बी.एस.सी./बी.ए. द्वितीय वर्ष

गणित, प्रथम प्रश्नपत्र

अमूर्त बीजगणित

(ABSTRACT ALGEBRA)

मध्यप्रदेश भोज (मुक्त) विश्वविद्यालय – भोपाल

MADHYA PRADESH BHOJ (OPEN) UNIVERSITY - BHOPAL

COURSE WRITERS

V K Khanna, Formerly Associate Professor, Department of Mathematics, Kirori Mal College, University of Delhi
S K Bhambri, Formerly Associate Professor, Department of Mathematics, Kirori Mal College, University of Delhi
(Units: 1-5)

Published by Registrar, MP Bhoj (Open) University, Bhopal in 2020

VIKAS®

Vikas® is the registered trademark of Vikas® Publishing House Pvt. Ltd.

VIKAS® PUBLISHING HOUSE PVT. LTD.
E-28, Sector-8, Noida - 201301 (UP)
Phone: 0120-4078900 • Fax: 0120-4078999
Regd. Office: A-27, 2nd Floor, Mohan Co-operative Industrial Estate, New Delhi 1100 44
• Website: www.vikaspublishing.com • Email: helpline@vikaspublishing.com

SYLLABI-BOOK MAPPING TABLE

अमूर्त बीजगणित

Syllabi	Mapping in Book
इकाई–1 : समूह की परिभाषा एवं सामान्य गुण, उपसमूह, उपसमुच्चय से जनित उपसमूह, चक्रीय समूह एवं सामान्य गुण।	**इकाई 1** : समूह एवं उपसमूह **(पृष्ठ 3–38)**
इकाई–2 सहसमुच्चय वियोजन, लैग्रांज प्रमेय एवं इसकी उपप्रमेय, फेर्मेट प्रमेय, सामान्य उपसमूह, भागफल समूह।	**इकाई 2** : समूह सिद्धांत **(पृष्ठ 39–67)**
इकाई–3 समूहों की समाकारिता एवं तुल्याकारिता, समाकारिता का मूलभूत प्रमेय, रूपान्तरण एवं क्रमचय, समूह S_n (S_n के विभिन्न उपसमूह संकल्पित है कि $n<5$), केली प्रमेय।	**इकाई 3** : समूह की समरूपता एवं तुल्याकारिता विशेषताएं **(पृष्ठ 69–105)**
इकाई–4 समूह स्वकारिता, अंतः स्वकारिता, स्वकारिताओं का समूह, संयुग्मिता संबंध और केन्द्रीयकारक, सामान्यीकरण, गणना सिद्धांत एवं परिमित समूह का वर्ग समीकरण, परिमित एबेलियन एवं अन–एबेलियन समूह के लिए कॉउची का प्रमेय।	**इकाई 4** : समूह स्वाकारिता, परिमित एवं एबेलियन समूह **(पृष्ठ 107–153)**
इकाई–5 वलय की परिभाषा एवं सामान्य गुण, वलय समाकारिता, उपवलय, आदर्श एवं भागफल वलय, बहुपद वलय एवं उसके गुण, समाकलित डोमेन एवं क्षेत्र।	**इकाई 5** : वलय एवं क्षेत्र **(पृष्ठ 155–260)**

विषय–सूची

परिचय

टिप्पणी

बीजगणित (Algebra) गणित के व्यापक विभागों में से एक है। संख्या सिद्धांत, ज्यामिति और विश्लेषण, आदि गणित के अन्य बड़े विभाग हैं। बीजगणित चर तथा अचर राशियों के समीकरण को हल करने तथा चर राशियों के मान निकालने पर आधारित है। बीजगणित के विकास के फलस्वरूप निर्देशांक ज्यामिति व कलन या कैलकुलस का विकास हुआ जिससे गणित की उपयोगिता बहुत बढ़ गयी। इससे विज्ञान और तकनीकी के विकास को गति मिली। अपने सबसे सामान्य रूप में, बीजगणित गणितीय प्रतीकों और इन प्रतीकों में समाविष्ट करने के नियमों का अध्ययन है। बीजगणित लगभग सम्पूर्ण गणित को एक सूत्र में व्यवस्थित करने वाला विषय है। आरम्भिक समीकरण हल करने से लेकर समूह (Groups), वलय और क्षेत्र का अध्ययन जैसे अमूर्त संकल्पनाओं का अध्ययन, आदि, अनेकानेक विषय बीजगणित के अन्तर्गत आती हैं। बीजगणित के प्रगत अमूर्त भाग को अमूर्त बीजगणित (Abstract Algebra) कहते हैं।

अमूर्त बीजगणित, बीजगणित के उन्नत विषयों का एक समुच्चय (Set) है जो सामान्य संख्या प्रणालियों के बजाय अमूर्त बीजगणितीय संरचनाओं की व्याख्या करता है। बीजगणितीय संरचनाओं में समूह, वलय, क्षेत्र, मापांक, सदिश रिक्त स्थान, और बीजगणित शामिल हैं। 'अमूर्त बीजगणित' शब्द को बीजगणित के अन्य भागों से अध्ययन के इस क्षेत्र को अलग करने के लिए 20 वीं शताब्दी की शुरुआत में समाविष्ट किया गया था। मुख्य रूप से, अमूर्त बीजगणित गणित का एक क्षेत्र है जिसमें वलय (Ring) और सदिश (Vector) रिक्त स्थान जैसे बीजीय संरचनाओं का अध्ययन शामिल है। हालाँकि, अध्ययन का यह क्षेत्र 'बीजगणित' शब्द से बिलकुल अलग है, जो बीजगणितीय अभिव्यक्तियों को हल करने के लिए सूत्रों का उपयोग करने के नियमों का अध्ययन करता है। समकालीन गणित और भौतिकी में अमूर्त बीजगणित का व्यापक रूप से उपयोग किया जाता है। मूल रूप से, बीजगणित, प्रतीकों का प्रयोग कर के गणित और उन प्रतीकों की व्याख्या करने के नियमों की एक शाखा है। प्राथमिक बीजगणित में, वे प्रतीक निश्चित मानों के बिना मात्राओं का प्रतिनिधित्व करते हैं, जिन्हें चर के रूप में जाना जाता है। जैसे वाक्य विशिष्ट शब्दों के बीच संबंधों का वर्णन करते हैं, बीजगणित में, समीकरण चर के बीच संबंधों का वर्णन करते हैं। बीजगणित की एक ठोस वैचारिक अवधारणा का निर्माण बिल्कुल मौलिक है।

बीजगणितीय संरचनाएं, उनकी संबद्ध समरूपता के साथ, गणितीय श्रेणियां बनाती हैं। श्रेणी सिद्धांत एक औपचारिकता है जो विभिन्न संरचनाओं के लिए समान गुणों और निर्माणों को व्यक्त करने के लिए एक एकीकृत तरीके की अनुमति देता है। लियोनहार्ड यूलर (Leonhard Euler) ने संख्याओं पर बीजीय संचालनों पर विचार किया, 'फ़र्मेटस लिटिल प्रमेय' (Fermat's Little Theorem) के अपने सामान्यीकरण में एक पूर्णांक – मापांक अंकगणित – पर अंकुश लगाया। कार्ल फ्रेडरिक गॉस (Carl Friedrich Gauss) द्वारा इन जांचों को बहुत आगे ले जाया गया, जिन्होंने अवशेषों एन (n) के गुणक समूहों की संरचना पर विचार किया और चक्रीय और सामान्य एबेलियन

टिप्पणी

समूहों के कई गुणों को स्थापित किया। द्विआधारी चतुर्थघाती प्रकारों की संरचना की अपनी जांच में, गॉस ने स्पष्ट रूप से इन की संरचना के लिए साहचर्य नियम (Associative Law) बनाया, लेकिन यूलर की तरह वह सामान्य सिद्धांत की तुलना में ठोस परिणामों में अधिक रुचि रखते थे। कई एक पदों के योगफल को बीजीय व्यंजक (Algebraic Expression) कहते हैं। अकेले या एकल पद को एकपद व्यंजक (Monomial), दो पदोंवाले व्यंजक को द्विपद (Binomial), तीन पदवाले को त्रिपद (Trinomial) कहते हैं। एक से अधिक पदवाले व्यंजक को बहुपद (Polynomial) कहते हैं। दो या अधिक पदों के गुणनफल से एक पद ही प्राप्त होता है। गुणा किया जानेवाला प्रत्येक पद गुणनफल वाले पद का गुणनखण्ड (Factor) कहलाता है।

एक समूह की अमूर्त धारणा 1854 में आर्थर केली (Arthur Cayley) के लेख्य में पहली बार दिखाई दी। क्रमपरिवर्तन के एक समूह के लिए तुल्याकारिक है। अमूर्त बीजगणित भौतिकी में व्यापक रूप से उन समूहों का अध्ययन करने के लिए उपयोग किया जाता है जो समरूपता संचालन का प्रतिनिधित्व करते हैं और बीजगणितीय समूह सिद्धांत का उपयोग अंतर समीकरणों को सरल बनाने के लिए किया जाता है।

इस पुस्तक *'अमूर्त बीजगणित'* में बीजगणित की मूल अवधारणाओं को संग्रहित किया गया है। यह समूह, उपसमूह, उपसमुच्चय से जनित उपसमूह, चक्रीय समूह, समुच्चय वियोजन, लैग्रांज प्रमेय एवं इसकी उपप्रमेय, फेर्मेट प्रमेय, सामान्य उपसमूह, भागफल समूह, समूहों की समाकारिता एवं तुल्याकारिता, समाकारिता का मूलभूत प्रमेय, रूपान्तरण एवं क्रमचय, समूह S_n (S_n के विभिन्न उपसमूह संकल्पित है कि $n<5$), केली प्रमेय, समूह स्वकारिता, अंतः स्वकारिता, स्वकारिताओं का समूह, संयुग्मिता संबंध और केन्द्रीयकरण, सामान्यीकरण, गणना सिद्धांत एवं परिमित समूह का वर्ग समीकरण, परिमित एबेलियन एवं अन–एबेलियन समूह के लिए कॉउची का प्रमेय, वलय की परिभाषा एवं सामान्य गुण, वलय समाकारिता, उपवलय, भागफल वलय एवं बहुपद वलय की मूल बातें समझने में छात्रों की मदद करेगा। इस पुस्तक को पांच इकाइयों में विभाजित किया गया है जो एक स्व–अधिगम पाठ्य सामग्री (Self-Instruction Mode) है।

इस पुस्तक में पांच इकाइयाँ हैं – प्रत्येक इकाई एक परिचय के साथ शुरू होती है जिसके बाद उद्देश्य की रूपरेखा होती है। तब विषय की विस्तृत सामग्री को एक सरल लेकिन संरचित तरीके से प्रस्तुत किया गया है ताकि छात्र आसानी से विषय को समझ सके। छात्र की समझ को परखने के लिए, बीच–बीच में 'अपनी प्रगति जांचिए' प्रश्न होते हैं, और विषय को आसानी से समझने हेतु सारांश, मुख्य शब्दावली, स्व–मूल्यांकन प्रश्न एवं अभ्यास भी प्रत्येक इकाई के अंत में दिया हुआ है।

इकाई 1 समूह एवं उपसमूह

टिप्पणी

संरचना

1.0 परिचय

गणित व अमूर्त बीजगणित (Abstract Algebra) में समूह सिद्धांत (Group Theory) में समूह नामक बीजगणितीय मानचित्रों का अध्ययन किया जाता है। अमूर्त बीजगणित में समूह की अवधारणा एक महत्त्वपूर्ण केन्द्र है तथा अन्य जाने–माने बीजगणितीय मानचित्रों, तथा वलय, क्षेत्र व सदिश क्षेत्र (Vector Spaces) को समूहों के रूप में देखा जा सकता है जिनके अतिरिक्त (Additional) संक्रिया (Operation) व अभिगृहीत (Axioms) हों। समूहों का सिद्धांत पूर्णता गणित में पाये जाते हैं व समूह सिद्धांत की विधियों का प्रभाव बीजगणित के कई भागों पर पड़ता है। समूह की अवधारणा बहुपद समीकरणों के अध्ययन से आरम्भ होती है, 1830 के दशक में इवारिस्ट गैलोज (Evariste Galois) से जिन्होंने कि समीकरण के घातों के सममित समूह (Symmetry Group) के लिये समूह (Group) शब्द का प्रयोग किया जिसे कि अब गैलोज समूह (Galois Group) कहा जाता है। समूहों का अध्ययन करने के लिये गणितज्ञों द्वारा विभिन्न धारणाएँ विकसित की गयीं एवं समूहों को छोटे खंड (Fragments) में विभक्त किया गया, जैसे कि उपसमूह, भागफल समूहों एवं सरल समूहों में। भागफल एवं उपसमूहों से संयुक्त रूप से वह तरीका निर्धारित हुआ कि हर समूह को इसके निरूपण (Presentation) द्वारा कैसे दर्शाया जाता है; जो समूह के उत्पन्नकर्ता (Generator) पर मुक्त समूह (Free Group) का भागफल होता है, उसे संबंध के उपसमूह द्वारा भागफलित (Quotiented) किया जाता है।

समूह G का उप–समुच्चय (Sub Set) H, G का उपसमूह है, यदि H स्वयं में G के संक्रिया में एक समूह है। समूह G में कम से कम दो उपसमूह हैं: G स्वयं एवं नगण्य (Trivial) समूह $\{e\}$ है। इन्हें क्रमशः G का अनुचित (Improper) व G के नगण्य (Trivial) उपसमूह कहा जाता है। स्पष्ट ही है, कि इस विधि द्वारा यह निर्धारित

टिप्पणी

किया जाता है कि समूह का प्रदर्शित उप–समुच्चय उपसमूह है अथवा नहीं। चक्रीय समूह ऐसा समूह होता है जिसे एक अवयव X समूह उत्पन्नकर्ता (Group Generator) द्वारा उत्पन्न किया जा सकता है। प्रत्येक चक्रीय समूह एक एबेलियन समूह होता है, अर्थात् इसका समूह संक्रिया (Group Operation) क्रमविनिमेय (Commutative) है, एवं प्रत्येक परिमित उत्पन्नकर्ता एबेलियन समूह चक्रीय समूहों का प्रत्यक्ष गुणन है।

इस इकाई में आप समूह, परिभाषा व समूहों की मूल विशेषताएं, उपसमूहों, उप–समुच्चय द्वारा उत्पन्न उपसमूहों, चक्रीय समूहों एवं इनके सरल विशेषताओं का अध्ययन करेंगे।

1.1 उद्देश्य

इस इकाई को पढ़ने के बाद आप–

- समूह के महत्त्वपूर्ण अभिलक्षण का वर्णन कर पाएंगे;
- समूहों की परिभाषा एवं मूल विशेषताओं को समझ पाएंगे;
- उपसमूहों का वर्णन कर पाएंगे;
- उप–समुच्चय द्वारा उत्पन्न उपसमूहों के विश्लेषण को समझ पाएंगे;
- चक्रीय समूहों की परिभाषा व इनके सरल विशेषताओं का वर्णन कर पाएंगे।

1.2 समूह : परिभाषा एवं मूल विशेषताएं

अमूर्त बीजगणित में समूह सिद्धांत समूहों के रूप में ज्ञात बीजीय संरचनाओं का अध्ययन करता है। एक समूह की अवधारणा बहुपद समीकरणों के अध्ययन से उत्पन्न हुई है, 1830 में इवारिस्ट गैलोज (Evariste Galois) के साथ शुरू, जिन्होंने समूह के लिए शब्द पेश किया एक समीकरण की घातों के सममित समूह (Symmetry Group), जिसे अब गैलोज समूह कहा जाता है। गणितज्ञों ने विभिन्न धारणाओं का विकसित किया है और छोटे खंड के समूह में विभाजित किया जाता है, जैसे उपसमूह, भागफल समूह और सरल समूह है। विचाराधीन समूहों की पंक्ति में परिमित क्रमचय समूह व एवं आव्यूह (Matrix) समूहों के विशेष उदाहरणों से लेकर ऐसे अमूर्त समूह सम्मिलित हैं, जिन्हें उत्पन्नकर्ता व संबंध (Relation) द्वारा प्रस्तुतीकरण के माध्यम से प्रदर्शित किया जा सकता है जिसे समूह का प्रस्तुतीकरण भी कहते हैं।

परिभाषा: गैर–रिक्त समुच्चय G के साथ द्विआधारी संरचना (Binary Composition) .* (स्टार) (Star) द्वारा समूह का निर्माण होना कहा जाता है, यदि इसमें निम्नांकित अभिधारणाएँ पूर्ण होती हों:

(i) संबद्धता (Associativity): समस्त $a, b, c \in G$ हेतु $a * (b * c) = (a * b) * c$

(ii) अस्तित्व के तत्समक (Existence of Identity) $\exists$ अवयव $e \in G$, ऐसा है कि

$a * e = e * a = a$ समस्त हेतु $a \in G$

(तो e को तत्समक कहते हैं)

(iii) अस्तित्व का व्युत्क्रम (Existence of Inverse): प्रत्येक हेतु $a \in G, \exists\, a' \in G$ (a पर निर्भर)

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

a' को a का व्युत्क्रम कहते हैं।

टिप्पणी

टिप्पणी: (i) चूँकि $*$ G पर एक द्विआधारी संरचना है, अतः यह समझा जाता है कि यह सभी $a, b \in G, a * b$ के लिये G का अद्वितीय सदस्य है। इस विशेषता को संवृत गुण (Closure Property) कहा जाता है।

(ii) यदि उपरोक्त अभिधारणाओं के योग (Addition) G द्वारा क्रमविनिमेय नियम (Commutative Law) की भी पूर्ति की जाती हो समस्त $a, b \in G$ हेतु $a * b = b * a$

तब G को एबेलियन समूह अथवा क्रमविनिमेय समूह कहा जाता है।

(*iii*) साधारणतया समूह के लिये द्विआधारी संरचना को '.' (Dot) से इंगित किया जाता है जिसे लिखना अत्यन्त सुविधापूर्ण है (एवं अभिगृहीत प्राकृतिक भी दिखते हैं)।

यदि समुच्चय G परिमित हो (अर्थात् इसमें अवयवों की परिमित संख्या हो) तो इसे परिमित समूह कहा जाता है, अन्यथा अपरिमित समूह कहा जाता है।

हम सदा ही (यदि कुछ और न कहा गया हो) समूह की तत्समक के लिये प्रतीक e का एवं समूह के अवयव a के व्युत्क्रम के लिये प्रतीक a^{-1} का प्रयोग करेंगे।

परिभाषा: समूह की कोटि से हमारा तात्पर्य समूह में अवयवों की संख्या होगा एवं इसे $o(G)$ या $|G|$ से इंगित करेंगे।

1.2.1 समूहों के स्वयंसिद्ध

औपचारिक रूप से समूह (Group) एक समुच्चय (Set) की क्रमबद्ध जोड़ी (Ordered Pair) है और इस समुच्चय पर एक द्विआधारी संक्रिया (Binary Operation) है जो **समूह के स्वयंसिद्धो (Group Axioms)** को संतुष्ट करता है।

समुच्चय को समूह का अंतर्निहित समुच्चय (Underlying Set) कहा जाता है और इस संक्रिया (Operation) को समूह संक्रिया (Group Operation) या समूह नियम (Group Law) कहते है। समुच्चय सिद्धांत (Set Theory) के अनुसार, यदि किसी समुच्चय के दो तत्वों (Elements) को एक संक्रिया के द्वारा संयुक्त (Combine) करके एक तीसरे तत्व को संयोजित किया जाता है जो उसी समुच्चय से संबंधित है और चार परिकल्पनाओं (Four Hypothesis) को संतुष्ट करता है। ये चार परिकल्पनायें है, संवरक, संबद्धता, व्युत्क्रमणीय तथा तत्समक और इन्हें समूह के स्वयंसिद्ध भी कहते हैं।

1. **संवरक (Closure):** यदि 'x' और 'y' समूह 'G' में दो तत्व है, तो x, y भी G में सम्मिलित होगा।
2. **संबद्धता (Associativity):** यदि 'x', 'y' और 'z' समूह 'G' में है तो x.(y.z) = (x.y).z होगा।
3. **व्युत्क्रमणीय (Invertibility):** समूह 'G' में प्रत्येक 'x' के लिए समूह 'G' में कुछ 'y' है इस प्रकार कि x.y = y.x.

4. **तत्समक (Identity):** समूह 'G' में किसी भी तत्व 'x' के लिए, समूह 'G' में एक तत्व 'I' इस प्रकार से है कि $x.I = I.x$, जहां 'I' को समूह 'G' का तत्समक कहा जाता है।

टिप्पणी

एक सामान्य उदाहरण जो उपयुक्त सभी चार स्वयंसिद्धों (Axioms) को संतुष्ट करता है वह है दो पूर्णांकों का योग (Addition of Two Integers), जिसके परिणामस्वरूप पूर्णांकों का योग स्वयं एक पूर्णांक बनाता है। इसलिए यह संवरक गुण (Closure Property) को संतुष्ट करता है। पूर्णांकों का योग संबद्धता गुण (Associative Property) को भी संतुष्ट करता है। समूह में एक तत्समक तत्व (Identity Element) 'शुन्य' (Zero) होता है जो किसी भी संख्या के साथ जोड़ने पर मूल संख्या (Original Number) देता है। प्रत्येक पूर्णांक (Integer) के लिए एक व्युत्क्रम (Inverse) होता है इस प्रकार कि जब उन्हें जोड़ा जाता है तो परिणाम (Result) में शुन्य (Zero) मिलता है।

इस प्रकार से सभी समूह स्वयंसिद्ध (Group Axioms) संतुष्ट होते है जब दो पूर्णांकों की योग संक्रिया (Addition Operation) होती है।

समूह सिद्धांत के स्वयंसिद्ध एवं प्रमाण (Group Theory Axioms and Proof)

निम्नलिखित उदाहरणों की सहायता से हम समूह सिद्धांत के स्वयंसिद्धों एवं प्रमाण को सिद्ध कर सकते है।

1. यदि 'G' एक समूह है जिसके तत्व 'a' और 'b' इस प्रकार है कि $a, b \in G$, तब $(a \times b)^{-1} = a^{-1} \times b^{-1}$ होगा।

   प्रमाण : हम प्रमाणित करते है कि $(a \times b) \times b^{-1} \times a^{-1} = I$ जहां 'I' एक तत्समक तत्व (Identity Element) है समूह 'G' का। हम उपयुकत समीकरण में L.H.S. को लेते है।

   L.H.S. $= (a \times b) \times b^{-1} \times a^{-1}$

   $\Rightarrow a \times (b \times b^{-1}) \times a^{-1}$

   $\Rightarrow a \times I \times a^{-1}$ (संबद्धता स्वयंसिद्ध (Associative Axiom) के अनुसार)

   $\Rightarrow (a \times I) \times a^{-1}$ (तत्समक स्वयंसिद्ध (Identity Axiom) के अनुसार)

   $= a \times a^{-1}$ (तत्समक स्वयंसिद्ध के अनुसार)

   $= I$ (तत्समक स्वयंसिद्ध के अनुसार)

   $=$ R.H.S.

   अतः प्रमाणित हुआ।

2. यदि किसी समूह 'G' में 'x', 'y', और 'z' तीन तत्व इस प्रकार से है कि $x \times y = z \times y$ तब $x = z$ होगा।

टिप्पणी

प्रमाण : हम मान लेते है कि $x \times y = z \times y$ ...(i)

चूंकि 'y' यहां समूह 'G' का एक तत्व है अतः इसका तात्पर्य है कि समूह 'G' में एक 'a' है जिसमें तत्समक तत्व 'I' है, इस प्रकार कि,

$y \times a = I$ ...(ii)

समीकरण (i) के दोनों ओर 'a' से गुणा करने पर हम प्राप्त करते है,

$x \times y \times a = z \times y \times a$

$x \times (y \times a) = z \times (y \times a)$ (संबद्धता (Associativity) के अनुसार)

समीकरण (ii) से,

$a \times I = c \times I$ (समीकरण (ii) से)

$a = c$ (तत्समक स्वयंसिद्ध (Identity Axiom) के अनुसार)

इस नियम को निष्कासित नियम (Cancellation Law) भी कहते है।

अतः प्रमाणित हुआ।

1.2.2 समूहों के कुछ उदाहरण

उदाहरण 1.1: पूर्णांकों (Integers) के समुच्चय **Z** द्वारा पूर्णांकों (Integers) के सामान्य योग (Usual Addition) के सन्दर्भ में एबेलियन समूह का निर्माण किया जाता है।

समूह की परिभाषा में अभिधारणाओं को सरलता से सत्यापित करने के लिये दो पूर्णांकों (Integers) के योग को एक अद्वितीय पूर्णांक (Unique Integers) द्वारा प्रदर्शित किया जाता है। योग (Addition) की संबद्धता हमें ज्ञात है। 0 (शून्य) तत्समक होगा व ऋणात्मक (Negative) सम्बन्धित व्युत्क्रम अवयव होंगे। क्रमविनिमेयता (Commutativity) पुनः स्पष्ट है।

उदाहरण 1.2: पूर्ववर्ती उदाहरण में प्रदर्शित जैसे कोई भी परख सकता है कि परिमेयों (Rational) के समुच्चय **Q**, वास्तविक संख्याओं के **R** द्वारा भी योग (Addition) के सन्दर्भ में एबेलियन समूहों का निर्माण किया जायेगा।

उदाहरण 1.3: सामान्य गुणन (Usual Multiplication) के सन्दर्भ में पूर्णांकों (Integers) का समुच्चय समूह को नहीं बनाता, फिर भी संवृत, संबद्धता, तत्समक स्थितियाँ होंगी।

ध्यान दें : गुणन (Multiplication) के सन्दर्भ में 2 में व्युत्क्रम नहीं होते है क्योंकि वहाँ कोई पूर्णांक (Integers) a उपस्थित नहीं है, जैसे कि $2.a = a.2 = 1$.

उदाहरण 1.4: G समस्त धनात्मक अपरिमेय संख्याओं का समुच्चय गुणन के अधीन 1 के साथ मिलकर समूह को नहीं बनाता क्योंकि संवृत नियंत्रित नहीं बन रहा। वस्तुतः $\sqrt{3}.\sqrt{3} = 3 \notin G$, भले ही यह देखा जा सकता हो कि समूह की परिभाषा के अन्य पद (Terms) यहाँ पूर्ण हो रहे हैं।

उदाहरण 1.5: माना $\{1, -1\}$ समुच्चय G है। तब इससे गुणन अधीन एबेलियन समूह का निर्माण होता है। विशेषताओं को परखना पुनः सरल है।

1 तत्समक होगा एवं प्रत्येक अवयव का अपना व्युत्क्रम होगा।

टिप्पणी

उदाहरण 1.6: आव्यूह योग के अधीन पूर्णांकों (Integers) में समस्त 2×2 आव्यूह (Matrix) का समुच्चय एबेलियन समूह का एक और उदाहरण होगा।

उदाहरण 1.7: समस्त गैर शून्य सम्मिश्रण की संख्या के समुच्चय से गुणन अधीन समूह इस अनुरूप निर्मित होता है,

$$(a + ib)\ (c + id) = (ac - bd) + i\ (ad + bc)$$

$1 = 1 + i.0$ तत्समक होगा,

$\frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2}$ $a + ib.$ का व्युत्क्रम होगा।

ध्यान दें : $a + ib$ शून्य नहीं है, अर्थात् a व b दोनों शून्य नहीं होंगे।

इस प्रकार $a^2 + b^2 \neq 0$

उदाहरण 1.8: माना $G = \{\pm 1, \pm i, \pm j, \pm k\}$। परस्पर सामान्य गुणन करते हुए G पर गुणन को परिभाषित करें,

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$

तदुपरान्त G समूह का रूप है। G, $ij \neq ji$ के समान एबेलियन नहीं है।

इसे चतुष्क समूह (Quaternion Group) कहा जाता है।

उदाहरण 1.9: माना $G = \{(a, b) \mid a, b$ परिमेय $a \neq 0\}$। $(a, b) * (c, d) = (ac, ad + b)$ द्वारा * पर G को परिभाषित करें।

संवृत इस प्रकार है $a, c \neq 0 \Rightarrow ac \neq 0$

$$[(a, b) * (c, d)] * (e, f) = (ac, ad + b) * (e, f)$$
$$= (ace, acf + ad + b)$$
$$(a, b) * [(c, d) * (e, f)] = (a, b) * (ce, cf + d)$$
$$= (ace, acf + ad + b)$$

इससे संबद्धता सिद्ध होती है।

$(1, 0)$ तत्समक होगा एवं $(1/a, -b/a,)$ यह किसी अवयव (a, b) का व्युत्क्रम होगा।

G एबेलियन नहीं है

$$(1, 2) * (3, 4) = (3, 4 + 2) = (3, 6)$$
$$(3, 4) * (1, 2) = (3, 6 + 4) = (3, 10).$$

उदाहरण 1.10: (अ) वास्तविकता में रूप $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ के सभी 2×2 आव्यूहों का समुच्चय G बनता है जहाँ $ad - bc \neq 0$, अर्थात् गैर शून्य सिद्ध से आव्यूह गुणन के अधीन गैर एबेलियन समूह बनता है।

इसके वास्तविकता पर 2×2 आव्यूहों का **साधारण रैखिक समूह** (General Linear Group) कहा जाता है एवं $GL(2, R)$ के रूप में दर्शाया जाता है।

आव्यूह $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ द्वारा तत्समक के रूप में कार्य किया जायेगा तथा

टिप्पणी

आव्यूह $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ का व्युत्क्रम होगा।

आव्यूहों को साधारणीकृत (Generalise) व सिद्ध करने की अवधारणा निम्नानुसार है।

(ब) यदि G वास्तविकता पर सभी $n \times n$ व्युत्क्रमणीय आव्यूह का समुच्चय हो तो G से आव्यूह गुणन के अधीन समूह का निर्माण होता है।

(स) सिद्ध मान 1 युक्त R पर 2×2 आव्यूह के समुच्चय से आव्यूह गुणन के अधीन एबेलियन समूह बनता है एवं **विशेष रैखिक समूह** (Special Linear Group) कहलाता है व इसे $SL(2, R)$ से इंगित करते हैं।

उपरोक्त उदाहरणों में R के स्थान पर कोई क्षेत्र (उदाहरण के लिये **Q**, **C** अथवा Z_p) को प्राप्त किया जा सकता है।

उदाहरण 1.11: समूह के अवशेष: माना $G = \{0, 1, 2, 3, 4\}$। $a \oplus_5 b = c$ के द्वारा G पर रचना $\oplus_5$ को परिभाषित करें जहाँ c कम तथा ऋणात्मक पूर्णांकों में नहीं है जो शेषफल (Remainder) के रूप में प्राप्त होता हो जब $a + b$ को 5 से भाग दिया जाता है। उदाहरणार्थ $3 \oplus_5 4 = 2, 3 \oplus_5 1 = 4$ इत्यादि। तदुपरान्त $\oplus_5$, G पर एक द्विआधारी संरचना है (जिसे योग (Addition) मापांको 5 कहा जाता है)। यह सत्यापित करना सरल है कि G से इसके अधीन समूह निर्मित होता है।

इस परिणाम को साधारणीकृत रूप $G = \{0, 1, 2, ..., n-1\}$ प्रदान किया जा सकता है।

मापांकों के योग n के अधीन जहाँ n कोई धनात्मक पूर्णांक है।

इस प्रकार हम देखते हैं,

$$a \oplus_n b = \begin{cases} a+b & \text{यदि } a+b < n \\ a+b-n & \text{यदि } a+b \geq n \end{cases}$$

असमंजस की सम्भावना न होने के प्रकरण में हम उप–प्रत्यय (Sub-Suffix) n को छोड़ देते हैं एवं सामान्य तौर पर $\oplus$ लिखते हैं। इस समूह को साधारणतः Z_n द्वारा इंगित करते हैं।

उदाहरण 1.12: $G = \{x \in \mathbf{Z} \mid 1 \leq x < n$, सहअभाज्य है जहाँ Z पूर्णांकों (Integers) का समुच्चय एवं x, n सहअभाज्य हैं, अर्थात् H.C.F के x तथा n, 1 है।

हम G पर द्विआधारी संरचना $\otimes$ को $a \otimes b = c$ द्वारा परिभाषित करते हैं जहाँ c प्राप्त कम धनात्मक शेषफल (Remainder) है, जब $a \,.\, b$ को n से भाग दिया जाता है। इस संरचना $\otimes$ को गुणन मापांक n कहा जाता है।

टिप्पणी

हम दर्शाते हैं, कि G से $\otimes$ के अधीन समूह बनता है।

संवृतः $a, b \in G$ हेतु माना $a \otimes b = c$। अब $c \neq 0$ अन्यथा $n \mid ab$ जो कि सम्भव नहीं क्योंकि a, n व b, n सहअभाज्य हैं।

इस प्रकार $c \neq 0$ व ऐसे तो $\leq c < n$ भी।

अब यदि c, n सहअभाज्य न हों तो $\exists$ कोई अभाज्य संख्या है, तो p इस प्रकार है, $p|c$ और $p|n$.

पुनः $ab = nq + c$ किसी q हेतु

हम प्राप्त करते है। $|ab \qquad [p|n \Rightarrow p|nq, p|c \Rightarrow p|nq + c]$

$\Rightarrow p|a$ या $p|b$ (चूँकि p अभाज्य है)

यदि $p|a$ तो $p|n$ के रूप में इसका तात्पर्य हुआ कि a, n सहअभाज्य नहीं हैं परन्तु a, n सहअभाज्य हैं।

इसी प्रकार $p|b$ से विरोधाभास आता है।

इसी कारण c, n सहअभाज्य हैं एवं इस प्रकार $c \in G.$, प्रदर्शित कर रहा है, कि संवृत रूप में स्थित है।

संबद्धताः माना, $a, b, c \in G$ अवयव हैं।

माना, $a \otimes b = r_1, (a \otimes b) \otimes c = r_1 \otimes c = r_2$ तो r_2 से $r_1 c = nq_2 + r_2$ प्रदर्शित है।

$a \otimes b = r_1$ का भी तात्पर्य हुआ $ab = q_1 n + r_1$

इस प्रकार $\qquad ab - q_1 n = r_1$

$$\Rightarrow (ab - q_1 n)c = r_1 c = nq_2 + r_2$$

$$\Rightarrow (ab)c = r_2 + nq_2 + nq_1 c = n(q_1 c + q_2) + r_2$$

अथवा वह r_2, n से $(ab)c$ को भाग देने पर कम गैर–ऋणात्मक शेषफल (Remainder) प्राप्त होता है।

इसी प्रकार, यदि $a \otimes (b \otimes c) = r_3$ तो हम दर्शा सकते हैं कि r_3, n द्वारा $a(bc)$ को भाग देने से कम गैर–ऋणात्मक शेषफल (Remainder) प्राप्त होता है।

परन्तु चूँकि $a(bc) = (ab)c, r_2 = r_3$

इसी कारण $a \otimes (b \otimes c) = (a \otimes b) \otimes c$

अस्तित्व के तत्समकः यह देखना सरल है कि $a \otimes 1 = 1 \otimes a = a$ सभी $a \in G$ के लिए

अथवा 1 द्वारा तत्समक का कार्य किया जायेगा।

अस्तित्व का व्युत्क्रमः $a \in G$ कोई अवयव हो तो a व n सहअभाज्य हैं एवं इस प्रकार हम पूर्णांक (Integer) x व y इस प्रकार प्राप्त कर सकते हैं कि $ax + ny = 1$

विभाजन एल्गोरिद्म (Division Algorithm) से हम लिख सकते हैं,

$$x = qn + r, \quad \text{जहाँ } 0 \leq r < n$$

$\Rightarrow ax = aqn + ar$

$\Rightarrow ax + ny = aqn + ar + ny$

$\Rightarrow 1 = aqn + ar + ny$

अथवा $ar = 1 + (-aq - y)n$

टिप्पणी

अर्थात् $a \otimes r = 1$। इसी प्रकार $r \otimes a = 1$। यदि r, n सहअभाज्य हों तो r, a का व्युत्क्रम होगा।

यदि r, n सहअभाज्य न हों तो हम अभाज्य संख्या p इस प्रकार प्राप्त कर सकते हैं कि $p \mid r, p \mid n$,

$\Rightarrow p \mid qn$ और $p \mid r$

$\Rightarrow p \mid qn + r$

$\Rightarrow p \mid x$

$\Rightarrow p \mid ax$ और $p \mid ny$

$\Rightarrow p \mid ax + ny = 1$

जो कि सम्भव नहीं। इस प्रकार r, n सहअभाज्य हैं एवं इस अनुसार $r \in G$ एवं यह a का आवश्यक व्युत्क्रम है।

यह देखना सरल है, कि G एबेलियन होगा। हम इस समूह को U_n या $U(n)$ से इंगित करते हैं एवं इसे गुणन मापांकों n के अधीन पूर्णांकों (Integers) का समूह कहते हैं।

टिप्पणी: मान लें कि $n = p$, एक अभाज्य (Prime) हो तो सभी पूर्णांकों (Integers) $1, 2, 3, ..., p-1$, p हेतु सहअभाज्य हैं, तो ये सभी G के सदस्य होंगे। पुनः दर्शाया जा सकता है, कि $G' = \{2, 4, 6, ..., 2(p-1)\}$

जहाँ $p > 2$ एक अभाज्य (Prime) रूप है, जो गुणन मापांक $2p$ के अधीन एक एबेलियन समूह का निर्माण करता है।

कुछ प्रारंभिक लैमाज़ (Lemmas)

लैमा: समूह G में,

(1) *तत्समक अवयव अद्वितीय है*।

(2) *प्रत्येक* $a \in G$ का व्युत्क्रम अद्वितीय है।

(3) *समस्त* $a \in G$ हेतु $(a^{-1})^{-1} = a$ जहाँ a^{-1} के व्युत्क्रम हेतु a है।

(4) *समस्त* $a, b \in G$ हेतु $(ab)^{-1} = b^{-1} a^{-1}$

(5) *समस्त* $a, b, c \in G$ हेतु $b = ac \Rightarrow b = c$

$ba = ca \Rightarrow b = c$ (यह निष्कासित नियम कहलाते हैं)

प्रमाण (Proof)

(1) मान लेते हैं कि e व e', G के दो अवयव हैं जो तत्समक के रूप में कार्य करते हों तो चूँकि $e \in G$ व e' तत्समक है अतः $e'e = ee' = e$

तथा चूँकि $e' \in G$ व e तत्समक है अतः $e'e = ee' = e'$

टिप्पणी

दो $\Rightarrow e = e'$

जिससे समूह में तत्समक की अद्वितीयता (Uniqueness) स्पष्ट होती है।

(2) माना $a \in G$ कोई अवयव है, एवं a' व a'', a के दो व्युत्क्रम अवयव हों

तब, $aa' = a'a = e$

$aa'' = a''a = e$

अब $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$.

इसके द्वारा यह प्रदर्शित हो रहा है कि अवयव का व्युत्क्रम अद्वितीय फल है। हम a के व्युत्क्रम को a^{-1} से इंगित करेंगे।

(3) चूँकि a^{-1}, a का व्युत्क्रम है। $aa^{-1} = a^{-1}a = e$

जिसका यह भी आशय है कि a का व्युत्क्रम a^{-1} है। इस प्रकार $(a^{-1})^{-1} = a$.

(4) हमें यह सिद्ध करना होगा कि, ab, $b^{-1}a^{-1}$ का व्युत्क्रम है जिसके लिये हम दर्शाते हैं,

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

अब $(ab)\,(b^{-1}a^{-1}) = [(ab)\,b^{-1}]\,a^{-1}$

$= [(a(bb^{-1})]\,a^{-1}$

$= (ae)\,a^{-1} = aa^{-1} = e$

इसी प्रकार $(b^{-1}a^{-1})\,(ab) = e$

तथा इस प्रकार परिणाम आया।

(5) माना $ab = ac$, तो $b = eb = (a^{-1}a)b$

$= a^{-1}(ab) = a^{-1}\,(ac)$

$= (a^{-1}\,a)c = ec = c$

इस प्रकार $ab = ac \Rightarrow b = c$

जिसे **बाएँ निष्कासित नियम** (Left Cancellation Law) कहा जाता है।

इसी प्रकार **दाएँ निष्कासित नियम** (Right Cancellation Law) सिद्ध हो सकता है।

प्रमेय 1.1: समूह G में अवयवों a, b के लिये समीकरणों $ax = b$ व $ya = b$ में G में x व y के लिये अद्वितीय हल हैं।

प्रमाण: अब $ax = b$,

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

$\Rightarrow ex = a^{-1}b$

अथवा $x = a^{-1}b$

जो कि समीकरण $ax = b$ के लिए आवश्यक हल है।

माना कि $x = x_1$ एवं $x = x_2$ इस समीकरणों के दो हल हैं,

तो $ax_1 = b$ व $ax_2 = b$

$\Rightarrow ax_1 = ax_2$

$\Rightarrow \quad x_1 = x_2$ दाएँ निष्कासित से।

प्रदर्शित हो रहा है कि अद्वितीय हल है।

इसी प्रकार $y = ba^{-1}$ समीकरण $ya = b$ का अद्वितीय हल होगा।

टिप्पणी

प्रमेय 1.2: गैर रिक्त समुच्चय G के साथ द्विआधारी संरचना '.' का एक समूह है, यदि

(1) समस्त $a, b, c \in G$ के लिये $a(bc) = (ab)c$

(2) किसी $a, b \in G$ के लिये समीकरणों $ax = b$ व $ya = b$ में G में हल हैं।

प्रमाण: यदि G एक समूह है, तो (1) व (2) परिभाषा व पूर्ववर्ती प्रमेय अनुरूप हैं। इसके विपरीत (1) व (2) को देखें। G को एक समूह दर्शाने के लिये हमें अस्तित्व के तत्समक एवं व्युत्क्रम (प्रत्येक अवयव के लिये) सिद्ध करने की आवश्यकता होती है।

$a \in G$ कोई अवयव है।

(2) से समीकरणों $ax = a,$

$ya = a,$

G का हल हैं।

माना $x = e$ व $y = f$ हल हैं।

इस प्रकार $\exists\, e, f \in G$ हैं कि $ae = a$

तथा $fa = a$

माना $b \in G$ अब कोई अवयव है, तो पुनः समीकरण (2) अनुरूप G में कुछ x, y इस प्रकार है कि, $ax = b$

$ya = b.$

अब $ax = b \Rightarrow f.(a\,.\,x) = f\,.\,b$

$\Rightarrow (f\,.\,a)\,.\,x = f\,.\,b$

$\Rightarrow a\,.\,x = f\,.\,b$

$\Rightarrow b = f\,.\,b$

पुनः $y.a = b \Rightarrow (y\,.\,a)\,.\,e = b\,.\,e$

$\Rightarrow y\,.\,(a\,.\,e) = b\,.\,e$

$\Rightarrow y\,.\,a = be$

$\Rightarrow b = be$

इस प्रकार हमें प्राप्त है, $b = fb$ ...(*i*)

$b = be$ ...(*ii*)

किसी $b \in G$ हेतु

समीकरण (*i*) में $b = e$ को एवं समीकरण (*ii*) में $b = f$ को रखने पर हम पाते हैं,

$e = fe$

$$f = fe$$

$$\Rightarrow e = f.$$

इसी कारण $ae = a = fa = ea$

टिप्पणी

अर्थात् $\exists\ e \in G$, इस प्रकार कि, $ae = ea = a$

$\Rightarrow e$ तत्समक है।

पुनः यदि कोई $a \in G$ तथा $e \in G$ तत्समक के लिए समीकरणों $ax = e$ व $ya = e$ में हल हों।

माना कि, $x = a_1$ व $y = a_2$ हों,

तब $aa_1 = e, \quad a_2a = e$

अब $a_1 = ea_1 = (a_2a)a_1 = a_2(aa_1) = a_2e = a_2.$

इसी कारण $aa_1 = e = a_1a$ किसी $a \in G$ के लिए

अर्थात् किसी $a \in G, \exists$ के लिये किसी $a_1 \in G$ द्वारा उपरोक्त संबंध की पूर्ति की जा रही है, a में एक व्युत्क्रम स्थित है। इस प्रकार हर अवयव में व्युत्क्रम स्थित है एवं परिभाषानुरूप G से समूह का निर्माण होता है।

टिप्पणी: उपरोक्त प्रमेय सिद्ध करते समय हमने मान लिया था कि $ax = b$ व $ya = b$ के समीकरणों में G में हल (Solution) हैं। तथा परिणाम विफल हो सकता है, यदि उपरोक्त समीकरणों में से एक ही प्रकार के हल (Solution) हो।

परिभाषा: गैर–रिक्त समुच्चय G के साथ द्विआधारी संरचना '.' को अर्द्ध समूह कहा जाता है, यदि समस्त $a\ .\ (b\ .\ c) = (a\ .\ b)\ .\ c$ हेतु $a, b, c \in G$ हो तब

स्पष्ट है कि प्रत्येक समूह एक अर्द्ध समूह है। इसका विपरीत वास्तविक नहीं है क्योंकि योग (Addition) के अधीन प्राकृतिक संख्याओं (Natural Numbers) को समुच्चय **N** के विचाराधीन रखा जा रहा है।

प्रमेय 1.3: हो सकता है, कि अर्द्ध समूह में निष्कासित नियम न हों।

प्रमाण: आव्यूह गुणन के अधीन पूर्णांकों (Integer) पर समस्त 2×2 आव्यूह के समुच्चय M का विचार करें, जिससे अर्द्ध समूह बनता है।

यदि हम $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}, C = \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix}$ लेते हैं

तो स्पष्ट है, कि $AB = AC = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

किन्तु $B \neq C$।

योग (Addition) के अधीन प्राकृतिक संख्याओं (Natural Numbers) का समुच्चय अर्द्ध समूह का एक उदाहरण है, जिसमें निष्कासित नियम (Cancellation Law) लागू होता हैं।

प्रमेय 1.4: जिस परिमित अर्द्ध समूह में निष्कासित नियम (Cancellation Laws) स्थित हैं वह एक समूह है।

प्रमाण: माना $G = \{a_1, a_2, ..., a_n\}$ ऐसा परिमित अर्द्ध समूह है, जिसमें निष्कासित नियम (Cancellation Law) स्थित हैं।

टिप्पणी

माना $a \in G$ कोई अवयव है, तो संवृत विशेषता द्वारा $aa_1, aa_2, ..., aa_n$

ये सभी G में स्थित हैं।

माना कि इन अवयवों में से कोई दो अवयव समतुल्य हैं $aa_i = aa_j$ कुछ के लिए $i \neq j$

तो $a_i = a_j$ निष्कासन से,

किन्तु $a_i \neq a_j$ जैसे $i \neq j$

इसी कारण $aa_1, aa_2, ..., aa_n$ में से कोई दो समतुल्य नहीं हो सकते।

ये संख्या n में होंगे जो कि G के सुनिश्चित सदस्य होंगे (ध्यान दें: $o(G) = n$)

इसी प्रकार यदि $b \in G$ कोई अवयव हो तब i के किसी मान के लिये $b = aa_i$

अर्थात् $a, b \in G$ हेतु समीकरण $ax = b$, G में $(x = a_i)$ का हल है।

इसी प्रकार समीकरण $ya = b$ में G का हल होगा।

G एक अर्द्ध समूह है, अतः G में संबंद्धता स्थित (Hold) है।

इसी कारण से G एक समूह है (प्रमेय 1.2 से)।

टिप्पणी: उपरोक्त प्रमेय परिमित अर्द्ध समूह में ही स्थित है। योग (Addition) के अधीन प्राकृतिक संख्याओं (Natural Numbers) का अर्द्ध समूह ऐसा उदाहरण है, जहाँ निष्कासित नियम स्थित हैं परन्तु यह एक समूह नहीं है।

प्रमेय 1.5: परिमित अर्द्ध समूह तभी, अर्द्ध समूह होता है, यदि उसमें निष्कासित नियम की पूर्ति होती हो।

प्रमाण: पूर्ववर्ती प्रमेय अनुरूप।

परिभाषा: गैर रिक्त समुच्चय G के साथ द्विआधारी संरचना '.' से एकाभ (Monoid) का निर्माण होना कहा जाता है, यदि

(*i*) $a(bc) = (ab)c \quad \forall\ a, b, c \in G$

(*ii*) $\exists$ एक अवयव (Element) $e \in G$ इस प्रकार है, $ae = ea, a\ \forall\ a \in G$

तो G को e की तत्समक कहते हैं। यह सरलता से प्रस्तुत किया जा सकता है, कि e अद्वितीय है।

अतः सभी समूह एकाभ हैं एवं सभी एकाभ अर्द्ध समूह (Semi Group) हैं।

जब हम समूह को परिभाषित करते हैं तो हम ध्यान देते हैं कि $\exists$ एक अवयव e है जो दाएँ व बाएँ तत्समक के रूप में कार्य करता है एवं प्रत्येक अवयव में दोनों ओर व्युत्क्रम होता है। अब हम दर्शाते हैं कि यह वास्तव में आवश्यक नहीं है एवं प्रत्येक

टिप्पणी

अवयव के लिये मात्र एक–ओर पहचान व समान ओर (Same Side) व्युत्क्रम द्वारा भी समूह का प्रणाली (System) बनाया जा सकता है।

प्रमेय 1.6: प्रणाली (System) $< G, . >$ द्वारा समूह का निर्माण किया जाता है यदि,

(*i*) $a(bc) = (ab)c$ सभी के लिए $a, b, c \in G$

(*ii*) $\exists\ e \in G$, इस प्रकार, $ae = a$ सभी के लिए $a \in G$

(*iii*) सभी के लिए $a \in G, \exists\ a' \in G, s.t., aa' = e.$

प्रमाण: यदि G एक समूह है तब हमें कुछ भी सिद्ध करने की आवश्यकता नहीं है, क्योंकि परिणाम परिभाषानुसार होगा। इसके विपरीत प्रदर्शित नियमों/पदों को देखें।

हम सबको यह दर्शाने की आवश्यकता है कि सभी $a \in G$ के लिए $ea = a$ यह दर्शाने की आवश्यकता होती है।

व $a \in G$ के लिए $a'a = a$

माना $a \in G$ कोई अवयव है।

पद (*iii*) के अनुसार $\exists\ a' \in G$, इस प्रकार, $aa' = e$

$\therefore$ $a' \in G$, के लिए $\exists\ a'' \in G$, इस प्रकार, $a'a'' = e$ ((*iii*) पद के अनुसार)

अब $$a'a = a'(ae) = (a'a)e = (a'a)(a'a'')$$
$$= a'(aa')a'' = a'(e)a'' = (a'e)a'' = a'a'' = e.$$

किसी भी $a \in G$ के लिए इस प्रकार, $\exists\ a' \in G,\quad aa' = a'a = e$

पुनः $$ea = (aa')a = a(a'a) = ae = a$$

$\therefore$ $$ae = ea = a \quad \text{सभी } a \in G \text{ के लिए}$$

अर्थात्, e, G के तत्समक है।

संकेतन: G ऐसा समूह है जिसकी द्विआधारी संरचना '.' है। यदि $a \in G$ कोई अवयव हो तो संवृत विशेषताओं से $a\ .\ a \in G$ हो। तब इसी प्रकार $(a\ .\ a)\ .\ a \in G$, इत्यादि।

यह अत्यन्त सुविधाजनक व स्वाभाविक होगा कि $a\ .\ a$ को a^2 से $a\ .\ (a\ .\ a)$ या $(a\ .\ a).\ a$ को a^3 से इत्यादि इंगित किया जाये। पुनश्च $a^{-1}.\ a^{-1}$ को a^{-2} से इंगित किया जायेगा एवं चूँकि $a\ .\ a^{-1} = e$ तो इसे $e = a^0$ द्वारा इंगित करना उचित ही रहेगा। अब हमारे संकेतन की विषयवस्तु को समझना सरल है,

$$a^m\ .\ a^n = a^{m+n}$$
$$(a^m)^n = a^{mn}$$

जहाँ m,n पूर्णांक (Integers) हैं।

यदि समूह के द्विआधारी संरचना को + से इंगित किया जाता है, तो हम गुणनफल व घातों (Powers) के स्थान पर गुणजों व योग की बात करेंगे। इस प्रकार यहाँ $2a = a + a$, व $na = a + a + ... + a$ (n बार) यदि n धनात्मक पूर्णांक (Positive Integer) है। यदि n ऋणात्मक पूर्णांक हो, तो $n = -m$ जहाँ m धनात्मक है, व हम m को $na = -ma = (-a) + (-a) + ... + (-a)$ परिभाषित करते हैं।

उदाहरण 1.13: यदि G कोटि n का परिमित समूह है, तो दर्शायें कि किसी $a \in G$, $\exists$ के लिये कोई धनात्मक पूर्णांक r, $1 \le r \le n$ इस प्रकार है कि $a^r = e$।

हल: चूँकि $o(G) = n$ अतः G में n अवयव हैं।

माना $a \in G$ कोई अवयव मानने पर संवृत गुणधर्म अनुरूप $a^2, a^3, \ldots$ हो तब ये सभी G से सम्बद्ध हैं।

$e, a, a^2, \ldots, a^n$ का विचार करें।

ये $n+1$ अवयव हैं (G में सभी) परन्तु G में मात्र n अवयव हैं।

इनमें से कम से कम दो अवयव समतुल्य हैं। यदि $a, a^2, \ldots, a^n$ में से कोई e के समतुल्य हो तो हमारा परिणाम सिद्ध हुआ। यदि नहीं तो कुछ $a^i = a^j$ के लिये i, j, $1 \le i, j \le n$। व्यापकता की किसी हानि के बिना हम $i > j$ प्राप्त कर सकते हैं।

तो $\quad a^i = a^j$

$\Rightarrow a^i \,.\, a^{-j} = a^j \,.\, a^{-j}$

$\Rightarrow a^{i-j} = e \quad$ जहाँ $1 \le i - j \le n.$

$i - j = r$ को रखने से हमें आवश्यक परिणाम ज्ञात होता है।

उदाहरण 1.14: मान लेते हैं कि $(ab)^n = a^n b^n$ समस्त $a, b \in G$ हेतु $n > 1$, जहाँ निश्चित पूर्णांक है।

दर्शायें कि $\quad (i)\ (ab)^{n-1} = b^{n-1}a^{n-1}$

$(ii)\ a^n\, b^{n-1} = b^{n-1}a^n$

$(iii)\ (aba^{-1}b^{-1})^{n(n-1)} = e \quad$ सभी $a, b \in G$

हल: (i) हमारे पास,

$$[b^{-1}(ba)b]^n = b^{-1}(ba)^n b$$

और $\quad [b^{-1}(ba)b]^n = (ab)^n$

$$(ab)^n = b^{-1}(ba)^n b$$

$$\Rightarrow (ab)^{n-1}ab = b^{-1}(b^n a^n)b$$

$$\Rightarrow (ab)^{n-1} = b^{n-1}a^{n-1} \quad \text{सभी } a, b \in G$$

(ii) अब $(a^{-1}b^{-1}ab)^n = a^{-n}b^{-n}a^n b^n$

$$(a^{-1}b^{-1}ab)^n = a^{-n}(b^{-1}ab)^n$$

$$= a^{-n}b^{-1}a^n b$$

$$\therefore \quad a^{-n}b^{-n}a^n b^n = a^{-n}b^{-1}a^n b$$

$$\Rightarrow a^n b^{n-1} = b^{n-1}a^n \quad \text{सभी } a, b \in G$$

(iii) मान लो $(aba^{-1}b^{-1})^{n(n-1)}$

$$= [(aba^{-1}b^{-1})^{n-1}]^n$$

$$= [(ba^{-1}b^{-1})^{n-1}a^{n-1}]^n \text{ पद } (i) \text{ के अनुसार}$$

$$= [ba^{-(n-1)}b^{-1}a^{n-1}]^n = [b(a^{-(n-1)}b^{-1}a^{n-1})]^n$$

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

टिप्पणी

$= a^{-(n-1)}b^n b^{-n}a^{n-1}$ पद (ii) के अनुसार

$= e$ सभी $a, b \in G$.

टिप्पणी

1.3 उपसमूह

हमने देखा है कि वास्तविक संख्याओं के समुच्चय **R** से योग (Addition) के अधीन समूह का निर्माण होता है, तथा पूर्णांकों के समुच्चय द्वारा भी योग के अधीन समूह निर्मित होता है। **Z, R** का उप–समुच्चय है। यह उन कई परिस्थितियों में से एक है जिनसे हम निम्नांकित को पढ़ने के लिए प्रेरित हुए।

परिभाषा: समूह G का गैर रिक्त उप–समुच्चय H, G का एक उपसमूह कहा जायेगा यदि H से G के द्विआधारी संरचना के अधीन समूह का निर्माण होता है।

स्पष्ट है कि यदि H, G का उपसमूह है एवं K, H का उपसमूह है तो K, G का उपसमूह है।

यदि G तत्समक अवयव e युक्त समूह है, तो उप–समुच्चयों $\{e\}$ व G, G के नगण्य उपसमूह हैं एवं हम इन्हें नगण्य उपसमूह कहते हैं। समस्त अन्य उपसमूहों को गैर नगण्य अथवा उचित उपसमूह (Proper Sub-Groups) कहा जायेगा।

इस प्रकार सरलता से यह देखा जा सकता है कि सम पूर्णांकों (Even Integers) से $(\mathbf{Z}, +)$ के उपसमूह का निर्माण होता है, जो कि $(\mathbf{Q}, +)$ का एक उपसमूह है जो कि $(\mathbf{R}, +)$ का एक उपसमूह है।

पुनः उप–समुच्चय $\{1, -1\}$ गुणन (Multiplication) के अधीन
$G = \{1, -1, i, -i\}$ का उपसमूह होगा।

ध्यान दें: $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ विधि 5 योग के अधीन **Z** का उपसमूह नहीं है क्योंकि मापांकों के योग 5, **Z** की संरचना नहीं है। इसी प्रकार $\mathbf{Z}_5$ $\mathbf{Z}_6$ का उपसमूह नहीं है, इत्यादि।

हम कभी–कभी यह दर्शाने के लिये संकेतन $H \leq G$ का प्रयोग करते हैं कि H, G का उपसमूह है, एवं $H < G$ का तात्पर्य यह है कि H, G का उचित उपसमूह है।

किसी समय यह परखना कठिन हो सकता है कि समूह G का प्रदर्शित उप–समुच्चय H एक उपसमूह है कि नहीं, इसमें समूह की परिभाषा में समस्त अभिगृहीत को परखना होगा। निम्नांकित दो प्रमेयों (विशेषतया द्वितीय) से इस कार्य के सरलीकरण में समय लगेगा।

प्रमेय 1.7: समूह G का गैर रिक्त उप–समुच्चय H, G का उपसमूह है, यदि

(i) $a, b \in H \Rightarrow ab \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$.

प्रमाण: H, G का उपसमूह है, तो परिभाषानुरूप इसमें (i) व (ii) के पदों की पूर्ति होती हैं।

इसके विपरीत प्रदर्शित पद H में हैं।

पद (i) द्वारा H में संवृत है।

पुनः $a, b, c \in H \Rightarrow a, b, c \in G \quad \Rightarrow \quad a(bc) = (ab)c$

इसी कारण संबद्धता H में है।

किसी भी $a \in H, a^{-1} \in H$ के लिये एवं इसलिये पद (i) के अनुसार

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

इस प्रकार H में तत्समक है।

H के प्रत्येक अवयव का व्युत्क्रम पद (ii) के अनुसार H में है।

इसी कारण H से समूह की परिभाषा में समस्त पदों की पूर्ति होती हैं, एवं इस प्रकार इससे समूह बनता है व इसीलिये G का उपसमूह भी।

प्रमेय 1.8: समूह G का गैर शून्य उप–समुच्चय H, G का उपसमूह यदि,

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

प्रमाणः यदि H, G का उपसमूह है, तो $a, b \in H \Rightarrow ab^{-1} \in H$ (परिभाषा का प्रयोग करते हुए सरलता अनुकरण)।

इसके विपरीत प्रदर्शित पद H में है।

H में संबंद्धता को पूर्ववर्ती प्रमेय अनुसार अनुकरण किया जाता है।

माना $a \in H$ कोई अवयव $(H \neq \varphi)$ है

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

अतः H में तत्समक है।

पुनः किसी $a \in H$, जैसे $e \in H$ के लिये $ea^{-1} \in H \Rightarrow a^{-1} \in H$

अर्थात् H में प्रत्येक अवयव का व्युत्क्रम है।

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

अर्थात् H गुणन (Multiplication) के अधीन संवृत (Closed) है।

इसी कारण H से समूह का निर्माण होता है एवं इसीलिये G के उपसमूह का भी।

टिप्पणीः यदि समूह का द्विआधारी संरचना + द्वारा इंगित किया जाता है तो उपरोक्त पदों को इस प्रकार पढ़ा जायेगा $a, b \in H \Rightarrow a - b \in H$। यह भी ध्यान दे, कि e सदा ही H में है।

हो सकता है कि निम्नांकित प्रमेय अत्यधिक उपयोगी सिद्ध न हो क्योंकि यह परिमित उप–समुच्चयों में ही सीमित है, परन्तु फिर भी इसका महत्त्व है।

उदाहरण 1.15: वास्तविकता पर समस्त 2×2 गैर एकाकी आव्यूह (Non-Singular Matrix) का समूह G है। G का केन्द्र ज्ञात करें।

हलः यदि $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $Z(G)$ के केन्द्र G का कोई अवयव हो, तो इसे G के समस्त सदस्यों के साथ क्रमविनिमय (Commute) एक विशेष रूप से होना चाहिए।

टिप्पणी

टिप्पणी

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

$$\Rightarrow\ b = c,\ a = d$$

अतः $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ प्राप्त होता है,

$$\begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix}$$

$$\Rightarrow\ a + b = a,\ b = c = 0$$

इसी कारण $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ का कोई सदस्य $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ प्रकार $Z(G)$ का हो जायेगा।

अन्य शब्दों में केन्द्र $Z(G)$ के सदस्यों G के 2×2 अदिश आव्यूह (Scalar Matrices) हैं।

उदाहरण 1.16: G ऐसा समूह है जिसमें

$$(ab)^3 = a^3b^3$$

$$(ab)^5 = a^5b^5, \quad \text{समस्त } a, b \in G$$

दर्शायें कि G एबेलियन (Abelian) है।

हल: हम सर्वप्रथम दर्शाते हैं, कि समस्त $b \in G$ हेतु $b^2 \in Z(G)$

हमें विदित है कि $(a^{-1}ba)^3 = a^{-1}\, b^3a$

दिये गए पद के अनुसार

$$(a^{-1}ba)^3 = a^{-3}\,(ba)^3 = a^{-3}\, b^3a^3$$

$$\Rightarrow \quad a^{-1}\, b^3a = a^{-3}\, b^3a^3$$

$$\Rightarrow \quad a^2b^3 = b^3a^2 \quad \text{समस्त } a, b \in G$$

इसी प्रकार $(a^{-1}\, ba)^5 = a^{-1}\, b^5\, a$

$$(a^{-1}\, ba)^5 = a^{-5}\, b^5a^5$$

$$\Rightarrow \quad a^{-1}\, b^5a = a^{-5}\, b^5a^5$$

$$\Rightarrow \quad a^4b^5 = b^5a^4 \Rightarrow a^4b^3b^2 = b^5a^4$$

$$\Rightarrow \quad (a^2)^2\, b^3b^2 = b^5a^4 \Rightarrow b^3a^4b^2 = b^5a^4$$

$$\Rightarrow \quad a^4b^2 = b^2a^4 \Rightarrow aa^3b^2 = b^2a^4$$

$$\Rightarrow \quad ab^2a^3 = b^2a^4$$

$$\Rightarrow \quad ab^2 = b^2a \quad \text{समस्त } a, b \in G$$

$$\therefore \quad b^2 \in Z(G) \quad \text{समस्त } b \in G$$

अब $(ab)^4 = (ab)^5\,(ab)^{-1} = a^5b^5b^{-1}\, a^{-1}$

$= a^5b^4a^{-1} = a^5a^{-1}b^4$, जैसे $b^2 \in Z(G) = a^4b^4$

तीन क्रमिक पूर्णांकों $i = 3, 4, 5$ के लिये $(ab)^i = a^ib^i$

अतः समस्त $a, b \in G$ हेतु $ab = ba$

इसी कारण G एबेलियन (Abelian) है।

टिप्पणी

उदाहरण 1.17: दर्शायें कि समस्त $a, x \in G$ हेतु $N(x^{-1} ax) = x^{-1} N(a)x$

हल: माना $y \in N(x^{-1} ax)$

तो $(x^{-1} ax)\, y = y\,(x^{-1} ax)$

$\Rightarrow$ $y^{-1} x^{-1} axy = x^{-1} ax$

$\Rightarrow$ $xy^{-1} x^{-1} a = axy^{-1} x^{-1}$

$\Rightarrow$ $xy^{-1} x^{-1} \in N(a)$

$\Rightarrow$ $xy^{-1} x^{-1} = b \in N(a)$

$y^{-1} = x^{-1} bx$

$\Rightarrow$ $y = x^{-1} b^{-1} x,\ b^{-1} \in N(a)$ जैसे $b \in N(a)$

$\Rightarrow$ $y \in x^{-1} N(a)x$

$\therefore$ $N(x^{-1} ax) \subseteq x^{-1} N(a)\, x$

माना $z \in x^{-1} N(a)x \Rightarrow z = x^{-1} cx,\ c \in N(a)$

$\therefore$ $z(x^{-1} ax) = (x^{-1} cx)\ (x^{-1} ax)$

$= x^{-1} cax$

$= x^{-1} acx$ as $c \in N(a)$

$= (x^{-1} ax)\ (x^{-1} cx)$

$= (x^{-1} ax)z$

$\Rightarrow$ $z \in N(x^{-1} ax)$

$\Rightarrow$ $x^{-1} N(a)x \subseteq N(x^{-1} ax)$

$\Rightarrow$ $x^{-1} N(a)x = N(x^{-1} ax)$ समस्त $a, x \in G$.

यह दर्शाना एक सरल कार्य होगा कि दो उपसमूहों का सर्वनिष्ठ (Inter-Section) एक उपसमूह होगा। वस्तुतः सिद्ध किया जा सकता है कि यदि $\{H_i \mid i \in I\}$ समूह G के उपसमूहों का कोई समुच्चय हो, तो $\underset{i \in I}{\cap} H_i$ G का उपसमूह होगा।

प्रमेय 1.9: दो उपसमूहों का संघ एक उपसमूह है, यदि इनमें से एक दूसरे में अन्तर्विष्ट हो।

प्रमाण: H, K समूह G के दो उपसमूह हैं, एवं मान लेते हैं कि $H \subseteq K$ तो $H \cup K = K$ जो कि G का उपसमूह है।

इसके विपरीत $H, K,\ G$ के दो उपसमूह इस प्रकार हैं, कि $H \cup K$ भी G का उपसमूह है। हम दर्शाते हैं कि उनमें से एक में दूसरा अन्तर्विष्ट होना चाहिए। मान लें कि यह वास्तविकता न हो, अर्थात् $H \not\subseteq K, K \not\subseteq H$

टिप्पणी

तो $\exists\, x \in H$ इस प्रकार, $x \notin K$

$\exists\, y \in K$ इस प्रकार, $y \notin H$

तो भी $x, y \in H \cup K$ और चूंकि $H \cup K$ उपसमूह है, $xy \in H \cup K$

$\Rightarrow xy \in H$ या $xy \in K$

यदि $xy \in H$ तो $x \in H, x^{-1}(xy) \in H \Rightarrow y \in H$ जो कि वास्तविकता नहीं है।

पुनः यदि $xy \in K$ तो $y \in K, (xy)y^{-1} \in K \Rightarrow x \in K$ जो कि वास्तविकता नहीं है, अर्थात् हर प्रकार से हम विरोधाभास की ओर बढ़ते हैं।

इसी कारण हमारी मान्यता है, कि $H \not\subseteq K$ व $K \not\subseteq H$ सत्य नहीं है।

इस प्रकार दो में से एक अन्य में अन्तर्विष्ट है।

परिभाषाः G समूह H का उपसमूह है। $a, b \in G$ हेतु $a,\ b \bmod H$ के अनुकूल (Congruent) है यदि $ab^{-1} \in H$

सांकेतन रूप में हम $a \equiv b \bmod H$ लिखते हैं।

सरलता से यह सिद्ध किया जा सकता है, कि यह सम्बन्ध एक समतुल्यता सम्बन्ध है। इस समतुल्यता सम्बन्ध के संगत (Corresponding) हम समतुल्यता वर्गों को प्राप्त कर सकते हैं। किसी $a \in G$ के लिये हमें विदित है कि a का समतुल्यता वर्ग इस प्रकार स्पष्ट होगा,

$$cl(a) = \{x \in G \mid x \equiv a \bmod H\}$$

परिभाषाः $H,\ G$ का उपसमूह है एवं $a \in G$ कोई अवयव तो $Ha = \{ha \mid h \in H\}$ को G में H का दाएँ सहसमुच्चय (Coset) कहते हैं।

निम्नांकित प्रमेय में हम दर्शाते हैं, कि G में H का कोई दाएँ सहसमुच्चय एक समतुल्यता वर्ग है। सटीक होने के लिये हमें निम्न प्रमेय को सिद्ध करना होगा।

प्रमेय 1.10: $Ha = \{x \in G \mid x \equiv a \bmod H\} = cl(a)$ समस्त $a \in G$.

प्रमाणः माना $x \in Ha$

तो $x = ha$ कुछ $h \in H$

$\Rightarrow xa^{-1} = h$

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

$\Rightarrow x \equiv a \bmod H$

$\Rightarrow x \in cl(a)$

इस प्रकार $Ha \subseteq cl(a)$.

पुनः माना $x \in cl(a)$ कोई अवयव है

तो $x \equiv a \bmod H$

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

$\Rightarrow xa^{-1} = h$ समस्त $h \in H$

$\Rightarrow x = ha \in Ha$

टिप्पणी

इस प्रकार $cl(a) \subseteq Ha$

एवं इसी कारण $Ha = cl(a)$.

पहले से स्पष्ट है कि दाएँ सहसमुच्चय समतुल्यता वर्ग हैं, हम उन परिणामों का प्रयोग करने के लिये स्वतन्त्र हैं जो हम समतुल्यता वर्गों के बारे में जानते हैं। इसीलिये हम अब कह सकते हैं, कि कोई भी दो दाएँ सहसमुच्चय या तो समतुल्य होते हैं अथवा इनमें सामान्य में कोई अवयव नहीं होता तथा H में G के समस्त दाएँ सहसमुच्चय का संघ G के समतुल्य होगा।

टिप्पणी: ध्यान दे, कि यह आवश्यक नहीं कि सहसमुच्चय एक उपसमूह हो ही। यदि G चतुष्क (Quaternion) समूह है, तो $H = \{1, -1\}$, G का उपसमूह है। $a = i$ प्राप्त करें तो $Ha = \{i, -i\}$ जो कि G का उपसमूह नहीं है (इसकी तत्समक नहीं है)।

लैमा: G में H के किन्हीं भी दो दाएँ सहसमुच्चय के मध्य मानचित्रण में सदा ही 1 – 1 होता है।

प्रमाण: माना Ha, Hb में G में H के दो दाएँ सहसमुच्चय हैं।

मानचित्रण को परिभाषित करते हैं $f: Ha \to Hb$, इस प्रकार,

$$f(ha) = hb$$

तो $$h_1a = h_2a \Rightarrow h_1 = h_2 \Rightarrow h_1b = h_2b$$

$$\Rightarrow f(h_1a) = f(h_2a)$$

अर्थात् f सुस्पष्ट है।

$f(h_1a) = f(h_2a) \Rightarrow h_1b = h_2b \Rightarrow h_1 = h_2 \Rightarrow h_1a = h_2a$

दिख रहा है कि f, (1–1) है।

अर्थात् बीच में f को सरलता से देखा जा सकता है– जैसे कि किसी $hb \in Hb$ के लिये ha इसकी पूर्व प्रतिबिंब होगी।

इस लैमा की तात्कालिक उपयोगिता दिख चुकी है यदि समूह G परिमित हो क्योंकि उस प्रकरण में लैमा इस बात को दृढ़ कर देता है कि G में H के किन्हीं दो दाएँ सहसमुच्चय में समान संख्या में अवयव हैं। चूँकि $H = He$ भी G में H का दाएँ सहसमुच्चय है तो इससे हम इस निष्कर्ष पर आते हैं, कि G में H के सभी दाएँ सहसमुच्चय में उतनी ही संख्या के अवयव हैं जितनी संख्या के अवयव H में हैं (G होने से यह परिमित है)। अब हम यह सिद्ध कर सकते हैं।

प्रमेय 1.11 (लैग्रांज (Lagrange) से): यदि G परिमित समूह हो व H, G का उपसमूह हो तो $o(H)$ से $o(G)$ को भाग देते हैं।

प्रमाण: माना $o(G) = n$

चूँकि G में प्रत्येक अवयव के संगत (Corresponding) हम G में H का दाएँ सहसमुच्चय (Right Coset) परिभाषित कर सकते हैं अतः G में H के सुनिश्चित (Distinct) दाएँ सहसमुच्चय की संख्या n से कम अथवा इसके समतुल्य है।

समतुल्यता–वर्गों की विशेषताओं का प्रयोग करते हुए हमें विदित है,

$$G = Ha_1 \cup Ha_2 \cup ... \cup Ha_t$$

जहाँ t = संख्या G में H के सुनिश्चित दाएँ सहसमुच्चय की संख्या,

$$\Rightarrow \quad o(G) = o(Ha_1) + o(Ha_2) + ... + o(Ha_t)$$

टिप्पणी

स्मरण रखना होगा कि दो दाएँ सहसमुच्चय या तो समान होते हैं अथवा कोई सामान्य अवयव नहीं होता।

$\Rightarrow o(G) = o(H) + o(Ha) \underset{t \text{ बार}}{+...+} o(H)$ उपरोक्त लैमा के प्रयोग से,

$$\Rightarrow \quad o(G) = t.\, o(H)$$

अथवा $o(H) \mid o(G)$

एवं हमने अति महत्त्वपूर्ण प्रमेय सिद्ध किया किन्तु सावधानी आवश्यक है। लैग्रांज–प्रमेय का विलोम नहीं होता।

टिप्पणी: (i) यदि G अभाज्य कोटि का समूह है तो इसमें दो ही उपसमूह होंगे: G व $\{e\}$।

(ii) $H \neq G$ के आधे अवयव से अधिक वाला उप–समुच्चय G, G का उपसमूह नहीं हो सकता।

हम G में H के दाएँ सहसमुच्चय की ही बात करते रहे हैं। क्या बाएँ सहसमुच्चय भी होते हैं? हम समानता की चर्चा कर सकते हैं,

$aH = \{ah \mid h \in H\}$, किसी $a \in G$

जिसे कि बाएँ सहसमुच्चय कहा जायेगा। इसी प्रकार समतुल्यता–सम्बन्ध ($a \equiv b \bmod H \Leftrightarrow a^{-1} b \in H$) परिभाषित करते हुए बाएँ सहसमुच्चय के लिये समस्त समान परिणामों को सिद्ध किया जा सकता है। यह पाठक के लिये वस्तुतः एक रोचक तैयारी होगी यदि इन परिणामों को स्वतन्त्र रूप से सिद्ध किया जाये तो।

अब हम सरल किन्तु अत्यन्त महत्त्वपूर्ण तथ्य की ओर बढ़ते हैं।

प्रमेय 1.12: H, G का उपसमूह हो तो

(i) $Ha = H \Leftrightarrow a \in H$; $aH = H \Leftrightarrow a \in H$

(ii) $Ha = Hb \Leftrightarrow ab^{-1} \in H$; $aH = bH \Leftrightarrow a^{-1} b \in H$

(iii) Ha (अथवा aH) G का उपसमूह है यदि $a \in H$

प्रमाण: (i) $Ha = H$

चूँकि $e \in H, ea \in Ha \Rightarrow ea \in H \Rightarrow a \in H.$

माना $a \in H$, हम दर्शाते हैं $Ha = H.$

माना $x \in Ha \Rightarrow x = ha$ के लिए $h \in H$

अब $h \in H, a \in H \Rightarrow ha \in H \Rightarrow x \in H \Rightarrow Ha \subseteq H$

पुनः $y \in H$, चूंकि $a \in H$

$ya^{-1} \in H$

टिप्पणी

$\Rightarrow ya^{-1} = h$ कुछ $h \in H$ के लिए

$\Rightarrow y = ha \in Ha$

$\Rightarrow H \subseteq Ha$

इसी कारण $Ha = H$.

(ii) $Ha = Hb$

$\Leftrightarrow (Ha)b^{-1} = (Hb)b^{-1}$

$\Leftrightarrow Hab^{-1} = He$

$\Leftrightarrow Hab^{-1} = H$

$\Leftrightarrow ab^{-1} \in H$ पद (i) के प्रयोग से।

(iii) यदि $a \in H$ तो $Ha = H$ जो कि एक उपसमूह है। इसके विपरीत यदि Ha G. का उपसमूह हो तो $e \in Ha$ तथा इस प्रकार Ha व He के दाएँ सहसमुच्चय में सामान्य में e एक अवयव है, एवं इसी कारण पद (i) से $Ha = He = H \Rightarrow a \in H$।

बाएँ सहसमुच्चय के लिये संगत परिणामों को भी इसी प्रकार पाया जा सकता है।

परिभाषा: माना H, G का समूह है एवं G का उपसमूह। अब G में H का निर्देशिका G में H के सुनिश्चित दाएँ, बाएँ सहसमुच्चय (Coset) की संख्या है। इसे $i_G(H)$ अथवा $[G:H]$ द्वारा इंगित किया जाता है।

लैग्रांज–प्रमेय के प्रमाण की ओर देखने पर सामने आता है, कि यदि G एक परिमित समूह है तो $i_G(H) = \frac{o(G)}{o(H)}$ ।

अपरिमित समूह G में सीमित निर्देशिका युक्त उपसमूह $H \neq G$ होना सम्भव है।

उदाहरण 1.18: माना $< \mathbf{Z}, + >$ योग (Addition) अधीन गुणांकों (Integers) का समूह है।

माना $H = \{3n \mid n \in \mathbf{Z}\}$ तो $\mathbf{Z}$ का उपसमूह H है। हम दर्शाते हैं, कि H में $\mathbf{Z}$ में तीन ही दाएँ सहसमुच्चय हैं: $H, H+1, H+2$ है।

यदि $a \in \mathbf{Z}$ $(\neq 0, 1, 2)$ कोई अवयव हो तो हम $a = 3n + r, 0 \leq r < 3$ यह लिख सकते हैं (विभाजन एल्गोरिद्म (Division Algorithm) द्वारा)।

जिससे $H + a = H + (3n + r) = (H + 3n) + r = H + r$

जहाँ $0 \leq r < 3$

इसी कारण $\mathbf{Z}$ के H में 3 ही दाएँ सहसमुच्चय हैं तथा इस प्रकार इसमें निर्देशांक 3 है।

ध्यान दें: $H - 1 = (H + 3) - 1 = H + (3 - 1) = H + 2$, इत्यादि।

परिभाषा: G समूह H का उपसमूह है, हम परिभाषित करते हैं $C(H) = \{x \in G \mid xh = hx$ सभी $h \in H$ के लिए$\}$ तो $C(H)$ को G में H का केन्द्रीयकरण (Centralization) कहा जाता है।

$N(H) = \{x \in G \mid xH = Hx\}$

$= \{x \in G \mid xHx^{-1} = H\}$ इसे G में H का सामान्यीकरण (Normalization) कहते हैं।

टिप्पणी

यह सरलता से देखा जा सकता है कि $C(H)$ व $N(H)$ G के उपसमूह हैं।

पुनरपि $x \in C(H) \Rightarrow xh = hx$ सभी $h \in H$ के लिए

$\Rightarrow xH = Hx$

$\Rightarrow x \in N(H)$

ध्यान दें: $C(H) \subseteq N(H)$

वैसे $C(H)$ को $N(H)$ के समतुल्य करने की आवश्यकता नहीं है, क्योंकि चतुष्क समूह है माना कि $H = \{\pm 1, \pm i\}$ तब विचार करें,

$G = \{\pm 1, \pm i, \pm j, \pm k\}$ तो $N(H) = G$ और $C(H) = \{\pm 1, \pm i\}$

प्रदर्शित है, कि $C(H) \neq N(H)$

उदाहरण 1.19: दर्शायें कि $C(H) = G \Leftrightarrow H \subseteq Z(G)$

हल: माना $C(H) = G$ कोई अवयव है तो $x \in G \Rightarrow x \in C(H) \Rightarrow xh = hx \Rightarrow$ में $h \in H$ अवयव h, H के समस्त अवयवों सहित क्रम विनिमेय है।

इसके विपरीत $G \Rightarrow h \in Z(G) \Rightarrow H \subseteq Z(G)$। चूँकि $H \subseteq Z(G)$ अतः माना $H \subseteq Z(G)$. माना $x \in G$ का हर अवयव H और G के प्रत्येक अवयव से क्रम विनिमेय है।

$\Rightarrow xh = hx$ सभी $h \in H$ के लिए

$\Rightarrow x \in C(H) \Rightarrow G \subseteq C(H) \Rightarrow G = C(H).$

उदाहरण 1.20: यदि $G = S_3$ व $H = \{I, (13)\}$, G में H के समस्त बाएँ सहसमुच्चय लिखें।

हल: $(12)H = \{(12)I, (12)(13)\} = \{(12), (132)\}$

$= (123)H$ दर्शाया गया है।

$(23)H = \{(23)I, (23)(13)\} = \{(23), (132)\} = (132)H$

$(13)H = H$ क्योंकि $(13) \in H$

$IH = H$

ये G में H के सभी बाएँ सहसमुच्चय हैं।

अपनी प्रगति जांचिए

1. एबेलियन समूह क्या है?
2. साधारण रैखिक समूह का उदाहरण प्रस्तुत करें।
3. क्या समूह में तत्समक अवयव अद्वितीय होता है?
4. उपसमूहों को परिभाषित करें।

1.4 उप–समुच्चय द्वारा उत्पन्न उपसमूह

टिप्पणी

परिभाषा: H व K समूह G के दो उपसमूह हैं। हम $HK = \{hk \mid h \in H, k \in K\}$ परिभाषित करते हैं, तो HK का गैर–रिक्त उप–समुच्चय होगा (जिसे कभी–कभी H व K का सम्मिश्रण (Complex) कहा जाता है)। इसकी व्युत्पत्ति निम्नलिखित प्रमेय द्वारा की जा सकती है।

प्रमेय 1.13: *HK, G* का उपसमूह है यदि $HK = KH$

प्रमाण: HK G का उपसमूह है। हम $HK = KH$ दर्शाते हैं।

माना $x \in HK$ का अवयव है

तो $x^{-1} \in HK$ (जो कि HK एक उपसमूह है)

$$\Rightarrow x^{-1} = hk \quad \text{कुछ } h \in H \text{ के लिए, } k \in K$$

$$\Rightarrow x = (hk)^{-1} = k^{-1} h^{-1} \in KH$$

इस प्रकार $HK \subseteq KH$

पुनः $y \in KH$ कोई अवयव हो

तो $y = kh$ कुछ $k \in K$ के लिए, $h \in H$

$$\Rightarrow y^{-1} = h^{-1} k^{-1} \in HK$$

$$\Rightarrow y \in HK \quad \text{(जैसे } HK \text{ उपसमूह है)}$$

$$\Rightarrow KH \subseteq HK$$

इसी कारण $HK = KH$

इसके विपरीत माना कि $HK = KH$

$a, b \in HK$ दो अवयव हैं, तो हम दर्शाते हैं $ab^{-1} \in HK$

$$a, b \in HK \Rightarrow \quad a = h_1 k_1 \quad \text{कुछ के लिए } h_1, h_2 \in H$$
$$b = h_2 k_2 \qquad k_1, k_2 \in K$$

तो $$ab^{-1} = (h_1 k_1)\,(h_2 k_2)^{-1} = (h_1 k_1)\,(k_2^{-1} h_2^{-1})$$
$$= h_1 (k_1 k_2^{-1})\, h_2^{-1}$$

अब $$(k_1 k_2^{-1})\, h_2^{-1} \in KH = HK$$

इस प्रकार $(k_1 k_2^{-1})\, h_2^{-1} = hk$ कुछ $h \in H$ के लिए, $k \in K$

तो $$ab^{-1} = h_1 (hk) = (h_1 h) k \in HK$$

इसी कारण HK एक उपसमूह है।

टिप्पणी: (क) $HK = KH$ का तात्पर्य यह नहीं है, कि H का प्रत्येक अवयव K के हर अवयव से क्रम विनिमय करता है। इसका तात्पर्य बस यह है, कि प्रत्येक $h \in H, k \in K, hk = k_1 h_1$ हेतु के लिये $k_1 \in K$ और $h_1 \in H$।

(ख) यदि G में द्विआधारी संरचना + स्थित है तो हम परिभाषित कर सकते है कि,

$$H + K = \{h + k \mid h \in H, k \in K\}$$

टिप्पणी

प्रमेय 1.14: यदि H व K समूह G के परिमित उपसमूह हों तो,

$$o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)}$$

प्रमाण: $D = H \cap K$ तो D, K का एक उपसमूह है, एवं लैग्रांज–प्रमेय के प्रमाण में प्रदर्शित अनुरूप K में D के असंबद्ध दाएँ सहसमुच्चय में K का ∃ में वियोजित है।

$K = Dk_1 \cup Dk_2 \cup ... \cup Dk_t$

एवं $t = \frac{o(K)}{o(D)}$ भी

पुनश्च $HK = H(\overset{t}{\underset{i=1}{\cup}} Dk_i)$ एवं चूँकि $D \subseteq H, HD = H$

इस प्रकार $HK = \overset{t}{\underset{i=1}{\cup}} Hk_i = Hk_1 \cup Hk_2 \cup ... \cup Hk_t$

अब $Hk_1, Hk_2, ..., Hk_t$ के i, j समतुल्य हो सकते हैं क्योंकि यदि कुछ $Hk_i = Hk_j$ हेतु $k_i k_j^{-1} \in H \Rightarrow k_i k_j^{-1} \in H \cap K \Rightarrow k_i k_j^{-1} \in D \Rightarrow Dk_i = Dk_j$

जो कि वास्तविक नहीं है।

इसी कारण $(HK) = o(Hk_1) + (Hk_2) + ... + o(Hk_t)$

$= o(H) + o(H) + ... + o(H)$

$= t \cdot o(H)$

$= \frac{o(H) \cdot o(K)}{o(H \cap K)}$

जिससे परिणाम सिद्ध होता है।

1.5 चक्रीय समूह एवं सरल विशेषताएं

परिभाषा: अवयव का कोटि: G एक समूह है एवं $a \in G$ कोई अवयव। हम कह सकते हैं कि a कोटि (अथवा अवधि) n की है यदि n कम धनात्मक पूर्णांक (Positive Integer) इस प्रकार है कि $a^n = e$। यदि G के द्विआधारी संरचना को + द्वारा इंगित करते हैं, तो इसे $na = 0$ पढ़ा जायेगा जहाँ 0, G की तत्समक है।

यदि यह n खोजना सम्भव न हो तो हम कहते हैं कि a में अपरिमित कोटि (Infinite Order) है। a की कोटि को $o(a)$ द्वारा इंगित किया जायेगा। यह स्पष्ट है कि $o(a) = 1$ यदि $a = e$।

टिप्पणी

चक्रीय समूह (Cyclic Group): समूह G को चक्रीय समूह कहा जाता है यदि $\exists$ अवयव $a \in G$ इस प्रकार हो कि G के प्रत्येक अवयव को a की घात (Power) के रूप में व्यक्त किया जा सके। इस प्रकरण में a को G का उत्पन्नकारक कहते हैं। हम इस तथ्य को व्यक्त करने के लिये $G = < a >$ या $G = (a)$ लिखते हैं।

इस प्रकार G को चक्रीय कहा जाता है यदि $\exists$ अवयव $a \in G$ इस प्रकार हो कि $G = \{a^n \mid n \in \mathbf{Z}\}$। पुनः यदि G के द्विआधारी संरचना को + से इंगित किया जाता है तो 'a की घात' शब्दों का तात्पर्य a का गुणज (Mean Multiple) होगा।

ध्यान दें: हम यह नहीं कह रहे कि उत्पन्न कारक अद्वितीय होता है। वस्तुतः यदि a उत्पन्नकारक है तो a^{-1} होगा। हम कुछ बाद में इस प्रश्न पर आते हैं कि चक्रीय समूह में उत्पन्नकारक की संख्या कितनी है। चक्रीय समूह का एक सरल उदाहरण योग (Addition) के अधीन पूर्णांकों (Integer's) का समूह है, 1 इसका उत्पन्नकर्ता है।

पुनः गुणन के अधीन समूह $G = \{1, -1, i, -i\}$ चक्रीय है क्योंकि हम इसके सदस्यों को i, i^2, i^3, i^4 के रूप में व्यक्त कर सकते हैं। इस प्रकार i (अथवा $-i$) इस समूह का उत्पन्नकर्ता है।

प्रमेय 1.15: चक्रीय समूह की कोटि इसके उत्पन्नकर्ता की कोटि के समतुल्य है।

प्रमाण: माना $G = < a >$ अर्थात् G ऐसा चक्रीय समूह है जो a द्वारा उत्पन्नकर्ता है।

प्रकरण (i): $o(a)$ परिमित (Finite) है: n तो n कम धनात्मक पूर्णांक इस प्रकार है कि $a^n = e$

अवयवों $a^0 = e, a, a^2, ..., a^{n-1}$ का विचार करें।

ये सभी G के अवयव हैं एवं संख्या में n हैं।

मान लेते हैं कि उपरोक्त में से दो अवयव समतुल्य हैं, अर्थात्

$a^i = a^j$ के साथ $i > j$

तो $a^i \,.\, a^{-j} = e \Rightarrow a^{i-j} = e$

परन्तु $0 < i - j \le n - 1 < n$, इस प्रकार $\exists$ एक $i - j$ धनात्मक पूर्णांक इस प्रकार है कि $a^{i-j} = e$ व $i - j < n$ जो कि $o(a) = n$ इस तथ्य का विरोधाभास है।

इस प्रकार उपरोक्त n अवयव में से दो समतुल्य नहीं हो सकते हैं, अर्थात् G में कम से कम n अवयव होंगे। हम दर्शाते हैं कि इसमें कोई अन्य अवयव नहीं होता। माना $x \in G$ कोई अवयव है। चूँकि G चक्रीय है, जो कि x द्वारा उत्पन्न (Generator) है तो x, a की कोई घात होगी।

माना $x = a^m$ विभाजन एल्गोरिद्म द्वारा हम $m = nq + r$ लिख सकते हैं, जहाँ $0 \le r < n$.

