle$ ایک سائکلی گروپ ہے اور $(o(a)=n)$ تب a^m بھی G کا generator ہوگا $\Leftrightarrow g\cdot c\cdot d(mn)=1$

(6) اگر سائکلی گروپ $G=\langle a\rangle$ کا رتبہ n(Order) ہو تب G کے $\phi(n)$ generator ہوں گے جہاں $\phi(n)$، Euler's $\phi-function$ ہے۔

19.2 عملی مسائل

19.2.1 عملی مسئلہ: ذیل میں دیے گئے ضربوں کو ذسجائنٹ سائکلس میں لکھو:

(i) $(132)(567)(261)(45)$ (ii) $(136)(1357)(67)(1234)$

19.2.2 عملی مسئلہ: ذیل کے کون سے مبادلے جفت یا طاق ہیں۔

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 7 & 6 & 2 & 5 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 6 & 1 & 7 & 9 & 8 \end{pmatrix}$

19.2.3 عملی مسئلہ: اگر $f = (1\ 2\ 3\ 4\ 5\ 6)$ ہو

تب بتلاؤ کہ $f^2 = (2\ 4\ 6)(1\ 3\ 5)$ اور $f^3 = (1\ 4)(2\ 5)(3\ 6)$

19.2.4 عملی مسئلہ: اگر $\mu \in S_6$ اس طرح ہیں کہ $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$ $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$

تب

(i) $\sigma^2\mu$ (ii) μ^{2009} (iii) σ^{2009} معلوم کرو۔

19.2.5 عملی مسئلہ: بتلاؤ کہ $G = \{1, 2, 3, 4, 5, 6\} \times 7$ ایک سائکل گروپ ہے۔اس کے تمام generators معلوم کرو۔

19.2.6 عملی مسئلہ: ذیل میں دیے گئے رتبہ والے سائکلی گروپس کے کتنے generator ہوں گے؟

(i) 5 (ii) 15 (iii) 60

اکائی20۔ گروپ کی ہم مارفیت اور یکمارفیت

(Homomorphisms and Isomorphisms in Groups)

20.0 مقصد

اس اکائی میں طلباء ہم مارفیت اور یکمارفیت کے مسائل کے بارے میں جانکاری حاصل کریں گے اور ان کے حل دریافت کریں گے۔

20.1 تعارف

اگر $(G, .)$ اور $(G', .)$ دو گروپس ہوں ایک تفاعل $f: G \to G'$ ، G سے G' میں ہم مارفیت کہلاتا ہے اگر $f(a.b) = f(a).f(b) \quad \forall a, b \in G$۔ اگر f ہر (onto) ہو تو f کو برہم مارفیت (onto homomorphism) کہتے ہیں اور چوں کہ $f(G) = G'$ ہے۔ G' کو G کی ہم مارفی امیج (homomorphic image) کہتے ہیں۔ ہم مارفیت $f: G \to G'$ جو 1-1 ہو مونومارفزم (monomorphism) کہلاتا ہے اور وہ ہم مارفیت جو G سے G میں جائے اسے endomorphism کہتے ہیں۔

تعریف: یک مارفیت (Isomorphism) :

ایک ہم مارفیت $f: G \to G'$ جو 1-1 اور onto ہو یکمارفیت کہلاتی ہے۔ یہاں $f(G) = G'$ ہے اور G' کو G کی یکمارفی امیج کہتے ہیں۔ یکمارفیت $f: G \xrightarrow{\text{on to}} G$ کو G پر آٹومارفزم (automorphism) کہتے ہیں۔

مثال: اگر $G = (\mathbb{Z}, +)$ اور $G' = (\{1. -1\}, .)$ دو گروپ ہیں اور $f: G \to G'$ کی تعریف اس طرح کی گئی ہے۔

$f(n) = 1$ (n جفت ہے) ، $f(n) = -1$ (n طاق ہے)

اگر $y \in G'$ ہو تب $y = 1$ یا $y = -1$ ہے۔

اگر ایک $n \in \mathbb{Z}$ ہو اس طرح کہ $f(n) = 1$ یا $f(n) = -1 \Leftarrow f$ برتفاعل ہے۔

فرض کرو کہ $n_1, n_2 \in G(= \mathbb{Z})$۔ اگر n_1, n_2 دونوں جفت ہو تب $f(n_1) = 1, f(n_2) = 1$ اور $n_1 + n_2$ بھی جفت ہے۔

$$\therefore f(n_1 + n_2) = 1 = 1.1 = f(n_1).f(n_2)$$

اگر n_1, n_2 طاق ہوں تب $n_1 + n_2$ جفت ہے اور $f(n_1 + n_2) = 1$ تب

$$\therefore f(n_1 + n_2) = 1 = (-1).(-1) = f(n_1).f(n_2)$$

اسی طرح اگر n_1 جفت اور n_2 طاق ہو تب بھی $\forall n_1, n_2 \in G \quad f(n_1 + n_2) = f(n_1).f(n_2)$ ہوگا

$\Leftarrow f: G \to G'$ onto ہم مارفیت ہوگا۔

20.2 عملی مسائل

20.2.1 فرض کرو کہ $G = \left(\mathbb{R}^+, .\right)$ اور $G' = \left(\mathbb{R}^+, +\right)$ اگر $\varnothing : G \to G'$ کی تعریف اس طرح ہے کہ $\varnothing\left(x\right) = \log_{10}^{x}$ تب بتلاؤ کہ $\varnothing$ یک مافیت ہے۔

20.2.2 عملی مسئلہ :ثابت کرو کہ ہر لامتناہی سائکل گروپ $\mathbb{Z}$ سے isomorphic ہے۔

20.2.3 عملی مسئلہ: ہر متناہی سائکل گروپ G جو 'a' سے generated ہے اور اگر $o(a) = n$ ہو $\mathbb{Z}_n$ سے isomorphic ہو گا۔