अब $a^m = a^{nq+r} = (a^n)^q \,.\, a^r = e^q . a^r = a^r \Rightarrow x = a^r$ जहाँ $0 \le r < n$

अर्थात् x $a^0 = e, a, a^2, ..., a^{n-1}$ में से एक है अथवा G में परिशुद्धतया n अवयव हैं।

$\Rightarrow o(G) = n = o(a)$

टिप्पणी

प्रकरण (*ii*): $o(a)$ अपरिमित है।

जिस प्रकरण में a की दो घातें (Powers) $a^n = a^m$ $(n > m)$ समतुल्य न हो सकती हों, तो $a^{n-m} = e$, अर्थात् $a + ve$ पूर्णांक $n - m$ को इस प्रकार पाना सम्भव है कि $a^{n-m} = e$, अर्थात् इसके द्वारा a में यह परिमित कोटि (Finite Order) का होगा।

इसी कारण a की दो घातें समतुल्य नहीं हो सकतीं। अन्य शब्दों में G में अपरिमित संख्या के अवयव होंगे।

प्रमेय 1.16: चक्रीय समूह का एक उपसमूह चक्रीय है।

प्रमाण: माना $G = < a >$ व H, G का उपसमूह है, वहाँ कुछ भी सिद्ध नहीं करना है। यदि $H = \{e\}$ अपार यह कुछ सिद्ध नहीं हुआ तो माना $H \neq \{e\}$ है। H के सदस्यों में a की घातें (Powers) होंगी। m कम धनात्मक पूर्णांक इस प्रकार है, कि $a^m \in H$। हम दावा करते हैं कि $H = < a^m >$ कोई अवयव है तो किसी $x \in H$ के लिये $x = a^k$ होता है k के लिए। विभाजन एल्गोरिद्म (Division Algorithm) द्वारा $k = mq + r$ जहाँ $0 \leq r < m$,

$$\Rightarrow \quad r = k - mq$$

$$\Rightarrow \quad a^r = a^k \,.\, a^{-mq} = x \,.\, (a^m)^{-q} \in H$$

परन्तु m कम धनात्मक पूर्णांक इस प्रकार है कि $a^m \in H$, अर्थात् इससे $r = 0$।

इस प्रकार $k = mq$

अथवा $x = a^k = (a^m)^q$

अर्थात् H का कोई सदस्य a^m की घात है।

अथवा H चक्रीय है, a^m द्वारा उत्पन्न।

ध्यान दें: इसीलिये $< \mathbf{Z}, + >$ का कोई उपसमूह $n\mathbf{Z} =$ के गुणजों (Multiples) के प्रकार n समुच्चय का होगा जहाँ n एक पूर्णांक (≥ 0) है। हम $n\mathbf{Z} = < n >$ लिखते हैं।

उपरोक्त के अतिरिक्त $m\mathbf{Z} \subseteq n\mathbf{Z}$ तभी होगा यदि $n \mid m$। अतः $m\mathbf{Z} = n\mathbf{Z}$ तभी होगा यदि $m = \pm n$।

प्रमेय 1.17: एक चक्रीय समूह एबेलियन है।

प्रमाण: माना $G = < a >$। यदि $x, y \in G$ कुछ अवयव हों तो कुछ पूर्णांकों $x = a^n$, $y = a^m$ के लिये m, n।

अब $\quad xy = a^n \,.\, a^m = a^{n+m} = a^{m+n} = a^m \,.\, a^n = y \,.\, x$

इसी कारण G एबेलियन है।

ध्यान दें: उपरोक्त परिणाम के आलोक में समस्त गैर–एबेलियन समूह एबेलियन हैं। $< \mathbf{Q}, + >$ योग के अधीन परिमेयों (Rational) का समूह एक ऐसे एबेलियन समूह का उदाहरण है जो कि चक्रीय नहीं है। उदाहरण हेतु मान लेंवें कि $\frac{m}{n} \in \mathbf{Q}$, $\mathbf{Q}$ का उत्पन्नकर्ता है तो $\mathbf{Q}$ का कोई अवयव $\frac{m}{n}$ का गुणज (Multiple) होगा। अब $\frac{1}{3n} \in \mathbf{Q}$

व यदि $\frac{m}{n}$ उत्पन्नकर्ता हो तो हम किसी k के लिये $\frac{1}{3n} = k\frac{m}{n}$ लिख सकेंगे $\Rightarrow \frac{1}{3}$ $= km$ जो कि सम्भव नहीं है क्योंकि k, m पूर्णांक हैं जबकि $\frac{1}{3}$ नहीं। इसी कारण कोई अवयव **Q** के उत्पन्नकर्ता का कार्य नहीं कर सकता।

टिप्पणी

क्लॅइन्स के चार समूह (Klein's Four Groups) परिमित एबेलियन समूह का एक उदाहरण होगा जो कि चक्रीय नहीं है। यह गुणन आव्यूह के अधीन आव्यूह $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$, $\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}$ व $\begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}$ का समूह है।

प्रमेय 1.18: यदि G एक परिमित समूह हो तो G के किसी अवयव का समूह G के कोटि को विभाजित (Divide) करता है।

प्रमाण: माना $a \in G$ कोई अवयव है।

माना $H = \{a^n \mid n$ एक पूर्णांक$\}$ है तो H G का चक्रीय उपसमूह हुआ, a द्वारा उत्पन्नकारक,

$$x, y \in H \Rightarrow x = a^n, y = a^m$$

$$\therefore \quad xy^{-1} = a^n \cdot a^{-m} = a^{n-m} \in H$$

लैग्रांज–प्रमेय द्वारा $o(H) \mid o(G)$ परन्तु $o(H) = o(a)$

$$\therefore \quad o(a) \mid o(G).$$

उपप्रमेय: यदि G एक परिमित समूह है, तो किसी $a \in G$ के लिये $a^{o(G)} = e$

प्रमाण: $.o(a) \mid o(G) \Rightarrow o(G) = o(a)k$ किसी k के लिये

अब $a^{o(G)} = a^{o(a)k} = (a^{o(a)})^k = e^k = e$

इस प्रकार परिमित समूह के किसी अवयव में परिमित कोटि है (जो कि समूह के कोटि के समतुल्य अथवा इससे कम है)। वैसे इसका विलोम वास्तविक नहीं है।

प्रमेय 1.19: यदि G कोटि n की एक परिमित चक्रीय समूह है तो G के सुनिश्चित उपसमूहों की संख्या n के सुनिश्चित भाजकों (Divisor) की संख्या है एवं किसी भी प्रदर्शित कोटि के G के एक उपसमूह में अधिकांशतः यह होता है।

अतः G के उपसमूह $< a^k >$ प्रकार के हैं जहाँ k, n का भाजक (Divisor) है एवं $< a^{n/m} >$ कोटि m का अद्वितीय उपसमूह है। एक प्रकरणविशेष के रूप में मान लें कि $G = < a >$ में कोटि 30 है। चूँकि 30 के भाजक (Divisor) हैं– 1, 2, 3, 5, 6, 10, 15, 30, ∃ आठ उपसमूह है, G के जो कि निम्न हैं–

$$< a > = \{e, a, a^2, ..., a^{29}\} = G$$

$$< a^2 > = \{e, a^2, a^4, ..., a^{28}\}$$

$$< a^3 > = \{e, a^3, a^6, ..., a^{27}\}$$

$< a^5 >, < a^6 >, < a^{10} >, < a^{15} >$ व $< a^{30} > = \{e\}$ में कोटि 30, 15, 10, 6, 5, 3, 2, 1 है।

टिप्पणी

पुनः योग मापांक (Addition Modulo) 30 के अधीन चक्रीय समूह $\mathbf{Z}_{30} = \{0, 1, 2, ..., 29\}$ का विचार करें। 30 व $o(\mathbf{Z}_{30}) = 30$ तथा चूँकि 30 में 8 भाजक (Divisor) 1, 2, 3, 5, 6, 10, 15, 30, $\mathbf{Z}_{30}$ हैं,

$< 1 > = \{0, 1, 2, ..., 29\} = \mathbf{Z}_{30}$

$< 2 > = \{0, 2, 4, ..., 28\}$

$< 3 > = \{0, 3, 6, ..., 27\}$

$< 5 >, < 6 >, < 10 >, < 15 >, < 30 > = \{0\}$ में आठ उपसमूह होंगे।

कोटि 30, 15, 10, 6, 5, 3, 2, 1.

इस प्रमेय की दृष्टि से ये $\mathbf{Z}_{30}$ के उपसमूह ही होंगे।

प्रमेय 1.20: अभाज्य कोटि का समूह G चक्रीय होगा एवं G के प्रत्येक अवयव को (तत्समक छोड़कर) को इसके उत्पन्नकर्ता के रूप में प्राप्त किया जा सकता है।

प्रमाण: माना $o(G) = p$ अभाज्य (Prime) है।

किसी $a \in G, a \neq e$ को प्राप्त करें।

तथा $H = \{a^n |$ एक पूर्णांक n तो H G का चक्रीय उपसमूह है।

$\therefore o(H) \mid o(G) \Rightarrow o(H) = 1$ या p किन्तु $o(H) \neq 1$ क्योंकि $a \in H, a \neq e$,

इस प्रकार $o(H) = p \Rightarrow H = G$ अर्थात् G, a द्वारा उत्पन्नकर्ता चक्रीय समूह है। चूँकि a को किसी अवयव (e को छोड़कर) प्राप्त किया गया था तो G का कोई अवयव इसके उत्पन्नकारी के रूप में कार्य कर सकता है।

उपप्रमेय: अभाज्य कोटि का एक समूह एबेलियन है।

प्रमेय 1.21: अभाज्य कोटि के समूह G में कोई गैर–नगण्य उपसमूह नहीं हो सकता।

प्रमाण: यदि G में H का कोई उपसमूह हो तो $o(H) \mid o(G) = p$ के अनुरूप अभाज्य (Prime) है।

हम पाते हैं $o(H) = 1$ या p

अर्थात् $H = \{e\}$ या $H = G$

प्रमेय 1.22: परिमित संयोजित कोटि के समूह में कम से कम एक गैर–नगण्य उपसमूह है।

प्रमाण: माना $o(G) = n = rs$ जहाँ $1 < r, s < n$

चूँकि $n > 1, \exists\ e \neq a \in G$। a^r का विचार करें।

प्रकरण (*i*): $a^r = e$ तो $o(a) \leq r$, माना $o(a) = k$

तो $1 < k \leq r < n$ ($k > 1$, क्योंकि $a \neq e$)

माना $H = \{a, a^2, a^3, ..., a^k = e\}$

तो H, G का गैर–रिक्त परिमित उप–समुच्चय है एवं यह गुणन के अधीन संवृत है, इस प्रकार H, G का एक उपसमूह है। चूँकि $o(H) = k < n$ अतः हमने परिणाम सिद्ध किया।

प्रकरण (*ii*): $a^r \neq e$ तो चूँकि $(a^r)^s = a^{rs} = a^n = a^o(G) = e$

$o(a^r) \leq s$. माना $o(a^r) = t$ तो $1 < t \leq s < n$

यदि हम $K = \{a^r, a^{2r}, ..., a^{tr} = e\}$ प्राप्त करें तो K, G का एक गैर–रिक्त परिमित उप–समुच्चय है, गुणन के अधीन संवृत है एवं इसीलिये G का उपसमूह है। इसका कोटि n से कम है, यह आवश्यक उपसमूह है।

टिप्पणी

प्रमेय 1.23: यदि G ऐसा समूह है, जिसमें गैर–नगण्य उपसमूह नहीं है तो G अभाज्य कोटि युक्त परिमित होगा।

प्रमाण: मान लेते हैं कि G में परिमित कोटि है तो हम प्राप्त कर सकते हैं $a \in G$, जैसे $a \neq e$

माना $H = < a >$ तो H G का एक चक्रीय उपसमूह है एवं $H \neq \{e\}$ किन्तु G में गैर–नगण्य उपसमूह नहीं हैं।

इस प्रकार $H = G$

$\Rightarrow G = < a >$

अब $K = < a^2 >$ उपसमूह का विचार करें।

अब $a \notin < a^2 >$ क्योंकि यदि $a \in < a^2 >$ तो $a = a^{2t}$ किसी पूर्णांक t के लिये

$\Rightarrow a^{2t-1} = e \Rightarrow o(a) \leq 2t - 1$

तात्पर्य यह है कि $o(a)$ यदि परिमित हो जो कि वास्तविक नहीं है। इस प्रकार $a \notin < a^2 >$

पुनः $< a^2 > \neq \{e\}$ क्योंकि तो $a^2 = e$ का पुनः अर्थ होगा कि $o(a)$ परिमित (≤ 2) है।

इस प्रकार $< a^2 >$ G का गैर–नगण्य उपसमूह है जो कि सम्भव नहीं। इसी कारण $o(G)$ अपरिमित नहीं हो सकता।

अतः $o(G)$ परिमित है एवं चूँकि इसे पूर्ववर्ती प्रमेय द्वारा संयोजित नहीं किया जा सकता इसलिये यह अभाज्य (Prime) होगा।

प्रमेय 1.24: वे ही समूह जिनमें गैर–नगण्य उपसमूह नहीं हैं वे अभाज्य कोटि के चक्रीय समूह हैं व समूह $\{e\}$ है।

अब तक हम इस विषय में आश्वस्त हुए बिना ही चक्रीय समूह व इनके उत्पन्न कारक की बात करते रहे हैं कि चक्रीय समूह में कितने उत्पन्न कारक हो सकते हैं। इसके समाधान के लिये हम निम्नांकित प्रमेय पर विचार करते हैं।

प्रमेय 1.25: एक अनंत चक्रीय समूह में परिशुद्धतः दो उत्पन्न कारक होते हैं।

प्रमाण: माना $G = < a >$ एक अपरिमित चक्रीय समूह है

जैसा कि पहले दर्शाया जा चुका है– यदि a, G का उत्पन्न हो तो a^{-1} होगा।

अब b, G का कोई उत्पन्न है तो $b \in G$ अनुरूप G से $b = a^n$ उत्पन्न होता है, हम किसी पूर्णांक n के लिये पाते हैं,

पुनः $a \in G$ के अनुरूप G से $a = b^m$ उत्पन्न होता है, किसी पूर्णांक m के लिये हम $a = b^m = (a^n)^m = a^{nm}$ प्राप्त करते हैं।

टिप्पणी

$\Rightarrow a^{nm-1} = e \Rightarrow o(a)$ परिमित है एवं $\leq nm - 1$

चूँकि $o(G) = o(a)$ अपरिमित है, तो उपरोक्त तभी हो सकता है यदि

$nm - 1 = 0 \Rightarrow nm = 1$

क्योंकि $m = \frac{1}{n}$ या $n = \pm 1$ जैसे m, n पूर्णांक हैं, अर्थात् $b = a$ या a^{-1}

अन्य शब्दों में: a व a^{-1} परिशुद्धतः G के उत्पन्न कारक हैं।

अब इस प्रश्न का उत्तर प्रस्तुत किया जाना है कि परिमित चक्रीय समूह के कितने उत्पन्नकारक होंगे। उत्तर से पहले हम सर्वप्रथम वह परिभाषित करते हैं जिसे यूलर (Euler) φ फलन (अथवा यूलर टोटियंट फलन (Euler Totient Function) कहा जाता है।

किसी पूर्णांक n के लिये हम $\varphi(1) = 1$ परिभाषित करते हैं एवं $n > 1$, के लिये $\varphi(n)$ को धनात्मक पूर्णांकों की संख्या n से कम होनी होगी एवं n से अपेक्षाकृत अभाज्य (Prime) है। उदाहरण $\varphi(6) = 2, \varphi(10) = 4$, इत्यादि के रूपों में।

ध्यान दे: 1, 5, 6 से कम हैं एवं 6 से अपेक्षाकृत अभाज्य (Prime) हैं तथा 1, 3, 7, 9 (संख्या में चार) 10 से कम हैं एवं 10 से अपेक्षाकृत अभाज्य (Prime) हैं, इत्यादि। स्पष्ट है कि $\varphi(p) = p - 1$ यदि p एक अभाज्य (Prime) हो। निम्नांकित दो परिणाम कई बार सहायक हो सकते हैं,

(i) यदि $p_1, p_2, ..., p_n$ n (>1) के सुनिश्चित अभाज्य गुणक हों तो,

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

(ii) यदि m, n सहअभाज्य हों तो,

$\varphi(mn) = \varphi(m)\ \varphi(n), (m, n \geq 1)$

प्रमेय 1.26: यदि G कोटि n का परिमित समूह हो एवं d अद्वितीय उपसमूह की कोटि $n \exists$ के प्रत्येक भाजक (Divisor) के लियेः तो G चक्रीय है।

प्रमाण: माना $d \mid n$ हो तो परिभाषित करें $A(d) = \{x \in G \mid o(x) = d\}$

मान लेते हैं कि $A(d) \neq \varphi$ तो $\exists\, x \in G$ इस प्रकार कि $o(x) = d$।

माना $H = < x >$ तो $o(x) = o(H) = d$। इससे $\varphi(d)$ के G उत्पन्नकर्ता अथवा $\varphi(d)$ में कोटि d के H अवयव पता चलते हैं। यदि $\exists\, y \in G, y \notin H$ इस प्रकार हो कि $o(y) = d$ तो $K = < y >$ कोटि d का एक उपसमूह है। यह प्रदर्शित है कि d में कोटि G का अद्वितीय उपसमूह है। अतः $K = < y >$ एक विरोधाभास है। इस प्रकार कोटि d के G में अवयवों की संख्या $\varphi(d)$ है।

अतः $o[A(d)] = \varphi(d)$ यदि $A(d) \neq \varphi$

एवं $o[A(d)] = 0$ यदि $A(d) = \varphi$ सभी $d \mid n$ के लिए।

स्पष्टतः $G = \underset{d|n}{\cup} A(d)$

माना $d_1, ..., d_s$ ये सभी n के भाजक (Divisor) हैं।

टिप्पणी

मान लें कि $A(d_1) = \varphi, ..., A(d_i) = \varphi$

एवं $A(d_{i+1}) \neq \varphi, ..., A(d_s) \neq \varphi$

ध्यान दें: यदि समस्त $d \mid n$ के लिये $A(d) = \varphi$ तो $o(G) = 0$ एक विरोधाभास है। अतः किसी $[d \mid n]$ के लिये $A(d) \neq \varphi$।

$\therefore \quad o[A(d_1)] = ... = o[A(d_i)] = 0$

एवं $o[A(d_{i+1})] = \varphi(d_{i+1}) ..., o[A(d_s)] = \varphi(d_s)$

अब $G = \underset{d|n}{\cup} A(d) \Rightarrow o(G) = \sum_{d|n} o[A(d)]$

$$\Rightarrow n = \varphi(d_{i+1}) + ... + \varphi(d_s)$$

हमें विदित है कि $n = \sum_{d|n} \varphi(d)$

$$\Rightarrow \varphi(d_1) + ... + \varphi(d_i) + \varphi(d_{i+1}) + ... + \varphi(d_s) = \varphi(d_{i+1}) + ... + \varphi(d_s)$$

$$\Rightarrow \varphi(d_1) + ... + \varphi(d_i) = 0, \text{ जो कि एक विरोधाभास है।}$$

अतः समस्त $d \mid n$ के लिये $A(d) \neq \varphi$

विशेषतया $A(n) \neq \varphi \Rightarrow \exists\, x \in A(n) \Rightarrow \exists\, x \in G$ इस प्रकार है कि

$o(x) = n = o(G) \Rightarrow G$ एक चक्रीय समूह है।

अपनी प्रगति जांचिए

5. दो उपसमूहों का संकुल क्या होता है?
6. चक्रीय समूह क्या हैं?
7. यूलर–फलन क्या है?

1.6 अपनी प्रगति जांचिए प्रश्नों के उत्तर

1. यदि समस्त $a, b \in G$ के लिये $a * b = b * a$ तो G को एबेलियन समूह अथवा क्रमविनिमेय समूह कहा जाता है।
2. $\begin{bmatrix} 2 & 3 \\ 2 & 5 \end{bmatrix}$
3. हाँ, तत्समक अवयव समूह में अद्वितीय है।
4. समूह H का गैर–रिक्त उप–समुच्चय G, G. का उपसमूह है यदि,
   (i) $a, b \in H \Rightarrow ab \in H$ (ii) $a \in H\ a^{-1} \in H$.
5. H व K को समूह G के दो उपसमूह, मानें। हम परिभाषित करते हैं कि $HK = \{hk \mid h \in H, k \in K\}$. तो HK G का गैर–रिक्त उप–समुच्चय होगा (जिसे H व K का सम्मिश्रित कह दिया जाता है)।

टिप्पणी

6. ग्रुप G को चक्रीय समूह कहा जाता है यदि अवयव $a \in G$ इस प्रकार हो कि G के प्रत्येक अवयव को a की घात (Power) के रूप में व्यक्त किया जा सके। इस प्रकरण में a को G का उत्पन्नकर्ता कहा जाता है। हम इस तथ्य को व्यक्त करने के लिये $G = < a >$ या $G = (a)$ लिखते हैं।
7. किसी पूर्णांक n के लिये हम परिभाषित करते हैं $\varphi(1) = 1$ व $n > 1$, के लिये $\varphi(n)$ धनात्मक पूर्णांकों की ऐसी संख्या होगी जो n से कम हो एवं n से अपेक्षाकृत अभाज्य हो।

1.7 सारांश

- $HK = KH$ का तात्पर्य यह नहीं है कि H का प्रत्येक अवयव K के प्रत्येक अवयव से क्रम विनिमेयता होता है। इसका तात्पर्य मात्र यह है, कि प्रत्येक $h \in H, k \in K, hk = k_1h_1$, कुछ $k_1 \in K$ व $h_1 \in H$ के लिये।
- G कोई समूह व $a \in G$ कोई अवयव हो। हम कहते हैं कि a कोटि (अथवा अवधि) n का है यदि n कम धनात्मक पूर्णांक इस प्रकार है कि $a^n = e$। यदि G के द्विआधारी संरचना को + द्वारा इंगित किया जाता है, तो इसे $na = 0$ पढ़ा जायेगा जहाँ 0, G की तत्समक है।
- चक्रीय समूह की कोटि इसके उत्पन्नकर्ता की कोटि के समतुल्य होता है।
- यदि G की कोटि n का एक परिमित चक्रीय समूह है तो G के सुनिश्चित उपसमूहों की संख्या n के सुनिश्चित भाजकों की संख्या है एवं किसी भी प्रदर्शित कोटि के एक उपसमूह में यह साधारणतया होता है।
- अभाज्य कोटि का समूह G चक्रीय होगा एवं G के प्रत्येक अवयव (अन्य तत्समकों छोड़कर) को इसके उत्पन्नकर्ता के रूप में प्राप्त किया जा सकता है।
- अभाज्य कोटि के समूह G में कोई गैर–नगण्य उपसमूह नहीं हो सकता।
- परिमित संयोजित कोटि के समूह में कम से कम एक गैर–नगण्य उपसमूह होता है।
- यदि G ऐसा समूह हो जिसमें गैर–नगण्य उपसमूह नहीं हो तो G अभाज्य कोटि युक्त परिमित होगा।
- सिर्फ इन्हीं समूहों में गैर–नगण्य उपसमूह नहीं होते जैसे कि अभाज्य कोटि के चक्रीय समूह एवं समूह $\{e\}$।
- अपरिमित चक्रीय समूह में परिशुद्धतः दो उत्पन्नकर्ता होते हैं।
- यदि G, n कोटि का एक परिमित समूह हो एवं d के प्रत्येक भाजक n, $\exists$ के लिये कोटि d अद्वितीय उपसमूह हो तो G चक्रीय है।

1.8 मुख्य शब्दावली

- **संबद्धता:** संबद्धता गुणधर्म में आप इस बात से परे जोड़ अथवा गुणा कर सकते हैं कि कितनी संख्याओं को समूहबद्ध किया जा रहा है।

टिप्पणी

- **तत्समकः** समुच्चय का ऐसा अवयव जिसे यदि विशिष्ट द्विआधारी संरचना द्वारा अन्य अवयव के साथ संयुक्त किया जाये तो वह अवयव अपरिवर्तित रहता है।
- **व्युत्क्रमः** ऐसा अवयव जिसे किसी संक्रिया में प्रदर्शित अवयव के साथ संयुक्त किये जाने पर उस संक्रिया के लिये तत्समक अवयव उपजता है।
- **द्विआधारी संरचनाः** फलन से परिवर्तन राशि तक क्रमित अनुप्रयोग से प्रथम फलन का मान दूसरे फलन का विषय बन जाता है, ऐसा ही आगे चलता रहता है।
- **सह–समुच्चयः** उपसमूह युक्त समूह के एक अवयव विशेष रूप से उपसमूह के प्रत्येक अवयव के गुणन में प्राप्त समस्त गुणनफलों से बना समुच्चय है।

1.9 स्व–मूल्यांकन प्रश्न एवं अभ्यास

लघु–उत्तरीय प्रश्न

1. समूह के संवृत विशेषताओं का वर्णन करें।
2. समूह के कुछ उदाहरण दीजिए।
3. समूह G में दर्शायें कि प्रत्येक $a \in G$ का व्युत्क्रम अद्वितीय है।
4. समूह का केन्द्र परिभाषित करें।
5. सिद्ध करें कि HK, G का उपसमूह है यदि $HK=KH$.
6. चक्रीय समूह से क्या अभिप्राय है?
7. चक्रीय समूह क्या एबेलियन होता है?
8. यूलर–फलन से आपका क्या आशय है?

दीर्घ–उत्तरीय प्रश्न

1. माना G ऐसा समुच्चय $\{\pm e, \pm a, \pm b, \pm c\}$ है जहाँ

$$e=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, a=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, b=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}, c=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

   दर्शायें कि G से गुणन आव्यूह के अधीन समूह का निर्माण होता है।
2. सिद्ध करें कि समूह G एबेलियन है यदि $(ab)^2 = a^2b^2$.
3. दर्शायें कि एकाभ एक समूह है यदि उसमें निष्कासित नियम हों।
4. यदि $G=\{2^r \mid r=0,\pm1,\pm2,...\}$ तो दर्शायें कि G से सामान्य गुणन के अधीन समूह का निर्माण होता है।
5. दर्शायें कि जिस परिमित अर्द्ध–समूह में निष्कासित नियम हैं वह एक समूह है।
6. दर्शायें कि समूह G का केन्द्र G का एक उपसमूह है।
7. सिद्ध करें कि यदि G एक परिमित समूह है व H, G का उपसमूह है तो $o(H)$ $o(G)$ को विभाजित करता है।

टिप्पणी

8. उप–समुच्चय द्वारा उपसमूह कैसे उत्पन्न होते हैं? व्युत्पत्ति व उदाहरण प्रस्तुत करते हुए व्याख्या करें।
9. सिद्ध करें कि चक्रीय समूह की कोटि इसके उत्पन्नकर्ता की कोटि के समतुल्य कैसे होती है।
10. उदाहरणसहित यूलर–फलन की चर्चा करें।
11. माना G कोई परिमित समूह है। माना $a \in G$ इस प्रकार है कि $o(a) = o(G)$। दर्शायें कि G चक्रीय है, a द्वारा उत्पन्न। सिद्ध करें कि कोटि n का समूह चक्रीय है यदि इसमें कोटि n का अवयव हो।
12. दर्शायें कि U_8 में प्रत्येक अवयव का अपना व्युत्क्रम होता है (जो कि कोटि 2 का है) एवं इसी कारण U_8 चक्रीय नहीं है।

1.10 सहायक पाठ्य सामग्री

Sharma, Dr Anil and Jitendra Saini. 2016. *Abstract Algebra* (अमूर्त बीजगणित) Jaipur (Rajasthan): RBD Publisher.

Pathak, Dr H. K. 2017. *Abstract Algebra* (अमूर्त बीजगणित). Kolkata (West Bengal): Siksha Sahitya Prakashan.

Herstein, I. N. 1975. *Topics in Algebra*, 2nd Edition. New York: John Wiley and Sons.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. UK: Cambridge University Press (Indian Edition).

Khanna, V. K. and S. K. Bhambari. 2016. *A Course in Abstract Algebra*, 5th Edition. New Delhi: Vikas Publishing House Pvt. Ltd.

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

Gilbert, Linda. 2008. *Elements of Modern Algebra*. Boston: Cengage Learning.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

Childs, Lindsay N. 2008. *A Concrete Introduction to Higher Algebra*. Berlin: Springer Science & Business Media.

इकाई 2 समूह सिद्धांत

टिप्पणी

संरचना

2.0 परिचय

आधुनिक बीजगणित में समूह सिद्धांत शब्द का तात्पर्य ऐसे समूहों के अध्ययन से है जो कि ऐसी प्रणाली होती हैं जिनमें अवयवों के समुच्चय तथा द्विआधारी संरचना (Binary Composition) होती है जिसे कि समुच्चयों के दो अवयवों पर लागू किया जा सकता है। ये दोनों मिलकर कुछ अभिगृहीत (Axioms) की पूर्ति करते हैं। इनमें यह आवश्यक है कि समूह संक्रिया (Group Operation) में संवृत हो, इसमें साहचर्य नियम (Associative Law) का पालन किया जाये, तत्समक (Identity) अवयव हो एवं प्रत्येक अवयव में एक व्युत्क्रम (Inverse) हो। यदि समूह द्वारा क्रमविनिमेय नियम (Commutative Law) की भी पूर्ति हो रही हो तो इसे क्रमविनिमेय अथवा एबेलियन (Abelian) समूह कहा जाता है।

मूलतः समूह सिद्धांत में 'समूह' नामक बीजगणितीय संरचनाओं का अध्ययन किया जाता है। समूहों के अध्ययन में सहसमुच्चय (Coset) मूलभूत साधन होते हैं, क्योंकि ये लैग्रांज प्रमेय (Lagrange's Theorem) में केन्द्रीय भूमिका निभाते हैं जिसके अनुसार किसी परिमित समूह (Finite Group) G के लिये G के प्रत्येक उप–समूह (Subgroup) H के अवयवों की संख्या G के अवयवों की संख्या को भागित करती है। समूह G का उप–समूह N, G का सामान्य उप–समूह तभी है यदि g के समस्त अवयवों G के लिये संगत (Corresponding) बायें व दायें सहसमुच्चय समतुल्य हों, अर्थात् gN = Ng। इसके अतिरिक्त N में G के सहसमुच्चय से भागफल समूह (Quotient Group) अथवा खंड समूह (Factor Group) नामक समूह का निर्माण होता है।

अमूर्त बीजगणित (Abstract Algebra) में सामान्य उप–समूह ऐसा उप–समूह होता है जो कि समूह के सदस्यों द्वारा संयुग्मन (Conjugation) के अधीन अक्रमविनिमेय (Invarient) होता है जिसका कि वह भाग है। सामान्य उप–समूह महत्त्वपूर्ण हैं क्योंकि ये प्रदर्शित समूह के भागफल समूह (Quotient Group) के निर्माण में विशिष्टता से

टिप्पणी

प्रयोग किये जा सकते हैं। इनके अतिरिक्त G के सामान्य उप–समूह परिशुद्धतः डोमैन G युक्त समूह समरूपता (Group Homomorphism) के आधारभूत हैं जिसका तात्पर्य यह हुआ कि ये उन समरूपता (Homomorphism) को आन्तरिकरूपेण वर्गीकृत करने में प्रयोग किये जा सकते हैं।

इस इकाई में आप समूह सिद्धांत (Group Theory), सह–समुच्चयों का वियोजन (Coset Decomposition) लैग्रांज प्रमेय (Lagrange's Theorem) व इसके उपप्रमेयों (Corollaries), फ़ेर्मेट प्रमेय (Fermat's Theorem), सामान्य उप–समूह व भागफल समूह का अध्ययन करेंगे।

2.1 उद्देश्य

इस इकाई को पढ़ने के बाद आप–

- समूह सिद्धांत (Group Theory) के महत्त्वपूर्ण अभिलक्षण को समझ पाएंगे;
- सहसमुच्चय वियोजन का वर्णन कर पाएंगे;
- लैग्रांज प्रमेय एवं इसके उपप्रमेय (Corollaries) का वर्णन कर पाएंगे;
- फ़ेर्मेट प्रमेय की व्याख्या कर पाएंगे;
- सामान्य उप–समूह को समझ पाएंगे;
- भागफल समूह के विश्लेषण की व्याख्या कर पाएंगे।

2.2 सहसमुच्चय वियोजन

बीजगणित में सहसमुच्चय बीजगणितीय समूहों के अध्ययन में मूलभूत साधन माने जाते हैं। मूलभूत रूप से लैग्रांज प्रमेय में सहसमुच्चय की महत्त्वपूर्ण केन्द्रीय भूमिका रहती है जिसके अनुसार किसी परिमित समूह (Finite Group) G के लिये G के प्रत्येक उपसमूह H के अवयवों की संख्या G के अवयवों की संख्या को भागित करती है।

समूह सिद्धांत में समूह G का अवयव g व एवं G का उपसमूह H है,

$gH = \{gh : h, H$ का एक अव्यव$\}$ के सन्दर्भ में G में H का **बायाँ सहसमुच्चय** है।

$Hg = \{hg : h, H$ का एक अव्यव$\}$ के सन्दर्भ में G में H का **दायाँ सहसमुच्चय** है।

यदि समूह संक्रिया (Group Operation) को योगशील (Additively) रूप में लिखा जाता है, तो $g + H$ या $H + g$ में परिवर्तित करने के लिये संकेत (Notation) प्रयोग किया जाता है।

अवयव g का सम्बन्ध सहसमुच्चय gH से होता है। यदि x का सम्बन्ध gH से हो तो $xH = gH$। इस प्रकार G का प्रत्येक अवयव उपसमूह H के बिल्कुल एक बायें सहसमुच्चय (Left Coset) से सम्बन्धित है। अवयवों g व x, H के समान बायें सहसमुच्चय से सम्बन्धित तभी होंगे यदि $g^{-1}x$ का सम्बन्ध H से हो। दायें सहसमुच्चयों (Right Cosets) के प्रकरण में भी यह सब लागू होगा (इकाई 1 देखें)।

टिप्पणी

यदि G एक एबेलियन समूह (Abelian Group) हो तो $gH = Hg$ के प्रत्येक उपसमूह H का G के लिये एवं G के प्रत्येक अवयव g के लिये। साधारणतया समूह G का उपसमूह H एवं अवयव प्रदर्शित रहता है; g के सन्दर्भ में H का दायाँ सहसमुच्चय तथा g के सन्दर्भ में संयुग्मित उपसमूह (Conjugate Subgroup) $g^{-1}Hg$ का बायाँ सहसमुच्चय भी स्थित है, अर्थात् $Hg = g\,(g^{-1}Hg)$। G में H के बायें सहसमुच्चय की संख्या G में H के दायें सहसमुच्चय की संख्या के समतुल्य होती है। सामान्य मान (Common Value) को G में H का निर्देशांक (Index) कहा जाता है।

समूह G का उपसमूह N, G का सामान्य उपसमूह तभी है, यदि G के समस्त अवयवों g के लिये संगत दायें व बायें सहसमुच्चय समतुल्य हों, अर्थात् $gN = Ng$। इसके अतिरिक्त G में N के सहसमुच्चय से जिस समूह का निर्माण होता है उसे भागफल समूह (Quotient Group) अथवा खंड समूह (Factor Group) कहते हैं।

सहसमुच्चय वियोजन (Coset Decomposition): समूह G का उपसमूह H है। परिभाषानुरूप G में H का दायाँ सहसमुच्चय रिक्त है एवं G में H के दो दायें सहसमुच्चय या तो असंबंधित (Disjoint) होते हैं अथवा एक समान (Identical) होते हैं। G में H के समस्त दायें सहसमुच्चयों का संघ G के समतुल्य होता है। इसी कारण G में H के समस्त दायें सहसमुच्चयों के समुच्चय से G का विभाजन (Partition) होता है। इस विभाजन को G का दायाँ सहसमुच्चय वियोजन कहा जाता है। इस विभाजन से पृथक्–पृथक् सदस्यों को प्राप्त करने की विधि निम्नानुसार है।

यहाँ H अपने आप में दायाँ सहसमुच्चय है। अब मान लें कि यदि $a \in G$ व $a \notin H$ तो Ha अन्य सुनिश्चित दायाँ सहसमुच्चय होगा। पुनः b को ऐसा अन्य अवयव मानें कि यदि $b \in G$ व $b \notin H$ एवं $b \notin Ha$ भी तो Hb अन्य सुनिश्चित (Distinct) दायाँ सहसमुच्चय होगा। इसी प्रकार G में H के सभी सुनिश्चित दायें सहसमुच्चय प्राप्त होंगे।

परिणामस्वरूप $G = H \cup Ha \;\; Hb \cup Hc \ldots\ldots$ जहाँ a, b, c, G के अवयव हैं, इसीलिये चयनित समस्त दायें सहसमुच्चय सुनिश्चित हैं। इसी प्रकार G के बायें सहसमुच्चय वियोजन (Coset Decomposition) को प्राप्त किया जा सकता है।

युग्मित सहसमुच्चय (Double Cosets)

प्रदर्शित दो उप–समूहों के लिये H व K समूह G के है, तो G में H व K के **युग्मित सहसमुच्चय** (Double Coset) के समुच्चय का रूप एक $HgK = \{hgk : h, H$ का अवयव है तथा k, एक अवयव K$\}|$ का है ये K के बायें सहसमुच्चय हैं व H के दायें सहसमुच्चय हैं, यदि क्रमशः $H = 1$ व $K = 1$।

परिभाषा: माना कि $H, K \leq G$. माना कि $a, b \in G$। G पर सम्बन्ध (Relation) '~' को निम्नरूप से परिभाषित कर सकते हैं,

$a \sim b \Leftrightarrow \exists\, h \in H, k \in K$ इस प्रकार कि $a = hbk$

यह सरलता से देखा जा सकता है कि '~' G पर समतुल्यता सम्बन्ध (Equivalence Relation) है। अतः यह G को समतुल्यता वर्गों (Equivalence Classes) के असंबंधित संघ (Disjoint Union) में भागित करता है। $a \in G$ का समतुल्यता वर्ग इस प्रकार प्रदर्शित किया जा सकता है,

$$cl(a) = \{x \in G \mid a \sim x\}$$

$= \{hak \mid h \in H, k \in K\}$

$= HaK$ को G में H व K का युग्मित सहसमुच्चय या द्विसहसमुच्चय कहा जाता है।

टिप्पणी

$$G = \bigcup_a cl(a) = \bigcup_a Hak$$

$f: HaK \to HaKa^{-1}$ को इस प्रकार परिभाषित करें कि,

$f(hak) = haka^{-1}$ सभी $h \in H$ के लिए, $k \in K$

स्पष्टतः f इस प्रकार स्पष्टतया परिभाषित है,

$$\Rightarrow haka^{-1} = h'ak'a^{-1}$$

f, 1–1 है, जैसे $f(hak) = f(h'ak')$

$$\Rightarrow haka^{-1} = h'ak'a^{-1}$$

$$\Rightarrow hak = h'ak'$$

माना $haka^{-1} \in HaKa^{-1} \Rightarrow hak \in Hak$ और,

$f(hak) = haka^{-1}$

$\therefore$ f, 1 और -1 दोनों आच्छादक (Onto) हैं।

इस प्रकार, $o(Hak) = o(HaKa^{-1})$, (यदि H और K परिमित हैं)

$$= \frac{o(H)\, o(aKa^{-1})}{o(H \cap aKa^{-1})} = \frac{o(H)\, o(K)}{o(H \cap aKa^{-1})}$$

यदि G एक परिमित समूह है तो

$$o(G) = \sum_a o(HaK) = \sum_a \frac{o(H)o(K)}{o(H \cap aKa^{-1})}$$

अब हम सइलो का द्वितीय प्रमेय सिद्ध कर सकते हैं।

प्रमेय 2.1 साइलो की द्वितीय प्रमेय (Sylow's Second Theorem): परिमित समूह G के दो सइलो p-उपसमूह G में संयुग्मित होते हैं।

प्रमाण: माना P तथा Q, G के साइलो p-उपसमूह हैं। माना $o(P) = p^n = o(Q)$ जहाँ $p^{n+1} = o(G)$। मान लें कि P व QG में संयुग्मित नहीं हैं।

अर्थात् $P \neq gQg^{-1}$ किसी $g \in G$

उपरोक्त चर्चानुसार

$$o(PxQ) = \frac{o(P)\, o(Q)}{o(P \cap xQx^{-1})}$$

चूँकि, $P \cap xQx^{-1} \leq P$

$o(P \cap xQx^{-1}) = p^m$, $m \leq n$

यदि $m = n$ तो $P \cap xQx^{-1} = P$

$\Rightarrow$ $P \subseteq xQx^{-1}$

टिप्पणी

$\Rightarrow$ $P = xQx^{-1}$ as $o(xQx^{-1}) = o(Q) = o(P)$

जो कि एक विरोधाभास है।

$\therefore$ $m < n$ और इस प्रकार $o(PxQ) = p^{2n-m}$, $m < n$ सभी $x \in G$ के लिए

$\Rightarrow$ $o(PxQ) = p^{n+1}$ $(p^{n-m+1}) = p^{n+1}$ के गुणांक हैं।

इस प्रकार, $o(G) = \sum_x o(PxQ) = p^{n+1}$ के गुणांक हैं।

$p^{n+1} \mid$ R.H.S. $\Rightarrow p^{n+1} \mid o(G)$, यह एक विरोधाभास है।

$\therefore$ $P = gQg^{-1}$ कुछ $g \in G$ के लिए।

साइलो के तीसरे प्रमेय को सिद्ध करने से पूर्व हम निम्नांकित लैमा सिद्ध करेंगे।

लैमा: माना P, G का साइलो p-उपसमूह है, तो G के साइलो p-उपसमूह की संख्या $\frac{o(G)}{o(N(P))}$ के समतुल्य होगी।

प्रमाण: आपको विदित है कि,

$$o(cl(P)) = \frac{o(G)}{o(N(P))}$$

चूँकि, $cl(P) = \{Q \mid Q \leq G, Q = gPg^{-1}, g \in G\}$

$= G$ के सभी साइलों p-उपसमूहों के समुच्चय

G के साइलो p-उपसमूहों की संख्या $\frac{o(G)}{o(N(P))}$ है।

प्रमेय 2.2 साइलो का तृतीय प्रमेय (Sylow's Third Theorem) : G के साइलो p-उपसमूहों की संख्या का रूप $1 + kp$ है, जहाँ $(1 + kp) \mid o(G)$, k ग़ैर–ऋणात्मक पूर्णांक हैं।

प्रमाण: माना P का साइलो p-उपसमूह है।

माना $o(P) = p^n$

अब $G = \bigcup_x PxP$

$$= \bigcup_{x \in N(P)} PxP \cup \bigcup_{x \notin N(P)} PxP$$

$$x \in N(P) \Rightarrow Px = xP \Rightarrow PPx = PxP$$

$\Rightarrow$ $Px = PxP$

$\therefore$ $\bigcup_{x \in N(P)} PxP = \bigcup_{x \in N(P)} Px = N(P)$

जैसे $P \leq N(P)$ और असंबद्ध दाएँ सहसमुच्चय (Disjoint Right Coset) के संघ (Union) समुच्चय के बराबर है।

$$x \notin N(P) \Rightarrow Px \neq xP \Rightarrow xPx^{-1} \neq P$$

टिप्पणी

$$\Rightarrow o(P \cap xPx^{-1}) = p^m,\ m < n$$

(जैसा कि साइलो की द्वितीय प्रमेय में है)

$$\Rightarrow o(PxP) = P^{2n-m}, \quad m < n$$

$$\therefore \quad o(G) = o(N(P)) + \sum_{x \notin N(P)} o(PxP)$$

$$= o(N(P)) + \sum_{x \notin N(P)} p^{2n-m}$$

$$\therefore \quad \frac{o(G)}{o(N(P))} = 1 + \sum \frac{p^{2n-m}}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))}, \quad t = \text{पूर्णांक}$$

चूँकि L.H.S. = पूर्णांक, $p^{n+1}\ \frac{t}{o(N(P))} = r = \text{पूर्णांक}$

$$\therefore \quad p^{n+1}t = r.o(N(P))$$

पुनः $\quad P \le N(P)$

$$o(P) \mid o(N(P))$$

$$\Rightarrow \quad p^n \mid o(N(P))$$

$$\Rightarrow \quad o(N(P)) = p^n u$$

$$P^{n+1}t = r\ o(N(P))$$

$$\Rightarrow \quad pt = r\,.u$$

$$\Rightarrow \quad p \mid ru$$

यदि $p \mid u$ तो $p^{n+1} \mid o(N(P)) \mid o(G) \Rightarrow p^{n+1} \mid o(G)$, एक विरोधाभास है।

$$\therefore \quad p \mid r \Rightarrow \frac{r}{p} = \text{पूर्णांक} \Rightarrow \frac{t}{u} = \text{पूर्णांक}\ k = \frac{r}{p}.$$

$$\therefore \quad \frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))} = 1 + p\frac{t}{u} = 1 + kp$$

उपरोक्त लैमा से $\frac{o(G)}{o(N(P))} = G$ के साइलो p-उपसमूहों की संख्या।

अतः साइलो p-उपसमूहों की संख्या का रूप $1 + kp = \frac{o(G)}{o(N(P))} \Rightarrow$ $(1 + kp) \mid o(G)$ है।

इससे प्रमेय सिद्ध हुआ।

ध्यान दें: यदि $o(G) = p^n q, (p, q) = 1$ तो साइलो p-उपसमूहों की संख्या होगी,

$$1 + kp, \text{ जहां } (1 + kp) \mid p^n q$$

$$\Rightarrow (1 + kp) \mid q \text{ as } (1 + kp, p^n) = 1$$

उपप्रमेय: यदि P, G का एकमात्र साइलो p-उपसमूह है, तो G में P सामान्य है, एवं इसके विपरीत।

प्रमाण: साइलो के तृतीय प्रमेय के अनुसार।

$$\frac{o(G)}{o(N(P))} = 1 \Rightarrow o(G) = o(N(P))$$

चूँकि $N(P) \leq G$

$N(P) = G$

$\Rightarrow$ G में P सामान्य है।

इसके विपरीत यदि G में साइलो p-उपसमूह P सामान्य हो तो,

$$N(P) = G \Rightarrow o(N(P)) = o(G)$$

$$\Rightarrow \quad \frac{o(G)}{o(N(P))} = 1$$

G के साइलो p-उपसमूहों की संख्या 1 है।

G P का एकमात्र साइलो p-उपसमूह है।

लैमा: माना P, G का साइलो p-उपसमूह है। माना कि $x \in N(P)$ इस प्रकार है कि $o(x) = p^i$ तो $x \in P$

प्रमाण: माना $o(P) = p^n$, $p^{n+1} = o(G)$

अब $(Px)^{pi} = Px^{p^i} = Pe = P$

[$N(P)$ और $x \in N(P)$ में P सामान्य है]

$\Rightarrow$ $o(Px) \mid p^i$

$\Rightarrow$ $o(Px) = p^j, j \geq o$

माना $j > 0$. $\bar{K} = < Px > \leq \frac{N(P)}{P}$ इस प्रकार, $o(\bar{K}) = p^j$

चूंकि $(\bar{K}) \leq \frac{N(P)}{P}$, $\bar{K} = \frac{K}{P}$ जहां $K \leq N(P)$

$$p^j = o(\bar{K}) = \frac{o(K)}{o(P)} = \frac{o(K)}{p^n}$$

$\Rightarrow$ $o(K) = p^{n+j}$, $j > 0$

लेकिन $o(K) \mid o(N(P)) \mid o(G)$

$\Rightarrow p^{n+j} \mid o(G)$, $j > 0$, जो एक विरोधाभास है।

$\therefore$ $j = 0$ $o(Px) = p^j = 1$

$\Rightarrow$ $Px = P \Rightarrow x \in P$

2.3 लैग्रांज प्रमेय एवं इसके उपप्रमेय

समूह सिद्धांत में लैग्रांज प्रमेय (Lagrange's Theorem) के अनुसार किसी परिमित समूह G के लिये G के प्रत्येक उप–समूह H कोटि (अवयवों की संख्या) G की कोटि को भागित करता है। प्रमेय का यह नामकरण जोसेफ़ लुईस लैग्रांज (Joseph Louis Lagrange) के नाम पर किया गया।

टिप्पणी

टिप्पणी

प्रमेय का परिणाम परिमित समूह के किसी अवयव की कोटि होती है, अर्थात् सबसे छोटी धनात्मक (Smallest Positive Integer) पूर्णांक संख्या $ak = e$ के साथ k जहाँ e समूह के तत्समक अवयव (Identity Elements) है। यह उस समूह की कोटि को भागित करता है, इसलिये a का कोटि a द्वारा उत्पन्न चक्रीय उपसमूह (Cyclic Subgroup) कोटि के समतुल्य है। यदि समूह में n अवयव हों तो इसका अनुकरण हो जाता है,

$$a^n = e$$

इस संकेतन का प्रयोग फ़ेर्मेट के लिटल प्रमेय (Fermat's Little Theorem) व इसके सामान्यीकरण (Generalization) को सिद्ध करने में किया जा सकता है। प्रमेय में यह भी दर्शाया गया कि अभाज्य कोटि का कोई भी समूह चक्रीय व सरल है। लैग्रांज प्रमेय का प्रयोग करते हुए यह भी दर्शाया जा सकता है कि अपरिमित रूप से कई अभाज्य होते हैं।

लैग्रांज प्रमेय से एक विपरीत प्रश्न उत्पन्न होता है कि समूह की कोटि प्रत्येक भाजक (Divisor) के किसी उपसमूह की कोटि है अथवा नहीं। ऐसा साधारणतया नहीं होता। प्रदर्शित है कि परिमित समूह G व d का भाजक $|G|$ है, कोटि d युक्त G का उपसमूह पाया जाना आवश्यक नहीं। सबसे छोटा उदाहरण A_4 (डिग्री 4 का एकान्तरण समूह (Alternating Group) है जिसमें 12 अवयव हैं किन्तु कोटि 6 का उपसमूह नहीं है।

लैग्रांज प्रमेय का विलोम (Converse of Langrang's Theorem, CLT) समूह इस गुणधर्म से युक्त एक परिमित समूह है कि समूह के कोटि के प्रत्येक भाजक (Divisor) के लिये उस कोटि का उपसमूह है। ऐसा जाना जाता है, कि CLT समूह हल–योग्य (Solvable) होना चाहिए एवं प्रत्येक उत्तम हल–योग्य समूह एक CLT समूह होता है। वैसे ऐसे हल–योग्य समूह होते हैं जो CLT नहीं होते (उदाहरणार्थ, A_4) एवं ऐसे CLT समूह होते हैं जो उत्तम हल–योग्य नहीं होते (उदाहरणार्थ, S_4, जो कि डिग्री 4 का सममित समूह है)।

लैग्रांज प्रमेय एवं इसके उपनिगमन/उपप्रमेय (Corollaries)

लैमा: माना H G का उपसमूह है। माना $r,s–G$। अब $Hr=Hs$ यदि एवं मात्र यदि $rs^{-1}\in H$। अन्यथा Hr, Hs में कोई अवयव सामान्य नहीं होगा। इसी प्रकार $rH=sH$, यदि $s^{-1}r\in H$, अन्यथा rH, sH में सामान्य में कोई अवयव नहीं होता।

प्रमाण: यदि $rs^{-1}=h\in H$ तो $H=Hh=(Hr)s^{-1}$। s से दोनों ओर दायें भाग में गुणन करते हुए $Hr=Hs$ मिलता है। इसके विपरीत यदि $Hr=Hs$ तो चूँकि $r\in Hr$ (क्योंकि $1\in H$) हमारे पास कुछ $r=h's$ के लिये $h'\in H$। s^{-1} द्वारा दायीं ओर गुणन करते हुए प्रदर्शित होता है कि $rs^{-1}\in H$।

अब मान लें कि Hr, Hs में सामान्य (Common) कोई अवयव है, अर्थात् कुछ h_1, $h_2\in H$ के लिये $h_1r=h_2s$। इसका अर्थ यह हुआ कि $rs^{-1}=h_1^{-1}h_2\in H$, इस प्रकार उपरोक्तानुसार $Hr= Hs$।

प्रमेय 2.3 (लैग्रांज के अनुसार) : यदि H, G का उप–समूह है तो किसी धनात्मक पूर्णांक n के लिये $|G|=n|H|$। इसे G में H का निर्देशिका कहा जाता है। इसके

अतिरिक्त $g1,...,gn$ इस प्रकार है, कि $G=Hr_1 \cup ... \cup Hr_n$ व इसी प्रकार H से सम्बन्ध बायीं ओर सहसमुच्चय सहित।

प्रमाणः कोई $r_1 \in G$ लें। ध्यान दे कि $|Hr_1|=|H|$। यदि $Hr_1 \neq G$ तो कोई $r_2 \in G \in Hr_1$ लें। लैमा अनुरूप Hr_1, Hr_2 असंबंधित हैं, अतः हमारे पास $|Hr_1 \cup Hr_2|=2|H|$। इस दिशा में आगे बढ़ते हुए किसी धनात्मक पूर्णांक n के लिये n चरणों के उपरान्त हमारे पास G के सभी अवयवों का हिसाब होगा। हमारे पास $|G|=n|H|$ व $G=Hr_1 \cup ... \cup Hr_n$ होंगे।

टिप्पणी

उपप्रमेयः G एक समूह हो एवं $g \in G$ तो g का कोटि $|G|$ को विभाजित करता है।

उपप्रमेयः G अभाज्य कोटि का एक समूह हो तो G का उपसमूह नहीं है एवं इसी कारण यह चक्रीय है।

2.4 फ़ेर्मेट प्रमेय

संख्या सिद्धांत में फ़ेर्मेट प्रमेय (Fermat's Theorem) को '**फ़ेर्मेट का लिटल प्रमेय**' (Fermat's Little Theorem) एवं 'फ़ेर्मेट का प्राइमेलिटी परीक्षण' (Fermat's Primality Test) भी कहा जाता है; इसे पियरे डि फ़ेर्मेट (Pierre de Fermat) नामक एक फ़्रान्सीसी गणितज्ञ द्वारा 1640 में लाया गया। इस प्रमेय के अनुसार किसी अभाज्य संख्या p व किसी पूर्णांक a की स्थिति में p द्वारा a को भागित नहीं किया जाता (युग्म/(Pair) अपेक्षाकृत अभाज्य है), p $a^p - a$ में सटीकता से विभक्त होता है। भले ही संख्या n किसी a के लिये $a^n - a$ में सटीकता से विभाजित नहीं होती तो a को संयोजित संख्या होना चाहिए फिर भी इसका विलोम वास्तविक होगा ऐसा आवश्यक नहीं। उदाहरणार्थ $a = 2$ व $n = 341$ हो तो a व n अपेक्षाकृत या अभाज्य हैं, एवं 341 सटीकता से $2^{341} - 2$ में विभक्त होता है।

वैसे $341 = 11 \times 31$, अतः यह एक संयोजित संख्या है, अर्थात् संयोजित संख्या का एक विशेष प्रकार जिसे छद्म अभाज्य (Pseudoprime) कहा जाता है। इस प्रकार फ़ेर्मेट प्रमेय में वह परीक्षण (Test) सामने आता है, जो आवश्यक तो है परन्तु प्रमुखता के लिये पर्याप्त नहीं।

कई फ़ेर्मेट प्रमेयों की भाँति फ़ेर्मेट गणितज्ञ द्वारा प्रस्तुत कोई प्रमाण नहीं पाया गया। इस प्रमेय का प्रथम ज्ञात प्रकाशित प्रमाण 1736 में लियोन्हार्ड यूलर (Leonhard Euler) नामक एक स्विस गणितज्ञ द्वारा लाया गया था। फ़ेर्मेट प्रमेय का विशेष प्रकरण जिसे 'चाईनीज़ संकल्पना (Chinese Hypothesis)' कहा जाता है, लगभग 2,000 वर्ष पुराना होना सम्भव है।

प्रमेय 2.4 (फ़ेर्मेट द्वारा): किसी पूर्णांक a व अभाज्य p के लिये,

$$a^p \equiv a \pmod{p}.$$

प्रमाणः यदि $(a, p) = 1$ तो यूलर प्रमेय (By Euler Theorem) द्वारा

$$a^{\varphi(p)} \equiv 1 \pmod{p}$$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

जैसे $\varphi(p) = p - 1$

$\Rightarrow a^p \equiv a \pmod{p}$

यदि $(a, p) = p$, तो $p \mid a \Rightarrow p \mid a^p$

$\therefore \quad p \mid a^p - a$

$\Rightarrow a^p \equiv a \pmod{p}$.

टिप्पणी

ध्यान दे: $(a, p) = 1$ या p जैसे 1 और p सभी p के भाजक हैं।)

उदाहरण 2.1: सिद्ध करें कि 3, 5 व 7 तीन ही निरंतर (Consecutive) विषम पूर्णांक (Odd Integer) हैं, जो कि अभाज्य हैं।

हल: मान लें कि p व $p+2$ निरंतर अभाज्य $p > 3$ हैं। हम दर्शाते हैं कि 12 उनके योगफल (Sum) को भागित करता है।

$p > 3 \Rightarrow (p, 3)$ महत्तम सामान्य भाजक $= 1$

$\Rightarrow p^2 \equiv 1 \pmod{3}$ फर्मेट प्रमेय के द्वारा।

$\Rightarrow 3 \mid p^2 - 1$

$\Rightarrow 3 \mid (p-1)(p+1)$

यदि $3 \mid p-1$ तो $p - 1 = 3k \Rightarrow p = 3k+1 \Rightarrow p+2 = 3k+3 =$ 3 का गुणज (Multiple)।

किन्तु $p+2$ एक अभाज्य > 3 है।

अतः हमें विरोधाभास मिलता है।

इसीलिये $3 \mid p+1 \Rightarrow p+1 =$ 3 का गुणज।

चूँकि p विषम है, $p+1$ भी 2 का गुणज है।

अतः $p+1$, 6 का गुणज है।

इसीलिये $p + (p+2) = 2p + 2 = 2(p+1) =$ 12 का गुणज

$\Rightarrow 12 \mid p + (p+2)$

मान लेते हैं कि $p, p+2, p+4$ तीन निरंतर विषम पूर्णांक हैं जो कि अभाज्य $p > 3$ हैं।

उपरोक्तानुसार $12 \mid 2p+2$, $12 \mid (p+2) + (p+4) = 2p + 6$,

अतः $12 \mid 2p + 6 - (2p + 2) = 4$, एक विरोधाभास है।

इसी कारण 3, 5 व 7 ही तीन निरंतर विषम अभाज्य हैं।

उदाहरण 2.2: दर्शायें कि यदि G की कोटि 10 का समूह है तो इसमें कोटि 5 का उपसमूह होना चाहिए।

हल: लैग्रांज प्रमेय अनुरूप ऐसा उपसमूह अस्तित्व में हो सकता है।

हम सर्वप्रथम दावा करते हैं, कि G के समस्त अवयव कोटि 2 के नहीं हो सकते। मान लेते हैं कि यदि ऐसा हो तो हम निम्नानुसार आगे बढ़ते हैं–

माना $a, b \in G$ यदि कोटि 2 के दो भिन्न–भिन्न अवयव हों

माना $H = < a >, K = < b >$, चक्रीय उप–समूह हों a व b द्वारा उत्पन्न, तो

$o(H) = 2, o(K) = 2$

चूँकि G के सभी अवयव की कोटि 2 के हैं इसलिये यह एक एबेलियन होगा ही।

अतः $HK = KH \Rightarrow HK$, G का उपसमूह है।

टिप्पणी

एवं चूँकि $o(HK) = \frac{o(H).o(K)}{o(H \cap K)} = \frac{2 \times 2}{1} = 4$

ध्यान दें: $H \cap K = \{e\}$ क्योंकि $a \neq b$

लैग्रांज प्रमेय के अनुसार $o(HK)$, $o(G)$ को भागित करेगा।

इसीलिये, $4 \mid 10$ जो कि वास्तविक नहीं है, इसी कारण हमारी धारणा मिथ्या है, एवं इस प्रकार G के समस्त अवयव कोटि 2 के नहीं हो सकते।

पुनः चूँकि G परिमित है, अतः समस्त $a \in G$ हेतु $o(a) \mid o(G)$।

$\Rightarrow \exists$ कम से कम एक अवयव $a \in G$ इस प्रकार है कि $o(a) = 5$ या 10

यदि $o(a) = 5$ तो $H = < a >$ कोटि 5 का एक उपसमूह है।

यदि $o(a) = 10$ तो $H = < a^2 >$ कोटि 5 का एक उपसमूह है।

किसी भी प्रकरण में हमारा परिणाम सिद्ध होता है।

उदाहरण 2.3: माना कि G कोई समूह इस प्रकार हो कि इसके समस्त उपसमूहों (जो $\{e\}$ से भिन्न हैं) का सर्वनिष्ठ $\{e\}$ से भिन्न एक उपसमूह है। सिद्ध करें कि G के प्रत्येक अवयव में परिमित कोटि के है।

हल: माना $a \in G$ कोई अवयव हो तो,

यदि $a = e, o(a) = 1$

$a \neq e$ हो एवं मान लेते हैं कि $o(a)$ परिमित नहीं है।

चक्रीय उपसमूहों $< a >, < a^2 >, < a^3 >, \ldots$ का विचार करें।

चूँकि $< a^i > \neq \{e\}$ के जैसे प्रत्येक $o(a)$ परिमित नहीं है।

दिये गए नियमानुसार $< a > \cap < a^2 > \cap < a^3 > \cap \ldots \neq \{e\}$

चूँकि चक्रीय उप–समूहों का सर्वनिष्ठ चक्रीय उपसमूह है तो किसी पूर्णांक m के लिये $\bigcap_i < a^i > = < a^m >$ होगा।

पुनश्च समस्त i के लिये $< a^m > \subseteq < a^i >$

विशेषतया $< a^m > \subseteq < a^{2m} >$

किन्तु $< a^{2m} > \subseteq < a^m >$

(m के गुणज $2m$ के गुणज हैं)

$\Rightarrow < a^m > = < a^{2m} >$

इस प्रकार $a^m \in < a^m > \Rightarrow a^m \in < a^{2m} >$

$\Rightarrow a^m = (a^{2m})^k$

$\Rightarrow a^{m(2k-1)} = e$

$o(a)$ परिमित है। जो एक विरोधाभास है।

इसी कारण परिणाम सिद्ध हुआ।

टिप्पणी

प्रमेय 2.5: यदि G कोटि n का एक परिमित समूह है एवं कोटि d के n ∃ अद्वितीय उपसमूह के प्रत्येक भाजक (Divisor) d के लिये; तो G चक्रीय है।

प्रमाण: माना $d \mid n$ हो तो परिभाषित करें कि $A(d) = \{x \in G \mid o(x) = d\}$

मान लेते हैं कि $A(d) \neq \varphi$ तो $\exists\, x \in G$ इस प्रकार है, कि $o(x) = d$

माना $H = < x >$ हो तो $o(x) = o(H) = d$। इससे H में कोटि d के H या $\varphi(d)$ अवयव अथवा $\varphi(d)$ के उत्पन्नकर्ता (Generator) सामने आते हैं। यदि $\exists, y \in G, y \notin H$ इस प्रकार हो कि $o(y) = d$ तो $K = < y >$ कोटि d का एक उपसमूह है। यह प्रदर्शित है कि G में कोटि d का अद्वितीय उपसमूह है।

अतः $K = H \Rightarrow y \in H$, एक विरोधाभास है। इस प्रकार की कोटि d के G में अवयवों की संख्या $\varphi(d)$ है।

अतः $o(A(d)) = \varphi(d)$ यदि $A(d) \neq \varphi$

एवं $o(A(d)) = 0$ यदि सभी $d \mid n$ के लिए $A(d) = \varphi$

स्पष्टतः $G = \underset{d|n}{\cup} A(d)$

माना कि $d_1, ..., d_s$ सभी n के भाजक (Divisor) हैं।

मान लें कि $A(d_1) = \varphi, ..., A(d_i) = \varphi$

एवं $A(d_{i+1}) \neq \varphi, ..., A(d_s) \neq \varphi$

ध्यान दें: समस्त $d \mid n$ के लिये $A(d) = \varphi$ तो $o(G) = 0$ एक विरोधाभास है। अतः किसी $d \mid n$ हेतु $A(d) \neq \varphi$।

अतः $o(A(d_1)) = ... = o(A(d_i)) = 0$

और $o(A(d_{i+1})) = \varphi(d_{i+1}) ..., o(A(d_s)) = \varphi(d_s)$

अब $G = \underset{d|n}{\cup} A(d) \quad \Rightarrow \quad o(G) = \sum_{d|n} o(A(d))$

$$\Rightarrow n = \varphi(d_{i+1}) + ... + \varphi(d_s)$$

$$n = \sum_{d|n} \varphi(d)$$

$\Rightarrow \quad \varphi(d_1) + ... + \varphi(d_i) + \varphi(d_{i+1}) + ... + \varphi(d_s) = \varphi(d_{i+1}) + ... + \varphi(d_s)$

$\Rightarrow \quad \varphi(d_1) + ... + \varphi(d_i) = 0$, एक विरोधाभास (Contradiction) है।

अतः समस्त $d \mid n$ हेतु $A(d) \neq \varphi$ है।

विशेषतया $A(n) \neq \varphi \Rightarrow \exists\, x \in A(n) \Rightarrow \exists\, x \in G, o(x) = n = o(G) \Rightarrow G$ एक चक्रीय समूह है।

टिप्पणी

अपनी प्रगति जांचिए

1. सहसमुच्चय वियोजन से आपका क्या अभिप्राय है?
2. लैग्रांज प्रमेय का विवरण बतायें।
3. लैग्रांज प्रमेय के उपनिगमन/उपप्रमेय क्या–क्या हैं?
4. फ़ेर्मेट प्रमेय में क्या परिभाषित होता है?

2.5 सामान्य उपसमूह

परिभाषा: समूह G के उपसमूह H को G का सामान्य उपसमूह (Normal Subgroup) कहा जाता है यदि समस्त $a \in G$ के लिये $Ha = aH$।

सामान्य उपसमूह को अपरिवर्तनीय (Invariant) अथवा स्वतः संयोजित (Self Conjugate) उपसमूह भी कहा जाता है।

स्पष्ट है, कि G व $\{e\}$, G के सामान्य उपसमूह हैं, एवं नगण्य सामान्य उपसमूह कहे जाते हैं। समूह $G \neq \{e\}$ को **सरल समूह** (Simple Group) तभी कहा जाता है यदि G के सामान्य उपसमूह $\{e\}$ व G ही हैं। अभाज्य कोटि के सभी समूह सरल होते हैं।

सरलता से यह देखा जा सकता है कि यदि H, G का सामान्य उपसमूह हो एवं K, G का उपसमूह इस प्रकार हो कि $H \subseteq K \subseteq G$ तो K में H सामान्य है। पुनः यदि G एबेलियन हो तो इसके सभी उपसमूह सामान्य होंगे। हम यह समझाने के लिये संकेतन का प्रयोग करते हैं कि $H \leq G$, G में H सामान्य है।

$H = \{1_b – 1\}$ एक सामान्य उपसमूह है, G चतुष्क (Quaternion) समूह का।

उदाहरण 2.4: $H = \{1, –1\}$ एक सामान्य उपसमूह है, G चतुष्क (Quaternion) समूह। वस्तुतः किसी $a \in G$ के लिये $Ha = \{a, –a\} = aH$।

निम्नांकित दो प्रमेयों से हमें समतुल्यता पदों से ज्ञात होता है, जिनमें कि समूह का कोई समूह सामान्य है अथवा नहीं यह देखा जाता है। अतः इनमें से भी किसी भी एक को सामान्य उपसमूह की परिभाषा के रूप में देखा जा सकता है।

प्रमेय 2.6: समूह G का उपसमूह H, G में सामान्य है, यदि समस्त $g \in G$ हेतु $g^{–1}Hg = H$।

प्रमाण: माना H, G में सामान्य मानें तो समस्त $g \in G$ हेतु,

$\Rightarrow g^{–1}Hg = g^{–1}\ (gH) = (g^{–1}g)\ H = H$

इसके विपरीत समस्त $g \in G$ मानने पर

$g^{–1}Hg = H$ सभी $g \in G$ के लिए

तो, $g(g^{–1}Hg) = gH$

$\Rightarrow (gg^{–1})Hg = gH$

$\Rightarrow \quad Hg = gH.$

इसी कारण H सामान्य है।

टिप्पणी

प्रमेय 2.7: समूह G का उपसमूह H, G में सामान्य है, यदि समस्त $h \in H, g \in G$ हेतु $g^{-1}hg \in H$।

प्रमाण: H, G में सामान्य है तो सभी $a \in G$ के लिए $Ha = aH$

माना $h \in H, g \in G$ कुछ अवयव हों तो,

$hg \in Hg = gH$

$\Rightarrow hg = gh_1$ कुछ $h_1 \in H$ के लिए

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

जिससे परिणाम सिद्ध हुआ।

इसके विपरीत माना $a \in G$ कोई अवयव हो तो,

$a^{-1}ha \in H$ सभी $h \in H$ के लिए

$\Rightarrow \quad a(a^{-1}ha) \in aH$ सभी $h \in H$ के लिए

$\Rightarrow \quad ha \in aH$ सभी $h \in H$ के लिए

$\Rightarrow \quad Ha \subseteq aH$

$b = a^{-1}$ लेने पर, जहाँ $b \in G$

$b^{-1}\, hb \in H\ h \in H$

$\Rightarrow \quad aha^{-1} \in H$ सभी $h \in H$ के लिए

$\Rightarrow \quad (aha^{-1})a \in Ha$ सभी $h \in H$ के लिए

$\Rightarrow \quad ah \in Ha$ सभी $h \in H$ के लिए

$\Rightarrow \quad aH \subseteq Ha.$

इसी कारण $Ha = aH$, दर्शा रहा है कि H सामान्य है।

टिप्पणी (Remark): स्पष्ट है कि तर्क में कोई अन्तर नहीं पड़ता यदि उपरोक्त पदों को समस्त $h \in H, g \in G$ हेतु $ghg^{-1} \in H$ के रूप में पढ़ा जाये।

आगामी प्रमेय में भी किसी उपसमूह के सामान्य होने के लिये समतुल्यता पद प्रस्तुत है, परन्तु इस प्रमेय का महत्व अत्यधिक है, क्योंकि यह हमें **'भागफल समूह' (Quotient Group)** के निर्माण में सहायता करता है। प्रमेय का मूल विवरण द्विआधारी संरचना (Binary Comparition) की उपस्थिति दर्शाता है।

प्रमेय 2.8: समूह G का उपसमूह H, G का सामान्य उपसमूह है, यदि G में H के दो दायें सहसमुच्चय का गुणन पुनः G में H का दायाँ सहसमुच्चय हो तो।

प्रमाण: H को G का सामान्य उपसमूह मान लेते हैं। माना Ha और Hb व G में H के दो दायें सहसमुच्चय हों तो,

$$(Ha)(Hb) = H(aH)b$$
$$= H(Ha)b$$

$$= HHab$$

$$= Hab\ ab \in G$$

इसके विपरीत हमें स्पष्ट है, कि G में H के किन्हीं दो दायें सहसमुच्चय का गुणन पुनः एक दायाँ सहसमुच्चय है।

टिप्पणी

H को सामान्य दर्शाने के लिये $g \in G$ का कोई अवयव मान लेते हैं।

अब G में H के दो दायें सहसमुच्चय Hg व Hg^{-1} हैं। इस प्रकार $HgHg^{-1}$ भी G में H का दायाँ सहसमुच्चय है।

हम दावा करते हैं कि $HgHg^{-1} = He$

अब $egeg^{-1} \in HgHg^{-1}$

$\Rightarrow$ $e \in HgHg^{-1}$

$e \in H$ भी

इस प्रकार H व $HgHg^{-1}$ एक अवयव सामान्य वाले दो दायें सहसमुच्चय हैं। समतुल्यता वर्गों के गुणधर्मों का पुनर्स्मरण करने पर हमें विदित है कि दो दायें सहसमुच्चय या तो समतुल्य होते हैं, अथवा सामान्य में इनमें कोई अवयव नहीं होता। इस प्रकार (चूँकि e सामान्य अवयव है)

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

अब $hgh_1g^{-1} \in HgHg^{-1}$ सभी $h, h_1 \in H, g \in G$ के लिए

$\Rightarrow$ $hgh_1g^{-1} \in H$ सभी $h, h_1 \in H, g \in G$ के लिए

$\Rightarrow$ $h^{-1}(hgh_1g^{-1}) \in h^{-1}H$

$\Rightarrow$ $gh_1g^{-1} \in H$ सभी $h_1 \in H, g \in G$ के लिए

H, G में सामान्य है।

इसी कारण यह परिणाम हुआ।

समूह G का उपसमूह H को मानें तो $g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$ को परिभाषित करें।

अब जैसा कि पूर्व में देख चुके हैं कि $g^{-1}Hg$ ये G के उपसमूह का निर्माण होता है।

पुनश्च यदि हम $f(h) = g^{-1}hg$ द्वारा मानचित्रण $f: H \to g^{-1}Hg$ को परिभाषित कर रहे हों तो f, 1–1 आच्छादक (Onto) प्रतिचित्रण है।

G परिमित होने की स्थिति में इसका तात्पर्य होगा कि दोनों H व $g^{-1}Hg$ (किसी $g \in G$ हेतु) में समान संख्या में अवयव होंगे।

इस परिणाम का प्रयोग करते हुए इस प्रकार हमने सिद्ध किया कि यदि G परिमित समूह H का उपसमूह इस प्रकार हो कि G का कोई ऐसा अन्य उपसमूह नहीं है जिसमें H के पास जितनी संख्या में अवयव हों तो H, G में सामान्य है। अन्ततः H व $g^{-1}Hg$ (किसी $g \in G$ के लिये) में समान संख्या में अवयव होने का तात्पर्य (प्रदर्शित नियम के अनुसार) यह होता है, कि ये समतुल्य हैं, एवं $H = g^{-1}Hg$ का तात्पर्य यह कि H सामान्य है।

टिप्पणी

उदाहरण 2.5: सिद्ध करें कि समूह G का गैर रिक्त उपसमुच्चय H समस्त $x, y \in H$, $g \in G, (gx)(gy)^{-1} \in H$ के लिये सामान्य उपसमूह G है।

हल: माना कि H, G का सामान्य उपसमूह हो एवं माना कि $x, y \in H, g \in G$ कोई भी अवयव हैं

तो, $(gx)(gy)^{-1} = (gx)(y^{-1}g^{-1}) = g(xy^{-1})g^{-1} \in H$

चूँकि $xy^{-1} \in H, g \in G$, अतः G में H सामान्य है।

इसके विपरीत हम दर्शाते हैं, कि H, G का सामान्य उपसमूह है।

माना $x, y \in H$ कोई भी अवयव हैं।

तो $xy^{-1} = exy^{-1}\ e = (ex)\ (ey)^{-1} \in H$ जैसे $e \in G$

अर्थात् H, G का एक उपसमूह है।

पुनश्च $h \in H, g \in G$ कोई भी अवयव हों तो

चूँकि $(gh)(ge)^{-1} \in H$

हम पाते हैं कि $(gh)(eg^{-1}) \in H$

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

$\Rightarrow$ H सामान्य है।

उदाहरण 2.6: दर्शायें कि समूह G में $N(a)$ का सामान्यीकरण हो सकता है, कि G का सामान्य उपसमूह न हो।

हल: माना $G = S_3$ व $a = (23)$ तो

$N(a) = N((23)) = \{\sigma \in S_3 \mid \sigma(23) = (23)\sigma\} = \{I, (23)\}$

चूँकि $N(a)(12) = \{(12), (132)\}$

एवं $(12)N(a) = \{(12), (123)\}$

हमें प्राप्त होता है $N(a)(12) \neq (12)N(a)$ अथवा यह कि $N(a)$ सामान्य नहीं है।

उदाहरण 2.7: यदि N कोटि 2 का सामान्य उपसमूह (समूह G के) हो तो दर्शायें कि $N \subseteq Z(G)$, G का केन्द्र है।

हल: माना $N = \{a, e\}$ हैं

चूँकि $e \in Z(G)$ (e केन्द्र उपसमूह होने पर e को अन्तर्विष्ट करता है) हम यह दर्शाना चाहते हैं कि $a \in Z(G)$ है।

अर्थात् सभी $g \in G$ के लिए $ag = ga$

अथवा सभी $g \in G$ के लिए $g^{-1}ag = a$

माना $g \in G$ कोई अवयव हो तो $a \in N$ व N सामान्य है

अतः $g^{-1}ag \in N = \{a, e\}$

$\Rightarrow g^{-1}ag = a$ या $g^{-1}ag = e$

चूँकि $g^{-1}ag = e \Rightarrow ag = ge \Rightarrow ag = eg \Rightarrow a = e,$ जो कि वास्तविक नहीं है।

हम पाते हैं $g^{-1}\ ag = a\ \Rightarrow a \in Z(G)$

अथवा $N \subseteq Z(G)$

उदाहरण 2.8: दर्शायें कि G का उपसमूह N सामान्य है, यदि $xy \in N \Rightarrow yx \in N$

हल: N को G में सामान्य एवं $xy \in N$ मानने पर।

टिप्पणी

चूँकि $yx = y(xy)y^{-1}$ एवं $xy \in N, y \in G$, में N सामान्य है, तो हमें प्राप्त होता है

$$y(xy)y^{-1} \in N \Rightarrow yx \in N$$

इसके विपरीत माना $n \in N, g \in G$ कोई भी अवयव हों तो $n \in N \Rightarrow (ng)\, g^{-1} \in N$

$\Rightarrow \quad g^{-1}(ng) \in N$ (दिये गए नियमानुसार)

G में N सामान्य है।

उदाहरण 2.9: सिद्ध करें कि G का उपसमूह H सामान्य है यदि,

$Ha \neq Hb \Rightarrow aH \neq bH$

हल: G में H में सामान्य हो एवं $Ha \neq Hb$ मान लेने से।

तो $\quad aH \neq bH$

चूँकि $Ha = aH, Hb = bH$ क्योंकि G में H सामान्य है।

इसके विपरीत माना कि $Ha \neq Hb \Rightarrow aH \neq bH$ हैं।

तो $aH = bH \Rightarrow Ha = Hb$

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

अब $g \in G, h \in H$ कोई भी अवयव हों तो,

$h^{-1} \in H \Rightarrow h^{-1}gg^{-1} \in H$

$\Rightarrow (h^{-1}g)\,(g^{-1}) \in H \Rightarrow (h^{-1}g)^{-1}\, g \in H$

$\Rightarrow g^{-1}hg \in H$

H, G में सामान्य है।

उदाहरण 2.10: माना कि H समूह G का उपसमुच्चय हो एवं माना $N(H) = \{x \in G \mid Hx = xH\}$, G में H का सामान्यीकरण हो तथा $N(H)$, G का एक उप–समूह हो।

(i) यदि H, G का उपसमूह हो तो $N(H)$, G का सबसे बड़ा उपसमूह है, जिसमें H सामान्य है।

(ii) यदि H, G का उपसमूह हो तो H, G में सामान्य है यदि $N(H) = G$।

(iii) उदाहरण से दर्शायें कि (i) का विपरीत विफल हो जाता है यदि H, G का एकमात्र उप–समुच्चय हो।

(iv) यदि H, G का एक उपसमूह हो एवं K, $N(H)$ का एक उपसमूह है तो H, HK का सामान्य उपसमूह है।

हल: (i) हम दर्शाते हैं कि H, $N(H)$ में सामान्य है।

चूँकि, सभी $h \in H$ के लिए $Hh = hH$

हम पाते हैं, सभी $h \in H$ के लिए $h \in N(H)$

टिप्पणी

इस प्रकार $H \leq N(H)$

सभी $x \in N(H)$ के लिए $N(H)$, $Hx = xH$ की परिभाषानुरूप।

$H, N(H)$ में सामान्य है।

$N(H)$, G का सबसे बड़ा उपसमूह है जिसमें H सामान्य है यह दर्शाने के लिये मान लें कि G का कोई उपसमूह K इस प्रकार है कि H, K में सामान्य है।

तो सभी $k \in K$ के लिए $k^{-1} Hk = H$

$\Rightarrow Hk = kH$ सभी $k \in K$ के लिए

$\Rightarrow k \in N(H)$ सभी $k \in K$ के लिए

$\Rightarrow K \subseteq N(H)$

(ii) H को G का सामान्य उपसमूह मानें तो $N(H) \subseteq G$ (परिभाषानुरूप)

माना $x \in G$ कोई अवयव हो तो $xH = Hx$ क्योंकि G में H सामान्य है।

$\Rightarrow x \in N(H) \Rightarrow G \subseteq N(H)$

इसी कारण $G = N(H)$

माना $G = N(H)$ इसके विपरीत H को G का उपसमूह मानें (जैसा कि दिया गया है) एवं माना $h \in H, g \in G$ कोई भी अवयव हों तो,

$g \in N(H)$ जैसे $N(H) = G$

$\Rightarrow gH = Hg$

$\Rightarrow H, G$ में सामान्य है।

(iii) $G = < a > = \{e, a, a^2, a^3\}$ का विचार करें तो चक्रीय होने से G एबेलियन समूह है।

यदि $H = \{a\}$ मान लें तो G $(e \notin H)$ एक उपसमुच्चय है एवं $N(H) = G$ का उपसमूह नहीं है क्योंकि G एबेलियन है।

(iv) यदि, K, $N(H)$ को एक उपसमूह मानें तो,

$k \in K \Rightarrow k \in N(H) \Rightarrow Hk = kH$

अर्थात् $Hk = kH$ सभी $k \in K$ के लिए

$\Rightarrow \quad HK = KH$

HK, $N(H)$ का उपसमूह है।

ध्यान दें: $h \in H \Rightarrow Hh = hH$ $(=H)$

$\Rightarrow H \subseteq N(H)$ और $K \subseteq N(H)$

पुनः $H \subseteq HK \subseteq N(H)$

इसी कारण HK, H का एक उपसमूह है।

$\Rightarrow HK$, H का सामान्य उपसमूह है।

$[a \in HK \Rightarrow a \in N(H) \Rightarrow Ha = aH]$

2.6 भागफल समूह

टिप्पणी

G कोई समूह एवं N, G का सामान्य समूह हो। G में N के समस्त दायें सहसमुच्चय एकत्र करें एवं वह समुच्चय निर्मित करें जिसे $\frac{G}{N}$ अथवा G/N से इंगित किया जाता है। चूँकि G में N सामान्य है अतः N के किन्हीं दो दायें सहसमुच्चय का गुणन पुनः G में N का दायाँ सहसमुच्चय होगा, अर्थात् $\frac{G}{N}$ पर हमारे पास सुपरिभाषित द्विआधारी संरचना है। अब हम औपचारिक रूप से दर्शाते हैं कि इस समुच्चय $\frac{G}{N}$ से इस गुणन के अधीन समूह का निर्माण इसके द्विआधारी संरचना के रूप में होता है।

$Na, Nb \in \frac{G}{N}, NaNb = Nab \in \frac{G}{N}$ हेतु

यदि $Na, Nb, Nc \in \frac{G}{N}$ कुछ सदस्य हों तो

$Na(NbNc) = Na(Nbc) = Na(bc) = N(ab)c = NabNc = (NaNb)\ Nc$

पुनः $Ne \in \frac{G}{N}$ द्वारा $\frac{G}{N}$ की तत्समक के रूप में कार्य किया जायेगा एवं किसी Na के लिये $Na \in \frac{G}{N}$, Na^{-1} का व्युत्क्रम होगा। इस प्रकार $\frac{G}{N}$ से समूह का निर्माण होता है जिसे G द्वारा N का **खंड समूह** (Factor Group) अथवा **भागफल समूह** (Quotient Group) कहा जाता है।

यह सरलता से देखा जा सकता है कि यदि G एबेलियन हो तो इसका कोई भागफल समूह इस प्रकार होगा,

$$NaNb = Nab = Nba = Nbnb$$

हो सकता है कि इस परिणाम का विलोम न हो।

टिप्पणी (Remarks): (i) $\frac{G}{N}$ में चूँकि N सामान्य है अतः यह महत्वहीन है, कि हम शब्द 'दायें सहसमुच्चयों' का प्रयोग करें अथवा 'बायें सहसमुच्चयों' का क्योंकि समस्त a हेतु $Na = aN$।

(ii) यह देखना वस्तुतः रोचक होगा कि $\frac{G}{\{e\}}$ व $\frac{G}{G}$ किसके समतुल्य हैं।

क्या ये क्रमशः G व $\{e\}$ हैं? वास्तव में तो नहीं, परन्तु 'लगभग'। हम इस विषय पर तब विस्तार से चर्चा करेंगे, जब तुल्याकारिता (Isomorphisms) की बात करेंगे।

प्रमेय 2.9: यदि G एक परिसीमित समूह है एवं N, G का सामान्य उपसमूह हो तो,

$$o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}$$

प्रमाण: चूँकि G परिसीमित है तो प्रमेय का प्रयोग करते हुए।

$\frac{o(G)}{o(N)}$, G में N के सुनिश्चित दायें सहसमुच्चयों की संख्या = $o\left(\frac{G}{N}\right)$

टिप्पणी

प्रमेय 2.10: चक्रीय समूह का प्रत्येक भागफल (Quotient) समूह चक्रीय होता है।

प्रमाण: माना $G = < a >$ एक चक्रीय समूह हो तो G एबेलियन है, अतः G का प्रत्येक उपसमूह सामान्य है।

H को G का कोई उपसमूह मानें।

हम दर्शाते हैं कि $\frac{G}{H}$ चक्रीय है। वस्तुतः हम दावा करते हैं कि $\frac{G}{H}$, Ha द्वारा उत्पन्न है।

माना $Hx \in \frac{G}{H}$ कोई भी अवयव हो तो $x \in G = < a >$,

अर्थात x की कोई घात a मानें

तो $x = a^m$

अर्थात् $Hx = \quad Ha^m \quad = Ha\ a\ .....\ a$ (m बार)

$= Ha\ Ha\ .....\ Ha \qquad (m$ बार)

$= (Ha)^m$

अर्थात $\frac{G}{H}$ का कोई अवयव Hx हैं जिसकी घात $Ha \Rightarrow Ha$ हैं, जो उत्पन्न करता है $\frac{G}{H}$, अतः $\frac{G}{H}$ एक चक्रीय है।

टिप्पणी: (i) उपरोक्त परिणाम $m > 0$ के लिये सिद्ध हुआ। इसी प्रकार $m \leq 0$ को भी हल करें तो समान प्रमाण आयेगा।

ध्यान दे: $a^m = a^{-n} = (a^{-1})^n$ जहाँ $n > 0$ तथा स्मरण करें कि $Ha^{-1} = (Ha)^{-1}$ तथा इसलिए $(Ha^{-1})^n = (Ha)^{-n} = (Ha)^m$

(ii) यदि $G = < a >$ चक्रीय हो एवं $H \leq G$ तो $o(G/H)$ कम धनात्मक पूर्णांक m इस प्रकार है कि $a^m \in H$

हमें विदित है कि यदि $H \leq G$ तो $H = <a^m>$, जहाँ m कम धनात्मक पूर्णांक इस प्रकार हो कि $a^m \in H$

(iii) इस परिणाम का विलोम वास्तविक नहीं है।

उदाहरण 2.11: G के प्रकार $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ के वास्तविकता पर 2×2 आव्यूह का समुच्चय मानें, जहाँ $ad \neq 0$, तो यह सरलता से देखा जा सकता है कि G से आव्यूह गुणन के अधीन समूह बनेगा। $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ एक तत्समक होगा, $\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}$ किसी अवयव $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ का व्युत्क्रम होगा। इसके अतिरिक्त G एबेलियन नहीं है।

N के प्रकार $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$ को सदस्ययुक्त उपसमुच्चय मानें एवं N, G का उपसमूह

टिप्पणी

हो तो सिद्ध करें कि यह प्रकार $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} 1 & akd + bd - \frac{b}{d} \\ 0 & 1 \end{bmatrix} \in N$

के गुणन के रूप में भी सामान्य है।

अतः हमें भागफल समूह $\frac{G}{N}$ मिलता है। हम $\frac{G}{N}$ में एबेलियन दर्शाते हैं।

माना $Nx, Ny \in \frac{G}{N}$ कोई भी अवयव हों तो $x, y \in G$

$x = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}, y = \begin{bmatrix} c & e \\ 0 & f \end{bmatrix}$ मानें।

$\frac{G}{N}$ एबेलियन होगा यदि $NxNy = NyNx.$

$\Leftrightarrow \; Nxy = Nyx$

$\Leftrightarrow \; xy\,(yx)^{-1} \in N$

$\Leftrightarrow \; xyx^{-1}\,y^{-1} \in N$

हम सबको अब यह परखने की आवश्यकता है कि यह वही गुणन है।

$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} c & e \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}\begin{bmatrix} \frac{1}{c} & -\frac{e}{cf} \\ 0 & \frac{1}{f} \end{bmatrix}, \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$ आव्यूहों के प्रकार (Types of Matrix) है।

इस प्रकार हमारे पास एबेलियन भागफल समूह हो सकता है, 'मूल' (Parent) समूह एबेलियन हुए बिना।

उदाहरण 2.12: माना $< \mathbf{Z}, + >$ पूर्णांकों का समूह हो एवं $N = \{3n \mid n \in \mathbf{Z}\}$ मान लें तो N, $\mathbf{Z}$ का सामान्य उप–समूह है।

$\frac{\mathbf{Z}}{N}$ में प्रकार $N + a, a \in \mathbf{Z}$ के सदस्य होंगे।

हम दर्शाते हैं कि $\frac{\mathbf{Z}}{N}$ में तीन ही अवयव हैं। यदि $a \in \mathbf{Z}$ को कोई अवयव मानें जहाँ $a \neq 0, 1, 2$ तो हम विभाजन एलगोरिद्म (Division Algorithm) से लिख सकते हैं,

$a = 3q + r$ जहां $0 \le r \le 2$

$\Rightarrow \; N + a = N + (3q + r) = (N + 3q) + r = N + r$ जैसे $3q \in N$

किन्तु r के मान 0, 1, 2 रख सकते हैं।

इसी कारण $N + a$, $N, N + 1, N + 2$ में से एक होगा।

अथवा $\frac{\mathbf{Z}}{N}$ में ये तीन ही सदस्य हैं।

टिप्पणी

टिप्पणी

(i) इस उदाहरण से यह भी ज्ञात होता है, कि सहसमुच्चय के प्रकरण में हो सकता है कि $Ha = Hb$ का तात्पर्य $a = b$ न हो। उदाहरणार्थ, उपरोक्त उदाहरण में $N+4 = N+1$ परन्तु $4 \neq 1$, $[N+4 = (N+3)+1 = N+1]$

(ii) यह अपरिमित समूह का एक उदाहरण है जिसमें G में परिमित निर्देशिका युक्त N उपसमूह है।

(iii) यह सीमित भागफल समूह G/N का एक उदाहरण भी है जहाँ मूल समूह G परिमित नहीं है। वैसे यह सरलता से देख सकते हैं कि परिमित समूह का भागफल समूह परिमित है।

(iv) यदि $\frac{G_1}{N} = \frac{G_2}{N}$ तो $G_1 = G_2$

माना $g_1 \in G_1$ कोई अवयव हो तो $Ng_1 \in \frac{G_1}{N} = \frac{G_2}{N}$

$\Rightarrow Ng_1 = Ng_2$ किसी भी $g_2 \in G_2$

$\Rightarrow g_1 g_2^{-1} \in N \subseteq G_2 \Rightarrow g_1 g_2^{-1} = g$ किसी भी $g \in G_2$ के लिए

$\Rightarrow g_1 = g g_2^{-1} \in G_2 \Rightarrow G_1 \subseteq G_2$. इसी प्रकार $G_2 \subseteq G_1$

इस कारण से $G_1 = G_2$

उदाहरण 2.13: समूह $\frac{\mathbf{Z}_8}{<6>}$ में अवयव $<6>+5$ की कोटि ज्ञात करें।

हल: हमारे पास $\mathbf{Z}_8 = \{0, 1, 2, ..., 7\}$ mod 8 हैं।

एवं $<6> = \{0, 6, 12\} = H$ (मानते हैं)

अब $\frac{\mathbf{Z}_8}{<6>} = \frac{\mathbf{Z}_8}{H} = \{H, H+1, H+2, H+3, H+4, H+5\}$

$= \{<6>, <6>+1, <6>+2, <6>+3, <6>+4, <6>+5\}$

अब $<6>+5 \neq <6>$ एक तत्समक हैं।

पुनः $2(<6>+5) = <6>+10 = <6>+4 \neq <6>$

इसी प्रकार $3(<6>+5), 4(<6>+5), 5(<6>+5)$ नहीं हैं $<6>$

जहाँ $6(<6>+5) = <6>+30 = <6>$ = तत्समक एवं इसी कारण $<6>+5$ की कोटि 6 होगी।

उदाहरण 2.14: G समूह N का सामान्य उपसमूह हो तो दर्शायें कि किसी $o(Na) | o(a)$ के लिये $a \in G$

हल: माना $o(a) = n$

तो n कम धनात्मक पूर्णांक इस प्रकार है, कि $a^n = e$

इससे प्राप्त होता है $Na^n = Ne$

$\Rightarrow$ $\underset{(n \text{ बार})}{Na \,.\, a.....a} = N$

$\Rightarrow$ $\underset{(n \text{ बार})}{Na \,.\, Na.....Na} = N$

$\Rightarrow$ $(Na)^n = N$, $Na \in \frac{G}{N}$ और N, $\frac{G}{N}$ की तत्समक है।

$\Rightarrow$ $o(Na) \mid n$ या $o(Na) \mid o(a)$

उदाहरण 2.15: यदि G ऐसा समूह हो कि $\frac{G}{Z(G)}$ चक्रीय हो जहाँ $Z(G)$, G का केन्द्र हो तो दर्शायें कि G एबेलियन है।

हल: $Z(G) = N$ लिखें तो $\frac{G}{N}$ चक्रीय है। मान लेते हैं कि यह Ng द्वारा उत्पन्न है।

माना $a, b \in G$ दो अवयव हों तो $Na, Nb \in \frac{G}{N}$

$\Rightarrow$ $Na = (Ng)^n$, $Nb = (Ng)^m$ किसी भी $\in n, m$ के लिए।

$\Rightarrow$ $Na = Ng \,.\, Ng$ ..... $Ng = Ng^n$

$Nb = Ng^m$

$\Rightarrow$ $ag^{-n} \in N$, $bg^{-m} \in N$

$\Rightarrow$ $ag^{-n} = x$, $bg^{-m} = y$ किसी भी $x, y \in N$ के लिए।

$\Rightarrow$ $a = xg^n$, $b = yg^m$

$\Rightarrow$ $ab = (xg^n)\,(yg^m) = x(g^n y)\, g^m$

$= x(yg^n)\, g^m$ जैसे $y \in N = Z(G)$

$= xyg^n\, g^m$

$= xyg^{n+m}$

इसी प्रकार $ba = (yg^m)\,(xg^n) = y\,(g^m x)\, g^n = y\,(xg^m)\, g^n$

$= (yx)g^{m+n}$

$\Rightarrow ab = ba$ क्योंकि $xy = yx$ जबकि $x, y \in Z(G)$

यह दर्शाता है कि G एबेलियन है।

टिप्पणी

(i) हम $\frac{G}{Z(G)}$ मानने की बात कर रहे हैं, इसीलिये $Z(G)$, G का सामान्य उपसमूह है, इस परिणाम को सरलता से वास्तविक होता देखा जा सकता है।

(ii) उपरोक्त हल में प्रदर्शित अनुसार दिशा में आगे बढ़ते हुए सिद्ध होता है कि G/H चक्रीय है जहाँ H, $Z(G)$ का उपसमूह है तो G एबेलियन है।

(iii) यदि G गैर–एबेलियन समूह हो तो $G/Z(G)$ चक्रीय नहीं है।

टिप्पणी

(iv) यदि H में G के किसी सामान्य उपसमूह $\frac{G}{H}$ के लिये चक्रीय हो तो हो सकता है कि G एबेलियन न हो।

टिप्पणी

G चतुष्क (Quaternion) समूह एवं $H = \{\pm 1, \pm i\}$ लेते हैं तो $o(G/H) = \frac{8}{4} =$ 2 अभाज्य (Prime) है। अतः G/H चक्रीय है परन्तु G एबेलियन नहीं है।

उदाहरण 2.16: G की कोटि pq का एक गैर–एबेलियन (Non-Abelian) समूह मानें जहाँ p, q अभाज्य (Primes) हों तो $o(Z(G)) = 1$

हल: चूँकि G गैर–एबेलियन है, तो उदाहरण 2.15 के अनुसार $\frac{G}{Z(G)}$ चक्रीय नहीं है।

अब $o(Z(G)) \mid o(G) = pq$

$\Rightarrow \quad o(Z(G)) = 1, p, q$ या pq

$o(Z(G)) = pq \Rightarrow Z(G) = G$

$\Rightarrow$ G एबेलियन है जबकि ऐसा नहीं है।

$o(Z(G)) = p \Rightarrow o(G/Z(G)) = \frac{pq}{p} = q.$ अभाज्य है, और $G(Z(G))$ चक्रीय हैं।

यह भी वास्तविक नहीं है।

इसी प्रकार यह $o(Z(G)) = q$ नहीं हो सकता है, एवं हमारे पास एक ही सम्भावना शेष रहती है कि $o(Z(G)) = 1$।

उदाहरण 2.17: ऐसे अपरिमित (Infinite) समूह का उदाहरण प्रस्तुत करें जिसमें प्रत्येक अवयव परिमित कोटि का है।

हल: (i) माना $< \mathbf{Q}, + >$ और $< \mathbf{Z}, + >$ को योग के अधीन पूर्णांकों (Integers) एवं परिमेयों (Rational) के समूह मानें तो भागफल समूह होगा,

$$\frac{\mathbf{Q}}{\mathbf{Z}} = \left\{ \mathbf{Z} + \frac{m}{n} \middle| \frac{m}{n} \in \mathbf{Q} \right\}$$

यह एक अपरिमित समूह है। $\frac{\mathbf{Q}}{\mathbf{Z}}$ के किसी सदस्य $\mathbf{Z} + \frac{m}{n}$ का विचार करें।

चूँकि $n\left(\mathbf{Z} + \frac{m}{n}\right) = \mathbf{Z} + n\frac{m}{n} = \mathbf{Z} + m = \mathbf{Z} =$ $\frac{\mathbf{Q}}{\mathbf{Z}}$ का शून्य है।

हम पाते हैं कि $\mathbf{Z} + \frac{m}{n}$ में परिमित कोटि $\leq n$ है। इसी कारण हमारे पास उदाहरण है।

(ii) पुनः विचार करें $G = \left\{ \mathbf{Z} + \frac{m}{p^n} \middle|_{n \geq 0} \right.$ m, n पूर्णांक है, p = निश्चित सम $\Big\}$

तो G, $\frac{\mathbf{Q}}{\mathbf{Z}}$ का एक उपसमूह है।

अब $p^n\left(\mathbf{Z}+\frac{m}{p^n}\right)=\mathbf{Z}+\frac{m}{p^n}p^n=\mathbf{Z}+m=\mathbf{Z}=G$ का शून्य हैं।

टिप्पणी

$\Rightarrow$ $\mathbf{Z}+\frac{m}{p^n}$ का क्रम p^n से विभाजित है।

$\Rightarrow$ $\mathbf{Z}+\frac{m}{p^n}$ का क्रम $p^r,\ r\le n$ है।

$\Rightarrow$ G में प्रत्येक अवयव का परिमित कोटि है एवं प्रकार p^r का है।

चूँकि G अनंत या अपरिमित है, अतः हम पाते हैं कि यह अनंत या अपरिमित p-समूह का एक उदाहरण होगा।

पुनः हम दर्शा सकते हैं, कि G का प्रत्येक उपसमूह $H(\neq G)$ परिमित कोटि का है। इसी कारण यह ऐसे अनंत या अपरिमित समूह का भी उदाहरण है जिसमें प्रत्येक समुचित उपसमूह कोटि का है।

उदाहरण 2.18: दर्शायें कि $<\boldsymbol{Q}, +>$ में परिमित निर्देशिका का समुचित उपसमूह नहीं है।

हल: मान लें कि $H, <\mathbf{Q}, +>$ का कोई समुचित उपसमूह है, जिसमें परिमित निर्देशिका n है तो, $o(\mathbf{Q}/H)=n$

चूँकि $H,\ \exists\ \frac{a}{b}\in\mathbf{Q}$, Q का समुचित उपसमूह इस प्रकार है, कि, $\frac{a}{b}\notin H$

अब यदि $x+H\Rightarrow\frac{\mathbf{Q}}{H}$ कोई अवयव हो तो,

$n(x+H)=H\Rightarrow nx+H=H$

$\Rightarrow nx\in H\quad\forall\ x\in\mathbf{Q}$

$x=\frac{a}{nb}$, को लेते हैं तो $n\frac{a}{nb}\in H$, अर्थात् $\frac{a}{b}\in H$ जो कि वास्तविक नहीं है।

इसी कारण ऐसा उपसमूह नहीं होता।

अपनी प्रगति जांचिए

5. सामान्य उपसमूह क्या है?
6. दो उपसमूह का सम्मिश्रित क्या होता है?
7. क्या चक्रीय समूह का प्रत्येक भागफल समूह चक्रीय होता है?

2.7 अपनी प्रगति जांचिए प्रश्नों के उत्तर

1. H को समूह G का उपसमूह मानें। परिभाषानुरूप G में H का कोई दायाँ सहसमुच्चय रिक्त नहीं है व G में H के दो दायें सहसमुच्चयों या तो असंबंधित हैं अथवा समान। G में H के समस्त दायें सहसमुच्चयों का सम्मिलन G के

टिप्पणी

समतुल्य है। इसी कारण G में H के समस्त दायें सहसमुच्चयों से G का विभाजन होता है। इस विभाजन को G का दाएँ सहसमुच्चय वियोजन कहा जाता है।

2. यदि H, G का उपसमूह हो तो किसी धनात्मक पूर्णांक n हेतु $|G|=n|H|$। इसे G में H का निर्देशिका कहते हैं। इसके अतिरिक्त $g1,...,gn$ इस प्रकार पाये जाते हैं कि $G=Hr_1 \cup ... \cup Hr_n$ एवं इसी प्रकार H के सम्बद्ध बाएँ सहसमुच्चय होते हैं।
3. (i) उपप्रमेय G एक समूह व $g \in G$ हो तो g की कोटि $|G|$ को भागित करता है।

   (ii) उपप्रमेय G अभाज्य कोटि का समूह है तो G में कोई उपसमूह नहीं है एवं इसी कारण यह चक्रीय है।
4. किसी पूर्णांक p व अभाज्य (Prime) a के लिये,

   $a^p \equiv a \pmod{p}$
5. समूह G के उपसमूह H को G का सामान्य उपसमूह कहा जाता है, यदि $Ha = aH$ समस्त $a \in G$ के लिये।
6. यदि H व K समूह G के दो उपसमूह हों एवं $HK = \{hk \mid h \in H, k \in K\}$ तो HK (G का गैर रिक्त उपसमूह)।
7. हाँ, चक्रीय समूह का प्रत्येक भागफल समूह चक्रीय होता है।

2.8 सारांश

- समूह सिद्धांत में समूह G का अवयव g एवं H का उपसमूह G प्रदर्शित है, g के सन्दर्भ में G में H का बायाँ सहसमुच्चय $gH = \{gh : H$ का h एक अवयव है$\}$ g के सन्दर्भ में G में H का दायाँ सहसमुच्चय $Hg = \{hg : H$ का h एक अवयव है$\}$।
- समूह G का उपसमूह N, G का सामान्य उपसमूह है, यदि एवं मात्र यदि G के समस्त अवयवों g के लिये संगत बायें व दायें सहसमुच्चय समतुल्य हों, अर्थात् $gN = Ng$। इसके अतिरिक्त G में N के सहसमुच्चय से जो समूह बनाया जाता है उसे भागफल समूह अथवा खंड समूह कहा जाता है।
- H को समूह G का उपसमूह मानें। परिभाषानुसार G में H का कोई दायाँ सहसमुच्चय रिक्त नहीं है एवं G में H के दो दायें सहसमुच्चय असंबंधित अथवा समान हैं। G में H के समस्त दायें सहसमुच्चयों का संघ G के समतुल्य है। इसी कारण G में H के समस्त दायें सहसमुच्चय के समुच्चय से G का विभाजन होता है। इस विभाजन को G का दाएं सहसमुच्चय वियोजन कहा जाता है।
- समूह G के प्रदर्शित दो उपसमूह H व K के लिये G में K व H के युग्मित सहसमुच्चय रूप $HgK = \{hgk : H$ का h एक अवयव है, k, का एक अवयव है$\}$ के समुच्चय हैं।
- G के साइलो p-उपसमूहों की संख्या रूप $1 + kp$ की है जहाँ $(1+kp) \mid o(G), k$ ऋणात्मक पूर्णांक नहीं है।
- प्रमेय का परिणाम यह है कि अवयव a परिमित कोटि समूह का है, अर्थात् सबसे छोटी धनात्मक पूर्णांक संख्या $k, ak = e$, हैं, जहाँ e समूह का तत्समक अवयव

है, यह उस समूह की कोटि को विभाजित करता है, क्योंकि a का कोटि a द्वारा उत्पन्न चक्रीय उपसमूह की कोटि के समतुल्य है।

टिप्पणी

- यदि H, G उपसमूह है तो किसी धनात्मक पूर्णांक $|G|=n|H|$ हेतु इसे G में H की निर्देशिका कहा जाता है। इसके अतिरिक्त $g1,...,gn$ का अस्तित्व इस प्रकार है कि $G=Hr_1 \cup ... \cup Hr_n$ तथा इसी प्रकार H से सम्बद्ध बायाँ सहसमुच्चय होते हैं।
- यदि G कोटि n का परिमित कोटि है एवं कोटि d के $n \exists$ अद्वितीय उपसमूह के प्रत्येक भाजक d है, तो G चक्रीय है।
- समूह G का उपसमूह H समस्त $g \in G$ हेतु $g^{-1}Hg = H$ के लिये G में सामान्य है।
- समूह G का उपसमूह H समस्त $h \in H, g \in G, g^{-1}hg \in H$ हेतु में सामान्य है।
- समूह G का उपसमूह H, G का सामान्य उपसमूह है यदि G में H के दो दायें सहसमुच्चयों का गुणन पुनः G में H का दायाँ सहसमुच्चय हो।
- यदि G परिमित समूह है एवं G में N का सामान्य उपसमूह है तो $o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}$
- चक्रीय समूह का प्रत्येक भागफल समूह चक्रीय है।
- समूह G के उपसमूह H को G का सामान्य उपसमूह कहा जाता है, यदि समस्त a G हेतु $Ha = aH$।
- सामान्य उपसमूह को अक्रमविनिमय अथवा स्वतः संयोजित उपसमूह भी कहा जाता है।
- G परिमित समूह H का उपसमूह है, G का ऐसा अन्य उपसमूह नहीं है जिसमें H के पास जितनी संख्या के अवयव हों तो H, G में सामान्य है।
- भागफल समूह अथवा खंड समूह ऐसा गणितीय समूह है जिसे प्राप्त करने के लिये समतुल्यता सम्बन्ध का प्रयोग करते हुए बड़े समूह के समान अवयव को संयुक्त किया जाता है जिससे समूह संरचना परिरक्षित रहती है।
- माना H, G का सामान्य उपसमूह हो तो यह सत्यापित किया जा सकता है कि H से सम्बद्ध G के सहसमुच्चय से समूह का निर्माण होता है। इस समूह को H से सम्बद्ध G का खंड समूह अथवा भागफल समूह कहा जाता है, एवं G/H इंगित किया जाता है।
- G के स्वतः संयुग्मित अवयवों के समुच्चय से एबेलियन समूह Z का निर्माण होता है जिसे G का केंद्र कहा जाता है।

2.9 मुख्य शब्दावली

- **सहसमुच्चयः** सहसमुच्चय को बीजगणितीय समूहों का अध्ययन करने के एक मूलभूत साधन के रूप में समझा जाता है। मूलतः लैग्रांज प्रमेय में सहसमुच्चय की महत्त्वपूर्ण केन्द्रीय भूमिका होती है जिसके अनुसार किसी परिमित समूह G के लिये G के प्रत्येक उपसमूह H के अवयवों की संख्या G के अवयवों की संख्या को विभाजित करती है।

टिप्पणी

- **सामान्य उपसमूहः** समूह G का उपसमूह N, G का सामान्य उपसमूह है, यदि और केवल यदि G के समस्त अवयवों g के लिये संगत बायाँ व दायाँ सहसमुच्चय समतुल्य है, अर्थात् $gN = Ng$।
- **दाएँ सहसमुच्चय वियोजन :** G में H के समस्त दायें सहसमुच्चयों का संघ G के समतुल्य है। इसी कारण G में H के समस्त दायें सहसमुच्चयों के समुच्चय से G का विभाजन सामने आता है जिसे कि G का दाएं सहसमुच्चय वियोजन कहा जाता है।
- **युग्मित सहसमुच्चयः** समूह G के H व K (दिए गए दो उपसमूहों) के लिये G में H व K के युग्मित सहसमुच्चय रूप $HgK = \{hgk : H$ का h एक अवयव है, K का k एक अवयव है$\}$ के समुच्चय हैं। ये K के बायें सहसमुच्चय व H के दायें सहसमुच्चय हैं, जब क्रमशः $H = 1$ व $K = 1$ हों।
- **लैग्रांज प्रमेयः** इस प्रमेय के अनुसार किसी परिमित समूह G के लिये H के प्रत्येक उपसमूह G की कोटि (अवयवों की संख्या) द्वारा G की कोटि भागित किया जाता है। जोसेफ़ लुईस लैग्रांज के कारण इस प्रमेय का ऐसा नामकरण किया गया।
- **उपसमूहः** उपसमूह वह समूह है जिसमें समूह के सदस्य अन्य समूह के समस्त सदस्य हों, और सभी समान संक्रिया का विषय हों।

2.10 स्व–मूल्यांकन प्रश्न एवं अभ्यास

लघु–उत्तरीय प्रश्न

1. सहसमुच्चय वियोजन से आपका क्या अभिप्राय है?
2. सिद्ध करें कि परिमित समूह G के दो साइलो p-उपसमूहों G में संयुग्मित हैं।
3. लैग्रांज प्रमेय के विलोम की व्याख्या करें।
4. सिद्ध करें कि यदि G कोटि n का एक परिमित समूह है एवं d के प्रत्येक भाजक $n \exists$ हेतु कोटि d का अद्वितीय उपसमूह हो तो G चक्रीय है।
5. स्वतः संयुग्मित उपसमूह को परिभाषित करें।
6. सरल समूह क्या होता है?
7. ज्ञात करें कि G का उपसमूह N सामान्य है यदि $xy \in \mathrm{N} \Rightarrow yx \ N$।
8. सिद्ध करें कि समूह G में a का सामान्यीकरण $N(a)$ हो सकता है यदि G का सामान्य उपसमूह न हो।

दीर्घ–उत्तरीय प्रश्न

1. साइलो के तृतीय प्रमेय की व्याख्या करते हुए इसका विवरण व प्रमाण ज्ञात कीजिए।
2. सामान्य उपसमूहों की परिचर्चा उपयुक्त उदाहरणों सहित करें।
3. लैग्रांज प्रमेय एवं इसके उपनिगमनों/उपप्रमेयों का वर्णन उदाहरण सहित करें।

4. फ़र्मेट प्रमेय एवं इसके प्रमाण का विवरण उदाहरण सहित प्रस्तुत करें।
5. सिद्ध करें कि समूह G का उपसमूह H, G में सामान्य है यदि समस्त gG हेतु $Hg = H$।
6. दर्शायें कि मात्र एबेलियन सरल समूह अभाज्य कोटि के समूह होते हैं।
7. भागफल समूहों का विवरण विस्तारपूर्वक करें।

टिप्पणी

2.11 सहायक पाठ्य सामग्री

Sharma, Dr Anil and Jitendra Saini. 2016. *Abstract Algebra* (अमूर्त बीजगणित) Jaipur (Rajasthan): RBD Publisher.

Pathak, Dr H. K. 2017. *Abstract Algebra* (अमूर्त बीजगणित). Kolkata (West Bengal): Siksha Sahitya Prakashan.

Herstein, I. N. 1975. *Topics in Algebra*, 2nd Edition. New York: John Wiley and Sons.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. UK: Cambridge University Press (Indian Edition).

Khanna, V. K. and S. K. Bhambari. 2016. *A Course in Abstract Algebra*, 5th Edition. New Delhi: Vikas Publishing House Pvt. Ltd.

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

Gilbert, Linda. 2008. *Elements of Modern Algebra*. Boston: Cengage Learning.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

Childs, Lindsay N. 2008. *A Concrete Introduction to Higher Algebra*. Berlin: Springer Science & Business Media.

इकाई 3 समूह की समरूपता एवं तुल्याकारिता विशेषताएं

टिप्पणी

संरचना

3.0 परिचय

बीजगणित में **समरूपता (Homomorphism)** समान प्रकार की दो बीजगणितीय संरचनाओं (Algebraic Structures) (जैसे दो समूह, दो वलय अथवा दो सदिश स्थान (Vector Spaces)) के मध्य संरचना–परिरक्षक का मानचित्र है। **'समरूपता'** यानि होमोमॉर्फिज़्म शब्द प्राचीन यूनानी शब्द **'होमोज़' (Homos)** (अर्थात् समान) व **'मॉर्फ़े' (Morphe)** (अर्थात् रूप अथवा आकृति) से बनाया गया है। होमोमॉर्फ़िज़्म शब्द 1892 में लाया गया व इसका श्रेय जर्मन गणितज्ञ फ़ेलिक्स क्लॅईन (Felix Klein) (1849–1925) को जाता है। सदिश स्थान के समरूपता को रैखिय मानचित्रों (Linear Maps) भी कहा जाता है एवं इनका अध्ययन रैखिक बीजगणित (Linear Algebra) का विषय है। समरूपता की अवधारणा को 'आकारिता' (Morphism) के नाम से व्यापक मान्यता प्रदान की जा चुकी है। 'आकारिता' (Morphism) कई अन्य संरचनाओं को भी कहा जाता है, जिनमें या तो आधार समुच्चय नहीं होता अथवा जो बीजगणितीय नहीं होतीं। यह व्यापकीकरण श्रेणी सिद्धांत (Category Theory) का आरम्भिक बिन्दु (Starting Point) है।

समरूपता को तुल्याकारिता, अंतरकारिता, स्वाकारिता इत्यादि भी कहा जा सकता है। इनमें से प्रत्येक को इस प्रकार परिभाषित किया जा सकता है जिसे आकारिता के किसी भी वर्ग में व्यापकीकृत किया जा सकता है। अमूर्त बीजगणित में समरूपता के मूलभूत प्रमेय को मूलभूत समरूपता प्रमेय के नाम से भी जाना जाता है, इसका सम्बन्ध दो विषयों के मानचित्र (Map) से है। जिनके मध्य समरूपता प्रदत्त है एवं यह आधारभूत (Kernel) व समरूपता का प्रतिबिंब भी है। समरूपता प्रमेय का प्रयोग करते हुए तुल्याकारिता प्रमेयों को सिद्ध करते हैं।

गणित में क्रमचय (Permutation) ऐसी क्रिया है जिसमें समुच्चय के सदस्यों को अनुक्रम (Sequence) अथवा कोटि में विन्यस्त (Rearrange) किया जाता है, अथवा यदि

टिप्पणी

समुच्चय पहले से कोटि युक्त है तो इसके अवयवों को पुनर्विन्यस्त (Reorder) करने को क्रमचय कहते हैं। बीजगणित में एवं विशेष रूप से समूह सिद्धांत (Group Theory) में समुच्चय S के क्रमचय को S से इसके स्वयं में एकैक आच्छादन (Bijection) के रूप में परिभाषित किया जाता है, अर्थात् यह S से S का एक फलन है, जिसके लिये प्रत्येक अवयव प्रतिबिंब के रूप में सटीक एक बार पाया जाता है।

समूह सिद्धांत में केली प्रमेय (Cayley's Theorem) का नामकरण आर्थर केली (Arthur Cayley) के सम्मान में किया गया है जिसके अनुरूप प्रत्येक समूह G, G पर पार्श्व सममित समूह (Symmetric Group Acting) के उपसमूह से तुल्यकारिक है। इसे G के अवयवों पर G के समूह क्रियाओं (Group Action) के उदाहरण के रूप में समझा जा सकता है। समुच्चय G का क्रमचय G आच्छादक G लेने पर कोई एकैक आच्छादन फलन है।

इस इकाई में आप समूहों के समरूपता (Homomorphism) व तुल्यकारिक (Isomorphism) एवं इनकी विशेषताएं, समरूपता के मूलभूत प्रमेय, रूपांतरण व क्रमचय समूह, S_n ($S_n, n < 5$ के विभिन्न उपसमूह) एवं केली प्रमेय का अध्ययन करेंगे।

3.1 उद्देश्य

इस इकाई को पढ़ने के बाद आप–

- समूहों की समरूपता एवं तुल्याकारिता का वर्णन कर पाएंगे;
- समूहों की समरूपता व तुल्याकारिता विशेषताओं का वर्णन कर पाएंगे;
- समरूपता के मूलभूत प्रमेय को समझ पाएंगे;
- समूह का रूपांतरण एवं क्रमचय की व्याख्या कर पाएंगे;
- S_n की व्याख्या ($S_n, n < 5$ के विभिन्न उपसमूह) कर पाएंगे;
- केली प्रमेय को समझ पाएंगे।

3.2 समूहों का समरूपता एवं तुल्याकारिता

बीजगणित में, समरूपता (Homomorphism) एक संरचना है जो दो बीजगणितीय संरचनाओं (Algebraic Structures) के बीच मानचित्र को संरक्षित करती है जिसमें एक ही प्रकार की संरचनाएं, जैसे दो समूह, दो वलय, या दो सदिश स्थान हों।

शब्द **'समरूपता'** प्राचीन ग्रीक भाषा 'होमोस' (Homos) से आया है जिसका अर्थ है समान और **'मोर्फे'** (Morphe) शब्द का अर्थ रूप व आकार होता है। 'समरूपता' शब्द की उत्पत्ति 1892 में हुई और इसका श्रेय जर्मन के गणितज्ञ फ़ेलिक्स क्लॅईन (Felix Klein) (1849–1925) को दिया गया।

समरूपता की अवधारणा को सामान्य रूप से आकारिता (Morphism) के नाम पर, कई अन्य संरचनाओं के लिए प्रयोग किया गया है, जिसमें या तो अंतर्निहित समुच्चय (Set) नहीं हैं, या यह बीजगणितीय नहीं है। यह सामान्यीकरण श्रेणी के सिद्धांत का प्रारंभिक बिंदु हैं। समरूपता एक तुल्याकारिता भी हो सकता है, एक

टिप्पणी

अंतरकारिता, या एक स्वाकारिता (Automorphism), आदि। उनमें से प्रत्येक को इस तरह से परिभाषित किया जा सकता है जिसे किसी भी वर्ग के लिए सामान्यीकृत द्वारा आकारित (Morphism) किया जा सकता है।

समूह समरूपता (Group Homomorphism) समूहों के मध्य का मानचित्र है जो समूह संक्रिया (Group Operation) को परिरक्षित करता है। इसका तात्पर्य यह है कि समूह समरूपता में दूसरे समूह के तत्समक अवयव से प्रथम समूह के तत्समक अवयव को मानचित्रित किया जाता है तथा प्रथम समूह के अवयव के व्युत्क्रम (Inverse) को इस अवयव की प्रतिबिंब के व्युत्क्रम पर मानचित्रित किया जाता है। इस प्रकार समूहों के मध्य अर्द्ध समूह समरूपता आवश्यकरूपेण समूह समरूपता होता है।

समरूपता के प्रकार निम्नांकित हैं, जिन्हें साधारण आकारिता (Morphism) के लिये भी परिभाषित किया जाता है।

तुल्याकारिता: समान प्रकार की बीजगणितीय संरचनाओं (Algebraic Structures) के मध्य तुल्याकारिता (Isomorphism) को सामान्यतया द्विभाजित समरूपता के रूप में परिभाषित किया जाता है।

अंतराकारिता: यह ऐसी समरूपता है जिसका डोमैन, कोडोमैन (Codomain) के समतुल्य होता है अथवा अधिक साधारण रूप में यह एक आकारिता है जिसका स्रोत लक्ष्य (Target) के समतुल्य है। बीजगणितीय संरचना के अथवा वर्ग का प्रयोजन के अंतराकारिता से संरचना के अधीन एकाभ (Monoid) का निर्माण होता है।

स्वाकारिता: यह एक ऐसी अंतराकारिता (Endomorphism) है, जो कि एक तुल्याकारिता भी है। बीजगणितीय संरचना अथवा वर्ग की संरचना (Composition) स्वाकारिता के अधीन समूह का निर्माण होता है जिसे कि संरचना का स्वाकारिता समूह कहा जाता है।

एकाकृतिकता: बीजगणितीय संरचनाओं के लिये एकाकृतिकता (Monomorphism) को सामान्यतः अंतः क्षेत्रण समरूपता के रूप में परिभाषित किया जाता है। श्रेणी सिद्धांत के अधिक व्यापक परिदृश्य में एकाकृतिकता को ऐसे आकारिता के रूप में परिभाषित किया जाता है जो कि रद्द करने से छूट गया था।

समूहों के समरूपता की सार्वत्रिक बीजगणितीय (Universal Algebraic) परिभाषा के अनुसार– "समूहों के मध्य मानचित्र के समरूपता होने के लिये यह जाँच पर्याप्त है कि इसमें द्विआधारी संरचना (Binary Composition) को परिरक्षित किया जा रहा है"।

तुल्याकारिता को बीजगणितीय प्रणालियों में 'परोक्ष' समता (Indirect Equality) भी कहा जा सकता है। वस्तुतः यदि दो प्रणालियों में समान संख्या के अवयवों हों एवं इनका व्यवहार बिल्कुल समान प्रकार का हो तो उन्हें समतुल्य कहने में क्या आपत्ति हो! भले ही समता का विचार कभी–कभी कुछ असहज लग सकता है, विशेषतया अपरिमित समुच्चयों के प्रकरण में।

परिभाषा: माना $< G, * >$ व $< G', o >$ से दो समूह हैं।

मानचित्रण $f: G \to G'$ को समरूपता कहा जाता है यदि,

$$f(a * b) = f(a)\ o\ f(b) \quad a, b \in G$$

टिप्पणी

जब असमंजस की सम्भावना न हो तो हम दोनों द्विआधारी संरचना (Binary Composition) के लिये '.' इसी एक प्रतीक का प्रयोग करेंगे।

उसे संकेतन के रूप में अपनाकर हम मानचित्र प्राप्त करेंगे

$f: G \to G'$ एक समरूपता है।

यदि $f(ab) = f(a)f(b)$

यदि योग में f एक–एक (One-One) आच्छादक (Onto) हो तो हम कहते हैं कि f एक तुल्याकारिता (Isomorphism) है एवं इस प्रकरण में $G \cong G'$ लिखते हैं।

अब यह भी स्पष्ट है कि,

$$f(a_1a_2 \ldots\ldots a_n) = f(a_1)f(a_2) \ldots\ldots f(a_n)$$

यह तुल्याकारिता (समरूपता) के अधीन है।

होमोमॉर्फ़िज़्म के आच्छादक (Onto) होने को आच्छादक समकारिता (Epimorphism) कहा जाता है।

एक–एक (One-One) समरूपता को एकाकृतिकता (Monomorphism) कहते हैं।

समूह G से समरूपता स्वयं G का अंतराकारिता (Endomorphism) कहलाता है।

समूह G से तुल्याकारिता को स्वयं G का स्वाकारिता (Automorphism) कहा जाता है।

यदि $f: G \to G'$ आच्छादक समरूपता हो तो G' को समरूपता प्रतिबिंब कहा जाता है।

उदाहरण 3.1: माना $< \mathbf{Z}, + >$ व $< \mathbf{E}, + >$ को पूर्णांकों व सम पूर्णांकों के समूह मानें तो मानचित्र (Map) $f: \mathbf{Z} \to \mathbf{E}$, को इस प्रकार परिभाषित करें कि,

$$\text{समी } x \in \mathbf{Z} \text{ के लिए } f(x) = 2x$$

अब f इस प्रकार सुपरिभाषित है. $x = y \Rightarrow 2x = 2y \Rightarrow f(x) = f(y)$

पदों को पीछे लेते हुए f, 1–1 स्पष्ट है।

f समरूपता इस रूप में है।

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$$

f भी आच्छादक है, क्योंकि किसी सम पूर्णांक $2x$ में x इसकी पूर्व–प्रतिबिंब के रूप में होगा।

इसी कारण f एक तुल्याकारिक है।

वस्तुतः इस उदाहरण में प्रदर्शित होता है कि उपसमूह अपने मूल समूह से तुल्याकारिक हो सकता है।

उदाहरण 3.2: गुणन के अधीन समूह $< \mathbf{Z}, + >$ में पूर्णांकों के समूह $G = \{1, -1\}$ से मानचित्रण (Mapping) f को मानें जिसे इस प्रकार परिभाषित किया गया है $f: \mathbf{Z} \to G$, इस प्रकार कि, $f(x) = 1$ यदि x सम हो।

टिप्पणी

$= -1$ यदि x विषम हो।

अब f स्पष्टतः सुपरिभाषित है। हम परखते हैं कि यह समरूप है कि नहीं।

$x, y \in \mathbf{Z}$ को कोई अवयव मानें।

प्रकरण (*i*): x, y ये दोनों सम हैं तो $x + y$ सम है एवं इस प्रकार,

$$f(x + y) = 1, f(x) = 1, f(y) = 1$$

हम देखते हैं कि $f(x + y) = 1 = 1.1 = f(x) \cdot f(y)$

प्रकरण (*ii*): x, y ये दोनों विषम हैं तो $x + y$ सम है तथा

$$f(x + y) = +1 = (-1)(-1) = f(x) f(y)$$

प्रकरण (*iii*): x विषम है, y सम है तो $x + y$ विषम है एवं

$$f(x + y) = -1 = (-1)\ (1) = f(x) f(y)$$

इस प्रकार समस्त प्रकरणों में $f(x + y) = f(x) f(y)$.

यह दर्शा हो रहा है कि इस प्रकार f समरूप है। क्या यह तुल्याकारिता है?

आच्छादक से स्पष्ट है परन्तु f, 1–1 (एक–एक) नहीं है क्योंकि यह आवश्यक नहीं कि $x = y$ का तात्पर्य $f(x) = f(y)$ हो। वस्तुतः $f(2) = f(4)$ किन्तु $2 \neq 4$।

उदाहरण 3.3: $\mathbf{R}^+$ को गुणन के अधीन धनात्मक वास्तविक संख्याओं का समूह मानें एवं $\mathbf{R}$ को योग के अधीन समस्त वास्तविक संख्याओं का समूह हो तो मानचित्र

$\theta : \mathbf{R}^+ \to \mathbf{R}$ इस प्रकार होगा,

$\theta(x) = \log x$

यह एक तुल्याकारिता है।

θ स्पष्टतया सुपरिभाषित है।

$$\theta(x) = \theta(y)$$
$$\Rightarrow \log x = \log y$$
$$\Rightarrow e^{\log x} = e^{\log y}$$
$$\Rightarrow x = y$$

यह दर्शा रहा होता है कि θ एक–एक (One-One) है।

चूँकि $\theta(xy) = \log xy = \log x + \log y = \theta(x) + \theta(y)$

हम पाते हैं कि θ समरूप है।

अन्ततः यदि $y \in \mathbf{R}$ कोई सदस्य हो तो चूँकि $e^y \in \mathbf{R}^+$ व $\theta(e^y) = y$, हम इस निष्कर्ष पर पहुँचते हैं कि θ आच्छादक है तथा इसी कारण तुल्याकारिता पर है।

(मानचित्र $f: \mathbf{R} \to \mathbf{R}^+$, इस प्रकार है कि $f(a) = e^a$ का भी विचार किया जा सकता है)

उदाहरण 3.4: G कोई समूह हो व G का एक सामान्य उपसमूह N हो तो मानचित्र

$f : G \to \frac{G}{N}$ इस प्रकार परिभाषित करें कि,

$f(x) = Nx, \ x \in G$

टिप्पणी

अब f स्पष्टतया सुपरिभाषित है।

पुनः $f(xy) = Nxy = NxNy = f(x)\,f(y)$

इससे प्रदर्शित होता है कि f एक समरूप है।

इसे कभी–कभी प्राकृतिक (अथवा प्रामाणिक (Canonical)) समरूपता कहा जाता है। वह f आच्छादक है, किसी टिप्पणी की आवश्यकता कम है।

समूहों में तुल्याकारिता का सम्बन्ध समतुल्यता सम्बन्ध होता है। इस प्रकार जब भी समूह G अन्य समूह G' से तुल्याकारिक (Isomorphic) हो तो G, G' से तुल्याकारिक होगा। अतः हम यही कहेंगे कि G व G' तुल्याकारिक हैं एवं इसे $G \cong G'$ से इंगित करेंगे।

जिन प्रमेयों व परिभाषाओं का हम अनुसरण करते हैं उनमें से अधिकांश में हम समूहों के लिये G, G', इत्यादि, का प्रयोग करेंगे।

प्रमेय 3.1: यदि $f: G \to G'$ एक समरूप हो तो,

(i) $f(e) = e'$

(ii) $f(x^{-1}) = (f(x))^{-1}$

(iii) $f(x^n) = [f(x)]^n$, n एक पूर्णांक है।

जहाँ e, e' क्रमशः G व G' के तत्समक अवयव (Identity Element) हैं।

प्रमाण (i) : दिया है,

$$e \,.\, e = e$$
$$\Rightarrow f(e \,.\, e) = f(e)$$
$$\Rightarrow f(e) \,.\, f(e) = f(e)$$
$$\Rightarrow f(e) \,.\, f(e) = f(e) \,.\, e'$$
$$\Rightarrow f(e) = e' \quad \text{(निष्कासन)}$$

(ii) पुनः $xx^{-1} = e = x^{-1}x$

$$\Rightarrow f(xx^{-1}) = f(e) = f(x^{-1}x)$$
$$\Rightarrow f(x)\,f(x^{-1}) = e' = f(x^{-1})\,f(x)$$
$$\Rightarrow (f(x))^{-1} = f(x^{-1}).$$

(iii) यदि n धनात्मक पूर्णांक हो,

$$f(x^n) = \underset{(n \text{ बार})}{f(x \,.\, x \,.....x)}$$
$$= f(x) \,.\, f(x) \,..... f(x) \quad (n \text{ बार})$$
$$= (f(x))^n.$$

यदि $n = 0$, हमारे पास पद (i) अनुरूप परिणाम है। जिस प्रकरण में n ऋणात्मक पूर्णांक हो तो परिणाम के लिये पद (ii) का प्रयोग करते हैं।

उदाहरण 3.5: दर्शायें कि $< \mathbf{Q}, + > < \mathbf{Q}^*, \cdot >$, से तुल्याकारिता नहीं हो सकता जहाँ $\mathbf{Q}^* = \mathbf{Q} - \{0\}$ व $\mathbf{Q}$ परिमेय (Rationals) है।

हल: मान लेते हैं कि $\mathbf{Q}$ से $\mathbf{Q}^*$ तक f तुल्याकारिक है तो चूँकि $2 \in \mathbf{Q}^*$, f आच्छादक है, और $\exists\ \alpha \in < \mathbf{Q}, + >$, इस प्रकार होगा कि $f(\alpha) = 2$.

टिप्पणी

$$\Rightarrow \quad f\left(\frac{\alpha}{2}+\frac{\alpha}{2}\right)=2$$

अथवा $f\left(\frac{\alpha}{2}\right)f\left(\frac{\alpha}{2}\right)=2$

$$\Rightarrow \quad x^2=2 \quad \text{जहां } x=f\left(\frac{\alpha}{2}\right)\in \mathbf{Q}^*$$

किन्तु यह एक विरोधाभास है क्योंकि यहाँ परिमेय संख्या x इस प्रकार नहीं है कि $x^2=2$ इसी कारण यह परिणाम सामने आता है।

उदाहरण 3.6: $\frac{\mathbf{Z}}{4\mathbf{Z}}$ से $\frac{\mathbf{Z}}{6\mathbf{Z}}$ तक समस्त समरूपक ज्ञात करें।

हल: $f:\frac{\mathbf{Z}}{4\mathbf{Z}}\to\frac{\mathbf{Z}}{6\mathbf{Z}}$ को समरूपक मानें तो $f(4\mathbf{Z}+n)=nf(4\mathbf{Z}+1)$

अतः f पूर्णतया ज्ञात होगा यदि $f(4\mathbf{Z}+1)$ ज्ञात हो।

अब $(4\mathbf{Z}+1)$ की कोटि (Order) 4 है एवं इसलिये यह $o(f(4\mathbf{Z}+1))4$ को भागित करता है। (उदाहरण 3.7 देखें)

$o(f(4\mathbf{Z}+1))$ से 6 विभाजित होता है एवं इस प्रकार $o(f(4\mathbf{Z}+1))=1$ या 2

यदि $o(f(4\mathbf{Z}+1))=1,$ तो $f(4\mathbf{Z}+1)=6\mathbf{Z}=$ का शून्य $\frac{\mathbf{Z}}{6\mathbf{Z}}$

इसी कारण $f(4\mathbf{Z}+n)=$ शून्य

यदि $o(f(4\mathbf{Z}+1))=2,$ तो $f(4\mathbf{Z}+1)=6\mathbf{Z}+3$

$$\Rightarrow \quad f(4\mathbf{Z}+n)=6\mathbf{Z}+3n$$

जैसे $f(4\mathbf{Z}+n+4\mathbf{Z}+m) = f(4\mathbf{Z}+n+m)$

$$= 6\mathbf{Z}+3(n+m)$$
$$= (6\mathbf{Z}+3n)+(6\mathbf{Z}+3m)$$
$$= f(4\mathbf{Z}+n)+f(4\mathbf{Z}+m)$$

इस प्रकार f के लिये दो विकल्प हैं एवं इसे इस प्रकार परिभाषित किया जा सकता है कि $f:\frac{\mathbf{Z}}{4\mathbf{Z}}\to\frac{\mathbf{Z}}{6\mathbf{Z}}$ इस प्रकार हो $f(4\mathbf{Z}+n)=6\mathbf{Z}+3n$

ध्यान दे: $4\mathbf{Z}+n = 4\mathbf{Z}+m$

$$\Rightarrow n-m\in 4\mathbf{Z}$$
$$\Rightarrow 3(n-m)\in 12\mathbf{Z}\subseteq 6\mathbf{Z}$$
$$\Rightarrow 3(n-m)\in 6\mathbf{Z}$$
$$\Rightarrow 6\mathbf{Z}+3n\in 6\mathbf{Z}+3m$$

अर्थात् f सुपरिभाषित है।

अतः दो समरूपक $\frac{\mathbf{Z}}{4\mathbf{Z}}\to\frac{\mathbf{Z}}{6\mathbf{Z}}$ हैं। वस्तुतः d से $\frac{\mathbf{Z}}{m\mathbf{Z}}\to\frac{\mathbf{Z}}{n\mathbf{Z}}$ साधारणतया समरूपक हैं जहाँ d सबसे बड़ा सामान्य भाजक (m, n) हैं।

टिप्पणी

परिभाषा: माना $f: G \to G'$ समरूपक है। f का **आधारभूत** (Kernel) (जिसे $Ker\, f$ द्वारा इंगित किया जाता है) इस प्रकार परिभाषित किया जाता है,

$$\text{Ker}\, f = \{x \in G \mid f(x) = e'\}$$

जहाँ e' तत्समक G' की है।

प्रमेय 3.2: यदि $f: G \to G'$ समरूपक हो तो $\text{Ker}\, f$, G का एक सामान्य उपसमूह है।

प्रमाण: चूँकि $f(e) = e', e \in \text{Ker}\, f$, इस प्रकार $f \neq \varphi$।

पुनः $x, y \in \text{Ker}\, f \Rightarrow f(x) = e'$

$f(y) = e'$

अब $f(xy^{-1}) = f(x) f(y^{-1}) = f(x)(f(y))^{-1} = e' \,.\, e'^{-1} = e'$

$\Rightarrow xy^{-1}$ Ker f

इसी कारण यह G का उपसमूह है।

पुनः, किसी $\in G, x \in \text{Ker}\, f$ के लिये

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

$= (f(g))^{-1} f(x)\, f(g) = (f(g))^{-1}\, e'\, f(g)$

$= (f(g))^{-1} f(g) = e'$

$\Rightarrow g^{-1}xg \in \text{Ker}\, f$....

अथवा यह G का सामान्य उपसमूह है।

प्रमेय 3.3: समरूपक $f: G \to G'$ एक–एक (One-One या 1–1) है। यदि $\text{Ker}\, f = \{e\}$

प्रमाण: माना $f: G \to G'$ को एक–एक मानें। माना $x \in \text{Ker}\, f$ कोई अवयव हो तो,

$f(x) = e'$ और जैसे $f(e) = e'$

$f(x) = f(e) \Rightarrow x = e$ जैसे f, 1-1 है।

इसी कारण $\text{Ker}\, f = \{e\}$.

इसके विपरीत माना $\text{Ker}\, f$ में एकमात्र तत्समक अवयव अंतर्विष्ट है।

मानें $f(x) = f(y)$

तो $f(x)\,(f(y))^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \text{Ker}\, f = \{e\}$

$\Rightarrow xy^{-1} = e$

$\Rightarrow x = y$

अथवा f (1–1) है।

उदाहरण 3.7: यदि $f: G \to G'$ को समरूपक मानें तो $a \in G$ इस प्रकार हो कि $o(a) = n$ और $o(f(a)) = m$। दर्शायें कि $o(f(a)) \mid o(a)$ व f, 1-1 है, यदि $m = n$।

हल: चूँकि $o(a) = n$,

हम पाते हैं $a^n = e \Rightarrow f(a^n) = f(e)$

$\Rightarrow f(a\,.\,a\,.....\,a) = f(e)$

$\Rightarrow (f(a))^n = e'$

$\Rightarrow o(f(a)) \mid n = o(a)$

टिप्पणी

पुनः, f को 1–1 मानें.

चूंकि $o(f(a)) = m$

हम पाते हैं $(f(a))^m = e'$

$\Rightarrow f(a)\,.\,f(a)\,.....\,f(a) = e'$

$\Rightarrow f(a\,.\,a\,.....\,a) = e'$

$\Rightarrow f(a^m) = e' = f(e)$

$\Rightarrow a^m = e \quad (f,\ 1\text{–}1)$

अर्थात, $o(a) \mid m$ या $n \mid m$, लेकिन यह पता है कि $m \mid n$ है।

इसी कारण से $m = n$.

इसके विपरीत मानें कि $o(a) = o(f(a))$.

तो $f(x) = f(y)$

$\Rightarrow f(x)\,(f(y))^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow o(f(xy^{-1})) = 1$

$\Rightarrow o\,(xy^{-1}) = 1 \ \Rightarrow xy^{-1} = e \ \Rightarrow x = y$

$\Rightarrow f,$ 1-1 है।

टिप्पणी: समरूपता के अधीन किसी अवयव की कोटि परिरक्षित (Preserved) रहती है।

उदाहरण 3.8: दर्शायें कि वास्तविक संख्याओं का समूह $<\mathbf{R}, +>$ गुणन के अधीन अशून्य (Nonzero) वास्तविक संख्याओं के समूह R^* से तुल्यकारिक नहीं हो सकता।

हल: $-1 \in R^*$ एवं -1 की कोटि 2 है, $(-1)^2 = 1$ अनुरूप परन्तु $\mathbf{R}$ में कोटि 2 का अवयव नहीं है। चूँकि यदि $x \in \mathbf{R}$ कोटि 2 का हो तो $2x = x + x = 0$, किन्तु यह किसी x के लिये $<\mathbf{R}, +>$ में नहीं है, $x = 0$ के अतिरिक्त।

उपरोक्त टिप्पणी में तुल्याकारिता के अधीन अवयव की कोटि परिरक्षित रहती है, इस प्रकार $<\mathbf{R}$, व $\mathbf{R}^*$ के मध्य कोई तुल्याकारिता नहीं हो सकती हैं।

उदाहरण 3.9: दर्शायें कि $<\mathbf{Q}, +>$ का प्रत्येक अशून्य समरूपता स्वयं में एक स्वाकारिता (Automorphism) है।

हल: माना $\theta : \mathbf{Q} \to \mathbf{Q}$, को कोई अशून्य समरूपता मानें। हम सर्वप्रथम दर्शाते हैं कि

$$q\left(\frac{m}{n}\right) = \frac{m}{n} q\,(1) \text{ किसी } \frac{m}{n} \in \mathbf{Q} \text{ के लिए।}$$

मान लेते हैं कि $\theta\,(1) = p/q$

तो $$\frac{\mathrm{p}}{\mathrm{q}} = \mathrm{q}(1) = \theta\left(\frac{\mathrm{n}}{\mathrm{n}}\right) = \mathrm{q}\left(\frac{1}{\mathrm{n}} + \frac{1}{\mathrm{n}} + \cdots + \frac{1}{\mathrm{n}}\right) = \mathrm{nq}\left(\frac{1}{\mathrm{n}}\right)$$

टिप्पणी

इस प्रकार $q\left(\frac{1}{n}\right)=\frac{1}{n}q(1)$

अतः $\theta\left(\frac{m}{n}\right)=q\left(\frac{1}{n}+\frac{1}{n}+\cdots+\frac{1}{n}\right)=mq\left(\frac{1}{n}\right)=\frac{m}{n}q(1)$

अब हम दर्शाते हैं कि θ, 1–1 आच्छादक है।

माना $\frac{m}{n}\in \text{Ker}\,\theta$ कोई अवयव हो तो,

$$\theta\left(\frac{\text{m}}{\text{n}}\right)=0\Rightarrow\left(\frac{\text{m}}{\text{n}}\right)\theta(1)=0\Rightarrow\frac{\text{m}}{\text{n}}=0 \quad \text{या} \quad \theta(1)=0$$

यदि $\theta(1)=0$, तो $\theta\left(\frac{1}{n}\right)=0$ एवं $\theta(\text{m})=\text{m}\theta(1)=0,\ \forall\ m,n,n\neq 0$

$$\Rightarrow \text{q}\left(\frac{m}{n}\right)=0 \quad \forall m,n,n\neq 0$$

अथवा θ शून्य समरूपक है जब कि वास्तव में नहीं है।

इसी कारण $\frac{m}{n}=0\Rightarrow \text{Ker}\,q=\{0\}$

$\Rightarrow$ θ , 1–1 है।

पुनः यदि $\frac{m}{n}\in\mathbf{Q}$ कोई अवयव अब इस प्रकार हो,

$$q\left(\frac{m}{n}\cdot\frac{q}{p}\right)=\frac{mq}{np}q(1)=\frac{m}{n}$$

हम इस निष्कर्ष पर आते हैं कि θ आच्छादक (Onto) है एवं इसी कारण एक स्वाकारिता है।

उदाहरण 3.10: माना G एक समूह हो एवं $f: G\to G$ इस प्रकार हो कि $f(x)=x^{-1}$ समरूपक हो। प्रदर्शित करें कि G एबेलियन (Abelian) है।

हल: माना $x, y\in G$ कोई भी अवयव हों।

$$\begin{aligned} xy &= (y^{-1}x^{-1})^{-1} = f(y^{-1}x^{-1}) \\ &= f(y^{-1})\,f(x^{-1}) \\ &= yx, \end{aligned}$$

इसी कारण G एबेलियन है।

प्रमेय 3.4: (समूह समरूपता का आधारभूत प्रमेय Fundamental Theorem of Group Homomorphism)। यदि $f: G\to G'$ $K=\text{Ker}\,f$, युक्त आच्छादक समरूपक हो तो $\frac{G}{K}\cong G'$।

अन्य शब्दों में समूह G की प्रत्येक समरूपक प्रतिबिंब G के भागफल समूह (Quotient Group) से तुल्याकारिक है।

टिप्पणी

प्रमाण: मानचित्र $\varphi : \frac{G}{K} \to G'$, इस प्रकार परिभाषित करें कि,

$$\varphi(Ka) = f(a), \quad a \in G$$

हम दर्शाते हैं कि φ तुल्याकारिक है।

φ निम्नानुसार सुपरिभाषित है,

$$\begin{aligned} & Ka = Kb \\ \Rightarrow\ & ab^{-1} \in K = \text{Ker}\, f \\ \Rightarrow\ & f(ab^{-1}) = e' \\ \Rightarrow\ & f(a)(f(b))^{-1} = e' \\ \Rightarrow\ & f(a) = f(b) \\ \Rightarrow\ & \varphi(Ka) = \varphi(Kb) \end{aligned}$$

पदों को फिर से दोहराते हुए हम सिद्ध करेंगे कि φ, 1–1 है।

पुनः $\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a) f(b)$

$$= \varphi(Ka)\ \varphi(Kb)$$

φ के रूप में हम पाते हैं कि φ समरूपक (Homomorphism) है।

φ आच्छादक है अथवा नहीं, इसे परखने के लिये हम मान लेते हैं कि $g' \in G'$ का कोई अवयव हैं। चूँकि $f : G \to G'$ आच्छादक इस प्रकार है कि $\exists\, g \in G$,

अब,

$$f(g) = g'$$
$$\varphi(Kg) = f(g) = g'$$

इसके द्वारा दर्शाया जा रहा है कि Kg', g' के अधीन φ की आवश्यक पूर्व प्रतिबिंब है।

इसी कारण φ तुल्याकारिक है।

टिप्पणी: उपरोक्त प्रमेय को तुल्याकारिता का प्रथम प्रमेय (First Theorem of Isomorphism) भी कहा जाता है। इसे इस प्रकार भी कहा जा सकता है कि यदि f: $G \to G'$ $K = \text{Ker}\, f$, युक्त समरूपक हो, $\frac{G}{\text{Ker} f} \cong f(G)$.।

प्रमेय 3.5: (तुल्याकारिता का द्वितीय प्रमेय Second Theorem of Isomorphism)। H व K को समूह G के दो उपसमूह मानें जहाँ G में H सामान्य है तो,

$$\frac{HK}{H} \cong \frac{K}{H \cap K}$$

प्रमाण: यह सरलता से देख सकते हैं कि $H \cap K$, K का सामान्य उपसमूह होगा एवं चूंकि $H \subseteq HK \subseteq G$ है और H भी HK में सामान्य होगा।

मानचित्र $f : K \to \frac{HK}{H}$, को इस प्रकार परिभाषित करें कि,

$$f(k) = Hk$$

तो चूँकि $k_1 = k_2 \Rightarrow Hk_1 = Hk_2 \Rightarrow f(k_1) = f(k_2)$

टिप्पणी

अतः हम पाते हैं कि f सुपरिभाषित है।

पुनः $f(k_1k_2) = Hk_1k_2 = Hk_1Hk_2 = f(k_1)f(k_2)$

यह दर्शाता है कि f समरूपक है।

यहाँ f आच्छादक है जो स्पष्ट है एवं इस प्रकार आधारभूत प्रमेय (Fundamental Theorem) का प्रयोग करते हुए हम पाते हैं,

$$\frac{HK}{H} \cong \frac{K}{\text{Ker}\, f}$$

चूँकि $k \in \text{Ker}\, f \Leftrightarrow f(k) = H$

$\Leftrightarrow Hk = H$

$\Leftrightarrow k \in H$

$\Leftrightarrow k \in H \cap K \quad (k \in K$ क्योंकि $\text{Ker}\, f \subseteq K)$

हम पाते हैं, $\text{Ker}\, f = H \cap K$

अतः हमारा प्रमेय सिद्ध हुआ।

लैमा: यदि H व K समूह G के दो सामान्य उपसमूह इस प्रकार हैं कि $H \subseteq K$, तो $\frac{K}{H}$ $\frac{G}{H}$ का सामान्य उपसमूह है एवं इसके विपरीत।

प्रमाण: $\frac{K}{H}$ $\frac{G}{H}$ का गैर–रिक्त उप–समुच्चय है (परिभाषानुरूप)।

किसी $Hk_1, Hk_2 \in \frac{K}{H}$ के लिये

$$(Hk_1)(Hk_2)^{-1} = (Hk_1)(Hk_2^{-1}) = Hk_1k_2^{-1} \in \frac{K}{H}$$

अर्थात् $\frac{K}{H}$ एक उपसमूह है।

पुनः किसी $Hk \in \frac{K}{H}$ व $Hg \in \frac{G}{H}$, के लिये हमें ज्ञात हैं,

$$(Hg)^{-1}(Hk)(Hg) = Hg^{-1}HkHg$$

$$= Hg^{-1}kg \in \frac{K}{H}$$

चूँकि $g \in G, k \in K$, अतः K में G सामान्य है और इससे $g^{-1}kg \in K$ मिलता है।

प्रमेय 3.6: (तुल्याकारिता का तृतीय प्रमेय (Third Theorem of Isomorphism))। यदि H व K, G के दो उपसमूह इस प्रकार हों कि $H \subseteq K$, तो,

$$\frac{G}{K} \cong \frac{G/H}{K/H}$$

प्रमाण: उपरोक्त लैमा से सुनिश्चित होता है कि $\frac{K}{H}$ $\frac{G}{H}$ का सामान्य उपसमूह है एवं इसीलिये, हम $\frac{G/H}{K/H}$ की बात कर सकते हैं।

मानचित्र $f : \frac{G}{H} \to \frac{G}{K}$ को इस प्रकार परिभाषित करें कि,

$$f(Ha) = Ka, \quad a \in G$$

टिप्पणी

f उचित रूप से सुपरिभाषित है।

$$\begin{aligned} & Ha = Hb \\ \Rightarrow \quad & ab^{-1} \in H \subseteq K \\ \Rightarrow \quad & Ka = Kb \\ \Rightarrow \quad & f(Ha) = f(Hb) \end{aligned}$$

f समरूपक है, क्योंकि

$$f(HaHb) = f(Hab) = Kab = KaKb = f(Ha)\, f(Hb)$$

f की आच्छादिकता (Ontoness) स्पष्ट है।

समूह समरूपता के आधारभूत प्रमेय का प्रयोग करते हुए हम कह सकते हैं,

$$\frac{G}{K} \cong \frac{G/H}{\text{Ker } f}$$

हम $\text{Ker}\, f = \frac{K}{H}$ का दावा कर सकते हैं।

$\text{Ker}\, f$ का सदस्य $\frac{G}{H}$ का कोई सदस्य होगा।

अब $\quad Ha \in \text{Ker}\, f \quad \Leftrightarrow f(Ha) = K$ (G/K का तत्समक)

$$\begin{aligned} & \Leftrightarrow Ka = K \\ & \Leftrightarrow a \in K \\ & \Leftrightarrow Ha \in \frac{K}{H} \end{aligned}$$

इसी कारण हम पाते हैं, $\quad \frac{G}{K} \cong \frac{G/H}{K/H}$

जिससे हमारा परिणाम सिद्ध होता है। इसे **फ्रॅश्मेन प्रमेय (Freshman's Theorem)** भी कहा जाता है।

टिप्पणी: चूँकि $\frac{K}{H} = \text{Ker}\, f$, हम देखते हैं कि $\frac{K}{H}$ $\frac{G}{H}$ का सामान्य उपसमूह है, एवं इसी कारण हम $\frac{G/H}{K/H}$ की बात कर सकते हैं। इस प्रकार हमें पृथक् या अलग से यह सिद्ध करने की आवश्यकता नहीं है कि $\frac{K}{H}$, $\frac{G}{H}$ का सामान्य उपसमूह है।

प्रमेय 3.7: माना कि $f : G \to G'$ एक आच्छादक समरूपक है। $\text{Ker}\, f = K$ G' के उपसमूह H' के लिये निम्न को परिभाषित करें :

$$H = \{x \in G \mid f(x) \in H'\}$$

तब,

(*i*) G, H का उपसमूह है एवं $K \subseteq H$

(*ii*) G' का H' का सामान्य उपसमूह है यदि G में H सामान्य हो

(*iii*) यदि G' में H' सामान्य हो तो $\frac{G'}{H'} \cong \frac{G}{H}$

टिप्पणी

(*iv*) यह संबद्ध (Association) G के सभी उपसमूहों की श्रेणी (Family) S के G के सभी उपसमूहों की श्रेणी (Family) S से मानचित्रण पर एक–एक आच्छादक (One-One Onto) है, जिसमें K होता है।

प्रमाणः (*i*) $H \neq \varphi$ चूंकि $f(e) = e' \in H'$ जो दर्शाता है कि $e \in H$

पुनः, $x, y \in H \Rightarrow f(x), f(y) \in H'$

$\Rightarrow f(x)(f(y))^{-1} \in H'.$

$\Rightarrow f(xy^{-1}) \in H' \Rightarrow xy^{-1} \in H$

इस प्रकार H एक उपसमूह है।

चूँकि $x \in \text{Ker}\, f = K \Rightarrow f(x) = e' \in H'$

हम पाते हैं $x \in H \Rightarrow K \subseteq H.$

(*ii*) H को G में सामान्य मानें।

माना कि $g' \in G', h' \in H'$ कोई भी अवयव है। चूँकि f आच्छादक $\exists\, g \in G$, $h \in G$ है, इस प्रकार है कि $f(g) = g', f(h) = h'$। क्योंकि $h' \in H, h \in H$

अब,

$g'^{-1} h'g' = (f(g))^{-1} f(h) f(g)$

$= f(g^{-1}) f(h) f(g) = f(g^{-1}hg) \in H'$

चूँकि $g \in G, h \in H,$ जहाँ H, G में सामान्य है, जिसका तात्पर्य है कि $g^{-1}hg \in H$

इस प्रकार G' में H' सामान्य है।

इसके विपरीत H' को G' में सामान्य मानें।

किन्हीं अवयवों $h \in H$ तथा $g \in G$ के लिये,

$f(g^{-1} hg) = (f(g))^{-1} f(h) f(g) \in H'$

क्योंकि $f(h) \in H', f(g) \in G',$ तथा H' G' में सामान्य है

$\Rightarrow$ $g^{-1}hg \in H$ अथवा G में H सामान्य है।

(*iii*) मानचित्रण $\varphi : G \to \frac{G'}{H'}$ को इस प्रकार परिभाषित करें कि,

$$\varphi(g) = H' f(g)$$

तो φ $g_1 = g_2$ के रूप में सुपरिभाषित है,

$\Rightarrow f(g_1) = f(g_2)$

$\Rightarrow H' f(g_1) = H' f(g_2)$

$\Rightarrow \varphi(g_1) = \varphi(g_2)$

टिप्पणी

φ इस प्रकार समरूपक होगा,

$\varphi(g_1g_2) = H'f(g_1g_2) = H'f(g_1)f(g_2) \quad = H'f(g_1)\,H'f(g_2)$

$= \varphi(g_1)\varphi(g_2)$

पुनः किसी $H'g' \in \dfrac{G'}{H'}$ के लिये चूँकि $g' \in G'$ व f आच्छादक $\exists\, g \in G$ है, इस प्रकार कि $f(g) = g'$.

अथवा $\varphi(g) = H'f(g) = H'g'$ जो दर्शाता है कि φ आच्छादक है।

आधारभूत प्रमेय के प्रयोग से अब,

$$\frac{G'}{H'} \cong \frac{G}{\text{Ker } \varphi}$$

अब $x \in \text{Ker } \varphi \quad \Leftrightarrow \varphi(x) = H'$

$\Leftrightarrow H'f(x) = H'$

$\Leftrightarrow f(x) \in H' \Leftrightarrow x \in H$

इसी कारण $\text{Ker } \varphi = H$

(*iv*) **मानचित्रण $\psi : S' \to S$**, को इस प्रकार परिभाषित करें कि,

$$\psi(H') = H$$

जहाँ पद (*i*) अनुसार S' में H' किसी H' के लिये $\{x \in G \mid f(x) \in H'\}$ है।

हमें विदित है कि यह G का उपसमूह है, जिसमें K स्थित है तथा इस प्रकार S का सदस्य (Member) ψ है। इसीलिये मानचित्रण सुपरिभाषित हुई।

अब $\psi(H') = \psi(T')$ जहाँ $H', T' \in S'$ जहाँ

अब, $H = T$ मान लें,

जहां $H = \{x \in G \mid f(x) \in H'\}$

$T = \{x \in G \mid f(x) \in T'\}$

अब किसी $h' \in H' \subseteq G'$, के लिये चूँकि $f: G \to G'$ आच्छादक है, हम ज्ञात कर सकते हैं कि $h \in G$, इस प्रकार कि $f(h) = h' \in H'$ है।

परन्तु यह दर्शाता है कि $h \in H = T$

$\Rightarrow f(h) \in T'$

$\Rightarrow h' \in T' \Rightarrow H' \subseteq T'$

इसी प्रकार $T' \subseteq H'$

अर्थात् $H' = T'$ अथवा ψ एक–एक है।

हम दर्शा सकते हैं कि अब ψ आच्छादक है।

माना कि $H \in S$ कोई सदस्य हैं तो H, G का उपसमूह है एवं $K \subseteq H$

हम मानते हैं कि $f(H) = \{f(h) \mid h \in H\}$

अब $f(H) \neq \varphi$ जैसे $e \in H \Rightarrow f(e) = e' \in f(H)$

पुनः किसी $f(h_1), f(h_2) \in f(H),\ h_1, h_2 \in H$ हेतु

टिप्पणी

एवं $(f(h_1))(f(h_2))^{-1} = f(h_1 h_2^{-1}) \in f(H)$

अर्थात् $f(H)\ G'$ का उपसमूह है।

हम दर्शाते हैं कि $f(H) = H'$ ψ के अधीन H का आवश्यक पूर्व प्रतिबिंब है।

अर्थात् हम दर्शाते हैं $\psi(H') = H$

अतः हमें यह दर्शाने की आवश्यकता है कि

$H = \{x \in G \mid f(x) \in H'\}$

माना कि $x \in H$ हो तो $f(x) \in f(H) = H'$

$$\Rightarrow x \in \{x \in G \mid f(x) \in H'\}$$

या तो $H \subseteq \{x \in G \mid f(x) \in H'\}$

पुनः, if $x \in \{x \in G \mid f(x) \in H'\}$

तो $f(x) \in H' = f(H)$

$\exists\ h \in H$, ऐसा है कि, $f(x) = f(h)$

$$\Rightarrow f(xh^{-1}) = e'$$

$$\Rightarrow xh^{-1} \in \text{Ker}\, f = K$$

$$\Rightarrow x \in Kh \subseteq H \quad [K \subseteq H]$$

इस प्रकार से $\{x \in G \mid f(x) \in H'\} \subseteq H$

इसी कारण $H = \{x \in G \mid f(x) \in H'\}$

अथवा $\psi(H') = H$ और ψ आच्छादक है।

जिससे प्रमाण पूर्ण हुआ।

निम्नांकित उदाहरण में हम उपरोक्त प्रमेय का सौम्य रूपान्तर (Milder Version) व उसके अनुप्रयोग को सिद्ध करते हैं।

उदाहरण 3.11: माना कि $f: G \to G'$ को समूह G से G' तक आच्छादक समरूपक है। यदि H, G का उपसमूह हो जो कि H', G' का उपसमूह है तो,

(*i*) $f(H)$, G का उपसमूह है।

(*ii*) $f^{-1}(H')$, G का उपसमूह है, $K = Ker\ f$, को सम्मिलित करते हुए, जहाँ $f^{-1}(H')$ के द्वारा $\{x \in G \mid f(x) \in H'\}$ औसत (Mean) है।

ध्यान दें: समुच्चय $f^{-1}(H')$ यहाँ इस प्रकार से परिभाषित है कि f में व्युत्क्रम है कि नहीं। संकेतन f^{-1} का प्रयोग यहाँ प्रतीकात्मक रूप से ही किया गया है।

हल: (*i*) चूँकि $e = H$ से सम्बद्ध G की तत्समक है।

दिया है, $f(e) \in f(H)$

$$\Rightarrow f(H) \neq \varphi.$$

माना, $x, y \in f(H) \Rightarrow x = f(h_1), y = f(h_2)$ जहां $h_1, h_2\ H.$

$$\therefore \quad xy^{-1} = f(h_1)\ (f(h_2))^{-1}$$

$$= f(h_1)\ (f(h_2^{-1})$$

$$= f(h_1 h_2^{-1}) \in f(H) \text{ जैसे } h_1, h_2 \in H \Rightarrow h_1 h_2^{-1} \in H$$

अतः $f(H)\ G'$ का उपसमूह है।

(*ii*) माना, $a, b \in f^{-1}(H')$

$\Rightarrow f(a), f(b) \in H'$

$\Rightarrow f(a)\ .\ f(b)^{-1} \in H'$

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

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

और $f(e) = e' = G' \in H'$ के तत्समक है।

$\Rightarrow\ e \in f^{-1}(H')$

$\Rightarrow f^{-1}(H') \neq \varphi$

तभी, $f^{-1}(H')$, G का उपसमूह है।

तथा $k \in K \Rightarrow f(k) = e' \in H$

$\Rightarrow\ k \in f^{-1}(H')$

$\Rightarrow\ K \subseteq f^{-1}(H')$

इससे पद (*ii*) सिद्ध हुआ।

उदाहरण 3.12: (*i*) माना कि $f: G \to G'$ समरूपक हो एवं मान लें कि $g \in G, f(g) = g'$ इस प्रकार हो कि $f^{-1}(g') = \{x \in G \mid f(g) = g'\}$। यदि ऐसा समुच्चय हो जिसमें f के अधीन g' की समस्त पूर्व प्रतिबिंब हों तो दर्शायें कि $f^{-1}(g') = Kg$ जहाँ $K = \text{Ker}\, f$.

(*ii*) यदि $f: U_{30} \to U_{30}$ समरूपता इस प्रकार हो कि $\text{Ker}\, f = \{1, 11\}$ एवं $f(7) = 7$ तो U_{30} के समस्त अवयव ज्ञात करें जिन्हें 7 तक मानचित्रित किया गया है। इसके विपरीत समरूपता $f: U_{30} \to U_{30}$ ज्ञात करें, इस प्रकार कि $\text{Ker}\, f = \{1, 11\}$ और $f(7) = 7$.

हल: (*i*) माना $x \in f^{-1}(g')$ कोई अवयव हो तो,

$f(x) = g' \Rightarrow f(x) = f(g)$

$\Rightarrow f(x)(f(g))^{-1} = e'$

$\Rightarrow f(xg^{-1}) = e'$

$\Rightarrow\ xg^{-1} \in \text{Ker}\, f = K$

$\Rightarrow\ x \in Kg \Rightarrow f^{-1}(g') \subseteq K$

पुनः माना $k \in K$ कोई अवयव हो तो,

$f(kg) = f(k)\, f(g) = e'g' = g'$

$\Rightarrow\ Kg \in f^{-1}(g')\quad \forall\ k \in K$

$\Rightarrow\ Kg \subseteq f^{-1}(g')$

तथा इसी प्रकार $f^{-1}(g') = Kg$

(*ii*) भाग (i) से, 7 की पूर्व प्रतिबिंब (Pre Image) का समुच्चय $K7$ हैं, जहां $K = \text{Ker}\, f = \{1, 11\}$

टिप्पणी

इस प्रकार 7 की पूर्व प्रतिबिंब का समुच्चय $K7 = \{1\otimes 7, 11\otimes 7\} = \{7, 17\}$ है।

इसके विपरीत माना $f: U_{30} \to U_{30}$ समरूपता इस प्रकार हो कि,

$$\text{Ker}\, f = \{1, 11\} \text{ और } f(7) = 7.$$

तो $$f(1) = 1, f(11) = 1, f(7) = 7$$

अब $7\otimes 11 = 17$.

$$f(7\otimes 11) = f(17) \Rightarrow f(17) = f(7)\otimes f(11) = 7\otimes 1 = 7$$

$$7\otimes 17 = 29 \Rightarrow f(29) = f(7)\otimes f(17) = 7\otimes 7 = 19$$

इसी प्रकार हम अन्य मानों को प्राप्त करते हैं,

$$f(13) = 13, f(19) = 19, f(23) = 13$$

टिप्पणी: पूर्ववर्ती समस्या में दिये गये अनुसार संकेतन f^{-1} प्रतीकमात्र है एवं इसका व्युत्क्रम होना आवश्यक नहीं हैं।

अपनी प्रगति जांचिए

1. समरूपता क्या है?
2. G के समरूपक प्रतिबिंब को आप कैसे परिभाषित करेंगे?
3. आधारभूत शब्द को परिभाषित करें।
4. तुल्याकारिता के द्वितीय प्रमेय की व्याख्या करें।

3.3 रूपांतरण एवं क्रमचय समूह

समुच्चय X का क्रमचय (Permutation) एक फलन $\sigma : X \to X$ इस प्रकार है जो कि एक–एक व आच्छादक है, अर्थात् द्विभाजित मानचित्र। क्रमचय के लिये यह आवश्यक है कि हमारे पास कितने विषय हैं, न कि विषयों का स्वरूप क्या है। उदाहरणार्थ हम n विषयों के समुच्चयों पर क्रमचय का विचार सदैव कर सकते हैं जहाँ विषयों को $\{1, \ldots, n\}$ सूचक (Label) द्वारा दर्शाते हैं। इसीलिये समुच्चय $X = \{1, 2, \ldots, n\}$ के समस्त क्रमचय से संरचना के अधीन समूह का निर्माण होता है। इस समूह को डिग्री n का सममित समूह (Symmetric Group) S_n कहा जाता है।

आधारभूत रूप से एकपक्षीय (Arbitary) समुच्चय X का क्रमचय X से स्वयं तक एकैक आच्छादन (Bijection) होता है।

प्रमेय 3.8 (केली प्रमेय) (Cayley's Theorem) : प्रत्येक समूह G क्रमचय समूह से तुल्याकारिक है।

प्रमाण: माना कि दिया गया समूह G है एवं $A(G)$ समुच्चय G के समस्त क्रमचयों का समूह हो।

किसी $a \in G$ के लिये मानचित्र $f_a : G \to G$, को इस प्रकार परिभाषित करें कि,

$$f_a(x) = ax$$

पुनः $x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$

टिप्पणी

अतः f_a सुपरिभाषित है।

पुनः, $f_a(x) = f_a(y)$

$\Rightarrow ax = ay$

$\Rightarrow x = y$ (समूह G में निष्कासन)

$\Rightarrow f_a$, 1–1 है।

किसी $y \in G$ के लिये चूंकि $f_a(a^{-1}y) = a(a^{-1}y) = y$ है। हम ज्ञात करते हैं कि पूर्व प्रतिबिंब y का है अथवा f_a आच्छादक है एवं इसी कारण G पर क्रमचय (Permutation) है।

इस प्रकार $f_a \in A(G)$

यदि K को समस्त ऐसे क्रमचय (Permutation) का समुच्चय मानें तो हम दर्शाते हैं कि K, $A(G)$ का उपसमूह है। $K \neq \varphi$ जैसे $f_e \in K$.

माना कि $f_a, f_b \in K$ कोई सदस्य हैं।

चूँकि $f_b \; o \; f_{b^{-1}}(x) = f_b(f_{b^{-1}}(x)) = f_b(b^{-1}x) = b(b^{-1}x)$

$= ex = f_e(x)$ सभी x के लिए।

हम प्राप्त करते हैं कि $f_{b^{-1}} = (f_b)^{-1}$ (ध्यान दें: $f_e = I$, $A(G)$ के तत्समक है)।

और क्योंकि $(f_a \; o \; f_b)\; x = f_a(bx) = a(bx) = (ab)x = f_{ab}(x)$ सभी x के लिए।

हम प्राप्त करते हैं $f_{ab} = f_a \; o \; f_b$

अब $f_a \; o \; (f_b)^{-1} = f_a \; o \; f_{b^{-1}} = f_{ab^{-1}} \in K$

यह दर्शाता है कि K, $A(G)$ का उपसमूह है।

अब मानचित्रण $\varphi : G \to K$ को इस प्रकार परिभाषित करें कि,

$$\varphi(a) = f_a$$

तो φ सुपरिभाषित है, 1–1 मानचित्र इस प्रकार है,

$a = b$

$\Leftrightarrow ax = bx$

$\Leftrightarrow f_a(x) = f_b(x) \quad \forall \; x$

$\Leftrightarrow f_a = f_b$

$\Leftrightarrow \varphi(a) = \varphi(b)$

φ स्पष्टतया आच्छादक है एवं चूँकि,

$$\varphi(ab) = f_{ab} = f_a \; o \; f_b = \varphi(a)\; \varphi(b)$$

φ समरूपता है एवं इसी कारण तुल्याकारिता भी है, जिससे हमारा अभिकथन (Assertion) सिद्ध हुआ।

ध्यान दें: K क्रमचय समूह का उपसमूह होने के नाते एक क्रमचय समूह है।

टिप्पणी: विशेषतया यदि G कोटि n का परिमित समूह हो तो G, S_n के उपसमूह से तुल्याकारिक है।

(ii) $\varphi : S_n \to A_{n+2}$ का मानचित्रण करें जहाँ $\varphi(+) = f$, जहाँ f सम व $\varphi(f) = f(n+1, n+2)$ हो जब f विषम हो तो समरूपता है। इस प्रकार की कोटि n का परिमित समूह A_{n+2} के उपसमूह का तुल्याकारिक है जो कि S_{n+2} के सम क्रमचय का उपसमूह है।

टिप्पणी

उदाहरण 3.13: केली प्रमेय का प्रयोग करते हुए उस क्रमचय समूह K को ज्ञात करें जो गुणन मापांक (Multiplication Modulo) 10 के अधीन समूह $G = \{2, 4, 6, 8\}$ के तुल्याकारिक है। (यहाँ 6 G की तत्समक है एवं $G = <2>$)।

हल: उपरोक्त केली प्रमेय के अनुसार समुच्चय K इस प्रकार परिभाषित है कि $K = \{f_a \mid a \in G\}$ जहाँ $f_a\, f_a(x) = ax$ द्वारा परिभाषित है। इस प्रकार यहाँ $a = 2, 4, 8, 6$ एवं,

$$f_2(2) = 4, \quad f_2(4) = 8, \quad f_2(8) = 6, \quad f_2(6) = 2$$
$$f_4(2) = 8, \quad f_4(4) = 6, \quad f_4(8) = 2, \quad f_4(6) = 4$$
$$f_8(2) = 6, \quad f_8(4) = 2, \quad f_8(8) = 4, \quad f_8(6) = 8$$
$$f_6(2) = 2, \quad f_6(4) = 4, \quad f_6(8) = 8, \quad f_6(6) = 6$$

इस प्रकार $f_6 = I$ और $K = \{f_2, f_4, f_8, f_6 = I\}$

यदि हम क्रमचय (1234) से f_2 की पहचान करें तो अन्य क्रमचय होंगे (13)(24), (1432) तथा इस प्रकार K {(1234), (13)(24), (1432), I} है एवं यह G का आवश्यक तुल्याकारिक क्रमचय समूह है।

वस्तुतः तुल्याकारिक को $\theta : G \to K$, के रूप में इस प्रकार देखा जा सकता है कि,

$$\theta\,(2) = (1234),\ \theta\,(4) = (13)(24),\ \theta\,(8) = (1432),\ \theta\,(6) = \mathrm{I}$$

प्रमेय 3.9: S_n में किसी क्रमचय f की कोटि लघुत्तम समापवर्त्य (L.C.M.) के असंबद्ध चक्रों की कोटि f के समतुल्य है।

प्रमाण: $f = f_1 f_2 \ldots\ldots f_n$ मानें।

प्रस्तुतीकरण असंबद्ध (Disjoint) चक्रों के गुणन के रूप में $f_1, f_2, \ldots\ldots, f_n$

माना कि $o(f_i) = r_i \quad i = 1, 2, \ldots\ldots, n$

अब $f_i^{r_i} = I$ (S_n के तत्समक)

r = L.C.M. $(r_1, r_2, \ldots\ldots, r_n)$

अब $f^r = (f_1 f_2 \ldots\ldots f_n)^r = f_1^r f_2^r \ldots\ldots f_n^r$ क्योंकि f_i असंबद्ध हैं एवं इसीलिये ये क्रमविनिमेय (Commutative) हैं।

चूँकि समस्त i के लिये $r_i \mid r$ हमारे पास है $r = r_i k_i, \quad i = 1, 2, \ldots\ldots, n$

इस प्रकार $f^r = f_1^{r_1 k_1} f_2^{r_2 k_2} \ldots\ldots f_n^{r_n k_n} = I \,.\, I \ldots\ldots I = I$

मान लें कि $f^t = I$

$$\Rightarrow (f_1 f_2 \ldots\ldots f_n)^t = I$$
$$\Rightarrow f_1^t f_2^t \ldots\ldots f_n^t = I$$
$$\Rightarrow f_1^t = f_2^t = \ldots\ldots = f_n^t = I$$

चूँकि $f_1, f_2, \ldots\ldots, f_n$ असंबद्ध हैं।

(**ध्यान दे**– यदि कोई $f_i \neq I$ तो बायें हाथ में, I नहीं हो सकता)।

$\Rightarrow r_i \mid t$ सभी i के लिए

$\Rightarrow r \mid t$

इसी कारण $r = o(f)$.