20.2.4 عملی مسئلہ: بتلاؤ کہ $U(10) \approx \mathbb{Z}_4$ اور $U(5) \approx \mathbb{Z}_4$

20.2.5 عملی مسئلہ: بتلاؤ کہ نقش $f:\mathbb{C}_+,\to\mathbb{C}_+$ جس کی تعریف $f(a+ib)=a-ib$ ہے ایک آٹومارفزم ہے۔

20.2.6 عملی مسئلہ: $(\mathbb{R}, +)$ اور $\mathbb{R}^o = (\mathbb{R} - \{0\}, .)$ دو گروپس ہیں۔ اگر $f : \mathbb{R}, \to \mathbb{R}^o$ کی تعریف $f(x) = e^x$ ہو تو بتلاؤ کہ f ایک یک مارفیت ہے۔

بلاک۔ 6

اس بلاک میں چار اکائیاں ہیں (21-24)۔ طلباء یونٹ -21 میں رنگس، انتگرال دامنہ اور فیلڈز کے تصورات کو جانیں گے۔ اگلی اکائی -22 میں تحت رنگ، ایدیال اور رنگ ہم مارفیت (ring homomorphism) کے مثالیں اور عملی مسائل دیے گئے ہیں۔ اگلی دو اکائیوں 23 اور 24 میں طلباء پریمٹیو کثیر رکنی (Primitive Polynomial) اور آئزن اسٹین کی کسوٹی اور ان سے متعلق عملی مسائل کو حل کر سکیں گے۔

اکائی 21۔ رنگ، انتگرال دامنہ اور فیلڈز

(Ring – Integral Domain & Fields)

21.0 مقصد

اس اکائی میں طلباء رنگ، انتگرال دامنہ اور فیلڈز کے مسائل کو جانیں گے اور ان کا حل معلوم کریں گے۔

21.1 تعارف (Introduction)

رنگ کی تعریف: رنگ ایک ایسا غیر خالی سٹ R ہے جو دو ثنائی اعمال $(+)$ اور $(.)$ سے درج ذیل اصول کی تکمیل کرتا ہے۔

(I) $(R,+)$ ایک ایبیلین گروپ ہے۔

(II) $(R,.)$ ایک نصف گروپ ہے۔

(III) $a.(b+c)=a.b+a.c$ ، $(a+b).c=a.c+b.c \quad \forall a,b\in\mathbb{R}$

اس رنگ کو $(R,+,.)$ سے بھی ظاہر کرتے ہیں۔

اس رنگ $(R,+,.)$ میں اگر ایک عنصر جسے ہم '1' سے ظاہر کرتے ہیں اس طرح وجود رکھتا ہو کہ $a.1=1.a=a \quad \forall\ a\in R$ تب $(R,+,.)$ کو ہم اکائی کے ساتھ والا رنگ کہتے ہیں۔ اگر $(R,+,.)$ میں $a.b=b.a \quad \forall\ a,b\in R$ ہو تو R کو commutative ring یا تقلیبی رنگ کہتے ہیں۔

مثال 1 : $(\mathbb{Z},+,.)$ اکائی کے ساتھ ایک تقلیبی رنگ ہے۔

مثال 2 : $(\mathbb{Q},+,.)$، $(\mathbb{R},+,.)$ اور $(\mathbb{C},+,.)$ بھی اکائی کے ساتھ والا تقلیبی رنگس (Commutative Rings with Unity) ہیں۔

مثال 3 : 2×2 ماترس والا سٹ $M_2(\mathbb{Z})=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in \mathbb{Z}\right\}$ جس کے عناصر صحیح اعداد ہوں ماترس کے جمع '+' اور ضرب '.' سے ایک اکائی کے ساتھ غیر تقلیبی رنگ ہے۔اس کی اکائی $I_2=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ہے۔

مثال 4 : $\left(\mathbb{Z}_m=\{0,1,2,-----m-1\},+_m,\times_m\right)$ ایک رنگ ہے۔

تعریف : (یونٹ) فرض کرو کہ $(R,+,.)$ ایک رنگ ہے۔ ایک عنصر $u\in R$، R کا یونٹ کہلاتا ہے اگر اس کا ضربی معکوس (multiplicative reverse) R میں وجود رکھتا ہو۔یعنی ایک $v\in R$ اس طرح ہوگا کہ $uv=vu=1$۔

رنگس کی کچھ بنیادی خصوصیات(Some Basic Properties of Rings) :

(1) کسی رنگ $(R,+,.)$ میں $0,a,b\in R$ کے لیے

i. $0.a=a.0=0$ ہوگا۔

ii. $a(-b)=(-a)b=-(ab)$ ہے۔

iii. $(-a)(-b)=ab$ اور

iv. $a(b-c)=ab-ac$ ہوگا

بولین رنگ(Boolean Ring): ایسا رنگ $(R,+,.)$ بولین رنگ کہلاتا ہے اگر ہر $a\in R$ کے لیے $a^2=a$ ہو۔بولین رنگ R میں ہر $a,b\in R$ کے لیے $a+a=0$، $a+b=0\Rightarrow a=b$ اور $\forall a,b\in R$ $a.b=b.a$ ہوتے ہیں۔

صفر کا قاسم (Zero Divisors) : ایک عنصر $a\neq 0\in R$، R کا صفر کا قاسم (zero divisor) کہلاتا ہے اگر $b\neq 0\in R$ اس طرح وجود رکھتا ہے کہ $a.b=0$ یا $b.a=0$ ہو۔

مثال 1 : رنگ $R=\{0,1,2,3,4,5\}+_6\ \times_6$ میں $2\times_6 3=0$ ہے اور $3\times_6 4=0$ اس لیے $2,3,4\in R$، R کے zero divisors ہیں۔