उदाहरण 3.14: दिया गया है कि क्रमचय की कोटि,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 1 & 3 \end{pmatrix} = (1245)(36)$$

यह L.C.M.(4, 2) = 4 है, जैसे $o(1245) = 4$ और $o(36) = 2$ है।

उदाहरण 3.15: दो उपसमूह H, K का उदाहरण प्रस्तुत करें जो सामान्य नहीं हों किन्तु H, K एक उपसमूह हो।

हल: मानें $H = \{I, (12)\}$

$K = \{I, (123), (132)\}$

माना कि S_4 के दो उपसमूह हों (ये ऐसे उपसमूह हैं जिन्हें सत्यापित किया जा सकता है)।

यहां $H, K = \{I, (12), (123), (132), (12)(123), (12)(132)\}$

$= \{I, (12), (123), (132), (23), (13)\}$

$K, H = \{I, (123), (132), (12), (123)(12), (132)(12)\}$

$= \{I, (12), (123), (132), (23), (13)\}$

इस प्रकार $H,K = KH \Rightarrow HK$ एक उपसमूह है।

अब $H(123) = \{(123), (12)(123)\} = \{(123), (23)\}$

$(123)H = \{(123), (13)\}$

अथवा $H(123) \neq (123)H$

अर्थात किसी भी $a \in S_4$ के लिए $Ha \neq aH$

$\Rightarrow H, S_4$ में सामान्य नहीं है।

इसी प्रकार यह परखा जा सकता है कि $K(14) \neq (14)K$

और K, S_4 में सामान्य नहीं है।

अथवा यह कि S_4 में K सामान्य नहीं है।

उदाहरण 3.16: दर्शायें कि $Z(S_n) = \{I\}, (n \geq 3)$

हल: $f \neq I$ इस प्रकार मानें कि $f \in Z(S_n)$

अब $\exists\, a$ है इस प्रकार कि $f(a) = b$ जहाँ $b \neq a$ माना कि $c \neq a, b$ कोई अवयव हो (**ध्यान दे**: $n \geq 3$)

माना g मानचित्रण हो जहाँ, $g(a) = a$

$g(b) = c$

टिप्पणी

$$g(c) = b$$

तो $$g \in S_n$$

अब $$(fg)a = f(g(a)) = f(a) = b$$

$$(gf)a = g(f(a)) = g(b) = c$$

$$\Rightarrow fg \neq gf, \text{ अर्थात्, } f \notin Z(S_n)$$

इस प्रकार यदि $f \neq I$ हो तो यह $Z(S_n)$ से संबंधित नहीं हो सकता अथवा $Z(S_n) = \{I\}$।

उपप्रमेय: S_n गैर–एबेलियन (Non-Abelian) $\forall\ n \geq 3$ है। **ध्यान दें:** G एबेलियन है यदि $G = Z(G)$।

समूह सिद्धांत में केली प्रमेय (Cayley's Theorem) का नामकरण आर्थर केली (Arthur Cayley) के सम्मान में किया गया। इस प्रमेय के अनुसार प्रत्येक समूह G, G पर पार्श्व सममित समूह के उपसमूह से तुल्याकारिक है। इसे G के अवयवों पर G के समूह क्रिया के एक उदाहरण के रूप में समझा जा सकता है। समुच्चय G का क्रमचय G आच्छादक G लेते हुए कोई द्विभाजित फलन (Bijective Function) है। G के समस्त क्रमचय के समुच्चय से फलन संरचना के अधीन समूह का निर्माण होता है जिसे G पर सममित समूह कहते हैं एवं इसे G के रूप में लिखा जाता है।

उदाहरण 3.17: केली प्रमेय का प्रयोग करते हुए कोटि 8 के द्वितल (Dihedra) समूह के साथ तुल्याकारिता क्रमचय समूह को ज्ञात करें।

हल: कोटि 8 का द्वितल समूह इस प्रकार दिया है,

$$G = \{a, a^2, a^3, a^4 = e, ab, a^2b, a^3b, b \mid a^4 = e = b^2, b^{-1}ab = a^{-1}\}$$

समुच्चय K को उपरोक्त केली प्रमेय में इस प्रकार परिभाषित किया गया है, कि $K = \{f_x \mid x \in G\}$ जहाँ f_x को $f_x(y) = xy$ से परिभाषित किया गया है एवं प्रमेय के अनुसार $G \cong K$। हम K को निर्धारित करते हैं जो कि आवश्यक क्रमचय समूह (Permutation Group) होगा।

अब $$f_a(a) = a^2,\ f_a(a^2) = a^3,\ f_a(a^3) = a^4 = e,\ f_a(ab) = a^2b$$

$$f_a(a^2b) = a^3b,\ f_a(a^3b) = b,\ f_a(b) = ab,\ f_a(e) = a$$

इस प्रकार क्रमचय (1234)(5678) से f_a की पहचान की जा सकती है।

पुनः $$f_{a^2}(a) = a^3,\ f_{a^2}(a^2) = e, f_{a^2}(a^3) = a,\ f_{a^2}(ab) = a^3b$$

$$f_{a^2}(a^2b) = b,\ f_{a^2}(a^2b) = ab, f_{a^2}(b) = a^2b,\ f_{a^2}(e) = a^2$$

तथा इस प्रकार (13)(24)(57)(68) से f_{a^2} की पहचान की जा सकती है।

इसी ओर आगे बढ़ते हुए हम कह सकते हैं कि $f_{a3} = (1432)(5876)$

पुनः $f_{ab}(a) = aba = b$, $f_{ab}(a^2) = aba^2 = a^3b$, इत्यादि, एवं हम प्राप्त करते हैं,

$$f_{ab} = (18)(27)(36)(45)$$

टिप्पणी

तथा इसी प्रकार

$$f_{a^2b} = (15)(28)(37)(46)$$

$$f_{a^3b} = (16)(25)(38)(47)$$

$$f_b = (17)(26)(35)(48)$$

एवं अन्ततः इसीलिये,

$K = \{(1234)(5678), (13)(24)(57)(68), (1432)(5876), I, (18)(27)(36)(45), (15)(28)(37)(46), (16)(25)(38)(47), (17)(26)(35)(48)\}$

जो कि आवश्यक क्रमचय समूह है, जो कि कोटि 8 के द्वितल (Dihedral) समूह से तुल्याकारिक है।

उदाहरण 3.18: दर्शायें कि विषम क्रमचय सम कोटि (Even Order) का होता है।

हल: σ को विषम क्रमचय व $\sigma = \sigma_1\sigma_2 \ldots \sigma_k$ (असंबद्ध चक्रों के गुणन के रूप में) मानें। यदि $l = \text{L.C.M.}(o(\sigma_1), o(\sigma_2)), \ldots \sigma(\sigma_k))$ तो $l = o(\sigma)$

यदि प्रत्येक σ_i विषम लम्बाई (Odd Length) का हो तो प्रत्येक σ_i सम क्रमचय है एवं इस प्रकार σ सम क्रमचय है जो कि वास्तविक नहीं है।

इसी कारण कोई चक्र σ_j सम लम्बाई (Even Length) का है एवं $o(\sigma_j) =$ सम

$\Rightarrow$ व $2 | o(\sigma_j)$ चूँकि $o(\sigma_j) | l$, हम प्राप्त करते हैं $2 \mid l$ अथवा $l = o(\sigma)$ जो कि सम है।

ध्यान दें: सम क्रमचय कोटि का अभाज्य कोटि का होना आवश्यक नहीं है। वस्तुतः (12)(34) कोटि 2 का सम क्रमचय है जबकि I कोटि 1 का सम क्रमचय है।

उदाहरण 3.19: मान लें कि $f = (123456)$। दर्शायें कि हम $f = gh$ लिख सकते हैं, जहाँ $o(g) = 2, o(h) = 3$।

हल: दिया है, $o(f) = 6 = 2 \times 3$।

चूँकि सबसे बड़ा सामान्य भाजक $(2, 3) = 1$, $\exists$ पूर्णांक x, y, इस प्रकार है कि, $2x + 3y = 1$

वस्तुतः $2(-1) + 3(1) = 1$

अब $f = f^1 = f^{2(-1)+3(1)} = f^{-2}.f^3 = f^3 \cdot f^{-2} = gh$ (कहते हैं),

जहां $g = f^3$ और $o(g) = o(f^3) = 2$

जहां $f^3 = (14)(25)(36)$, $(f^3)^2 = f^6 = I$

तथा $h = f^{-2}$ और $o(h) = o(f^{-2}) = o(f^2) = 3$

चूंकि $f^2 = (123456)(123456) = (135)(246)$

प्रमेय 3.10: S_n $(n \geq 2)$ के समस्त सम क्रमचय का समुच्चय A_n, S_n का सामान्य उपसमूह है एवं $o(A_n) = \frac{o(S_n)}{2}$ तथा S_n में A_n का निर्देशिका 2 है।

प्रमाण: चूँकि तत्समक क्रमचय सम है अतः S_n का गैर रिक्त (Non Empty) उप–समुच्चय A_n है।

टिप्पणी

पुनः, $f, g \in A_n \Rightarrow f, g$ सम क्रमचय हैं।

$\Rightarrow f, g^{-1}$ सम क्रमचय हैं।

$\Rightarrow fog^{-1}$ सम है।

$\Rightarrow fog^{-1} \in A_n$

अथवा S_n का उपसमूह A_n है।

यदि $f \in A_n$ व $g \in S_n$ कोई भी सदस्य हों तो $g^{-1}\, o\, fog$ सम क्रमचय होगा, जो यह दर्शाता है कि $g^{-1}\, o\, fog \in A_n$ अथवा A_n, S_n का सामान्य उपसमूह है।

माना $G = \{1, -1\}$ गुणन के अधीन समूह है।

मानचित्र $\varphi : S_n \to G$, को इस प्रकार परिभाषित करें कि,

$\varphi(f) = 1$ यदि f सम क्रमचय है।

$= -1$ यदि f विषम क्रमचय है।

अब φ एक आच्छादक मानचित्रण है क्योंकि $S_n\,(n \geq 2)$ में सम व विषम क्रमचय होने चाहिए। (तत्समक क्रमचय व $(12)\, S_n$ में होगा)। φ एक समरूपता है इसे दर्शाने के लिये $f, g \in S_n$ को कोई भी अवयव (Members) सदस्य मानें।

प्रकरण (*i*): दोनों f, g सम हों, तो fog विषम है,

$$\varphi(fog) = 1 = 1.1 = \varphi(f)\varphi(g)$$

प्रकरण (*ii*): दोनों f, g विषम हों, तो fog सम है,

$$\varphi(fog) = 1 = (-1)\,(-1) = \varphi(f)\varphi(g)$$

प्रकरण (*iii*): यदि f, g में से एक विषम है तथा दूसरा सम।

मान लें कि f विषम है एवं g सम है तो fog विषम है

$$\varphi(fog) = -1 = (-1)\,(1) = \varphi(f)\varphi(g)$$

इसी कारण φ आच्छादक समरूपता है एवं इस प्रकार समरूपता के आधारभूत प्रमेय के अनुसार :

$$G \cong \frac{S_n}{\text{Ker } \varphi}$$

चूंकि $f \in \text{Ker } \varphi \quad \Leftrightarrow \varphi(f) = 1$

$\Leftrightarrow f$ सम है $\Leftrightarrow f \in A_n$

हमारे पास है $\text{Ker } \varphi = A_n$

अथवा $$G \cong \frac{S_n}{A_n}$$

परंतु $o(G) = 2 \Rightarrow o\left(\frac{S_n}{A_n}\right) = 2$

$$\Rightarrow \frac{o(S_n)}{o(A_n)} = 2$$

$$\Rightarrow \frac{o(S_n)}{2} = o(A_n)$$

तदुपरान्त S_n में A_n का निर्देशांक 2 है।

टिप्पणी

ध्यान दें: A_n को डिग्री n का एकांतर समूह कहा जाता है। यह लैग्रांज प्रमेय (Lagrange's Theorem) की दृष्टि से S_n का सबसे बड़ा उपसमूह भी होगा।

उदाहरण 3.20: दर्शाएँ कि यदि $H, S_n (n \geq 2)$ का कोई उपसमूह हो तो या तो H में समस्त क्रमचय सम होंगे अथवा सटीकता में आधे (Half) सम होंगे।

हल: चूँकि H एक उपसमूह है इसलिए इसमें तत्समक क्रमचय होना चाहिए जो सम हो। अतः H में विषम क्रमचय ही नहीं हो सकते। यदि H के समस्त सदस्य सम हों तो हमारा कार्य पूर्ण हुआ। मान लें कि इसमें दोनों विषम व सम क्रमचय हैं। मान लेते हैं कि $G = \{1, -1\}$ गुणन के अधीन एक समूह है।

मानचित्र $\varphi : H \to G$, को इस प्रकार परिभाषित करें कि,

$\varphi(f) = 1$ यदि f सम है।

$= -1$ यदि f विषम है।

अब उपरोक्त प्रमेय में दी गई परिभाषा के अनुसार φ एक आच्छादक समरूपक है। यदि H, K के समस्त सम क्रमचय का समुच्चय हो तो $\text{Ker}\,\varphi = K$।

आधारभूत प्रमेय के अनुसार

$$\frac{H}{\text{Ker}\,\varphi} \cong G \text{ or } \frac{H}{K} \cong G$$

$$\Rightarrow o\left(\frac{H}{K}\right) = o(G) = 2$$

$$\Rightarrow \frac{o(H)}{2} = o(K)$$

जिससे परिणाम सिद्ध हुआ।

उदाहरण 3.21: H, S_n का उपसमूह इस प्रकार हो कि H में विषम क्रमचय अंतर्विष्ट है। दर्शायें कि H में निर्देशांक 2 सहित M, H का उपसमूह है।

हल: चूँकि $A_n \trianglelefteq S_n$ व $H \leq S_n$, अतः $K = HA_n$ भी S_n का उपसमूह होगा।

$A_n \subseteq K \subseteq S_n$ का तात्पर्य या तो $K = S_n$ है अथवा $K = A_n$ (A_n सबसे बड़ा है)।

$H \subseteq HA_n = K$ एवं H में विषम क्रमचय है। K में विषम क्रमचय है एवं इसलिये $K \neq A_n$

इसी कारण $K = S_n$

अब $\frac{HA_n}{A_n} \cong \frac{H}{H \cap A_n}$ (तुल्याकारिता का द्वितीय प्रमेय)

तथा चूँकि $HA_n = K = S_n$,

हमारे पास $\frac{S_n}{A_n} \cong \frac{H}{H \cap A_n} \Rightarrow o\left(\frac{H}{H \cap A_n}\right) = o\left(\frac{S_n}{A_n}\right) = 2$

टिप्पणी

$M = H \cap A_n$ को प्राप्त करने पर H में M का निर्देशांक 2 है।

उदाहरण 3.22: $S_3 = \{I, (12), (13), (23), (123), (132)\}$ विचार करें।

हल : A_3 एकांतर (Alternating) समूह मानें तो,

$$A_3 = \{I, (123), (132)\}$$

$$o\left(\frac{S_3}{A_3}\right) = \frac{o(S_3)}{o(A_3)} = \frac{6}{3} = 2$$

वस्तुतः $$\frac{S_3}{A_3} = \{A_3, A_3(12)\}$$

तथा $$A_3 = (A_3(12))^2$$

$$A_3(12) = (A_3(12))^1$$

हम ज्ञात करते हैं कि $\frac{S_3}{A_3}$ जो कि $A_3(12)$ द्वारा उत्पन्न एक चक्रीय समूह है। अन्यथा अभाज्य कोटि का समूह चक्रीय भी है।

चूँकि S_3 एबेलियन नहीं है, S_3 चक्रीय नहीं हो सकता।

हम उन परिणामों का पुनर्स्मरण करते हैं जिन्हें पूर्व में सिद्ध कर चुके हैं।

1. चक्रीय समूह का भागफल समूह चक्रीय है।
2. एबेलियन समूह का भागफल समूह एबेलियन है।
3. एबेलियन समूह की समरूपता प्रतिबिंब एबेलियन है।
4. चक्रीय समूह की समरूपता प्रतिबिंब चक्रीय है।

इन समस्त परिणामों का विपरीत उपरोक्त उदाहरण में वास्तविक नहीं है।

ध्यान दे: दिया है, $S_3 \to S_3/A_3$ एवं S_3/A_3 जो प्राकृतिक आच्छादक समरूपता है तथा एबेलियन है।

उदाहरण 3.23: दर्शायें कि $n \geq 3$, (3–चक्रों द्वारा उत्पन्न उपसमूह) हेतु A_n है।

हल: H को 3–चक्रों द्वारा उत्पन्न एक उपसमूह मानें तो H का प्रत्येक अवयव 3–चक्रों की परिमित संख्या का गुणन है एवं चूँकि प्रत्येक 3–चक्र सम क्रमचय है तो H का प्रत्येक अवयव सम क्रमचय होगा अथवा $H \subseteq A_n$। पुनः यदि $f \in A_n$ हो तो f स्थानांतरण (Transpositions) की अभाज्य संख्या का गुणन है।

चूँकि किन्हीं दो सुनिश्चित स्थानांतरण के गुणन को तीन चक्रों के गुणन $[(ab)(cd) = (abc)(bcd), (ab)(bc) = (abc)]$ के रूप में लिखा जा सकता है, हम प्राप्त करते हैं कि f को 3–चक्रों $\Rightarrow f \in H$ के गुणन के रूप में व्यक्त किया जा सकता है एवं इसी कारण $H = A_n$ है।

उदाहरण 3.24: यदि H, S_n का उपसमूह हो निर्देशांक (Index) 2 सहित तो दर्शायें कि $H = A_n$। इस प्रकार A_n, S_n में निर्देशांक 2 का एकमात्र उपसमूह है।

हल: चूँकि S_n में H का निर्देशांक 2 है इसलिए S_n में H सामान्य है एवं $o\left(\frac{S_n}{H}\right) = 2$

टिप्पणी

यदि $H\sigma \in \frac{S_n}{H}$ कोई अवयव है।

r c $(H\sigma)^2 = H \Rightarrow H\sigma^2 = H \Rightarrow \sigma^2 \in H \; \forall \; \sigma \in S_n$

माना कि σ लम्बाई 3 का एक चक्र हो तो,

$\sigma^3 = \mathrm{I} \Rightarrow \sigma^4 = \sigma$ और क्योंकि $\sigma^2 \in H$

हम प्राप्त करते हैं $\sigma^4 \in H$ अर्थात् $\sigma \in H$

इस प्रकार लम्बाई 3 का प्रत्येक चक्र H में है परन्तु A_n लम्बाई 3 के चक्रों द्वारा उत्पन्न है। इस प्रकार $A_n \subseteq H$ अथवा $H = A_n$।

उदाहरण 3.25: दर्शायें कि S_n के सबसे छोटे उपसमूह जिसमें (12) है और जो कि (1 2 3 ..... n) है) S_n में है।

हल: माना कि H यहाँ S_n का सबसे छोटा उपसमूह हैं जिसमें (12) और (1 2 3 ..... n) अंतर्विष्ट है। हमें यह दर्शाने की आवश्यकता है कि $S_n \subseteq H$.

यदि $f \in S_n$ कोई अवयव हो तो f को स्थानांतरण (Transposition) के गुणन के रूप में व्यक्त किया जा सकता है एवं चूँकि किसी स्थानांतरण $(ab) = (1a)(1b)(1a)$ के प्रकार $(1x)$ को f के स्थानांतरण के उत्पाद के रूप में व्यक्त किया जा सकता है। हम दर्शाते हैं कि समस्त स्थानांतरण (12), (13), (14), ..., $(1n)$ H में है जिसका तात्पर्य यह है कि f, H में स्थित होगा क्योंकि f कुछ नहीं है, बस ऐसे कुछ सदस्य का उत्पाद है।

अब $(1n) = (n\,n-1 \ldots 321)(12)(123 \ldots n) \in H$

$\Rightarrow$ $(n\,n-1) = (n\,n-1 \ldots 321)(1n)(123 \ldots n) \in H$

$(n-1\;n-2) = (n\,n-1 \ldots 321)(n\,n-1)(123 \ldots n) \in H$

इत्यादि।

यह दर्शाता है कि (43), (32), इत्यादि, H में हैं।

अब $(12) \in H$

$\Rightarrow$ $(13) = (12)(23)(12) \in H$

$\Rightarrow$ $(14) = (13)(34)(13) \in H$

.....

$(1n) \in H$

इसी कारण $H = S_n$.

उदाहरण 3.26: दर्शायें कि S_n में लम्बाई r के सुनिश्चित चक्रों की संख्या $\frac{1}{r} \cdot \frac{n!}{(n-r)!}$, $(r \le n)$ है।

हल: चूँकि r विषयो की सुनिश्चित व्यवस्था (Distinct Arrangement) की संख्या ${}^nP_r = \frac{n!}{(n-r)!}$ में n विषयों (Objects) एवं चक्रों से चुनी गयी है,

$(a_1a_2 \ldots\ldots a_r), (a_2a_3 \ldots\ldots a_ra_1), (a_3a_4 \ldots\ldots a_ra_1a_2), \ldots\ldots, (a_ra_1 \ldots\ldots a_{r-1})$

जो कि समान हैं, अतः हम पाते हैं कि सुनिश्चित (Distinct) r–चक्रों की संख्या $\frac{1}{r}\cdot\frac{n!}{(n-r)!}$ होगी।

टिप्पणी

उदाहरण 3.27: उदाहरण सहित दर्शायें कि सम्भव है कि लैग्रांज प्रमेय का विलोम नहीं होगा।

हल: एकांतरण समूह A_4 का विचार करें।

$$o(A_4)=\frac{o(S_4)}{2}=\frac{|4}{2}=12$$

हम दर्शाते हैं कि यद्यपि $6 \mid 12$ का A_4 में कोटि 6 का उपसमूह नहीं है। मान लें कि H, A_4 का उपसमूह है व $o(H)=6$।

पूर्ववर्ती उदाहरण से S_4 में सुनिश्चित 3–चक्रों की संख्या,

$\frac{1}{3}\cdot\frac{4!}{(4-3)!}=\frac{4.3.2.1}{3.1}=8$ है।

पुनः चूँकि प्रत्येक 3–चक्र में सम क्रमचय (Even Permutation) होगा अतः ये समस्त 3–चक्र A_4 में हैं।

अब स्पष्ट है कि कम से कम एक 3–चक्र, जैसे कि σ, $H\,(\text{o}(H)=6)$ से संबंधित नहीं है।

अब $\sigma \notin H \Rightarrow \sigma^2 \notin H$, क्योंकि यदि $\sigma^2 \in H$, हो।

चूँकि $\sigma^4 \in H$

$\Rightarrow \sigma \in H$

एवं $\sigma^3 = I$ जैसे $o(\sigma) = 3$.

माना $K = <\sigma> = \{I, \sigma, \sigma^2\}$ तो $o(K) = 3\ (= o(\sigma))$

और $H \cap K = \{\text{I}\}\ \ (\sigma, \sigma^2 \notin H)$

$\Rightarrow\ o(HK) = \frac{o(H).o(K)}{o(H\cap K)}=\frac{6.3}{1}=18$, सम्भव नहीं है क्योंकि $HK \subseteq A_4$ व $o(A_4) = 12$।

उदाहरण 3.28: दर्शायें कि A_4 कोटि 12 का एकमात्र उपसमूह है S_4 में।

हल: माना H, S_4 में कोटि 12 का कोई उपसमूह है।

माना कि $H \neq A_4$

मान लें कि H में अंतर्विष्ट विषम क्रमचय (Odd Permutation) है।

इस प्रकार H में अंतर्विष्ट 6 विषम व 6 सम क्रमचय हैं।

$H \cap A_4$ कोटि 6 के A_4 का एक उपसमूह है।

A_4 में कोटि 6 का उपसमूह है।

टिप्पणी

किन्तु यह उपरोक्त उदाहरण से सम्भव नहीं है। इसी कारण परिणाम है।

उदाहरण 3.29: माना G कोई समूह हो एवं $H = \{g^2 \mid g \in G\}$। दर्शायें कि हो सकता है कि H, G का उपसमूह न हो एवं जिस प्रकरण में यह एक उपसमूह हो तो यह अवश्य ही सामान्य होगा।

हल: प्रथम भाग के लिये मान लेते हैं कि $G = A_4$ तो A_4 में S_4 के समस्त बारह सम क्रमचय हैं जो कि I, (12)(34), (13)(24), (14)(23) तथा 3–चक्र चूंकि $I^2 = I$, $((ab)(cd))^2 = I$ तथा 3–चक्र का वर्ग भी 3–चक्र है। (उदाहरण 3.27 देखें)

ध्यान दे: H में I होगा एवं 3–चक्र अथवा यह $o(H) = 9$ एवं चूँकि $9 \nmid 12$ तो H उपसमूह नहीं हो सकता। अब मान लें कि H एक उपसमूह हो तो यदि $h \in H$, $g \in G$ कोई अवयव हो तो,

$$g^{-1} \in G \Rightarrow g^{-2} \in H, \text{ और } gh \in G \Rightarrow (gh)^2 \in H$$

$$\Rightarrow g^{-2}(gh)(gh) \in H \Rightarrow g^{-1}hg \in H \text{ अथवा } G \text{ में } H \text{ सामान्य है।}$$

टिप्पणी: यहाँ देखा जा सकता है कि यदि G एबेलियन (Abelian) होता है तो H एक उपसमूह होगा।

उदाहरण 3.30: दर्शायें कि (123) S_n के किसी अवयव का घन (Cube) नहीं है।

हल: हम सर्वप्रथम दर्शाते हैं कि यदि $(\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)$ कोई चक्र हो।

तो $(\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)^3 = (\alpha_1\ \alpha_4\ \alpha_7)\ (\alpha_2\ \alpha_5\ \alpha_8)\ (\alpha_3\ \alpha_6\ \alpha_9)$

चूँकि $(\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)^2 = (\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)\ (\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)$

$$= (\alpha_1\ \alpha_3\ \alpha_5\ \alpha_7\ \alpha_9\ \alpha_2\ \alpha_4\ \alpha_6\ \alpha_8)$$

$$(\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)^3 = (\alpha_1\ \alpha_2 \ldots\ldots\ldots \alpha_9)\ (\alpha_1\ \alpha_3\ \alpha_5\ \alpha_7\ \alpha_9\ \alpha_2\ \alpha_4\ \alpha_6\ \alpha_8)$$

$$= (\alpha_1\ \alpha_4\ \alpha_7)\ (\alpha_2\ \alpha_5\ \alpha_8)\ (\alpha_3\ \alpha_6\ \alpha_9)$$

अब मान लेते हैं कि किसी $\alpha \in S_n$, के लिये $(1\ 2\ 3) = \alpha^3$ है, तो चूँकि α को असंबद्ध चक्रों के गुणन (Product) के रूप में व्यक्त किया जा सकता है।

मान लेते हैं $\alpha = \sigma_1\ \sigma_2 \ldots\ldots \sigma_k$ जहाँ σ_i असंबद्ध चक्र हैं।

तो $\alpha^3 = \alpha_1^3\ \alpha_2^3 \ldots\ldots \alpha_k^3$ (असंबद्ध चक्रीय क्रमविनिमय (Disjoint Cycles Commute) के रूप में)

$$\alpha^3 = (123)$$

और $$\Rightarrow \alpha^9 = (123)^3 = I \Rightarrow o(\alpha) = 9$$

इस प्रकार प्रत्येक σ_i की लम्बाई 3 अथवा 9 की होगी। क्योंकि क्रमचय की कोटि इसके असंबद्ध चक्रों की कोटि लम्बाइयों का L.C.M. है।

पुनः कम से कम एक σ_i ऐसा है जिसकी लम्बाई 9 है, अन्यथा यदि सबकी लम्बाई 3 हो तो L.C.M., 3 होगा जिसका तात्पर्य यह कि $o(\alpha) = 3$ जो कि वास्तविक नहीं है।

सामान्य कथन की हानि के बिना σ_i की लम्बाई 9 लेते हैं।

अब यदि किसी σ_i की लम्बाई 3 हो तो $\sigma_i^3 = I$

टिप्पणी

अतः $\alpha^3 = (123) = \sigma_1^3\ \sigma_2^3\ .....\ \sigma_k^3$

$= \sigma_1^3 \times$ लम्बाई 9 के चक्रों के अन्य घन

माना कि $\sigma_1 = (\alpha_1\ \alpha_2.....\alpha_9)$

$\Rightarrow \sigma_1^3 = (\alpha_1\ \alpha_4\ \alpha_7)(\alpha_2\ \alpha_5\ \alpha_8)(\alpha_3\ \alpha_6\ \alpha_9)$

$\Rightarrow (123) = (\alpha_1\ \alpha_4\ \alpha_7)(\alpha_2\ \alpha_5\ \alpha_8)(\alpha_3\ \alpha_6\ \alpha_9) \times$ अन्य चक्र जिनमें $\alpha_1, \alpha_2....., \alpha_9$ नहीं अंतर्विष्ट हैं,

चूँकि सभी असंबद्ध हैं, जो कि विरोधाभास होगा क्योंकि प्रत्येक α_i अलग है, इसलिये यदि $\alpha_1 = 1, \alpha_2 = 2, \alpha_3 = 3$ तो

α_4 इस प्रकार है कि यह L.H.S. में नियत है परन्तु R.H.S. में $\alpha_4 \to \alpha_7$ है।

इसी कारण यह परिणाम है।

उदाहरण 3.31: $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$ का विचार करें।

यदि इन अवयवों को e, x, y, z से इंगित करते हैं तो निम्नांकित सारणी से हमें सम्बन्धित गुणन प्राप्त होते हैं।

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

जिससे यह पता लगता है कि संवृत K_4 में स्थित है एवं इस प्रकार K_4 समूह का निर्माण होता है। इसे **क्लॅईन के चार समूह (Klein's Four Group)** कहा जाता है जो कि S_4 का उपसमूह है। यह परिमित एबेलियन समूह है जो कि चक्रीय नहीं है (क्योंकि इसमें कोटि $4 = o(K_4)$ का कोई अवयव नहीं है)।

टिप्पणी: (*i*) हम अवयवों e, x, y, z को आव्यूह गुणन (Matrices Multiplication) के अधीन आव्यूह $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}$ के रूप में ले सकते हैं।

(*ii*) हम आगे देख सकते हैं कि कोटि 4 का कोई अचक्रीय एबेलियन (Non-Cyclic Abelian) समूह $G = \{e, a, b, ab\}$ प्रकार का है। यहाँ प्रत्येक अवयव (e के अतिरिक्त) कोटि 2 में होगा।

$[x \in G \Rightarrow o(x) \mid o(G) \Rightarrow o(x) = 1, 2$ या 4 परन्तु $o(x) = 4$ से $x^4 = e$ प्राप्त होता है एवं अब G चक्रीय होगा।

इस प्रकार $o(a) = o(b) = o(ab) = 2$

अर्थात् $a^2 = b^2 = (ab)^2 = e$

स्पष्ट है कि यह समूह G क्लॅईन के चार समूह $[e \to I, a \to (12)\ (34), b \to (13)(24), ab \to (14)(23)]$ से तुल्याकारिक है। इसी कारण कोटि 4 का प्रत्येक अचक्रीय एबेलियन समूह क्लॅईन के चार समूह से तुल्याकारिक होगा।

उदाहरण 3.32: दिया हुआ है कि A_4 के किसी अवयव की कोटि 1, 2 अथवा 3 हो तो दर्शायें कि $o(Z(A_4)) = 1$.

हलः हम दर्शाते हैं कि $Z(A_4)$ में कोटि 2 अथवा 3 का कोई अवयव नहीं है।

माना कि $a \in Z(A_4)$ इस प्रकार है कि $o(a) = 2$

माना कि $b \in A_4$ कोटि 3 का कोई अवयव हो तो चूँकि $ab = ba$ (a केन्द्र में है)।

$(o(a), o(b)) = 1$, हम ज्ञात करते हैं कि $o(ab) = o(a).o(b) = 2 \times 3 = 6$

जो कि दिए गए नियमानुसार सम्भव नहीं है। अतः $Z(A_4)$ में कोटि 2 का कोई अवयव नहीं है।

इसी प्रकार इसमें कोटि 3 का कोई अवयव नहीं है। अतः इसमें I ही अंतर्विष्ट हो सकता है।

उदाहरण 3.33: उदाहरण से दर्शायें कि हम तीन समूह $E \subseteq F \subseteq G$ इस प्रकार ज्ञात कर सकते हैं कि E, F में सामान्य है, F, G में सामान्य है, जबकि E, G में सामान्य नहीं है।

हलः $E = \{I, (12)(34)\}$ मानें।

$F = K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$

$G = A_4$

तो E, G में सामान्य नहीं है क्योंकि,

$E(123) = \{I\,(123), (12)(34)(123)\} = \{(123), (243)\}$

$(123)E = \{(123)\,I, (123)(12)(34)\} = \{(123), (134)\}$

यह दर्शाता है कि $E(123) \neq (123)E$ $\quad (123) \in A_4 = G.$

E, F में सामान्य होगा क्योंकि E में F का निर्देशांक 2 है। अन्यथा चूँकि F एबेलियन है तो E भी F में सामान्य होगा।

G में F सामान्य है।

$\theta \in A_4$ मान लें एवं $(ab)(cd) \in K_4$ कोई अवयव हो।

यदि a, b, c, d किसी भी 1, 2, 3, 4 है तो $\theta(ab)(cd)\theta^{-1} = (\theta(a)\,\theta(b))\,(\theta(c)\,\theta(d)) \in K_4$ क्योंकि इस चक्र संरचना (Cycle Structure) के समस्त क्रमचय K_4 में हैं।

K_4 भी A_4 में सामान्य है।

ध्यान दें: K_4 में समस्त अवयव सम क्रमचय हैं एवं इसलिये A_4 से संबंधित हैं।

3.4 केली प्रमेय

समूह सिद्धांत, में केली प्रमेय (Cayley's Theorem) का नामकरण आर्थर केली (Arthur Cayley) के सम्मान में किया गया। इस प्रमेय के अनुसार प्रत्येक समूह G को G पर पार्श्व सममित (Acting Symmetric) समूह के उपसमूह से तुल्याकारिक कहा जाता है। इसे G के अवयवों पर G के समूह क्रियाओं के उदाहरण के रूप में समझा जा सकता है। समुच्चय G का क्रमचय G आच्छादक G को लेते हुए कोई द्विभाजित फलन (Bijective Function) माना जाता है। G के समस्त क्रमचय के समुच्चय से फलन

संरचना (Function Composition) के अधीन समूह का निर्माण होता है जिसे G पर सममित समूह (Symmetric Group) कहा जाता है एवं Sym (G) के रूप में लिखा जाता है।

टिप्पणी

प्रमेय 3.11: (व्यापीकृत केली प्रमेय (Generalised Cayley's Theorem)): H, G का उपसमूह व $\mathcal{L} = \{aH \mid a \in G\}$ हो तो $\exists$ समरूपता (Homomorphism) $\theta : G \to A(\mathcal{L})$ इस प्रकार है कि $\text{Ker}\,\theta$, G का सबसे बड़ा सामान्य उपसमूह है जो H में अंतर्विष्ट है।

प्रमाण: $\theta : G \to A(\mathcal{L})$ को इस प्रकार परिभाषित करें कि $\theta(g) = f_g$ जहाँ $f_g : \mathcal{L} \to \mathcal{L}$ इस प्रकार है कि $f_g(aH) = gaH$

θ सुपरिभाषित है यह दर्शाने के लिये हमें $f_g \in A(\mathcal{L})$ को सिद्ध करने की आवश्यकता है।

अब $\quad f_g(aH) = f_g(bH)$

$\Rightarrow gaH = gbH$

$\Rightarrow aH = bH \quad \Rightarrow f_g$, 1-1 हैं।

पुनः किसी $aH \in \mathcal{L}$ के लिये $f_g(g^{-1}aH) = aH$, दर्शाता है कि f_g आच्छादक है एवं इस प्रकार $f_g \in A(\mathcal{L})$

दिया है, $\theta(gh) = f_{gh}$, $\theta(g)\theta(h) = f_g f_h$

एवं चूँकि $f_{gh}(aH) = ghaH$

$f_g f_h(aH) = f_g(f_h(aH)) = f_g(haH) = ghaH$

हम ज्ञात करते हैं $f_{gh} = f_g f_h$

अथवा वह θ समरूपक है।

चूँकि समरूपता का आधारभूत सामान्य उपसमूह है तो हमारे पास $\text{Ker}\,\theta$ है जो कि G का सामान्य उपसमूह है।

पुनः यदि $g \in \text{Ker}\,\theta$ तो $\theta(g) = I = A(\mathcal{L})$ के तत्समक है।

$\Rightarrow f_g = I$

$\Rightarrow f_g(aH) = aH \quad \forall\ aH \in \mathcal{L}$

विशेषतया $f_g(eH) = eH \quad \Rightarrow geH = eH \quad \Rightarrow gH = H$

$\Rightarrow g \in H$

$\Rightarrow \text{Ker}\,\theta \subseteq H$

अब K को G का कोई सामान्य उपसमूह मानें, जो H में अंतर्विष्ट है। माना कि $k \in K$ कोई अवयव हो। हम यह दर्शाना चाहते हैं कि $k \in \text{Ker}\,\theta$ या $\theta(k) = I$

अथवा $f_k = I$

या $\quad f_k(aH) = aH \quad \forall\ aH$

अब $\quad f_k(aH) = kaH = a(a^{-1}ka)\,H = ahH = aH$

[**ध्यान दें:** $a^{-1}ka \in K \subseteq H$]

इसी कारण $K \subseteq \text{Ker}\,\theta$, जिससे प्रमेय सिद्ध हुआ।

टिप्पणीः (i) यदि हम दायें सहसमुच्चय के साथ कार्य करना चाहें तो θ को $\theta(g) = f_g$ द्वारा परिभाषित किया जा सकता है, जहाँ $f_g(Ha) = Hag^{-1}$

(ii) यदि $H = \{e\}$ तो उपरोक्त प्रमेय केली प्रमेय है क्योंकि $\text{Ker}\theta = \{e\} \Rightarrow \theta$ 1–1 है।

उपप्रमेयः (निर्देशांक प्रमेय (Index Theorem)**):** यदि $H \neq G$ परिमित समूह G का उपसमूह इस प्रकार हो कि $o(G)$, $i_G(H)!$ को विभाजित न करे तो G में गैर–नगण्य सामान्य उपसमूह है। (अर्थात् G सरल नहीं है)।

प्रमाणः उपरोक्त प्रमेय से हम ज्ञात करते हैं कि $\text{Ker}\,\theta$, G का सामान्य उपसमूह है।

चूँकि $\text{Ker}\,\theta \subseteq H \neq G, \text{Ker}\,\theta \neq G$

यदि $\text{Ker}\,\theta = \{e\}$ तो θ, 1–1 है तथा इस प्रकार $\theta : G \to A(\mathcal{L})$, 1–1 समरूपक है, अर्थात् G, T के उपसमूह $A(\mathcal{L})$ से तुल्याकारिक है।

$\Rightarrow o(G) = o(T)$ परन्तु $o(T) \mid o(A(\mathcal{L})) \Rightarrow o(G) \mid o(A(\mathcal{L})) = i_G(H)!$ एक विरोधाभास है तथा इसलिये $\theta \neq \{e\}$ एवं यह आवश्यक गैर–नगण्य (Non-Trivial) सामान्य उपसमूह है।

उदाहरण 3.34: माना G परिमित समूह H का उपसमूह $o(H)$ इस प्रकार हो एवं $(i_G(H)–1)!$ सहअभाज्य हो तो दर्शायें कि H, G में सामान्य है।

हलः G में H के बायें सहसमुच्चय का समुच्चय $S = \{aH \mid a \in G\}$ मानें तो $\theta : G \to A(S)$ को इस प्रकार परिभाषित करें कि $\theta(g) = T_g$

जहाँ $T_g : S \to S$ इस प्रकार कि $T_g(aH) = gaH$

तो व्यापीकृत केली प्रमेय में दर्शायें अनुसार θ एक समरूपक है एवं $\text{Ker}\,\theta \subseteq H$।

तदुपरान्त $\frac{G}{\text{Ker}\theta} \cong T$ जहाँ $T \leq A(S)$

$\Rightarrow \quad o(G/\text{Ker}\,\theta) = o(T)$ जहाँ $o(T) \mid o(A(S)) = \underline{|i_G(H)}$

$i_G(H) = \frac{o(G)}{o(H)} = n$ मानें तो $o(T) \mid \underline{|n}$ तथा इस प्रकार $\frac{o(G)}{o(\text{Ker}\theta)} \mid \underline{|n}$

पुनः $\text{Ker}\,\theta \leq H \Rightarrow o(\text{Ker}\,\theta) \mid o(H)$

$\Rightarrow o(H) = m.o(\text{Ker}\,\theta)$ किसी भी m के लिए

$\Rightarrow \frac{o(G)}{n} = m.o(\text{Ker}\,\theta)$

$\Rightarrow nm = \frac{o(G)}{o(\text{Ker}\,\theta)}$

अथवा $nm \mid \underline{|n} \Rightarrow nm \mid n.\underline{|n-1} \Rightarrow m \mid \underline{|n-1}$,

$m \mid o(H)$ व चूँकि ये सहअभाज्य हैं, अतः $m = 1$ अथवा $H = \text{Ker}\,\theta$, अर्थात् $H \trianglelefteq G$।

टिप्पणी

अपनी प्रगति जांचिए

5. केली प्रमेय को परिभाषित करें।
6. निर्देशांक प्रमेय क्या है?

3.5 अपनी प्रगति जांचिए प्रश्नों के उत्तर

1. माना $< G, * >$ व $< G', o >$ दो समूह हों तो मानचित्रण $f: G \to G'$ को समरूपक कहा जाता है। यदि $f(a * b) = f(a)\, o\, f(b) \quad a, b \in G$ हो।
2. यदि $f: G \to G'$ आच्छादक समरूपता हो तो G' को G की समरूपक प्रतिबिंब कहते हैं।
3. $f: G \to G'$ समरूपता हो तो f के आधारभूत ($\text{Ker}\, f$ द्वारा इंगित) को $\text{Ker}\, f = \{x \in G \mid f(x) = e'\}$ से परिभाषित किया जाता है जहाँ e', G' का तत्समक है।
4. यदि H व K समूह G के दो उपसमूह हों जहाँ H, G में सामान्य हो तो $\frac{HK}{H} \cong \frac{K}{H \cap K}$ होगा।
5. प्रत्येक समूह G क्रमचय समूह से तुल्याकारिक है।
6. यदि $H \neq G$ परिमित समूह G का उपसमूह इस प्रकार हो कि $o(G)$, $i_G(H)!$ को विभाजित न करे तो G में गैर–नगण्य सामान्य उपसमूह है। (अर्थात् G सरल नहीं है)।

3.6 सारांश

- यदि दो प्रणाली में समान संख्या के अवयव हों एवं ये बिल्कुल समान रीति में व्यवहार करें तो उन्हें समतुल्य कहने में कोई घाटा नहीं है, भले ही कई बार हो सकता है कि समता का विचार कुछ असहज लगे, विशेषतः अपरिमित समुच्चयों के प्रकरण में।
- आच्छादक समरूपता को समकारिता कहा जाता है।
- एक–एक समरूपता को एकाकारिता कहा जाता है।
- समूह G से स्वयं तक समरूपता को G का अंतराकारिता कहा जाता है।
- समूह G से स्वयं तक तुल्याकारिता को G का स्वाकारिता कहते हैं।
- समूहों में तुल्याकारिता का सम्बन्ध एवं समतुल्यता सम्बन्ध है। इस प्रकार जब भी समूह G अन्य समूह G' से तुल्याकारिक हो तो G', G से तुल्याकारिक होगा। अतः हम सरलता से यह कह सकते हैं, कि G व G' तुल्याकारिक हैं एवं इसे $G \cong G'$ से इंगित करते हैं।
- यदि $f: G \to G'$ समरूपता हो तो $\text{Ker}\, f$, G का सामान्य उपसमूह है।

टिप्पणी

- समरूपता $f: G \to G'$ एक–एक है, यदि $\text{Ker}\, f = \{e\}$।
- यदि $f: G \to G'$, $K = Ker\, f$ के साथ आच्छादक समरूपक हो तो $\frac{G}{K} \cong G'$।
- यदि H व K समूह G के दो सामान्य उपसमूह इस प्रकार हों कि $H \subseteq K$, तो $\frac{K}{H}$, $\frac{G}{H}$ का सामान्य उपसमूह है तथा इससे विपरीत होगा।
- यदि $f: G \to G'$ को $\text{Ker}\, f = K$ अंतर्विष्ट आच्छादक समरूपता मानें तो G' के उपसमूह H' के लिये G' को परिभाषित कर सकते हैं।
- S_n में किसी क्रमचय f की कोटि L.C.M. के असंबद्ध चक्रों की कोटि के f के समतुल्य होता है।
- H को G का उपसमूह मानें एवं $\mathcal{L} = \{aH \mid a \in G\}$ है, तो $\exists$ समरूपता $\theta : G \to A(\mathcal{L})$ इस प्रकार है कि $\text{Ker}\, \theta$, G का सबसे बड़ा सामान्य उपसमूह है जो कि H में अंतर्विष्ट है।

3.7 मुख्य शब्दावली

- **समरूपता** : समरूपता एक संरचना है जो दो बीजगणितीय संरचनाओं के बीच मानचित्र को संरक्षित करती है जिसमें एक ही प्रकार की संरचनाएं, जैसे दो समूह, दो वलय, या दो सदिश स्थान हों।
- **समूह समरूपता** : समूह समरूपता समूहों के मध्य का मानचित्र है जो समूह संक्रिया को परिरक्षित करता है। इसका तात्पर्य यह है कि समूह समरूपता में दूसरे समूह के तत्समक अवयव से प्रथम समूह के तत्समक अवयव को मानचित्रित किया जाता है तथा प्रथम समूह के अवयव के व्युत्क्रम को इस अवयव की प्रतिबिंब के व्युत्क्रम पर मानचित्रित किया जाता है।
- **तुल्याकारिता** : समान प्रकार की बीजगणितीय संरचनाओं के मध्य तुल्याकारिता को सामान्यतया द्विभाजित समरूपता के रूप में परिभाशित किया जाता है।
- **अंतराकारिता** : यह ऐसी समरूपता है जिसका डोमैन, कोडामैन के समतुल्य होता है अथवा अधिक साधारण रूप में यह एक आकारिता है जिसका स्रोत लक्ष्य के समतुल्य है। बीजगणितीय संरचना के अथवा वर्ग का प्रयोजन के अंतराकारिता से संरचना के अधीन एकाभ का निर्माण होता है।
- **स्वाकारिता** : यह एक ऐसी अंतराकारिता है, जो कि एक तुल्याकारिता भी है। बीजगणितीय संरचना अथवा वर्ग की संरचना स्वाकारिता के अधीन समूह का निर्माण होता है जिसे कि संरचना का स्वाकारिता समूह कहा जाता है।
- **एकाकृतिकता** : बीजगणितीय संरचनाओं के लिये एकाकृतिकता को सामान्यतः अंतः क्षेत्रण समरूपता के रूप में परिभाषित किया जाता है। श्रेणी सिद्धांत के अधिक व्यापक परिदृश्य में एकाकृतिकता को ऐसे आकारिता के रूप में परिभाषित किया जाता है जो कि रद्द करने से छूट गया था।

टिप्पणी

- **केली प्रमेय** : समूह सिद्धांत, में केली प्रमेय का नामकरण आर्थर केली के सम्मान में किया गया। इस प्रमेय के अनुसार प्रत्येक समूह G को G पर पार्श्व सममित समूह के उपसमूह से तुल्याकारिक कहा जाता है। इसे G के अवयवों पर G के समूह क्रियाओं के उदाहरण के रूप में समझा जा सकता है।

3.8 स्व–मूल्यांकन प्रश्न एवं अभ्यास

लघु–उत्तरीय प्रश्न

1. समूहों के समरूपता एवं तुल्याकारिता क्या होते हैं?
2. दर्शायें कि समूहों में तुल्याकारिता का सम्बन्ध एक समतुल्यता सम्बन्ध है।
3. तुल्याकारिता का क्या तात्पर्य है?
4. समरूपता के आधारभूत प्रमेय का प्रयोग कब किया जाता है?
5. समूह a में निर्धारित अवयव G के लिये $fa : G \to G$ को इस प्रकार परिभाषित करें कि $fa\,(x) = a^{-1}\,xa, x \in G$।
6. प्रदर्शित करें कि एबेलियन समूह की समरूपता प्रतिबिंब एबेलियन है।
7. समूहों के रूपांतरण एवं क्रमचय शब्दों को परिभाषित करें।
8. S_n में किसी क्रमचय f की कोटि L.C.M. के असंबद्ध चक्रों की कोटि के f के समतुल्य कैसे होता है?
9. दर्शायें कि यदि $H \neq G$ परिमित समूह G का उपसमूह इस प्रकार हो कि $o(G)$ से $i_G(H)!$ विभाजित नहीं हो तो G में गैर–नगण्य सामान्य उपसमूह है।
10. केली प्रमेय क्या है?

दीर्घ–उत्तरीय प्रश्न

1. उपयुक्त उदाहरणों सहित समूहों के समरूपता व तुल्याकारिता विशेषताओं का विस्तारपूर्वक वर्णन करें।
2. समूहों के समरूपता व तुल्याकारिता के प्रमेयों एवं व्युत्पत्ति का उदाहरण सहित वर्णन करें।
3. उपयुक्त उदाहरणों की सहायता से समरूपता के आधारभूत प्रमेय की व्याख्या करें।
4. समूहों के रूपांतरण एवं क्रमचय की अवधारणाओं का वर्णन उदाहरण सहित करें।
5. $S_n (n < 5)$ के विभिन्न उपसमूहों की उदाहरण सहित चर्चा करें।
6. यदि G कोटि n का एक चक्रीय समूह है एवं $p \mid n$ तो सिद्ध करें कि G का समरूपता कोटि p के चक्रीय समूह में आच्छादक है। इसका आधारभूत ज्ञात करें।
7. प्रदर्शित करें कि U_{10}, $\mathbf{Z}_4$ से तुल्याकारिक है परन्तु U_{12} से नहीं।

8. दर्शायें कि कोटि n का चक्रीय समूह की ईकाई के nवा मूल के गुणक समूह से तुल्याकारिक है। $a^r \to e^{2\pi ir/n}$ का विचार करें।
9. "प्रत्येक समूह G क्रमचय समूह से तुल्याकारिक होता है"। इस कथन को उदाहरण सहित सिद्ध करें।
10. उदाहरण की सहायता से व्यापकीकृत केली प्रमेय सिद्ध करें।

टिप्पणी

3.9 सहायक पाठ्य सामग्री

Sharma, Dr Anil and Jitendra Saini. 2016. *Abstract Algebra* (अमूर्त बीजगणित) Jaipur (Rajasthan): RBD Publisher.

Pathak, Dr H. K. 2017. *Abstract Algebra* (अमूर्त बीजगणित). Kolkata (West Bengal): Siksha Sahitya Prakashan.

Herstein, I. N. 1975. *Topics in Algebra*, 2nd Edition. New York: John Wiley and Sons.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. UK: Cambridge University Press (Indian Edition).

Khanna, V. K. and S. K. Bhambari. 2016. *A Course in Abstract Algebra*, 5th Edition. New Delhi: Vikas Publishing House Pvt. Ltd.

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

Gilbert, Linda. 2008. *Elements of Modern Algebra*. Boston: Cengage Learning.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

Childs, Lindsay N. 2008. *A Concrete Introduction to Higher Algebra*. Berlin: Springer Science & Business Media.

इकाई 4 समूह स्वाकारिता, परिमित एवं एबेलियन समूह

टिप्पणी

संरचना

4.0 परिचय

बीजगणित में समूह के स्वाकारिता (Automorphism) समूह को ऐसे समूह के रूप में परिभाषित किया जाता है जिसके सभी अवयव आधार समूह (Base Group) के स्वाकारिता होते हैं एवं जहाँ समूह संक्रिया स्वाकारिता की संरचना (Structure) होती है। अन्य शब्दों में इसकी समूह संरचना (Group Structure) समूह के समस्त क्रमचय के समूहों का उपसमूह बन जाता है। समूह G की स्वाकारिता को तुल्याकारिता $G \rightarrow G$ से दर्शाया जा सकता है। G के स्वाकारिता के समुच्चय को Aut G से इंगित किया जाता है। मूलतः समूह स्वाकारिता समूह से स्वयं तक एक गुणन समूह है। यदि G परिमित गुणन (Finite Multiplicative) समूह हो तो G के स्वाकारिता को इसकी गुणन सारणी का पुनर्लेखन करते हुए दर्शाया जा सकता है किन्तु पुनरावृत्त (Repeated) अवयवों के इसके प्रारूप (Pattern) को परिवर्तन किए बिना।

आन्तरिक स्वाकारिता (Inner Automorphism), वलय अथवा बीजगणित के स्वाकारिता समूह है तथा इसे साधारणतया निर्धारित अवयव के समूह, वलय द्वारा प्रदर्शित किया जाता है जिसे संयुग्मित अवयव कहते हैं। इन आन्तरिक स्वाकारिता से स्वाकारिता समूह के उपसमूह का निर्माण होता है एवं इस उपसमूह द्वारा स्वाकारिता समूह के भागफल से बाह्य स्वाकारिता (Outer Automorphism) समूह की अवधारणा की जाती है। आन्तरिक स्वाकारिता ऐसा स्वाकारिता है जिसकी अवधारणा संयुग्मन से की जाती है।

टिप्पणी

गणित में, विशेषतया समूह सिद्धान्त में समूह G के उपसमुच्चयों में S का केन्द्रीकरण (इसे क्रमविनिमेय भी कहा जाता है) G के अवयवों का समुच्चय है जो S के प्रत्येक अवयव के साथ क्रमविनिमेय (Commuted) करता है एवं S का सामान्यीकरण अवयवों का ऐसा समुच्चय है जो अशक्त व्यवस्था की पूर्ति करता है। S के केन्द्रीकरण व सामान्यीकरण (Normalizer) G के उपसमूह हैं तथा G की संरचना से काफ़ी जानकारियाँ मिल सकती हैं। ये परिभाषाएँ एकाभ व अर्द्ध समूह में भी लागू होती हैं।

गणित में, विशेषतया समूह सिद्धांत में समूहों के दो अवयव a व b संयुग्मित होते हैं यदि समूह में अवयव g ऐसा हो कि $b = g^{-1}ag.$। यह समतुल्यता सम्बन्ध है जिसके समतुल्यता वर्गों को संयुग्मित वर्ग कहा जाता है। अमूर्त बीजगणित में एबेलियन (Abelian) समूह जिसे क्रमविनिमेय समूह भी कहा जाता है ऐसा समूह है जिसमें दो समूह अवयवों में समूह संक्रिया लागू करने का परिणाम उस कोटि (Order) पर निर्भर नहीं होता जिसमें वे लिखे जाते हैं। इसका तात्पर्य यह हुआ कि ये ऐसे समूह हैं जो क्रमविनिमय (Commutativity) के अभिगृहीत का पालन करते हैं। एबेलियन (Abelian) समूह पूर्णांकों के योग के अंकगणित (Arithmetic) का व्यापीकरण करते हैं। आरम्भिक उन्नीसवीं शताब्दी के गणितज्ञ निएल्स हेनरिक एबॅल (Niels Henrik Abel) के कारण यह नामकरण किया गया। गणित में, विशेषतः समूह सिद्धांत में गैर एबेलियन (Abelian) समूह (जिसे कभी–कभी गैर क्रमविनिमय समूह भी कहा जाता है।) ऐसा समूह $(G, *)$ है जिसमें G के कम से कम एक जोड़ी अवयव a व b पाये जाते हैं, जैसे कि $a * b \neq b * a$। समूह का यह वर्ग एबेलियन समूह का विपरीत है। इसीलिये एबेलियन समूह में समूह अवयवों (Group Elements) के समस्त युग्मों (Pairs) क्रमविनिमय (Commute) होते हैं।

इस इकाई में आप समूह स्वाकारिता, आन्तरिक स्वाकारिता, संयुग्मित सम्बन्ध व केन्द्रीकरण, सामान्यीकरण, गणना सिद्धान्त व परिमित समूह के वर्ग समीकरण, परिमित एबेलियन समूह व गैर–एबेलियन समूह के लिये कॉउची प्रमेय का अध्ययन करेंगे।

4.1 उद्देश्य

इस इकाई को पढ़ने के बाद आप–

- समूह स्वाकारिता एवं इसके अभिलक्षणों को समझ पाएंगे;
- आन्तरिक स्वाकारिता का वर्णन कर पाएंगे;
- समूह स्वाकारिता, समरूपता एवं आन्तरिक स्वाकारिता के प्रमेयों का विस्तारपूर्वक वर्णन कर पाएंगे;
- संयुग्मित सम्बन्ध, केन्द्रीकरण एवं सामान्यीकरण की चर्चा कर पाएंगे;
- परिमित समूह के गणना सिद्धान्त व वर्ग समीकरण की व्याख्या कर पाएंगे;
- परिमित एबेलियन समूहों को समझ पाएंगे;
- गैर–एबेलियन समूहों के लिये कॉउची प्रमेय को स्पष्ट कर पाएंगे।

4.2 समूह स्वाकारिता

टिप्पणी

बीजगणित में समूह के स्वाकारिता (Automorphism) समूह को ऐसे समूह के रूप में परिभाषित किया जाता है जिसके सभी अवयव आधार समूह के स्वाकारिता हों एवं जहाँ समूह संक्रिया स्वाकारिता की संरचना हो। अन्य शब्दों में इसका समूह संरचना समूह के समस्त तुल्याकारिता के समूह का उपसमूह हो जाता है। समूह G के समूह संरचना एक तुल्याकारिता $G \to G$ है। G के स्वाकारिता के समुच्चय को Aut G से इंगित किया जाता है।

मूलतः, समूह स्वाकारिता समूह से स्वयं तक का तुल्याकारिक है। यदि G एक परिमित गुणन समूह हो तो G के स्वाकारिता को इसकी गुणन सारणी के पुनर्लेखन के रूप में दर्शाया जा सकता है परन्तु पुनरावृत्ति अवयव के इसके प्रारूप को परिवर्तित किये बिना। उदाहरणार्थ इकाइयां $= \{1, -1, i, i\}$ के चौथे मूल के समूह की गुणन सारणी का तात्पर्य है कि $1 \mapsto 1, -1 \mapsto -1, i \mapsto -i, \ -i \mapsto i$ द्वारा परिभाषित मानचित्र G का स्वाकारिता है। स्वाकारिता समूह को सममित समूह भी कहा जाता है एवं स्वाकारिता समूह के उपसमूह को स्थानान्तरण (Transformation) समूह कहते हैं।

मानक परिभाषा के अनुसार, "स्वाकारिता गणितीय विषय से स्वयं तक एक तुल्याकारिता है। किसी अर्थ में यह विषय की सममित है एवं एक रीति है जिसमें उपसमूह से स्वयं मानचित्रण की जाती है किन्तु इसकी समूची संरचना को परिरक्षित रखते हुए। मानचित्रण के समस्त स्वाकारिता के समुच्चय से समूह का निर्माण होता है जिसे स्वाकारिता समूह कहा जाता है"।

स्वाकारिता से हमारा आशय समूह G से स्वयं तक तुल्याकारिता है। क्रमचय समूहों के अधीन हमने देखा ही था कि समस्त क्रमचयों (Permutations) (1–1 आच्छादक मानचित्र One-One Onto Maps) के समुच्चय से समूह का निर्माण होता है। समस्त स्वाकारिता के समुच्चय से भी समूह निर्मित होता है, ये दो परस्पर निकटसम्बन्धी होते हैं। आरम्भ में हम कुछ ऐसे बिन्दु लेते हैं जिनसे स्वाकारिता प्रदर्शित होता है।

1. G कोई समूह हो तो तत्समक मानचित्र $I: G \to G$ इस प्रकार हो कि $I(x) = x$, G का नगण्य स्वाकारिता है। वस्तुतः इसे कभी–कभी G का नगण्य स्वाकारिता कहा जाता है।
2. माना $\mathbf{Z} =$ को योग के अधीन पूर्णांक समूह मानें तो $f: \mathbf{Z} \to \mathbf{Z}$, इस प्रकार कि $f(n) = -n$ एक स्वाकारिता $f(n) = f(m) \Rightarrow -n = -m \Rightarrow n = m \Rightarrow f$ 1–1 है।

   पुनः चूँकि किसी $n \in \mathbf{Z}, f(-n) = n$ के लिये हम पाते हैं कि f आच्छादक (Onto) है।

   अब $f(n + m) = -(n + m) = -n - m = f(n) + f(m)$

   दर्शाया गया है कि f समरूपता है एवं इसी कारण स्वाकारिता है।
3. यदि G एबेलियन समूह है एवं $f: G \to G$ इस प्रकार है कि $f(x) = x^{-1}$ तो $f(xy) = (xy)^{-1} = y^{-1} x^{-1} = x^{-1} y^{-1} = f(x) f(y)$ f एक समरूपता है।

पुनः $f(x) = f(y) \Rightarrow x^{-1} = y^{-1}$

$\Rightarrow x = y \Rightarrow f$, 1–1 है।

f स्पष्टतया आच्छादक है एवं इसी कारण स्वाकारिता है।

टिप्पणी

4. यदि G गैर–एबेलियन समूह है तो उपरोक्त परिभाषित मानचित्र $f: G \to G$ इस प्रकार हुआ कि $f(x) = x^{-1}$ स्वाकारिता नहीं है।

चूँकि G गैर–एबेलियन है $\exists\, x, y \in G$ इस प्रकार हुआ $xy \neq yx$,

अब यदि $f(xy) = f(x) f(y)$

तो $(xy)^{-1} = x^{-1} y^{-1}$

$\Rightarrow (xy)^{-1} = (yx)^{-1}$

$\Rightarrow xy = yx$, एक विरोधाभास है।

इसी कारण f स्वाकारिता नहीं है।

नोटः $f: G \to G$ इस प्रकार कि $f(x) = x^{-1}$ एक स्वाकारिता है यदि G एबॅलियन हो।

5. G को कोटि n (n = विषम > 1) का एक परिमित एबेलियन समूह मानें तो। हम दर्शाते हैं कि G में गैर–नगण्य (Non-Trivial) स्वाकारिता है।

$f: G \to G$, को इस प्रकार परिभाषित करें कि $f(x) = x^{-1}$ (ऊपर प्रदर्शित अनुसार)

अब यदि $f = I$

तो $f(x) = x$ सभी $x \in G$ के लिए

$\Rightarrow x^{-1} = x$ सभी $x \in G$ के लिए

$\Rightarrow x^2 = e$ सभी $x \in G$ के लिए

$\Rightarrow o(x) \mid 2$ सभी $x \in G$ के लिए

$\Rightarrow o(x) = 1$ या 2 सभी $x \in G$ के लिए

यदि $x \neq e$ तो $o(x) = 2$ व $o(x) \mid o(G)$

$2 \mid o(G) \Rightarrow o(G)$ सम है जो कि वास्तविक नहीं है।

इसी कारण $f \neq I$

तथा परिणाम सिद्ध हुआ।

G कोई समूह हो एवं G से G के समस्त स्वाकारिता का समुच्चय इंगित हो रहा है। साधारणतया कोई भी यह दर्शा सकता है कि मानचित्र (Mappings) के संरचना के अधीन G से समूह का निर्माण होता है। वैसे हम प्रमेय 4.1 के माध्यम से यह परिणाम सिद्ध करते हैं जिससे हमें Aut G के बारे में कुछ अधिक जानकारियाँ मिलती हैं।

प्रमेय 4.1: G कोई समूह हो। Aut G से G के समस्त स्वाकारिता का समुच्चय इंगित किया जा रहा हो एवं Aut (G), G के समस्त क्रमचय का समूह हो तो Aut G, A (G) का उपसमूह है।

टिप्पणी

प्रमाण: चूँकि $I \in \text{Aut } G, \text{Aut } G \neq \varphi$

अतः $T \in \text{Aut } G$. तो T , 1–1 आच्छादक G से G.

इस प्रकार T, का क्रमचय G.

$\therefore$ $T \in A(G)$. इसलिए, Aut $G \subseteq A(G)$.

माना $T_1, T_2 \in \text{Aut } G$.

तो $(T_1\ T_2)(xy) = T_1(T_2(xy))$

$= T_1(T_2(x)T_2(y))$ जहाँ T_2 समरूपक है।

$= T_1(T_2(x))T_1(T_2(y))$ जहां T_1 समरूपक है।

$= (T_1T_1)(x).(T_1T_2)(y)$ सभी $x, y \in G$ के लिए।

$\therefore$ $T_1\ T_2$, G में G तक समरूपता है।

पुनः $(T_1T_2)\ (x) = (T_1\ T_2)\ (y)$

$\Rightarrow$ $T_1\ (T_2\ (x)) = (T_1\ (T_2\ (y))$

$\Rightarrow$ $T_2\ (x) = T_2\ (y)$ क्योंकि T_1, 1–1 है।

$\Rightarrow$ $x = y$ क्योंकि T_2, 1–1 है।

$\therefore$ T_1T_2, 1–1 है।

माना $x \in G$. चूंकि $T_1 : G \to G$ आच्छादक है $\exists\ y \in G$, इस प्रकार $T_1(y) = x$.

पुनः जहां $T_2 : G \to G$ आच्छादक है, $\exists\ z \in G$, इस प्रकार $y = T_2\ (z)$

$\Rightarrow T_1(T_2\ (z)) = x$

$\Rightarrow (T_1\ T_2)(z) = x$

$\therefore$ T_1T_2 भी आच्छादक है।

तभी, $T_1T_2 \in \text{Aut } G$.

माना $T \in \text{Aut } G$. तो T , 1–1 आच्छादक है। $\Rightarrow$ T व्युत्क्रमणीय (Invertible) है और,

$T^{-1} : G \to G$, इस प्रकार $T^{-1}\ (x) = y \Leftrightarrow T(y) = x$

जैसे $TT^{-1} = I = T^{-1}\ T$

T^{-1} है 1–1 जैसे $T^{-1}\ (x_1) = T^{-1}\ (x_2)$

$\Rightarrow$ $TT^{-1}\ (x_1) = TT^{-1}\ (x_2)$

$\Rightarrow$ $I(x_1) = I\ (x_2)$

$\Rightarrow$ $x_1 = x_2$

माना $x \in G$ तो $y = T(x) \in G$

$\therefore$ $T^{-1}(y) = T^{-1}\ (T\ (x)) = (T^{-1}T)\ x = x$

$\therefore$ T^{-1} आच्छादक हैं।

माना $T^{-1}\ (xy) = z$ तो $T(z) = xy$

माना $T^{-1}\ (x) = x_1,\ T^{-1}\ (y) = y_1$

टिप्पणी

तो $x = T(x_1),\ y = T(y_1)$

$\Rightarrow T(z) = xy = T(x_1)\ T(y_1) = T(x_1 y_1)$

जहां T समरूपता है।

$\therefore \quad z = x_1 y_1$ जहां $T,\ 1 - 1$ है।

तभी $T^{-1}(xy) = z = x_1 y_1 = T^{-1}(x)\ T^{-1}(y)$ सभी $x, y \in G$ के लिए

$\Rightarrow T^{-1}$ समरूपता है।

इस प्रकार $T^{-1} \in \text{Aut}\, G$

इसी कारण Aut G, $A(G)$ का एक उप समूह है।

(इस प्रकार Aut G से समूह निर्मित होता है)

4.2.1 आन्तरिक स्वाकारिता

आन्तरिक स्वाकारिता, वलय अथवा बीजगणित का एक स्वाकारिता समूह है तथा यह साधारणतया निर्धारित अवयव के संयुग्मित क्रियाओं (Conjugation Action) द्वारा प्रदर्शित होता है जिसे निर्धारित अवयव कहा जाता है। इन आन्तरिक स्वाकारिता से स्वाकारिता समूह के उपसमूह का निर्माण होता है एवं इस उपसमूह द्वारा स्वाकारिता समूह के भागफल से बाह्य स्वाकारिता समूह की अवधारणा बनती है। आन्तरिक स्वाकारिता ऐसा कोई स्वाकारिता है जो संयुग्मन से उत्पन्न होता है। समूह G का स्वाकारिता आन्तरिक होगा यदि एवं केवल तभी जब यह G अंतर्विष्ट (Containing) प्रत्येक समूह तक विस्तारित हो।

$g \in G$ मान लें तो $T_g : G \to G$ को इस प्रकार परिभाषित करें कि

$$T_g(x) = gxg^{-1} \quad \text{सभी } x \in G$$

तो T_g, 1–1 है जैसे

मान लें $T_g(x) = T_g(y)$

$\Rightarrow \quad gxg^{-1} = gyg^{-1}$

$\Rightarrow \quad x = y.$

माना $x \in G.$ तो $g^{-1} xg \in G.$

एवं $T_g(g^{-1} xg) = g(g^{-1} xg)\, g^{-1} = x$

$\therefore \quad T_g$ आच्छादक (Onto) है।

$$T_g(xy) = g(xy)\, g^{-1}$$
$$= (gxg^{-1})\ (gyg^{-1})$$
$$= T_g(x)\ T_g(y) \text{ सभी } x, y, \in G \text{ के लिए।}$$

इसी कारण T_g, G का स्वाकारिता है एवं इसे G का आन्तरिक स्वाकारिता कहा जाता है।

प्रमेय 4.2: $I(G)$ के समस्त आन्तरिक स्वाकारिता का समुच्चय G, Aut G का उपसमूह है।

टिप्पणी

प्रमाण: $T_e \in I(G)$ जहाँ e, G के तत्समक है।

$\therefore \quad I(G) \neq \varphi$

$T_{g_1}, T_{g_2} \in I(G)$ मानें।

तो $T_{g_1} T_{g_2}(x) = T_{g_1}(g_2 x g_2^{-1}) = g_1 g_2 \, x \, g_2^{-1} \, g_1^{-1}$

$= (g_1 g_2) \, x \, (g_1 g_2)^{-1}$

$= T_{g_1 g_2}(x)$ समस्त $x \in G$ हेतु

$\therefore \; T_{g_1} T_{g_2} = T_{g_1 g_2} \in I(G)$

माना $T_g \in I(G)$ हो तो $T_g \, T_{g-1} = T_e = I$ (क्योंकि $T_e(x) = exe^{-1} = x$ सभी $x \in G$ के लिए।)

एवं $T_{g-1} \, T_g = I$

$\therefore \qquad T_{g-1} = (T_g)^{-1} \Rightarrow (T_g)^{-1} \in I(G)$

अतः Aut G, $I(G)$ का एक उप समूह है।

वस्तुतः $I(G)$, Aut G में सामान्य (Normal) है।

प्रश्न तब उत्पन्न होता है, जब $T_{g_1} = T_{g_2}$?

मान लें कि $T_{g_1} = T_{g_2}$

तो $T_{g_1}(x) = T_{g_2}(x)$ सभी $x \in G$ के लिए।

$\Leftrightarrow \quad g_1 \, x \, g_1^{-1} = g_2 \, x \, g_2^{-1}$ सभी $x \in G$ के लिए।

$\Leftrightarrow \quad g_2^{-1} \, g_1 \, x = x \, g_2^{-1} \, g_1$ सभी $x \in G$ के लिए।

$\Leftrightarrow \quad g_2^{-1} \, g_1 \in Z(G)$

$\Leftrightarrow \quad g_1 Z(G) = g_2 Z(G)$

$\therefore \quad T_{g_1} = T_{g_2} \Leftrightarrow g_1 Z(G) = g_2 Z(G)$

प्रमेय 4.3: $\dfrac{G}{Z(G)} \cong I(G)$

प्रमाण: $\theta : \dfrac{G}{Z(G)} \to I(G)$ को इस प्रकार परिभाषित करें कि $\theta(g\,Z(G)) = T_g$

θ इस प्रकार सुपरिभाषित है $g_1 Z(G) = g_2 Z(G) \quad \Rightarrow g_2^{-1} \, g_1 \in Z(G)$

$\Rightarrow \quad T_{g_1} = T_{g_2}$ (जैसी कि परिचर्चा पहले की जा चुकी है)।

$\Rightarrow \quad \theta(g_1 Z(G)) = \theta(g_2 Z(G))$

θ है 1–1 जहां $\theta(g_1 Z(G)) = \theta(g_2 Z(G))$

$\Rightarrow \quad T_{g_1} = T_{g_2}$

$\Rightarrow \quad g_2^{-1} \, g_1 \in Z(G)$

$\Rightarrow \quad g_1 Z(G) = g_2 Z(G)$

टिप्पणी

θ आच्छादक है जैसे $T_g \in I(G) \Rightarrow g \in G$

और $gZ(G) \in \frac{G}{Z(G)}$ इस प्रकार, $\theta(gZ(G)) = T_g$

भी $\theta(g_1 Z(G)\, g_2(Z(G)) = \theta(g_1 g_2 Z(G))$

$= T_{g_1} T_{g_2}$

$= T_{g_1} T_{g_2}$

$= \theta(g_1 Z(G))\theta(g_2 Z(G))$

अतः θ समरूपता है एवं इसी कारण तुल्याकारिता है।

यदि G परिमित समूह हो तो $o(Z(G))$ = परिमित।

$\therefore\ o\left(\frac{G}{Z(G)}\right) = \frac{o(G)}{o(Z(G))}$, लेकिन $o\left(\frac{G}{Z(G)}\right) = o(I(G))$

$\therefore\quad o(I(G)) = \frac{o(G)}{o(Z(G))}$.

ध्यान दे : प्रमेय 4.3 को निम्नानुसार भी सिद्ध किया जा सकता है,

$\varphi : G \to I(G)$ को इस प्रकार परिभाषित करें कि समस्त $g \in G$ हेतु $\varphi(g) = T_g$

तो φ आच्छादक समरूपता है। दर्शायें कि $\text{Ker}\,\varphi = Z(G)$, तो $\frac{G}{\text{Ker}\,\varphi} \cong I(G)$

उदाहरण 4.1: माना G अपरिमित चक्रीय समूह (Infinite Cyclic Group) हो तो Aut G को निर्धारित करें।

हलः $G = < a >$ व $T \in \text{Aut}\, G$ मानें तो हम दर्शाते हैं कि $G = < Ta >$

$x \in G$ हो तो चूँकि T आच्छादक है $\exists\, y \in G$ इस प्रकार, $x = T(y)$

$y \in G \Rightarrow y = a^r$, r के कुछ पूर्णांक है।

$\therefore\quad x = Ty = Ta^r = (Ta)^r$

$\therefore\quad Ta$, G के उत्पन्नकर्ता है।

परन्तु G में दो ही उत्पन्नकर्ता हैं: a व a^{-1}

$\therefore\quad Ta = a$ या $Ta = a^{-1}$.

T को इस प्रकार परिभाषित करें कि,

$o(\text{Aut}\, G) \le 2$

परिभाषित $T : G \to G$ इस प्रकार,

$T(x) = x^{-1}$

तो $T \in \text{Aut}\, G$

और भी $T \ne I$ as $T = I \Rightarrow T(x) = x$ सभी x के लिए।

$\Rightarrow\quad x^{-1} = x$ सभी $x \Rightarrow a^{-1} = a \Rightarrow a^2 = e$ के लिए।

$\Rightarrow\ o(a)$ परिमित है जो कि एक विरोधाभास है।

टिप्पणी

अतः $T \neq I$। इस प्रकार G में कम से कम दो स्वाकारिता हैं।

$\therefore o(\text{Aut } G) \geq 2$

$\Rightarrow o(\text{Aut } G) = 2.$

वस्तुतः Aut $G = \{I, T \mid T(x) = x^{-1}$ सभी $x \in G\}$ के लिए।

चूँकि $o(\text{Aut } G) = 2$, Aut G का एक चक्रीय समूह कोटि 2 है एवं चूँकि कोटि n का कोई चक्रीय समूह Zn (योग मापांक (Addition Module) n के अधीन समूह) से तुल्याकारिक है तो Aut $G \cong \mathbf{Z}_2$

(**ध्यान दें**: यहाँ G में बहुत छोटी कोटि है जबकि G बहुत बड़ी कोटि का है)।

उदाहरण 4.2: n कोटि G का परिमित चक्रीय समूह हो तो Aut G निर्धारित करें।

हल: माना $G = < a >, o(G) = o(a) = n$, $T \in \text{Aut } G$ हो तो उदाहरण 4.1 के अनुरूप $G = < Ta >$, किन्तु G में केवल $\varphi(n)$ उत्पन्न कारक हैं, इसीलिये T में केवल $\varphi(n)$ विकल्प चयन होंगे।

अतः $.o(\text{Aut } G) \leq \varphi(n)$

$T_m : G \to G$ को इस प्रकार परिभाषित करें कि,

$T_m(x) = x^m$, $(m, n) = 1$, $1 \leq m < n$

तो $T_m \in \text{Aut } G$ (सत्यापित करें)।

यदि $T_r = T_s$, तो $T_r(a) = T_s(a)$

$\Rightarrow \quad a^r = a^s$. माना $r > s$

$\Rightarrow \quad a^{r-s} = e$

$\Rightarrow \quad o(a) \mid r - s$

$\Rightarrow \quad n \mid r - s$

$\Rightarrow \quad n \leq r - s < n$, एक विरोधाभास (Contradiction) है

$T_r \neq T_s$ सभी r के लिए, s $(r \neq s)$, $1 \leq r, s \leq m$ जहाँ $(r, n) = (s, n)$

इससे G के कम से कम $\varphi(n)$ स्वाकारिता आते हैं।

$o(\text{Aut } G) \geq \varphi(n)$

$\Rightarrow o(\text{Aut } G) = \varphi(n)$

वस्तुतः Aut $G = \{T_m \mid T_m(x) = x^m, (m, n) = 1\}$
$1 \leq m < n$

इस प्रकार हम पाते हैं $o(\text{Aut } G) = \varphi(n)$

हम दर्शाते हैं कि $G \cong U_n$ समूह के पूर्णांक गुणन के मापां (Modulo) क में n

$\theta : \text{Aut } G \to U_n$ को इस प्रकार परिभाषित करें कि,

$\theta(T_m) = m$, $1 \leq m < n$, $(m, n) = 1$

तो $\theta(T_r) = \theta(T_s)$

$\Rightarrow \quad r = s$

$\Rightarrow \quad T_r = T_s \Rightarrow \theta$ is 1–1

टिप्पणी

दिया हुआ है, $m \in U_n$, $1 \le m < n$, $(m, n) = 1$,

$\exists\ T_m \in \text{Aut}\ G$, इस प्रकार $\theta(T_m) = m$

दर्शाया गया है कि θ आच्छादक है।

θ समरूपता है यह दर्शाने के लिये हम सिद्ध करते हैं,

$\theta(T_r T_s) = \theta(T_r) \otimes \theta(T_r)$

अब $1 \le r, s < n, (r, n) = 1 = (s, n)$ के लिये।

$T_r T_s(x) = T_r(x^s) = (x^s)^r = x^{r \otimes s} = T_{r \otimes s}(x)$

$\Rightarrow\ T_r T_s = T_{r \otimes s}$

$\Rightarrow\ \theta(T_r T_s) = \theta(T_{r \otimes s})$

$= r \otimes s = \theta(T_r) \otimes \theta(T_s).$

अतः θ एक समरूपता है एवं इसलिये तुल्याकारिता है।

इसी कारण $\text{Aut}\ G \cong U_n$

इससे $\text{Aut}\ G$ पूर्णतया निर्धारित हो गया।

ध्यान दें: उदाहरणों 4.1 व 4.2 द्वारा कोटि 3 व 4 के चक्रीय समूहों एवं अपरिमित चक्रीय समूहों में कोटि 2 के तुल्याकारिक है परन्तु समूहों अपने आप में गैर–तुल्याकारिक हैं। $\text{Aut}\ G$ एबेलियन है जब भी G चक्रीय हों।

उदाहरण 4.3: यदि $f: G \to G$ इस प्रकार हो कि $f(x) = x^n$

एक तुल्याकारिक है जहाँ n कोई निर्धारिता पूर्णांक है, प्रदर्शित करें कि

$a^{n-1} \in Z(G)$ सभी $a \in G$ के लिए।

हल: माना कि $a \in G$ कोई अवयव है।

माना कि $f(a^{-n}\ x\ a^n) = (a^{-n}\ x\ a^n)^n$

$= a^{-n}\ x^n\ a^n$

$= f(a^{-1})\ f(x)\ f(a)$

$= f(a^{-1}\ xa)$

$\therefore\ \ a^{-n}\ x\ a^n = a^{-1}\ xa$ क्योंकि f एक–एक है।

$\therefore\ \ \ xa^{n-1} = a^{n-1}\ x$ सभी x के लिए

इस प्रकार $a^{n-1} \in Z(G)\ \ \forall\ a \in G.$

उदाहरण 4.4: माना कि $f: G \to G$ एक समरूपक हो (अर्थात् f, G का अंतराकारिता (Endomorphism) है) मान लो कि f, G) के प्रत्येक आंतरिक स्वाकारिता से क्रमविनिमय करता है, तो दर्शाएं कि,

(*i*) $K = \{x \in G \mid f^2(x) = f(x)\}$, G का सामान्य उपसमूह है।

(*ii*) G/K एबेलियन है।

हल: (*i*) $f^2(e) = f(f(e)) = f(e) \Rightarrow\ e \in K$ (जहाँ e, G के तत्समक (Identity) है।)

$\therefore\ \ K \ne \varphi$

टिप्पणी

माना $x, y \in K$ तो $f(x) = f^2(x)$

$f(y) = f^2(y)$

इसलिए $f^2(xy^{-1}) = f(f(xy^{-1}))$

$= f(f(x)\, f(y^{-1})) = f(f(x)\, f(y)^{-1})$

$= f^2(x)\, f(f(y))^{-1}$

$= f^2(x)\, f^2(y)^{-1}$

$= f(x)\, f(y^{-1})$

$= f(xy^{-1})$

$\Rightarrow xy^{-1} \in K.$

इस प्रकार K, G का उपसमूह है।

माना $g \in G, x \in K$. मान लें कि,

$f^2(gxg^{-1}) = f(f(gxg^{-1}))$

$= f(f T_g(x))$

$= f(T_g f(x))$ क्योंकि $f T_g = T_g f$

$= f(g)\, f^2(x)\, f(g^{-1})$

$= f(g)\, f(x)\, f(g^{-1})$ क्योंकि $x \in K \Rightarrow f(x) = f^2(x)$

$= f(gxg^{-1})$

$\therefore \quad gxg^{-1} \in K$ सभी $x \in K$ के लिए, $g \in G$

$\therefore$ K, G का सामान्य उपसमूह है।

(*ii*) अब $\frac{G}{K}$ एबेलियन है।

$\Leftrightarrow KxKy = KyKx$ सभी x के लिए, $y \in G$

$\Leftrightarrow Kxy = Kyx$ सभी $x, y \in G$ के लिए।

$\Leftrightarrow xyx^{-1}y^{-1} \in K$ सभी $x, y \in$ के लिए।

अब, $f^2(xyx^{-1}\, y^{-1}) = f(f(xyx^{-1}\, y^{-1}))$

$= f(f(T_x yy^{-1})) = f(f T_x y))\, f(y^{-1}))$

$= f(T_x f(y))\, f(y)^{-1} = f(x)\, f(y)\, x^{-1})\, f(y)^{-1})$

$= f(x\, T_{f(y)}\, x^{-1}) = f(x)\, f\, T_{f(y)}\, x^{-1}$

$= f(x)\, T f_{(y)}\, f(x^{-1}) = f(x)\, f(y)\, f(x^{-1})\, f(y)^{-1}$

$= f(x)\, f(y)\, f(x^{-1})\, f(y^{-1})$

$= f(xyx^{-1}\, y^{-1})$

$\therefore \quad xyx^{-1}\, y^{-1} \in K$

$\Rightarrow \frac{G}{K}$ एबेलियन है।

उदाहरण 4.5: किसी पूर्णांक $a > 1, n > 0$ के लिये दर्शायें कि $n \mid \varphi(a^n - 1)$

टिप्पणी

हल: $G = < b >$ इस प्रकार हो कि $o(G) = o(b) = a^n - 1$ तो $T : G \to G$ को इस प्रकार परिभाषित करें कि $T(x) = x^a$

चूँकि $(a , a^n - 1) = 1,\ T \in \text{Aut } G$

और भी $T^2(x) = T(T(x))$

$= T(x^a) = (x^a)^a = x^{a^2}$

साधारणतया $T^r(x) = x^{a^r}$

$\therefore \quad T^n(x) = x^{a^n} = x$ सभी $x \in G$ के लिए।

(जैसे $x^{o(G)} = e \Rightarrow x^{a^n - 1} = e \Rightarrow x^{a^n} = x$)

$\therefore \quad T^n = 1$

यदि $T^m = 1$ तो $T^m(b) = b$

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

$\Rightarrow o(b) \mid (a^m - 1)$

$\Rightarrow a^n - 1 \mid (a^m - 1) \Rightarrow a^n - 1 \le (a^m - 1)$

$\Rightarrow a^n \le a^m \Rightarrow n \le m$

$\therefore \quad o(T) = n$

और भी $o(\text{Aut } G) = \varphi(a^n - 1)$, उदाहरण 4.2 से,

$T \in \text{Aut } G \Rightarrow o(T) \mid o(\text{Aut } G)$

$\Rightarrow n \mid \varphi(a^n - 1).$

4.2.2 स्वाकारिता समूह एवं इनके क्रमविनिमय

G के उपसमूह H को G का अभिलाक्षिणिक उपसमूह कहा जाता है यदि,

$T(H) \subseteq H$ सभी $T \in \text{Aut } G$ के लिए

माना G कोटि 4 का कोई चक्रीय समूह हो $G = \{e, a, a^2, a^3\}$

तो $\text{Aut } G = \{I, T\}$ जहाँ समस्त $x \in G$ के लिये $x \in G$ उदाहरण 4.2 से।

माना $H = \{e, a^2\} \le G$

$\therefore \quad I(H) = \{I(e), I(a^2)\} = H$

$T(H) = \{T(e), T(a^2)\} = \{e, a^6 = a^2\} = H$

अतः H, G का एक अभिलाक्षणिक उपसमूह है।

उदाहरण 4.6: दर्शाएँ कि समूह G का अभिलाक्षणिक उपसमूह G का सामान्य उपसमूह है। क्या इसका विलोम वास्तविक है?

हल: H, G का अभिलाक्षणिक उपसमूह हो तो $g \in G, h \in H$ मान लेते हैं।

अब $T(H) \subseteq H, \quad \forall\ T \in \text{Aut } G$

विशेषतया $T_g(H) \subseteq H$, T_g आन्तरिक स्वाकारिक है।

टिप्पणी

इस प्रकार $ghg^{-1} = T_g(h) \in T_g(H) \subseteq H$

अतः H, G का सामान्य उपसमूह है।

वैसे इसका विपरीत वास्तविक नहीं है।

G को कोटि 4 का एबेलियन समूह मानें।

तो $G = \{e, a, b, ab \mid a^2 = e = b^2 = (ab)^2, ab = ba\}$

$H = \{e, a\} \leq G$ मानने पर H, G का सामान्य उपसमूह है क्योंकि G में H का निर्देशांक (Index) 2 है।

$T : G \to G$ इस प्रकार मानें कि $T(a) = b, T(b) = a, T(ab) = ab, T(e) = e$

तो $T \in \text{Aut } G$ किन्तु $T(a) = b \notin H \Rightarrow H$, G का अभिलाक्षणिक उपसमूह नहीं है।

उदाहरण 4.7: दर्शायें कि यदि $o(\text{Aut } G) > 1$ तो $o(G) > 2$

हल: मान लेते हैं कि $o(G) \leq 2$

यदि $o(G) = 1$ तो G में केवल एक ही स्वाकारिता है: अर्थात तत्समक मानचित्र (Identity Map) I है, तो यह विरोधाभासी है $o(\text{Aut } G) > 1$

यदि $o(G) = 2$, तो $G = \{e, a \mid a^2 = e, a \neq e\}$

चूँकि $o(\text{Aut } G) > 1, \exists\ T \in \text{Aut } G$ इस प्रकार है कि $T \neq I$

$\therefore\ \exists\ x \in G$ इस प्रकार है $T(x) \neq x$ परन्तु $T(e) = e$

अतः $T(a)$, a होगा ही जो कि विरोधाभासी इस प्रकार है, कि $\exists\ x$

इसी कारण $T(x) \neq x$.

$\therefore \quad o(G) \neq 2$

इस प्रकार $o(G) > 2$.

उदाहरण 4.8: दर्शायें कि $\text{Aut } S_3 \cong S_3$

हल: $H = \{(12), (13), (23)\}$ मानें, अर्थात् H, S_3 का उपसमुच्चय है जिसमें $G = S_3$ में कोटि 2 के समस्त अवयव अंतर्विष्ट हैं।

माना $T \in \text{Aut } G$ कोई अवयव (Member) हो तो $T : G \to G$ एक तुल्याकारिता है। चूँकि $H \subseteq G, T(h) \in G\ \forall\ h \in H$, $o(T(a)) = o(a)\ \forall\ a \in G$, इस प्रकार यदि $h \in H$ कोई सदस्य हो तो $o(h) = 2$ एवं इसलिये $o(T(h)) = o(h) = 2$, अर्थात् $T(h) \in H$ है $\forall\ h \in H$।

अतः $T : H \to H$ एक मानचित्रण है (अर्थात् T, H तक परिमित हो सकता है एवं हम H के प्रति T के इस परिसीमन को T से इंगित करते हैं)। चूँकि T' अतः $T : G \to G$ 1–1 होगा। पुनः चूँकि H परिमित है, $T' : H \to H$ 1–1 है यह आच्छादक भी होगा एवं इसी कारण T' H पर एक क्रमचय है, अर्थात् $T' \in A(H)$

$\theta : \text{Aut } G \to A(H)$ को इस प्रकार परिभाषित करें कि $\theta(T) = T'$

टिप्पणी

तो θ इस प्रकार सुपरिभाषित है $T_1 = T_2 \Rightarrow T_1' = T_2' \Rightarrow \theta(T_1) = \theta(T_2)$

और भी θ है 1–1, क्योंकि $\theta(T_1) = \theta(T_2)$

$\Rightarrow T_1' = T_2'$

$\Rightarrow T_1'(h) = T_2'(h) \qquad \forall\ h \in H$

$\Rightarrow T_1(h) = T_2(h) \qquad \forall\ h \in H$

अर्थात् T_1 व T_2, H के निर्धारित अवयव बन रहे हैं। हम दर्शाते हैं कि ये G के समस्त अवयव होंगे।

अब $T_1[(123)] = T_1[(13)(12)] = T_1(13)\,T_1(12) = T_2(13)\,T_2(12)$

$= T_2(13)(12) = T_2[(123)]$

इसी प्रकार $T_1[(132)] = T_2[(132)]$ एवं निश्चय ही $T_1(I) = T_2(I)$

इस प्रकार T_1 व T_2, G के समस्त अवयवों पर हैं एवं इसलिये $\theta(T_1) = \theta(T_2)$

$\Rightarrow T_1 = T_2 \Rightarrow \theta$, 1–1 है।

चूँकि $\theta, \text{Aut}\, G \to \theta(\text{Aut}\, G)$ से आच्छादक होगा। $o(\text{Aut}\, G) = o(\theta(\text{Aut}\, G))$

परन्तु $\theta(\text{Aut}\, G) \subseteq A(H)$

$\Rightarrow o((\theta(\text{Aut}\, G)) \le o(A(H)) = \underline{|3} = 6$

अर्थात् $o(\text{Aut}\, G) \le 6$

चूँकि $G \cong I(G)$ जब $G = S_3$

$o(I(G)) = o(G) = 6$

परन्तु $I(G) \le \text{Aut}\, G$ एवं इसलिये $6 \le o(\text{Aut}\, G)$

इसी कारण $o(\text{Aut}\, G) = 6$

$\Rightarrow \text{Aut}\, G = I(G)$

तथा $\text{Aut}\, S_3 \cong S_3$

अपनी प्रगति जांचिए

1. यदि G ऐसा समूह हो जिसमें किसी $g \in G$ हेतु $g^2 \neq e$ है, तो दर्शायें कि G में गैर–नगण्य स्वाकारिता है।
2. स्वाकारिता से क्या अभिप्राय है?

4.3 संयुग्मित सम्बन्ध

समूह के दो अवयव a व b संयुग्मित कहलायेंगे यदि समूह में अवयव g इस प्रकार हो कि $b = g^{-1}ag$। यह समतुल्यता सम्बन्ध है जिसके समतुल्यता वर्गों को संयुग्मित वर्ग कहा जाता है।

समान संयुग्मित वर्ग के अवयवों (Members) को समूह संरचना के प्रयोग से अलग–अलग नहीं पहचाना जा सकता एवं इसीलिये कई विशेषताएं साझा होते हैं।

गैर–एबेलियन समूहों के संयुग्मित वर्गों का अध्ययन इनकी संरचना के अध्ययन के लिये आधारभूत है। किसी एबेलियन समूह के लिये प्रत्येक संयुग्मित वर्ग एक अवयव अंतर्विष्ट समुच्चय है, जिसे एकल समुच्चय (Singleton Set) भी कहते हैं।

टिप्पणी

परिभाषाः माना G एक समूह $a, b \in G$ हो तो $\sim G$ पर सम्बन्ध $a \sim b \Leftrightarrow \exists\, c \in G$ को निम्नानुरूप से परिभाषित करें:

$a \sim b \Leftrightarrow \exists\, c \in G$ इस प्रकार कि $a = c^{-1} bc$

यह सरलता से देखा जा सकता है कि $\sim$, G पर एक समतुल्यता सम्बन्ध है। यदि $a \sim b$ तो हम कहते हैं कि a, b से संयुग्मित है (अथवा a, b संयुग्मित हैं एवं सम्बन्ध $\sim$ को G पर संयुग्मित सम्बन्ध कहा जाता है)।

यदि $cl(a)$ से G में a का समतुल्यता वर्ग इंगित होता हो तो $cl(a)$ को $\sim$ में G का संयुग्मित वर्ग कहा जाता है। चूँकि $\sim$, G पर एक समतुल्यता सम्बन्ध हो तो यह G को असंबद्ध समतुल्यता वर्गों में विभाजित करता है।

अतः $G = \underset{a \in G}{\cup} cl(a)$, जहाँ,

$$cl(a) = \{x \in G \mid x \sim a\}$$
$$= \{x \in G \mid x = y^{-1} ay, y \in G\}$$
$$= \{y^{-1} ay \mid y \in G\}$$

G में a के समस्त संयुग्मित का समुच्चय,

ध्यान दें:

(*i*) $cl(a) = \{a\} \Leftrightarrow a \in Z(G)$

मान लें कि $cl(a) = \{a\}$. तो $y^{-1}ay = a$ सभी $y \in G$ के लिए।

$\therefore \quad ya = ay$ सभी $y \in G$ के लिए।

$\therefore \quad a \in Z(G)$

इसके विपरीत माना $a \in Z(G), x \in cl(a)$ कोई अवयव हो तो किसी $y \in G$ के लिये $x = y^{-1}ay$

$\Rightarrow x = ay^{-1} y$ (As $a \in Z(G)$

$\Rightarrow x = a \Rightarrow cl(a) = \{a\}$.

(*ii*) G एबेलियन है $\Leftrightarrow cl(a) = \{a\}$ सभी $a \in G$ के लिए।

G एबेलियन है $\Leftrightarrow G = Z(G)$

$\Leftrightarrow a \in Z(G)$ सभी $a \in G$ के लिए।

$\Leftrightarrow cl(a) = \{a\}$ सभी $a \in G$ के लिए।

हम G में संयुग्मित वर्गों की संख्या को $k(G)$ अथवा k द्वारा इंगित करेंगे। ध्यान दे कि प्रकरण (*ii*) में $o(G) = k \Leftrightarrow G$ एबेलियन है।

अवयव $a \in G$ के **सामान्यीकरण** को समुच्चय होने के लिये परिभाषित किया गया है।

टिप्पणी

$N(a) = \{x \in G \mid xa = ax$ सभी $x \in G\}$ के लिए जैसे $N(a) \leq G$.

यह दर्शा सकता है कि $N(a) = G \Leftrightarrow a \in Z(G)$

$N(a) = G \Leftrightarrow g \in N(a)$ सभी $g \in G$ के लिए।

$\Leftrightarrow ga = ag$ सभी $g \in G$ के लिए।

$\Leftrightarrow a \in Z(G)$.

अतः ध्यान दे कि प्रकरण (i) से $N(a) = G \Leftrightarrow cl(a) = \{a\}$.

उदाहरण 4.9: मान लें कि $a \in G$ में G में दो ही संयुग्मित हैं तो दर्शायें कि $N(a)$ G का सामान्य उपसमूह है।

हल: माना $a, g^{-1}ag$, G में a के दो संयुग्मित हैं। हम दर्शाते हैं कि,

$G = N(a) \cup N(a)g$

माना $x \in G$. $x^{-1}ax$ मानने पर तो $x^{-1}ax = a$ या $g^{-1}ag$.

यदि $x^{-1}ax = a$, तो $xa = ax \Rightarrow x \in N(a)$

यदि $x^{-1}ax = g^{-1}\ ag$, तो $xg^{-1}a = axg^{-1}$

$\Rightarrow xg^{-1} \in N(a)$

$\Rightarrow x \in N(a)g$

$\therefore \quad G = N(a) \cup N(a)g$....

तथा इस प्रकार $N(a)$ में G का निर्देशांक 2 है, जिससे प्रदर्शित हो रहा है कि $N(a)$, G में सामान्य उपसमूह है।

उदाहरण 4.10: माना G परिमित समूह एवं x, y के संयुग्मित अवयव हों तो दर्शायें कि सुनिश्चित अवयवों G, $g \in G$ की संख्या इस प्रकार $g^{-1}xg = y$, $o(N(x))$ है।

हल: माना $g = g_1, g_2 ..., g_n$ G के सुनिश्चित अवयव इस प्रकार हैं कि $g_i^{-1}xg_i = y$

माना $S = \{g = g_1, g_2..., g_n\}$

हम दर्शाते हैं कि $S = N(x)g$

मान लें कि $s \in S$ तो $s = g_i$ कुछ i के लिए, $1 \leq i \leq n$

यदि $s = g_1 = g$ तो $s = g = eg \in N(x)\ g$

यदि $s \neq g_1$ तो $s = g_i$, $i \neq 1$

एवं $g^{-1}\ xg = g_i^{-1}\ xg_i$

$\Rightarrow g_ig^{-1}\ x = xg_ig^{-1}$

$\Rightarrow g_ig^{-1} \in N(x)$

$\Rightarrow g_i \in N(x)$

$\Rightarrow s \in N(x)g$

और $S \subseteq N(x)g$

पुनः $z \in N(x)g \Rightarrow z = hg, \quad h \in N(x)$

$\Rightarrow z^{-1}\ xz = g^{-1}\ h^{-1}\ xhg$

टिप्पणी

$\Rightarrow z^{-1} xz = g^{-1} xg$ जैसे $xh = hx$

$\Rightarrow z^{-1} xg = y$

$\Rightarrow z = g_i$ किसी भी i के लिए।

$\Rightarrow z \in S$

$\Rightarrow N(x)g \subseteq S$

इसी कारण $S = N(x)g$

एवं इस प्रकार $(S) = o(N(x)g) = o(N(x))$

ध्यान दे: जैसे $gg_i^{-1} x = xgg_i^{-1}$ सभी $i = 1,..., n$ के लिए।

$gg_i^{-1} \in N(x)$ सभी i के लिए।

$\Rightarrow N(x)g = N(x)g_i$ सभी i के लिए)।

उदाहरण 4.11: कोटि p^2 (p = अभाज्य (Prime)) का समूह एबेलियन है।

हल: मान लें कि $o(G) = p^2$ व G गैर–एबेलियन है तो $Z(G) \neq G$. इसलिए $\exists\ a \in G$ इस प्रकार कि $a \notin Z(G)$ एवं पूर्ववर्ती समस्या में प्रदर्शित अनुसार $N(a) \subsetneq G$

पुनः $Z(G) \subseteq N(a)$ सदैव परन्तु चूँकि $a \notin Z(G), Z(G) \subsetneq N(a)$

अब, $o(Z(G) \mid o(G) = p^2 \Rightarrow o(Z(G)) = 1, p$ या p^2

किन्तु $o(Z(G)) > 1$

एव $o(Z(G)) = p^2 \Rightarrow Z(G) = G$ जो कि वास्तविक नहीं है।

इसी कारण $o(Z(G)) = p$

पुनः $o(N(a)) \mid o(G) = p^2$ देता है $o(N(a)) = 1, p$ या p^2

चूँकि $N(a) \neq G, \quad o(N(a)) \neq p^2$ भी।

अतः $Z(G) \subsetneq N(a) \Rightarrow o(N(a)) > 1$

$o(N(a)) = p$

किन्तु इसका तात्पर्य हुआ कि $Z(G) = N(a)$, जो एक विरोधाभास है।

इसी कारण G एबेलियन है।

प्रश्न यह उत्पन्न होता है कि कोटि p^3 (p = अभाज्य) का समूह एबेलियन है अथवा नहीं? इसका उत्तर 'नहीं' है क्योंकि चतुष्क समूह गैर–एबेलियन (Non-Abelian) है एवं इसमें कोटि 2^3 है। वस्तुतः समस्त अभाज्य p के लिये कोटि p^3 के गैर–एबेलियन समूह होते हैं।

उदाहरणार्थ मान ले कि $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} f \right.$ क्षेत्र (Field) a, b, c के तुल्यकारिक अवयव (Arbitary Elements) हैं, तो कोटि p^3, G का गैर–एबेलियन समूह है यदि F कोटि p का क्षेत्र है। इसे F पर हेइसेन्बर्ग समूह (Heisenberg Group) कहा जाता है। साधारणतया F पर हेइसेन्बर्ग समूह का कोटि $(o(F))^3$ होता है।

उदाहरण 4.12: p^3 कोटि F का गैर–एबेलियन समूह हो तो $o(Z(G))$ को एवं G के संयुग्मित वर्गों की K संख्या निर्धारित करें।

टिप्पणी

हल: चूँकि G गैर–एबेलियन है $\exists\, a \in G$ इस प्रकार कि $Z(G) \subsetneqq N(a) \subsetneqq G$ जैसा कि पूर्ववर्ती उदाहरणों में दर्शाया गया है।

अब $o(Z(G)) \mid o(G) = p^3 \Rightarrow o(Z(G)) = 1, p, p^2$ या p^3

इसी प्रकार, $o(N(a)) = 1, p, p^2$ या p^3

$o(Z(G)) \neq 1.$

$o(Z(G)) \neq p^3$ क्योंकि $Z(G) \neq G$

अतः $o(Z(G)) = p$ या p^2

इसी प्रकार $o(N(a)) = p$ or p^2 और जैसे $Z(G) \subsetneqq N(a)$

हम पाते हैं कि $o(Z(G)) = p$ और $o(N(a)) = p^2$

अब मान लें कि k संयुग्मित वर्गों की कुल संख्या है। चूँकि,

$$G = \bigcup_{a \in G} cl(a)$$

$$o(G) = \sum_{a \in G} (cl(a)) = \sum_{a \in Z(G)} o(cl(a)) + \sum_{a \notin Z(G)} o(cl(a))$$

अर्थात्, $p^3 = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$

चूँकि संयुग्मित वर्गों की संख्या जब $a \in Z(G), o(Z(G)) = p$ होती है।

$[a \in Z(G) \Leftrightarrow cl(a) = \{a\}$, अर्थात्, $o(cl(a)) = 1]$

अतः शेष वर्ग $k - p$ हैं, प्रत्येक कोटि का वर्ग दिए गए नियम अनुसार होगाः

$$o(cl(a)) = \frac{o(G)}{o(N(a))} = \frac{p^3}{p^2} = p$$

इसी कारण $p^3 = p + (k - p)p \Rightarrow k = p^2 + p - 1$

उदाहरण 4.13: मान लें कि G परिमित समूह है व $k(G)$ के संयुग्मित वर्गों की संख्या G_3 है। तो दर्शायें कि या तो G कोटि 3 का चक्रीय समूह है अथवा कोटि 6 (तुल्याकारिता तक) का गैर–एबेलियन समूह S_3 है।

हल: यदि G के समस्त तीन वर्ग एक लम्बाई के हों तो $o(G) = 3 \Rightarrow G$ कोटि 3 का चक्रीय समूह है। मान लें कि G में 1 से कम लम्बाई का एक वर्ग हो तो G गैर–एबेलियन है। C_1, C_2, C_3 तीन वर्ग हों।

मान लें कि $o(C_3) > 1$

यदि $o(C_1) = o(C_2) = 1$

तो $o(C_3) = n - 2$

जहाँ $n = o(G)$ परन्तु $o(C_3) = n - 2 \mid o(G) = n$

भी $n - 2 \mid n - 2$

$\therefore$ $n - 2 \mid n - (n - 2) = 2$

टिप्पणी

$\Rightarrow \quad n - 2 = 1$ या 2

$\Rightarrow n = 3$ या 4

किसी एक प्रकरण में G एबेलियन है।

(ऐसे $n = 3 \Rightarrow o(G) = 3$ = अभाज्य $\Rightarrow G$ चक्रीय है।

$\Rightarrow G$ एबेलियन है।

$n = 4 \Rightarrow o(G) = p^2 = 2^2 \Rightarrow G$ एबेलियन है)।

G इस प्रकार हमारे पास एक ही विकल्प बचता है कि 1 में केवल एक वर्ग लम्बाई 1 का है। $o(C_1) = 1, o(C_2) > 1, o(C_3) > 1$. $o(Z(G) = 1$ हो तो,

वर्ग समीकरण से, $n = o(G) = o(C_1) + o(C_2) + o(C_3)$

$= 1 + o(C_2) + o(C_3)$

किन्तु $\quad o(C_3) \mid o(G) = n, o(C_3) \mid o(C_3)$

$\Rightarrow o(C_3) \mid n - o(C_3) = 1 + o(C_2)$

$\Rightarrow o(C_3) \leq 1 + o(C_2)$

इसी प्रकार, $o(C_2) \leq 1 + o(C_3)$

यदि, $o(C_3) < 1 + o(C_2)$ और $o(C_2) < 1 + o(C_3)$

तो $\quad o(C_3) \leq o(C_2), o(C_2) \leq o(C_3)$

$\therefore \quad o(C_2) = o(C_3)$

$\therefore \quad o(C_3) \mid 1 \quad o(C_3) \Rightarrow o(C_3)\, 1 \Rightarrow o(C_3) = 1$, जो कि एक विरोधाभास है।

इस प्रकार या तो $o(C_3) = 1 + o(C_2)$ अथवा $o(C_2) = 1 + o(C_3)$

यदि $\quad o(C_3) = 1 + o(C_2)$

तो $\quad o(G) = 1 + o(C_2) + 1 + o(C_2)$

$\Rightarrow o(G) - 2\, o(C_2) = 2$

परन्तु $\quad o(C_2) \mid o(G)\,, o(C_2) \mid o(C_2) \Rightarrow o(C_2) \mid 2\, o(C_2)$

$\therefore \quad o(C_2) \mid o(G) - 2\, o(C_2) = 2$

$\therefore \quad o(C_2) = 2$ और $o(C_3) = 3$

अथवा $\quad o(G) = 6$

इसी प्रकार यदि $o(C_2) = 1 + o(C_3)$ तो $o(G) = 6$।

अतः G कोटि 6 का गैर–एबेलियन समूह है एवं इसलिये S_3 से तुल्याकारिक है।

उदाहरण 4.14: G कोई समूह हो एवं $e \neq a \in G$ इस प्रकार हो कि $o(a) =$ परिमित। मान लें कि G में दो ही संयुग्मित वर्ग हैं तो दर्शायें कि G कोटि 2 का एक परिमित समूह है।

हल: माना $e \neq b \in G$ हो। चूँकि G में दो ही संयुग्मित वर्ग हैं: $\{e\}$ व $cl(a).\, b \in cl(a)$ $\therefore b = g^{-1} ag$ । कुछ $g \in G$ के लिए $\therefore o(b) = o(a)$ कुछ G में $b \neq e$ के लिए।

मान लें कि $o(a) = mn,\ m > 1,\ n > 1$ तो $o(a^m) = m$

टिप्पणी

चूँकि G में समस्त गैर–एबेलियन अवयवों की कोटि समान है, $o(a^m) = mn$

अतः $n = mn \Rightarrow m = 1$ एक विरोधाभास है।

$\therefore \quad o(a) = p$ = अभाज्य

$\therefore \quad o(b) = p$ सभी $e \neq b \in G$ के लिए।

मान लें कि $p \neq 2$ तो $a^2 \neq e \Rightarrow a^2 \in cl(a)$

$\therefore \quad a^2 = g^{-1} ag$ G कुछ $g \in G$ के लिए।

$$\therefore \quad (a^2)^2 = (g^{-1} ag)^2$$
$$= g^{-1} a^2 g$$
$$= g^{-1} (g^{-1} ag) g$$
$$= g^{-2} ag^2$$

$$\therefore \quad a^{2^2} = g^{-2} ag^2$$

इस प्रकार हम प्राप्त करते हैं $a^{2^p} = g^{-p} ag^p$

चूँकि $o(g) = o(a) = p$

$$a^{2^p} = eae = a$$

$$\Rightarrow a^{2^p - 1} = e \Rightarrow o(a) = p \mid 2^p - 1$$

फ़र्मेट प्रमेय अनुरूप $p \mid 2^p - 2$

अतः $p \mid (2^p - 1) - (2^p - 2) = 1$ एक विरोधाभास है।

$\therefore \quad p = 2$

$\Rightarrow o(a) = 2$. इसलिए $o(b) = 2$ सभी $e \neq b \in G$ के लिए

G एबेलियन है।

अतः G में प्रत्येक संयुग्मित वर्ग लम्बाई 2 का है।

चूँकि G में दो ही वर्ग हैं, G की कोटि 2 है।

ध्यान दें: जिन $\exists$ अपरिमित समूहों में कोई गैर–नगण्य अवयव नहीं होता तो ऐसे समूहों में केवल 2 संयुग्मित वर्ग हैं, जो परिमित कोटि के हैं।

इसीलिये उपरोक्त समस्या में यह मान लेना आवश्यक है कि $\exists\, e \neq a \in G$ इस प्रकार है $o(a)$ = परिमित।

उदाहरण 4.15: सिद्ध करें कि कोटि 15 होने पर एबेलियन समूह चक्रीय है।

हल: मान लें कि G कोटि 15 युक्त एक समूह है। मान ले कि यह गैर–एबेलियन है, तो $Z(G) \neq G$

$\therefore o(Z(G)) = 1, 3$ अथवा 5 क्योंकि $o(Z(G)) \mid o(G) = 15$

यदि $o(Z(G)) = 3$ या 5, तो $o\left(\frac{G}{Z}\right) = 5$ या 3 = अभाज्य (Prime)

$\Rightarrow \frac{G}{Z(G)}$ चक्रीय (Cyclic) है G एबेलियन है जो कि विरोधाभासी हैं।

$\therefore \; o(Z(G)) = 1$

टिप्पणी

इस प्रकार लम्बाई एक का एक ही संयुग्मित वर्ग है। समस्त अन्य वर्ग लम्बाई 3 अथवा 5 के हैं क्योंकि वर्ग का कोटि $o(G) = 15$ विभाजित करता है। यदि समस्त अन्य वर्ग लम्बाई 3 के हों तो वर्ग समीकरण द्वारा $o(G) = 15 = 1 + 3k$ जो कि वास्तविक नहीं है।

इसीलिये लम्बाई 5 का एक वर्ग C है एवं यह लम्बाई 5 का केवल एक वर्ग है (वर्ग समीकरण से)

$x \in C$ हो तो $C = cl(x)$ एवं,

$$5 = o(C) = o(cl(x)) = \frac{o(G)}{o(N(G))} \Rightarrow o(N(x)) = 3$$

चूँकि $x \neq e$ व $x \in N(x)$, $o(x) \mid o(N(x)) = 3 \Rightarrow o(x) = 3$

इसके विपरीत हम मान लेते हैं कि $o(x) = 3$।

चूँकि $o(x) \mid o(N(x)), o(N(x)) = 3k$ जहाँ $k = 1$ अथवा 5 क्योंकि,

$o(N(x)) \mid o(G) = 15$।

यदि $o(x) = 3$ तो $o(N(x)) = 15 = o(G) \Rightarrow N(x) = G$

$\Rightarrow x \in Z(G) \Rightarrow x = e$ as $Z(G) = \{e\}$, जो एक विरोधाभास है।

$$\therefore \quad k = 1 \quad \Rightarrow o(N(x)) = 3$$

$$\Rightarrow o(cl(x)) = \frac{o(G)}{o(N(G))} = \frac{15}{3} = 5$$

$$\Rightarrow cl(x) = C$$

चूँकि C लम्बाई 5 का एकमात्र वर्ग है। चूँकि $x \in cl(x)$ हम पाते हैं $x \in C$

अतः कोटि 3 के अवयवों की संख्या 5 है जो कि एक विरोधाभास है क्योंकि कोटि p (p = अभाज्य) के अवयवों की संख्या $p - 1$ का गुणज (Multiple) है (इस प्रकरण में कोटि 3 के अवयवों की संख्या 2 का गुणज होगी)।

अतः G एबेलियन ही होगा।

माना $e \neq x \in G$ हो। चूँकि $o(x) \mid o(G) = 15$, $o(x) = 3$ या 5। यदि G में समस्त गैर–तत्समक अवयव कोटि 3 के हों तो $o(x) = 3$, $o(y) = 3$, $H = < x >$, $K = < y >$ मान लेने पर $o(H) = 3 = o(K)$। चूँकि G एबेलियन है G में H सामान्य है, $G \Rightarrow HK \leq G \Rightarrow o(HK) \mid o(G) = 15$ में K सामान्य है।

$$\text{परन्तु } o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)} = \frac{3 \times 3}{1} = 9 \text{ एवं } 9 \nmid 15$$

हमें विरोधाभास प्राप्त होता है।

अतः $\therefore \; \exists\, a \in G$ इस प्रकार है कि $o(a) = 5$। उपरोक्तानुसार समान तर्क से $\exists\, b \in G$ इस प्रकार है कि $o(b) = 3$। चूँकि $ab = ba$, $o(a)$ व $o(b)$ आपेक्षाकृत (Relatively) अभाज्य (Prime) हैं।

$$o(ab) = o(a)\, o(b)$$
$$= 3 \times 5 = 15$$
$$= o(G)$$

टिप्पणी

अतः G कोटि 15 का चक्रीय समूह है।

ध्यान दे: हम साइलो प्रमेयों की सहायता से उपरोक्त परिणाम सिद्ध करेंगे।

प्रमेय 4.4: माना $H \leq G$, G परिमित समूह हो तो $o(cl(H)) = \frac{o(G)}{o(N(H))}$

प्रमाण: चूँकि $N(H) \leq G$,

$$G = \bigcup_{i=1}^{t} N(H)x_i$$

जहाँ $N(H)\, x_i \cap N(H)\, x_j = \varphi$ किसी भी $i \neq j$ के लिए

$S = \{x_1^{-1} Hx_1, ..., x_t^{-1} Hx_t\}$ मान लेने से

हम दर्शाते हैं कि $S = cl(H)$,

माना $g^{-1} Hg \in cl(H), \quad g \in G$

$$g \in G \Rightarrow g \in N(H)x_i \text{ किसी भी } i \text{ के लिए}$$
$$\Rightarrow g = yx_i, \quad y \in N(H)$$
$$\Rightarrow g^{-1} Hg = x_i^{-1} y^{-1} Hyx_i$$
$$= x_i^{-1} Hx_i \text{ जैसे } y \in N(H) \Rightarrow y^{-1} Hy = H$$
$$\Rightarrow g^{-1} Hg \in S$$
$$\therefore \quad cl(H) \subseteq S$$

स्पष्ट है कि $S \subseteq cl(H)$

$$\therefore \quad S = cl(H).$$

तथा
$$x_i^{-1} Hx_i = x_j^{-1} Hx_j$$
$$\Rightarrow x_i\, x_j^{-1} H = Hx_i\, x_j^{-1}$$
$$\Rightarrow x_i\, x_j^{-1} \in N(H)$$
$$\Rightarrow N(H)x_i = N(H)x_j$$
$$\Rightarrow i = j$$
$$\therefore \quad o(S) = t$$
$$\Rightarrow o(cl(H)) = t = \frac{o(G)}{o(N(H))}.$$

4.3.1 कॉउची प्रमेय

प्रमेय 4.5 कॉउची का प्रमेय (Cauchy's Theorem) : G परिमित समूह हो एवं p को $p \mid o(G)$ का अभाज्य इस प्रकार मान लें कि $\exists\, x \in G$ तो $o(x) = p$।

प्रमाण: हम सर्वप्रथम परिणाम तब सिद्ध करते हैं जब G एबेलियन हो। $n = o(G)$ पर प्रवेशण (Induction) द्वारा हम इसे सिद्ध करते हैं। परिणाम सत्य है जब $n = 1$ होगा।

इसे $o(G)$ से कम कोटि वाले समस्त समूहों के लिये वास्तविक मानें। यदि G में गैर–नगण्य (Non-Trivial) उपसमूह न हों तो G अभाज्य कोटि का चक्रीय समूह है।

चूँकि $p \mid o(G), o(G) = p, G = < x >$ इस प्रकार है कि $o(x) = o(G) = p$। अतः परिणाम इस प्रकार होगा।

टिप्पणी

अब H को G का गैर–नगण्य (Non-Trivial) उपसमूह मानें, अर्थात् $H \neq \{e\}$, G, चूँकि G एबेलियन है, G में H सामान्य है। यदि $p \mid o(H)$ तो $o(H) < o(G), H$ के रूप में समावेशन परिकल्पना (Induction Hypothesis) से $\exists\, x \in H$ एबेलियन $o(x) = p, x \in H \Rightarrow x \in G$। इस प्रकार है कि अतः परिणाम पुनः वास्तविक है।

$p \nmid o(H)$ मानें।

चूँकि $o(G) = o(G/H).\, o(H)$ और $p \mid o(G)$ व $p \mid o\left(\frac{G}{H}\right).\, o(H)$, हम पाते हैं

किन्तु $p \nmid o(H)$, इसी कारण $p \mid o(G/H)$। $o\left(\frac{G}{H}\right) < o(G)$ भी है क्योंकि $H \neq \{e\}$ व G एबेलियन है, अर्थात् $\frac{G}{H}$ एबेलियन है।

अतः प्रवेशण परिकल्पना (Induction Hypothesis) से $\frac{G}{H}$ में कोटि p का एक अवयव Hy है।

$$(Hy)^p = H$$
$$\Rightarrow Hy^p = H$$
$$\Rightarrow y^p \in H$$
$$\Rightarrow (y^p)^t = e \qquad \text{जहाँ } t = o(H)$$
$$\Rightarrow (y^t)^p = e$$
$$\Rightarrow o(y^t) \mid p$$
$$\Rightarrow o(y^t) = 1 \text{ या } p$$

यदि $y^t = e$ (अर्थात्, $o(y^t) = 1$) तो $Hy^t = He = H$

$$\Rightarrow (Hy)^t = H$$
$$\Rightarrow o(Hy) \mid t$$

$\therefore \quad o(y^t) = p,\ y^t \in G$ जो कि एक विरोधाभास है।

अतः इस प्रकरण में परिणाम वास्तविक है।

प्रवेशण से परिणाम समस्त एबेलियन समूह के लिये वास्तविक है।

G कोई समूह हो तो हम पुनः $o(G)$ पर प्रवेशण का प्रयोग करते हैं। परिणाम $o(G) = 1$ के लिये वास्तविक है। मान लें कि परिणाम $o(G)$ से कम की कोटि वाले समस्त समूहों के लिये वास्तविक है। यदि $T < G$ व $p \mid o(T)$ तो प्रवेशण परिकल्पना से $\exists\, x \in T$ है। इस प्रकार कि $o(x) = p$। अतः इस प्रकरण में परिणाम वास्तविक है। मान लें कि समस्त $T < G$ हेतु $p \nmid o(T)$। G के वर्ग समीकरण का विचार करें,

टिप्पणी

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

अब, $a \notin Z(G) \quad \Rightarrow N(a) < G$

$$\Rightarrow p \nmid o(N(a))$$

$$\Rightarrow p \mid \frac{o(G)}{o(N(a))} \quad \text{(जैसे } o(G) = \frac{o(G)}{o(N(a))} . o(N(a))$$

$$\Rightarrow p \mid \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))},$$

चूँकि, $p \mid o(G)$,

दिया है, $p \mid o(G) - \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))} = o(Z(G))$

परन्तु $p \nmid o(T) \quad \forall\ T < G$

तथा $Z(G) = G \Rightarrow G$ एबेलियन है।

किन्तु परिणाम एबेलियन समूहों के लिये वास्तविक है। इसी कारण प्रवेशण से परिणाम समस्त समूहों के लिये वास्तविक है।

उदाहरण 4.16: दर्शायें कि कोटि pq (p, q सुनिश्चित अमाज्य) का एबेलियन समूह चक्रीय है।

हल: कॉउची प्रमेय से $\exists\ a, b \in G$ इस प्रकार है कि $o(a) = p, o(b) = q$। वैसे भी चूँकि

$$(p, q) = 1, ab = ba,$$

$$o(ab) = o(a).\ o(b) = pq$$

अर्थात् ab में $o(G)$ के समतुल्य कोटि का अवयव G है।

इसी कारण G एबेलियन है।

ध्यान दें: उदाहरण 4.16 की दृष्टि से कोटि 6, 10, 15, इत्यादि, के समस्त एबेलियन समूह चक्रीय हैं।

समान क्रमचय (Similar Permutations)

दो क्रमचय σ व $\eta \in S_n$ को समान कहा जाता है यदि इनमें समान चक्रीय निर्माण हो जब असंबद्ध चक्रीय के गुणन के रूप में वियोजित (Decomposed) किया जाता है।

उदाहरणार्थ $\sigma = (12)(345) \in S_5$

एवं $\eta = (123)(45) \in S_5$

समान हैं क्योंकि σ में लम्बाई 2 का 1 चक्रीय है एवं लम्बाई 3 का 1 चक्रीय η के समान हैं।

वैसे $\sigma = (1\ 2)\ (3\ 4), \eta = (1\ 2\ 3\ 4)$ S_4 में समान नहीं हैं क्योंकि लम्बाई 2 के 2 चक्रीय हैं व η में लम्बाई 2 का कोई चक्रीय नहीं है।

ध्यान दें: हम समान क्रमचय की बात तभी करते हैं यदि इन्हें असंबद्ध चक्रीय के गुणन (Product) के रूप में प्रस्तुत किया जाता रहा हो।

प्रमेय 4.6: दो क्रमचय $\sigma, \eta \in S_n$ समान हैं यदि एवं केवल यदि ये S_n में संयुग्मित हैं।

प्रमाण: मान लेते हैं कि $\sigma, \eta \in S_n$ समान हैं।

मान लें $\sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k})$

$\eta = (a_1' \ldots a'_{n_1}) \ldots (b_1' \ldots b'_{n_k})$

जहाँ $n_1 + n_2 + \ldots + n_k = n$

$\theta = \begin{pmatrix} a_1 \ldots a_{n_1} \ldots b_1 \ldots b_{n_k} \\ a_1' \ldots a'_{n_1} \ldots b_1' \ldots b'_{n_k} \end{pmatrix}$ को परिभाषित करें।

तो $\theta \in S_n$

तथा $\theta \sigma \theta^{-1} = (\theta a_1 \ldots \theta a_{n_1}) \ldots (\theta b_1 \ldots \theta b_{n_k})$

$= (a_1' \ldots a'_{n_1}) \ldots (b_1' \ldots b'_{n_k})$

$= \eta$

अतः S_n में σ, η संयुग्म हैं।

इसके विपरीत मान लें कि σ, η, S_n में संयुग्मित हैं।

तो $\exists\ \theta \in S_n$ इस प्रकार कि $\theta\sigma\theta^{-1} = \eta$

$\sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k})$ मान लें तो

$\eta = \theta\sigma\theta^{-1} = (\theta a_1 \ldots \theta a_{n_1}) \ldots (\theta b_1 \ldots \theta b_{n_k})$

अतः σ, η समान हैं।

एक पूर्णांक का विभाजन (Partition of An Integer)

n को एक धनात्मक पूर्णांक मानें। धनात्मक पूर्णांकों $n_1, n_2, \ldots, n_k$, का अनुक्रम जहाँ $n_1 \le n_2 \le \ldots \le n_k$, ऐसा हो कि $n = n_1 + n_2 + \ldots + n_k$ को n का विभाजन कहा जाता है एवं $n_1, n_2, \ldots, n_k$ को विभाजन के भाग कहते हैं।

उदाहरणार्थ: $n = 3$ मानें तो $3 = 1 + 1 + 1,\ 3 = 1 + 2,\ 3 = 3$ ये सभी $n = 3$ के विभाजन हैं। इससे n के 3 विभाजन मिलते हैं। $n = 4$ में 5 विभाजन हैं।

$4 = 1 + 1 + 1 + 1,\ 4 = 1 + 1 + 2,\ 4 = 1 + 3,\ 4 = 2 + 2,\ 4 = 4$ के विभाजन की संख्या को $p(n)$ द्वारा इंगित किया जाता है। अतः $p(3) = 3, p(4) = 5$, इत्यादि।

प्रमेय 4.7: $p(n)$ में संयुग्मित वर्गों की संख्या S_n है।

प्रमाण: $A = S_n$ में समस्त संयुग्मित वर्गों का समुच्चय हो एवं $B = n$ के समस्त विभाजन का समुच्चय हो तो विचार करें $cl(\sigma), \sigma \in S_n$

अब असंबद्ध चक्रों के गुणन के रूप में $\sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k})$ को देखने पर यहाँ $n_1 + \ldots + n_k = n$

हम चक्रों को इस प्रकार विन्यस्त करते हैं कि $n_1 \le \ldots \le n_k$। इससे $\{n_1, n_2, \ldots, n_k\}$, n का विभाजन सामने आता है।

टिप्पणी

टिप्पणी

$f: A \to B$ को इस प्रकार परिभाषित करें कि $f(cl(\sigma)) = \{n_1, n_2,..., n_k\}$

f, $cl(\sigma) = cl(\eta)$ के रूप में सुपरिभाषित है।

$\Rightarrow \sigma, \eta \in cl(\sigma)$

σ, η, S_n में संयुग्मित हैं।

σ, η, S_n में समान हैं।

$\Rightarrow \sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k})$

$\eta = (a_1' \ldots a'_{n_1}) \ldots (b_1' \ldots b'_{n_k})$

$\Rightarrow f(cl(\sigma)) = \{n_1,..., n_k\} = f(cl(\eta))$

मान लेते हैं कि $cl(\sigma) \neq cl(\eta)$

तो σ व η संयुग्मित नहीं हैं एवं इसलिये समान नहीं हैं।

σ, η में विभिन्न (Different) चक्रीय निर्माण संरचना है

संगत (Corresponding) विभाजन विभिन्न (Different) हैं।

अर्थात् $\{n_1, n_2,..., n_k\} \neq \{n'_1, n'_2,..., n'_r\}$ जहाँ निश्चय ही

$n = n_1 + n_2 + ... + n_k = n'_1 + n'_2 + ... + n'_r$

$\Rightarrow f(cl(\sigma) \neq f(cl(\eta)$

$\Rightarrow f$, 1–1 है।

f आच्छादक है, माना $\{n_1,..., n_k\} \in B$ के लिए जो n का क्रमचय है। तो $n = n_1 + ... + n_k$.

$\sigma = (a_1 \ldots a_{n_1}) \ldots (b_1 \ldots b_{n_k}) \in S_n$ को परिभाषित करें।

तो $cl(\sigma) = \{n_1,..., n_k\}$

f, (1–1) और आच्छादक दोनों हैं।

एवं $o(A) = o(B) = p(n)$

S_n में संयुग्मित वर्गों की संख्या $p(n)$ है।

उदाहरण 4.17: माना $(12) \in S_n$ हो तो S_n में समस्त अवयव निर्धारित करें जो (12) से क्रमविनिमय (Commute) करते हैं।

हल: माना $\sigma \in S_n$ इस प्रकार मानें कि $\sigma(1) = 1, \sigma(2) = 2$

तो $\sigma(12)\sigma^{-1} = (\sigma 1 \sigma 2) = (12)$

$\Rightarrow \sigma(12) = (12)\sigma$

ऐसे $\sigma \in S_n$ की संख्या स्पष्टतया $(n-2)!$ है $(n-2)!$ (जैसे $\sigma(1) = 1, \sigma(2) = 2$, द्वारा शेष $n-2$ अक्षर को स्वयं में ले लिया जायेगा एवं इसलिये σ, $n-2$ अक्षर पर क्रमचय होगा।

यहाँ $\eta = \sigma(12) \in S_n$

एवं $\eta(12)\eta^{-1} = (\eta 1 \eta 2) = (21) = (12)$

$\Rightarrow \eta(12) = (12)\eta$

ηs ∈ S_n की संख्या σ ∈ S_n (= $(n-2)!$) की संख्या के समतुल्य है।

इससे $2(n-2)!$ सामने आता है! S_n में सुनिश्चित क्रमचय (12) से क्रमविनिमय हैं।

अब $o(cl(12)) = \frac{o(S_n)}{o(N(12))} = \frac{n!}{o(N(12))}$

टिप्पणी

किन्तु $cl(12)$, S_n में उन क्रमचय का समुच्चय है जो (12) से संयुग्मित (अथवा समान) हैं।

अतः $o(cl(12)) = S_n$ में लम्बाई 2 के चक्रों की संख्या।

चूँकि (12) = (21) एवं प्रथम स्थान को n तरीकों में चुना जा सकता है, द्वितीय को $(n-1)$ तरीकों में, दिया गया है, लम्बाई 2 के $n(n-1)$ चक्र हैं परन्तु ऐसे हर चक्रों को दो बार गिना जाता है, हम लम्बाई 2 के $\frac{n(n-1)}{2}$ सुनिश्चित चक्र प्राप्त करते हैं।

$\therefore \quad o(cl(12)) = \frac{n(n-1)}{2}$

$\therefore \quad o(N(12)) = \frac{2n!}{n(n-1)} = 2\,(n-2)!$

$\therefore \quad N(12) = \{\sigma, \sigma(12) \mid \sigma(1) = 1, \sigma(2) = 2, \sigma \in S_n\}$, S_n में समस्त क्रमचय का समुच्चय (12) से विनिमेय करता है।

उदाहरण 4.18: A_5 में दो क्रमचय ज्ञात करें जो समान हैं परन्तु A_5 में संयुग्मित नहीं हैं।

हल: माना कि σ = (12345) ∈ A_5

η = (13245) ∈ A_5

चूँकि σ, η लम्बाई 5 के चक्र हैं, अतः ये समान क्रमचय हैं।

यदि σ, η, A_5 में संयुग्मित हों तो ∃ θ ∈ A_5 इस प्रकार है कि $\theta\,\sigma\,\theta^{-1} = \eta$

चूँकि (13245) को 5 तरीकों में लिखा जा सकता है अतः इसके 5 प्रकरण निम्नानुसार हैं।

प्रकरण 1: $\theta 1 = 1, \theta 2 = 3, \theta 3 = 2, \theta 4 = 4, \theta 5 = 5$

$\therefore\ \theta = (23) \notin A_5$

प्रकरण 2: $\theta 1 = 3, \theta 2 = 2, \theta 3 = 4, \theta 4 = 5, \theta 5 = 1$

$\therefore\ \theta = (1345) = (15)(14)(13) \notin A_5$

प्रकरण 3: $\theta 1 = 2, \theta 2 = 4, \theta 3 = 5, \theta 4 = 1, \theta 5 = 3$

$\therefore\ \theta = (124)(35) = (14)(12)(35) \notin A_5$

प्रकरण 4: $\theta 1 = 4, \theta 2 = 5, \theta 3 = 1, \theta 4 = 3, \theta 5 = 2$

$\therefore\ \theta = (143)(25) = (13)(14)(25) \notin A_5$

प्रकरण 5: $\theta 1 = 5, \theta 2 = 1, \theta 3 = 3, \theta 4 = 2, \theta 5 = 4$

$\therefore\ \theta = (1542) = (12)(14)(15) \notin A_5$

अतः प्रत्येक प्रकरण में हम विरोधाभास प्राप्त करते हैं।

इसी कारण σ, η, A_5 में संयुग्मित नहीं हैं।

टिप्पणी

ध्यान दें: दो संयुग्मित क्रमचय सदा समान होंगे।

उदाहरण 4.19: दर्शायें कि A_5 सरल है।

हल: N को $A_5, N \neq \{I\}, N \neq A_5$ में सामान्य मान लेते हैं। हमें विदित है कि N, A_5 में कुछ संयुग्मित वर्गों का संघ है। चूँकि $I \in N, o(N), o(A_5) = 60$ को विभाजित नहीं कर सकता, इस प्रकार A_5 सरल है।

अपनी प्रगति जांचिए

3. G में a के संयुग्मित वर्ग को आप कैसे प्रस्तुत करेंगे?
4. G को परिमित गैर–नगण्य, p को लघुत्तम अभाज्य विभक्त $o(G)$ एवं $k(G) > \frac{o(G)}{p}$ मानें तो दर्शायें कि $Z(G) \neq \{e\}$.

4.4 सामान्यीकरण, गणना सिद्धांत एवं परिमित समूह का वर्ग समीकरण

हमने देखा कि वास्तविक संख्याओं के समुच्चय **R** से योग के अधीन समूह का निर्माण होता है एवं पूर्णांकों के समुच्चय **Z** से भी योग के अधीन एक समूह का निर्माण होता है। **Z, R** का उपसमुच्चय है। यह उन कई परिस्थितियों में से एक है जिनमें हम निम्नांकित परिभाषा की ओर प्रेरित होते हैं।

परिभाषा: समूह G का गैर–रिक्त (Non-Empty) उपसमुच्चय H, G का उपसमूह कहा जाता है यदि H से G के द्विआधारी संरचना (Binary Composition) के अधीन समूह का निर्माण होता है।

स्पष्टतः, यदि H, G का उपसमूह हो एवं K, H का उपसमूह हो तो K, G का उपसमूह है।

यदि G तत्समक अवयव e का समूह हो तो उपसमुच्चयों {e} व G, G के नगण्य उपसमूह हैं तथा हम उन्हें नगण्य उपसमूह कहते हैं। अन्य समस्त उपसमूहों को गैर–नगण्य (अथवा उचित उपसमूह) कहेंगे।

ध्यान दें: $Z_5 = \{0, 1, 2, 3, 4\}$ मापांक 5 योग के अधीन Z का उपसमूह नहीं है क्योंकि योग मापकों 5, Z का संरचना नहीं है। इसी प्रकार Z_5, Z_6 का उपसमूह नहीं है, इत्यादि।

हम कभी–कभी यह दर्शाने के लिये संकेतन (Notation) $H \leq G$ का प्रयोग करते हैं कि H, G का उपसमूह है एवं $H < G$ का तात्पर्य है कि H, G का उचित उपसमूह है।

अनेक बार यह परखना कुछ जटिल (Cumbersome) लग सकता है कि समूह G का प्रदर्शित उपसमुच्चय H उपसमूह है अथवा नहीं, समूहों की परिभाषा में समस्त

अभिगृहीतों को परखते हुए ऐसा करना कठिन है। इस अभ्यास को सरल करने में निम्नांकित दो प्रमेय (विशेषतया द्वितीय) उपयोगी रहेंगे।

टिप्पणी

प्रमेय 4.8: समूह G का गैर–रिक्त उपसमुच्चय H, G का उपसमूह है यदि

(i) $a, b \in H \Rightarrow ab \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H.$

प्रमाण: H को G का उपसमूह मानें तो परिभाषानुसार (i) व (ii) स्थिति (Condition) इसमें हैं।

इसके विपरीत प्रदर्शित पद H में हैं ऐसा मानें।

पद (i) से H में संवृत है।

पुनः $a, b, c \in H \Rightarrow a, b, c \in G \quad \Rightarrow \quad a(bc) = (ab)c$

इसी कारण H में संबद्धता है।

किसी $a \in H, a^{-1} \in H$ के लिये भी एवं इसलिये पद (i) के अनुसार,

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

इस प्रकार H में तत्समक है।

H के प्रत्येक अवयव का व्युत्क्रम (Inverse) पद (ii) के अनुसार H में है।

इसी कारण H से समूह की परिभाषा में समस्त पद की पूर्ति होती है एवं इस प्रकार इससे समूह बनता है व इसीलिये G का उपसमूह हैं।

प्रमेय 4.9: समूह H का गैर–रिक्त उपसमुच्चय G, G का उपसमूह है

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

प्रमाण: यदि H, G का उपसमूह है तो $a, b \in H \Rightarrow ab^{-1} \in H$ (परिभाषा के सरल प्रयोग से)।

इसके विपरीत प्रदर्शित पद H में मानें।

संबद्धता (Associativity) H में प्रमेय 4.8 के अनुसार है।

$a \in H$ कोई अवयव $(H \neq \varphi)$ हो

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

अतः H में तत्समक है।

पुनः किसी $a \in H$ जैसे $e \in H$ के लिये $ea^{-1} \in H \Rightarrow a^{-1} \in H$

अर्थात् H में प्रत्येक अवयव का व्युत्क्रम है।

अन्ततः किसी $a, b \in H,\ a, b^{-1} \in H$ के लिये।

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

अर्थात् H गुणन के अधीन संवृत (Closed) है।

इसी कारण H से एक समूह का निर्माण होता है एवं इसीलिये G का उपसमूह।

ध्यान दे: यदि समूह के द्विआधारी संरचना को $+$ से इंगित किया जाता है तो उपरोक्त पद को $a, b \in H \Rightarrow a - b \in H$ के रूप में पढ़ा जायेगा। स्मरण रहे कि e, H में सदा है।

टिप्पणी

हो सकता है कि निम्नांकित प्रमेय उतना अधिक उपयोगी सिद्ध न हो जितना कि परिमित उपसमुच्चयों में ही सिद्ध होता है परन्तु फिर भी यह महत्त्वपूर्ण है।

प्रमेय 4.10: समूह G का गैर–रिक्त परिमित उपसमुच्चय H, G का उपसमूह है यदि H गुणन के अधीन संवृत है।

प्रमाण: यदि H, G का उपसमूह है तो यह परिभाषानुरूप गुणन के अधीन संवृत है, अतः यहाँ सिद्ध करने को कुछ नहीं है।

इसके विपरीत H को परिमित उपसमुच्चय इस प्रकार मानें कि,

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

अब $a, b, c \in H \Rightarrow a, b, c \in G$

$\Rightarrow a(bc) = (ab)c$

अतः संबद्धता H में है।

$\Rightarrow H$ एक अर्द्ध–समूह है।

पुनः निष्कासित नियम H में हैं (जिस प्रकार G यह में हैं) एवं इस प्रकार H एक परिमित अर्द्ध–समूह है जिसमें निष्कासित नियम हैं। इसी कारण H से समूह बनता है।

अलिटर (Aliter): H को ऐसा परिमित उपसमुच्चय मानें कि $a, b \in H \Rightarrow ab \in H$

हम दर्शाते हैं $a \in H \Rightarrow a^{-1} \in H$

यदि $a = e$ तो $a^{-1} = a \in H$

$a \neq e$ हो तो संवृत्त (Closure) से $a, a^2, a^3 \ldots \in H$

चूँकि H कुछ $n, m,\ a^n = a^m,\ n > m$ के लिये परिमित है, अर्थात्

अर्थात् $a^{n-m} = e,\ n - m > 1$ जहाँ $a \neq e$

अर्थात् $a^{n-m-1}.\ a = e$

$\Rightarrow \quad a^{n-m-1} = a^{-1}$

जहाँ $n–m–1 \geq 1$ एवं इसीलिये $a^{n-m-1} \in H$

इसी कारण $a \in H \Rightarrow a^{-1} \in H$ तथा इस प्रकार $H,\ C$ का उपसमूह है।

परिभाषा: G कोई समूह हो एवं माना कि $Z(G) = \{x \in G \mid xg = gx$ सभी हैं $g \in G\}$ के लिए तो $Z(G)$ को G का केन्द्र कहा जाता है।

प्रमेय 4.11: समूह G का केन्द्र G का उपसमूह है।

प्रमाण: माना कि $Z(G)$ को समूह G का केन्द्र हैं तो $Z(G) \neq \varphi$ जैसे $e \in Z(G)$

पुनः $x, y \in Z(G) \Rightarrow xg = gx$

$yg = gy$ (सभी $g \in G$ के लिए)।

$\Rightarrow g^{-1} x^{-1} = x^{-1} g^{-1}$

$g^{-1} y^{-1} = y^{-1} g^{-1}$ (सभी $g \in G$ के लिए)।

अब $g(xy^{-1}) = (gx)y^{-1} = (xg)y^{-1}$

$= (xg)y^{-1} (g^{-1}g)$

$= xg(y^{-1}\, g^{-1})g = xg(g^{-1}\, y^{-1})g$

$= x(gg^{-1})y^{-1}g$

$= (xy^{-1})g$ सभी $g \in G$ के लिए।

$\Rightarrow \quad xy^{-1} \in Z(G)$

इसी कारण $Z(G)$ एक उपसमूह है।

ध्यान दे: स्पष्टतः G एबेलियन है यदि $Z(G) = G$

परिभाषा: माना कि G कोई समूह हो। $a \in G$ कोई अवयव। उपसमुच्चय $N(a) = \{x \in G \mid xa = ax\}$ को G में a का **सामान्यीकरण (Normalization)** अथवा **केन्द्रीकरण (Centralization)** कहा जाता है।

यह सरलता से देखा जा सकता है कि यह सामान्यीकरण G का उपसमूह है।

प्रमेय 4.12: HK, G का उपसमूह है यदि $HK = KH$

प्रमाण: HK को G का उपसमूह मानें। हम दर्शाते हैं $HK = KH$

माना $x \in HK$ कोई अवयव हो तो $x^{-1} \in HK$ (क्योंकि HK एक उपसमूह है)

$\Rightarrow \quad x^{-1} = hk$ इस प्रकार $h \in H, k \in K$

$\Rightarrow \quad x = (hk)^{-1} = k^{-1}\, h^{-1} \in KH$

इसलिए, $\quad HK \subseteq KH$

पुनः $y \in KH$ को कोई अवयव मान लेते हैं।

तो $y = kh$ कुछ $k \in K, h \in H$

$\Rightarrow \quad y^{-1} = h^{-1}\, k^{-1} \in HK$

$\Rightarrow \quad y \in HK$ (क्योंकि HK एक उपसमूह है)

$\Rightarrow \quad KH \subseteq HK$

इसी कारण $\quad HK = KH$

इसके विपरीत $HK = KH$

$a, b \in HK$ दो अवयव हों; हम दर्शाते हैं,

$a, b \in HK \Rightarrow a = h_1 k_1$ किसी भी $h_1, h_2 \in H$ के लिए।

$b = h_2 k_2 \qquad k_1, k_2 \in K$

तो $ab^{-1} = (h_1 k_1)\,(h_2 k_2)^{-1} = (h_1 k_1)\,(k_2^{-1} h_2^{-1})$

$= h_1 (k_1 k_2^{-1})\, h_2^{-1}$

अब $(k_1 k_2^{-1})\, h_2^{-1} \in KH = HK$

इस प्रकार $(k_1 k_2^{-1})\, h_2^{-1} = hk$ किसी भी $h \in H, k \in K$ के लिए।

तो $ab^{-1} = h_1(hk) = (h_1 h)k \in HK$

इसी कारण HK एक उपसमूह है।

ध्यान दे

1. $HK = KH$ का तात्पर्य यह नहीं है कि H का प्रत्येक अवयव K के प्रत्येक अवयव से क्रमविनियम करता है। इसका तात्पर्य तो मात्र यह है कि प्रत्येक $h \in H, k \in K, hk = k_1 h_1$ के लिये $k_1 \in K$ एवं कुछ $h_1 \in H$ के लिये।

टिप्पणी

2. यदि G में द्विआधारी संरचना + है, हम परिभाषित करते हैं,

$H + K = \{h + k \mid h \in H, k \in K\}$

टिप्पणी

4.5 परिमित एबेलियन समूह एवं गैर–एबेलियन समूह

समूह G के एबेलियनीकरण (Abelianization) को निम्नांकित समकक्ष (Equivalent) रीतियों में परिभाषित किया जाता है :

1. यह समूह का भागफल है, इसके क्रमविनिमेय उपसमूह के द्वारा, अर्थात् यह समूह $G / [G, G]$ है।
2. यह G का भागफल है (सम्बन्ध $xy = yx$ द्वारा)।
3. यह एक एबेलियन समूह A इस प्रकार है कि आच्छादी समरूपता $f: G \to A$ इस विशेषताओं के साथ है कि जब भी $\varphi : G \to H$ समरूपता व H एक एबेलियन समूह हो तो अद्वितीय समरूपता $\psi: A \to H$ इस प्रकार है, $\varphi = \psi \circ f$

उपरोक्त समस्त विशेषताओं की व्याख्या निम्नानुसार की जा सकती है:

अमूर्त बीजगणित (Abstract Algebra) में समूह का क्रमविनिमय उपसमूह समूह के समस्त क्रमविनिमय द्वारा उत्पन्न उपसमूह है।

समूह G के अवयवों g व h के लिये g व h का क्रमविनिमय $[g, h]: = g^{-1}h^{-1}gh$ है। क्रमविनिमय $[g, h]$ तत्समक अवयव e के समतुल्य है यदि एवं केवल यदि $gh = hg$, अर्थात् यदि एवं केवल यदि g व h क्रमविनिमय हों। साधारणतया $gh = hg[g, h]$।

समरूपता के रूप में एबेलियनीकरण भागफल मानचित्र $G \to G/[G, G]$ है जहाँ आधारभूत $f: G \to A$, G का क्रमविनिमेय उपसमूह है। इसे इस गुण के साथ एबेलियन समूह A में समरूपता रूप में परिभाषित किया जा सकता है कि जब भी $\varphi : G \to H$ समरूपता हो व H एक एबेलियन समूह हो तो अद्वितीय समरूपता $\psi: A \to 122\ H$ इस प्रकार होगा कि $\varphi = \psi \circ f$।

दिया है कि समूह G, खंड समूह G/N एबेलियन है यदि एवं केवल यदि $[G, G] \leq N$। भागफल $G / [G, G]$ एक एबेलियन समूह है जिसे G का एबेलियनीकरण कहा जाता है। इसे प्रायः G^{ab} अथवा G_{ab} द्वारा इंगित किया जाता है।

$\phi: G \to G^{ab}$ हो तो φ, G से H एबेलियन समूह $f: G \to H$ तक समरूपता के लिये सर्वभौम है तथा समूहों के समरूपता $F : G^{ab} \to H$ के लिये अद्वितीय समरूपता $f = F \circ \phi$ इस प्रकार है कि इससे एबेलियनीकरण G^{ab} की अद्वितीयता प्रमाणिक (Canonical) तुल्याकारिता तक दर्शायी जाती है जबकि सुनिश्चित (Explicit) निर्माण $G \to G/[G, G]$ से अस्तित्व (Existence) दर्शाया जाता है।

4.5.1 परिमित एबेलियन समूह हेतु प्रमेय

प्रत्यक्ष गुणन का अध्ययन करते हुए व्यक्ति यह जानना चाहेगा कि किन–किन समूहों को किन्हीं 'सरल दिखने वाले' समूहों के प्रत्यक्ष गुणन के रूप में लिखा जा सकता है। सौभाग्यवश इस प्रकार के समूहों का वर्ग अस्तित्व में होता है जिन्हें परिमित एबेलियन

समूह कहा जाता है। इस अनुभाग (Section) का प्रमुख प्रयोजन यह सिद्ध करना है कि समूह एबेलियन समूह के बारे में मूलभूत प्रमेय नामक समस्त महत्वपूर्ण प्रमेयों के अनुसार परिमित एबेलियन समूह चक्रीय समूहों का एक प्रत्यक्ष गुणन है। इससे हम वह विधि बता पाते हैं कि जिससे दिए गए कोटि के गैर–तुल्याकारिता परिमित एबेलियन समूह की संख्या ज्ञात की जाती है।

टिप्पणी

हम सर्वप्रथम यह दर्शाते हैं कि परिमित एबेलियन समूह को p समूह के प्रत्यक्ष गुणन के रूप में लिखा जा सकता है।

प्रमेय 4.13: परिमित एबॅलियन समूह इसके सइलो p उपसमूहों का प्रत्यक्ष गुणन है।

प्रमाण: कोटि G का परिमित एबेलियन समूह n है। $n = p_1^{\alpha 1} \ldots p_r^{\alpha r}\, p_i's$ सुनिश्चित अभाज्य मानें।

माना $S_1,\ldots S_r$ क्रमशः सुनिश्चित सइलो p_i उपसमूह हों। समस्त $i = 1,\ldots, r$ के लिये $o(S_i) = p_i^{\alpha i}$।

हम दर्शाते हैं कि $G = S_1 \times \ldots \times S_r$

चूँकि G एबेलियन है, अतः प्रत्येक G, S_i का सामान्य उपसमूह है।

$m = p_2^{\alpha 2} \ldots p_r^{\alpha r}$ मानें

एवं $T = \{x \in G \mid x^m = e\}$

तो T, G का उपसमूह है क्योंकि G एबेलियन है।

अब $x \in S_1 \cap T \Rightarrow o(x) \mid o(S_1) = p_1^{\alpha 1}$

एवं $o(x) \mid m$

अतः $o(x) \mid (p_1^{\alpha 1}, m) = 1$

$\Rightarrow o(x) = 1$

$\Rightarrow x = e$

$\therefore \quad S_1 \cap T = \{e\}$

चूँकि $(p_1^{\alpha 1}, m) = 1$, $\exists$ पूर्णांक u, v इस प्रकार हैं कि,

$up_1^{\alpha 1} + vm = 1$

$x \in G$ मानें तो $x = x^1$

$= x^{up1^{\alpha_1} + vm}$

$= x^{vm} \cdot x^{up1^{\alpha_1}}$

$\in S_1$. T (जैसे $(x^{vm})^{p1^{\alpha_1}} = x^{vn} = (x^n)^v = e$

$\Rightarrow o(x^{vm}) \mid p_1^{\alpha_1}$

$\Rightarrow o(x^{vm}) = p_1^{\beta_1} < x^{vm} > \subseteq S_1$ समूह है।

$\Rightarrow < x^{vm} > \subseteq S_1$

$\Rightarrow x^{vm} \in S_1$

जैसे $(x^{up1^{\alpha_1}})^m = x^{un} = e$

$\Rightarrow x^{up1^{\alpha_1}} \in T)$

$\therefore \quad G = S_1 T$

चूँकि G एबेलियन है अतः S_1 व T, G के सामान्य उपसमूह हैं।

टिप्पणी

$\therefore \quad G = S_1 \times T$

जैसे, $o(G) = o(S_1 T)$

$= o(S_1)\, o(T)$

$\Rightarrow n = p_1^{\alpha_1}\, o(T)$

$\Rightarrow o(T) = p_2^{\alpha_2} \ldots p_r^{\alpha r} = m$

उपरोक्तानुसार हम यह दर्शा सकते हैं कि,

$T = S_2 \times U$ जहाँ U, T का उपसमूह इस प्रकार है कि $o(U) = p_3^{\alpha_3} \ldots p_r^{\alpha r}$। इस प्रकार हमारे पास होगा,

$$G = S_1 \times S_2 \ldots S_r$$

G को p उपसमूहों के गुणन में खण्डित करने पर हमने परिणाम परिमित एबेलियन p समूहों पर सिद्ध किये, न कि G स्वयं पर।

प्रमेय 4.14: G कोटि p^n का एबेलियन समूह हो, p अभाज्य (Prime) हो एवं $a \in G$ में G में समस्त अवयवों का महत्तम कोटि (Maximal Order) हो तो $G = A \times Q$ जहाँ A, a द्वारा उत्पन्न एक चक्रीय उपसमूह है एवं $Q \leq G$।

प्रमाणः हमने n पर समावेशन द्वारा परिणाम सिद्ध किया। यदि $n = 1$ तो $o(G) = p$। अतः G कोटि p का चक्रीय उपसमूह है। इस प्रकार G में सर्वाधिक कोटि p का एक अवयव है।

अतः $o(a) = p = o(G)$ एवं $G = < a > = A$। इसलिये परिणाम इस प्रकरण में वास्तविक है।

मान लें कि परिणाम समस्त $m < n$ के लिये वास्तविक है। मान लें कि $\exists\, b \in G$ इस प्रकार है कि $b \notin A = < a >$ व $o(b) = p$। हम दर्शाते हैं कि परिणाम इस प्रकरण में वास्तविक है।

$B = < b >$ मान लें तो $A \cap B \leq B \Rightarrow o(A \cap B) = 1$ या p

यदि $o(A \cap B) = p = o(B)$ तो $A \cap B = B \Rightarrow B \subseteq A \Rightarrow b \in A$ जो कि एक विरोधाभास है।

$\therefore\ A \cap B = \{e\}.$

माना $\overline{G} = \dfrac{G}{B}$. माना $\overline{a} = Ba$

अब $(\overline{a})^{o(a)} = (Ba)^{o(a)}$

$= Ba^{o(a)}$

$= B$

$\Rightarrow o(\overline{a}) \mid o(a)$

टिप्पणी

अब $Ba^{o(\bar{a})} = Ba^{o(\bar{a})} = B$

$\Rightarrow a^{o(\bar{a})} \in B$

अब $a^{o(\bar{a})} \in A$

$\Rightarrow a^{o(\bar{a})} \in A \cap B = \{e\}$

$\Rightarrow a^{o(\bar{a})} = \{e\}$

$\Rightarrow o(a) \mid o(\bar{a})$

$\Rightarrow o(a) = o(\bar{a})$

अब $\bar{a}$ अवयव की महत्तम कोटि में $\bar{G}$ के लिए यदि $\bar{c} \in \bar{G}$ के पास $o(\bar{c})$ से अधिक कोटियां होगी।

तो $o(\bar{c}) \mid o(c) \Rightarrow o(\bar{c}) \leq o(c)$

$\Rightarrow o(c) \geq o(\bar{c}) > o(\bar{a}) = o(a)$

$\Rightarrow o(c) > o(a)$

यह विरोधाभासी है कि a में G में महत्तम कोटि (Maximal Order) है।

समावेशन परिकल्पना (Induction Hypothesis) से $\bar{G} = <\bar{a}> \times T$ के किसी उपसमूह T के लिये $\bar{G}$ परन्तु T के किसी उपसमूह $\bar{G} \Rightarrow T = \frac{Q}{B}$ के लिये Q, G का उपसमूह है। हम दर्शाते हैं कि $G = A \times Q$

$x \in A \cap Q$ मानें तो $x \in A \Rightarrow x = a^i$

किन्तु $x \in Q \Rightarrow a^i \in Q \Rightarrow Ba^i \in T \Rightarrow (Ba)^i \in T \Rightarrow a^{-i} \in T$

$\Rightarrow a^{-i} \in <\bar{a}> \cap T \Rightarrow a^{-i} = \bar{e} \Rightarrow Ba^i = Be \Rightarrow a^i \in B$

$\therefore \quad a^i \in A \cap B = \{e\}$

$\Rightarrow a^i = e \Rightarrow x = e \Rightarrow A \cap Q = \{e\}$

$x \in G$ मानें।

तो $\bar{x} = Bx \in \bar{G} = <\bar{a}>. T$

$\Rightarrow \bar{x} = a^{-j}\bar{y}, \ \bar{y} \in T$

$\Rightarrow xy^{-1} a^{-j} \in B \subseteq Q$

$\Rightarrow x = a^j z, \ z \in Q$

$x \in <a>. Q$

$\Rightarrow G = AQ$

अतः $G = A \times Q$ एवं इसलिये यह परिणाम सामने आया।

मान लेते हैं कि कोई अवयव $b \in G, b \notin A$ इस प्रकार नहीं है कि $o(b) = p$। हम दर्शाते हैं कि इस प्रकरण में $G = A$। मान लें कि $G \neq A$। $x \in G. x \notin A$ हो। मान लेते हैं कि x में सबसे छोटी संभव कोटि है।

अब $o(x^p) = \frac{o(x)}{(p, o(x))} = \frac{p^i}{(p, p^i)} = \frac{p^i}{p} = p^{i-1}$

$\Rightarrow o(x^p) < o(x)$

$\Rightarrow x^p \in A$

$\Rightarrow x^p = a^j$

टिप्पणी

मान लें कि $p \nmid j$

$o(a) = m = p^s$ हो।

अब $c \in G \Rightarrow o(c) = p^r$

$\Rightarrow p^r \leq o(a) = p^s$ क्योंकि a में महत्तम कोटि है।

$\Rightarrow r \leq s$

$\Rightarrow o(c) \mid o(a) = m$

$\Rightarrow c^m = e$ सभी $c \in G$ के लिए।

$p \nmid j \Rightarrow m \nmid \frac{jm}{p}$

और, $(a)^{\frac{jm}{p}} \neq e$

$\therefore x^m = (x^p)^{\frac{m}{p}}$

$= (a^j)^{\frac{m}{p}} = (a)^{\frac{jm}{p}}$

$\neq e$, a का विरोधाभास (Contradiction) है।

$\therefore p \mid j$. माना $j = kp$. तो $x^p = a^j = a^{kp}$.

माना $y = a^{-k}x$

चूंकि $x \notin A, y \notin A$

और $y^p = a^{-kp} x^p = a^{-j} a^j = e$

अतः $o(y) = p$ एक विरोधाभास है (क्योंकि हमारी धारणा अनुसार कोटि p का कोई अवयव A में नहीं है)।

अतः $G = A$ एवं इसलिये परिणाम इस प्रकरण में वास्तविक है।

इसी कारण समावेशन द्वारा यह परिणाम आया।

हम अब परिमित एबेलियन समूह पर आधारभूत प्रमेय सिद्ध करने को तैयार हैं।

प्रमेय 4.15: (परिमित एबेलियन समूह पर आधारभूत प्रमेय): परिमित एबेलियन समूह चक्रीय समूह का प्रत्यक्ष समूह होता है।

प्रमाण: G एक परिमित एबेलियन समूह है। हम $o(G)$ पर समावेशन द्वारा परिणाम सिद्ध करते हैं। यदि $o(G) = 1$ तो परिणाम नगण्य वास्तविक है। मान लेते हैं कि परिणाम कोटि $< o(G)$ के समस्त एबेलियन समूह के लिये वास्तविक है।

$o(G) = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ हो, $p_i s$ सुनिश्चित अभाज्य हैं।

बीजगणित के मानक प्रमेय के अनुसार $G = S_1 \times \ldots \times S_r$ जहाँ S_i कोटि $p_i^{\alpha i}$ $(i = 1, 2, \ldots, r)$ का सइलो p_i उपसमूह है।

बीजगणित के मानक प्रमेय के अनुसार,

$S_i = A_i \times Q_i$, जहाँ प्रत्येक A_i एक चक्रीय उपसमूह है।

$G = (A_1 \times Q_1) \times ... \times (A_r \times Q_r)$

$= (A_1 \times ... \times A_r) \times (Q_1 \times ... \times Q_r)$

अब $o(Q_1 \times ... \times Q_r) < o(G)$ एवं $Q_1 \times Q_2 ... \times Q_r$ एक एबेलियन समूह है। समावेशित परिकल्पना से $Q_1 \times ... \times Q_r = T_1 \times ... \times T_s$ जहाँ प्रत्येक G, T_i का चक्रीय उपसमूह है।

$\therefore \quad G = A_1 \times ... \times A_r \times T_1 \times ... \times T_s$

= चक्रीय उपसमूहों का प्रत्यक्ष गुणन।

अतः परिणाम इस प्रकरण के भी लिये वास्तविक है।

समावेशन द्वारा परिणाम समस्त परिमित एबेलियन समूह G के लिये वास्तविक है।

ध्यान दे : मान लें कि परिमित एबेलियन समूह G को $G = A_1 \times ... \times A_k, A_i =$ के रूप में लिखा जा रहा हो एवं चक्रीय समूह तो,

$G = A_1 \times (A_2 \times ... \times A_k)$

$\Rightarrow o(G) = o(A_1)\, o(A_2 \times ... \times A_k)$

$= o(A_1)\, o(A_2)\, o(A_3 \times ... \times A_k)$

इस प्रकार हमें $o(G) = o(A_1)\, o(A_2) ... o(A_k)$ प्राप्त होता है।

प्रमेय 4.16: p^n कोटि G का परिमित एबेलियन समूह हो, p एक अभाज्य (Prime) हो। मान लें कि $G = A_1 \times ... \times A_k$ जहाँ प्रत्येक A_i कोटि p^{ni} का एक चक्रीय समूह है: $n_1 \geq n_2 \geq ... \geq n_k > 0$ सहित तो पूर्णांक $n_1,..., n_k$ अद्वितीयतः निर्धारित किये जाते हैं जिन्हें G के अक्रमविनिमय (Invariant) कहा जाता है।

प्रमाण: मान लें कि $G = A_1 \times ... \times A_k$

एवं $G = B_1 \times ... \times B_l$

जहाँ A_i व $B_j s$ चक्रीय समूह इस प्रकार हैं कि $o(A_i) = p^{ni}$, $o(B_j) = p^{hj}$

$n_1 \geq n_2 \geq ... \geq n_k > 0$, $h_1 \geq h_2 \geq ... \geq h_l > 0$

हमारा लक्ष्य यह दर्शाना है कि समस्त i हेतु $k = l$ व $n_i = h_i$ है।

तो $g = a_1 a_2 ... a_k$, $a_i \in A_i$

चूँकि समस्त $i = 1,..., k$ के लिये $n_1 \geq n_i$

समस्त $i = 1,..., k$ के लिये $p^{ni} \mid p^{n1}$

अतः समस्त $i = 1,..., k$ के लिये $p^{n1} = p^{ni}\, p^{ui}$

समस्त i के लिये $g^{p^{n_1}} = a_1^{p^{n1}}\, a_2^{p^{n1}} ... a_k^{p^{nk}}$

$= a_1^{pn1} a_2^{pn2\, pn2} ... a_k^{pnk\, pnk}$

$= e$ जैसे $(a_i)^{p^{ni}} = a_i^{o(Ai)} = e$

टिप्पणी

$\therefore \quad o(g) \mid p^{n1}$ सभी $g \in G$ के लिए।

$\Rightarrow \quad o(g) \leq p^{n1}$ सभी $g \in G$ के लिए।

$p^{n1} \Rightarrow \exists$ कोटि A_1 का एक चक्रीय समूह है p^{n1} कोटि का अवयव है।

अतः p^{n1}, G में अवयवों का महत्तम कोटि है। इसी प्रकार $G = B_1 \times ... \times B_l$ को प्राप्त करने पर हम p^{n1} को G में अवयवों का महत्तम लेते हैं।

अतः $p^{n1} = p^{h1} \Rightarrow n_1 = h_1$

मान लें कि हमने सिद्ध किया कि $n_1 = h_1, n_2 = h_2, ..., n_{t-1} = h_{t-1}$। मान लेते हैं कि $n_t > h_t = m$ हो तो $C = \{x^{p^m} \mid x \in G\}$ को परिभाषित करें। चूँकि G एबेलियन है इसलिये C, G का उपसमूह है।

$A_1 = < a_1 >, ..., A_k = < a_k >, o(a_i) = o(A_i) = p^{n_i}$

$B_1 = < b_1 >, ..., B_k = < b_k >, o(b_j) = o(B_j) = p^{h_j}$ है।

हम दावा करते हैं कि,

$C = < b_1^{p^m} > \times ... \times < b_{t-1}^{p^m} >$ है

अब $x^{p^m} \in C, x \in G$

$x_j \in B_j \Rightarrow x_j = b_j^{r_j}$

$\therefore \quad x^{p^m} = x_1^{p^m} ... x_l^{p^m}$

$= b_1^{r_1 p^m} ... b_{t-1}^{r_{t-1} p^m} b_t^{r_t p^m} ... b_l^{r_1 p^m},$

समस्त $x \in G \Rightarrow x = x_1 ... x_{t-1} x_t ... x_l$, $x_j \in B_j$ के लिये।

अब $j \geq t, o(B_j) = p^{h_j} \mid p^{h_t} = p^m$

$\Rightarrow p^m = p^{h_j p^{v_j}} = e$ सभी $j \geq t$ के लिए।

$\Rightarrow b_j^{p^m} = b_j^{p^{h_j p^{v_j}}} = e$ सभी $j \geq t$ के लिए।

$\therefore \quad x^{p^m} = b_1^{r_1 p^m} ... b_{t-1}^{r_{t-1} p^m}$

$\therefore \quad x^{p^m} = b_1^{r_1 p^m} ... b_{t-1}^{r_{t-1} p^m}$

$\in < b_1^{p^m} > ... < b_{t-1}^{p^m} >$

$\therefore \quad C \subseteq < b_1^{p^m} > ... < b_{t-1}^{p^m} >$

किन्तु $b_j^{p^m} \in C \Rightarrow < b_j^{p^m} > \subseteq C$

$\therefore \quad C = < b_1^{p^m} > ... < b_{t-1}^{p^m} >$

और भी $x \in < b_1^{p^m} > \cap < b_2^{p^m} > ... < b_{t-1}^{p^m} >$

$\Rightarrow x \in B_1, x \in B_2 ... B_{t-1}$

$\Rightarrow x \in B_1, x \in B_2 ... B_{t-1} B_t ... B_l$

$\Rightarrow x = e.$

इसी प्रकार अन्य सर्वनिष्ठ (Intersection) के लिये।

अतः $C = < b_1^{p^m} > \times ..... \times < b_{t-1}^{p^m} >$

इस प्रकार $o(C) = o(b_1^{p^m}) ..... o(b_{t-1}^{p^m})$

टिप्पणी

$$= \frac{o(b_1)}{(p^m, o(b_1))} \ldots \frac{o(b_{t-1})}{(p^m, o(b_{t-1}))}$$

$$= \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m}$$

अब $G = A_1 \times \ldots\ldots \times A_k = < a_1 > \times \ldots\ldots \times < a_k >$ एवं $C \leq G$

$\Rightarrow C = < a_1^{p^m} > \times \ldots\ldots \times < a_k^{p^m} >$

$$\Rightarrow o(C) = \frac{o(a_1)}{(p^m, o(a_1))} \ldots\ldots \frac{o(a_k)}{(p^m, o(a_k))}$$

$$= \frac{p^{n_1}}{(p^m, p^{n_1})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

चूँकि $n_1 = h_1, \ldots, n_{t-1} = h_{t-1}$

$$o(C) = \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} \cdot \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

अतः $\frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} = \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} \cdot \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$

$$\Rightarrow 1 = \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

$$\geq \frac{p^{n_t}}{(p^m, p^{n_t})}, \text{ क्योंकि } \frac{p^{n_j}}{(p^m, p^{n_j})} \geq 1$$

> 1 as $n_t > m \quad \Rightarrow (p^m, p^{n_t}) = p^m$

$$\Rightarrow \frac{p^{n_t}}{(p^m, p^{n_t})} = \frac{p^{n_t}}{p^m} = p^{n_t - m} > 1$$

जो कि एक विरोधाभास है।

अतः समस्त i के लिये $n_i = h_i$

इसलिये $o(G) = o(A_1) \ldots\ldots o(A_k) = o(B_1) \ldots\ldots o(B_l)$

$\Rightarrow p^{n1} \ldots\ldots p^{nk} = p^{h1} \ldots\ldots p^{ht}$

यदि $k > l, p^{n1} \ldots\ldots p^{nt}\, p^{nt+1} \ldots\ldots p^{nk} = p^{h1} \ldots\ldots p^{ht}$.

$\Rightarrow p^{nl+1} + p^{nk} = 1$ जैसे $n_i = h_i$ सभी i के लिए

जो कि वास्तविक नहीं है।

अतः k, l से बड़ा नहीं है। इसी प्रकार l, k से बड़ा नहीं है।

ध्यान दे : बीजगणित के मानक प्रमेय के अनुसार $n_1, \ldots, n_k$ को अद्वितीयतः निर्धारित किया जाता है, न कि संगत (Corresponding) चक्रीय समूह से। उदाहरणार्थ $G =$ क्लॅईन्स के 4 समूह को चक्रीय समूहों के प्रत्यक्ष गुणन के रूप में दो रीतियों में लिखा जा सकता है।

$G = A \times B = A \times C$, जहाँ $A = \{I, (12)(34)\}$

$B = \{I, (13)(24)\}$, $C = \{I, (14)(23)\}$

टिप्पणी

प्रमेय 4.17: कोटि p^n के दो एबेलियन समूह तुल्याकारिक हैं यदि और केवल यदि इनमें समान अक्रमविनिमय हों।

प्रमाण: मान लें कि G, G' कोटि p^n के परिमित एबेलियन समूह हैं। G व G' तुल्याकारिक हैं एवं θ, G से तुल्याकारिता है।

$G = A_1 \times ... \times A_k$, $A_i = < a_i >$, $o(A_i) = p^{n_i}$ है।

चूँकि θ एक तुल्याकारिक है, G' समस्त $i = 1,..., k$ के लिये $\theta(A_i)$ का सामान्य उपसमूह G'।

अतः $\theta(A_1)..... \theta(A_k)$, G का उपसमूह है।

$g' \in G' \Rightarrow \exists\, g \in G$ भी इस प्रकार है कि $\theta(g) = g$

$g \in G \Rightarrow g = x_1 ..... x_k,\ x_i \in A_i$

$\Rightarrow g' = \theta(g) = \theta(x_1) ..... \theta(x_k)$

$\in \theta(A_1) ..... \theta(A_k)$

$\Rightarrow G' \subseteq \theta(A_1) ..... \theta(A_k)$

$\Rightarrow G' = \theta(A_1) ..... \theta(A_k)$ भी, $\theta(A_1) \cap \theta(A_2) ... \theta(A_k) = \{e'\}$, $e' = G'$ की तत्समक है।

चूँकि $x \in \theta(A_1), x \in \theta(A_2) ..... \theta(A_k)$

$\Rightarrow x = \theta(x_1) = \theta(x_2).....\theta(x_k),\ x_i \in A_i$

$\Rightarrow \theta(x_1) = \theta(x_2.....x_k)$

$\Rightarrow x_1 = x_2 ..... x_k$

$\Rightarrow x_1^{-1} x_2 ..... x_k = e$

$\Rightarrow x_i = e$ समस्त i के लिए

$\Rightarrow x = e.$

इसी प्रकार अन्य प्रतिच्छेदन या सर्वनिष्ट (Intersection) के लिये।

अतः $G' = \theta(A_1) \times ... \times \theta(A_k)$। चूँकि $A_i = < a_i >$, $\theta(A_i) = < \theta(a_i) >$

इसलिये समस्त i के लिये $o(\theta(A_i)) = o(\theta(a_i)) = o(a_i)$

समस्त i हेतु p^{n_i}

इस प्रकार G व G' में समान अक्रमविनिमय (Invariants) हैं।

इसके विपरीत मान लें कि G व G' में समान अक्रमविनिमय हैं।

$G = A_1 \times ... \times A_k$, $A_i = < a_i >$ मानें।

तो $G' = B_1 \times ... \times B_k$, $B_i = < b_i >$, $o(A_i) = o(B_i)$

चूँकि G व G' में समान अक्रमविनिमय हैं।

परन्तु समान कोटि की दो चक्रीय समूह तुल्याकारिक हैं। A_i व B_i समस्त i के लिये तुल्याकारिक हैं। अतः $A_1 \times ... \times A_k = G$ व $B_1 \times ... \times B_k = G'$ तुल्याकारिक हैं।

अब हम इस स्थिति में हैं कि कोटि p^n के गैर–तुल्याकारिक परिमित एबेलियन समूह की संख्या को स्पष्टतया दर्शायें।

टिप्पणी

प्रमेय 4.18: कोटि p^n के गैर–तुल्याकारिक एबेलियन समूह की संख्या, p अभाज्य (Prime) n के विभाजन की संख्या के समतुल्य है।

प्रमाण: माना कि p^n कोटि G का एबेलियन समूह हो।

हमें ज्ञात है कि $G = A_1 \times ... \times A_k, A_i = < a_i >, o(A_i) = p^{n_i}$

$o(G) = o(A_1) \ ... \ o(A_k)$

$\Rightarrow \ p^n = p^{n1} ... \ p^{nk} = p^{n1 \ + \ ..... \ + \ nk}$

$\Rightarrow \ n = n_1 + ... + n_k, \ \ n_1 \geq n_2 \geq ..... \geq n_k > 0$

n का विभाजन है।

इसके विपरीत n के किसी विभाजन का विचार करें।

माना कि $n = n_1 + ... + n_k, \ n_1 \geq n_2 \geq ... \geq n_k > 0$, n का विभाजन है।

समस्त i के लिये p^{n_i} कोटि A_i के चक्रीय समूह हैं।

$G = A_1 \times ... \times A_k$ हो तो G कोटि $p^{n1 \ + ... + \ nk = p^n}$ का एबेलियन समूह है।

p^n कोटि A के समस्त गैर–तुल्याकारिक एबेलियन समूह का समुच्चय है।

n, B के समस्त विभाजन का समुच्चय।

$\theta : A \rightarrow B$ को निम्नानुसार परिभाषित करें:

माना $G \in A$. माना $G = A_1 \times ... \times A_k, A_i = < a_i >, o(A_i) = p^{n_i}$.

माना $\theta(G) = n_1 + ... + n_k = n$

स्पष्टतया θ सुपरिभाषित है।

$\theta(G) = \theta(G')$ भी

$\Rightarrow \ \ n_1 + ... + n_k = m_1 + ... + m_l = n$

$\Rightarrow \ k = l, n_i = m_i$ सभी i के लिए।

G व G' में समान अक्रमविनिमय हैं।

G व G' तुल्याकारिक हैं।

$\Rightarrow \ G = G'$

$\Rightarrow \ \theta$, 1–1 है।

माना $n = n_1 + ... + n_k, n_1 \geq n_2 \geq ... \geq n_k > 0, n$ का विभाजन है तो जैसा कि ऊपर देखा जा चुका है $G = A_1 \times ... \times A_k, A_i = < a_i >, p^n$ कोटि $o(A_i) = p^{n_i}$ का एबेलियन समूह है तथा $\theta(G) = n_1 + ... + n_k$

$\therefore \quad \theta$ आच्छादक है।

अतः $o(A) = o(B)$, जिससे परिणाम सिद्ध हुआ।

यह सिद्ध करना कठिन नहीं है कि दो परिमित एबेलियन समूह तुल्याकारिक हैं यदि एवं केवल यदि इनके सइलो उपसमूह तुल्याकारिक हैं। अब प्रमेय 4.14 से हम प्राप्त करते हैं।

प्रमेय 4.19: $n = p_1^{\alpha 1} \ldots p_r^{\alpha r}$ हों जहाँ $p_i s$ सुनिश्चित अभाज्य हैं। तो कोटि n के गैर–तुल्याकारिक एबेलियन समूह की संख्या $p(\alpha_1)\, p(\alpha_2) \ldots\ldots p(\alpha_r)$ है जहाँ $p(\alpha_i)$ से α_i के विभाजन की संख्या इंगित होती है।

टिप्पणी

उदाहरण 4.20: कोटि $(i)\ 8\ \ (ii)\ 6\ \ (iii)\ 20$. के समस्त गैर–तुल्याकारिक एबेलियन समूह ज्ञात करें।

हल:

(i) चूँकि $8 = 2^3$ हो तो $p(3)$, कोटि 8 के गैर–तुल्याकारिक एबेलियन समूह की कोटि 8 द्वारा प्रदर्शित है जहाँ $p(3)$ से 3 के विभाजन की संख्या इंगित होती है।

चूँकि $p(3) = 3$ क्योंकि $3 = 1 + 1 + 1, 3 = 1 + 2, 3 = 3$ केवल 3 के विभाजन मात्र हैं अतः हम कोटि 8 गैर–तुल्याकारिक एबेलियन समूह की संख्या 3 के रूप में ज्ञात करते हैं। तब समूह होंगे: $\mathbf{Z}_8, \mathbf{Z}_2 \times \mathbf{Z}_4, \quad \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$

(ii) चूँकि $6 = 2^1 \times 3^1$ हो तो $p(1)\, p(1)$, गैर–तुल्याकारिक एबेलियन समूह की संख्या $= 1.\ 1 = 1$ है। समूह $\mathbf{Z}_2 \times \mathbf{Z}_3 \cong \mathbf{Z}_6$ चक्रीय समूह हैं।

(iii) चूँकि $20 = 2^2 \times 5^1$ हो तो $p(2)\, p(1) = 2.\ 1 = 2$, कोटि 20 के गैर–तुल्याकारिक एबेलियन समूह की संख्या को इस प्रकार दर्शा सकते हैं: $\mathbf{Z}_4 \times \mathbf{Z}_5, \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5$ जो कि समूह हैं।

4.5.2 गैर–एबेलियन समूह

यदि G के उचित उपसमूह H कोटि p द्वारा विभाजित हो तो समावेशन द्वारा H में p की कोटि का अवयव है, जिससे हमें G में p कोटि का अवयव मिलता है। इस प्रकार हम ऐसा मान सकते हैं कि G के किसी उचित उपसमूह में p द्वारा विभाजित कोटि नहीं है। किसी उचित उपसमूह H के लिये $\#G = (\#H)|G : H|$ व $\#H, p$ द्वारा विभाज्य नहीं है, अतः प्रत्येक उचित उपसमूह H के लिये $p \| G : H|$ है।

अब 1 से अधिक आकार वाले G में संयुग्मित वर्गों को $g_1, g_2, \ldots g_k$ द्वारा प्रस्तुत करते हैं। आकार 1 के संयुग्मित वर्ग $Z(G)$ में अवयव हैं। चूँकि संयुग्मित वर्ग G के विभाजन हैं, संयुग्मित वर्गों की गणना करते हुए $\#G$ की गणना की जाती है।

$$\#\mathrm{G} = \#Z(\mathrm{G}) + \sum_{i=1}^{k} (g_i \text{ के संयुग्मन का आकार}) = \#Z(G) + \sum_{i=1}^{k} |\, G : Z(g_i)\,|$$

जहाँ $Z(g_i), g_i$ का केन्द्रीकरण है। चूँकि प्रत्येक g_i के संयुग्मित वर्ग का आकार 1 से अधिक है, $[G : Z(g_i)] > 1$ अतः $Z(g_i) \neq G$। इसीलिये $p[G : Z(g_i)]$। समीकरण में बाएँ तरफ p द्वारा विभाज्य है व दाएँ तरफ पर योगफल में प्रत्येक निदेशांक p द्वारा विभाज्य है, अतः $\#Z(G)$, p द्वारा विभाज्य है। चूँकि G के उचित उपसमूह में p द्वारा विभाज्य कोटि नहीं है, $Z(G)$ में उप G होने होंगे। इसका तात्पर्य यह कि G एबेलियन है जो एक विरोधाभास (Contradiction) है।

टिप्पणी

अपनी प्रगति जांचिए

7. समूह G के एबेलियनीकरण से आपका क्या अभिप्राय है?
8. परिमित एबेलियन समूह पर आधारभूत प्रमेय का अभिकथन बतायें।

4.7 अपनी प्रगति जांचिए प्रश्नों के उत्तर

1. यदि G एबेलियन हो तो $T: G \to G$ इस प्रकार है कि समस्त $x \in G$ के लिये $T(x) = x-1$, G का स्वाकारिता है।

   यदि $T = I$ तो $T(g) = I(g) \Rightarrow g-1 = g \Rightarrow g2 = e$, तो यह एक विरोधाभास है।

   यदि G गैर–एबेलियन है, तो G का कोई आन्तरिक स्वाकारिता गैर–नगण्य इस प्रकार है,

   $Tx = I$ सभी $x \in G$ के लिए $\Rightarrow Tx(y) = y$ सभी $x, y \in G$ के लिए

   $\Rightarrow xyx-1 = y$ सभी $x, y \in G$ के लिए

   $\Rightarrow xy = yx$ सभी $x, y \in G$ के लिए

   G एबेलियन है जो कि एक विरोधाभास है।

   किसी प्रकरण में G में गैर–नगण्य स्वाकारिता है।

2. स्वाकारिता का आशय समूह G से स्वयं तक तुल्याकारिता से है।
3. G में a के संयुग्मित वर्ग को $cl(a)$ के रूप में प्रस्तुत किया जा सकता है।
4. माना $Z(G) = \{e\}$। माना $o(G)$ हो जहाँ $p, p_1, p_2, ..., p_n$ सुनिश्चित अभाज्य इस प्रकार हों कि,

   $p < p_1 < ... < p_n$, $a > 0$, $\alpha_i \geq 0$. $k(G) > \dfrac{o(G)}{p} = p^{\alpha-1} p_1^{\alpha_1} ... p_n^{\alpha_n}$ एवं

   $Z(G) = \{e\} \Rightarrow \exists$ लम्बाई एक का एकमात्र वर्ग हो एवं कम से कम $p^{\alpha-1} p_1^{\alpha_1} ... p_n^{\alpha_n}$ वर्ग लम्बाई $\geq p$ के हों (चूँकि वर्ग की कोटि $o(G)$ को विभाजित करता है)। इससे एक तत्समक अवयव मिलता है एवं कम से कम $p(p^{\alpha-1} p_1^{\alpha_1} ... p_n^{\alpha_n}) = p^{\alpha} p_1^{\alpha_1} ... p_n^{\alpha_n} = o(G)$ के कम से कम G अवयव जो कि $o(G)$ से अधिक हैं, यह विरोधाभास है। इसी कारण $Z(G) \neq \{e\}$।
5. यदि G तत्समक अवयव e युक्त समूह हो तो उपसमुच्चय $\{e\}$ व G, G के नगण्य उपसमूह हैं एवं हम इन्हें नगण्य उपसमूह कहते हैं। अन्य समस्त उपसमूहों को गैर–नगण्य कहेंगे।
6. G कोई समूह है। $a \in G$ कोई अवयव। उपसमुच्चय $N(a) = \{x \in G \mid xa = ax\}$ को G में a का सामान्यीकरण अथवा केन्द्रीकरण कहा जाता है। यह सरलता से देखा जा सकता है कि सामान्यीकरण G का एक उपसमूह है।

टिप्पणी

7. (i) यह समूह का भागफल है: अपने क्रमविनिमेय उपसमूह द्वारा, अर्थात् यह समूह $G/[G, G]$ है।

   (ii) यह सम्बन्ध G द्वारा $xy = yx$ का भागफल है।

   (iii) यह एक एबेलियन समूह A इस प्रकार है कि आच्छादी सामरूपता इस गुणधर्म वाला है कि जब भी $f: G \to A$ एक समरूपक है एवं $\varphi : G \to H$ एक एबेलियन समूह तो अद्वितीय समरूपक H इस प्रकार होगा कि $\psi: A \to H$ हो $\varphi = \psi \circ f$

8. परिमित एबेलियन समूह चक्रीय समूहों का प्रत्यक्ष गुणन है।

4.8 सारांश

- G कोई समूह हो तो तत्समक मानचित्र $I : G \to G$ इस प्रकार है कि $I(x) = x$, G का नगण्य स्वाकारिता है। वस्तुतः इसे कभी–कभी G का नगण्य स्वाकारिता कहा जाता है।
- यदि G गैर–एबेलियन समूह हो तो उपरोक्त परिभाषित मानचित्र $f: G \to G$ इस प्रकार है कि $f(x) = x^{-1}$ स्वाकारिता नहीं है।
- $I(G)$ के समस्त आन्तरिक स्वाकारिता का समुच्चय G का उपसमूह $\text{Aut}\, G$ है।
- G के उपसमूह H को G का अभिलाक्षणिक उपसमूह कहा जाता है यदि समस्त $T \in \text{Aut}\, G$ हेतु $T(H) \subseteq H$।
- G परिमित समूह हो एवं मान लें कि p एक अभाज्य इस प्रकार है कि $p \mid o(G)$ तो $\exists\, x \in G$ इस प्रकार होगा $o(x) = p$।
- दो क्रमचय $\sigma, \eta \in S_n$ समान होते हैं यदि एवं केवल यदि ये S_n में संयुग्मित हों।
- n एक धनात्मक पूर्णांक है। धनात्मक पूर्णांकों $n_1, n_2, ..., n_k$ का अनुक्रम इस प्रकार है जहाँ $n_1 \le n_2 \le ... \le n_k$ इस प्रकार है कि $n = n_1 + n_2 + ... + n_k$ को n का विभाजन कहा जाता है एवं $n_1, n_2, ..., n_k$ को संयुग्मित के भाग कहा जाता है।
- S_n में संयुग्मित वर्गों की संख्या $p(n)$ है।
- समूह H के गैर–रिक्त उपसमुच्चय G को G का उपसमूह कहा जाता है यदि H से G के द्विआधारी संरचना के अधीन समूह का निर्माण हो।
- यदि G तत्समक अवयव e युक्त समूह हो तो उपसमुच्चय $\{e\}$ व G, G के नगण्य अवयव हैं एवं हम इन्हें नगण्य अवयव कहते हैं। अन्य समस्त उपसमूहों को गैर–नगण्य (अथवा उचित उपसमूह) कहेंगे।
- समूह H का गैर–रिक्त उपसमुच्चय G, G का उपसमूह है यदि,

  $a, b \in H \Rightarrow ab^{-1} \in H$ हो।
- समूह G का गैर–रिक्त परिमित उपसमुच्चय H, G का उपसमूह है यदि G^+, H गुणन के अधीन संवृत हो।

टिप्पणी

- $HK = KH$ का तात्पर्य यह नहीं कि H का प्रत्येक अवयव K के प्रत्येक अवयव से क्रमविनिमय करता है। इसका तात्पर्य केवल यह है कि प्रत्येक $h \in H, k \in K, hk = k_1h_1$ के लिये कुछ $k_1 \in K$ एवं $h_1 \in H$ हो।
- समरूपक के रूप में एबेलियनीकरण भागफल मानचित्र $G \to G/[G, G]$ है जहाँ आधारभूत $[G, G]$, G का क्रमविनिमेय उपसमूह है।
- परिमित एबेलियन समूह इसके साइलो p उपसमूह का प्रत्यक्ष गुणन है।
- माना कि p^n कोटि G का एक एबेलियन समूह हो, p एक अभाज्य एवं G में $a \in G$ में समस्त अवयवों की महत्तम कोटि हो तो $G = A \times Q$ जहाँ A, a द्वारा उत्पन्न एक चक्रीय उपसमूह है एवं $Q \leq G$।
- माना कि p^n कोटि G का एक परिमित एबेलियन समूह हो, p को एक अभाज्य एवं मान लें कि $G = A_1 \times ... \times A_k$ जहाँ प्रत्येक A_i, p^{n_i} युक्त कोटि $n_1 \geq n_2 \geq ... \geq n_k > 0$ का एक चक्रीय उपसमूह है तो पूर्णांक $n_1,..., n_k$ अद्वितीयता से निर्धारित किये जाते हैं एवं ये G के अक्रमविनिमय कहलाते हैं।
- कोटि p^n के दो एबेलियन समूह तुल्याकारिक होते हैं यदि और केवल यदि इनमें समान अक्रमविनिमय हैं।
- कोटि p^n के गैर–तुल्याकारिक एबेलियन समूह की संख्या, p अभाज्य n के विभाजन की संख्या में समतुल्य होती है।
- माना कि $n = p_1^{\alpha 1} ... p_r^{\alpha r}$ हो जहाँ $p_i s$ सुनिश्चित अभाज्य हैं तो कोटि n के गैर–तुल्याकारिक एबेलियन समूहों की संख्या $p(\alpha_1)\, p(\alpha_2).....p(\alpha_r)$ है जहाँ $p(\alpha_i)$ से α_i के विभाजन की संख्या इंगित होती है।

4.9 मुख्य शब्दावली

- **समूह** : यह ऐसी बीजगणितीय संरचना है जिसमें एक संक्रिया के साथ एक हुआ समुच्चय होता है जिसमें तीसरा अवयव निर्माण के लिये इसके कोई दो अवयव संयुक्त होते हैं।
- **नगण्य स्वाकारिता** : यदि G एक समूह हो तो तत्समक मानचित्रण $I : G \to G$ इस प्रकार होगा कि $I(x) = x$, G का नगण्य स्वाकारिता है, इसी कारण इसे G का नगण्य स्वाकारिता कहा जाता है।
- **स्वाकारिकता समूह** : समूह के स्वाकारिक समूहों को ऐसे समूह के रूप में परिभाषित किया जाता है जिसके आधार समूह के समस्त स्वाकारिक अवयव होते हैं, एवं जहाँ समूह संक्रिया स्वाकारिता की संरचना होती है। G के स्वाकारिता के समुच्चय को Aut G से इंगित किया जाता है।
- **तुल्याकारिता** : समूह G का स्वाकारिता एक तुल्याकारिता $G \to G$ है।
- **आन्तरिक स्वाकारिता** : समूह G का स्वाकारिता आन्तरिक है यदि और केवल यदि यह G अंतर्विष्ट प्रत्येक समूह तक विस्तारित है।
- **रूपांतरण समूह** : स्वाकारिता समूह को सममित समूह भी कहा जाता है एवं स्वाकारिता समूह के उपसमूह को रूपांतरण समूह कहा जाता है।

टिप्पणी

- **संयुग्मित** : समूह के दो अवयव a व b संयुग्मित होते हैं यदि समूह में अवयव g इस प्रकार हो कि $b = g^{-1}ag$। यह एक समतुल्यता सम्बन्ध है जिसके समतुल्यता वर्गों को संयुग्मित वर्ग कहा जाता है।

4.10 स्व–मूल्यांकन प्रश्न एवं अभ्यास

लघु–उत्तरीय प्रश्न

1. समूह स्वाकारिता की व्याख्या सोदाहरण करें।
2. आन्तरिक स्वाकारिता के प्रमेय बतायें।
3. स्वाकारिता के समूहों का सोदाहरण वर्णन करें।
4. संयुग्मित सम्बन्ध की व्याख्या करें।
5. केन्द्रीकरण एवं सामान्यीकरण क्या है? सोदाहरण परिभाषित करें।
6. गणना सिद्धांत एवं परिमित समूह के वर्ग समीकरण हेतु प्रमेय बतायें।
7. कॉउची प्रमेय क्या है?
8. कब दो क्रमचय समान होते हैं?
9. 'पूर्णांक के विभाजन' का आशय स्पष्ट करें।
10. परिमित एबेलियन समूहों एवं गैर–एबेलियन समूहों हेतु प्रमेयों की व्याख्या करें।

दीर्घ–उत्तरीय प्रश्न

1. समूह स्वाकारिता की अवधारणा का वर्णन उपयुक्त प्रमेयों, इनके व्युत्पत्ति व उदाहरणों सहित करें।
2. उदाहरणों व प्रासंगिक प्रमेयों की सहायता से आन्तरिक समूह स्वाकारिता की व्याख्या करें।
3. प्रमेय एवं उदाहरणों की सहायता संयुग्मिता सम्बन्ध का वर्णन करें।
4. समूह सिद्धांत के आधार पर उपयुक्त उदाहरणों की सहायता से केन्द्रीकरण व सामान्यीकरण की व्याख्या करें।
5. गणना सिद्धांत एवं परिमित समूहों के वर्ग समीकरण का वर्णन करें। समूह सिद्धांत में इसके महत्व को भी दर्शायें।
6. समूह सिद्धांत हेतु कॉउची प्रमेय का विश्लेषण सोदाहरण करें।
7. परिमित एबेलियन समूह एवं गैर–एबेलियन समूह क्या हैं? उपयुक्त उदाहरणों व प्रमेयों के साथ विस्तृत व्याख्या करें।
8. G एक समूह हो एवं $a \in G$। दर्शायें कि $H = < a > = \{a^n \mid n$ एक पूर्णांक है$\}$ यह G का एक उपसमूह है एवं यदि K अगर G के कोई भी उपसमूह है, तो $a \in K$, तो $H \subseteq K$
9. माना कि $H_n = < n >$ व $H_m = < m >$ हो तो दर्शायें कि $H_n \cap H_m = < k >$ जहाँ $k = \text{L.C.M. } (n, m)$।

टिप्पणी

10. मान लेते हैं कि G परिमित है। सिद्ध करें कि यदि $o(G)$ विषम हो, तो $\{e\}$ एकमात्र संयुग्मित वर्ग X इस प्रकार होगा कि $X = \bar{X}$ । यदि $o(G)$ सम हो, तो दर्शायें कि $\exists$ कम से कम एक संयुग्मित वर्ग $X \neq \{e\}$ इस प्रकार है कि $X = \bar{X}$ ।

11. $o(G) = p^n$, p एक अभाज्य हो एवं $n > 0$। N, G में सामान्य हो G, $(N \neq \{e\})$ तो दर्शायें कि $N \cap Z(G) \neq \{e\}$ ।

12. निम्नांकित कोटि के समस्त गैर–तुल्याकारिक एबेलियन समूह ज्ञात करें:

    (i) 360 [6]

    (ii) 15 [1]

    (iii) 35 [1]

    (iv) p^3, p एक अभाज्य है [3]

4.11 सहायक पाठ्य सामग्री

Sharma, Dr Anil and Jitendra Saini. 2016. *Abstract Algebra* (अमूर्त बीजगणित) Jaipur (Rajasthan): RBD Publisher.