مثال 2 : $\left(M_2(\mathbb{Z}),+,.\right)$ کے لیے $A=\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\neq 0,\ B=\begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}\neq 0$ ہیں۔اور $AB=O$ ہے۔اس لیے A اور B دونوں $\left(M_2(\mathbb{Z}),+,.\right)$ کے zero divisors ہیں۔

انتگرال دامنہ (Integral Domain) ایک اکائی والی تقلیبی رنگ D جس میں zero divisors نہ ہوں انتگرال دامنہ کہلاتی ہے۔

مثال: $(\mathbb{Z},+,.)$ ایک Integral Domain ہے۔

رزلٹس:

(1) ایک فیلڈ کے zero divisors نہیں ہوں گے۔

(2) ہر فیلڈ انتگرال دامنہ ہے اور اس کا معکوس صحیح نہیں۔

(3) ہر متناہی انتگرال دامنہ field ہو گا۔

(4) اگر p ایک prime number ہو تب $\mathbb{Z}_p = \{0,1,2,...p-1\} +_p \times_p$ ایک field ہے۔

21.2 عملی مسائل

21.2.1

(i) $\mathbb{Z}_{14}$ کے سارے یونٹس (Units) معلوم کرو

(ii) $M_2(\mathbb{Z}_2)$ کے تمام Units معلوم کرو

21.2.2

(i) $\mathbb{Z}_3[i]$ پر $x^2 - x + 2 = 0$ کے تمام حل معلوم کروا گر وجود رکھتے ہوں تو۔

(ii) $\mathbb{Z}_{14}$ پر $x^2 + x - 6 = 0$ کے حل معلوم کرو۔

21.2.3 بتلاؤ کہ $\mathbb{R} = \{0, 2, 4, 6\}$ $+_8$ $\times_8$ ایک رنگ ہے۔

21.2.4 ثابت کرو کہ $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \quad / \ a, b \in \mathbb{Q}\right\}$ ایک field ہے جس کے ثنائی اعمل '+' اور '.' ہیں۔

21.2.5 بتلاؤ کہ $\mathbb{R} = \{0,1,2,3,4,5,6\} +_7 \times_7$ ایک فیلڈ ہو گا۔

اکائی22۔ تحت رنگ، ایدیال، خارج قسمت رنگ اور ہم مارفیت

(Subrings – Ideals – Quotient Rings and Homomorphisms)

22.0 مقصد

اس اکائی میں مواد کے مختصر تعارف کے بعد طلباء رنگس، ایدیال اور خارج قسمت رنگس کے مختلف عملی مسائل کی مشق کریں گے۔

22.1 تعارف

ایک غیر خالی سٹ S، رنگ $(R,+,.)$ کی تحت رنگ (subring) کہلاتی ہے اگر $(S,+,.)$ خود میں ایک رنگ ہو۔

نوٹ: R کا صفر عنصر 0، S کا بھی zero element ہوگا۔

مثال 1 : $S=\{2n / n\in\mathbb{Z}\}$ جفت صحیح اعداد کا سٹ $(\mathbb{Z},+,.)$ کی تحت رنگ ہے۔

مثال 2 : $(\mathbb{Z},+,.)$، $(\mathbb{Q},+,.)$ تحت رنگس ہے $(\mathbb{R},+,.)$ کے۔

مثال 3 : $S=\left\{\begin{bmatrix} p & 0\\ 0 & q\end{bmatrix} / \ p,q\in\mathbb{Z}\right\}$، $M_2(\mathbb{Z})=\left\{\begin{bmatrix} a & b\\ c & d\end{bmatrix} / \ a,b,c,d\in\mathbb{Z}\right\}$ کی بلحاظ '+' اور '.' تحت رنگ ہے۔

مثال 4 : گاسین (Gaussian) صحیح اعداد کا رنگ $\mathbb{Z}[i]=\{a+ib \ / \ a,b\in\mathbb{Z}\}$، $(\mathbb{C},+,.)$ کا تحت رنگ ہے۔

تحت رنگ کی ضروری اور کافی شرط (Necessary and Sufficient Condition for Subrings)

ایک غیر خالی سٹ S کسی رنگ $(R,+,.)$ کا تحت رنگ ہوگا۔

$$\Leftrightarrow \quad \text{(i)} \quad a-b\in S \ \ \forall a,b\in S \qquad \text{(ii)} \quad a\cdot b\in I \ \ \forall a,b\in I$$

نظریہ: کسی رنگ $(R,+,.)$ دو تحت رنگس کا تقاطع بھی R کا تحت رنگ ہے۔

نوٹ: دو تحت رنگس کا اتحاد کا تحت رنگ ہونا ضروری نہیں ہے۔ جسے ہم اس مثال کے ذریعہ جان سکتے ہیں $(\mathbb{Z},+,.)$ کے $S_1=\{2n \ / n\in\mathbb{Z}\}$، $S_2=\{3n \ / n\in\mathbb{Z}\}$ دو تحت رنگس ہیں لیکن $S_1\cup S_2$، $(\mathbb{Z},+,.)$ کا تحت رنگ نہیں ہے۔ چوں کہ $2,3\in S_1\cup S_2$ ہے لیکن $2+3=5\notin S_1\cup S_2$۔

تعریفات : رنگ $(R,+,.)$ کا ایک تحت سٹ I، R کا بایاں ایدیال (left ideal) کہلاتا ہے اگر

(i) $a-b\in I \ \ \forall a,b\in I$ یعنی $(I,+)$، $(R,+)$ کا تحت گروپ ہے۔

(ii) $rs\in I \ \ \forall r\in R, \ s\in I$

I، R کا دایاں ایدیال (right ideal) کہلاتا ہے اگر

(i) $a-b\in I \ \ \forall a,b\in I$ اور

$sr \in I \quad \forall r \in R,\ s \in I$ (ii)