Pathak, Dr H. K. 2017. *Abstract Algebra* (अमूर्त बीजगणित). Kolkata (West Bengal): Siksha Sahitya Prakashan.

Herstein, I. N. 1975. *Topics in Algebra*, 2nd Edition. New York: John Wiley and Sons.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. UK: Cambridge University Press (Indian Edition).

Khanna, V. K. and S. K. Bhambari. 2016. *A Course in Abstract Algebra*, 5th Edition. New Delhi: Vikas Publishing House Pvt. Ltd.

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

Gilbert, Linda. 2008. *Elements of Modern Algebra*. Boston: Cengage Learning.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

Childs, Lindsay N. 2008. *A Concrete Introduction to Higher Algebra*. Berlin: Springer Science & Business Media.

इकाई 5 वलय एवं क्षेत्र

टिप्पणी

संरचना

5.0 परिचय

अमूर्त बीजगणित में विषयों के तीन प्रकार होते हैं, समूह (Groups), वलय (Rings) एवं क्षेत्र (Field)। समूह को ऐसे अवयवों के समुच्चय के रूप में परिभाषित किया जाता है जो उस संक्रिया (Operations) में एकसाथ होते हैं जो इन अवयवों के युग्मों (Pairs) पर प्रदर्शित (Performed) किया जाता है। वलय दो संक्रियाओं (Operations) वाले अवयवों का समुच्चय हैः योग एवं गुणन। वलय के अवयवों (जो योग संक्रिया से एकसाथ हैं) द्वारा समूह बनता है। योग समुच्चय के किन्हीं दो अवयवों के लिये क्रमविनिमेय (Commutative) होता है। निएल्स हेनरिक एबॅल (Niels Henrik Abel) नामक एक गणितज्ञ के सम्मान में 'क्रमविनिमेय' (Commutative) के लिये 'एबेलियन' (Abelian) शब्द का भी प्रयोग किया जाता है। जिसमें गुणन संक्रिया संबद्ध होती है। क्षेत्र ऐसी वलय है जिसमें अवयवों योग के लिये तत्समक (Identity) अवयव एवं गुणन संचालक (Operator) को छोड़कर भी समूह बनता है। गणित में क्षेत्र ऐसा समुच्चय है जिस पर योग, घटाव (Subtraction), गुणन व विभाजन परिमेय व वास्तविक संख्याओं पर संगत (Corresponding) संक्रिया के रूप में परिभाषित होते एवं व्यवहार करते हैं। इसीलिये क्षेत्र एक आधारभूत बीजगणितीय संरचना (Fundamental Algebraic Structure) है जो बीजगणित, संख्या सिद्धांत एवं गणित के अनेक अन्य क्षेत्रों में व्यापक रूप से प्रयोग की जाती है।

प्रधानतया, वलय एक बीजगणितीय संरचना है जिसमें योग व गुणन नामक दो द्विआधारी संक्रिया (Binary Operations) से एकजुट समुच्चय अंतर्विष्ट होता है जहाँ समुच्चय योग के अधीन एक एबेलियन समूह होता है (जिसे वलय का योज्य (Additive) समूह कहते हैं) एवं गुणन के अधीन एक एकाभ (Monoid) इस प्रकार होता है कि योग पर गुणन वितरित हो जाये। वलय अभिगृहीत (Ring Aximos) में आवश्यक है कि योग

टिप्पणी

क्रमविनिमेय (Commutative) हो, योग व गुणन संबद्ध (Associate) हों, गुणन योग पर वितरित हो, समुच्चय में प्रत्येक अवयव में एक योज्य व्युत्क्रम (Additive Inverse) होता है एवं योज्यो का तत्समक मौजूद होता है। वलय के सर्वाधिक देखे जाने वाले उदाहरणों में से एक उदाहरण पूर्णांकों का ऐसा समुच्चय है जिसमें योग व गुणन की अपनी सहज या प्राकृतिक संक्रियाएँ (Natural Operations) सम्पन्न हों।

इस इकाई में आप अमूर्त बीजगणित के संदर्भ में वलय की विभिन्न अवस्थाओं, वलय की परिभाषा व मूलभूत विशेषता/गुण, वलय समरूपता, उपसमूह, आदर्श व योगफल वलय, बहुपद वलय व इनके विशेषता/गुण समाकलित डोमेन व क्षेत्र के बारे में अध्ययन करेंगे।

5.1 उद्देश्य

इस इकाई को पढ़ने के बाद आप–

- वलय सिद्धान्त को समझ पाएंगे;
- वलयों की परिभाषाएँ एवं मूलभूत विशेषताओं गुणों का वर्णन कर पाएंगे;
- वलय समरूपता की व्याख्या कर पाएंगे;
- वलय समरूपता के विभिन्न प्रमेयों को सिद्ध कर पाएंगे;
- उपवलयों की विशेषताओं को पहचान पाएंगे व परिचर्चा कर पाएंगे;
- आदर्श, भागफल व बहुपद वलयों के गुणों एवं विशेषताओं को समझ पाएंगे;
- युक्लिडीयन (Euclidean) के प्रयोग से समाकलित डोमेन एवं क्षेत्रों की परिचर्चा कर पाएंगे;
- अद्वितीय गुणनखंड डोमेन (यूएफ़डी या UFD) का वर्णन कर पाएंगे।

5.2 वलय : परिभाषा एवं मूलभूत विशेषताएं

समूह गैर–रिक्त समुच्चय व द्विआधारी संरचना (Binary Composition) वाली एक प्रणाली है। दो द्विआधारी संरचना वाले गैर–रिक्त समुच्चयों (Non-Empty Sets) की भी चर्चा की जा सकती है, सामान्य योग व गुणन के अधीन पूर्णांकों का समुच्चय एक उदाहरण है। भले ही इस समुच्चय से योग के अधीन समूह का निर्माण होता है, न कि गुणन के अधीन फिर भी इसमें गुणन के सन्दर्भ में भी कुछ विशिष्ट विशेषताएं होती हैं। इनमें से कुछ अलग हटकर होते हैं एवं अवधारणा को वलय के रूप में व्यापीकृत किया जाता है। औपचारिक परिभाषा की चर्चा यहाँ की जा रही है।

परिभाषा: गैर–रिक्त समुच्चय R के साथ दो द्विआधारी संरचना + एवं वलय का निर्माण होना कहा जाता है, यदि निम्नांकित अभिगृहीतों (Axioms) की पूर्ति हो रही हो:

1. समस्त $a + (b + c) = (a + b) + c$ हेतु $a, b, c \in R$
2. $a + b = b + a$ हेतु $a, b \in R$

3. R में $\exists$ कोई अवयव 0 (शून्य) कहा जाता है। इस प्रकार है कि समस्त $a \in R$ हेतु
   $a + 0 = 0 + a = a$
4. प्रत्येक $a \in R$, के लिये $\exists$ अवयव $(-a) \in R$ इस प्रकार हो कि,
   $a + (-a) = (-a) + a = 0$
5. समस्त $a, b, c \in R$ हेतु $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$
6. समस्त $a, b, c \in R$ हेतु $a \,.\, (b + c) = a \,.\, b + a \,.\, c$

   $(b + c) \,.\, a = b \,.\, a + c \,.\, a$

टिप्पणी

ध्यान दें

1. ऐसा कहा जाता है कि + व R पर द्विआधारी संरचना (Binary Composition) हैं ऐसा समझा जाता है कि इनके सन्दर्भ में संवृत (Closure) विशेषताएं R में होते हैं। अन्य शब्दों में समस्त $a, b \in R, a + b$ तथा $a.b$ जो R में है। अद्वितीय हैं।
2. आप + व . के स्थान पर कोई भी अन्य प्रतीक उपयोग में ला सकते हैं परन्तु स्पष्ट कारणों के लिये ये दो प्रतीक प्रयोग किये जाते हैं (इनसे विशेषताएं इतने सहज जो लगते हैं)। वस्तुतः भविष्य में "R एक वलय है" इस अभिकथन का तात्पर्य होगा कि R में दो द्विआधारी संरचना + व . उस पर परिभाषित हैं एवं पूर्ववर्ती अभिगृहीत की पूर्ति करते हैं।
3. अभिगृहीत (5) . के सन्दर्भ में नामांकित संबद्धता है एवं अभिगृहीत (6) को . व + के सन्दर्भ में वितरक (बायीं व दायीं) के रूप में सन्दर्भित (Referred) किया गया है।
4. अभिगृहीत (1) से (4) को सरलता से यह कहते हुए पुनर्कथित किया जा सकता है कि $< R, + >$ से एबेलियन समूह का निर्माण होता है।
5. चूँकि अभिगृहीत (3) में 0, + के सन्दर्भ में तत्समक है, यह स्पष्ट है कि यह अवयव अद्वितीय है।

परिभाषाएँ: वलय R को **क्रमविनिमेय वलय (Commutative Ring)** कहा जाता है यदि समस्त $a, b \in R$ हेतु $ab = ba$ । पुनः यदि $\exists$ अवयव $e \in R$ इस प्रकार हो कि समस्त $a \in R$ हेतु $ae = ea = a$

आप कह सकते हैं कि R ईकाई युक्त वलय है। ईकाई को साधारणतया 1 से इंगित किया जाता है। इसे ईकाई अवयव अथवा गुणक तत्समक (Multiplicative Identity) भी कहा जाता है।

यह सरलता से देखा जा सकेगा कि यदि वलय में ईकाई हो तो यह अद्वितीय ही होगी।

ध्यान दें: स्मरण करें कि समूह में a^2 का तात्पर्य $a \,.\, a$ है जहाँ '.' समूह का द्विआधारी संरचना से था। वलय में भी इसी संकेतन (Notation) के साथ आगे बढ़ें। वस्तुतः यह संकेतन (Notation) योग के लिये यहाँ लाया गया था एवं na का उपयोग यहां $a + a + ...+ a$ (n बार) दर्शाने के लिये किया गया था, जहां n पूर्णांक है।

टिप्पणी

अवधारणा को निम्नांकित उदाहरण स्पष्ट कर देंगे:

- सामान्य योग व गुणन के सन्दर्भ में वलय बनाने वाले पूर्णांकों, परिमेय संख्याओं व वास्तविक संख्याओं के समुच्चय ईकाईयाँ युक्त क्रमविनिमेय वलय हैं।
- समस्त सम पूर्णांकों के समुच्चय **E** से ईकाईयाँ रहित क्रमविनिमेय वलय का निर्माण होता है (सामान्य योग व गुणन के अधीन)।
- माना कि M को आव्यूह योग व आव्यूह गुणन के अधीन पूर्णांकों पर समस्त 2 $\times$ 2 आव्यूहों का समुच्चय मानें। यह देखा जा सकता है कि M से ईकाई युक्त वलय $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ का निर्माण होता है किन्तु यह क्रमविनिमेय नहीं है।
- माना कि M को आव्यूह योग व आव्यूह गुणन के अधीन पूर्णांकों पर प्रकार $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ के समस्त आव्यूह का समुच्चय मानें तो M से ईकाई रहित अक्रमविनिमेय वलय (Non-Commutative Ring) का निर्माण होता है।
- समुच्चय $\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ से योग व गुणन मापांको (Multiplication Module) 7 के अधीन वलय का निर्माण होता है (वस्तुतः हम 7 के स्थान में n को मान सकते हैं)।
- F को समस्त 'सतत् फलनों' (Continuous Functions) $f: \mathbf{R} \to \mathbf{R}$ का समुच्चय मानें जहाँ **R** वास्तविक संख्याओं का समुच्चय हो तो F से योग व गुणन के अधीन वलय का निर्माण निम्नानुसार परिभाषित अनुरूप होता है:

  किसी f हेतु $g \in F$

  समस्त $x \in \mathbf{R}$ हेतु $(f + g)x = f(x)$

  समस्त $x \in \mathbf{R}$ हेतु $(f\,g)x = f(x)g(x)$

  इस वलय का शून्य (Zero) मानचित्रण $O: \mathbf{R} \to \mathbf{R}$ इस प्रकार है कि x समस्त $x \in \mathbf{R}$ हेतु $O(x) = 0$

  किसी $f \in F$ का योज्य व्युत्क्रम फलन (Additive Inverse Function) $(-f) : \mathbf{R} \to \mathbf{R}$ इस प्रकार $(-f)x = -f(x)$

  वस्तुतः F में भी ईकाई होगी, इस फलन के नाम से समस्त $x \in \mathbf{R}$ हेतु $i : \mathbf{R} \to \mathbf{R}$ द्वारा $i(x) = 1$ जो कि परिभाषित है।
- माना कि **Z** पूर्णांकों का समुच्चय हो तो $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$ से सम्मिश्र संख्याओं $a + ib$ के सामान्य योग व गुणन के अधीन वलय का निर्माण होता है जहाँ $a, b \in \mathbf{Z}$ को गॉसियन पूर्णांक (Gaussian Integer) कहा जाता है एवं $\mathbf{Z}[i]$ को गुआसियन पूर्णांक की वलय भी कहा जाता है।

  आपको इसी प्रकार $\mathbf{Z}_n[i]$ गॉसियन पूर्णांक मापांक n की वलय हो सकती है।
  उदाहरण हेतु $\mathbf{Z}_3[i] = \{a + ib \mid a, b \in \mathbf{Z}_3 = \{0, 1, 2\} \bmod 3\}$
  $= \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$

टिप्पणी

- X एक गैर–रिक्त समुच्चय हो तो $P(X)$, X का घात समुच्चय (Power Set) है। (, समस्त उपसमुच्चयों का समुच्चय है।) से + व . जिसके अधीन वलय का निर्माण होता है, जिसे $A + B = (A \cup B) - (A \cap B)$ तथा,

  $A \,.\, B = A \cap B$ द्वारा परिभाषित किया जाता है।

  वस्तुतः यह ईकाई युक्त क्रमविनिमेय वलय है एवं इस गुण की पूर्ति भी करती हैः समस्त $A \in P(X)$ हेतु $A^2 = A$ ।

- पूर्णांक मापांक 2 वलयों से अवयवों (Members) पर समस्त 2×2 आव्यूहों (Matrices) का समुच्चय M है। यह परिमित अक्रमविनिमय वलय (Finite Non-Commutative) होगी। M में $2^4 = 16$ अवयव होंगे क्योंकि आव्यूह $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ में प्रत्येक अवयव a, b, c, d का चयन दो रूपों में किया जा सकता है। M में संरचना (Composition) इस प्रकार दिए गए हैं,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} a \oplus x & b \oplus y \\ c \oplus z & d \oplus u \end{bmatrix}$$

  जहाँ $\oplus$ से योग मापांक 2 दर्शाता है एवं

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} a \otimes x \oplus b \otimes z & a \otimes y \oplus b \otimes u \\ c \otimes x \oplus d \otimes z & c \otimes y \oplus d \otimes u \end{bmatrix}$$

  $\otimes$ से गुणन मापांक 2 दर्शाता है।

  M अक्रमविनिमेय इस प्रकार है $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

  परन्तु $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

- माना $R = \{0, a, b, c\}$ हो। R पर + व . को इस प्रकार परिभाषित करें,

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

.	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	a	b	c
c	0	0	0	0

अब आप देख सकते हैं कि R से ईकाई रहित अक्रमविनिमेय वलय (Non-Commutative Ring) का निर्माण होता है।

वस्तुतः यह लघुतम अक्रमविनिमेय (Smallest Non-Commutative) वलय का उदाहरण है।

प्रमेय 5.1: वलय R में निम्नांकित परिणाम हैं,

(i) $a \,.\, 0 = 0 \,.\, a = 0$ सभी $a \in R$ के लिए

टिप्पणी

(ii) $a(-b) = (-a)b = -ab$ सभी $a, b \in R$ के लिए

(iii) $(-a)(-b) = ab \ \forall \ a, b \in R$

(iv) $a(b-c) = ab - ac \ \forall \ a, b, c \in R$

प्रमाण: (i) $a \cdot 0 = a \cdot (0 + 0)$

$\Rightarrow \quad a \cdot 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow \quad a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow \quad 0 = a \cdot 0$

समूह $< R, + >$ के सन्दर्भ में निष्कासन का प्रयोग करते हुए,

(ii) $a \cdot 0 = 0$

$\Rightarrow \quad a(-b + b) = 0$

$\Rightarrow \quad a(-b) + ab = 0$

$\Rightarrow \quad a(-b) = -(ab)$

इसी प्रकार $(-a)\, b = -ab$

(iii) $(-a)(-b) = -[a(-b)] = -[-ab] = ab$

(iv) $a(b-c) = a(b + (-c))$

$= ab + a(-c)$

$= ab - ac.$

ध्यान दें

1. यदि R ईकाई युक्त एक वलय है एवं $1 = 0$ तो चूँकि किसी $a \in R$ हेतु $a = a.1 = a.0 = 0$ तो आप $R = \{0\}$ पायेंगे जिसे कि नगण्य वलय (Trivial Ring) कहा जाता है। यह प्रकरण साधारणतया वर्जित (Excluded) रहता है एवं जब भी ऐसा कहा जाता है कि R ईकाई युक्त एक वलय है तब यह समझ लिया जाता है कि R में $1 \neq 0$ है।

2. यदि n, m पूर्णांक हों एवं a, b वलय में अवयव हों तो यह सरलता से देखा जा सकता है कि,

$$n(a+b) = na + nb$$
$$(n+m)a = na + ma$$
$$(nm)a = n(ma)$$
$$a^m \, a^n = a^{m+n}$$
$$(a^m)^n = a^{mn}$$

जब भी $ab = 0$ तो या तो $a = 0$ अथवा $b = 0$। यह समझाने में अधिक ज़ोर देने की आवश्यकता पड़ सकती है कि परिणाम सदैव वास्तविक न हो। वस्तुतः पूर्णांकों (वास्तविक अथवा परिमेयों) की वलय में यह गुण होता है। पूर्णांकों पर 2×2 आव्यूह की वलय का विचार करते हैं। आपके पास दो अशून्य (Nonzero) अवयव A, B इस

प्रकार हो सकते हैं कि $A\,B = 0$ परन्तु $A \neq 0\; B \neq 0$। वस्तुतः $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ व

$B = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$ को मान लें तो $A \neq 0, B \neq 0$ किन्तु $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$। हम निम्नांकित परिभाषाओं के माध्यम से इस संकेतन (Notation) को औपचारिक रूप प्रदान करते हैं।

टिप्पणी

परिभाषा 1: R कोई वलय हो। अवयव $0 \neq a \in R$ को शून्य भाजक (Zero Divisor) कहा जाता है यदि $\exists$ अवयव $0 \neq b \in R$ इस प्रकार हो कि $ab = 0$ अथवा $ba = 0$।

परिभाषा 2: क्रमविनिमेय वलय R को समाकलित डोमेन (Integral Domain) कहा जाता है कि R में $ab = 0$ या तो $a = 0$ अथवा $b = 0$ । अन्य शब्दों में क्रमविनिमय वलय R को समाकलित डोमेन कहा जाता है यदि R में कोई शून्य भाजक (Zero Divisors) न हो।

समाकलित डोमेन का एक सुस्पष्ट उदाहरण $< \mathbf{Z}, +, \cdot >$ पूर्णांकों की वलय है जबकि आव्यूहों के वलय (Ring of Matrices) ऐसी वलय का उदाहरण है जो कि समाकलित डोमेन नहीं है।

ध्यान दे : समाकलित डोमेन की परिभाषा के एक भाग के रूप में क्रमविनिमेयता के पद (Condition of Commutativity) पर कुछ लेखक ज़ोर नहीं देते। आपके पास शून्य भाजक (Zero Divisor) रहित अक्रमविनिमेय वलय हो सकती हैं।

किसी क्रमविनिमय वलय को समाकलित डोमेन कब कहा जाता है इस सन्दर्भ में निम्नांकित प्रमेय में हमें आवश्यक व यथात् पद देता है।

प्रमेय 5.2: क्रमविनिमय वलय R समाकलित डोमेन है यदि $a, b, c \in R$ $(a \neq 0)$ सभी के लिए $ab = ac \Rightarrow b = c$।

प्रमाण: माना कि R कोई समाकलित डोमेन हो, तब $ab = ac$ $(a \neq 0)$ है

तो $\quad ab - ac = 0$

$\Rightarrow \quad a(b - c) = 0$

$\Rightarrow \quad a = 0$ तथा $b - c = 0$

चूँकि $\quad a \neq 0$, हम प्राप्त करते हैं $b = c$

इसके विपरीत दिया गया पद यहाँ पूर्ण हो रही है।

माना $a, b \in R$, $a \neq 0$ युक्त कुछ अवयव हों एवं मान लेते हैं कि $ab = 0$

तो $ab = a.0$

$\Rightarrow \quad b = 0$ दिए गए पद के प्रयोग से।

इसलिए $ab = 0 \Rightarrow b = 0$ जब भी $a \neq 0$ अथवा R एक समाकलित डोमेन है।

ध्यान दें: वलय R में बाएँ निष्कासित नियम (Left Cancellation Law) की पूर्ति हुई मानी जाती है यदि समस्त $a, b, c \in R, a \neq 0$ सभी के लिए $ab = ac \Rightarrow b = c$।

इसी प्रकार दाएँ निष्कासित नियम (Right Cancellation Law) की चर्चा की जा सकती है। यह उल्लेखनीय हो सकता है कि निष्कासन केवल अशून्य अवयवों का ही होता है।

टिप्पणी

परिभाषा 1: ईकाई युक्त वलय R में अवयव a को गुणन के सन्दर्भ में अक्रमविनिमेय अथवा ईकाई कहा जाता है यदि $\exists$ किसी भी $b \in R$ में इस प्रकार हों कि $ab = 1 = ba$ है।

ध्यान दें: ईकाई व ईकाई अवयव (Unity) की भिन्न–भिन्न अवधारणाएँ हैं एवं इनमें पारस्परिक असमंजस में न पड़ें।

परिभाषा 2: ईकाई युक्त वलय R को विभक्त वलय अथवा तिरछा क्षेत्र (Skew Field) कहा जाता है यदि R के अशून्य अवयवों (Non Zero Elements) से गुणन के सन्दर्भ में समूह बनता हो।

अन्य शब्दों में ईकाई युक्त वलय R एक विभक्त वलय है यदि R के अशून्य अवयवों में गुणात्मक प्रतिलोम (Multiplication-Inverse) हो।

परिभाषा 3 : क्रमविनिमय विभक्त वलय (Commutative Division Ring) को क्षेत्र (Field) कहते हैं।

वास्तविक संख्याओं (Real Numbers) से क्षेत्र का निर्माण होता है, न कि पूर्णांकों से, सामान्य योग व गुणन के अधीन। चूँकि विभक्त वलय से दो द्विआधारी संरचना के सन्दर्भ में समूहों का निर्माण होता है इसमें दो तत्समक अवयवों 0 व 1 (योग व गुणन के सन्दर्भ में) संरचना ही एवं इस प्रकार विभक्त वलय में कम से कम दो अवयव होते हैं।

प्रमेय 5.3: क्षेत्र एक समाकलित डोमेन है।

प्रमाण: माना कि, $< R, +, . >$ एक क्षेत्र हो तो R एक क्रमविनिमय वलय है।

माना कि, R में $ab = 0$ है। हम $a = 0$ अथवा $b = 0$ दर्शाना चाहते हैं। मान लें कि $a \neq 0$ तो a^{-1} का अस्तित्व है (क्षेत्र की परिभाषा)।

इस प्रकार $ab = 0$

$\Rightarrow \quad a^{-1}(ab) = a^{-1}0$

$\Rightarrow \quad b = 0$

जिससे यह दर्शाया गया है कि R एक समाकलित डोमेन है।

पूर्ववर्ती परिणाम का 'आंशिक विपर्याय' (Partial Converse) भी है।

प्रमेय 5.4: अशून्य परिमित समाकलित डोमेन एक क्षेत्र है।

प्रमाण: R एक अशून्य परिमित समाकलित डोमेन है।

R', R का उपसमुच्चय है जिसमें R के अशून्य अवयव अंतर्विष्ट हैं।

चूँकि R में संबद्धता है अतः यह R' में होगी। इस प्रकार R' एक परिमित अर्द्ध–समूह है।

पुनः निष्कासित नियम (अशून्य अवयवों के लिए) हैं एवं इसीलिये ये R' में हैं।

इसी कारण गुणन के सन्दर्भ में R' एक परिमित अर्द्ध–समूह है जिसमें निष्कासित नियम हैं।

अतः $\therefore < R', \cdot >$ से समूह निर्मित होता है।

अन्य शब्दों में $< R, +, \cdot >$ एक क्षेत्र है। यह क्रमविनिमय है क्योंकि यह एक समाकलित डोमेन है।

टिप्पणी

एलिटरः माना $R = \{a_1, a_2, ..., a_n\}$ एक परिमित अशून्य समाकलित डोमेन (Finite Non Zero Integral Domain) है। माना कि, $0 \neq a \in R$ कोई अवयव हो तो $aa_1, aa_2, ..., aa_n$, सभी R में हैं एवं यदि किसी $i \neq j$ के लिए $aa_i = aa_j$ तो निष्कासन से हम $a_i = a_j$ प्राप्त करते हैं जो कि वास्तविक नहीं है। इसीलिये $aa_1, aa_2, ..., aa_n$, R के सुनिश्चित अवयव हैं।

चूँकि किसी i के लिए $a \in R$, $a = aa_i$ है।

माना कि $x \in R$ कोई अवयव हो तो, किसी j के लिए $x = aa_j$।

इस प्रकार $ax = (aa_i)x = a(a_ix)$

अर्थात् $x = a_ix$

इसी कारण क्रमविनिमेयता के प्रयोग से हम पाते हैं $x = a_ix = xa_i$

अथवा यह a_i, R की ईकाई है। $a_i = 1$ मानें।

इस प्रकार $1 \in R$ हेतु

चूँकि किसी k के लिए $1 = aa_k$

हम पाते हैं कि a_k का गुणात्मक प्रतिलोम (Multiplicative Inverse) a है। इसी कारण R के किसी भी अशून्य अवयव में गुणात्मक प्रतिलोम है अथवा जो कि R क्षेत्र है।

परिभाषाः वलय R को बूलियन वलय (Boolean Ring) कहते हैं यदि $x \in R$ सभी के लिए $x^2 = x$।

उदाहरण 5.1: दर्शायें कि बूलियन वलय क्रमविनिमय है।

हलः माना कि $a, b \in R$ कुछ अवयव हों तो $a + b \in R$ संवृत (Closure) है।

दिए गए पदानुसार,

$$(a + b)^2 = a + b$$

$$\Rightarrow \quad a^2 + b^2 + ab + ba = a + b$$

$$\Rightarrow \quad a + b + ab + ba = a + b$$

$$\Rightarrow \quad ab + ba = 0$$

$$\Rightarrow \quad ab = -ba \qquad ...(i)$$

$$\Rightarrow \quad a(ab) = a(-ba)$$

$$\Rightarrow \quad a^2b = -aba$$

$$\Rightarrow \quad ab = -aba \qquad ...(ii)$$

पुनः समीकरण (i) से

$$(ab)a = (-ba)a$$

$$\Rightarrow \quad aba = -ba^2 = -ba \qquad ...(iii)$$

समीकरण (ii) व समीकरण (iii) से निम्नानुसार समीकरण की प्राप्ति होती है।

$ab = ba\ (= -aba)$

अथवा R क्रमविनिमय है।

टिप्पणी

उदाहरण 5.2: (*i*) दर्शायें कि $\mathbf{Z}_n$, a में अशून्य अवयव एक ईकाई है यदि a व n आपेक्षाकृत अभाज्य (Primes) हों।

(*ii*) यदि a, a ईकाई न हो तो यह एक शून्य भाजक (Zero Divisor) है।

हल: (*i*) $\mathbf{Z}_n = \{0, 1, 2, ..., n-1\} \bmod n$

माना कि, $a \in \mathbf{Z}_n$ एक ईकाई हो तो $\exists\ b \in \mathbf{Z}_n$ इस प्रकार है कि $a \otimes b = 1$

अर्थात् जब ab, n द्वारा विभाजित हो, शेषफल (Remainder) 1 है, अन्य शब्दों में $ab = nq + 1$

अथवा $ab - nq = 1$

a व n आपेक्षाकृत अभाज्य (Prime) हैं।

इसके विपरीत माना कि, $(a, n) = 1$ हो तो $\exists$ पूर्णांक u, v इस प्रकार हैं कि

$$au + nv = 1$$

$$\Rightarrow \quad au = n(-v) + 1$$

मान लें कि $u = nq + r, \quad 0 \le r < n, \quad r \in \mathbf{Z}_n,$

तो $au = anq + ar = n(-v) + 1$

$$\Rightarrow \quad ar = n(-v - aq) + 1, \quad r \in \mathbf{Z}_n$$

अर्थात् $a \otimes r = 1, \quad r \in \mathbf{Z}_n$

अर्थात् a एक ईकाई है।

(*ii*) माना कि, a एक ईकाई न हो एवं मान लें कि महत्तम उभयनिष्ठ भाजक (Greatest Common Divisor) $(a, n) = d > 1$ है।

चूँकि किसी k के लिये $d|a,\ a = dk,\ d|n \Rightarrow n = dt$ भी है,

$$\Rightarrow \quad a.t = dk\ \frac{n}{d} = kn = 0 \bmod n$$

अर्थात् a शून्य भाजक (Zero Divisor) है।

उदाहरण 5.3: दर्शाए कि, $\mathbf{Z}_p = \{0, 1, 2, ..., p-1\}$ का एक क्षेत्र p मापांक है, जहां P एक अभाज्य (Prime) हो।

हल: माना कि, $\mathbf{Z}_p$ एक क्षेत्र हो। मान लें कि p एक अभाज्य (Prime) नहीं है तो $\exists\ a$, b, इस प्रकार होंगे $p = ab,\ 1 < a, b < p$

$\Rightarrow a \otimes b = O$ जहाँ a, b अशून्य हैं, $\mathbf{Z}_p$ में शून्य भाजक (Zero Divisor) हैं।

अर्थात् $\mathbf{Z}_p$ एक समाकलित डोमेन नहीं है जो कि एक विरोधाभास है क्योंकि एक क्षेत्र होने से $\mathbf{Z}_p$ एक समाकलित डोमेन है।

इसी कारण p अभाज्य (Prime) है।

टिप्पणी

इसके विपरीत p एक अभाज्य (Prime) है। अब यह दर्शाते हैं कि $\mathbf{Z}_p$ एक समाकलित डोमेन है (यह परिमित होने के बाद इसी नाते क्षेत्र होगा)।

माना $a \otimes b = 0, a, b \in \mathbf{Z}_p$ हो तो ab, p का गुणज है।

$p \mid a$ अथवा $p \mid b$ (p अभाज्य होता है)

$a = 0$ अथवा $b = 0$ (**ध्यान दें:** $a, b \in \mathbf{Z}_p \Rightarrow a , b < p$))

$\mathbf{Z}_p$ समाकलित डोमेन है एवं इसी कारण क्षेत्र है।

उदाहरण 5.4: यदि ईकाई युक्त वलय R में $x, y \in R$ सभी के लिए $(xy)^2 = x^2y^2$ तो दर्शायें कि R क्रमविनिमय (Commutative) है।

हल: माना कि, $x, y \in R$ कुछ अवयव है तो $y + 1 \in R$ क्योंकि $1 \in R$

दिए गए, पद अनुसार,

$$(x(y + 1))^2 = x^2 (y +1)^2$$

$$\Rightarrow \quad (xy + x)^2 = x^2 (y + 1)^2$$

$$\Rightarrow \quad (xy)^2 + x^2 + xyx + xxy = x^2(y^2 + 1 + 2y)$$

$$\Rightarrow \quad x^2y^2 + x^2 + xyx + xxy = x^2y^2 + x^2 + 2x^2y$$

$$\Rightarrow \quad xyx = x^2y \qquad \text{...(i)}$$

चूँकि समीकरण (i) R में सभी के लिए x, y है अतः यह $x + 1, y$ के लिए भी है। इस प्रकार x से $x + 1$ को विस्थापित करते हुए हमें प्राप्त होता है

$$(x + 1)\, y(x +1) = (x +1)^2y$$

$$\Rightarrow \quad (xy + y)\, (x +1) = (x^2 +1 +2x)y$$

$$\Rightarrow \quad xyx + xy + yx + y = x^2y + y + 2xy$$

समीकरण (i) के प्रयोग से $yx = xy$

इसी कारण R क्रमविनिमेय (Commutative) है।

उदाहरण 5.5: दर्शाएँ कि, कि $[0, 1]$ पर वास्तविक मान के सतत् फलनों का वलय R में शून्य भाजक (Zero Divisor) हैं।

हल: $[0, 1]$ में परिभाषित अनुसार फलनों f व g का विचार इस प्रकार करें

$$f(x) = \frac{1}{2} - x, \quad 0 \le x \le \frac{1}{2}$$

$$= 0, \qquad \frac{1}{2} \le x \le 1$$

एवं $g(x)$-I- $= 0, \quad 0 \le x \le \frac{1}{2}$

$$= x - \frac{1}{2}, \quad \frac{1}{2} \le x \le 1$$

अब f व g सतत् फलन हैं एवं $f \neq 0, g \neq 0$

जबकि $g f(x) = g(x)f(x) = 0 \cdot \left(\frac{1}{2} - x\right)$ यदि $0 \le x \le \frac{1}{2}$

$$= \left(x - \frac{1}{2}\right).0 = 0 \quad \text{यदि} \quad \frac{1}{2} \le x \le 1$$

अर्थात् x सभी के लिए $gf(x) = 0$

टिप्पणी

अर्थात् $gf = 0$ परन्तु $f \neq 0, g \neq 0$

उपवलय (Subrings)

परिभाषा: वलय R के गैर–रिक्त उपसमुच्चय S को R का उपवलय कहा जाता है यदि S से R के द्विआधारी संरचना के अधीन वलय का निर्माण होता है।

पूर्णांकों की वलय $< \mathbf{Z}, +, \cdot >$ वास्तविक संख्याओं की वलय $< \mathbf{R}, +, \cdot >$ का उपवलय है।

यदि R एक वलय है तो $\{0\}$ व R सदा R का उपवलय होंगे जिन्हें R की नगण्य उपवलय (Trivial Subring) कहा जाता है।

यह स्पष्ट है कि समाकलित डोमेन की उपवलय एक समाकलित डोमेन होगी।

व्यवहार में वलय की परिभाषा में समस्त अभिगृहीत को परखना कठिन व समयसाध्य होगा कि कौन–कौन सा उपसमुच्चय उपवलय है व कौन–कौन सा नहीं। प्रमेय 5.5 में यह कार्य तुलनात्मक रूप से सरल हो जायेगा।

प्रमेय 5.5: वलय R का गैर–रिक्त उपसमुच्चय (Non Empty Subset) S, R का उपवलय है यदि,

$a, b \in S$

$\Rightarrow ab, a - b \in S$।

प्रमाण: S, R की उपवलय हो तो $a, b \in S \Rightarrow ab \in S$ (संवृत)

$a, b \in S \Rightarrow a - b \in S$ चूँकि $< R, + >$, $< S, + >$ का उपसमूह है।

इसके विपरीत चूँकि $a, b \in S \Rightarrow a - b \in S$ है। अतः हम पाते हैं कि $< S, + >$ से $< R, + >$ के उपसमूह का निर्माण होता है। पुनः किसी $a, b \in S$ के लिये $S \subseteq R$, चूँकि $a, b \in R$

$\Rightarrow a + b = b + a$

एवं इसलिये S एबेलियन है।

इसी तर्क से हम पाते हैं कि S में गुणन संबद्धता (Multiplicative Associativity) व वितरणशीलता (Distributivity) है।

अन्य शब्दों में S से वलय की परिभाषा में समस्त अभिगृहीत की पूर्ति होती है।

इसी कारण S, R की उपवलय है।

परिभाषा: क्षेत्र F के गैर–रिक्त (Non-Empty) उपसमुच्चय S को उपक्षेत्र (Subfield) कहा जाता है यदि F में संक्रियाओं (Operations) के अधीन S से क्षेत्र का निर्माण होता है। इसी प्रकार हम विभक्त वलय की उपविभक्त वलय (Subdivision Ring) को परिभाषित कर सकते हैं।

यह सिद्ध किया जा सकता है कि S, F का उपक्षेत्र होगा यदि $a, b \in S$, $b \neq 0 \Rightarrow a - b, ab^{-1} \in S$।

ध्यान दें: उपक्षेत्र में सदा ही कम से कम दो अवयव होते हैं, क्षेत्र के 0 व 1 (उस उपसमूह का स्मरण करें जिसमें समूह के तत्समक होते हैं एवं दोनों संरचना के अधीन उपक्षेत्र क्षेत्र का उपसमूह है)।

टिप्पणी

दो उपसमूह का योग (Sub of Two Subrings)

परिभाषा: S व T वलय R की दो उपक्षेत्र हैं। हम परिभाषित करते हैं

$$S + T = \{s + t \mid s \in S, t \in T\}$$

तो स्पष्ट है कि $S + T$, R का गैर–रिक्त उपसमुच्चय (Non Void Subset) है। वस्तुतः,

$$0 = 0 + 0 \in S + T$$

किन्तु योग को परिभाषित करने का हमारा उत्साह यहाँ समाप्त हो जाता है जब हम पाते हैं कि हो सकता है कि दो उपवलय का योग उपवलय न हो।

उदाहरणार्थ पूर्णांकों पर M की 2×2 आव्यूह की वलय मान लें।

माना $S =$ प्रकार $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} a, b$ पूर्णांकों के समस्त आव्यूह का समुच्चय,

$T =$ प्रकार $\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}, x$ पूर्णांकों के समस्त आव्यूह का समुच्चय हो,

तो M व T, S के उपवलय हैं।

$S + T$ में प्रकार $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} + \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$ के अवयव होंगे

अर्थात् प्रकार $\begin{bmatrix} a & c \\ b & 0 \end{bmatrix}$ के आव्यूह

$S + T$ से उपवलय नहीं बनती क्योंकि गुणन के सन्दर्भ में संवृत नहीं है क्योंकि

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \notin S + T.$$

परिभाषा 1: माना कि, S वलय R का उपसमुच्चय हो तो S युक्त R अंतर्विष्ट की सबसे छोटी सबवलय को S द्वारा उत्पन्न उपवलय कहा जाता है।

चूँकि उपवलय का प्रतिच्छेदन या सर्वनिष्ठ (Intersection) एक उपवलय है, इसलिये यह स्पष्ट है कि R के उपसमुच्चय S द्वारा उत्पन्न उपवलय R की समस्त उपवलय का प्रतिच्छेदन या सर्वनिष्ठ (Intersection) होगी जिसमें S अंतर्विष्ट है। हम इसे $<S>$ द्वारा इंगित करते हैं। अब स्पष्ट है कि $< S > = \{0\}$ यदि $S = \varphi$।

परिभाषा 2: माना कि R वलय है, सभी $r \in R$ के लिए समुच्चय $Z(R) = \{x \in R \mid xr = rx$ को वलय का केन्द्र कहते हैं।

यह सरलता से दर्शाया जा सकता है कि $Z(R)$, R का उपवलय है।

उदाहरण 5.6: यदि R एक विभक्त वलय हो तो दर्शायें कि $Z(R)$ का केन्द्र R एक क्षेत्र है।

टिप्पणी

हल: $Z(R)$ एक वलय है (क्योंकि यह एक उपवलय (Subring) है)।

$Z(R)$ की परिभाषानुसार क्रमविनिमेय (Commutative) है।

$Z(R)$ में ईकाई है क्योंकि सभी $x \in R$ के लिए $1 \,.\, x = x \,.\, 1 = x$ ।

इस प्रकार हमें यह दर्शाना है कि $Z(R)$ के प्रत्येक अशून्य अवयव में गुणात्मक प्रतिलोम $\neq Z(R) \neq$ में) है।

माना $x \in Z(R)$ कोई अशून्य अवयव हो तो $x \in R$ तथा चूँकि R एक विभक्त वलय है जो $x^{-1} \in R.$ है।

माना कि, $y \in R$ कोई अशून्य अवयव हो तो $y^{-1} \in R$, अब

$$x^{-1}y = (y^{-1}\, x)^{-1}$$

$= (xy^{-1})^{-1} = yx^{-1}, x^{-1}$ के समस्त अशून्य अवयवों से क्रमविनिमय (Commute) करता है।

पुनः चूँकि $x^{-1} \,.\, 0 = 0 \,.\, x^{-1} = 0$

हम पाते हैं कि सभी $r \in R$ के लिए

$$\Rightarrow \quad x^{-1} \in Z(R)$$

समीकरण यह दर्शा रहा है कि $Z(R)$ एक क्षेत्र है।

उदाहरण 5.7: यदि वलय R में सभी a, b $(a \neq 0)$ के लिए समीकरण $ax = b$ में हल हो तो दर्शायें कि R एक विभक्त वलय (Division Ring) है।

हल: हम सर्वप्रथम यह दर्शाते हैं कि R में शून्य भाजक (Zero Divisor)नहीं है।

मान लें कि $ab = 0, a \neq 0, b \neq 0$

चूँकि $a \neq 0, ax = a$ में हल है, $x = e_1$

तो $\quad ae_1 = a$

पुनः $bx = e_1$ में हल है, माना $x = e_2$ इसका हल हो तो $be_2 = e_1$

अब $ab = 0 \Rightarrow (ab)e_2 = 0 \,.\, e_2 = 0$

$$\Rightarrow a(be_2) = 0$$

$$\Rightarrow ae_1 = 0$$

$a = 0$ परन्तु $a \neq 0$

इसी कारण R शून्य भाजक रहित है।

अब किसी $a \neq 0$ के लिये $ax = a$ में हल है,

टिप्पणी

$x = e$ हल हो तो $ae = a$

सभी x के लिए $aex = ax$

सभी x के लिए $a(ex - x) = 0$

किन्तु सभी x के लिए $a \neq 0 \Rightarrow ex - x = 0$

अथवा e बायीं तत्समक (Left Identity) है।

पुनः $(xe - x)e = xee - xe = x(ee) - xe$

$= xe - xe$ (क्योंकि e बायीं तत्समक है)

$= 0$

परन्तु $e \neq 0$, इस प्रकार $xe - x = 0$ अथवा सभी x के लिए $xe = x$

अर्थात् e दायीं तत्समक (Right Identity) है।

अब समीकरण $ax = e$ में सभी $a \neq 0 \Rightarrow \exists\, b$ के लिये हल इस प्रकार है कि $ab = e$ है।

इसी कारण a में दायाँ प्रतिलोम (Right Inverset) है। चूँकि दायीं तत्समक का भी अस्तित्व है अतः $< R, . >$ से समूह बनता है अथवा R एक विभक्त वलय है।

उदाहरण 5.8: माना R को वास्तविकता पर 3×3 आव्यूह के वलय मानें तो दर्शायें कि,

$$S = \left\{ \begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix} | x \text{ वास्तविक (Real)} \right\}$$

R की उपवलय है एवं इसमें R की ईकाईयाँ से भिन्न ईकाईयाँ हैं।

हल: यह सरलता से देखा जा सकता है कि S, R की उपवलय है। वस्तुतः

$$\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix} \begin{bmatrix} y & y & y \\ y & y & y \\ y & y & y \end{bmatrix} = \begin{bmatrix} 3xy & 3xy & 3xy \\ 3xy & 3xy & 3xy \\ 3xy & 3xy & 3xy \end{bmatrix}$$ जो कि S से संबंधित है।

पुनः चूँकि $\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix} \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix} = \begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix}$ हम पाते हैं।

S में ईकाई $\begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}$ है जो कि R की ईकाई $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ से भिन्न है।

टिप्पणी

ध्यान दे : पूर्ववर्ती उदाहरण में आगे बढ़ते हुए हम निम्नांकित अवलोकन करते हैं:

1. $< \mathbf{Z}, +, . >$ में ईकाई 1 है, परन्तु सम पूर्णांकों की इसकी उपवलय $< \mathbf{E}, +, . >$ में ईकाई नहीं है।
2. $< \mathbf{Z}, +, . >$ में समान ईकाई 1 है, जो कि इसकी मूल वलय (Parent Ring) $< \mathbf{Q}, +, . >$ में है।
3. अन्ततः हम देख सकते हैं कि हमारे पास ईकाई रहित वलय हो सकती है जिसमें ईकाई युक्त वलय है। उदाहरणार्थ वलय $R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} | a,b \in \mathbf{Z} \right\}$ मान लें।

अब यदि $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ इस वलय की ईकाई हो तो $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} a & a \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ होगा, अर्थात् $a = 1$

तथा $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ भी $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ होगा, अर्थात् $a = 1 = b$

इसीलिये यदि R में ईकाई हो तो यह $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ होगा।

किन्तु $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

इसी कारण R में ईकाई नहीं है।

यह परखना सरल है कि $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} | a \in \mathbf{Z} \right\}$, R का उपवलय है एवं इसमें ईकाई $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ है।

उदाहरण 5.9: दर्शायें कि :

(*i*) अभ्याज्य क्रम (Prime Order) की कोई भी वलय क्रमविनिमेय (Commutative Ring) होती है।

(*ii*) हो सकता है कि कोटि p^2 (p अभाज्य) की वलय क्रमविनिमेय (Ring Commutative) न हो।

(*iii*) सबसे छोटी अक्रमविनिमेय वलय क्रम 4 की है।

(*iv*) क्रम p^2 (p अभाज्य) की ईकाई युक्त वलय क्रमविनिमेय (Ring Commutative) है।

हल: इसका हल निम्न हैं–

(*i*) p अभाज्य क्रम (Prime Order) R की वलय हो तो $< R, + >$ एक चक्रीय समूह है। माना कि, $< R, + > = < a >$ हो तो $o(a) = o(R) = p$। माना कि, $x, y \in R$ कुछ अवयव हों तो कुछ पूर्णांकों n, m के लिये $x = na, y = ma$।

टिप्पणी

अब $xy = (na)(ma) = nma^2 = mna^2 = (ma)(na) = yx$। इसी कारण R क्रमविनिमेय (Commutative) है।

(*ii*) R शून्य प्रविष्टि युक्त द्वितीय पंक्ति वाले $\mathbf{Z}_2$ पर 2×2 आव्यूह $\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}, \begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}$ का समुच्चय हो तो R आव्यूह योग (Matrix Addition) व आव्यूह गुणन (Matrix Multiplication) के अधीन वलय है। चूँकि $\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} = \begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$ व $\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix} = \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}$, हम पाते हैं कि R अक्रमविनिमेय है एवं इसमें $4 = 2^2$ अवयव हैं।

(*iii*) क्रम 1 की वलय शून्य (Ring Zero) वलय होने से क्रमविनिमय है। कोटि 2 व कोटि 3 की वलय क्रमविनिमेय से अलग होंगी। इस प्रकार भाग (*ii*) के दृष्टिकोण से हम पाते हैं कि लघुत्तमा अक्रमविनिमय वलय में 4 कोटि होती है।

(*iv*) R ईकाई युक्त एक क्रमविनिमेय हो एवं कोटि p^2 की हो तो यदि $< R, + >$ एक चक्रीय समूह है तो $< R, + >$ क्रमविनिमय है p। यदि $< R, + >$ चक्रीय नहीं है तो $< R, + >$ का प्रत्येक अशून्य अवयव अभाज्य कोटि (Prime Order) p का है। [अवयव की कोटि समूह की कोटि को विभाजित करता है एवं यदि अवयव की कोटि समूह के अवयव के समतुल्य हो तो समूह चक्रीय है]

माना, e से R की ईकाई इंगित करें तो $o(e) = p$ (योग के अधीन)।

माना $S = < e >, R$ की उपवलय है, कोटि p की

तो $S = \{e, 2e, ..., (p-1)e, pe = 0\}, o(S) = p$

चूँकि $o(R) = p^2, \exists\ a \in R$ इस प्रकार है, कि $a \notin S$ व $o(a) = p$ योग के अधीन है।

माना कि, $T = \{a, 2a, ..., (p-1)a, pa = 0\}$ कोटि p के R की उपवलय है। T में प्रत्येक अशून्य अवयव योग के अधीन कोटि p का है।

यदि na से सम्बद्ध $T, (n \neq 0), S$ से भी संबंधित हो तो योग के अधीन उपवलय $< na > = T, S$ में अंतर्विष्ट है।

परन्तु $o(T) = o(S)$ एवं इस प्रकार $< na > = T = S$

अर्थात् $a \in S$, जो कि एक विरोधाभास है।

इसी कारण $S \cap T = \{0\}$

तथा $o(S + T) = \dfrac{o(S) \cdot o(T)}{o(S \cap T)} = p^2 = o(R),$

इस प्रकार $R = S + T$

माना कि $x, y \in R$ हो तो $x = ne + ma, y = re + sa,$ जहाँ n, m, r, s पूर्णांक हैं।

अब $xy = (nr)e + (ns)a + (mr)a + msa^2$

$= yx$

दर्शाया जा रहा है कि R क्रमविनिमेय है।

टिप्पणी

वलय के अभिलक्षण (Characteristic of Ring)

परिभाषाः R एक वलय हो। यदि एक धनात्मक पूर्णांक n इस प्रकार हो कि सभी $a \in R$ के लिए $na = 0$ तो R में परिमित (Finite) गुण कहा जायेगा एवं यह सबसे छोटा धनात्मक पूर्णांक R का अभिलक्षण कहलाता है।

इस प्रकार यह सबसे छोटा धनात्मक पूर्णांक n इस प्रकार है कि R में $1 + 1 + ...+ 1 = 0,\ n$ बार

यदि ऐसा कोई धनात्मक पूर्णांक न हो तो R में अभिलाक्षणिक शून्य (अथवा अनन्त) कहा जाता है।

R के अभिलक्षण को $\text{char}\, R$ अथवा $\text{ch}\, R$ से इंगित किया जाता है।

इसमें निम्नांकित अभिलक्षण होते हैं :

- पूर्णांकों के वलय, सम पूर्णांक, परिमेय, वास्तविक (Reals), सम्मिश्र संख्याएँ सभी Ch शून्य (Zero) होते हैं।
- $R = \{0, 1\}$ का विचार करें तो Mod 2

  $\text{ch}\ R = 2$ जैसे,

  $2 \,.\, 1 = 1 \oplus 1 = 0$

  $2 \,.\, 0 = 0 \oplus 0 = 0$

  इस प्रकार 2 छोटा धनात्मक पूर्णांक इस प्रकार है कि सभी $a \in R$ के लिए $2a = 0$

  ध्यान दें: $1 \,.\, 1 = 1 \neq 0$
- यदि R अशून्य परिमित वलय (Finite Ring) हो तो $\text{ch}\, R \neq 0$ माना कि $o(R) = m > 1$ है। चूँकि $\langle R, + \rangle$ एक समूह है, तब $ma = 0\ \forall\ a \in R$। इसी कारण $\text{ch}\ R \neq 0$

  नोटः $\text{ch}\, R = 1$ यदि $R = \{0\}$।
- $\text{ch}\, \mathbf{Z}_n = n$

  पूर्ववर्ती बिन्दु अनुसार $\text{ch}\ \mathbf{Z}_n \neq 0$. माना $\text{ch}\, \mathbf{Z}_n = m,$

  तो $ma = 0\ \forall\ a \in \mathbf{Z}_n$

  अर्थात् $m \,.\, 1 = 0$

  अर्थात् $1 \oplus 1 \oplus ..... \oplus 1 = 0$ (m बार)

  अथवा $m = nq \Rightarrow n \mid m \Rightarrow m \geq n$

  परन्तु $na = 0\ \forall\ a \in \mathbf{Z}_n$ क्योंकि $o(\mathbf{Z}_n) = n$

एवं इस प्रकार ch $\mathbf{Z}_n \leq n$

अर्थात् $m \quad \leq n, m = n$ देता है

टिप्पणी

प्रमेय 5.6: R ईकाई युक्त वलय (Ring With Unity) है। यदि '1' योज्य कोटि n की है तो ch $R = n$। यदि '1' अनंत योज्य कोटि (Additive Order Infinity) का है तो ch R, 0 है।

प्रमाण: '1' का योज्य कोटि (Additive Order) n हो (इस प्रकार हमारा तात्पर्य है कि समूह $(R, +)$ में 1 का कोटि n है) तो $n \,.\, 1 = 0$ एवं n ऐसा कम धनात्मक पूर्णांक है।

अब किसी $x \in R$ के लिए

$$nx = x + x + ...+ x = 1 \,.\, x + 1 \,.\, x +....+ 1 \,.\, x$$
$$= (1 + 1 + ... + 1)x = 0.x = 0$$

दर्शाया जा रहा है कि ch $R = n$

यदि योग के अधीन 1 में अपरिमित कोटि (Infinite Order) हो तो $\exists . n$ इस प्रकार कि $n \,.\, 1 = 0$ एवं इस प्रकार ch $R = 0$।

ध्यान दे: पूर्ववर्ती परिणाम को इस प्रकार भी लिखा जा सकता है,

यदि R ईकाई युक्त वलय हो R में $n > 0$ है यदि n सबसे छोटा धनात्मक पूर्णांक इस प्रकार है कि $n \,.\, 1 = 0$

प्रमेय 5.7: यदि D एक समाकलित डोमेन (Integral Domain) हो तो D का अभिलाक्षणिक या तो शून्य अथवा अभाज्य संख्या होगा।

प्रमाण: यदि D शून्य हो तो हमारे पास सिद्ध करने को कुछ नहीं है। मान लेते हैं कि D में परिमित अभिलक्षण है तो $\exists\, a$ +ve पूर्णांक m इस प्रकार है कि सभी $a \in D$ के लिए $ma = 0$।

माना k ऐसा कम धनात्मक पूर्णांक हो तो ch $D = k$। हम दर्शाते हैं कि k अभाज्य है। मान लेते हैं कि k अभाज्य नहीं है तो हम लिख सकते हैं,

$k = rs, \;\; 1 < r, s < k$

अब सभी $a \in D$ के लिए $ka = 0$

$\Rightarrow (rs)\, a^2 = 0 \quad \forall \;\; a \in D$

$\Rightarrow a^2 + a^2 + ... + a^2 = 0 \;\; (rs$ बार)

$\Rightarrow (a + a +.....+ a)(a + a +.....+ a) = 0$
(r बार, s बार)

$\Rightarrow (ra)\,(sa) = 0 \;\; \forall \;\; a \in D$

$\Rightarrow ra = 0$ या $sa = 0 \;\; \forall \;\; a \in D$

किसी भी प्रकरण में यह एक विरोधाभास होगा क्योंकि $r, s < k$ व k कम धनात्मक पूर्णांक इस प्रकार है कि $ka = 0$।

इसी कारण k एक अभाज्य है।

टिप्पणी

उदाहरण 5.10: यदि D एक समाकलित डोमेन है एवं यदि किसी $na = 0$ के लिए $0 \neq a \in D$ एवं कोई पूर्णांक $n \neq 0$ तो दर्शायें कि D का अभिलक्षण परिमित है।

हल: चूँकि $na = 0$

सभी $x \in D$ के लिए $(na)x = 0$

$\Rightarrow (a + a + ... + a)x = 0$

$\Rightarrow ax + ax + ... + ax = 0$ (n बार)।

$\Rightarrow a(x + x + ... + x) = 0$ सभी $x \in D$ के लिए।

$\Rightarrow x + x + ...+ x = 0$ सभी $x \in D$ जैसे $a \neq 0$ के लिए।

$\Rightarrow nx = 0$ सभी $x \in D, n \neq 0$ के लिए।

$\Rightarrow$ ch D परिमित है।

ध्यान दे: पूर्ववर्ती परिस्थिति में यदि ch $D = k$, तो $k | n$ है।

चूँकि ch $D = k$, $kx = 0 \forall x \in D$

विभाजन एल्गोरिद्म से (By Division Algorithm),

$$n = kq + r, \quad 0 \leq r < k$$

$\Rightarrow na = kqa + ra$

$\Rightarrow \quad 0 = 0 + ra, \quad 0 \leq r < k$

$\Rightarrow \quad r = 0$ क्योंकि $a \neq 0$.

इसलिए कारण $n = kq \Rightarrow k | n$

उदाहरण 5.11: R एक परिमिति (अशून्य) समाकलित डोमेन है तो $o(R) = p^n$ जहाँ p एक अभाज्य है।

हल: ch R परिमिति है व अभाज्य हो (प्रमेय 5.7 देखें)।

माना ch $R = p$ एक अभाज्य हो।

माना q एक अभाज्य हो जो $o(R)$ को विभाजित कर रहा है। चूँकि $< R, + >$ एक समूह है तो कॉउची प्रमेय (Cauchy's Theorem) के अनुसार $\exists\, a \in R$ इस प्रकार कि $o(a) = q$

तथा $R = p \Rightarrow pa = 0$

$\Rightarrow o(a) | p$

$\Rightarrow q | p$ भी

$\Rightarrow q = p$ क्योंकि p, q अभाज्य (Primes) हैं।

इस प्रकार p एकमात्र अभाज्य है जो $o(R)$ को विभाजित कर रहा है।

$\Rightarrow o(R) = p^n$

उपप्रमेय: (i) परिमित क्षेत्र (Finite Field) की कोटि किसी अभाज्य p के लिये p^n है।

टिप्पणी

(*ii*) ऐसे किसी कोटि वाला समाकलित डोमेन नहीं हो सकता जो दो सुनिश्चित अभाज्य द्वारा विभाज्य (Divisible) हो (अर्थात् क्रम n युक्त ऐसा कोई समाकलित डोमेन हमारे पास नहीं हो सकता जहाँ n को एक से अधिक अभाज्य के गुणनों के रूप में व्यक्त किया जा सके)। अतः हमारे पास 6 अथवा 10 अथवा 12, इत्यादि, अवयवों वाले समाकलिक डोमेन नहीं हो सकते।

ध्यान दे : परिमित डोमेन में ch है, जबकि अपरिमित समाकलित डोमेन में परिमित अथवा शून्य ch हो सकता है।

उदाहरण 5.12: अशून्य (Nonzero) वर्गसम (Idempotent, कभी भी शून्यभावी ≠ Nilpotent) नहीं हो सकता।

हल: माना x अशून्य वर्गसम (Idempotent) हो तो $x^2 = x$।

यदि x शून्यभावी (Nilpotent) भी हो तो $\exists$ पूर्णांक $n \geq 1$ इस प्रकार हुआ $x^n = 0$

किन्तु $x^2 = x \quad \Rightarrow x^3 = x^2 = x$

$\Rightarrow x^4 = x^2 = x$

$\Rightarrow x^n = x \Rightarrow x = 0$ जो कि एक विरोधाभास है।

उदाहरण 5.13: समाकलित डोमेन R (ईकाई युक्त) में वर्गसम (Idempotents) शून्य व ईकाई ही हैं।

हल: माना, $x \in R$ कोई वर्गसम हो तो,

$$x^2 = x \Rightarrow x^2 - x = 0$$

$$\Rightarrow x(x - 1) = 0$$

$\Rightarrow x = 0$ अथवा $x = 1$ क्योंकि R एक समाकलित डोमेन है।

उदाहरण 5.14: यदि R ऐसी वलय है जिसमें अशून्य शून्यभावी अवयव न हो तो दर्शायें कि किसी वर्गसम के लिये $e \in Z(R)$ एवं सभी e, $ex = xe$ के लिए $x \in R$ तथा इस प्रकार है।

हल: e (वर्गसम) $\Rightarrow e^2 = e$,

माना $x \in R$ कोई अवयव हो तो,

$(exe - ex)^2 = exeexe - exeex - exexe + exex$

$= 0$ (को लेने पर $e^2 = e$)

$\Rightarrow exe - ex$ (शून्यभावी) है।

दिए गए पदानुसार $exe - ex = 0 \Rightarrow exe = ex$

इसी प्रकार हम प्राप्त हैं $exe = xe$

इसी कारण $ex = xe$

टिप्पणी

उदाहरण 5.15: वलय $\mathbf{Z}_4$ के सभी वर्गसम व शून्यभावी अवयव ज्ञात करें।

हल: $\mathbf{Z}_4 = \{0, 1, 2, 3\} \bmod 4$

चूँकि $0 \otimes 0 = 0,\ 1 \otimes 1 = 1,\ 2 \otimes 2 = 0,\ 3 \otimes 3 = 1$ हम पाते हैं कि 0 व 1 शून्यभावी हैं।

पुनः चूँकि $2^2 = 2 \otimes 2 = 0$, 2 शून्यभावी है।

0 निश्चय ही शून्यभावी है, 3 शून्यभावी नहीं है क्योंकि $3^3 = 3 \otimes 3 \otimes 3 = 3$

$3^4 = 3 \otimes 3 \otimes 3 \otimes 3 = 1,\ 3^5 = 3$, यह स्पष्ट है कि 3 की घात (Power) में शून्य नहीं आयेगा।

वलयों के गुणन (Product of Rings)

R_1 व R_2 दो वलय हैं।

$R = \{(a, b) \mid a \in R_1, b \in R_2\}$ हो तो यह सरलता से सत्यापित किया जा सकता है कि R से योग व गुणन के अधीन वलय का निर्माण निम्नानुसार होता है :

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) \,.\, (a_2, b_2) = (a_1a_2, b_1b_2)$$

अर्थात् अवयव रीति (Component Wise) से योग व गुणन के सामान्य संघटनों के अधीन। इस वलय को R_1 व R_2 का प्रत्यक्ष गुणन (Direct Product) कहा जाता है। इसी प्रकार दो से अधिक वलय के गुणन की परिभाषा तक पहुँच सकते हैं। R_1 व R_2 को प्रत्यक्ष गुणन (Direct Product) के अवयव वलय कहते हैं।

उदाहरण 5.16: यदि R व S दो वलय हों तो,

ch $(R \times S) = 0$ यदि ch $R = 0$ अथवा $ch\ S = 0$

k जहाँ $k =$ L.C.M. $(ch\ R,$ ch $S)$

हल: माना ch $R = 0$ हो एवं मान लें कि ch $(R \times S) = t \neq 0$

तो $\quad t(a, b) = (0, 0)\ \forall\ a \in R, b \in S$

$\Rightarrow \quad (ta, tb) = (0, 0)$

$ta = 0 \quad \forall\ a \in R$ जो कि एक विरोधाभास है क्योंकि $R = 0$

इस प्रकार ch $(R \times S) = 0$

इसी प्रकार यदि ch $S = 0$ तो ch $(R \times S) = 0$

अब ch $R = m$, ch $S = n$ व $k =$ L.C.M. (m, n)

तो $\quad k(a, b) = (ka, kb) = (0, 0) \quad \forall\ a \in R, b \in S$

चूँकि m, n व k को विभाजित करते हैं।

मान लें कि $p(a, b) = (0, 0)$ तो $(pa, pb) = (0, 0)$

$\Rightarrow \quad pa = 0 = pb \Rightarrow m \mid p, n \mid p$

$\Rightarrow k \mid p \Rightarrow k \leq p \Rightarrow$ ch $(R \times S) = k.$

टिप्पणी

अपनी प्रगति जांचिए

1. $i^2 = j^2 = k^2 = -1$ युक्त $D = \{a + bi + cj + dk \mid a, b, c, d \in R\}$ का विचार करें तो D से गुणन के अधीन वलय बनती है। सिद्ध करें कि D एक विभक्त वलय है परन्तु क्षेत्र नहीं है।
2. वलय में अवयव e को वर्गसम कब कहा जाता है?

5.3 वलय समरूपता

माना कि, $< R, +, \cdot >, < R', *, o >$ दो वलय हैं। मानचित्रण $\theta : R \to R'$ को समरूपता (Homomorphism) कहा जाता है यदि,

$$\theta(a + b) = \theta(a) * \theta(b)$$

$$\theta(ab) = \theta(a)\ o\ \theta(b) \qquad a, b \in R$$

चूँकि हम वलय में द्विआधारी संरचना (Binary Composition) के लिये प्रतीकों + व '.' का प्रयोग वरीयता से करते हैं हम इन प्रतीकों का प्रयोग एक से अधिक वलय के प्रकरण में भी करेंगे। इस प्रकरण में उपरोक्त परिभाषा को यह कहते हुए सरल किया जा रहा है कि मानचित्रण $\theta : R \to R'$ को मानचित्रण कहा जाता है यदि,

$$\theta(a + b) = \theta(a) + \theta(b)$$

$$\theta(ab) = \theta(a)\ .\ \theta(b).....$$

अब वलय में एक–एक आच्छादक (Onto) के रूप में तुल्याकारिता (Isomophism) की चर्चा करते हैं। मानचित्र $f : \mathbf{C} \to \mathbf{C}$, को इस प्रकार विचार करें कि

$$f(a + ib) = a - ib$$

तो f एक समरूपता है जहाँ $\mathbf{C}$ = सम्मिश्र संख्याएँ (Complex Numbers) हैं।

चूँकि $f[(a + ib) + (c + id)] = f((a + c) + i(b + d))$

$$= (a + c) - i(b + d)$$

$$= (a - ib) + (c - id)$$

$$= f(a + ib) + f(c + id)$$

एवं $f[(a + ib)(c + id)] = f((ac - bd) + i(ad + bc))$

$$= (ac - bd) - i(ad + bc)$$

$$= (a - ib)\ c - id\ (a - ib)$$

$$= (a - ib)(c - id)$$

$$= f(a + ib)\ f(c + id)$$

R क्रमविनिमय वलय है एवं मान लें कि सभी $x \in R$ के लिए $px = 0$ जहाँ p एक अभाज्य संख्या है तो मानचित्रण (Mapping) $f : R \to R$ को $f(x) = x^p$ द्वारा परिभाषित किया जाता है, जहाँ $x \in R$ एक समरूपता है।

टिप्पणी

वस्तुतः परिणाम तुलनात्मक रूप से सरलता से आ जाता है यदि हम यह दर्शा सकें $p \mid p_{C_r}, 1 \le r \le p-1$

अब $n = p_{C_r} = \frac{p!}{(p-r)!r!}$

$$= \frac{p(p-1).....(p-r+1)(p-r)!}{(p-r)!1.2....r}$$

$\Rightarrow$ $nr! = p(p-1) .....(p-r+1)$

चूँकि *R.H.S., P* से विभाजित होते हैं अतः इससे $nr!$ विभाजित होगा।

$\Rightarrow p \mid n$ अथवा $p \mid r!$ (जब भी अभाज्य गुणन a, b को विभाजित करता है तो यह a अथवा b में से कम से कम एक पर विभाजित हो) परन्तु $p \nmid r!$ क्योंकि $1, 2, ..., r-1$, p से कम हैं एवं इनमें से किसी के द्वारा p को विभाजित नहीं किया जाता, अतः p द्वारा इनमें से किसी को विभाजित नहीं किया जा सकता। इस प्रकार $p \nmid r!$

अर्थात् $p \mid n$

अब किसी $x, y \in R$ के लिये।

$f(x+y) = (x+y)^p = x^p + p_{C_1} x^{p-1} y + p_{C_2} x^{p-2} y^2 + ... + y^p$

(R क्रमविनिमेय है)

अब $p_{C_1} x^{p-1} y = px^{p-1} y = 0$ क्योंकि $x^{p-1} y \in R$

$p_{C_2} x^{p-2} y^2 = (kp) x^{p-2} y^2 = 0$ क्योंकि $p \mid p_{C_2}$

किसी k के लिए $p_{C_2} = kp$

इसी प्रकार प्रत्येक p_{C_r}, p का कोई गुणज होगा जिसमें अन्य पद (Terms) आ रहे होंगे जो भी शून्य हैं।

इसी कारण $f(x+y) = x^p + y^p = f(x) + f(y)$

$f(xy) = (xy)^p = x^p y^p$ (R क्रम विनिमेय)

$= f(x) f(y)$

इस प्रकार f एक समरूपता है।

प्रमेय 5.8: यदि $\theta : R \to R'$ एक समरूपता हो तो,

(*i*) $\theta(0) = 0'$

(*ii*) $\theta(-a) = -\theta(a)$

जहाँ $0, 0'$ क्रमशः R व R' वलय के शून्य हैं।

प्रमाण: (*i*) चूँकि $0 + 0 = 0$

हमारे पास $\theta(0+0) = \theta(0)$

$\Rightarrow$ $\theta(0) + \theta(0) = \theta(0) + 0'$

$\Rightarrow$ $\theta(0) = 0'$

(*ii*) पुनः चूँकि $a + (-a) = 0,$

$$\theta(a + (-a)) = \theta(0)$$

$$\Rightarrow \quad \theta(a) + \theta(-a) = \theta(0) = 0$$

$$\Rightarrow \quad -\theta(a) = \theta(-a)$$

टिप्पणी

उपप्रमेय: यह स्पष्ट है कि,

$$\theta(a - b) = \theta(a + (-b))$$
$$= \theta(a) - \theta(b)$$

ध्यान दे : आच्छादक समकारिता (Epimorphism), एकाकारिकता (Monomorphism), इत्यादि, की शब्दावली वलयों में भी उसी विस्तारित रूप में अपनायी जाती है जैसे कि समूहों में।

परिभाषा: माना $f: R \to R'$ समरूपक हो तो हम f के आधारभूत (Kernel) को इस प्रकार परिभाषित करते हैं $\text{Ker}\, f = \{x \in R \mid f(x) = 0'\}$

जहाँ $0', R'$ का शून्य है।

निम्नांकित दो प्रमेय सिद्ध करने सरल हैं अतः हम बिना प्रमाण परिणाम कह सकते हैं।

यदि $R \to R'$ समरूपक है तो निम्नांकित प्रमेय लागू होता है।

प्रमेय 5.9: $\text{Ker}\, f$, R का आदर्श (Ideal) है।

प्रमेय 5.10: $\text{Ker}\, f = (0)$ यदि f एक–एक है।

उदाहरण 5.17: यदि R ईकाई युक्त वलय है, एवं $f: R \to R'$ समरूपक है जहाँ R' समाकलित डोमेन इस प्रकार है कि $Ker f \neq R$ तो दर्शायें कि $f(1)$, R' की ईकाई है।

हल: माना $a' \in R'$ कोई अवयव है। हम दर्शाते हैं

$$f(1)\, a' = a' f(1) = a'$$

अब $\quad f(1)\, a' - f(1)\, a' = 0'$

$$\Rightarrow \quad f(1.1)\, a' - f(1)\, a' = 0'$$

$$\Rightarrow \quad f(1) f(1)\, a' - f(1)\, a' = 0'$$

$$\Rightarrow \quad f(1)\, [f(1)\, a' - a'] = 0'$$

$\Rightarrow \quad f(1) = 0'$ अथवा $f(1)\, a' - a' = 0'$ क्योंकि R' एक समाकलित डोमेन है।

$f(1) = 0' \Rightarrow 1 \in \text{Ker}\, f \Rightarrow \text{Ker}\, f = R$ जो कि वास्तविक नहीं है।

इसी कारण $f(1)a' - a' = 0'$

$$\Rightarrow \quad f(1)\, a' = a'$$

इसी प्रकार हम दर्शा सकते हैं कि $a' = a' f(1)$

उदाहरण 5.18: माना $f: R \to R'$ आच्छादक समरूपक है जहाँ R ईकाई युक्त वलय है। प्रदर्शित करें कि $f(1)$, R' की ईकाई है।

हल: माना $a' \in R'$ कोई अवयव है।

टिप्पणी

चूँकि f आच्छादक है, $\exists\ a \in R$ इस प्रकार है $f(a) = a'$

अब $\quad a'.f(1) = f(a).f(1) = f(a.1) = f(a) = a'$

इसी प्रकार $f(1).a' = a'$.

दर्शाया जा रहा है कि $f(1)$, R' की ईकाई है।

उदाहरण 5.19: सोदाहरण दर्शायें कि हमारे पास समरूपता $f: R \to R'$ इस प्रकार हो सकता है कि $f(1)$, R' की ईकाई न हो जहाँ R की ईकाई '1' है।

हल: मानचित्र $f: \mathbf{Z} \to \mathbf{Z}$, का विचार इस प्रकार करें कि सभी $x \in \mathbf{Z}$ के लिए $f(x) = 0$

जहाँ $\mathbf{Z}$ = पूर्णांकों की वलय।

तो f एक समरूपक (Homomorphism) है (सत्यापित करें)

पुनः $f(1) = 0$ परन्तु '0' $\mathbf{Z}$ की ईकाई नहीं है।

इस प्रकार यद्यपि $\mathbf{Z}$ जो **R.H.S.** में है। में ईकाई हो फिर भी यह $f(1)$ के समतुल्य नहीं है।

ध्यान दे :

1. यदि हम मानचित्र $f: \mathbf{Z} \to \mathbf{E}$ को मान लें जहाँ $\mathbf{E}$ अभाज्य पूर्णांकों की वलय तो सभी x के लिए $f(x) = 0$ द्वारा परिभाषित करते हुए हम पाते हैं कि $\mathbf{E}$ में ईकाई नहीं है जबकि '1', $\mathbf{Z}$ की ईकाई है।
2. मानचित्र $f: \mathbf{Z} \to \mathbf{E}$ इस प्रकार है कि $f(x) = 2x$ समूह तुल्याकारिक है। इस प्रकार समूहों के रूप में $\mathbf{Z}$ व $\mathbf{E}$ तुल्याकारिक हैं जबकि $\mathbf{Z}$ व $\mathbf{E}$ वलय के रूप में तुल्याकारिक नहीं हैं। वस्तुतः $\mathbf{Z}$ में ईकाई है परन्तु $\mathbf{E}$ में ईकाई नहीं है। वस्तुतः f में वलय समरूप नहीं होगा।

उदाहरण 5.20: माना कि, $\mathbf{Z}$ को पूर्णांकों की वलय है। दर्शायें कि $\mathbf{Z} \to \mathbf{Z}$ से ही समरूपता तत्समक हैं एवं शून्य मानचित्रण हैं।

हल: माना $f: \mathbf{Z} \to \mathbf{Z}$ समरूपता है।

चूँकि $\quad (f(1))^2 = f(1)f(1) = f(1.1) = f(1)$

$$f(1)[f(1) - 1] = 0$$

$\Rightarrow \qquad f(1) = 0$ अथवा $f(1) = 1$

यदि $f(1) = 0$ तो $f(x) = 0\ \forall$ पूर्णांक x

चूँकि $f(x) = f(1 \cdot x) = f(1)f(x) = 0 \cdot f(x) = 0\ \forall\ x$

इस प्रकार इस प्रकरण में f शून्य (Zero) समरूपता है।

यदि $f(1) = 1$ तो किसी $x \in \mathbf{Z}$ के लिये।

$$f(x) = f(1 + 1 + ...+ 1) = x\,f(1) = x\ (x > 0)$$

$$f(x) = f(-y) = -f(y) = -[f(1 + 1 + ...+ 1)]$$

$$= -y\,f(1) = x\,f(1) = x \ (x < 0,\ y = -x)$$

$$f(0) = 0$$

अतः इस प्रकरण में f तत्समक मानचित्र (Identity Map) है जिससे परिणाम सिद्ध हुआ।

टिप्पणी

प्रमेय 5.11: (वलय समरूप का आधारभूत प्रमेय (Fundamental Theorem of Ring Homomorphism))।

यदि $f: R \to R'$ एक आच्छादक समरूपता हो तो R', R की भागफल वलय (Quotient Ring) से समरूपक है। वस्तुतः $R' \cong \frac{R}{\text{Ker } f}$

प्रमाण: माना कि, f: $R \to R'$ आच्छादक समरूपता हो।

$\varphi : \frac{R}{\text{Ker } f} \to R'$ इस प्रकार परिभाषित करें कि सभी $x \in R$ के लिए $\varphi(x + I) = f(x)$ जहाँ $I = \text{Ker } f$

तो φ इस प्रकार सुपरिभाषित है,

$$x + I = y + I$$

$$\Rightarrow \quad x - y \in I = \text{Ker } f$$

$$\Rightarrow \quad f(x - y) = 0$$

$$\Rightarrow \quad f(x) - f(y) = 0$$

$$\Rightarrow \quad f(x) = f(y)$$

$$\Rightarrow \quad \varphi(x + I) = \varphi(y + I)$$

पूर्वानुसार दिए गए पद द्वारा हम सिद्ध करते हैं कि φ, 1–1 है।

पुनः चूँकि

$$\varphi[(x + I) + (y + I)] = \varphi((x + y) + I) = f(x + y) = f(x) + f(y)$$
$$= \varphi(x + I) + \varphi(y + I)$$

$$\varphi[(x + I)(y + I)] = \varphi(xy + I) = f(xy) = f(x)\,f(y)$$
$$= \varphi(x + I)\ \varphi(y + I)$$

φ एक समरूपता है।

अब यदि $r' \in R'$ कोई अवयव हो तो $f: R \to R'$ आच्छादक है, तो चूँकि $\exists\, r \in R$ आच्छादक है इसलिये r इस प्रकार है कि $f(r) = r'$ के लिए $\varphi(r + I) = f(r) = r'$

हम पाते हैं कि φ के अधीन r' की आवश्यक पूर्व प्रतिबिंब $r + I$ है जिससे दिख रहा है कि φ आच्छादक है एवं इसी कारण तुल्याकारिता है।

इस प्रकार $\frac{R}{\text{Ker } f} \cong R'$। सममित (Symmetry) से $R' \cong \frac{R}{\text{Ker } f}$।

टिप्पणी

प्रमेय 5.12: (तुल्याकारिता का प्रथम प्रमेय (First Theorem of Isomorphism))।

माना कि, $B \subseteq A$ वलय R के दो आदर्श हों तो $\frac{R}{A} \cong \frac{R/B}{A/B}$

प्रमाणः मानचित्रण $f: \frac{R}{B} \to \frac{R}{B}$ को इस प्रकार परिभाषित करें कि $f(r+B) = r+A$ तो f आच्छादक समरूपता है (सिद्ध करें)।

आधारभूत प्रमेय अनुसार, $\frac{R}{A} \cong \frac{R/B}{\text{Ker}\, f}$

पुनः चूँकि $r + B \in \text{Ker}\, f \Leftrightarrow (r + B) = A$

$\Leftrightarrow r + A = A$

$\Leftrightarrow r \in A$

$\Leftrightarrow r + B \in \frac{A}{B}$

हम पाते हैं कि $\text{Ker}\, f = A/B$ है।

इसी कारण $\frac{R}{A} \cong \frac{R/B}{A/B}$.

प्रमेय 5.13: (तुल्याकारिता का द्वितीय प्रमेय (Second Theorem of Isomorphism))।

माना A, B वलय R के दो आदर्श हों तो $\frac{A+B}{A} \cong \frac{B}{A \cap B}$.

प्रमाणः मानचित्रण $f: B \to \frac{A+B}{A}$ को इस प्रकार परिभाषित करें कि $b \in B$ सभी हेतु $f(b) = b + A$ तो f सुपरिभाषित समरूपता है।

पुनः यदि $x + A \in \frac{A+B}{A}$ कोई अवयव हो तो,

$x \in A + B \quad \Rightarrow x = a + b,\ a \in A,\ b \in B$

अतः $x + A = (a + b) + A = (b + a) + A = b + (a + A) = b + A$

इस प्रकार $x + A = b + A = f(b)$

अर्थात् f के अधीन b के पूर्व प्रतिबिंब (Pre-Image) $x + A$ है अथवा f आच्छादक है।

अब आधारभूत प्रमेय अनुसार $\frac{A+B}{A} \cong \frac{B}{\text{Ker}\, f}$

अब $x \in \text{Ker}\, f \Leftrightarrow f(x) = A$

$\Leftrightarrow x + A = A \Leftrightarrow x \in A$

$\Leftrightarrow x \in A \cap B\ (x \in \text{Ker}\, f \subseteq B)$

इसलिए $\text{Ker}\, f = A \cap B$ एवं इस प्रकार $\frac{A+B}{A} \cong \frac{B}{A \cap B}$.

ध्यान दे : अब स्पष्टतया $\frac{A+B}{B} \cong \frac{A}{A \cap B}$

उदाहरण 5.21: दर्शायें कि $\frac{\mathbf{Z}}{<2>} \cong \frac{5\mathbf{Z}}{10\mathbf{Z}}$

टिप्पणी

हल: $A = <2>, B = <5> = 5\mathbf{Z}$, $\mathbf{Z}$ के आदर्श मान लें,

तो $A + B = <d>$ जहाँ d = G.C.D. (2, 5) = 1

$A \cap B = <l>$ जहाँ l = L.C.M. (2, 5) = 10

अतः $A + B = <1> = \mathbf{Z}$

$A \cap B = <10> = 10\mathbf{Z}$

इसी कारण पूर्ववर्ती परिणाम $\frac{A+B}{A} \cong \frac{B}{A \cap B}$ का प्रयोग करते हुए हम प्राप्त करते हैं

$$\frac{\mathbf{Z}}{<2>} \cong \frac{5\mathbf{Z}}{10\mathbf{Z}}$$

प्रमेय 5.14: यदि N वलय R का आदर्श हो तो एक–एक आच्छादक मानचित्रण का अस्तित्व R के सभी आदर्श के समुच्चय के मध्य है, जिनमें N है एवं R/N के आदर्श का समुच्चय।

प्रमाण: माना $f: R \to R/N$, $f(r) = r + N$ द्वारा परिभाषित प्राकृतिक समरूपता है। अब यदि A, R का कोई आदर्श हो तो चूँकि $f: R \to R/N$ आच्छादक समरूपक है, $f(A)$, R/N का आदर्श है।

पुनः $f(A) = \{f(a) \mid a \in A\}$

$= \{a + N \mid a \in A\}$

$= \frac{A}{N}$.

अब, $\mathcal{R}$ के समस्त आदर्श का समुच्चय R है जिसमें N अंतर्विष्ट है एवं $\mathcal{R}'$ के सभी आदर्श का समुच्चय $\frac{R}{N}$ है।

$\varphi : \mathcal{R} \to \mathcal{R}'$ को इस प्रकार परिभाषित करें कि $\varphi(A) = f(A) = \frac{A}{N}$

φ स्पष्टतया सुपरिभाषित है।

पुनः $\varphi(A) = \varphi(B)$

$\Rightarrow f(A) = f(B)$

$\Rightarrow \frac{A}{N} = \frac{B}{N}$

यदि $a \in A$ कोई अवयव हो तो $a + N \in \frac{A}{N} \Rightarrow a + N \in \frac{B}{N}$

टिप्पणी

किसी $b \in B$ के लिए $\Rightarrow a + N = b + N$

$$\Rightarrow a - b \in N \subseteq B$$

किसी $b' \in B$ के लिए $a - b = b'$

तथा इस प्रकार $\Rightarrow \quad a = b + b' \in B$

अर्थात् $A \subseteq B$.

इसी प्रकार $B \subseteq A$ एवं इस प्रकार $A = B$ से दर्शा हो रहा है कि φ एक–एक है।

φ आच्छादक है यह दर्शाने के लिये $X \in \mathcal{K}'$ को कोई अवयव मानें तो X, $\frac{R}{N}$ का आदर्श है।

$A = \{x \in R \mid f(x) \in X\}$ को परिभाषित करें।

हम दर्शाते हैं कि A, φ के अधीन X की आवश्यक पूर्व प्रतिबिंब है।

यह सरलता से परखा जा सकता है कि A, R का आदर्श है।

पुनः $n \in N = \text{Ker}\, f$

$\Rightarrow f(n) = N = \frac{R}{N}$ का शून्य है।

$0 + N \in X$ [क्योंकि आदर्श में शून्य अंतर्विष्ट है]

अतः $f(n) \in X \Rightarrow n \in A$ अथवा $N \subseteq A$

इस प्रकार A, $\mathcal{K}$ का अवयव है।

अब A की परिभाषा से यह पुष्टि होती है कि यह आवश्यक पूर्व प्रतिबिंब है। इसी कारण φ आच्छादक है।

उपप्रमेय (Corollary) : यदि R वलय N का आदर्श हो तो R/N का कोई आदर्श प्रकार A/N का है जहाँ A, R का आदर्श है जिसमें N है।

उदाहरण 5.22: दर्शायें कि $\mathbf{Z}_n \cong \frac{\mathbf{Z}}{(n)}$ होगा।

हल: हमारे पास है $\mathbf{Z}_n = \{0, 1, 2, ..., n-1\}$

$$\frac{\mathbf{Z}}{(n)} = \{(n), 1+(n), 2+(n), ..., \overline{(n-1)}+(n)\}$$

$\theta : \frac{\mathbf{Z}}{(n)} \to \mathbf{Z}_n$, को इस प्रकार परिभाषित करें कि $\theta(r + (n)) = r$,

$0 \le r \le n-1$

माना $\quad r + (n) = s + (n)$ हो एवं मान लें कि $r \neq s$

तो $\quad r - s \in (n) \Rightarrow n \mid (r - s) \Rightarrow n \le r - s$

जहाँ $\quad r, s \le n$। इस प्रकार हमें विरोधाभास मिलता है।

इसी कारण $r = s$ एवं इसलिये θ सुपरिभाषित है।

यह स्पष्टतया 1–1 दर्शा रहा है।

पुनः चूँकि $\theta((r + (n)) + (s + (n))) = \theta(\overline{r + s} + (n))$

किसी $q, t, 0 \le t < n$ हेतु

$= \text{किसी } q, t, 0 \le t < n \text{ के लिए } \theta((nq + t) + (n))$

$= \theta(t + (n)) = t = r \oplus s = \theta(r + (n)) \oplus \theta(s + (n)).$

किसी $q', k, 0 \le k < n$ हेतु $\theta((r + (n))(s + (n))) = \theta(rs + (n))$

$= \theta((nq' + k + (n))$

$= \theta(k + (n)) = k = r \otimes s = \theta(r + (n)) \otimes \theta(s + (n))$

हम पाते हैं कि θ समरूपता है एवं इसी कारण तुल्याकारिता है।

टिप्पणी

अपनी प्रगति जांचिए

3. मानचित्रण $\theta: R \to R'$ को कब समरूपता कहा जाता है?
4. $\mathbf{Z}_{30}$ में अशून्य शून्यभावी अवयव क्यों नहीं हैं?

5.4 आदर्श वलय

वलय में आदर्श की धारणा समूहों में सामान्य उपसमूह की अवधारणा के समानान्तर है। सामान्य उपसमूहों से भागफल समूह का निर्माण होता है, आदर्श तब कार्य करते हैं जब हम भागफल वलय को परिभाषित करते हैं। कई समरूप (Analogous) परिणाम सामने आते हैं। हम निम्नांकित से आरम्भ करते हैं।

परिभाषा: वलय R के गैर–रिक्त उपसमुच्चय I को R का दायाँ आदर्श (Right Ideal) कहा जाता है यदि,

$(i)\ a, b \in I \Rightarrow a - b \in I$

$(ii)\ a \in I, r \in r \Rightarrow ar \in I.$

I को R का बायाँ आदर्श (Left Ideal) कहा जाता है यदि,

$(i)\ a, b \in I \Rightarrow a - b \in I$

$(ii)\ a \in I, r \in R \Rightarrow ra \in I.$

I को R का द्वितरफा (Two Sided) अथवा दोनों ओर (Both Sided) आदर्श कहा जाता है यदि यह बायाँ व दायाँ दोनों आदर्श हो। वस्तुतः यदि हम कहते हैं कि I, R का आदर्श है तो इसका तात्पर्य होगा कि I, R का द्वितरफा (Two Sided) आदर्श है। आदर्श हेतु अन्य तथ्य निम्नानुसार हैं :

- वलय R में $\{0\}$ व R सदैव दोनों ओर आदर्श होते हैं।

  उक्त दो को छोड़कर प्रत्येक आदर्श को उचित (Proper) आदर्श कहा जाता है (वस्तुतः 'गैर–नगण्य आदर्श' (Non-Trivial Ideal) नाम अधिक उपयुक्त होगा)

टिप्पणी

- माना $< \mathbf{Z}, +, \cdot >$ पूर्णांकों की वलय हो तो $\mathbf{E}$ = सम पूर्णांकों का समुच्चय $\mathbf{Z}$ का आदर्श है,

  $a, b \in \mathbf{E} \Rightarrow a = 2n, b = 2m$

  इस प्रकार $a - b = 2(n - m) \in \mathbf{E}$

  पुनः यदि $2n \in \mathbf{E}, r \in \mathbf{Z}$ तो इस अनुरूप $(2n)r$ में $r(2n)$ अथवा $\mathbf{E}, \mathbf{E}$ दोनों आदर्श है।

- माना R = पूर्णांकों पर 2×2 आव्यूह की वलय है।

  माना $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \text{ पूर्णांक} \right\}$ हों तो A, R का दायाँ आदर्श इस प्रकार होगा,

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

  $$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} ax+bz & ay+ba \\ 0 & 0 \end{bmatrix} \in A$$

  किन्तु A, R का दायाँ आदर्श नहीं है क्योंकि $\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} \in I$, $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R$

  परन्तु $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} \notin A.$

- उसी वलय में देखा जा सकता है कि $B = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \right\}$ जहां a, b पूर्णांक है।

  पूर्णांकों से a, b का बायाँ (किन्तु दायाँ नहीं) आदर्श निर्मित होता है। हमें समय के सापेक्ष आदर्श के कई अन्य उदाहरण दिखेंगे। आदर्श व उपवलय की परिभाषा में पदों को देखें तो ज्ञात होता है कि ये दो वस्तुतः निकट सम्बन्धी हैं। वस्तुतः यह सरलता से देखा जा सकता है कि एक आदर्श सदा उपवलय होता है।

  I वलय R का आदर्श है। I एक उपवलय है यह दर्शाने के लिये हमें यह दिखाने की आवश्यकता है कि $a, b \in I$ के लिये $ab \in I$

  अब $a, b \in I \Rightarrow a \in I, b \in I \subseteq R$

  $\Rightarrow ab \in I$ (आदर्श की परिभाषा के अनुसार।)

  इसी कारण I उपवलय है।

- हो सकता है कि उपवलय आदर्श न हो।

  हमें विदित है कि $< \mathbf{Z}, +, \cdot >$, $< \mathbf{Q}, +, \cdot >$ की उपवलय है जहाँ $\mathbf{Z}$ = पूर्णांक, $\mathbf{Q}$ = परिमेय संख्याएँ।

  $3 \in \mathbf{Z}, \frac{1}{5} \in \mathbf{Q}$ परन्तु $3 . \frac{1}{5} \notin \mathbf{Z}$

  इस प्रकार $\mathbf{Z}$ आदर्श नहीं है।

टिप्पणी

हम उपसमूहों, उपवलय इत्यादि के प्रतिच्छेदन या सर्वनिष्ठ (Intersection) व संघ (Union) के बारे में चर्चा करते रहे हैं। ये ही परिणाम आदर्श के प्रकरण में भी होते हैं।

बायें व दायें आदर्श के प्रतिच्छेदन या सर्वनिष्ठ (Intersection) के बारे में हम क्या कह सकते हैं? क्या यह एक आदर्श होगा? उत्तर 'नहीं' में है।

यदि हम पूर्ववर्ती तथ्यों में आदर्श का विचार करें तो हम पाते हैं कि $A \cap B$ में प्रकार,

$\left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a, \text{एक पूर्णांक} \right\}$ के अवयव होंगे।

चूँकि $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin A \cap B$

हम देखते हैं कि $A \cap B$ दायाँ आदर्श नहीं है।

उदाहरण 5.23: R वलय R का गैर–रिक्त उपसमुच्चय है। दर्शायें कि $r(s) = \{x \in R \mid Sx = 0\}$ व $l(s) = \{x \in R \mid xS = 0\}$, R के क्रमशः दायें व बायें आदर्श हैं।

हल: $r(s) \neq \varphi$ क्योंकि $0 \in r(s)$

पुनः $x, y \in r(s) \Rightarrow sx = 0, sy = 0$

अब $S(x - y) = Sx - Sy = 0 - 0 = 0$

$\Rightarrow x - y \in r(s)$

पुनः यदि $r \in R$ कोई अवयव हो तो,

$S(xr) = (Sx)r = 0 \,.\, r = 0$

$\Rightarrow xr \in r(s)$

इसी कारण $r(s)$ दायाँ आदर्श है। इसी प्रकार $l(s)$ यह बायाँ आदर्श बनेगा।

$r(s)$ व $l(s)$ को S के क्रमशः दायें व बायें ऐनहीलेटर (Annihilators) कहा जाता है।

$r(s)$ व $l(s)$ दोनों ही R के आदर्श होंगे यदि R आदर्श है (सत्यापित करें)।

उदाहरण 5.24: R ऐसी वलय हो कि R की प्रत्येक उपवलय R की आदर्श हो। इससे आगे $ab = 0$ में $R \Rightarrow a = 0$ अथवा $b = 0$। दर्शायें कि R क्रमविनिमेय (Commutative) है।

हल: माना $0 \neq a \in R$ कोई अवयव है तो $N(a) = \{x \in R \mid xa = ax\}$, R की उपवलय है एवं इसीलिये R का आदर्श है। $r \in R$ कोई अवयव है। चूँकि $a \in N(a), r \in R$ अतः हम पाते हैं कि $ra \in N(a)$ (आदर्श की परिभाषा (Definition of Ideal))।

तदुपरान्त $a(ra) = (ra)a$ भी है।

एवं इसलिये $(ar - ra)a = 0$

$ar - ra = 0$ क्योंकि $a \neq 0$

टिप्पणी

इस प्रकार $ar = ra \ \forall \ r \in R, \ \forall \ 0 \neq a \in R$

एवं चूँकि $0.r = r.0 = 0$, हम पाते हैं कि $ar \ = ra \ \forall \ a, r \in R$

इसी कारण R क्रमविनिमेय (Commutative) है।

दो आदर्शों का योग (Sum of Two Ideals)

A व B वलय R के दो आदर्श हैं। हम परिभाषित करते हैं कि $A + B$, $\{a + b \mid a \in A, b \in B\}$ ऐसा समुच्चय है जिसे A व B आदर्शों का योग कहा जाता है।

प्रमेय 5.15: यदि A व B, R के दो आदर्श (Ideals) हों तो $A + B$, R का आदर्श है जिसमें A व B दोनों अंतर्विष्ट हैं।

प्रमाण: $A + B \neq \varphi$ क्योंकि $0 = 0 + 0 \in A + B$

पुनः $x, y \in A + B$

$\Rightarrow \qquad x \ = a_1 + b_1$

किसी $a_1, a_2 \in A; b_1, b_2 \in B$ हेतु $y = a_2 + b_2$

चूँकि $\qquad x - y \ = (a_1 + b_1) - (a_2 + b_2)$

$= (a_1 - a_2) + (b_1 - b_2)$

हम पाते हैं कि, $x - y \qquad \in A + B$

माना कि, $x = a + b \in A + B, r \in R$ कुछ अवयव हों तो $xr = (a + b)r = ar + br \in A + B$ क्योंकि A, B आदर्श हैं,

$rs = r(a + b) = ra + rb \in A + B$

इस प्रकार $A + B$, R का आदर्श (Ideal) है।

पुनः किसी $a \in A$ के लिए चूँकि $a = a + 0 \in A + B$ एवं किसी $b \in B$ के लिये, चूँकि $b = 0 + b \in A + B$

हम पाते हैं $A \subseteq A + B$

$B \subseteq A + B.$

ध्यान दें

1. हम दर्शा सकते हैं कि A, $A + B$ का आदर्श है।

   $a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A$ क्योंकि A, R का आदर्श है। पुनः यदि $a \in A$ व $s \in A + B$ कुछ अवयव हों तो कुछ $a_1 \in A, b_1 \in B$ हेतु $s = a_1 + b_1$

   a जैसे $s = a(a_1 + b_1)$

   $= aa_1 + ab_1 \in A$भी

   चूँकि $\qquad a, a_1 \in A \Rightarrow aa_1 \in A$

   $a \in A, b_1 \in B \subseteq R \Rightarrow ab_1 \in A$

   $\Rightarrow \ aa_1 + ab_1 \in A$

   इसी प्रकार $sa \in A$। प्रदर्शित हो रहा है कि A, $A + B$ का आदर्श है।

2. यदि A बायाँ आदर्श हो एवं B, R का दायाँ आदर्श हो तो सम्भव है कि $A+B$, R का आदर्श न हो।

$A+B$ में प्रकार $\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$ के अवयव होंगे।

एवं चूँकि $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 2 & 2 \end{bmatrix} \notin A+B$

$A+B$, R का आदर्श नहीं है।

टिप्पणी

परिभाषाः S वलय R का कोई उपसमुच्चय हो। R का आदर्श A, S द्वारा उत्पन्न कहलायेगा यदि,

(i) $S \subseteq A$

(ii) R के किसी आदर्श I के लिये $S \subseteq I \Rightarrow A \subseteq I$.

हम इसे $A = < S >$ अथवा $A = (S)$ लिखते हुए इंगित करते हैं।

वस्तुतः $< S >$, R के सभी आदर्श (Ideal) का प्रतिच्छेदन या सवनिष्ठ (Intersection) होगा जिसमें S है तथा यह S युक्त सबसे छोटा आदर्श अंतर्विष्ट है। यदि S परिमित हो तो हम कह सकते हैं कि $A = < S >$ परिमित रूप में उत्पन्न हुआ है।

यदि $S = \varphi$ हो तो चूँकि $S = \varphi$ युक्त R का आदर्श है एवं इसलिये

$S = \varphi, < S > \subseteq \{0\}$ और $< S > = \{0\}$।

यदि $S = \{a\}$ तो हम $< S >$ द्वारा $< a >$ इंगित करते हैं एवं अथवा (a) एवं यह प्रकरण हमारी विशेष रुचि का है क्योंकि इसे वास्तव में अत्यधिक उपयोग में लाया जाता है। परिभाषानुसार $a \in < a >$ एवं चूँकि यह आदर्श (Ideal) है, प्रकार $ra, as, r_1 as_1$, na के अवयव $< a >$ में हैं जहाँ $r, r_1, s, s_1 \in R$ व n पूर्णांक है। ऐसे आदर्श को a द्वारा उत्पन्न आदर्श सिद्धांत (Principal Ideal) कहा जाता है। सत्यापित किया जा सकता है कि,

- यदि R क्रमविनिमेय (Commutative) वलय है तो,

  $< S > = \{\Sigma n_i x_i + \Sigma r_j y_j \mid n_i \in \mathbf{Z}, r_j \in R, x_i, y_j \in S\}$
- यदि R ईकाई युक्त क्रमविनिमेय (Commutative) है तो,

  $< S > = \{\Sigma r_j y_j \mid r_j \in R, y_j \in S\}$
- यदि $S = \{a\}$, तो

  $< a > = < S > = \{na + ra + as + xay \mid n \in \mathbf{Z}, r, s, x, y \in R\}$
- इसके आगे यदि R में ईकाई हो $< a > = \{\Sigma\, xay \mid x, y \in R\}$

  योगफल सर्वत्र परिमित है।

प्रमेय 5.16: यदि A व B वलयों R के दो आदर्श हों तो $A + B = < A \cup B >$

प्रमाणः हमने पहले ही सिद्ध कर दिया है, कि $A+B$, R का आदर्श है जिसमें A व B हैं, इस प्रकार $A+B$, $A \cup B$ युक्त आदर्श अंतर्विष्ट है।

माना I, R का आदर्श इस प्रकार है कि $A \cup B \subseteq I$

टिप्पणी

माना $x \in A + B$ अवयव हो तो किसी $x = a + b$ के लिये $a \in A, b \in B$

चूँकि $a \in A \subseteq A \cup B \subseteq I$

$b \in B \subseteq A \cup B \subseteq I$

हम पाते हैं $a + b \in I$ क्योंकि I आदर्श है।

$\Rightarrow \quad x \in I$ अथवा $A + B \subseteq I$

जिससे प्रमेय सिद्ध हुआ।

इस प्रकार $A + B$, R का सबसे छोटा आदर्श है जिसमें A व B है। निश्चय ही दो से अधिक आदर्शों के योग की चर्चा समान रीति में की जा सकती है।

उदाहरण 5.25: यदि $a \in R$ कोई अवयव हो एवं $I = aR = \{ar \mid r \in R\}$ जहाँ R एक क्रमविनिमेय (Commutative) वलय हो तो I, R का आदर्श है।

हल: $I \neq \varphi$ क्योंकि $0 = a \,.\, 0 \in I$

किसी $r_1, r_2 \in R$ के लिए

$$x, y \in I \Rightarrow x = ar_1,\ y = ar_2$$

$$\Rightarrow \qquad x - y = a(r_1 - r_2) \in I$$

पुनः यदि $x = ar_1 \in I$ एवं $r \in R$ अवयव हों तो $x\,r = (ar_1)\,r = a\,(r_1\,r) \in I$ से दर्शाया जाता है कि I दायाँ आदर्श है। R क्रमविनिमेय होने से यह दोनों ओर आदर्श होगा।

ध्यान दे : यदि वलय क्रमविनिमेय न हो तो दर्शाया जा सकता है कि aR, दायाँ आदर्श में अंतर्विष्ट है व $Ra = \{ra \mid r \in R\}$, R का बायाँ आदर्श है।

aR, $< a >$ में सदैव है। यदि R ईकाई युक्त क्रमविनिमेय वलय है तो $aR = Ra = (a)$।

दो आदर्शों के गुणन (Product of Two Ideals)

R वलय A, B के दो आदर्श हैं। हम A, B के A व B के गुणनों को इस प्रकार परिभाषित करते हैं कि

जहाँ $AB = \{\Sigma\, a_i b_i \mid a_i \in A,\ b_i \in B\}$ योगफल परिमित है।

पुनः यदि A एवं B कुछ अवयव हों तो AB से प्रदर्शित होता है कि R दायाँ आदर्श है। क्रमविनिमेय होने से R दोनों ओर आदर्श होगा।

ध्यान दे: यदि वलय क्रमविनिमेय न हो तो दर्शाया जा सकता है कि aR दायाँ आदर्श है व $Ra = \{ra \mid r \in R\}$,. R का बायाँ आदर्श।

aR सदैव $< a >$ में होता है। यदि R ईकाई युक्त क्रमविनिमेय (Commutative) वलय है तो $aR = Ra = (a)$।

प्रमेय 5.17: वलय R के किन्हीं दो आदर्श A व B का गुणन AB, R का आदर्श है।

प्रमाण: $AB \neq \varphi$ क्योंकि $0 = 0 \,.\, 0 \in AB$

$x, y \in AB$ दो अवयव हों

तो $x = a_1b_1 + a_2b_2 + ... + a_nb_n$

$y = a'_1b'_1 + ... + a'_mb'_m$

किसी $a_i, a'_j \in A, b_i, b'_j \in B$ के लिये

$x - y = (a_1b_1 + ... + a_nb_n) - (a'_1b'_1 + ... + a'_mb'_m)$

जो स्पष्टया AB से सम्बद्ध हैं क्योंकि R.H.S. को इस प्रकार लिखा जा सकता है।

$x_1y_1 + x_2y_2 + ... + x_ky_k \quad (k = n + m)$

जहाँ $x_i \in A, y_i \in B.$

पुनः किसी $x = a_1b_1 + ... + a_nb_n \in AB$ हेतु $r \in R$

व $rx = r(a_1b_1 + ... + a_nb_n)$

$= (ra_1)b_1 + (ra_2)b_2 + ... + (ra_n)b_n \in AB$

क्योंकि $ra_i \in A$ क्योंकि $a_i \in A, r \in R$ व A आदर्श है।

इसी प्रकार $xr \in AB.$

इस प्रकार यह दर्शा रहा है कि AB, R का आदर्श है।

ध्यान दे :

1. माना $S = \{ab \mid a \in A. b \in B\}$

तो $< S > = AB$

स्पष्टतः $S \subseteq AB$ एवं चूँकि AB आदर्श है अतः $< S > \subseteq AB$

पुनः $x \in AB \quad \Rightarrow x = \Sigma a_ib_i, a_i \in A, b_i \in B$

$a_i \in A, b_i \in B \Rightarrow a_ib_i \in S, \forall i = 1, 2, ...,$

$\Rightarrow a_ib_i \in < S > \forall i$

$\Rightarrow x \in < S >$

$\Rightarrow AB \subseteq < S >$

तथा इसी कारण $< S > = AB$

2. यदि R ईकाई युक्त क्रमविनिमेय (Commutative) वलय हो एवं R, AB के परिमित उत्पन्नकर्ता (Finitely Generated) आदर्श हों तो इसलिये $A + B$ व AB हैं। वस्तुतः यदि, $A = < a_1, a_2, ..., a_n >$ एवं $B = < b_1, b_2, ..., b_s >$ तो

$A + B = < a_1, a_2, ..., a_r, b_1, b_2, ..., b_s >$

$AB = < a_1b_1, ..., a_1b_s, ..., a_rb_1, ..., a_rb_s >$

वैसे हो सकता है कि यह $A \cap B$ के लिये वास्तविक न हो।

निम्नांकित उदाहरण से हमें आदर्शों के गुणन के विषय में अधिक जानकारियाँ मिल पाती हैं।

उदाहरण 5.26: यदि A व B वलय R का क्रमशः बायाँ व दायाँ आदर्श हो तो दर्शायें कि AB, R का द्वितरफा आदर्श (Two Sided Ideal) है जबकि BA के लिये R का एक ओर आदर्श होना तक आवश्यक नहीं।

टिप्पणी

टिप्पणी

हलः AB, R का द्वितरफा आदर्श उपरोक्त प्रमेयानुसार होगा हम उदाहरण द्वारा यह दर्शाते हैं कि BA को एक–तरफा आदर्श होना भी आवश्यक नहीं है।

$$A = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} | \, a, b, \in \mathbf{Z} \right\}$$

$$B = \left\{ \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} | \, c, d, \in \mathbf{Z} \right\} \text{ मान लेते हैं।}$$

पूर्णांकों पर 2×2 आव्यूह के वलय R में (पहले देखे गये अनुसार अब) A व B, R का क्रमशः बायाँ व दायाँ आदर्श है।

$\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ में प्रकार BA का अवयव होगा।

अर्थात् प्रकार $\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}, x \in \mathbf{Z}$ का,

अब यदि हम BA में $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ व R में $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ मान लें तो,

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin BA$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \notin BA$$

इसी कारण BA, R का न तो दायाँ, न ही बायाँ आदर्श है।

उदाहरण 5.27: यदि A , B, C वलय R के आदर्श इस प्रकार हों: $B \subseteq A$ तो दर्शायें कि $A \cap (B + C) = (A \cap B) + (A \cap C) = B + (A \cap C)$.

हलः $x \in A \cap (B + C)$ अवयव हो तो $x \in A$ व $x \in B + C$

किसी भी $b \in B, c \in C$ के लिए $\Rightarrow x = b + c$

अब $b \in B \subseteq A$, भी $b + c = x \in A$ है।

$\Rightarrow (b + c) - b \in A$

$\Rightarrow c + b - b \in A$

$\Rightarrow c \in A$

$\Rightarrow x \in A \cap C$

अर्थात् $x = b + c, b \in B, c \in A \cap C$

इस प्रकार $x \in B + (A \cap C)$

इसी कारण $A \cap (B + C) \subseteq B + (A \cap C)$.

पुनः $x \in B + (A \cap C)$

तो कुछ $b \in B, k \in A \cap C$ हेतु $x = b + k$

टिप्पणी

चूँकि $b \in B, k \in C$

$x = b + k \in B + C$

एवं $b \in B \subseteq A, k \in A \Rightarrow b + k \in A$

$\Rightarrow x \in A$

$\Rightarrow x \in A \cap (B + C)$

अथवा $B + (A \cap C) \subseteq A \cap (B + C)$

जिससे अन्ततः $A \cap (B + C) = B + (A \cap C)$ मिलता है।

चूँकि $B \subseteq A, A \cap B = B$ भी

इस प्रकार $A \cap (B + C) = (A \cap B) + (A \cap C) = B + (A \cap C)$.

ध्यान दे : पूर्ववर्ती समता को कभी–कभी मापांक (Modular Equality) समता कहा जाता है।

परिभाषा: वलय $R \neq \{0\}$ को सरल वलय (Simple Ring) कहा जाता है यदि R में दो आदर्श न हों (अपवाद R व $\{0\}$)।

प्रमेय 5.18: विभक्त वलय (Division Ring) सरल वलय है।

प्रमाण: माना कि R विभक्त वलय हो। A, R का कोई आदर्श इस प्रकार हो कि $A \neq \{0\}$ तो $\exists$ कम से कम $a \in A$ इस प्रकार होगा $a \neq 0$। R विभक्त वलय होने से $a^{-1} \in R$ एवं $aa^{-1} = 1$।

चूँकि $a \in A, a^{-1} \in R, aa^{-1} \in A$ (आदर्श की परिभाषा के अनुसार)।

$\Rightarrow 1 \in A$

$\Rightarrow A = R$

अर्थात् R के पास दो ही आदर्श हो सकते हैं: R अथवा $\{0\}$ R एक सरल वलय है।

उदाहरण 5.28: R ऐसी वलय है कि R व $\{0\}$ ही R के दायें आदर्श हैं। दर्शायें कि या तो R एक विभक्त वलय है अथवा इसमें अभाज्य संख्या के अवयव इस प्रकार हैं कि समस्त $a, b \in R$ हेतु $ab = 0$।

हल: माना कि $I = \{a \in R \mid aR = \{0\}\}$ हो तो I,R का दायाँ आदर्श है (सत्यापित करें)।

दिए गए पद के अनुसार $I = \{0\}$ अथवा $I = R$

यदि $I = \{0\}$ तो $aR = \{0\}$ तभी जब $a = 0$

अन्य शब्दों में – सभी $0 \neq a \in R$ के लिए $aR = R$ (**ध्यान दे:** aR दायाँ आदर्श है)।

इस प्रकार पूर्ववर्ती समस्या देखें तो R एक विभक्त वलय है (इस प्रकरण में R में एक से अधिक अवयव हैं क्योंकि यदि $R = \{0\}$ तो $R = I$ जो कि आगामी प्रकरण है)।

अब मान लें कि $I = R$ तो समस्त $a \in R$ हेतु $aR = \{0\}$

टिप्पणी

सभी $a, r \in R$ के लिए $ar = 0$

यदि S, $< R, + >$ का कोई उपसमूह हो तो S का दायाँ आदर्श होगा $R\,(a \in S \subseteq R, r \in R \Rightarrow ar = 0 \in S)$। दिए गए पदानुसार R के पास दो ही दायें आदर्शस R व $\{0\}$ हैं। इस प्रकार $< R, + >$ में दो ही उपसमूह R व $\{0\}$ हो सकते हैं।

$\Rightarrow$ $< R, + >$ अभाज्य कोटि (Prime Order) का एक चक्रीय समूह है।

इस प्रकार R में अभाज्य संख्या के अवयव हैं (एवं जैसा कि पहले देखा जा चुका है कि समस्त $a, b \in R$ हेतु $ab = 0$)।

उदाहरण 5.29: सोदाहरण दर्शाएँ कि ईकाई युक्त ऐसी वलय R सम्भव है जहाँ $\{0\}$ व R ही R के आदर्श हों परन्तु R विभक्त विलय न हो।

हल: R, R पर 2×2 आव्यूह की वलय हो तो यह विभक्त विलय नहीं है क्योंकि $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in R$ व्युत्क्रमणीय नहीं है। हम दर्शाते हैं कि R में आदर्श नहीं हैं ($\{0\}$ व R के अतिरिक्त) है। R को $A \neq \{0\}$ का आदर्श मानें।

चूँकि $A \neq \{0\}$ अतः $\exists\ 0 \neq A \in A$। मान लें कि $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$। चूँकि $A \neq 0$, अतः A में कोई प्रविष्टि (Entry) अशून्य है। $a \neq 0$ मानें। माना E_{ij} से R में आव्यूह इंगित होती है जिसकी (i, j) प्रविष्टि 1 व 0 अन्यत्र है। तदुपरान्त 1 व 0 यदि,

$E_{ij}E_{jk} = E_{ik}$ और $E_{ij}E_{rk} = 0$ if $j \neq r$.....

अब $A = aE_{11} + bE_{12} + cE_{21} + dE_{22}$

अतः $AE_{11} = aE_{11} + cE_{21}$

इस प्रकार $a^{-1} E_{11}AE_{11} = E_{11} \Rightarrow E_{11} \in < A >$

$\Rightarrow < E_{11} > \subseteq < A >$

अब $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = E_{11} + E_{22} = E_{11} + E_{21}E_{11}E_{12} \in < E_{11} >$

अतः $< E_{11} > \Rightarrow < E_{11} > = R$ से सम्बद्ध R की ईकाई।

$\Rightarrow R \subseteq < A >$

$\Rightarrow < A > = R$

एवं इसलिये $R = < A > \subseteq A$ क्योंकि $A \in A$

अथवा $A = R$

इसी कारण R अपेक्षित वलय है।

इस प्रकार हम यह समझ सकते हैं कि ईकाई युक्त सरल वलय विभक्त वलय न हो, इसका विपरीत भी वास्तविक हो सकता है।

टिप्पणी

अपनी प्रगति जांचिए

5. यदि A ईकाई युक्त वलय R का एक आदर्श इस प्रकार है कि $1 \in A$ तो दर्शायें कि $A = R$।
6. सिद्ध करें कि विभक्त वलय एक सरल वलय है।

5.5 भागफल वलय

माना कि, R एक वलय है एवं R, I का आदर्श मानें। चूँकि $a, b \in I \Rightarrow a - b \in I$ अतः हम पाते हैं कि $I, <R, +>$ का उपसमूह है। पुनः चूँकि $<R, +>$ एबेलियन है इसलिये I, R का सामान्य उपसमूह होगा एवं इस प्रकार हम $\frac{R}{I}$ भागफल समूह की चर्चा कर सकते हैं जो कि R में I के सभी सहसमुच्चय का समुच्चय $\frac{R}{I} = \{r + I \mid r \in R\}$ है (स्पष्टतया बायें अथवा दायें सहसमुच्चय समतुल्य हैं)।

हमें विदित हैं कि R/I से 'योग' के अधीन समूह का निर्माण इस प्रकार परिभाषित अनुसार होता है,

$$(r + I) + (s + I) = (r + s) + I$$

हम अब R/I पर द्विआधारी संरचना को इस प्रकार परिभाषित करते हैं,

$$(r + I) \cdot (s + I) = rs + I$$

यह परखना एक नियमित कार्य होता है कि यह गुणन R/I पर सुपरिभाषित है।

चूँकि
$$\begin{aligned}(a+I)[(b+I)(c+I)] &= (a+I)(bc+I)\\ &= a(bc) + I\\ &= (ab)c + I\\ &= (ab+I)(c+I)\\ &= [(a+I)(b+I)](c+I)\end{aligned}$$

इस गुणन के सन्दर्भ में संबद्धता (Associativity) है।

पुनः चूँकि
$$\begin{aligned}(a+I)[(b+I)+(c+I)] &= (a+I)(b+c+I)\\ &= a\,(b+c) + I\\ &= (ab+ac) + I\\ &= (ab+I) + (ac+I)\\ &= (a+I)(b+I) + (a+I)(c+I)\end{aligned}$$

हम पाते हैं कि बायीं वितरणशीलता (Left Distributivity) है। इसी प्रकार यह परखा जा सकता है कि दायीं वितरणशीलता (Right Distributivity) भी R/I में है एवं इसी कारण R/I से वलय बनती है जिसे भागफल वलय (Quotient Ring) अथवा I द्वारा R का अवशेष वर्ग (Residue Class) वलय कहते हैं।

टिप्पणी

हम इसे दूसरी दृष्टि से देखते हैं। माना कि R एक वलय हो एवं I, R का आदर्श है। a के लिए $b \in R, a \equiv b \pmod{I}$ को परिभाषित करें यदि $a - b \in I$। यह परखना सरल है कि यह सम्बन्ध R पर समतुल्यता सम्बन्ध है। इस प्रकार यह कि R समतुल्यता वर्गों में विभाजित करता है। a को $a \in R$, $cl(a)$ का संगत (Corresponding) समतुल्यता वर्ग मानें तो$cl(a)$ $= \{r + R \mid r \equiv a \pmod{I}\}$

$$= \{r \in R \mid r - a \in I)\}$$

किसी भी $x \in I$ के लिए $r \in R \mid r - a = x\}$

किसी भी $x \in I$ के लिए $r \in R \mid r = a + x\}$

$$= \{a + x \mid x \in I\}$$

$$= a + I$$

इस प्रकार भागफल वलय R/I कुछ और नहीं, बस पूर्व में परिभाषित अनुसार समस्त समतुल्यता वर्गों की वलय है।

वस्तुतः पूर्व में परिभाषित द्विआधारी संरचना को निम्नांकित में रूपान्तरित किया जायेगा,

$$cl(a) + cl(b) = cl(a + b) \qquad a, b \in R$$

$$cl(a) \,.\, cl(b) = cl(ab)$$

पाठक को यह कार्य रोचक लगेगा जब यह R/I को सत्यापित करेगा जिससे वलय का निर्माण परिभाषित किया जाता है। वस्तुतः यदि R में ईकाई 1 है तो $cl(1)$ में R/I की ईकाई होगी।

इसीलिये R/I को R (Modulo) I का भागफल वलय भी कहा जाता है।

ध्यान दें: यदि $I = R$ तो R/I शून्य वलय (Zero Ring) $\{0\}$ से तुल्याकारिता है एवं यदि $I = \{0\}$ तो $\frac{R}{I} \cong R$।

माना कि $H_4 = \{4n \mid n \in \mathbf{Z}\}$ है जहाँ $< \mathbf{Z}, + \cdot >$ पूर्णांकों की वलय हो तो H_4, $\mathbf{Z}$ का आदर्श है, एवं इस प्रकार $\frac{\mathbf{Z}}{H_4}$ एक भागफल वलय है व इस प्रकार दिया गया है,

$$\frac{\mathbf{Z}}{H_4} = \{H_4, H_4 + 1, H_4 + 2, H_4 + 3\}$$

इस उदाहरण से हमें यह भी दर्शा सकते हैं कि सम्भव है समाकलित डोमेन का भागफल वलय समाकलित डोमेन न हो।

ध्यान दें: $(H_4 + 2)(H_4 + 2) = H_4 + 4 = H_4$, $\frac{\mathbf{Z}}{H_4}$ का शून्य परन्तु $H_4 + 2 \neq H_4$ है।

वहीं दूसरी ओर यदि हम यह विचार करें।

$$R = \{0, 2, 4, 6, 8, 10\} \bmod 12$$

$$S = \{0, 6\} \bmod 12$$

तो R समाकलित डोमेन नहीं है जबकि R/S एक समाकलित डोमेन है।

हमारे पास है, $R/S = \{S, S+2, S+4\}$

चूँकि, $(S+2)(S+2) = S+2$, $(S+2)(S+4) = S+8 = S+2$

एवं, $(S+4)(S+4) = (S+16) = S+4$,

हम पाते हैं, कि R/S में शून्य भाजक नहीं हैं।

टिप्पणी

समाकलित डोमेन के भागफल क्षेत्र (Field of Qutient of Integral Domain)

अमूर्त बीजगणित में समाकलित डोमेन की 'भिन्नों के क्षेत्र' अथवा 'भागफलों के क्षेत्र' सबसे छोटा ऐसा क्षेत्र है जिसमें समाकलित डोमेन समा सकता हो। समाकलित डोमेन R के भिन्नों के क्षेत्र के अवयवों द्वारा a/b के साथ R में a का एवं b 0 के साथ b का निर्माण किया जाता है। वलय R की भिन्नों के क्षेत्र को Quot(R) अथवा Frac(R) से इंगित किया जाता है। इसे भागफल क्षेत्र, भिन्नों के क्षेत्र अथवा भिन्न या खंड क्षेत्र (Fraction Field) कहा जाता है।

यदि R शून्य भाजक रहित कोई क्रमविनिमेय (Commutative) वलय है, एवं कम से कम एक अशून्य अवयव e है तो युग्मों R के समतुल्यता वर्गों के समुच्चय के रूप में Quot(R) की भिन्नों के क्षेत्र (n, d) का निर्माण किया जा सकता है, जहाँ n व d, R के अवयव हैं तथा $d, 0$ नहीं है एवं (n, d), दिए गए नियम के अनुसार समतुल्यता सम्बन्ध (m, d) के समतुल्य है यदि केवल यदि $(nb=md)$। (n, d) व (m, d) के समतुल्यता वर्गों का योग $(nb + md, db)$ का वर्ग है एवं इनका गुणन (mn, db) का वर्ग है। (en, e) के समतुल्यता वर्ग में n मानचित्रण करते हुए अंतःस्थापन (Embedding) दर्शाते हैं। यह अंतःस्थापन e के विकल्प पर निर्भर नहीं है। यदि R एक समाकलित डोमेन हो तो (en, e), $(n, 1)$ के समतुल्य होगा।

R की भिन्नों के क्षेत्र को इस सार्वत्रिक गुणों से पहचाना जाता है कि यदि $f : R \to F$ से क्षेत्र F में अंतःक्षेपित वलय समरूपता (Injective Ring Homomorphism) है तो अद्वितीय वलय समरूपता R का अस्तित्व होता है जो $g : \text{Quot}(R) \to F$ जो f को आगे बढ़ता है।

5.6 बहुपद वलय एवं इनकी विशेषताएं

R कोई वलय है। R पर बहुपद (Polynomial) द्वारा हमारा अभिप्राय R रूप के व्यंजक (Expression) से है।

$$f(x) = a_o + a_1x + a_2x^2 + \ldots + a_mx^m, \qquad a_i \in R$$

x क्या है? यहाँ प्रतीक $x, x^2, \ldots$ अज्ञात अवयवों अथवा वलय R से चर (Variable) नहीं हैं। ये यहाँ केवल सुविधा के लिये हैं, कह सकते हैं कि वलय के अवयवों $a_o, a_1, a_2, \ldots$ के लिये स्थान संसूचकों के रूप में। संकेतन (Notation) के आधार में इस प्रकार के बहुपदों के प्रति हमारा अवगत होना मात्र है जिन्हें हम उपयोग में लाते रहे हैं (एवं इसीलिये x द्वारा चर को प्रस्तुत (Represent) नहीं किया जाता)। इस चिन्ह या संकेतन को अधिक तर्कसंगत करने का प्रयास तब किया जाता है जब हम सामान्य रीति में बहुपदों के योग व गुणन को परिभाषित कर रहे होते हैं।

टिप्पणी

वैकल्पिक रूप से R के अवयवों के अनंत या अपरिमित (Infinite) अनुक्रम (a_o, $a_1, a_2, ...$) को R पर बहुपद कहा जाता है यदि इसके सभी अवयव शून्य हों (इसके पद a_i के परिमित संख्या को छोड़कर), इस प्रकार परिमित संख्या के पद (Finite Number of Terms) के बाद सभी अवयव शून्य होंगे। प्रथम पद a_o को बहुपद का नियतांक कहते हैं। यदि m सबसे बड़ा गैर–ऋणात्मक (Non-Negative) पूर्णांक इस प्रकार हो कि $a_m \neq 0$ तो a_m को बहुपद का अन्तिम गुणांक कहा जाता है।

यदि $\quad f(x) = a_o + a_1x + ... + a_mx^m, \quad a_i \in R$

$\quad g(x) = b_0 + b_1x + ... + b_nx^n, \quad b_j \in R$

R पर दो बहुपद हों तो हम $f(x) = g(x)$ कह सकते हैं कि यदि सभी i के लिए $m = n$ व $a_i = b_i$।

पुनः बहुपदों $f(x)$ व $g(x)$ का योग इस प्रकार परिभाषित किया जा सकता है,

$$f(x) + g(x) = (a_o + b_o) + (a_1 + b_1)\, x + (a_2 + b_2)\, x^2 + ...$$

गुणन भी सामान्य रीति में परिभाषित किया जाता है,

$$\begin{aligned} f(x)\, g(x) &= (a_o + a_1x + ... + a_mx^m)\, (b_o + b_1x + ... + b_nx^n) \\ &= a_ob_o + (a_1b_o + a_ob_1)\, x ... \\ &= c_o + c_1x + c_2x^2 + ... + c_{m+n}\, x^{m+n} \end{aligned}$$

जहाँ $c_k = a_ob_k + a_1b_{k-1} + ... + a_kb_o$

माना कि, $R[x]$, R पर सभी बहुपदों का समुच्चय हो तो $R[x]$ गैर–रिक्त समुच्चय है एवं योग व गुणन को $R[x]$ के अवयवों पर उपरोक्त परिभाषानुरूप देखा जाता है, ये स्पष्टतया द्विआधारी संरचना हैं। यह सरलता से देखा जा सकता है कि $R[x]$ से इन संक्रियाओं (Operations) के अधीन वलय का निर्माण होता है। वलय का शून्य बहुपद होगा।

$$O(x) = 0 + 0x + 0x^2 + ...$$

$f(x) = a_o + a_1x + ... + a_mx^m$ का योज्य व्युत्क्रम (Additive Inverse) का बहुपद $-f(x) = -a_0 - a_1x + ... + (-a_m)\, x^m$ होगा। वस्तुतः यदि R में ईकाई 1 हो तो बहुपद $e(x) = 1 + 0x + 0x^2 +...$, $R[x]$. $e[x]$ की ईकाई होगा। $e[x]$ को कभी–कभी '1' द्वारा भी इंगित किया जाता है। वलय R के स्थान पर यदि हम क्षेत्र F से आरम्भ करें तो हमें बहुपदों (Polynomials) की संगत (Corresponding) वलय $F[x]$ मिलती है।

ध्यान दें: माना $R = \mathbf{Z}_3 = \{0, 1, 2\}$ मापांक 3 हो तो परिभाषित करें कि $f: \mathbf{Z}_3 \to \mathbf{Z}_3$ इस प्रकार है $f(x) = x^3 + 2x$ एवं $g : \mathbf{Z}_3 \to \mathbf{Z}_3$ इस प्रकार है $g(x) = x^5 + 2x$

तदुपरान्त $f(0) = 0 = g(0)$, $f(1) = 1 + 2 = g(1)$

$$f(2) = 5 + 1 = 2 + 4 = g(2)$$

इसी कारण $f(a) = g(a)\ \forall\ a \in \mathbf{Z}_3$

तथा इस प्रकार फलन (Function) द्वारा हमारी परिभाषा है, $f(x) = g(x)$।

वहीं दूसरी ओर $\quad f(x) = (0, 2, 0, 1, 0, 0, ...)$

$$g(x) = (0, 2, 0, 0, 0, 1, 0, ...)$$

$\mathbf{Z}_3$ पर बहुपदों के रूप में समतुल्य नहीं हैं। इस प्रकार $\mathbf{Z}_3[x]$ में $f(x) \neq g(x)$।

परिभाषा: $f(x) = a_o + a_1x + a_2x^2 + ... + a_mx^m$, $R[x]$ में कोई अशून्य बहुपद (Non-Zero Polynomial) है। हम कहते हैं कि $f(x)$ में श्रेणी (Degree) m है यदि सभी $i > m$ के लिए $a_m \neq 0$ व $a_i = 0$ एवं $f(x) = m$ लिखते हैं।

टिप्पणी

हम शून्य बहुपद की श्रेणी (Degree) परिभाषित नहीं करते।

हम कहते हैं कि $f(x)$ की श्रेणी (Degree) शून्य है यदि सभी $i > 0$ हेतु $a_o \neq 0$, $a_i = 0$। इस प्रकरण में इसे अचर बहुपद (Constant Polynomial) कहा जाता है। यह भी स्पष्ट है,

$\deg(-f(x)) = \deg f(x)$ है।

मान लें कि R कोई वलय हो एवं $R[x]$, R पर बहुपदों की संगत वलय है। यदि हम मानचित्र $f: R \to R[x]$ को इस प्रकार परिभाषित करें कि $f(a) = a + 0.x + 0x^2 + ...$

तो यह सरलता से देखा जा सकता है कि

f में 1–1 समरूपता (Homomorphism) होगी। वस्तुतः,

$$\begin{aligned} f(a + b) &= (a + b) + 0x + 0x^2 + ... \\ &= (a + 0x + 0x^2 + ...) + (b + 0x + 0x^2 + ...) \\ &= f(a) + f(b) \\ f(ab) &= ab + 0.x + 0.x^2 + ... \\ &= (a + 0x + 0x^2 + ...)\ (b + 0x + ...) \\ &= f(a)\, f(b) \end{aligned}$$

इसी कारण R को वलय $R[x]$ में समाया जा सकता है। अन्य शब्दों में R, $R[x]$ की उपवलय से तुल्याकारिक है।

इस प्रकार $R[x]$ की उपवलय से R की पहचान की जा सकती है जिसको देखते हुए हम कभी–कभी R को $R[x]$ की उपवलय कह दिया करते हैं।

क्रमविनिमेय वलय (Commutative Ring) वलय पर बहुपद वलय (Polynomial Ring)

निम्नांकित प्रमेय को अब सिद्ध करना सरल है।

प्रमेय 5.19: माना $R[x]$ वलय R पर बहुपदों के वलय हो तो,

(i) R क्रमविनिमेय है, यदि $R[x]$ क्रमविनिमेय हो।

(ii) R में ईकाई है यदि $R[x]$ में ईकाई हो।

प्रमाण: (i) यदि $R[x]$ क्रमविनिमेय हो तो $R[x]$ की कोई उपवलय क्रमविनिमेय है एवं चूँकि R, $R[x]$ की उपवलय से तुल्याकारिक है अतः R क्रमविनिमेय होगा।

इसके विपरीत यदि R क्रमविनिमेय हो एवं

टिप्पणी

$$f(x) = a_o + a_1x + a_2x^2 + ... + a_mx^m$$

$$g(x) = b_o + b_1x + b_2x^2 + ... + b_nx^n$$

$R[x]$ के दो अवयक हों तो गुणन की परिभाषानुसार,

$$f(x)g(x) = a_ob_o + (a_1b_o + a_ob_1)x + ...$$
$$= b_oa_o + (b_1a_o + b_oa_1)x + ...$$
$$= g(x)f(x).$$

(ii) यदि R में ईकाई '1' हो तो बहुपद $e(x) = 1 + 0x + 0x^2 + ..., R[x]$ की ईकाई है क्योंकि $f(x)e(x)$ किसी बहुपद $f(x)$ हेतु $f(x)$ होगा।

इसके विपरीत माना $R[x]$ में ईकाई है।

मानचित्र $\theta : R[x] \to R$ को इस प्रकार परिभाषित करें कि

$$\theta(f(x)) = \theta(a_o + a_1x + .. + a_mx^m) = a_o$$

तो θ आच्छादक समरूपता है।

इस प्रकार R, $R[x]$ की समरूपक प्रतिबिंब (Homomorphic Image) है तथा इसी कारण ईकाई है क्योंकि ईकाई युक्त वलय की समरूपक प्रतिबिंब ईकाई युक्त वलय है। वस्तुतः $\theta(e(x))$, R की ईकाई होगी जहाँ $e(x)$, $R[x]$ की ईकाई है।

प्रमेय 5.20: माना $R[x]$ वलय R के बहुपद की वलय हो एवं मान लें कि,

$$f(x) = a_o + a_1x + ... + a_mx^m$$

$$g(x) = b_o + b_1x + ... + b_nx^n$$

क्रमशः श्रेणी n व m के दो अशून्य बहुपद हैं तोः

1. यदि $f(x) + g(x) \neq 0$, $\deg(f(x) + g(x)) \leq max(m, n)$
2. यदि $f(x)\,g(x) \neq 0$, $\deg(f(x)\,g(x)) \leq m + n$
3. यदि R एक समाकलित डोमेन है, तो $\deg(f(x)\,g(x)) = m + n$ होगा।
4. R समाकलित डोमेन है यदि $R[x]$ एक समाकलित डोमेन हो
5. यदि F एक क्षेत्र हो, $F[x]$ क्षेत्र न हो।

प्रमाणः (1) परिभाषानुसार

$$f(x) + g(x) = (a_o + b_o) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... + (a_t + b_t)x^t$$

जहाँ $t = \text{Max}(m, n)$

अब $a_k + b_k = 0$ सभी $k > t$ जैसे $a_k = 0$, $b_k = 0$ के लिए।

इस प्रकार $f(x) + g(x)$ की श्रेणी $t = \text{Max}(m, n)$ से कम अथवा इसके समतुल्य है।

ध्यान दें: $\deg(f(x) + g(x)) < \text{Max}(m, n)$ होना सम्भव है। पूर्णांकों की वलय $\mathbf{Z}$ का विचार करें।

माना कि $f(x) \quad = 1 + 2x - 2x^2$

टिप्पणी

$g(x) = 2 + 3x + 2x^2$ को $\mathbf{Z}[x]$ के दो अवयव मानें तो,

$f(x) + g(x) = (1 + 2) + (2x + 3x) + (-2x^2 + 2x^2)$

$= 3 + 5x$.....

इस प्रकार $\deg (f(x) + g(x)) = 1$ जबकि $\deg f(x) = 2 = \deg g(x)$

(2) माना कि $f(x)\, g(x) = c_0 + c_1x + c_2x^2 + ...$ हो

जहाँ $c_k = (a_kb_0 + a_{k-1}\, b_1 + ... + a_0b_k)$.

यहाँ $c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + ... + a_mb_n$ ..... $+ a_{m+n}b_0$

$= a_mb_n$

चूँकि समस्त अन्य पद शून्य होंगे (समस्त $i, j > 0$ हेतु $a_{m+i} = 0, b_{n+j} = 0$)।

पुनः समस्त $t > 0$ हेतु $c_{m+n+t} = 0$ तथा,

इस प्रकार $\deg (f(x)\, g(x)) \le m + n$ (a_mb_n शून्य हो सकता है यहाँ तक कि यदि $a_m \neq 0\ b_n \neq 0$ हो तब भी।

हम दर्शाते हैं कि ऐसा सम्भव है $\deg (f(x)\, g(x)) < m + n$

वलय $R = \{0, 1, 2, 3, 4, 5\}$ पर मापांक 6 का विचार करें।

$f(x) = 1 + 2x^3$

$g(x) = 2 + x + 3x^2$को मान लें जो कि क्रमशः श्रेणी 3 व 2 के $R[x]$ में दो बहुपद हैं।

यहाँ $f(x)g(x) = 2 + x + 3x^2 + 4x^3 + 2x^4$

जिसकी श्रेणी $4 < 5$ है।

ध्यान दें: यहाँ R समाकलित डोमेन नहीं है।

(3) यदि R एक समाकलित डोमेन हो तो चूँकि $a_m \neq 0, b_n \neq 0$ इसीलिये $a_mb_n \neq 0$ तथा इसी कारण $c_{m+n} = a_mb_n \neq 0$ में दिख रहा है कि $\deg (f(x)g(x)) = m + n$।

(4) यदि $R[x]$ समाकलित डोमेन हो तो चूँकि R, $R[x]$ की उपवलय से तुल्याकारिक है, R भी समाकलित डोमेन होगा।

इसके विपरीत मान लें कि R समाकलित डोमेन है।

माना $f(x)$, $g(x)$, $R[x]$ के दो अशून्य अवयव इस प्रकार हों कि $f(x)g(x) = 0$

जहाँ $f(x) = a_o + a_1x + ... + a_mx^m$

$g(x) = b_o + b_1x + ... + b_nx^n$

अब $f(x)$ व $g(x)$ दोनों ही अचर बहुपद नहीं हो सकते क्योंकि $a_o \neq 0, b_o \neq 0$ तथा $c_o = a_ob_o \neq 0$ है।

अतः $f(x)g(x) \neq 0$

चूँकि $f(x), g(x)$ में से कम से कम एक तो गैर–अचर बहुपद (Non Constant Polynomials) है, इसकी श्रेणी ≥ 1 है। R समाकलित डोमेन होने से $\deg (f(x)g(x)) = \deg f(x) + \deg g(x) \ge 1$

जो कि एक विरोधाभास है क्योंकि तब इसका तात्पर्य होगा कि किसी $k > 0$ हेतु $c_k \neq 0$ है।

जबकि $f(x)g(x) = 0$

टिप्पणी

इसी कारण $f(x)g(x) = 0 \Rightarrow f(x) = 0$ या $g(x) = 0$

$\Rightarrow$ $R[x]$ एक समाकलित डोमेन है।

(5) F एक क्षेत्र हो तो चूँकि F क्रमविनिमेय है जिसमें कि ईकाई है, पूर्ववर्ती परिणामों से हमने प्राप्त किया कि $F[x]$ ईकाई युक्त क्रमविनिमेय वलय (Commutative Ring) वलय होगी। वस्तुतः F समाकलित डोमेन है, $F[x]$ भी समाकलित डोमेन होगा। हम दर्शाते हैं कि $F[x]$ के समस्त अशून्य अवयवों में गुणात्मक व्युत्क्रम (Multiplicative Inverse) नहीं होगा। अशून्य बहुपद (Non-Zero Polynomial) $f(x) = 0 + 1x + 0x^2 + 0x^3 + ... (= a_o + a_1x + a_2x^2 + ...)$ का विचार करें।

मान लें कि $g(x) = b_o + b_1x + b_2x^2 + ...$ इसका गुणात्मक व्युत्क्रम (Multiplicative Inverse) है

तो $f(x)g(x) = c_o + c_1x + c_2x^2 + ..., e(x) = 1 + 0x + 0x^2 + ...$ है $F[x]$

$\Rightarrow$ $c_o = 1, c_i = 0$ सभी $i > 0$ के लिए की ईकाई होगी

जहाँ $c_o = a_o b_o = 0 . b_o = 0 \neq 1.$

इसी कारण $g(x), f(x) = x$ का गुणात्मक व्युत्क्रम (Multiplicative Inverse) नहीं हो सकता।

दर्शाया जा रहा है कि $F[x]$ क्षेत्र नहीं है।

यदि R वलय है, हम बहुपदों की संगत वलय $R[x]$ प्राप्त करते हैं। चूँकि $R[x]$ एक वलय है हम इसी प्रकार $R[x, y]$ के बहुपदों की संगत वलय प्राप्त करते हैं एवं प्रक्रिया को विस्तारित किया जा सकता है। यदि F क्षेत्र है तो $F[x]$ ईकाई युक्त वलय है एवं इसी प्रकार $F[x, y]$ ईकाई युक्त वलय होगी। हम इसका प्रयोग कुछ बाद में करेंगे जब गुणनखंड डोमेन (Factorisation Domains) की ओर बढ़ेंगे।

उदाहरण 5.30: R व S दो तुल्याकारिक वलय हैं। दर्शायें कि $R[x]$ व $S[x]$ भी तुल्याकारिक हैं।

हल: माना कि, $\phi : R \to S$ तुल्याकारिक हो तो मानचित्रण $f : R[x] \to S[x]$ को इस प्रकार परिभाषित करें कि,

$$f(a_o + a_1x + ... + a_nx^n) = \phi(a_0) + \phi(a_1)x + ... + \phi(a_n)x^n.$$

यह दर्शाना अब पाठक के लिये एक नियमित अभ्यास हो जायेगा कि यह f तुल्याकारिक है।

प्रमेय 5.21: यदि F क्षेत्र है तो $F[x]$ युक्लिडीन डोमेन (Euclidean Domain) है।

प्रमाण: हमने देखा है कि $F[x]$ ईकाई युक्त समाकलित डोमेन है।

किसी $f(x) \in F[x], f(x) \neq 0$ हेतु $d(f(x)) = \deg f(x)$ परिभाषित करें जो कि अऋणात्मक पूर्णांक (Non-Negative Integer या Non '–' ve Integer) है।

चूँकि किसी $f(x), g(x) \in F[x], f(x), g(x) \neq 0$ हेतु,

$$\deg (f(x)\, g(x)) = \deg f(x) + \deg g(x)$$

हम प्राप्त करते हैं $\deg (f(x)) \le \deg (f(x)g(x))$, जहाँ $\deg (g(x)) \ge 0$

$$\therefore \qquad d(f(x)) \le d(f(x)g(x))$$

टिप्पणी

अन्तिम रूप से हम किसी अशून्य $F[x]$ के लिये $f(x)$ को $g(x)$ में व $\exists\, t(x)$ को $r(x)$ में इस प्रकार दर्शाते हैं कि,

$$f(x) = t(x)g(x) + r(x)$$

जहाँ या तो $r(x)$ शून्य है अथवा $\deg r(x) < \deg g(x)$

यदि $\deg f(x) < \deg g(x)$ तो $f(x) = 0.\ g(x) + f(x)$ से परिणाम आता है।

अब मान लें कि परिणाम deg के $F[x]$ में समस्त (अशून्य) बहुपदों के लिये वास्तविक है जो कि $\deg f(x)$ से कम है।

माना कि, $f(x) = a_0 + a_1 + \ldots + a_m x_m$

$$g(x) = b_0 + b_1 x + \ldots + b_n x_n$$

$\deg f(x) \ge \deg g(x)$ मान लें तो परिभाषित करें कि,

$f_1(x) = f(x) - a_m b_n^{-1}\, x^{m-n}$ तो x^m का गुणांक $f_1(x)$ में $a_m - a_m b_n^{-1}.\ b_n = a_m - a_m = 0$ है।

या तो $f_1(x) = 0$ (शून्य बहुपद) अथवा $\deg f_1(x) < m$

यदि $f_1(x) = 0$ तो $0 = f(x) - a_m b_n^{-1}\, x^{m-n}\, g(x)$

$f(x) = a_m b_n^{-1}\, x^{m-n}\, g(x) + 0$ प्राप्त होता है।

अतः $t(x) = a_m b_n^{-1} x^{m-n}$ व $r(x) = 0$ को मानते हुए हम अपेक्षित परिणाम प्राप्त करते हैं।

मान लेते हैं कि $f_1(x) \ne 0$ तो $\deg f_1(x) < m$

अर्थात् $\deg f_1(x) < \deg f(x)$

प्रवेशण परिकल्पना (Induction Hypothesis) के अनुसार, $f_1(x) = t_1(x)\, g(x) + r(x)$

जहाँ या तो $r(x) = 0$ अथवा $\deg r(x) < \deg g(x)$

$$\therefore \qquad f(x) - a_m b_n^{-1}\, x^{m-n}\, g(x) = t_1(x)\, g(x) + r(x)$$

अथवा $\qquad f(x) = [a_m b_n^{-1}\, x^{m-n} + t_1(x)]\, g(x) + r(x)$

$$= t(x)g(x) + r(x)$$

जहाँ $r(x) = 0$ अथवा $\deg r(x) < \deg g(x)$

तथा इसी कारण $F[x]$ युक्लिडीन डोमेन है (एवं इसीलिये PID भी है)।

ध्यान दे :

1. इस प्रकार $\mathbf{Q}[x]$ युक्लिडीन डोमेन (Euclidean Domain) है जो कि क्षेत्र नहीं है।

टिप्पणी

2. दर्शाया जा सकता है कि उपरोक्त परिभाषित $t(x)$ व $r(x)$ अद्वितीय हैं।

मान लें कि $f(x) = t(x)\, g(x) + r(x)$ जहाँ $r(x) = 0$ अथवा $\deg r < \deg g$

तथा $f(x) = t'(x)\, g(x) + r'(x)$ जहाँ $r'(x) = 0$ अथवा $\deg r' < \deg g$

तो $(x)\, g(x) + r(x) = t'(x)\, g(x) + r(x)$

$$\Rightarrow \qquad g(t - t') = r' - r \qquad \text{...(i)}$$

मान लें कि $t(x) \neq t'(x)$ तो $t - t' \neq 0$ एवं इस प्रकार इसमें श्रेणी ≥ 0 है।

समीकरण (i) से $\Rightarrow \deg (g(t - t')) = \deg (r' - r)$

$$\Rightarrow \deg g + \deg (t - t') = \deg (r' - r) \qquad \text{...(ii)}$$

चूँकि $g(t - t')$ में धनात्मक श्रेणी $(\geq n)$ है $r' - r$ शून्य नहीं हो सकती, अन्यथा $g(t - t')$ अचर बहुपद होगा, अतः इसकी श्रेणी $\geq n$ नहीं हो सकती।

$r' - r$ शून्य नहीं हो सकती r व r' दोनों एकसाथ शून्य नहीं हो सकते।

अब समीकरण (ii) का L.H.S. $\deg g$ से बड़ा अथवा इसके समतुल्य है

जबकि समीकरण (ii) का R.H.S., $\leq \text{Max} (\deg r', \deg r) < \deg g$ है।

चूँकि यदि दोनों r व r' अशून्य हों तो $\deg r < \deg g$

$$\deg r' < \deg g$$

$$\Rightarrow \qquad \text{Max} (\deg r, \deg r') < \deg g$$

यदि r में से एक शून्य हो तो अन्य में r' से कम $\deg g$ है। किसी भी प्रकरण में R.H.S. $< \deg g$ होगा।

जो कि एक विरोधाभास है।

इस प्रकार $t - t' = 0 \Rightarrow t = t'$

अतः समीकरण (i) से $\Rightarrow r = r'$.

इसी कारण अद्वितीयता की पुष्टि होती है।

यदि F क्षेत्र हो तो युक्लिडीन डोमेन होने से $F[x]$, PID होगा।

प्रमेय 5.22: यदि F एक क्षेत्र हो तो $F[x]$ में प्रत्येक आदर्श सिद्धांत (Ideal Principal) है।

उदाहरण 5.31: माना $R = \{0, 1) \bmod 2$ हो तो $R[x]$ अपरिमित समाकलित (Infinite Integral) डोमेन है। यदि $f(x) \in R[x]$ कोई अवयव हो एवं,

यदि $f(x) = a_o + a_1 x + ... + a_m x^m$

तो हमारे पास है,

$$\begin{aligned} 2\, f(x) &= f(x) + f(x) \\ &= (a_o \oplus a_o) + (a_1 \oplus a_1)\, x + ... + (a_m \oplus a_m)\, x^m \\ &= 0 + 0.x + 0.x^2 + ... \end{aligned}$$

$O(x)$ का शून्य $R[x]$ है।

इस प्रकार $2f(x) = 0 \; \forall f \in R[x]$, है, जो यह दर्शा रहा है कि $R[x]$ परिमित अभिलक्षण का है (भले ही यह अपरिमित है)। यह भी उल्लेखनीय है कि ch R = ch $R[x]$।

टिप्पणी

उदाहरण 5.32: R ईकाई युक्त क्रमविनिमेय वलय है। A, R का आदर्श है। दर्शायें कि $\frac{R[x]}{A[x]} \cong \frac{R}{A}[x]$

इसी कारण अन्यथा सिद्ध होता अथवा नहीं होता है।

A, $R \Rightarrow A[x]$ का अभाज्य आदर्श (Prime Ideal) है जो कि $R[x]$ का अभाज्य आदर्श है।

हल: मानचित्रण $\theta : R[x] \to \frac{R}{A}[x]$ इस प्रकार परिभाषित करें कि,

$$\theta\,(f(x)) = \theta(a_o + a_1x + \ldots\ldots + a_nx^n)$$
$$= (a_o + A) + (a_1 + A)\,x + \ldots\ldots + (a_n + A)x^n\ldots\ldots$$

तो θ स्पष्टतया सुपरिभाषित है।

यदि $f(x) = a_o + a_1x + a_2x^2 + \ldots\ldots$

$g(x) = b_o + b_1x + b_2x^2 + \ldots\ldots$

$f(x)g(x) = c_o + c_1x + c_2x^2 + \ldots\ldots$

तो $\theta\,(f(x) + g(x)) = \theta\,((a_o + b_o) + (a_1 + b_1)\,x + \ldots\ldots)$

$= [(a_o + b_o) + A] + [(a_1 + b_1) + A]\,x + \ldots\ldots$

$= (a_o + A) + (b_o + A) + (a_1 + A)x + (b_1 + A)\,x + \ldots\ldots$

$= ((a_o + A) + (a_1 + A)x + \ldots\ldots) + ((b_o + A) + (b_1 + A)\,x + \ldots\ldots)$

$= \theta(f(x)) + \theta(g(x))$

$\theta(f(x)g(x)) = \theta(c_o + c_1x + c_2x^2 + \ldots\ldots)$

$= (c_o + A) + (c_1 + A)x + \ldots\ldots$

$= (a_ob_o + A) + (a_1b_o + a_ob_1 + A)x + \ldots\ldots$

$= (a_o + A)\,(b_o + A) + [(a_1b_o + A) + (a_ob_1 + A)]x + \ldots\ldots$

$= (a_o + A)\,(b_o + A) +$

$[(a_1 + A)\,(b_o + A) + (a_o + A)\,(b_1 + A)]x + \ldots\ldots$

$\theta(f(x))\;\theta(g(x)) = [(a_o + A) + (a_1 + A)x + \ldots\ldots]\;[(b_o + A) + \ldots\ldots]$

$= (a_o + A)\,(b_o + A) + [(a_1 + A)\,(b_o + A) + (a_o + A)\,(b_1 + A)]x + \ldots\ldots$भी

θ समरूपता (Homomorphism) है।

θ आच्छादक है जो कि θ की परिभाषा से स्पष्ट है एवं इसी कारण आधारभूत प्रमेय अनुसार $\frac{R[x]}{\text{Ker }\theta} \cong \frac{R}{A}[x]$

टिप्पणी

अब $f(x) \in \text{Ker}\,\theta \Leftrightarrow \theta(f(x)) = (0 + A) + (0 + A)\,x + ...$

$\Leftrightarrow \quad (a_0 + A) + (a_1 + A)\,x + ... = (0 + A) + (0 + A)\,x + ...$

सभी i के लिए $a_i + A = A$

सभी i के लिए $a_i \in A$

$f(x) \in A[x]$

इसी कारण $\frac{R[x]}{A[x]} \cong \frac{R}{A}[x]$

अन्ततः A, R का अभाज्य आदर्श है।

तो $\frac{R}{A}$ एक समाकलित डोमेन है।

$\Rightarrow \frac{R}{A}[x]$ समाकलित डोमेन है।

$\Rightarrow \frac{R[x]}{A[x]}$ समाकलित डोमेन है क्योंकि तुल्याकारिता है।

$A[x]$, $R[x]$ का अभाज्य आदर्श है।

ध्यान दे: यह स्पष्ट है कि यदि A वलय R का आदर्श है तो $A[x]$, $R[x]$ का आदर्श (आधारभूत आदर्श हैं (Kernels are Ideals)) है।

प्रमेय 5.23: R ईकाई युक्त क्रमविनिमेय वलय इस प्रकार हो कि $R[x]$, PID है तो R क्षेत्र है।

प्रमाण: पूर्ववर्ती प्रमेय अनुसार $\frac{R[x]}{< x >} \cong R$

हम दावा करते हैं कि $< x >$, $R[x]$ का महत्तम (Maximal) आदर्श है।

मान लें कि I कोई आदर्श इस प्रकार हो कि $< x > \subseteq I \subseteq R[x]$

चूँकि किसी भी $f(x) = a_0 + a_1x + ... + a_nx_n$ हेतु $R[x]$, PID है।

अब $x \in < x > \subseteq I = < f(x) >$

किसी भी $g(x) \in R[x]$ हेतु $\Rightarrow x = f(x)g(x)$

जिसका तात्पर्य यह है कि या तो $f(x) = x, \quad g(x) = 1$($R[x]$ की ईकाई है,

अथवा $\qquad f(x) = \alpha x,\ g(x) = \alpha^{-1},\ \alpha \in R$

अथवा $\qquad f(x) = 1, \quad g(x) = x$

(दूसरा प्रकरण α^{-1} के होने पर पद की पूर्ति होती है)

यदि $\qquad f(x) = x, \qquad I = < f(x) > \Rightarrow I = < x >$

यदि $\qquad f(x) = \alpha x, \qquad I = < f(x) > \Rightarrow I = < \alpha x > = < x >$

यदि $\qquad f(x) = 1, \qquad I = < f(x) > \Rightarrow I = < 1 > = R[x]$

इसी कारण $< x >$ महत्तम आदर्श (Maximal Ideal) है।

अतः $\frac{R[x]}{< x >}$ एक क्षेत्र है।

इसी कारण R क्षेत्र है।

टिप्पणी

उदाहरण 5.33: माना R ईकाई युक्त क्रमविनिमेय वलय हो एवं $< x >, R[x]$ का अभाज्य आदर्श है। दर्शायें कि R समाकलित डोमेन होगा ही।

हल: माना कि, $a, b \in R$ इस प्रकार है कि $ab = 0$

तो बहुपद $(0 + 1x + 0x^2 + ...) + (a + 0x + 0x^2 + ...)$

व $(0 + 1x + 0x^2 + ...) + (b + 0x + 0x^2 + ...)$ $R[x]$ से सम्बद्ध हैं।

$\Rightarrow x + a, x + b \in R[x]$

$\Rightarrow (x + a)(x + b) \in R[x]$

$\Rightarrow x^2 + x(a + b) + ab \in R[x]$

चूँकि $ab = 0, x^2 + x(a + b) = x[x + a + b] \in < x >$

इस प्रकार $(x + a)(x + b) \in < x >$

$\Rightarrow$ $(x + a) \in < x >$ or $(x + b) \in < x >$ as $< x >$ अभाज्य आदर्श है।

अब किसी $f(x) \in R[x]$ हेतु $(x + a) \in < x > \Rightarrow x + a = xf(x)$

$= x(a_0 + a_1x + ...)$

$\Rightarrow a = 0$

इसी प्रकार यदि $(x + b) \in < x >$ तो $b = 0$

इसी कारण R समाकलित डोमेन है।

उदाहरण 5.34: दर्शाये कि आदर्श $A = \{xf(x) + 2g(x) \mid f(x), g(x) \in \mathbf{Z}[x]\}$ के $\mathbf{Z}[x]$ आदर्श सिद्धांत नहीं है।

हल: मान लें कि A, $k(x), k(x) \in \mathbf{Z}[x]$ द्वारा उत्पन्न आदर्श सिद्धांत है।

चूँकि $x = x(1 + 0x + 0x^2 + ...) + 2(0 + 0x^2 + ...) \in A = <k(x)>$

$x = k(x)\, h(x)$

$2 \in < k(x) > \Rightarrow 2 = k(x)t(x)$ ...(i) भी है।

इस प्रकार $xk(x)t(x) = 2k(x)h(x)$

$\Rightarrow 2h(x) = xt(x)$

$\Rightarrow t(x)$ का प्रत्येक गुणांक एक सम पूर्णांक (Even Integers) है,

अर्थात् किसी $r(x) \in \mathbf{Z}[x]$ हेतु $t(x) = 2r(x)$

$\Rightarrow 2 = 2k(x)r(x)$

$\Rightarrow r(x)k(x) = 1$

टिप्पणी

$\Rightarrow 1 \in < k(x) >$

$\Rightarrow < k(x) > = \mathbf{Z}[x]$ (ईकाई युक्त आदर्श)

$\Rightarrow A = \mathbf{Z}[x]$ जो कि वास्तविक नहीं है A, $\mathbf{Z}[x]$ का उचित आदर्श (Proper Ideal) है।

उदाहरण 5.35: दर्शाये कि उपरोक्त आदर्श A, $\mathbf{Z}[x]$ में महत्तम आदर्श है।

हल: माना कि, I आदर्श इस प्रकार है कि $A \subset I \subseteq \mathbf{Z}[x]$।

चूँकि $A \neq I$, $\exists$ $h(x) \in I$ इस प्रकार कि $h(x) \notin A$।

$h(x) = b_o + b_1x + b_2x^2 + ... + b_mx^m$ हों तो b_o विषम है क्योंकि यदि b_o सम हो तो $h(x) \in A$

$h(x) = 2k + b_1x + b_2x^2 + ... + b_mx^m = g(x) + xf(x)$

इस प्रकार $h(x) = (2a + 1) + b_1x + b_2x^2 + ... + b_mx^m$

$h(x) = g(x) + 1$

$\Rightarrow 1 = h(x) - g(x)$

$\Rightarrow 1 \in I$ क्योंकि $h(x) \in I, g(x) \in A \subseteq I$

$\Rightarrow I = \mathbf{Z}[x]$

$\Rightarrow A$ एक महत्तम (Maximal) है।

ध्यान दे : हम आदर्श A के लिए संकेतन (Notation) $(2, x)$ का भी प्रयोग करते हैं।

परिमेय क्षेत्र पर बहुपद (Polynomials Over the Rational Fields)

परिमेय क्षेत्र में भिन्न (Fraction) a/b होते हैं जहाँ a व b पूर्णांक हैं एवं $b \neq 0$ है। ऐसे भिन्न (Fraction) का योज्य व्युत्क्रम (Additive Inverse) a/b के समतुल्य है एवं गुणात्मक व्युत्क्रम $a \neq 0$, b/a के समतुल्य है। क्षेत्र अभिगृहीत जैसे कि वितरणशीलता, क्रमविनिमेयता एवं संबद्धता के नियम परिमेय संख्याओं के मानक विशेषताओं में मूल स्थान में हो जाते हैं।

प्रकार $a_mx^m + a_{m-1}x^{m-1} + ... + a_1x + a_0 = 0$ के समीकरणों (जहाँ m धनात्मक पूर्णांक है एवं a परिमेय क्षेत्र के अवयव हैं) को x में बहुपद समीकरण (Polynomial Equations) कहा जाता है।

F कोई परिमेय क्षेत्र हो तो $a_mx^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$ किसी व्यंजक प्रकार $a_m, a_{m-1}, \ldots, a_1, a_0 \in F$ को गुणांकों x युक्त

अनिश्चित (Indeterminate) x में F पर **बहुपद (Polynomial Over)** कहा जाता है। F में गुणांकों युक्त समस्त बहुपदों के समुच्चय को $F[x]$ द्वारा इंगित किया जाता है। यदि n सबसे बड़ा अऋणात्मक पूर्णांक इस प्रकार हो कि $a_n \neq 0$ तो हम कहते हैं कि बहुपद $f(x) = a_nx^n + \ldots + a_0$ में श्रेणी n है जिसे $\deg(f(x)) = n$ के रूप में लिखा जा सकता है एवं a_n को $f(x)$ का अग्रणी गुणांक (Leading Coefficient) कहा जाता है।

टिप्पणी

अपनी प्रगति जांचिए

7. भागफल वलय क्या है?

8. दर्शायें कि $\frac{\mathbf{Z}_3[x]}{I}$ होगा जहाँ $I = < x^2 + x + 1 >$ समाकलित डोमेन नहीं है।

9. दर्शायें करें कि ईकाई युक्त समाकलित डोमेन R एक क्षेत्र है यदि $R[x]$, एक PID है।

5.7 समाकलित डोमेन एवं क्षेत्र

समाकलित डोमेन (Integral Domain) R को युक्लिडीन डोमेन (अथवा युक्लिडीन वलय) कहते हैं यदि समस्त $a \in R$ हेतु $a \neq 0$, वहाँ परिभाषित अऋणात्मक पूर्णांक $d(a)$ इस प्रकार है,

(i) सभी के लिए $a, b \in R, a \neq 0, b \neq 0$ के लिए $d(a) \leq d(ab)$

(ii) सभी के लिए $a, b \in R, a \neq 0, b \neq 0$ के लिए $\exists\, t$ तथा r में R इस प्रकार कि

$a = tb + r$

जहाँ $r = 0$ अथवा $d(r) < d(b)$।

पूर्णांकों के समाकलित डोमेन $< \mathbf{Z}, +, . >$ का विचार करें। किसी $0 \neq a \in \mathbf{Z}$ हेतु $d(a) = |a|$ परिभाषित करें तो $d(a)$ अऋणात्मक पूर्णांक है।

पुनः $a, b \in \mathbf{Z}$ कुछ अवयव इस प्रकार हों कि $a \neq 0, b \neq 0$

तो $d(a) = |a|$

$d(ab) = |ab| = |a|\,|b|$

इस प्रकार $d(a) \leq d(ab)$ क्योंकि $|a| \leq |a|\,|b|$

पुनः $a, b \in \mathbf{Z}\ (a, b \neq 0)$ मानें।

मान लें कि $b > 0$ तो इसे इस प्रकार लिखना सम्भव है $a = tb + r$

जहाँ $0 \leq r < bt, r \in \mathbf{Z}$

यदि $r \neq 0$ तो $r < b \Rightarrow |r| < |b|$

$\Rightarrow d(r) < d(b)$

यदि $b < 0$ तो $(-b) > 0, \therefore \exists\, t, r \in \mathbf{Z}$ इस प्रकार कि $a = (-b)t + r$

जहाँ $0 \leq r < -b$

$a = (-t)\, b + r$

तथा यदि $r \neq 0,\ r < -b \Rightarrow |r| < |b|$

$\Rightarrow d(r) < d(b)$

इसी कारण, $< \mathbf{Z}, +, . >$ युक्लिडीन डोमेन है।

ध्यान दे :

1. जब हम परिभाषा में यह कहते हैं कि किसी $\exists$ हेतु $d(a)$ अऋणात्मक पूर्णांक $0 \neq a$ है तो हमारा तात्पर्य d से $R - \{0\}\ \mathbf{Z}^+ \cup \{0\}$ तक d फलन होता है जहाँ

$\mathbf{Z}^+$ धनात्मक पूर्णांकों का समुच्चय है। इस फलन d को R पर युक्लिडीन मूल्य निर्धारण कहा जाता है। परिभाषा में अन्तिम पद को युक्लिडीन एल्गोरिद्म (Euclidean Algorithm) कहते हैं।

टिप्पणी

2. हम दर्शा सकते हैं कि युक्लिडीन डोमेन की परिभाषा में अन्तिम (युक्लिडीन एल्गोरिद्म) पद में दर्शित t व r अद्वितीयतया निर्धारित हैं यदि,

$d(a+b) \le \text{Max. } \{d(a), d(b)\}$

मानें कि $d(a+b) \le \text{Max. } \{d(a), d(b)\}$ व

मान लें कि $a = tb + r = t_1 b + r_1$

मान लें $r_1 - r \neq 0$ तो $b(t - t_1) = r_1 - r \neq 0$ व $t - t_1 \neq 0$

अब $d(b) \le d(b(t - t_1))$

$= d(r_1 - r)$

$\le \text{Max. } \{d(r_1), d(-r)\}$ (दिए गए पद के अनुसार)

$= \text{Max. } \{d(r_1), d(-r)\}$

$< d(b)$ जो कि सम्भव नहीं।

इस प्रकार $r_1 - r = 0 \Rightarrow b(t - t_1) = 0$

अथवा $t - t_1 = 0$ क्योंकि $b \neq 0$

$\Rightarrow$ $t = t_1$ और $r = r_1$

इसके विपरीत t व r को अद्वितीयतः निर्धारित मानें एवं मान लें कि कुछ a, b हेतु $d(a+b) > \text{Max. } \{d(a), d(b)\}$ में (अशून्य) है।

अब $b = 0(a+b) + b = 1 \,.\, (a+b) - a$

$d(-a) = d(a) < d(a+b)$ भी

एवं $d(b) < d(a+b)$

इस प्रकार $1 \in R, \exists\, t = 0, r = b$ हेतु b इस प्रकार कि $b = t.1 + r, b = t_1 \cdot 1 + r_1$

जहाँ $r \neq r_1$ (क्योंकि $a + b \neq 0$) $t \neq t_1$, जो कि अद्वितीयता में एक विरोधाभास है।

इस कारण $d(a+b) \le \text{Max. } (d(a), d(b))$

ध्यान दें: युक्लिडीन डोमेन में ईकाई है।

प्रमेय 5.24: R युक्लिडीन डोमेन मानें एवं A, R का आदर्श हो तो $\exists\, a_o \in A$ इस प्रकार है कि $A = \{a_o x \mid x \in R\}$

प्रमाण: यदि $A = \{0\}$ पर हम $a_o = 0$ मान सकते हैं।

मान लें कि $A \neq \{0\}$ तो $\exists$ कम से कम $0 \neq a \in A$।

$a_o \in A$ को इस प्रकार मानें कि $d(a_o)$ अल्पतम (Minimal) है (उच्च कोटि के सिद्धांत का अस्तित्व (Existence of Well-ordering Principle)) द्वारा सुनिश्चित है

जिसके अनुसार अऋणात्मक पूर्णांकों के प्रत्येक गैर–ऋणात्मक पूर्णांकों में सबसे छोटा अवयव होता है)।

टिप्पणी

हम दावा करते हैं कि A इस a_o से उत्पन्न हुआ है।

माना $a \in A, a \neq 0$ हो तो परिभाषानुसार $\exists\ t, r \in R$ इस प्रकार होगा कि,

$a = a_o t + r$ जहाँ या तो $r = 0$ अथवा $d(r) < d(a_o)$

मान लें कि $r \neq 0$

तो $\quad a_o \in A, t \in R \Rightarrow ta_o \in A$

$\therefore \quad a \in A, ta_o \in A \Rightarrow a - ta_o \in A$

$\Rightarrow r \in A$

परन्तु $d(a_o)\ A$ में सबसे छोटा d का मान है एवं $d(r) < d(a_o)$ जिससे कि विरोधाभास होता है। इसी कारण,

$r = 0$

$\Rightarrow a = ta_o$

इस प्रकार किसी $a \in A$ को रूप ta_o में रखा जा सकता है।

$\Rightarrow A \subseteq \{a_o x \mid x \in R\}$

परन्तु $\{a_o x \mid x \in R\} \subseteq A$ क्योंकि सभी $x \in R$ के लिए $a_o \in A \Rightarrow xa_o \in A$

इसी कारण $A = \{a_o x \mid x \in R\}$

जिससे प्रमेय सिद्ध हुआ।

परिभाषा: ऐसा आदर्श A जिसमें अवयव a_o के गुणज अंतर्विष्ट हैं इसे a_o के सहित R का आदर्श सिद्धांत कहा जाता है जो a_o द्वारा उत्पन्न है। हम इसे $A = (a_o)$ से इंगित करते हैं।

अन्य शब्दों में R के सबसे छोटे आदर्श (जिसमें a_o है) को a_o द्वारा उत्पन्न आदर्श सिद्धांत कहते हैं।

प्रमेय 5.25: युक्लिडीन डोमेन में प्रत्येक आदर्श सिद्धांत आदर्श है।

उपप्रमेय (Corollary) : युक्लिडीन डोमेन में ईकाई है।

प्रमाण: माना कि, R युक्लिडीन डोमेन हो तो R इसका अपने आप में आदर्श है एवं इसीलिये R, R के किसी अवयव r_o द्वारा उत्पन्न है।

इस प्रकार R का प्रत्येक अवयव r_o का गुणज है।

विशेषतया r_o, r_o का गुणज है।

अर्थात् किसी $k \in R$ के लिए $r_o = r_o k$

अब यदि $a \in R$ कोई अवयव हो तो चूँकि $R = (r_o)$

किसी x हेतु $a = xr_o$

इसी कारण $ak = (xr_o)\ k = x(r_o k) = xr_o = a$

अर्थात् k, R की ईकाई (Unity) है।

टिप्पणी

परिभाषा: ईकाई युक्त समाकलित डोमेन R को आदर्श सिद्धांत डोमेन या (PID) कहते हैं यदि R का प्रत्येक आदर्श एक आदर्श सिद्धांत हो तो।

वस्तुतः यदि R पूर्ववर्ती पद के अनुसार ईकाई युक्त क्रमविनिमेय (Commutative) वलय होता है तो हम इसे आदर्श सिद्धांत वलय (Principal Ideal Ring) कहते हैं।

पूर्ववर्ती प्रमेय व उपप्रमेय (Corollary) को देखने पर हमें निम्नांकित की प्राप्ति होती है।

प्रमेय 5.26: युक्लिडीन डोमेन एक पीआईडी है।

इस प्रकार विशेषतया पूर्णांकों की वलय $< \mathbf{Z}, +, . >$ एक पीआईडी है। यह परिणाम स्वतन्त्रतया सामने आता है यदि हम स्मरण करें कि $< \mathbf{Z}, +, . >$ में प्रत्येक आदर्श एक आदर्श सिद्धांत है।

ध्यान दें

1. क्षेत्र F सदा एक पीआईडी है क्योंकि इसमें दो ही आदर्शस F व $\{0\}$ हैं। F, 1 द्वारा व $\{0\}$, 0 द्वारा उत्पन्न है।
2. यह दर्शाया जा सकता है कि ऐसे पीआईडी भी हैं जो युक्लिडीन डोमेन नहीं हैं। विशेष रूप से। $\mathbf{Z}[\sqrt{-19}] = \{a + \sqrt{-19}\, b \mid a, b \in \mathbf{Z}\}$ जहाँ a, b दोनों ही विषम हैं अथवा दोनों ही सम हैं, यह पीआईडी है परन्तु युक्लिडीन डोमेन नहीं है।

उदाहरण 5.36: दर्शाये कि पीआईडी में प्रत्येक अशून्य अभाज्य आदर्श महत्तम है।

हल: माना $P = (p), p \neq 0$ हो, PID में R अशून्य अभाज्य आदर्श हो एवं $P \subseteq Q = (q) \subseteq R$ मान लें तो,

$P \subseteq Q = (q) \subseteq R$

$p \in P \subseteq Q = (q)$

$\Rightarrow \quad p = qr$

$\Rightarrow \quad qr \in P$

$\Rightarrow \quad q \in P$ अथवा $r \in P$

यदि $q \in P$ तो $P \Rightarrow Q \subseteq P$ में q के समस्त गुणज हैं, इस प्रकार $Q = P$

यदि $r \in P$ तो $r = pt \Rightarrow r = qrt$

$\Rightarrow \quad r(1 - qt) = 0$

$\Rightarrow \quad 1 = qt \quad (r \neq 0)$

किन्तु $q \in Q, t \in R \Rightarrow qt \in Q \Rightarrow 1 \in Q \Rightarrow Q = R$

ध्यान दें: $r = 0$ का आशय $p = q \,.\, 0 \Rightarrow p = 0 \Rightarrow P = (0)$ से होगा।

उदाहरण 5.37: $\frac{\mathbf{Z}_n}{(n)}, (n > 1)$ के समस्त अभाज्य आदर्श ज्ञात करें एवं इसी कारण $\mathbf{Z}_n$ को भी।

हलः हमें विदित है कि $\frac{A}{N}$ का कोई आदर्श R/N प्रकार का है जहाँ A, R का आदर्श है जिसमें N अंतर्विष्ट है।

माना कि $(n) = N$ व $n = p_1^{\alpha_1} p_2^{\alpha_2} .... p_r^{\alpha r}$ है जहाँ p_i सुनिश्चत अभाज्य है।

टिप्पणी

$\frac{A}{N}$ को $\frac{\mathbf{Z}}{N}$ का कोई अभाज्य आदर्श मानें तो $A, \mathbf{Z}$ का आदर्श है। हम दर्शाते हैं कि यह $\mathbf{Z}$ का अभाज्य आदर्श है। चूँकि A, $\mathbf{Z}$ का आदर्श है यह प्रकार $A = (a)$ का है। मान लें कि A, $\mathbf{Z}$ का अभाज्य आदर्श नहीं है तो $\exists\, x, y \in \mathbf{Z}$ इस प्रकार है कि $xy \in A$ परन्तु x व y, A में नहीं हैं।

अब $xy \in A \Rightarrow Nxy \in A/N \Rightarrow NxNy \in A/N$

$\Rightarrow$ Nx अथवा $Ny \in A/N$ क्योंकि A/N अभाज्य आदर्श है।

$\Rightarrow$ x अथवा y, A में है जो कि विरोधाभास है।

इसी कारण $A = (a)$ अभाज्य आदर्श है एवं इस प्रकार a एक अभाज्य है। $(n) \subseteq (a)$ भी है। चूँकि $n \in (n) \subseteq (a)$ हम पाते हैं कि $a \mid n$ है।

किन्तु n को विभाजित करते अभाज्य $p_1, p_2, ..., p_r$ हैं।

इस प्रकार समान $i, 1 \le i \le r$ के लिये $a = p_i$ है।

इसी कारण यदि $A/(n)$, $\frac{\mathbf{Z}}{(n)}$ का कोई अभाज्य आदर्श हो तो यह कुछ i, $1 \le i \le r$ के लिये प्रकार $\frac{(p_i)}{(n)}$ का है।

इसके विपरीत प्रकार $\frac{(p_i)}{(n)}, 1 \le i \le r$ का कोई आदर्श $\frac{\mathbf{Z}}{(n)}$ का अभाज्य आदर्श होगा क्योंकि $\frac{\mathbf{Z}/(n)}{(p_i)/(n)} \cong \frac{\mathbf{Z}}{(p_i)}$ ।

चूँकि $(p_i), \mathbf{Z}$ का अभाज्य आदर्श है $\frac{\mathbf{Z}}{(p_i)}$ एक समाकलित डोमेन है।

इस प्रकार $\frac{\mathbf{Z}/(n)}{(p_i)/(n)}$ एक समाकलित डोमेन है एवं इसी कारण $\frac{(p_i)}{(n)}$, $\frac{\mathbf{Z}}{(n)}$ के अभाज्य आदर्श हैं।

जहाँ p_i, n को विभाजित करते अभाज्य हैं।

इस प्रकार हम निष्कर्ष पर आते हैं कि यदि $n = p_1^{\alpha_1} p_2^{\alpha_2} .... p_r^{\alpha_r}$

तो $\frac{(p_1)}{(n)}, \frac{(p_2)}{(n)}, ..., \frac{(p_r)}{(n)}, \frac{\mathbf{Z}}{(n)}$ के अभाज्य आदर्श हैं।

टिप्पणी

आपने पहले देखा है कि $\theta : \frac{\mathbf{Z}}{(n)} \to \mathbf{Z}_n$ इस प्रकार हैं कि,

$\theta(m + (n)) = m, 0 \le m < n$ एक तुल्याकारिता है।

अब यदि P, $\frac{\mathbf{Z}}{(n)}$ का अभाज्य आदर्श है तो $\theta(P)$, $\mathbf{Z}_n$ का अभाज्य आदर्श है।

चूँकि $\frac{(p_i)}{(n)}$, $\frac{\mathbf{Z}}{(n)}$ के अभाज्य आदर्श हैं, θ के अधीन इनके प्रतिबिंब $\mathbf{Z}_n$ के अभाज्य आदर्श हैं, अर्थात् $(p_1), (p_2), ..., (p_r)$, $\mathbf{Z}_n$ के अभाज्य आदर्श हैं।

ध्यान दे

1. विशेषतया $\mathbf{Z}_p$ का अभाज्य आदर्श (जहाँ p अभाज्य है) $(p) = (0)$ है क्योंकि $\mathbf{Z}_p$ में $p = 0$ है। स्मरण करें कि क्षेत्र में कोई गैर–नगण्य आदर्श नहीं है एवं $\mathbf{Z}_p$ एक आदर्श है जब p अभाज्य है।
2. चूँकि $\mathbf{Z}$ में अशून्य आदर्श अधिकतम (Maximal) है यदि यह अभाज्य है, पूर्ववर्ती परिणाम अधिकतम (Maximal) आदर्श के लिये भी समान प्रकार से सिद्ध हो सकता है।

उदाहरण 5.38: दर्शायें कि $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$ गाऊसियान पूर्णांकों (Gaussian Integers) की वलय एक युक्लिडीन डोमेन है।

हल: हमें विदित है कि $\mathbf{Z}[i]$ एक समाकलित पूर्णांक है।

किसी $0 \ne x \in \mathbf{Z}[i]$ लिए है, जहाँ $x = a + ib$, परिभाषित करें कि,

$d(x) = d(a + ib) = a^2 + b^2$

तो चूँकि $x \ne 0$, या तो $a \ne 0$ अथवा $b \ne 0$

इस प्रकार $d(a + ib) = a^2 + b^2 > 0$

अब मान लें $x, y \in \mathbf{Z}[i]$ इस प्रकार है कि $x \ne 0, y \ne 0$ व मान लेते हैं कि $x = a + ib$, $y = c + id$

तो $d(xy) = d((a + ib)(c + id)) = d((ac - bd) + i(ad + bd))$

$= (ac - bd)^2 + (ad + bc)^2$

$= (a^2 + b^2)(c^2 + d^2)$

$= d(x)\, d(y)$

चूँकि $y \ne 0, d(y) \ge 1$ का तात्पर्य है कि $y \ne 0$ अथवा c, d अशून्य है।

इस प्रकार $d(xy) \ge d(x)$

हम अब युक्लिडीन डोमेन की परिभाषा में अन्तिम पद सिद्ध करते हैं।

माना $x, y \in \mathbf{Z}[i]$ दो अवयव हैं जहाँ x साधारण धनात्मक पूर्णांक $n\,(x = n + io)$ व $y = a + ib$ है।

यूक्लिड विभाजन एल्गोरिद्म के अनुसार (By Euclid's Division Algorithm)

$$a = un + r_1 \qquad 0 \le r_1 < n$$
$$b = vn + r_2 \qquad 0 \le r_2 < n$$

टिप्पणी

अब $r_1 \le \frac{n}{2}$ अथवा $r_1 > \frac{n}{2}$

यदि $r_1 > \frac{n}{2}$ तो $-r_1 < -\frac{n}{2}$

$\Rightarrow \quad n - r_1 < n - \frac{n}{2} = \frac{n}{2}$

इस प्रकार $a = un + r_1 = un + n - n + r_1$

$= n(u + 1) - (n - r_1)$

$= nq + k_1$ जहाँ $k_1 = -(n - r_1)$

$| k_1 | = n - r_1 < \frac{n}{2}$

इस प्रकार $r_1 \le \frac{n}{2}$ हो अथवा $\frac{n}{2} < r_1$

हम $a = nq + k_1$ व्यक्त कर सकते हैं जहाँ $|k_1| \le \frac{n}{2}$

इसी प्रकार $b = nq' + k_2$ जहाँ $|k_2| \le \frac{n}{2}$

अर्थात् $a + ib = n(q + iq') + (k_1 + ik_2)$

अथवा $y = tn + r$ $[t = q + iq',\ r = k_1 + ik_2]$

जहाँ या तो $r = 0$ (k_1 व k_2 शून्य हो सकते हैं)।

अथवा $d(r) = d(k_1 + ik_2) = k_1^2 + k_2^2 \le \frac{n^2}{4} + \frac{n^2}{4} < n^2 = d(n)$

इस प्रकार इस प्रकरण विशेष में परिणाम सिद्ध हुआ।

अब मान लें कि $x, y \in \mathbf{Z}[i]$ दो अशून्य अवयव हों तो $x\bar{x}$ का एक धनात्मक पूर्णांक, n मान लेते हैं।

हम पूर्ववर्ती सिद्ध परिणाम को $y\bar{x}$ व n में प्रयोग करते हैं एवं ज्ञात करते हैं कि, $y\bar{x}$ व n हेतु $\exists\ t, r \in \mathbf{Z}[i]$ इस प्रकार कि $y\bar{x} = tn + r$

जहाँ $r = 0$ अथवा $d(r) < d(n)$

यदि $r = 0$ तो $y\bar{x} = tn = tx\bar{x} \Rightarrow y = tx + 0$

यदि $d(r) < d(n)$ तो $d(y\bar{x} - tn) < d(x\bar{x})$

$\Rightarrow \quad d(y\bar{x} - tx\bar{x}) < d(x)\ d(\bar{x})$

$\Rightarrow \quad d(\bar{x})\ d(y - tx) < d(x)\ d(\bar{x})$

टिप्पणी

$\Rightarrow \quad d(y - tx) < d(x) \quad [d(\bar{x}) > 0]$

$y - tx = r_o$ के मान को रखें तो $d(r_o) < d(x)$

अतः $y = tx + r_o$ जहाँ $d(r_o) < d(x)$ को संयुक्त करने पर हम पाते हैं कि,

$y = tx + r_o$, जहाँ $r_o = 0$ अथवा $d(r_o) < d(x)$

इसी कारण परिणाम सिद्ध हुआ।

उदाहरण 5.39: दर्शाये कि $\mathbf{Z}[\sqrt{2}] = \{a + \sqrt{2}\, b \mid a, b \in \mathbf{Z}\}$ एक युक्लिडीन डोमेन है।

हलः यह सरलता से देखा जा सकता है कि $\mathbf{Z}[\sqrt{2}]$ एक समाकलित डोमेन है। मानचित्रण $d : \mathbf{Z}[\sqrt{2}] - \{0\} \to \mathbf{Z}$ परिभाषित इस प्रकार करें कि,

$d(a + \sqrt{2}b) = |\, a^2 - 2b^2|$

तो $\quad |\, a^2 - 2b^2| \geq 1$ जहाँ $a^2 - 2b^2 = 0 \Rightarrow \sqrt{2} = \frac{a}{b}$ जो कि सम्भव नहीं हैं।

पुनः $\quad d[(a + \sqrt{2}\, b)\,(c + \sqrt{2}\, d)]$

$= d[(ad + 2bd) + \sqrt{2}\,(ad + bc)]$

$= |\,(ac + 2bd)^2 - 2\,(ad + bc)^2\,|$

$= |\,(a^2 - 2b^2)\,(c^2 - 2d^2)\,|$

$= \quad |\, a^2 - 2b^2|\,|\, c^2 - 2d^2\,|$ ...(i)

$\geq \quad |\, a^2 - 2b^2| = d(a + \sqrt{2}\, b)$

अर्थात् $d(a + \sqrt{2}\, b) \leq d[(a + \sqrt{2}b)\,(c + \sqrt{2}\, d)]$

अब मान लें कि $a + \sqrt{2}\, b$ व $c + \sqrt{2}\, d$, $\mathbf{Z}[\sqrt{2}]$ के दो अवयव हों एवं मान लें कि $c + \sqrt{2}\, d \neq 0$, तो

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

$= m + \sqrt{2}\, n$ (कहते हैं)

तदुपरान्त m व n परिमेय हैं।

अब $m = [m] + \theta$ जहाँ $[m]$ ऐसा सबसे बड़ा पूर्णांक है जो m से बड़ा नहीं है एवं θ, m का भिन्नात्मक भाग (Fractional Part) है।

यदि $0 \leq \theta \leq \frac{1}{2}$, $p = [m]$ लेते हैं तथा यदि $\frac{1}{2} < \theta < 1$, तो $p = [m] + 1$ को लेते हैं।

इस प्रकार $\exists$ पूर्णांक p इस प्रकार है, $|\, m - p\,| \leq \frac{1}{2}$

इसी प्रकार हम प्राप्त कर सकते हैं कि पूर्णांक q इस प्रकार है, $|\, n - q\,| \leq \frac{1}{2}$

$m - p = \alpha, n - p = \beta$ रखें तो $|\alpha| \le \frac{1}{2}, |\beta| \le \frac{1}{2}$

तदुपरान्त $\frac{a+\sqrt{2}b}{c+\sqrt{2}d} = (p+\alpha) + \sqrt{2}(q+\beta)$

$\Rightarrow \quad \frac{a+\sqrt{2}b}{c+\sqrt{2}d} = (p+\sqrt{2}\,q) + (\alpha+\sqrt{2}\,\beta)$

$\Rightarrow \quad a+\sqrt{2}\,b = (c+\sqrt{2}d)(p+\sqrt{2}q) + (c+\sqrt{2}d)[(m-p)+\sqrt{2}(n-q)]$

जहाँ $(p+\sqrt{2}q) \in \mathbf{Z}[\sqrt{2}]$ क्योंकि p, q पूर्णांक हैं।

इस प्रकार हम $a+\sqrt{2}b = (c+\sqrt{2}d)(p+\sqrt{2}q) + r$ लिख सकते हैं,

जहाँ $r = (c+\sqrt{2}d)[(m-p)+\sqrt{2}(n-q)]$

एवं चूँकि $r = (a+\sqrt{2}b) - (c+\sqrt{2}d)(p+\sqrt{2}q)$

ध्यान दे : $r \in \mathbf{Z}[\sqrt{2}]$

अब यदि $r \neq 0, d(r) = d[(c+\sqrt{2}d)\{(m-p)+(n-q)\sqrt{2}\}]$

$= d[(c+\sqrt{2}d)][d((m-p)+\sqrt{2}(n-q))]$

समीकरण (i) का प्रयोग करते हुए यहाँ उल्लेखनीय है कि समीकरण (i) को सिद्ध करने में हमारे लिये यह आवश्यक नहीं है कि a, b, c, d पूर्णांक हों।

$\Rightarrow d(r) = |c^2 - 2d^2|\,|(m-p)^2 - 2(n-q)^2|$

$\le |c^2 - 2d^2|\,|(m-p)^2 + 2(n-q)^2|$

$\le |c^2 - 2d^2| \left|\frac{1}{4} + \frac{2}{4}\right|$

$\le |c^2 - 2d^2| = d(c+\sqrt{2}\,d)$

इसी कारण $a+\sqrt{2}b$ हेतु $c+\sqrt{2}\,d \in \mathbf{Z}[\sqrt{2}]\ \exists\ p+\sqrt{2}\,q, r \in \mathbf{Z}[\sqrt{2}]$ इस प्रकार,

$(a+\sqrt{2}\,b) = (c+\sqrt{2}\,d)(p+\sqrt{2}\,d) + r$

जहाँ या तो $r = 0$ अथवा $d(r) < d(c+\sqrt{2}\,d)$

दर्शाया जा रहा है कि $\mathbf{Z}[\sqrt{2}]$ युक्लिडीन डोमेन (Euclidean Domain) है।

प्रमेय 5.27: a, b युक्लिडीन डोमेन R के दो अशून्य अवयव हैं। यदि b, R में a ईकाई नहीं हो तो $d(a) < d(ab)$।

प्रमाण: मान लें कि b ईकाई नहीं है तो $R\ \exists\ t$ में a, ab के लिये $r \in R$ इस प्रकार है कि,

$a = tab + r$

जहाँ या तो $r = 0$ अथवा $d(r) < d(ab)$

यदि $r = 0$ तो $a = tab \Rightarrow a(1 - t\,b) = 0$

टिप्पणी

टिप्पणी

$\Rightarrow \quad tb = 1$ अथवा b ईकाई है जब कि ऐसा है नहीं।

इस प्रकार $r \neq 0$ व $d(r) < d(ab)$

अब $r = a - tab = a(1 - tb)$

इसी कारण $d(a) \quad \leq d(a(1 - tb)) = d(r) < d(ab)$

उपप्रमेय: यदि a, b युक्लिडीन डोमेन R के अशून्य अवयव हों तो $d(a) = d(ab)$ यदि b ईकाई है।

यदि b ईकाई है तो $\exists\, c$ इस प्रकार है कि $bc = 1$

अब $d(a) \leq d(ab) \leq d((ab)c) = d(a)$

$\Rightarrow \quad d(a) \quad = d(ab)$

इसका विपरीत पूर्ववर्ती प्रमेय से संभव है।

उदाहरण 5.40: दर्शायें कि x युक्लिडीन डोमेन में अवयव एक ईकाई है यदि केवल यदि $d(x) = d(1)$।

हल: मान लें $d(x) = d(1)$.