I، R کا ایدیال (Ideal) کہلاتا ہے اگر

$a-b \in I \quad \forall a,b \in I$ اور (i)

$rs, sr \in I \quad \forall r \in R,\ s \in I$ (ii)

مثال: ایک مثبت صحیح عدد n کے لیے $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, ---\}$، $(\mathbb{Z}, +, .)$ کا ideal ہے۔

نوٹ: ہر رنگ $(R \neq (0), +, .)$ کے ہمیشہ دو ایدیال ہوں گے $I = \{0\}$ اور $I = R$ انہیں improper ایدیال کہتے ہیں۔

رزلٹس:

(1) اگر U، R کا ایک ایدیال ایسا ہے کہ $1 \in U$ تب $U = R$ ہو گا۔

(2) کسی بھی فیلڈ کے proper ایدیال نہیں ہوں گے۔

(3) اگر R ایک تقلیبی رنگ ہے اور $a \in R$ تب $Ra = \{ra / r \in \mathbb{R}\}$، R کا ایدیال ہے اور اسے ہم Principal ایدیال کہتے ہیں جسے (a) سے ظاہر کرتے ہیں۔

پرنسپل ایدیال رنگ (Principal Ideal Ring): اکائی کے ساتھ والا تقلیبی رنگ R کا ہر ایدیال اگر پرنسپل ایدیال ہو تب R کو پرنسپل ایدیال رنگ کہتے ہیں۔

مثال 1 : ہر فیلڈ پرنسپل ایدیال رنگ ہے۔

مثال 2 : $(\mathbb{Z}, +, .)$ ایک پرنسپل ایدیال رنگ ہے۔

تعریف: خارج قسمت رنگ (Quotient Ring) یا فیاکٹر رنگ (Factor Ring).

اگر S رنگ R کا ایدیال ہے تب $R / S = \{S + x / x \in \mathbb{R}\}$ بہ لحاظ

$$(S + x) + (S + y) = S + (x + y)$$

$$(S + x)(S + y) = S + (xy)$$

$$\forall\ S + x, S + y \in R / S$$

ایک رنگ ہو گا جسے ہم خارج قسمت رنگ یا Factor Ring کہتے ہیں۔

نوٹ : (I R تقلیبی $\Leftarrow R / S$ بھی تقلیبی ہو گا۔

(II R اگر اکائی کے ساتھ ہو تو R / S بھی اکائی کے ساتھ ہو گا۔

پرائم ایدیال (Prime Ideal): ایک تقلیبی رنگ R کا ایدیال P، پرائم ایدیال کہلائے گا اگر $a,b \in R$ کے لیے $b \in P$ یا $a \in P$، $a.b \in P \Rightarrow$۔

مثال: ایدیال (3) $(\mathbb{Z}, +, .)$ کا Prime ایدیال ہے۔

عظیمی ایدیال(Maximal Ideal)

ایک ایدیال $M(\neq R)$ کسی رنگ R کا maximal ایدیال کہلاتا ہے اگر ہر ایدیال U کے لیے $U = R$ یا $U = M$

$M \subseteq U \subseteq R \Rightarrow$۔

مثال: پرنسپل ایدیال (2) اور (3) رنگ $(\mathbb{Z}, +, .)$ کے maximal ایدیال ہیں۔

نظریات:

(1) اگر R اکائی والا تقلیبی رنگ ہے تب R کا کوئی ایدیال P پرائم ہوگا $\Leftrightarrow R/P$ ایک انتگرال دامنہ ہے۔

(2) $(\mathbb{Z}, +, .)$ کا ایدیال maximal ہوگا $\Leftrightarrow$ وہ کسی پرائم صحیح عدد سے generated ہو۔

(3) اکائی کے ساتھ والا تقلیبی رنگ R کا ایدیل M عظیمی (maximal) ہوگا $\Leftrightarrow R/M$ ایک فیلڈ ہے۔

ہم مارفیت(Homomorphism)

ایک تفاعل $f: R \to R'$ ، R کی ہم مارفیت R' میں کہلاتا ہے اگر $f(a+b) = f(a) + f(b), \forall a, b \in R$ اور $f(ab) = f(a)f(b)$ اگر f ہر تفاعل ہو تب f کو برہم مارفیت (onto homomorphism) کہتے ہیں۔ یہاں $f(R) = R'$ ہوگا اور R' کو R کی ہوموارفک امیج کہتے ہیں۔

اگر f، 1-1، onto اور ہم مارفیت ہو تو f کو یکمارفیت (Isomorphism) کہتے ہیں اور R' کو R کا Isomorphic Image کہتے ہیں۔

اگر $f: R \to R$ ایک isomorphism ہو تو f کو آٹومارفزم (auto morphism) کہتے ہیں۔

ہم مارفیت کے خصوصیات(Properties of Homomorphism) :

(1) اگر $\phi: R \to R'$ ایک ہم مارفیت ہو اور o', o R اور R' کے zero عناصر ہوں تب

$$\phi(o) = o'$$

$$\phi(-a) = -\phi(a)$$

$$\phi(a-b) = \phi(a) - \phi(b) \quad \forall a, b \in R$$

(2) اگر $\phi: R \to R'$ ایک رنگ ہم مارفیت R سے R' میں ہو اور اگر A، R کا تحت رنگ ہو تب $\phi(A)$، R' کا تحت رنگ ہوگا۔

(3) اگر $\phi: R \xrightarrow{onto} R'$ ایک ہم مارفیت ہو تب $\phi(A)$، R' کا ایدیال ہوگا۔ R کے ہر ایدیال A کے لیے۔

(4) ہر رنگ کا ہم مارفی امیج رنگ ہوگا۔

(5) تقلیبی رنگ کا ہم مارفی امیج تقلیبی رنگ ہوگا۔

ہم مارفیت کا کرنل(Kernel of a Homomorphism):

اگر $\phi: R \to R'$ ایک ہم مارفیت ہو تب ϕ کا کرنل جسے ہم $\ker \phi$ سے ظاہر کرتے ہیں کی تعریف ہے۔

$$K = \ker\phi = \{x \in \mathbb{R} \ / \phi(x) = o'\}$$

نظریات:

(1) $\ker\phi$ ، R کا ایدیال ہوگا۔

(2) ایک ہم مارفیت $\phi : R \to R'$ یک مارفیت ہوگا $\Leftrightarrow \ker\phi = \{o\}$

(3) اگر $\phi : R \xrightarrow{onto} R'$ ایک ہم مارفیت ہے جس کا کرنل K ہو تب $R/K \cong R'$۔

22.2 عملی مسائل

22.2.1 بتلاؤ کہ $\begin{pmatrix} p & q \\ o & r \end{pmatrix}$ ماتر سوں والا سٹ جہاں $p,q,r \in \mathbb{Z}$ ہو $(M_2(\mathbb{Z}),+,\cdot)$ کی تحت رنگ ہے۔

22.2.2 ثابت کرو کہ $S_1 = \{0,3\}$ اور $S_2 = \{0,2,4\}$، $(\mathbb{Z}_6, +_6, \times_6)$ کے تحت رنگس ہیں۔

22.2.3 $\mathbb{Z}_{10}$ اور $\mathbb{Z}_{12}$ کے تمام عظیمی ایدیال (Maximal ideals) معلوم کرو۔ (a) (b)

22.2.4 بتلاؤ کہ $\frac{\mathbb{R}[x]}{\langle x^2+1\rangle}$ ایک فیلڈ ہے۔

22.2.5 $\mathbb{Z}_6$ کے تمام پرائم اور عظیمی (Maximal) ایدیال معلوم کرو۔

22.2.6 اگر R ایک تقلیبی رنگ ہے جس کا Characteristic 2 ہے $\phi : R \to R$ جس کی تعریف $\phi(x) = x^2$ ہو ایک ہم مارفیت ہے۔

22.2.7 بتلاؤ کہ $\phi: \mathbb{Z}(\sqrt{2}) \to \mathbb{Z}(\sqrt{2})$ جس کی تعریف $\phi\left(a+b\sqrt{2}\right)=a-b\sqrt{2} \quad \forall a+b\sqrt{2} \in \mathbb{Z}\sqrt{2}$ ایک آٹومارفزم (Automorphism) ہے۔

22.2.8 (i) $\mathbb{Z}$ سے $\mathbb{Z}$ اور (ii) $\mathbb{Z}\times\mathbb{Z}$ سے $\mathbb{Z}$ کے تمام ہم مارفیت معلوم کرو۔

اکائی۔ 23 کثیر رکنیوں کا رنگ اور پریمٹیو کثیر رکنیاں

(Ring of Polynomial and Primitive Polynomials)

23.0 مقصد

اس اکائی میں مواد کے مختلف تعارف کے بعد طلباء کثیر رکنیوں کے رنگ، پریمٹیو کثیر رکنیاں اور ان کے مختلف عملی مسائل کے بارے میں جانکاری حاصل کر کے انہیں حل کریں گے۔

23.1 تعارف

فرض کرو کہ $(R, +, .)$ ایک رنگ ہے۔ ایک کثیر رکنی $f(x) = a_0 + a_1x + a_2x^2 + ...a_nx^n$ جہاں $a_0, a_1, a_2, ... a_n \in R$ پر کثیر رکنی کہلاتی ہے۔ (x ایک متغیر ہے)

یہاں $f(x)$ کا درجہ n ہوگا اگر $a_n \neq 0$ ہو۔

اگر $f(x) = a_0 + a_1x + a_2x^2 + ...a_nx^n$

$$g(x) = b_0 + b_1x + b_2x^2 + ... b_mx^m$$

کسی رنگ R پر دو کثیر رکنیاں ہوں تب

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... + (a_m + b_m)x^m + a_{m+1}x^{m+1} + .. + a_nx^n \quad (if\ n > m)$$

$$f(x).g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + ...$$

$$R[x] = \{f(x) = a_0 + a_1x + a_2x^2 + ... a_nx^n + .../a_0, a_1, ... \in R\}$$

اوپر دیے گئے '+' اور '.' سے ایک رنگ بنتا ہے جسے ہم کثیر رکنیوں کا رنگ کہتے ہیں۔

مثال: $\mathbb{Z}[x]$ ایک کثیر رکنیوں کی رنگ $\mathbb{Z}$ پر ہے۔

نظریات :

(1) اگر $(F, +, .)$ ایک فیلڈ ہو تب متغیر x اور F کے عددی سروں سے بننے والے تمام کثیر رکنیوں کا سٹ $F[x]$ ایک انتگرال دامنہ ہے۔

(2) (Division Algorithm) فرض کرو کہ $(F, +, .)$ ایک فیلڈ ہے۔ دو کثیر رکنیاں $f(x), g(x) \neq 0 \in F[x]$ کے لیے یکتا کثیر رکنیاں $q(x), r(x) \in F[x]$ اس طرح وجود رکھتے ہیں کہ $f(x) = q(x)g(x) + r(x)$ جہاں $r(x) = 0$ یا $\deg(r(x)) < \deg(g(x))$ ہے۔

(3) ایک عنصر $a \in F$، $f(x) \in F[x]$ کا zero یا root ہوگا $\Leftrightarrow$ $x - a$، $f(x)$ کا فیاکٹر (Factor) ہو۔

تعریف:پریمٹیو کثیر رکنی(Primitive Polynomial) :

ایک کثیر رکنی $p(x) = a_0 + a_1x + a_2x^2 + ...a_nx^n \in \mathbb{Z}[x]$ ، پریمٹیو(primitive) کثیر رکنی کہلاتی ہے اگر $g.c.d(a_0, a_1, a_2.....a_n) = 1$ ہو۔

مثال: $f(x) = 2+3x+4x^2 \in \mathbb{Z}[x]$ ایک پریمٹیو کثیر رکنی ہے چوں کہ g.c.d (2, 3, 4) = 1 ہے۔

نوٹ:

(1) دو پریمٹیو کثیر رکنیوں کا حاصل ضرب بھی پریمٹیو کثیر رکنی ہے۔

مثال: $f(x) = 2+3x+4x^2$ ، $g(x) = 5x+7 \in \mathbb{Z}[x]$ دو پریمٹیو کثیر رکنیاں ہیں اور $f(x).g(x) = 14+31x+43x^2+20x^3$ بھی پریمٹیو کثیر رکنی ہے۔

(2) F ایک فیلڈ اور $F[x]$ ایک کثیر رکنیوں کی رنگ ہے تب

i. $f(x)$ ، F میں تحویل پذیر (reducible) ہوگا اگر ایک $\alpha \in F$ اس طرح ہو کہ $f(\alpha) = 0$ ہو۔ یعنی $f(x) = (x-\alpha)g(x)$ کسی $g(x) \in F[x]$ کے لیے۔

ii. اگر $f(x) \in F[x]$ کا درجہ 2 یا 3 ہو تب $f(x)$ reducible ہے $\Leftarrow$ F میں $f(x)$ کا ایک root ہوگا۔

مثال: $g(x) = 1+4x+5x^2+3x^3 \in \mathbb{Z}_6[x]$ ، $f(x) = 5 + 4x + 2x^2 + 2x^3$ کا جمع اور حاصل ضرب معلوم کرو۔ نیز $f(x)+g(x)$ اور $f(x).g(x)$ کا درجہ معلوم کرو۔

حل: دیا گیا ہے کہ

$$f(x) = 5 + 4x + 2x^2 + 2x^3$$

اور $$g(x) = 1 + 4x + 5x^2 + 3x^3 \in \mathbb{Z}_6[x]$$

اس لیے

$$\begin{aligned} f(x) + g(x) &= (5+_6 1) + (4+_6 4)x + (2+_6 5)x^2 + (2+_6 3)x^3 \\ &= (0) + (2)x + (1)x^2 + (5)x^3 \\ &= 2x + x^2 + 5x^3 \end{aligned}$$

$$\begin{aligned} f(x).g(x) = {} & (5 \times_6 1) + (5 \times_6 4 +_6 4 \times_6 1)x + (5 \times_6 5 +_6 4 \times_6 4 +_6 2 \times_6 1)x^2 \\ & +(5 \times_6 3 +_6 4 \times_6 5 +_6 2 \times_6 4)x^3 \\ & +(4 \times_6 3 +_6 2 \times_6 5 +_6 2 \times_6 4)x^4 \\ & +(2 \times_6 5 +_6 2 \times_6 3)x^5 + (2 \times_6 3)x^6 \end{aligned}$$

$$= 5 + 0x + 1.x^2 + 1.x^3 + 0.x^4 + 4.x^5 + 0.x^6$$

$$= 5 + x^2 + x^3 + 4x^5$$

چوں کہ

$$\deg(g(x)) = 3، \deg(f(x)) = 3$$

اس لیے

$$\deg(f(x) + g(x)) = max\{3,3\} = 3$$

اور

$$\deg(f(x).g(x)) = 5 < \deg(f(x)) + \deg(g(x)) = 6$$

مثال : $\mathbb{Z}_7[x]$ میں اگر $f(x) = 5x^4 + 3x^3 + 1$ کو $g(x) = 3x^2 + 2x +$ سے تقسیم کریں تو quotient اور باقی (remainder) معلوم کرو۔

حل: دیا گیا ہے کہ $f(x) = 5x^4 + 3x^3 + 1$ ، $g(x) = 3x^2 + 2x + 1$ اور $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$

$$3x^2 + 2x + 1\overline{)5x^4 + 3x^3 + 1}\,(4x^2 + 3x + 6$$

$$5x^4 + 1x^3 + 4x^2$$

$$\_\_\_\_\_$$

$$2x^3 + 3x^2 + 1$$

$$2x^3 + 6x^2 + 3x$$

$$\_\_\_\_\_$$

$$4x^2 + 4x + 1$$

$$4x^2 + 5x + 6$$

$$\_\_\_\_\_$$

$$6x + 2$$

اس طرح quotient کی قدر $q(x) = 4x^2 + 3x + 6$ اور باقی $r(x) = 6x + 2$ ہے۔

مثال : $f(x) = 3 + 4x^2, g(x) = 2 + x^3 \in \mathbb{Z}_7[x]$ کے لیے $f(x)+g(x)$ ، $f(x)$ اور $\deg(f(x)+g(x))$ ، $\deg(f(x)\cdot g(x))$ معلوم کرو۔

حل: دیا گیا ہے۔

$$f(x) = 3 + 0x + 4x^2 + 0x^3$$

اور

$$g(x) = 2 + 0x + 0x^2 + 1\cdot x^3$$

تب

$$f(x) + g(x)$$

$$= (3 +_7 2) + 0 + (4 +_7 0)x^2 + (0 +_7 1)x^3$$

$$= 5 + 4x^2 + x^3$$

$$f(x)\cdot g(x) = (3 \times_7 2) + (3 \times_7 1)x^3 + (4 \times_7 2)x^2 + (4 \times_7 1)x^5$$

$$= 6 + 3x^3 + x^2 + 4x^5$$
$$= 6 + x^2 + 3x^3 + 4x^5$$

اور $\deg(f(x)+g(x)=3 \quad \deg(f(x)\cdot g(x)=5$ ہے۔

مثال : $\mathbb{Z}_7[x]$ میں اگر $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ کو $g(x) = x^2 + 2x - 3$ سے تقسیم کریں تو حاصل quotient اور باقی (remainder) معلوم کرو۔

حل: دیا گیا ہے کہ $f(x) = x^6 + 3x^5 + 0x^4 + 0x^3 + 4x^2 - 3x + 2$ ، $g(x) = x^2 + 2x - 3$

تب

$$x^2 + 2x - 3 \overline{)\, x^6 + 3x^5 + 0x^4 + 0x^3 + 4x^2 - 3x + 2}$$
$$x^6 + 2x^5 - 0x^4$$
$$\_\_\_\_\_$$
$$x^5 + 3x^4 + 0x^3$$
$$x^5 + 2x^4 - 3x^3$$
$$\_\_\_\_\_$$
$$x^4 + 3x^3 + 4x^2$$
$$x^4 + 2x^3 - 3x^2$$
$$\_\_\_\_\_$$
$$x^3 + 0x^2 - 3x$$
$$x^3 + 2x^2 - 3x$$
$$\_\_\_\_\_$$
$$-2x^2 + 0x + 2$$
$$-2x^2 - 4x + 6$$
$$\_\_\_\_\_$$
$$4x - 4$$

23.2 عملی مسائل

23.2.1 $\mathbb{Z}_6[x]$ میں اگر $f(x) = 2 + 3x + 5x^2$ اور $g(x) = 3 + 5x + 2x^3$ ہوں تب $f(x).g(x)$ ، $f(x)+g(x)$ اور ان کے درجات معلوم کرو۔

23.2.2 $\mathbb{Z}_7[x]$ میں اگر $f(x)=7+9x+5x^2+11x^3-2x^4$ اور $g(x)=3-2x+7x^2+8x^3$ ہوں تب ثابت کرو کہ

(i) $\deg(f(x)+g(x))=4$ اور

(ii) $\deg(f(x).g(x))=7$

23.2.3 اگر $f(x) = 3x^4 + x^3 + 2x^2 + 1$ اور $g(x) = x^2 + 4x + 2$ دو کثیر رکنیاں $\mathbb{Z}_5[x]$ میں ہوں تب $q(x)$ ، $r(x)$ کی قدر اس طرح معلوم کرو کہ $f(x) = g(x).q(x) + r(x)$

23.2.4 $x^4 + 4 \in \mathbb{Z}_5[x]$ کے فیاکٹرس(factors)معلوم کرو۔

23.2.5 $x^4 + 3x^3 + 2x + 4 \in \mathbb{Z}_5[x]$ کے factors معلوم کرو۔

اکائی۔ 24 آئزن اسٹین کی کسوٹی اور غیر تحویل پذیل کثیر رکنیاں

(Eisenstein's Criteria and Irreducibility of Polynomials)

24.0 مقصد

اس اکائی میں طلبا آئزن اسٹین کی کسوٹی اور غیر تحویل پذیر کثیر رکنیوں سے متعلق مسائل کو حل کریں گے۔

24.1 تعارف

ایک کثیر رکنی $f(x) \in F[x]$ جس کا درجہ 1 سے بڑا ہے F پر غیر تحویل پذیر (irreducible) کہلاتا ہے اگر $f(x) = g(x).h(x)$ ہو۔ جہاں $g(x), h(x) \in F[x]$ تب $\deg(g(x)) = 0$ یا $\deg(h(x)) = 0$ ہوگا (یعنی $g(x)$ یا $h(x)$ میں سے ایک مستقل ہوگا)۔

مثال 1 : $x^2 - 3 \in \mathbb{Q}[x]$ ، $\mathbb{Q}$ پر irreducible ہے۔ چوں کہ $x^2 - 3 = (x+\sqrt{3})(x-\sqrt{3})$ ہے اور $\pm\sqrt{3} \in \mathbb{R}$ ہے۔ $x^2 - 3$ ، $\mathbb{R}$ پر تحویل پذیر (reducible) ہے۔

مثال 2 : $x^2 + 5 \in \mathbb{R}[x]$ ، $\mathbb{R}$ پر غیر تحویل پذیر ہے۔ چوں کہ $x^2 + 5 = (x+\sqrt{5}i)(x-\sqrt{5}i)$ ہے۔ $x^2 + 5$ ، $\mathbb{C}$ پر تحویل پذیر ہوگا۔

رزلٹس :

1) اگر $f(x) \in F[x]$ پر یمٹیو ہے تب $\mathbb{Q}$ پر $f(x)$ تحویل پذیر ہوگا $\Leftrightarrow$ $f(x)$ ، $\mathbb{Z}$ پر تحویل پذیر ہو۔

2) $f(x) = a_0 + a_1x + a_2x^2 + ...a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$ ایک monic کثیر رکنی ہے تب $f(x)$ کا $\mathbb{Q}$ میں ایک root α ہوگا $\Leftarrow$ $\alpha \in \mathbb{Z}$ اور $\alpha \mid a_o$۔

Eisenstein's Criteria: فرض کرو کہ $f(x) = a_0 + a_1x + a_2x^2 + ...a_{n-1}x^{n-1} + x^n \in \mathbb{Z}[x]$ اور $n \geq 1$ ہے۔ اگر ایک پرائم عدد (prime number) 'p' اس طرح وجود رکھتا ہو کہ $p / a_0, a_1, a_2, ...a_{n-1}$ اور $p \nmid a_n$ ، $p^2 \nmid a_o$ تب $f(x)$، Q پر غیر تحویل پذیر (irreducible) ہوگا۔

مثال 1: بتلاؤ کہ $f(x) = x^2 - 2$، Q پر irreducible ہے۔

حل : دیا گیا ہے $f(x) = x^2 - 2 = -2 + 0.x + 1.x^2$ یہاں $a_o = -2, a_1 = 0, a_2 = 1$ میں $p = 2$ اس طرح ہے کہ $p = 2 / a_o = -2, a_1 = 0$، $p = 2 \nmid a_2 = 1$ اور $p^2 = 2^2 = 4 \nmid -2$ تب Eisenstein کی کسوٹی کی مدد سے ہم کہہ سکتے ہیں کہ $f(x)$ Q پر irreducible ہے۔

24.2 عملی مسائل

24.2.1 عملی مسئلہ: آئزن اسٹین کی کسوٹی کی مدد سے بتلاؤ کہ $f(x)=14+7x+x^5 \in \mathbb{Z}[x]$، Q پر غیر تحویل پذیر ہو گا۔

24.2.2 عملی مسئلہ: ثابت کرو کہ $f(x) = 2x^4 + 6x^3 - 9x^2 + 15$، Q پر غیر تحویل پذیر ہے۔

24.2.3 عملی مسئلہ: بتلاؤ کہ $f(x)=6+8x+72x^{29}+18x^{99}+7x^{100}\in\mathbb{Z}[x]$ Q پر غیر تحویل پذیر ہو گا۔

24.2.4 عملی مسئلہ: بتلاؤ کہ ذیل کی کثیر رکنیاں

$f(x) = 6 + 18x^8 + 12x^9 + 9x^{10} + 4x^{13}$ اور $g(x) = 12 + 30x^4 + 12x^5 + 5x^7$، Q پر

غیر تحویل پذیر ہوں گے۔

نمونہ امتحانی پرچہ

ریاضیات (لیب مینول)

BSMM350CCP

بی۔ایس سی۔(تیسرا سمسٹر)

وقت: Hrs 3 کل نمبر: 35

نوٹ: درج ذیل میں سے کوئی پانچ سوالات کے جواب دیجیے $5\times 7 = 35$

1 ۔ اگر $\mu, \sigma \in S_6$ اور $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$ $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$ ہوں تب معلوم کرو:

(i) $\sigma^2\mu$

(ii) μ^{2009}

(iii) σ^{2009}

2- فرض کرو کہ $(G, \cdot)$ ایک گروپ ہے $a \in G$ اور $O(a) = 15$ تب ذیل میں دے گیے عناصر کے رتبے (orders) معلوم کرو۔

(i) a^3, a^6, a^9, a^{12}

(ii) a^5, a^{10}

(iii) a^2, a^4, a^8, a^{14}

3. ذیل کے کونسے مبادلے جفت (even) یا طاق (odd) ہیں۔

(i) $(1\ \ 3\ \ 5)$

(ii) $(1\ \ 3\ \ 5\ \ 6)$

(iii) $(1\ \ 3\ \ 5\ \ 6\ \ 7)$

(iv) $(1\ \ 3)(1\ \ 2\ \ 4)(1\ \ 5\ \ 2)$

(v) $(1\ \ 2\ \ 3\ \ 4)(3\ \ 5\ \ 2\ \ 1)$

4 ۔فرض کرو کہ $G = \{a_0 + a_1 i + a_2 j + a_3 k \ / a_0, a_1, a_2, a_3 \in \mathbb{R}\}$

جہاں i, j, k اس طرح ہیں کہ $i^2 = j^2 = k^2 = -1, ij = -ji = k$, $jk = -kj = i$

اگر $\oplus : G \times G \to G$ کی تعریف اس طرح کی گئی ہے کہ $ijk = -1$ اور $ki = -ik = j$

$$(a_0 + a_1 i + a_2 j + a_3 k) \oplus (b_0 + b_1 i + b_2 j + b_3 k)$$
$$= (a_0 + b_0) + (a_1 + b_1) i + (a_2 + b_2) j + (a_3 + b_3) k$$

تب بتلاؤ کہ $(G,\oplus)$ ایک تقلیبی گروپ(Abelian group)ہوگا۔

5. فرض کرو کہ $R=\{a,b,c,d\}$ اوراس پر جمع(+)اور ضرب(x)سے حاصل کردہ کیلی ٹیبل ذیل میں دیا گیا ہے۔

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

x	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	c	a	c
d	a	d	a	d

بتلاؤ کہ یہ بغیر اکائی کے ایک غیر تقلیبی رنگ ہے۔

6- دئے گیئے کثیر رکنی رنگ کے کثیر رکنیوں کا جمع اور حاصل ضرب معلوم کرو .

$$f(x)=4x-5\,,\quad g(x)=2x^2-4x+2\in Z_8[x] \qquad \text{(i)}$$

$$f(x)=2x^2+3x+4\,,g(x)=3x^2+2x+3\in Z_6[x] \qquad \text{(ii)}$$

7- (i) بتلاؤ کہ $\left(R=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix} \;/\; a,b,c,d\in\mathbb{Z}\right\},\ .\right)$ کا سٹ $A=\left\{\begin{bmatrix}p & 0\\ q & 0\end{bmatrix} \;/\; p,q\in\mathbb{Z}\right\}$

ایک بایاں ایدیال(left ideal)ہے لیکن دایاں ایدیال (right ideal) نہیں ہے۔

(ii) بتلاؤ کہ رنگ $\left(R=\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix} \;/\; a,b,c,d\in\mathbb{Z}\right\},\ .\right)$ کا سٹ $B=\left\{\begin{bmatrix}p & q\\ 0 & 0\end{bmatrix} \;/\; p,q\in\mathbb{Z}\right\}$ ، R کا

دایاں ایدیال (right ideal) ہے لیکن بایاں ایدیال(left ideal)نہیں ہے۔

8- $\mathbb{Z}_6$ کے تمام پرایم ایدیال اور عظیمی ایدیال معلوم کرو۔

*****