मान लेते हैं कि x ईकाई नहीं है तो पूर्ववर्ती प्रमेय अनुसार,

$d(1) < d(1 \,.\, x)$

$a = 1, b = x$ रखने पर को मान लें अर्थात् $d(1) < d(x)$

जो कि एक विरोधाभास है

अतः x ईकाई है।

इसके विपरीत x, R में ईकाई है तो $\exists\, y \in R$ इस प्रकार है कि,

$xy = 1$

अब $d(x) \leq d(xy)$ (परिभाषानुसार),

$\Rightarrow \qquad d(x) \leq d(1)$

$d(1) \leq d(1 \,.\, x)$ भी

$\Rightarrow \qquad d(1) \leq d(x)$

इसी कारण $d(x) = d(1)$

प्रमेय 5.28: युक्लिडीन डोमेन R के दो अशून्य अवयवों a,b में महत्तम उभयनिष्ठ भाग (Greatest Common Division) d है एवं ऐसा लिखा जा सकता है।

कुछ $\lambda, \mu \in R$ हेतु $d = \lambda a + \mu b$

प्रमाण: $A = \{ra + sb \mid r, s \in R\}$ मान लें तो A, R का एक आदर्श इस प्रकार है,

$0 = 0.\, a + 0.\, b \in A \;\Rightarrow A \neq \varphi$

$x, y \in A$ मान लें।

$\Rightarrow \qquad x = r_1 a + s_1 b,\; y = r_2 a + s_2 b \qquad r_1, r_2, s_1, s_2 \in R$

इस प्रकार $x - y = (r_1 - r_2)a + (s_1 - s_2)b \in A$

पुनः $x \in A, r \in R, x = r_1 a + s_1 b$

$\Rightarrow$ $rx = r(r_1 a + s_1 b) = (rr_1)a + (rs_1)b \in A$ दर्शा रहा है कि A, R का आदर्श है।

चूँकि युक्लिडीन डोमेन PID है, A किसी अवयव (जैसे कि d) द्वारा उत्पन्न होगा।

हम दावा करते हैं $d = \text{g.c.d.}(a, b)$

अब किसी $\lambda, \mu \in R$ के लिए $d \in A \Rightarrow d = \lambda a$

पुनः चूँकि $a = 1.a + 0.b \in A$

$b = 0 \cdot a + 1 \cdot b \in A$

(**ध्यान दे**: युक्लिडीन डोमेन होने से R में ईकाई है)

अतः किसी भी $\alpha \in R$ के लिए $a \in A$, $A = (d) \Rightarrow a = \alpha d$

किसी भी $\beta \in R$ के लिए $b \in A$, $A = (d) \Rightarrow b = \beta d$

$\Rightarrow d \mid a$ व $d \mid b$

पुनः यदि $c \mid a$ एवं $c \mid b$ तो $c \mid \lambda a$, $c \mid \mu b \Rightarrow c \mid \lambda a + \mu b$

अर्थात् $c \mid d \Rightarrow d = \text{g.c.d.}(a, b)$

ध्यान दें

1. अब प्रमेय स्पष्टतया PID या पीआईडी में है एवं PID में आगामी जिस परिणाम को हमने सिद्ध किया वह युक्लिडीन डोमेन में है।
2. इसी प्रकार यह दर्शाया जा सकता है कि युक्लिडीन डोमेन (PID) $a_1, a_2 ..., a_n$ में अशून्य अवयवों R के किसी परिमित संख्या में g.c.d. है जिसे रूप $\lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_n a_n, \lambda_i \in R$ में रखा जा सकता है।

प्रमेय 5.29: a, b में किन्हीं दो अशून्य अवयवों PID R में लघुतम उभयनिष्ठ गुणज (Least Common Multiple) है।

प्रमाण: a व b द्वारा उत्पन्न आदर्श $A = (a), B = (b)$ हैं

तो $A \cap B$, PID R का आदर्श है। मान लें कि यह l द्वारा उत्पन्न है।

हम दर्शाते हैं कि $l = \text{L.C.M.}(a, b)$,

अब $A \cap B \subseteq A, A \cap B \subseteq B$

किसी भी u के लिए $l \in (l) \Rightarrow l \in (a) \Rightarrow l = au$

किसी भी v के लिए $l \in (l) \Rightarrow l \in (b) \Rightarrow l = bv$

$\Rightarrow a \mid l$ व $b \mid l$

पुनः मान लें कि $a \mid x$ व $b \mid x$,

$\Rightarrow x = a\alpha, x = b\beta$ $\alpha, \beta \in R$

$\Rightarrow x \in (a), x \in (b)$

टिप्पणी

टिप्पणी

$\Rightarrow x \in A \cap B = (l)$

$\Rightarrow x = kl \Rightarrow l \mid x$

इसी कारण $l = \text{L.C.M.}(a, b)$

परिभाषा: ईकाई युक्त समाकलित डोमेन R में a, b (अशून्य) को सहअभाज्य अथवा आपेक्षाकृत (Prime) कहा जाता है यदि महत्तम उभयनिष्ठ भाग $(a, b), R$ में ईकाई है।

अभाज्य (Prime) एवं अलघुकरणीय अवयव (Irreducible Element)

परिभाषाएँ: R ईकाई युक्त क्रमविनिमेय वलय हो। अवयव $p \in R$ को अभाज्य अवयव (Prime Element) माना जाता है यदि:–

(i) $p \neq 0, p$ ईकाई नहीं है।

(ii) किसी $a, b \in R$ के लिये यदि $p \mid ab$ तो $p \mid a$ or $p \mid b$

R ईकाई युक्त क्रमविनिमेय (Commutative) वलय मानें। अवयव $p \in R$ को अलघुकरणीय अवयव (Irreducible Element) कहा जाता है यदि,

1. $p \neq 0, p$ ईकाई नहीं है।
2. जब भी $p = ab$ तो a अथवा b में कोई एक ईकाई होगी ही (अन्य शब्दों में p में उचित कारक नहीं हैं)।

पूर्णांकों की वलय $< \mathbf{Z}, +, \cdot >$ में प्रत्येक अभाज्य संख्या (Prime Number) अभाज्य अवयव (Prime Element) व अलघुकरणीय अवयव (Irreducible Element) दोनों होती है।

वलय $\mathbf{Z}[\sqrt{-5}] = \{a + \sqrt{-5}b \mid a, b \in \mathbf{Z}\}$ का विचार निम्नांकित परिभाषानुरूप संक्रियाओं (Operations) के अधीन करें,

$$(a + \sqrt{-5}b) + (c + \sqrt{-5}d) = (a + c) + \sqrt{-5}(b + d)$$

$$(a + \sqrt{-5}b) \cdot (c + \sqrt{-5}d) = (ac - 5bd) + \sqrt{-5}(ad + bc)$$

(i) हम दर्शाते हैं कि $\sqrt{-5}$ अभाज्य अवयव (Prime Element) है।

$\sqrt{-5} \neq 0$ यह एक ईकाई भी है क्योंकि यदि यह ईकाई हुई तो $\exists\ a + \sqrt{-5}b$ इस प्रकार होगा कि $\sqrt{-5}(a + \sqrt{-5}b) = 1$

जो कि सम्भव नहीं है क्योंकि $\Rightarrow \sqrt{-5} = 1 + 5b$ पूर्णांक है जबकि R.H.S. एक पूर्णांक है और L.H.S. एक पूर्णांक नहीं है।

मान लें कि अब $\sqrt{-5}$ से $(a + \sqrt{-5}b)(c + \sqrt{-5}d)$, विभाजित होता है तो $\exists$ $(x + \sqrt{-5}y)$ इस प्रकार कि,

$$\sqrt{-5}(x + \sqrt{-5}y) = (a + \sqrt{-5}b)\ (c + \sqrt{-5}d)$$

तुलना करने पर जिससे हमें मिलता है,

$$-5y = ac - 5bd$$

टिप्पणी

$5(bd - y) = ac \Rightarrow 5 \mid ac$

किन्तु 5 अभाज्य संख्या (Prime Number) है

$5 \mid a$ अथवा $5 \mid c$

यदि $5 \mid a$ तो $(\sqrt{-5})(\sqrt{-5}) \mid a$

$\Rightarrow \sqrt{-5} \mid a$

$\Rightarrow \sqrt{-5} \mid a + b\sqrt{-5}$

इसी प्रकार यदि $5 \mid c$ तो $\sqrt{-5} \mid c + \sqrt{-5}d$

इसी कारण $\sqrt{-5}$ अभाज्य अवयव (Prime Element) है।

(*ii*) हम आगे दर्शाते हैं कि 3 एक अलघुकरणीय अवयव (Irreducible Element) है जो कि अभाज्य (Prime) नहीं है।

मान लें कि $3 = (a + \sqrt{-5}b)\ (c + \sqrt{-5}d)$, $a, b, c, d \in \mathbf{Z}$

संयुग्मित मान लेने पर हम पाते हैं $\overline{3} = (a - \sqrt{-5}b)(c - \sqrt{-5}d)$

इस प्रकार $3.\overline{3} = (a^2 + 5b^2)(c^2 + 5d^2)$

अर्थात् $9 = (a^2 + 5b^2)(c^2 + 5d^2)$

अब $a^2 + 5b^2 = 3$ सम्भव नहीं क्योंकि $a, b \in \mathbf{Z}$

यदि $a^2 + 5b^2 = 1$ तो $a = \pm 1$ और $b = 0$ ईकाई

यदि $a^2 + 5b^2 = 9$ तो $a^2 + 5d^2 = 1$, इससे $c = \pm 1$ व $d = 0$ मिलता हैं।

इस प्रकार यदि $a^2 + 5b^2 = 1$ तो $a^2 + \sqrt{-5}b = \pm 1$ ईकाई है।

एवं यदि $a^2 + 5b^2 = 9$ तो $c + \sqrt{-5}d = \pm 1$ ईकाई है।

इसी कारण 3 $\mathbf{Z}[\sqrt{-5}]$ का अलघुकरणीय अवयव (Irreducible Element) है।

अब $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$ एवं इस प्रकार $3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$

हम दर्शाते हैं कि यह इनमें से किसी को विभाजित नहीं करता। मान लें कि $3 \mid (2 + \sqrt{-5})$ में $\mathbf{Z}[\sqrt{-5}]$

तो $(2 + \sqrt{-5}) = 3\,(a + \sqrt{-5}b)$ $a, b \in \mathbf{Z}$

$\Rightarrow \quad 2 - \sqrt{-5} = 3(a - \sqrt{-5}b)$

$\Rightarrow \quad 9 = 9\ (a^2 + 5b^2)$

$\Rightarrow \quad 1 = a^2 + 5b^2 \Rightarrow a = \pm 1,\ b = 0$

$\Rightarrow \quad 2 + \sqrt{-5} = \pm 3$ जो कि सम्भव नहीं है।

इस प्रकार $3 \nmid (2 + \sqrt{-5})$। इसी प्रकार $3 \nmid (2 - \sqrt{-5})$

इसी कारण 3, $\mathbf{Z}[\sqrt{-5}]$ का अभाज्य अवयव (Prime Element) नहीं है।

उदाहरण 5.41: $\mathbf{Z}[\sqrt{-5}]$ की समस्त ईकाइयाँ ज्ञात करें।

हल: मान लें कि $a+\sqrt{-5}b$ में $\mathbf{Z}[\sqrt{-5}]$ ईकाई है।

टिप्पणी

तदुपरान्त कुछ $c, d \in \mathbf{Z}$ हेतु $(a+\sqrt{-5}b)(c+\sqrt{-5}d) = 1+\sqrt{-5}.0$

अतः $(a-\sqrt{-5}b)(c-\sqrt{-5}d) = \bar{1} = 1$

$\mathbf{Z}$ में $(a^2+5b^2)(c^2+5b^2)=1$ दिया है।

$\Rightarrow \quad a^2+5b^2 = 1 \Rightarrow a = \pm 1, b = 0$

इस प्रकार $a+\sqrt{-5}b = \pm 1$, $\mathbf{Z}[\sqrt{-5}]$ में ईकाईयाँ हैं।

निम्नांकित प्रमेय में अलघुकरणीय अवयव एवं अभाज्य (Prime) की 'निकटता' (Closeness) प्रदर्शित होती है।

प्रमेय 5.30: PID में एक अवयव अभाज्य है यदि केवल यदि यह अलघुकरणीय हो।

प्रमाण: माना D को PID व $p \in D$ को अभाज्य अवयव मानें। हमें यही सिद्ध करने की आवश्यकता है कि यदि $p = ab$ तो a अथवा b ईकाई है।

अतः $p = ab$ तो $p \mid ab \Rightarrow p \mid a$ अथवा $p \mid b$ (p अभाज्य है)।

यदि $p \mid a$ तो किसी भी $a = px$ के लिए x

अतः $p = ab = (px)b$

$\Rightarrow \qquad p(1-xb) = 0$

$\Rightarrow \qquad 1 - xb = 0$ क्योंकि $p \neq 0$

$xb = 1 \Rightarrow b$ एक ईकाई है।

इसी प्रकार यदि $p \mid b$ तो a एक ईकाई होगी।

इसके विपरीत p को अलघुकरणीय अवयव मानें एवं $p \mid ab$ मान लें। हम दर्शाते हैं कि $p \mid a$ अथवा $p \mid b$।

यदि $p \mid a$, हमारे पास सिद्ध करने को कुछ नहीं है।

मान लें कि $p \nmid a$

चूँकि p, a PID के अवयव हैं इनमें महत्तम उभयनिष्ठ भाग d है।

हम दर्शाते हैं कि d ईकाई है।

अब $d \mid p$ व $d \mid a$

$\Rightarrow \quad \exists\, u, v$ इस प्रकार है कि $p = du, a = dv$

यदि d ईकाई न हो तो चूँकि p अलघुकरणीय है एवं $p = du$, u ईकाई होगा।

$\Rightarrow \quad u^{-1}$ विद्यमान् है।

$\Rightarrow \quad pu^{-1} = d$

$\therefore \quad a = pu^{-1}v \Rightarrow p \mid a$ जबकि ऐसा है नहीं।

इस प्रकार d ईकाई है।

पुनः हमें विदित है कि d को इस प्रकार व्यक्त किया जा सकता है,

$d = \lambda a + \mu p$

जिससे मिलता है,

$dd^{-1} = d^{-1}\lambda a + d^{-1}\mu p$

$\Rightarrow \quad b \,.\, 1 = \lambda d^{-1}ab + \mu d^{-1}bp$

$p \mid ab,\ p \mid \mu d^{-1}\, bp$

परन्तु $p \mid (ab\lambda d^{-1} + \mu d^{-1}bp)$

$\Rightarrow \quad p \mid b$

इसी कारण यह परिणाम सामने आता है।

टिप्पणी

उपप्रमेयः ईकाई युक्त समाकलित डोमेन में प्रत्येक अभाज्य अवयव अलघुकरणीय है। इसका विलोम वास्तविक नहीं हैं।

वलय $\boldsymbol{Z}_6 = \{0, 1, 2, 3, 4, 5\} \bmod 6$ का विचार करें।

2, $\mathbf{Z}_6$ में एक अभाज्य अवयव है किन्तु अलघुकरणीय नहीं है।

2 निश्चय ही अशून्य, गैर–ईकाई (Non-Unit) है।

मान लें कि $2 \mid a \otimes b$

चूँकि किसी भी $ab = 6q + a \otimes b$ के लिए q है।

तथा चूँकि $2 \mid 6q, 2 \mid a \otimes b,$ हम प्राप्त करते हैं $2 \mid ab$

$\Rightarrow \quad 2 \mid a$ या $2 \mid b$

$\Rightarrow \quad 2 \mid a$ या $2 \mid b$ में $\mathbf{Z}_6$

इसी कारण 2 अभाज्य अवयव है।

पुनः चूँकि $2 \otimes 4 = 2$, जहाँ 2 व 4 कोई भी ईकाई नहीं है, हम पाते हैं कि 2 अलघुकरणीय नहीं है (ध्यान देः $\mathbf{Z}_6$ समाकलित डोमेन नहीं है)।

प्रमेय 5.31: R ऐसा पीआईडी हो जो कि क्षेत्र नहीं है तो आदर्श $A = (a_o)$ महत्तम आदर्श है यदि केवल यदि a_o अलघुकरणीय अवयव हो।

प्रमाणः $A = (a_o)$ को महत्तम आदर्श मान लेते हैं।

(*i*) $\quad a_o \neq 0$

मान लें कि $a_o = 0$ तो चूँकि R क्षेत्र नहीं है, $\exists$ लघुत्तम $0 \neq b \in R$ (जैसे कि b^{-1}) विद्यमान् नहीं है। $B = (b)$ मान लेते हैं एवं चूँकि $a_o = 0, A = (0)$

एवं $(0) \subseteq B \subseteq R \Rightarrow A \subseteq B \subseteq R$

अब $B \neq A$ क्योंकि $b \in B, b \neq 0$ व $A = (0)$

$B \neq R$ क्योंकि $1 \in R$, परन्तु $1 \notin B$

ध्यान दें: यदि $1 \in B = (b)$ तो $\exists$ कोई x इस प्रकार है $1 = bx$

यह दर्शा रहा है कि b व्युत्क्रमणीय (Invertible) है जब कि ऐसा है नहीं।

टिप्पणी

इसी कारण $a_o \neq 0$

(*ii*) a_o ईकाई नहीं है।

मान लेते हैं कि a_o ईकाई है तो $a_o a_o^{-1} = 1$

$a_o \in A, a_o^{-1} \in R \Rightarrow a_o a_o^{-1} \in A$

$\Rightarrow 1 \in A$

$\Rightarrow A = R$

जो कि सम्भव नहीं है क्योंकि A महत्तम है।

इस प्रकार a_o ईकाई नहीं है।

(*iii*) अब किसी भी $b, c \in R$ के लिए $a_o = bc$। हम दर्शाते हैं कि b अथवा c ईकाई है।

मान लेते हैं कि $B = (b)$

चूँकि $a_o = bc, a_o \in B$

a_o के समस्त गुणज B में हैं।

$A \subseteq B$

परन्तु A महत्तम है, इस प्रकार या तो $B = R$ अथवा $B = A$

यदि $B = R$ तो $1 \in B = (b)$ क्योंकि $1 \in R$

किसी भी x के लिए $1 = xb$

b ईकाई है।

यदि $B = A$ तो $b \in A = (a_o)$

किसी भी y के लिए $b = ya_o$

$\Rightarrow a_o = bc = ya_o c$

$\Rightarrow a_o - ya_o c = 0$

$\Rightarrow a_o(1 - yc) = 0$

$\Rightarrow 1 - yc = 0$ (जैसे $a_o \neq 0$)

c ईकाई है।

इसी कारण परिणाम सिद्ध हुआ।

इसके विपरीत a_o को अलघुकरणीय अवयव मानें।

हम दर्शाते हैं कि $A = (a_o)$ महत्तम है।

I को कोई आदर्श इस प्रकार मानें कि $A \subset I \subseteq R$

चूँकि R पीआईडी (PID) है, I किसी अवयव x द्वारा उत्पन्न है।

अब $x \notin A$ क्योंकि यदि $x \in A$ तो $(x) \subseteq A$

अर्थात् $I \subseteq A$ परन्तु $A \subseteq I$ का तात्पर्य $A = I$ हुआ जो कि ऐसा है नहीं।

इस प्रकार $x \notin A$

टिप्पणी

पुनः $A = (a_o) \subseteq I$

किसी y हेतु $\Rightarrow a_o = xy$

$a_o\ x \Rightarrow$ अलघुकरणीय है अथवा y ईकाई है।

यदि y ईकाई है तो $yy^{-1} = 1$

तथा $a_o = xy$

$\Rightarrow \quad a_o y^{-1} = x$

परन्तु $a_o \in A, y^{-1} \in R \Rightarrow a_o y^{-1} \in A$

$\Rightarrow \quad x \in A$, जो कि वास्तविक नहीं है।

इस प्रकार y ईकाई नहीं है।

अतः x ईकाई है एवं $xx^{-1} = 1$

अब $x \in I,\ x^{-1} \in R,\ I$ एक आदर्श है।

$xx^{-1} \in I \Rightarrow 1 \in I \Rightarrow I = R, A, R$ का महत्तम आदर्श है।

ध्यान दें: स्मरण करें कि क्षेत्र F में दो ही आदर्शस F व $\{0\}$ हैं। F महत्तम नहीं है एवं 0 अलघुकरणीय नहीं है।

5.7.1 अद्वितीय गुणनखंड डोमेन

परिभाषा: माना कि, R ईकाई युक्त समाकलित डोमेन हो तो R को अद्वितीय गुणनखंड डोमेन (Unique Factorization Domains) (यूएफ़डी या UFD) कहा जाता है यदि,

(i) R के प्रत्येक अशून्य, गैर–ईकाई अवयव a को R के अलघुकरणीय अवयवों की परिमित संख्या के गुणन के रूप में व्यक्त किया जा सके।

(ii) यदि $a = p_1 p_2 \ldots\ldots p_m$

$a = q_1 q_2 \ldots\ldots q_n$

जहाँ p_i व q_j, R में अलघुकरणीय हों तो $m = n$ एवं प्रत्येक p_i किसी q_j का संबद्ध है।

(वास्तव में q_i को इस प्रकार लिखना सम्भव हो जायेगा कि प्रत्येक $p_{i'}$ q_i का संबद्ध होगा)।

उदाहरणार्थ, पूर्णांकों की वलय $< \mathbf{Z}, +, \cdot >$ एक यूएफ़डी है। हमें विदित है कि यह ईकाई युक्त समाकलित डोमेन है। यदि $n \in \mathbf{Z}$, अर्थात, $n \neq 0, \pm 1$ का कोई अशून्य, गैर–ईकाई अवयव $\mathbf{Z}$ हो तो यदि $n > 0$ तो हम लिख सकते हैं।

$n = p_1^{\alpha_1}\ p_2^{\alpha_2} \ldots\ldots\ p_m^{\alpha m}$ जहाँ p_i अभाज्य हैं।

$\Rightarrow\ n = (p_1 p_1 \ldots\ldots p_1)\ (p_2 p_2 \ldots\ldots p_2) \ldots\ldots (p_r p_r \ldots\ldots p_r)$

अथवा $n, \mathbf{Z}$ के अभाज्य (एवं इस प्रकार अलघुकरणीय) अवयवों का गुणन है। पुनः n का यह निरूपण (Representation) अद्वितीय है (अंकगणित के आधारभूत प्रमेय से (By Fundamental Theorem of Arithmetic))।

टिप्पणी

जिस प्रकरण में $n < 0$, मान लें कि $n = (-m)$ है, जहाँ $m > 0$ तो हम $\mathbf{Z}$ को m में अभाज्य (इसीलिये अलघुकरणीयों) के गुणन के रूप में व्यक्त कर सकते हैं।

$m = q_1 q_2 \ldots\ldots q_k$ मानें

तो $(-m) = n = (-q_1)\,(q_2) \ldots\ldots (q_k)$

क्षेत्र $< F, +, \cdot >$ सदा यूएफ़डी है क्योंकि इसमें अशून्य, गैर–ईकाई अवयव नहीं हैं।

$\mathbf{Z}[\sqrt{-5}]$ एक समाकलित डोमेन है जो कि यूएफ़डी नहीं है।

$46 \in \mathbf{Z}[\sqrt{-5}]$ गैर–ईकाई, अशून्य अवयव है एवं हम इसे अलघुकरणीयों के गुणन के रूप में दो रीतियों में व्यक्त कर सकते हैं,

$46 = 2 \,.\, 23$

$46 = (1+3\sqrt{-5})(1-3\sqrt{-5})$

किन्तु 2, $1+3\sqrt{-5}$ अथवा $1-3\sqrt{-5}$ का संबद्ध नहीं है। इसी कारण $\mathbf{Z}[\sqrt{-5}]$ यूएफ़डी नहीं है।

ध्यान दे : $\mathbf{Z}[\sqrt{-5}]$ में अलघुकरणीय है परन्तु अभाज्य नहीं एवं इस प्रकार आगामी प्रमेय के प्रयोग से $\mathbf{Z}[\sqrt{-5}]$ यूएफ़डी नहीं हो सकता।

प्रमेय 5.32: यूएफडी में R अवयव एक अभाज्य है यदि यह अलघुकरणीय है।

प्रमाण: $a \in R$ कोई अभाज्य अवयव हो तो चूँकि R ईकाई युक्त एक समाकलित डोमेन है, a अलघुकरणीय होगा।

इसके विपरीत $a \in R$ अलघुकरणीय हो तो a अशून्य, गैर–ईकाई है। $a \mid bc$ मान लें तो किसी भी k के लिए $bc = ak$।

प्रकरण 1: b ईकाई है तो,

$c = akb^{-1} = a\,(kb^{-1}) \Rightarrow a \mid c$

प्रकरण 2: c ईकाई है तो इसी प्रकार $a \mid b$ है।

प्रकरण 3: b, c गैर–ईकाई हैं।

यदि k ईकाई है तो $bc = ak$

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

चूँकि a अलघुकरणीय है, b अथवा ck^{-1} एक ईकाई है परन्तु b ईकाई नहीं है। इस प्रकार ck^{-1} ईकाई है।

परन्तु इसका तात्पर्य हुआ कि c एक ईकाई है जो कि पुनः अवास्तविक है। इसी कारण k ईकाई नहीं है। इस प्रकार हम व्यक्त कर सकते हैं,

$b = p_1 p_2 \ldots\ldots p_m$.

$c = q_1 q_2 \ldots\ldots q_n$

$k = r_1 r_2 \ldots\ldots r_t$

अलघुकरणीयों के गुणनों के रूप में (यूएफ़डी की परिभाषानुसार)।

अतः $bc = ak, p_1p_2 ..... p_m\, q_1q_2 ..... q_n = ar_1\, r_2 ..... r_t = x$ में रूपान्तरित हो जाता है।

तदुपरान्त x ऐसा अवयव है जिसमें अलघुकरणीय अवयवों के गुणनों के रूप में दो निरूपण हैं। यूएफडी की परिभाषानुसार एक निरूपण में प्रत्येक अवयव अन्य निरूपण में किसी अवयव का संबद्ध है।

टिप्पणी

p_i किसी q_j अथवा किसी a का संबद्ध है।

किसी भी ईकाई u के लिए $ua = p_i$ अथवा $ua = q_j$

$a \mid p_i$ अथवा $a \mid q_j$

$\Rightarrow\ a \mid b$ अथवा $a \mid c \quad (p_i \mid b, q_j \mid c)$

a अभाज्य अवयव है।

प्रमेय 5.33: यदि R ईकाई युक्त एक समाकलित डोमेन है जिसमें प्रत्येक अशून्य, गैर–ईकाई अवयव अलघुकरणीय अवयवों का एक परिमित गुणन है एवं प्रत्येक अलघुकरणीय अवयव एक अभाज्य है तो R यूएफ़डी है।

प्रमाणः R एक यूएफ़डी है यह दर्शाने के लिये हमें यह सिद्ध करने की आवश्यकता है कि यदि $a \in R$ अशून्य, गैर–ईकाई अवयव है एवं $a = p_1p_2 ..... p_m = q_1q_2 ..... q_n$ है, जहाँ p_i व q_j अलघुकरणीय अवयव हैं तो $m = n$ तथा प्रत्येक p_i किसी q_j का एक संबद्ध है।

हम n पर प्रवेशण का प्रयोग करते हैं।

$n = 1$ मानें तो $a = p_1p_2 ..... p_m = q_1$ एवं चूँकि q_1 अलघुकरणीय है इसलिये कोई p_i एक ईकाई है परन्तु अलघुकरणीय होने से प्रत्येक p_i ईकाई नहीं हो सकता। इस प्रकार $m = 1$

अतः $a = p_1 = q_1$ अथवा परिणाम $n = 1$ हेतु वास्तविक है। इसे $n - 1$ हेतु वास्तविक मान लेते हैं।

अब मान लें $a = p_1p_2 ..... p_m = q_1q_2 ..... q_n$

तो $p_1p_2 ..... p_m = q_1(q_2 ..... q_n)$

$\Rightarrow \quad q_1 \mid p_1p_2 ..... p_m$

चूँकि q_1 अलघुकरणीय है अतः यह अभाज्य है (दिये गये पद के अनुसार)।

किसी भी i के लिए $q_1 \mid p_i$

व्यापकता की हानि हुए बिना हम मान सकते हैं कि $i = 1$

तो $\Rightarrow q_1 \mid p_1 \Rightarrow p_1 = q_1u_1$

किन्तु p_1 अलघुकरणीय $\Rightarrow q_1$ अथवा u_1 एक ईकाई है।

चूँकि q_1 ईकाई नहीं है (अलघुकरणीय है), u_1 ईकाई होगा एवं इस प्रकार p_1, q_1 संबद्ध हैं।

अब $(q_1u_1)p_2p_3 ..... p_m = q_1q_2 ..... q_n$

टिप्पणी

अथवा $(u_1p_2)p_3 ..... p_m = q_2q_3 ..... q_n$

$\Rightarrow p_2'p_3 ..... p_m = q_2q_3 ..... q_n, \quad p_2' = u_1p_2$ अलघुकरणीय है।

R.H.S. में $n-1$ अवयव अंतर्विष्ट हैं एवं परिणाम $n-1$ हेतु वास्तविक है, तो हम पाते हैं कि $m-1 = n-1 \Rightarrow m = n$

वैसे भी जिस प्रकार हमने दर्शाया कि q_1 एक संबद्ध अथवा p_1 है, हम दर्शा सकते हैं कि q_2, p_2 से संबद्ध है, $p_1p_2 ..... p_m = q_2(q_1q_3 ..... q_n)$ का विचार करते हुए,

इस प्रकार q_i, p_i का संबद्ध होगा।

इसी कारण R एक यूएफ़डी है।

चूँकि यह पहले से ही सिद्ध हो चुका है कि यूएफ़डी में प्रत्येक अलघुकरणीय अवयव अभाज्य होता है, इसी कारण यह सिद्ध हुआ।

प्रमेय 5.34: ईकाई युक्त समाकलित डोमेन R एक यूएफ़डी है यदि और केवल यदि प्रत्येक अशून्य, गैर–ईकाई अवयव अलघुकरणीय अवयवों का परिमित गुणन (Finite Product) है एवं प्रत्येक अलघुकरणीय अवयव अभाज्य है।

यूएफ़डी की द्वितीय परिभाषा का प्रयोग विभिन्न यूएफ़डी आधारित समस्याओं के हल हेतु किया जाता है।

प्रमेय 5.35: ईकाई युक्त समाकलित डोमेन R एक यूएफ़डी है यदि प्रत्येक अशून्य, गैर–ईकाई अवयव अभाज्यों (Primes) का परिमित गुणन है।

प्रमाण: यदि R एक यूएफ़डी है तो प्रत्येक अशून्य, गैर–ईकाई अवयव अलघुकरणीयों का परिमित गुणन है (परिभाषानुरूप) तथा प्रत्येक अलघुकरणीय अवयव अभाज्य भी है, इसी कारण यह परिणाम आया।

इसके विपरीत माना $a \in R$ अशून्य, गैर–ईकाई अवयव हो तो $a = p_1p_2 ..... p_n$ जहाँ p_i अभाज्य अवयव $\forall\ i$ हैं। चूँकि R एक समाकलित डोमेन है, अभाज्य अवयव अलघुकरणीय हैं एवं इसलिये प्रत्येक p_i अलघुकरणीय है। हम अब यह दर्शाते हैं कि R का प्रत्येक अलघुकरणीय अवयव एक अभाज्य अवयव है। माना कि, $x \in R$ कोई अलघुकरणीय अवयव है तो $x \neq 0$ गैर–ईकाई है। इस प्रकार $x = q_1q_2 ..... q_m$ जहाँ q_i अभाज्य हैं। मान लें कि $m > 1$। चूँकि x अलघुकरणीय है, या तो q_1 अथवा $(q_2q_3 .. q_m)$ ईकाई है किन्तु q_1 अभाज्य है व इस प्रकार ईकाई नहीं हो सकता। अतः $(q_2q_3 ..... q_m)$ ईकाई है जिसका तात्पर्य है कि q_2 ईकाई है किन्तु वास्तविक नहीं है क्योंकि q_2 अभाज्य है। इसी कारण $m = 1$ अथवा x अभाज्य है। प्रमेय 5.33 के अनुसार अब R एक यूएफ़डी है। अन्ततः पूर्ववर्ती परिणामों में हमने सिद्ध किया।

प्रमेय 5.36: यदि R ईकाई युक्त समाकलित डोमेन हो तो निम्नांकित समकक्ष हैं:

(i) R यूएफ़डी है।

(ii) R का प्रत्येक अशून्य, गैर–ईकाई अवयव अलघुकरणीय अवयवों का परिमित गुणन है एवं प्रत्येक अलघुकरणीय अवयव अभाज्य है।

(iii) R का प्रत्येक अशून्य, गैर–ईकाई अवयव अभाज्य अवयवों का परिमित उत्पाद है।

प्रमेय 5.37: R, UFD में किन्हीं दो अशून्य अवयवों में महत्तम उभयनिष्ठ भाग है।

प्रमाण: माना a, b को R के दो अशून्य अवयव मानते हुए मान लें कि इनमें से एक (a कहते हैं) ईकाई है तो,

टिप्पणी

$\therefore \quad b = (aa^{-1})b = a(a^{-1}\ b) \Rightarrow a \mid b$

$a = 1.\ a \Rightarrow a \mid a$ भी।

अब यदि $c \mid a$ व $c \mid b$ तो चूँकि इसका तात्पर्य $c \mid a$ है।

हम पाते हैं $a = \text{G.C.D.}(a, b)$

इसी प्रकार यदि b ईकाई हो $b = \text{G.C.D.}(a, b)$

अब मान लेते हैं कि a व b गैर–इकाइयाँ हैं। चूँकि R एक यूएफ़डी है हम व्यक्त कर सकते हैं कि,

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots\ldots p_n^{\beta_n}$$

अलघुकरणीयों के गुणन के रूप में (ध्यान दे: उपर्युक्त घातों का चयन करते हुए समान अलघुकरणीयों के गुणन के रूप में a, b दोनों को व्यक्त किया जाना सम्भव है)।

$s_i = \text{न्यूनतम } (\alpha_i, \beta_i)$ मान लेते हैं।

हम दर्शाते हैं कि $d = p_1^{s_1}\ p_2^{s_2} \ldots\ldots p_n^{s_n}$, $\text{G.C.D.}(a, b)$ है।

अब $a = (\ p_1^{s_1}\ p_2^{s_2} \ldots\ldots p_n^{s_n}\ )\ (\ p_1^{\alpha_1 - s_1}\ p_2^{\alpha_2 - s_2} \ldots\ldots p_n^{\alpha_n - s_n}\ )$

$= d\ (\ p_1^{\alpha_1 - s_1}\ p_2^{\alpha_2 - s_2} \ldots\ldots p_n^{\alpha_n - s_n}\ )$

$\Rightarrow d \mid a$

इसी प्रकार $d \mid b$

अब $c \mid a$ व $c \mid b$ मान लेते हैं।

यदि c एक ईकाई है $d = (cc^{-1})d \Rightarrow c \mid d$

यदि c ईकाई नहीं है तो हम लिख सकते हैं $c \quad = p_1^{r_1}\ p_2^{r_2} \ldots\ldots p_n^{r_n}$

चूँकि सभी i के लिए $\mid a, r_i \quad \leq \alpha_i$

सभी i के लिए $c \mid b, r_i \leq \beta_i$

सभी i के लिए $r_i \leq \text{Min } (\alpha_i, \beta_i) = s_i$

इस प्रकार $d = p_1^{s_1}\ p_2^{s_2} \ldots\ldots p_n^{s_n} = (\ p_1^{r_1}\ p_2^{r_2} \ldots\ldots p_n^{r_n}\ )\ (\ p_1^{s_1 - r_1} \ldots\ldots p_n^{s_n - r_n}\ )$

$\Rightarrow \quad c \mid d$

इसी कारण $d = \text{G.C.D.}(a, b)$

जिससे हमारा परिणाम सिद्ध हुआ।

जैसा कि पहले देखा जा चुका है कि यदि d_1 व d_2, a, b के दो महत्तम अभ्यनिष्ट भाजक हों तो d_1 व d_2 में संबद्ध हैं।

टिप्पणी

प्रमेय 5.38: यूएफ़डी में किन्हीं दो अशून्य अवयवों में L.C.M है।

उदाहरण 5.42: यदि UFD R में a, b आपेक्षाकृत अभाज्य हों तो $a \mid bc \Rightarrow a \mid c$

हल: $a \mid bc$ मान लें तो $\exists\, r$ इस प्रकार है कि $bc = ar$

यदि a ईकाई है तो,

$c = (aa^{-1})c = a(a^{-1}c) \Rightarrow a \mid c$

यदि b ईकाई है,

$ba = ar \Rightarrow c = b^{-1} ar$

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

यदि c ईकाई है $bc = ar$

$\Rightarrow \quad b = arc^{-1} \Rightarrow a \mid b$

$\Rightarrow \quad \text{g.c.d.}(a, b) = a$

परन्तु a, b आपेक्षाकृत अभाज्य होने से G.C.D.(a, b) ईकाई होगा।

a ईकाई है।

$a \mid c$ (पूर्व की भाँति)।

यदि r ईकाई है तो,

$bc = ar$

$\Rightarrow \quad bcr^{-1} = a \Rightarrow a \mid b$

$\Rightarrow \quad \text{G.C.D.}(a, b) = b \Rightarrow b$ ईकाई है।

$a \mid c$ (पूर्व की भाँति)।

मान लें कि अब a, b, c, r में कोई भी ईकाई नहीं है।

यदि $b = 0$, तो महत्तम उभयनिष्ठ भाजक $(a, b) = a$ ईकाई है जो कि वास्तविक नहीं हैं।

$\therefore \quad b \neq 0$

यदि $c = 0$ तो $c = a \,.\, 0 \Rightarrow a \mid c$

अतः मान लें कि $b \neq 0, c \neq 0$, हमें प्राप्त होगा $a \neq 0, r \neq 0$

(चूँकि $bc = ar$)

अब a, b, c, r में UFD या यूएफडी अशून्य, गैर–इकाइयाँ होने से हम व्यक्त कर सकते हैं कि,

$a = a_1 a_2 \ldots\ldots a_m$

$b = b_1 b_2 \ldots\ldots b_n$

$c = c_1 c_2 \ldots\ldots c_t$

$r = r_1 r_2 \ldots\ldots r_k$

जो कि अलघुकरणीय अवयवों के गुणन हैं।

टिप्पणी

इस प्रकार $(b_1b_2 ..... b_n)(c_1c_2 ..... c_t) = (a_1a_2 ..... a_m)(r_1r_2 ..... r_k) = x$ (कहें) तो x में अलघुकरणीय अवयवों के गुणन के रूप में दो निरूपण हैं। इसीलिये यूएफडी (UFD) की परिभाषानुसार इन निरूपणों में अवयवों की समान संख्या होगी एवं एक ओर का प्रत्येक अवयव अन्य ओर के एक अवयव का संबद्ध होगा। अतः $n + t = m + k$ एवं प्रत्येक a_i किसी b_i अथवा c_i का संबद्ध है।

यदि a_i किसी b_i का संबद्ध है तो

ईकाई u के लिए $b_i = a_i u$

व चूँकि $a_i \mid b_i$

हम पाते हैं $a_i \mid b$

$a_i \mid$ महत्तम उभयनिष्ठ भाग $(a, b) = 1$ क्योंकि $a_i \mid a$

a_i ईकाई है जो कि वास्तविक नहीं है क्योंकि a_i अलघुकरणीय है।

इसी कारण प्रत्येक a_i को किसी c_i का संबद्ध होना होगा,

ईकाई u_i हेतु $a_i = c_i u_i$

जिससे $(b_1b_2 ..... b_n)(c_1c_2 ..... c_t) = (c_1u_1c_2u_2 ..... c_mu_m)(r_1r_2 ..... r_k)$ सामने आता है,

$\Rightarrow \quad b(c_{m+1}c_{m+2} ..... c_t) = (u_1u_2 ..... u_m)r$

$\Rightarrow \quad b(c_{m+1}c_{m+2} ..... c_t)(u_1u_2 ..... u_m)^{-1} = r$

किसी d हेतु $b \mid r \Rightarrow r = bd$

$bc = ar = abd$

$\Rightarrow \quad b(c - ad) = 0 \Rightarrow c = ad. \quad \Rightarrow a \mid c$

हम अब अतिमहत्त्वपूर्ण प्रमेय के प्रमाण की बात करते हैं कि प्रत्येक पीआईडी (PID) यूएफ़डी (UFD) है परन्तु इस चर्चा से पहले कुछ लैमाज़ को सिद्ध कर लेने से बड़ी सहायता होगी।

लैमा (Lemma) 1: वलय R में आदर्श $A_1 \subseteq A_2 \subseteq A_3 \subseteq .....$ की आरोही शृंखला का संघ R का आदर्श है।

प्रमाण: $A = \cup A_i$ मानें एवं किसी भी i, j के लिए $\Rightarrow x \in A_i, y \in A_j$

व्यापकता की हानि बिना हम मान लें $i \leq j$ तो $A_i \subseteq A_j$

$\therefore x, y \in A_j = x - y \in A_j \subseteq A$

पुनः $x \in A, r \in R$ का तात्पर्य होगा जो कि इसी समान है $xr; rx \in A$। इसी कारण यह लैमा है।

लैमा (Lemma) 2: (आरोही शृंखला पद): PID R में आदर्श की प्रत्येक आरोही शृंखला पदों की परिमित संख्या के उपरान्त समाप्त होनी चाहिए।

प्रमाण: $A_1 \subseteq A_2 \subseteq A_3 \subseteq .....$ को प्रदर्शित शृंखला मानें।

माना $A = \cup A_i$ हो तो A, R का आदर्श है जिसके पीआईडी (PID) होने का तात्पर्य है कि A एक आदर्श सिद्धांत है।

टिप्पणी

$A = (a)$ मान लें तो $a \in (a) = A = \cup A_i$

किसी भी i के लिए $a \in A_i$

A_i में a के समस्त गुणज $A_i \Rightarrow (a) \subseteq A_i$

$A \subseteq A_i \subseteq A_{i+1} \subseteq .....$

अर्थात् $A \subseteq A_t$ प्रत्येक $t \geq i$ के लिए,

अर्थात् $A \subseteq A_i \subseteq A_t \subseteq A$ के लिए,

$\Rightarrow \quad A_i = A_t$

जिससे हमारा अभिकथन (Assertion) सिद्ध हुआ।

लैमा (Lemma) 3: PID R में प्रत्येक अशून्य, गैर–ईकाई अवयव अलघुकरणीय अवयव द्वारा विभाज्य है।

प्रमाण: $a \in R$ को अशून्य, गैर–ईकाई अवयव मान लें। मान लेते हैं कि $I_1 = (a)$.

यदि I_1 महत्तम आदर्श है तो a अलघुकरणीय है एवं चूँकि $a \mid a$, हमारा लैमा सिद्ध हो गया। मान लें कि I_1 महत्तम नहीं हो तो $\exists$ कोई आदर्श $I_2 \neq R$ इस प्रकार है कि $I_1 \subset I_2 \subset R$।

मान लें कि $I_2 = (p_2)$

यदि I_2 महत्तम हो तो p_2 अलघुकरणीय होगा एवं चूँकि $p_2 \mid a$ अतः लैमा सिद्ध हुआ। $(a \in I_1 \subset I_2 = (p_2) \Rightarrow a = tp_2)$

मान लें कि I_2 महत्तम नहीं है तो $\exists$ आदर्श I_3 इस प्रकार है कि $I_1 \subset I_2 \subset I_3 \subset R$ एवं इस दिशा में आगे बढ़ने से हमें R में आदर्श की आरोही श्रृंखला प्राप्त होती है जो कि लैमा 2 द्वारा पदों की परिमित संख्या के उपरान्त समापित होनी ही है, $I_n = (p_n)$ पर जो कि अब महत्तम होगा एवं $p_n, p_n \mid a$ के साथ अलघुकरणीय होगा।

प्रमेय 5.39: पीआईडी R एक यूएफडी है।

प्रमाण: $a \in R$ को कोई अशून्य, गैर–ईकाई अवयव मानें। यदि a अलघुकरणीय हो तो चूँकि $a = a$, हम a को अलघुकरणीयों के परिमित गुणन के रूप में व्यक्त कर सकते हैं। यदि a अलघुकरणीय न हो तो लैमा 3 के अनुसार a किसी अलघुकरणीय अवयव p_1 द्वारा विभाज्य है।

किसी a_1 हेतु $p_1 \mid a \Rightarrow a = a_1 p_1$

यदि a_1 अलघुकरणीय हो तो आप a को अलघुकरणीय अवयवों की परिमित संख्या के गुणन के रूप में व्यक्त कर सकते हैं।

मान लेते हैं कि a_1 अलघुकरणीय नहीं है।

तदुपरान्त a_1 अशून्य, गैर–ईकाई अवयव है क्योंकि $a_1 = 0 \Rightarrow a = 0$ जो कि ऐसा है नहीं। पुनः यदि a_1 ईकाई हो तो चूँकि $a = a_1 p_1$ हम पाते हैं कि a व p_1 संबद्ध हैं एवं अतः a अलघुकरणीय है क्योंकि p_1 अलघुकरणीय है, परन्तु a_1 अलघुकरणीय नहीं है।

टिप्पणी

इस प्रकार पुनः लैमा 3 द्वारा $\exists$ अलघुकरणीय अवयव p_2 इस प्रकार है कि $p_2 \mid a_1$ होगा।

किसी भी a_2 के लिए $a_1 = p_2 a$

यदि a_2 अलघुकरणीय हो तो,

$a = a_1 p_1 = p_2 p_1 a_2$

इसी कारण सिद्ध हुआ कि यदि a_2 अलघुकरणीय न हो तो हम इस प्रकार आगे बढ़ सकते हैं।

आदर्श $(a), (a_1), (a_2), \ldots$ का विचार करें।

तो $(a) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$

चूँकि $x \in (a) \Rightarrow x = ar = p_1 a_1 r \in (a_1)$, इत्यादि।

इस प्रकार हमें आदर्श की आरोही श्रृंखला प्राप्त होती है जिसे पदों की परिमित संख्या के पश्चात् समापित होना ही है (लैमा 2 अनुसार)। इसी कारण आपको कोई अलघुकरणीय अवयव a_n प्राप्त होगा,

अतः $a = p_1 p_2 \ldots p_n a_n$

अर्थात् a को अलघुकरणीय अवयवों की परिमित संख्या के गुणन में रूप में व्यक्त किया जाता है।

हमें अब यह दर्शाने की आवश्यकता है कि यदि a ऐसे दो से अधिक निरूपण हों तो अवयवों की संख्या दोनों में समान होगी तथा एक निरूपण में प्रत्येक अवयव अन्य निरूपण में एक अवयव का संबद्ध है।

$a = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$ मान लें तथा प्रमेय 5.32 में दर्शाये अनुसार ही आगे बढ़ते हैं एवं हमारा परिणाम सिद्ध हुआ।

प्रमेय 5.40: यदि $f(x)$ $R[x]$ में अशून्य बहुपद हो जहाँ R एक यूएफ़डी है तो $f(x) = df_1(x)$ जहाँ f_1 आद्यक (Primitive) है एवं $d = c(f)$

प्रमाण: $f(x) = a_o + a_1 x + \ldots + a_n x^n$ मान लें,

तथा मान लेते हैं कि $c(f) = d = \text{G.C.D.}(a_o, a_1, \ldots a_n)$

तो सभी i के लिए $d \mid a_i$

किसी u_i के लिए $a_i = du_i$

$f(x) = du_o + du_1 x + \ldots + du_n x^n$

$= d(u_o + u_1 x + \ldots + u_n x^n) = df_1(x)$ जहाँ $f_1(x)$ आधक होगा।

ध्यान दें: यदि $t = \text{G.C.D.}(u_o, u_1, \ldots, u_n)$

तो $t \mid u_i \; \forall \; i \Rightarrow td \mid du_i \; \forall \; i$

$td \mid a_i \; \forall \; i$ एवं इस प्रकार $td \mid d$

$t \mid 1$ अथवा t एक ईकाई है।

टिप्पणी

प्रमेय 5.41 (गॉस–लैमा (Gauss's Lemma)): माना R को यूएफ़डी मानें तो $R[x]$ में दो आधक बहुपदों का गुणन आधक बहुपद है।

प्रमाण: मान लें कि $f(x) = a_o + a_1x + ... + a_mx^m$

$g(x) = b_o + b_1x + ... + b_nx^n$, $R[x]$ में दो आधक बहुपद हैं तो $f(x)$ व $g(x)$ अशून्य हैं (परिभाषानुसार)। इस प्रकार,

$f(x)g(x) = c_o + c_1x + c_2x^2 + ...$ भी अशून्य है।

मान लेते हैं $d = \text{g.c.d.}(c_o, c_1, c_2, ...)$

हम दर्शाते हैं कि d ईकाई है। मान लें कि ऐसा न हो तो अलघुकरणीय अवयव p इस प्रकार विद्यमान् होगा कि $p|d$।

[स्मरण रहे कि यूएफ़डी में गैर–ईकाई अवयव a को अलघुकरणीयों के गुणन $a = p_1p_2 ..... p_n \Rightarrow p_1 \mid a$ के रूप में व्यक्त किया जा सकता है।]

इस प्रकार सभी i के लिए $p \mid d \Rightarrow p \mid c_i$ ...(i)

अब यदि सभी i के लिए $p \mid a_i$ तो $p \mid \text{g.c.d.}\ (a_o, a_1, ..., a_m)$ जो कि एक ईकाई है (जैसे u)।

अब $p \mid u \Rightarrow u = pk \Rightarrow 1 = p(ku^{-1})$

p ईकाई है।

जो कि वास्तविक नहीं है क्योंकि p अलघुकरणीय है।

किसी भी i के लिए $p \nmid a_i$ होगा।

i को ऐसा लघुतम धनात्मक पूर्णांक मानें तो,

$p \mid a_o, p \mid a_1, ..., p \mid a_{i-1}, p \nmid a_i$

इसी प्रकार $\exists$ कोई पूर्णांक j इस प्रकार है,

$p \mid b_o, p \mid b_1, ..., p \mid b_{j-1}, p \nmid b_j$

अब $c_{i+j} = (a_ob_{i+j} + a_1b_{i+j-1} + ... + a_{i-1}\, b_{j+1})$

$+ a_ib_j + (a_{i+1}\, b_{j-1} + ... + a_{i+j}\, b_o)$

चूँकि समीकरण (i) के अनुसार $p \mid c_{i+j}$ तथा

$p \mid (a_ob_{i+j} + a_1b_{i+j-1} + ... + a_{i-1}\, b_{j+1})$,

$p \mid (a_{i+1}\, b_{j-1} + ... + a_{i+j}\, b_0)$

हम पाते हैं कि $p \mid a_ib_j, p$ परन्तु यूएफ़डी में अलघुकरणीय होने से p अभाज्य है।

$p \mid a_i$ अथवा $p \mid b_j$ जो कि एक विरोधाभास है। इसी कारण यह परिणाम आया।

उपप्रमेय (Corollary) : यदि R एक यूएफ़डी है एवं $f(x), g(x) \in R[x]$ तो,

$c(f(g)) = c(f)\, c(g)$ (आच्छादक इकाइयाँ)

चूँकि हम लिख सकते हैं कि $f(x) = df_1(x)$, $d = c(f)$

$g(x) = d'g_1(x)$, $d' = c(g)$

टिप्पणी

$f(x)g(x) = dd' f_1(x)\ g_1(x)$

जहाँ f_1, g_1 आधक होने से $f_1 g_1$ आधक मिलता है।

$c(f_1 g_1) = 1$ (अथवा ईकाई)

$\therefore \qquad c(fg) = dd' = c(f)\ c(g)$

गॉस लैमा का विलोम भी वास्तविक है क्योंकि हम सिद्ध कर सकते हैं।

प्रमेय 5.42: यदि $f(x)g(x)$ $R[x]$ में आधक बहुपद हो, R यूएफ़डी हो तो इसलिये $f(x)$ व $g(x)$ होंगे।

प्रमाण: fg आधक है।

$c(fg)$ ईकाई है।

$\exists$ अवयव $r \in R$ इस प्रकार है कि $c(fg)r = 1$

$\Rightarrow \quad c(f)\ c(g)\ r = 1$

$\Rightarrow \quad c(f)\ [c(g)\ .\ r] = 1$

$c(f)$ ईकाई है $\Rightarrow f$ आधक है।

इसी प्रकार $c(g)$ ईकाई है g आधक है।

प्रमेय 5.43: यदि R ईकाई युक्त समाकलित डोमेन है तो R व $R[x]$ की इकाइयाँ समान होंगी।

प्रमाण: a_o को R की ईकाई मानें तो $\exists\ b_o \in R$ इस प्रकार है कि $a_o b_o = 1$

मान लेते हैं कि $f(x) = a_o + 0.x + 0.x^2 + ...$

$g(x) = b_o + 0.x + 0.x^2 + ...$

तो $f(x)g(x) = a_o b_o + 0.x + 0.x^2 + ...$

$= 1 = 1 + 0.x + 0.x^2 + ...$

$f(x),\ R[x]$ में ईकाई है।

अर्थात् $a_o,\ R[x]$ में ईकाई है।

इसके विपरीत $f(x)$ को $R[x]$ की ईकाई मानें तो,

$\exists\ g(x) \in R[x]$ इस प्रकार है कि,

$f(x)g(x) = 1\ (= 1 + 0.x + 0.x^2 + ...)$

$\Rightarrow$ deg (fg) = deg 1

$\Rightarrow$ deg f + deg g = 0

$\Rightarrow$ deg f = deg g = 0

$\Rightarrow f$ व g अचर बहुपद हैं।

अर्थात् $f(x) = a_o + 0x + 0x^2 + ...a_o \in R$

$g(x) = b_o + 0x + 0x^2 + ...b_o \in R$

टिप्पणी

चूँकि $fg = a_o b_o = 1$

हम पाते हैं $a_o = f(x)$, R की ईकाई है।

इसी कारण यह परिणाम है।

उदाहरण 5.43: दर्शायें कि $2x + 1$, $\mathbf{Z}_4[x]$ में ईकाई है।

हल: चूँकि $(2x + 1)(2x + 1) = 0x^2 + 0x + 1 = 1$

$[4 = 0\ \mathbf{Z}_4$ में]

हम पाते हैं कि $2x + 1$, $\mathbf{Z}_4[x]$ में एक ईकाई है।

ध्यान दे: $2x + 1$ एक अनियतांक / गैर–अचर बहुपद है एवं इसीलिये यह $\mathbf{Z}_4$ से संबंधित नहीं है तथा इस प्रकार $\mathbf{Z}_4$ में ईकाई नहीं हो सकता परन्तु अब $\mathbf{Z}_4$ समाकलित डोमेन नहीं है। वस्तुतः 1 व 3 $\mathbf{Z}_4$. $[3 \otimes 3 = 1]$ की ईकाइयां हैं।

प्रमेय 5.44: यदि R इकाई युक्त समाकलित डोमेन हो एवं R का अलघुकरणीय अवयव हो तो यह $R[x]$ का अलघुकरणीय अवयव है।

प्रमाण: मान लें कि $a, R[x]$ का अलघुकरणीय अवयव नहीं है तो $\exists\, p(x), q(x) \in R[x]$ इस प्रकार है कि $a = p(x)\, q(x)$

जहाँ $p(x)$ व $q(x)$ गैर–इकाइयाँ हैं।

अब $a = pq$

$\Rightarrow \quad \deg a = \deg p + \deg q$

$\Rightarrow \quad 0 = \deg p + \deg q$

$\Rightarrow \quad \deg p = \deg q = 0$

p, q अचर बहुपद हैं $\Rightarrow p, q \in R$

इस प्रकार $a = pq, p, q \in R$ व p, q गैर–इकाइयां हैं, [जहाँ R व $R[x]$ की इकाइयां समान हैं], यह इस तथ्य से विरोधाभासी है कि a, R में अलघुकरणीय है।

इसी कारण यह परिणाम आया।

परिभाषा: R को इकाई युक्त समाकलित डोमेन मानें। धनात्मक श्रेणी (अर्थात् ≥ 1 की) के बहुपद $f(x) \in R[x]$ को R पर अलघुकरणीय बहुपद कहा जाता है यदि इसे धनात्मक श्रेणी के दो बहुपदों के गुणन के रूप में व्यक्त न किया जा सके।

अन्य शब्दों में यदि कभी $f(x) = g(x)h(x)$

तो $\deg g = 0$ अथवा $\deg h = 0$

धनात्मक श्रेणी का बहुपद (जो कि अलघुकरणीय नहीं है) R पर अलघुकरणीय कहा जाता है।

प्रमेय 5.45: यदि F एक क्षेत्र हो तो $F[x]$ में आदर्श $< p(x) > \neq \{0\}$ महत्तम है यदि $p(x)$, $F[x]$ में अलघुकरणीय है।

प्रमाण: यदि $p(x), F$ पर अलघुकरणीय बहुपद है तो यह $F[x]$ का अलघुकरणीय अवयव है एवं चूँकि F एक क्षेत्र है, $F[x]$ ऐसा पीआईडी है जो कि क्षेत्र नहीं है। अब परिणाम प्रमेय में आता है।

उदाहरण 5.44: दर्शायें कि $\frac{\mathbf{Q}[x]}{I}$ जहाँ $I = < x^2 - 5x + 6 >$ क्षेत्र नहीं है।

हल: चूँकि $x^2 - 5x + 6 = (x - 2)(x - 3)$ हम पाते हैं कि यह Q पर अलघुकरणीय बहुपद नहीं है।

टिप्पणी

इस प्रकार $I = < x^2 - 5x + 6 >$, $\mathbf{Q}[x]$ का महत्तम आदर्श नहीं है एवं इसी कारण $\frac{\mathbf{Q}[x]}{I}$ क्षेत्र नहीं है।

उदाहरण 5.45: दर्शाएँ कि $f(x) = x^3 - 9$, $\mathbf{Z}_{11}$ में परिवर्तक (Reducible) लेने योग्य है।

हल: चूँकि $\mathbf{Z}_{11}$ में $4 \otimes 4 \otimes 4 = 9$ हम पाते हैं कि $(x - 4)$, $x^3 - 9$ का एक गुणक (Factor) है। यथार्थ विभाजन से हम पाते हैं:

$\mathbf{Z}_{11}$ में $x^3 - 9 = (x - 4)(x^2 + 4x + 5)$

इसी कारण $x^3 - 9$ परिवर्तक (Reducible) लेने योग्य है।

उदाहरण 5.46: दर्शाएँ कि $\mathbf{Z}_5[x]$ एक यूएफ़डी है। क्या $x^2 + 2x + 3$, $\mathbf{Z}_5[x]$ पर परिवर्तक (Reducible) लेने योग्य है?

हल: चूँकि 5 एक अभाज्य है अतः $\mathbf{Z}_5$ एक क्षेत्र है।

$\Rightarrow$ $\mathbf{Z}_5$ एक यूएफ़डी है।

$\Rightarrow$ $\mathbf{Z}_5[x]$ एक यूएफ़डी है।

पुनः $x^2 + 2x + 3$ पर परिवर्तक (Reducible) लेने योग्य होगा यदि इसमें $\mathbf{Z}_5$ में मूल (रूट या root) हो परन्तु $\mathbf{Z}_5$ में कोई अवयव $x^2 + 2x + 3$ का मूल (Root) नहीं है, इसी कारण यह $\mathbf{Z}_5$ पर अलघुकरणीय बहुपद है।

उदाहरण 5.47: दर्शाएँ कि बहुपद $x^2 + x + 2$, $F = \{0, 1, 2\}$ पर अलघुकरणीय है। 9 अवयवों की क्षेत्र बनाने में इसका प्रयोग करें।

हल: मान लें कि $f(x) = x^2 + x + 2$। यदि यह F पर परिवर्तक लेने योग्य है तो हम किसी $\alpha \in F$ को इस प्रकार ज्ञात कर पायेंगे कि $f(\alpha) = 0$

परन्तु $\alpha \in F, f(\alpha) = 0$ के लिये नहीं। उदाहरणार्थ $\alpha = 1$, $1^2 + 1 + 2 = 1 \neq 0$, इत्यादि।

इस प्रकार $f(x)$, F पर अलघुकरणीय बहुपद है एवं चूँकि F एक क्षेत्र है, $f(x)$, $F[x]$ का अलघुकरणीय अवयव है। इसी कारण $< f(x) >$, $F[x]$ का महत्तम आदर्श है, जिससे सिद्ध हो रहा है कि $\frac{F[x]}{< f(x) >}$ एक क्षेत्र है।

इस क्षेत्र का कोई अवयव इस प्रकार का है,

$p(x) + < f(x) >$, जहाँ $p(x) \in F[x]$

चूँकि $F[x]$ युक्लिडीन डोमेन है,

$f(x)$ हेतु $p(x) \in F[x]$, $\exists$ $t(x)$, $r(x)$ इस प्रकार कि,

टिप्पणी

$p(x) = f(x)\,t(x) + r(x)$

जहाँ या तो $r(x) = 0$ अथवा $\deg r(x) < \deg f(x) = 2$

किसी भी प्रकरण में $r(x), ax + b, \quad a, b \in F$ इस प्रकार का है,

अतः $p(x) - r(x) = f(x)\ t(x) \in < f(x) >$

अर्थात् $p - r \in I$ जहाँ $I = < f(x) >$

$\Rightarrow \qquad p - r + I = I$

अर्थात् $p + I = r + I = ax + b + < f(x) >$

इसी कारण कोई अवयव $p + < f(x) >$ of $\frac{F[x]}{< f(x) >}$ इस $ax + b + < f(x) >$ प्रकार का है।

इस प्रकार $\frac{F[x]}{< f(x) >} = \{ax + b + < f(x) > \mid a, b \in F\}$

चूँकि $a \in F = \{0, 1, 2\}$ को तीन रीतियों में चयन किया जा सकता है एवं a, b के प्रत्येक विकल्प के लिये b का चयन तीन रीतियों में किया जा सकता है, हम पाते हैं कि $\frac{F[x]}{< f(x) >}$ के अवयवों की संख्या $3 \times 3 = 9$ होगी। इस प्रकार $\frac{F[x]}{< f(x) >}$ नौ अवयवों की अपेक्षित क्षेत्र है।

ध्यान दे: प्रमेय 5.47 का तात्पर्य यह भी है कि यदि F एक क्षेत्र है व $<p(x)>, F[x]$ का आदर्श तो $\frac{F[x]}{< p(x) >}$ क्षेत्र होगी यदि $p(x), F$ पर अलघुकरणीय है।

उदाहरण 5.48: दर्शायें कि बहुपद $x^3 + 2x + 1, \mathbf{Z}_3[x]$ में अलघुकरणीय है एवं 27 अवयवों वाली क्षेत्र बनाने के लिये इसका प्रयोग करें। उस क्षेत्र में $x^2 + I$ का व्युत्क्रम (Inverse) ज्ञात करें जहाँ $I = < x^3 + 2x + 1 >$ है।

हल: यह सरलता से देखा जा सकता है कि कोई $\alpha \in \mathbf{Z}_3 = \{0, 1, 2\}$ इस प्रकार विद्यमान् नहीं है कि $\alpha^3 + 2\alpha + 1 = 0$। इसी कारण $f(x) = x^3 + 2x + 1, \ \mathbf{Z}_3$ पर अलघुकरणीय है तथा पूर्ववर्ती उदाहरण में दिए अनुसार $\frac{\mathbf{Z}_3[x]}{< f(x) >}$ एक क्षेत्र है। इस क्षेत्र को निम्नानुसार भी प्रदर्शित किया जाता है।

$$\frac{\mathbf{Z}_3[x]}{< f(x) >} = \{a_0 + a_1 x + a_2 x^2 + < f(x) > \mid a_i \in \mathbf{Z}_3\}$$

मान लें कि $< f(x) > = I$

तो $\frac{\mathbf{Z}_3[x]}{I} = \{a_0 + a_1 x + a_2 x^2 + I \mid a_i \in \mathbf{Z}_3\}$

स्पष्टतः चूँकि a_i, भिन्न है $\mathbf{Z}_3 = \{0, 1, 2\}$ इसलिए, $\frac{\mathbf{Z}_3[x]}{I}$ में $3 \times 3 \times 3 = 27$ अवयव हैं।

टिप्पणी

अब मान लें कि $p(x) + I$, $\frac{\mathbf{Z}_3[x]}{I}$ में $x^2 + I$ का व्युत्क्रम है।

तो $(p(x) + I)(x^2 + I) = 1 + I$

$\Rightarrow \quad p(x)\, x^2 + I = 1 + I \quad \Rightarrow p(x)\, x^2 - 1 \in I = < f(x) >$

अर्थात् $p(x)x^2 - 1, f(x)$ का गुणज है। इस प्रकार $\exists$ कोई $t(x)$ इस प्रकार है,

$p(x)x^2 + t(x)\, f(x) = 1$

$p(x)$ को ज्ञात करने के लिये हम युक्लिडीन एल्गोरिद्म (Euclidean Algorithm) का प्रयोग करते हैं

$$\begin{array}{r} x \\ x^2\overline{)\,x^3 + 2x + 1} \\ \underline{x^3} \\ 2x + 1 \end{array} \qquad \begin{array}{r} 2x + 2 \\ 2x + 1\overline{)\,x^2} \\ \underline{x^2 + 2x} \\ x \\ \underline{x + 2} \\ 1 \end{array}$$

ध्यान दें: संक्रियाएँ $\mathbf{Z}_3$ में हैं।

इस प्रकार $x^3 + 2x + 1 = x(x^2) + (2x + 1)$

$x^2 = (2x + 2)(2x + 1) + 1$

दिया गया है $1 = x^2 - (2x + 2)(2x + 1)$

$= x^2 - [(2x + 2)\{(x^3 + 2x + 1) - x(x^2)\}]$

$= x^2 - (2x + 2)(x^3 + 2x + 1) + x(x^2)(2x + 2)$

$= x^2[1 + x(2x + 2)] - (2x + 2)(x^3 + 2x + 1)$

$1 = x^2(2x^2 + 2x + 1) - (2x + 2)(x^3 + 2x + 1)$

इसी कारण $p(x) = 2x^2 + 2x + 1$ तथा इस प्रकार $x^2 + I$ में $\frac{\mathbf{Z}_3[x]}{I}$ का व्युत्क्रम $(2x^2 + 2x + 1) + I$ है।

लैमा: यदि R एक यूएफ़डी है एवं $p(x), R[x]$ में आघक बहुपद है तो इसे $R[x]$ के अलघुकरणीय अवयवों के गुणन के रूप में अद्वितीय रीति में खंडित (Factored) किया जा सकता है।

प्रमाण: K को R की भागफलों के क्षेत्र मानें तो $K[x]$ एक युक्लिडीन डोमेन है एवं इसी कारण पीआईडी (PID) है एवं इस प्रकार एक यूएफ़डी (UFD) है।

अब $p(x) \in R[x] \Rightarrow p(x) \in K[x]$ एवं चूँकि $K[x]$ एक यूएफ़डी है जो हम $p(x) = p_1(x)\, p_2(x) \ldots\ldots p_k(x)$ व्यक्त कर सकते हैं।

$p_i(x)$ के अलघुकरणीय अवयवों $K[x]$ के गुणन के रूप में।

पुनः $p_i(x) \in K[x] \Rightarrow p_i(x) = \frac{1}{a_i} f_i(x)$

जहाँ $a_i \in R, \quad f_i \in R[x]$

टिप्पणी

चूँकि $p_i(x) \in K[x] \Rightarrow p_i(x) = \alpha_o + \alpha_1 x + \alpha_2 x^2 + ...$

जहाँ $\alpha_i \in K$ जो R की भागफलों के क्षेत्र है जिसका तात्पर्य हुआ कि α_i को $\frac{b_i}{a_i}$ $a_i, b_i \in R, a_i \neq 0$ के रूप में व्यक्त किया जा सकता है।

अथवा $p_i(x) = \frac{b_o}{a_o} + \frac{b_1}{a_1} x + \frac{b_2}{a_2} x^2 + ...$

$= \frac{1}{a} [c_o + c_1 x + c_2 x^2 + ...] = \frac{1}{a} f(x), \quad f \in R[x]$

पुनः $p_i(x)$, $K[x]$ में अलघुकरणीय अवयव है।

$f_i(x)$, $p_i = \frac{d_i}{a_i} f_i^*$ में अलघुकरणीय अवयव होगा क्योंकि यदि यह ऐसा न होता तो हम इसे $K[x]$ के रूप में लिख सकते जहाँ g_i, h_i गैर–इकाई हैं।

$f_i = g_i h_i$ जहाँ g_i, h_i गैर–इकाई हैं।

$\Rightarrow p_i$ अलघुकरणीय अवयव नहीं है।

पुनः $f_1(x) \in R[x] \Rightarrow f_i = d_i f_i^*(x)$ जहाँ $f_i^*(x)$ आघक है एवं $d_i = c(f_i)$

$\therefore \qquad p_i = \frac{d_i}{a_i} f_i^*, \; i = 1, 2, ..., k$

$\Rightarrow p_1 p_2 ..... p_k = \frac{d_1 d_2 ... d_k}{a_1 a_2 ... a_k} f_1^* f_2^* ..... f_k^*$

$\Rightarrow p = \frac{d_1 d_2 ... d_k}{a_1 a_2 ... a_k} f_1^* f_2^* ..... f_k^*$

$\Rightarrow (a_1 a_2 ..... a_k) p = (d_1 d_2 ..... d_k)(f_1^* f_2^* ..... f_k^*)$ ...(i)

अब चूँकि $p_i = \frac{d_i}{a_i} f_i^*$ व p_i अलघुकरणीय अवयव है अतः हम पाते हैं कि f_i^* भी $K[x]$ का अलघुकरणीय अवयव होगा, अन्यथा p_i अलघुकरणीय अवयव नहीं रह जायेगा (जैसा कि पूर्व में देखा गया)।

समीकरण (i) के $(a_1 a_2 ..... a_k)$ का अंश (Component) किसी इकाई u हेतु p है क्योंकि R.H.S. आघक है एवं समीकरण (i) के $(d_1 d_2 ..... d_k)$ का अंश किसी इकाई v हेतु f_i^* आघक हैं।

दोनों ओर के अंशों को समीकृत (समीकरणबद्ध) करते हुए हम पाते हैं,

$a_1 a_2 ..... a_k = (d_1 d_2 ..... d_k) w$ जहाँ $w = vu^{-1}$ एक इकाई है।

इस प्रकार $p(x) = (w^{-1} f_1^*)(f_2^* f_3^* ..... f_k^*)$

जो कि $K[x]$ में अलघुकरणीय अवयवों का गुणन है। पुनः f_i^* आघक है एवं $K[x]$ में अलघुकरणीय अवयव हैं, हम पाते हैं कि f_i^*, $R[x]$ में अलघुकरणीय अवयव होंगे। अद्वितीयता (Uniqueness) दर्शाने के लिये, मान लेते हैं कि $p(x) = r_1(x) r_2(x) ..... r_k(x)$ जहाँ $r_i(x)$, $R[x]$ में अलघुकरणीय नहीं हैं।

(**ध्यान दे**: गुणन में अवयवों की संख्या k के समान रहती है जो हमारे पास UFD में हैं।)

टिप्पणी

अब $p(x)$ आघक है $\Rightarrow$ प्रत्येक r_i आघक है।

क्योंकि $p = r_1 r_2 \ldots . r_k \Rightarrow c(p) = c(a_1)\, c(a_2) \ldots . c(a_k)$

$\Rightarrow \quad d = d_1 d_2 \ldots . d_k$

$\Rightarrow$ प्रत्येक d_i एक ईकाई है।

$\Rightarrow$ प्रत्येक a_i आघक है।

इसी कारण प्रत्येक a_i आघक है एवं $R[x]$ में अलघुकरणीय अवयव है।

सभी i के लिए $r_i(x)$ अलघुकरणीय है।

किन्तु $K[x]$ यूएफ़डी होने से प्रत्येक r_i, $K[x]$ में संबद्धता तक अद्वितीयता से निर्धारित होता है।

$\Rightarrow \quad r_i$ और f_i^* सभी i के लिए संबद्धता हैं।

$\Rightarrow \quad r_i = u_i f_i^*$

जहाँ $u_i, K[x]$ में एक ईकाई है एवं इस प्रकार $K \Rightarrow u_i$ में $\frac{a_i}{b_i}$ रूप में है

इसी कारण $r_i = \frac{a_i}{b_i} f_i^*$

$\Rightarrow \quad b_i r_i = a_i f_i^*$

दोनों ओर अंशों को समीकृत करने पर हम पाते हैं कि R में किसी ईकाई u के लिये $b_i = u a_i$ अथवा $\frac{a_i}{b_i} = u^{-1}$ में R ईकाई अथवा $r_i, R[x]$ में f_i^* का संबद्धता है।

प्रमेय 5.46: R एक यूएफ़डी है $\Rightarrow R[x]$ एक यूएफ़डी है।

प्रमाण: माना कि $f \in R[x]$ को अशून्य, गैर–ईकाई अवयव हैं।

$f = d f^*(x)$ मानें जहाँ $d = c(f)$, f^* आघक है।

लैमा $f^* = f_1^* f_2^* \ldots . f_x^*$ अनुसार जहाँ $f_i^*, R[x]$ के अलघुकरणीय अवयव हैं एवं यह निरूपण संबद्धता तक अद्वितीय है।

$d \in R$ भी व R यूएफ़डी है, इस प्रकार या तो d एक ईकाई है अथवा इसे इस प्रकार लिखा जा सकता है,

$d = d_1 d_2 \ldots . d_r$

जहाँ d_i, R में अलघुकरणीय अवयव हैं।

यदि d ईकाई हो

$f = d f^*$ से मिलता है कि,

$f = (d f_1^*) f_2^* \ldots . f_k^*, \quad d f_1^*, f_2^*, \ldots . f_x^*$ अलघुकरणीय हैं।

टिप्पणी

जिससे हमें परिणाम प्राप्त होता है।

यदि d ईकाई न हो तो मान लें कि $d = d_1 d_2 \ldots . d_r$

चूँकि प्रत्येक d_i, R का अलघुकरणीय अवयव है, प्रत्येक $d_i, R[x]$ का अलघुकरणीय अवयव होगा, इस प्रकार $f, R[x]$ में अलघुकरणीय अवयवों का परिमित गुणन है एवं निरूपण संबद्धता तक अद्वितीय है जिससे हमारा प्रमेय सिद्ध हो रहा है।

ध्यान दे: $a, b \in R$ में संबद्धता हैं यदि $a, b, R[x]$ में संबद्धता हैं। यह परिणाम आता है क्योंकि R व $R[x]$ की इकाईयां समान हैं।

F एक क्षेत्र मानें। आपने पहले ही देखा है कि $F[x, y]$ पीआईडी नहीं है।

अब F के क्षेत्र होने से यह यूएफ़डी है एवं इसीलिये पूर्ववर्ती प्रमेय अनुसार $F[x, y]$ यूएफ़डी होगा। इस प्रकार $F[x, y]$ यूएफ़डी (UFD) का एक उदाहरण है जो कि पीआईडी (PID) नहीं है।

$\mathbf{Z}$ पीआईडी है एवं इस प्रकार $\Rightarrow \mathbf{Z}[x]$ यूएफ़डी है।

परन्तु $\mathbf{Z}[x]$ पीआईडी नहीं है, अन्यथा $\mathbf{Z}$ को क्षेत्र होना होता जो कि है नहीं तथा इसी कारण $\mathbf{Z}[x]$ एक यूएफ़डी है किन्तु पीआईडी नहीं है।

प्रमेय 5.47: R को यूएफ़डी मानें एवं $f(x) \in R[x]$ को आघक बहुपद। यदि $f(x), K[x]$ का अलघुकरणीय अवयव हो तो $f(x), R[x]$ का अलघुकरणीय अवयव है।

प्रमाण: मान लें कि $f(x), R[x]$ का अलघुकरणीय अवयव नहीं है।

तो $f = gh, \quad g, h \in R[x]$ गैर–ईकाइयाँ हैं।

हम यह भी लिख सकते हैं, $g = dg^*(x)$

$h = d'h^*(x)$ जहाँ g^* व h^* आघक हैं।

$\Rightarrow \quad f = dd'g^*h^*$

दोनों ओर अंशों को समीकृत करते हुए हम पाते हैं कि $u = dd'vw$

क्योंकि f आघक है व इसलिये g^*, h^* हैं।

जहाँ u, v, w ईकाइयाँ हैं।

इस प्रकार $1 = dd'vwu^{-1}$

$\Rightarrow \quad d$ ईकाई है।

इसी प्रकार d' एक ईकाई है।

$\Rightarrow \quad g = dg*$

$\Rightarrow \quad c(g) = c(dg^*) = dc(g^*) =$ इकाई $\times$ इकाई $=$ इकाई।

$\Rightarrow \quad g$ आघक है।

h आघक है।

पुनः $g, h \in R[x] \Rightarrow g, h \in K[x]$

अब $f = gh, K[x]$ का अलघुकरणीय अवयव f है।

g अथवा $h, K[x]$ की ईकाई है।

व्यापकता की हानि हुए बिना मान लेते हैं कि $g, K[x]$ में ईकाई है।

तो $\exists\ r \in K[x]$ इस प्रकार है कि $gr = 1$

$\Rightarrow \deg g + \deg r = 0$

$\Rightarrow \deg g = \deg r = 0$

$\Rightarrow g, r \in K$

मान लें $g = \frac{\alpha}{\beta}, \quad \alpha, \beta \in R$

तो $f = \frac{\alpha}{\beta} h$ अथवा $\beta f = \alpha h$

$\Rightarrow c(\beta f) = c(\alpha h)$

$\Rightarrow \beta u = \alpha v,$ u, v ईकाइयाँ होने से (f, g आघक हैं)

$\Rightarrow \frac{\alpha}{\beta} = uv'$

$\Rightarrow g = \frac{\alpha}{\beta} = uv' = R$ में ईकाई है।

$g, R[x]$ में एक ईकाई है।

विरोधाभास से हमें परिणाम प्राप्त होता है।

हम अब निम्नांकित प्रमेय में विपरीत को सिद्ध करते हैं।

प्रमेय 5.48: यदि $f(x) \in R[x]$ आघक है एवं $R[x]$ का अलघुकरणीय अवयव भी तो $f(x)$, $K[x]$ का अलघुकरणीय अवयव है।

प्रमाण: मान लेते हैं कि $f(x)$, $K[x]$ का अलघुकरणीय अवयव नहीं है।

तो $f = gh$ जहाँ $f, g, K[x]$ में गैर–इकाइयाँ हैं।

इस प्रकार f, g, K की गैर–इकाइयाँ हैं।

अर्थात् $f, g \notin K$

ध्यान दें: यदि $g \in K$ तो चूँकि $g \neq 0$, अवयवों के क्षेत्र होने से इसमें गुणात्मक व्युत्क्रम होगा एवं इसी कारण ईकाई होगी।

इस प्रकार $\deg g, \quad \deg h > 0$

अब $g(x) = \frac{1}{d}\ g_o(x)$

$\Rightarrow \quad g_o(x) = dg(x) \in R[x]$

इसी प्रकार $h_o(x) = d'h(x) \in R[x]$

पुनः $g_o(x) = \alpha g^*(x)$

$h_o(x) = \beta h^*(x)$ जहाँ g^*, h^* आघक हैं।

तथा α, β, g_o व h_o के गुणांकों के महत्तम उभयनिष्ठ भाजक हैं।

टिप्पणी

टिप्पणी

$\therefore \quad c(g_o) = \alpha,\ c(h_o) = \beta$

$\therefore \quad f(x) = \frac{1}{dd'}\ \alpha\beta g^* h^*$

$\Rightarrow \quad dd'f = \alpha\beta\, g^* h^*$

चूँकि g^*, h^* आघक हैं, गॉस लैमा के अनुसार $g^* h^*$ आघक होगा।

$\Rightarrow \quad c(dd'f) = c(\alpha\beta\, g^* h^*) = \alpha\beta$

$\Rightarrow \quad dd' = u\alpha\beta$ क्योंकि f आघक है।

$\Rightarrow \quad f(x) = u^{-1}g^*(x)\ h^*(x), \qquad g^*, h^* \in R[x],\ u \in R$

$\deg u^{-1}g^* = \deg g^* = \deg \alpha g^*$

$= \deg g_0 = \deg \frac{1}{d} g_0 = \deg g > 0$ भी।

अतः $\deg h^* = \deg h > 0$, $u^{-1}g^*, h^*, R[x]$ में गैर–इकाइयाँ हैं।

ध्यान दें: $\deg h^* > 0 \Rightarrow h^*, R$ का अवयव नहीं है।

अर्थात् h^*, R की ईकाई नहीं हो सकता एवं इसीलिये $R[x]$ की ईकाई है।

इसी कारण $f = (u^{-1}g^*)\ h^*$

जहाँ $u^{-1}g^*$ और h^*, $R[x]$ में गैर–इकाइयाँ है।

f, $R[x]$ में अलघुकरणीय नहीं है जो कि एक विरोधाभास है जिससे हमारा परिणाम सिद्ध हो रहा है।

उदाहरण 5.49: $\mathbf{Z}[x]$ में g.c.d.$(2, x)$ ज्ञात करें एवं दर्शायें कि इसे किसी $r(x), s(x) \in \mathbf{Z}[x]$ हेतु $2r(x) + xs(x)$ रूप में नहीं रखा जा सकता।

हल: हमारे पास हैं,

$2 = 2 + 0.x + 0.x^2 + ...$

$x = 0 + 1.x + 0.x^2 + ...$

अब $1 \mid 2$ व $1 \mid x$ परिभाषानुसार स्पष्ट हैं क्योंकि '1' ईकाई है।

मान लें कि $f \mid 2$ व $f \mid x$। हम दर्शाते हैं कि $f \mid 1$

अब किसी भी g के लिए $f \mid 2 \Rightarrow 2 = fg$ है।

$\Rightarrow \deg 2 = \deg f + \deg g$

$\Rightarrow 0 = \deg f + \deg g$

$\Rightarrow \deg f = 0$ अथवा f एक अचर बहुपद है।

मान लेते हैं कि $f = a_o + 0.x + 0.x^2 + ...$

पुनः $f \mid x \quad \Rightarrow a_o \mid x \Rightarrow x = a_o h(x)$

इस प्रकार $\deg x = 0 + \deg h$ जिससे मिलता है $\deg h = 1$

मान लें कि $h(x) = b_o + b_1 x + 0\ .\ x^2 + 0\ .\ x^3 + ...$

तो $x = a_o h = a_o(b_o + b_1 x) = a_o b_o + a_o b_1 x$

$\Rightarrow 1 = a_o b_1 = f(x)\ b_1$

अथवा $f \mid 1$

इसी कारण $1 = \text{G.C.D.}(2, x)$

कोई अन्य G.C.D.$(2, x)$ 1 का संबद्ध होगा। इस प्रकार 1, −1, '2' के x हैं एवं $\mathbf{Z}[x]$ में हैं (स्मरण करें कि $\mathbf{Z}$ व $\mathbf{Z}[x]$ की इकाइयाँ समान हैं एवं ईकाई का संबद्ध भी ईकाई होगा)।

टिप्पणी

अब मान लें कि किसी भी महत्तम उभयनिष्ट भाजक $(2, x)$ को $f = 2r + xs$ के रूप में व्यक्त करना सम्भव है तो,

$1 = (2r + xs)\ b_1 = 2b_1\ (c_o + c_1x + c_2x^2 + ...) + b_1xs(x)$

जहाँ $\quad r(x) = c_o + c_1x + c_2x^2 + ...$

अर्थात् $1 = 2b_1c_o$ में यह दर्शाया जा रहा है कि '2', $\mathbf{Z}$ में ईकाई है जो कि वास्तविक नहीं। इसी कारण ऐसा परिणाम आया।

ध्यान दें: $\mathbf{Z}[x]$ एक यूएफ़डी है परन्तु पीआईडी नहीं है।

हम अब परिमेयों की वलय $\mathbf{Q}$ पर $\mathbf{Z}[x]$ में बहुपद की अलघुकरणीयता के लिये एक परीक्षण करते हैं।

आईसेण्टीन की मापदंड (Eisenstein's Criterion)

प्रमेय 5.49 (आईसेण्टीन–मापदंड): मान लें कि $f(x) = a_o + a_1x + a_2x^2 + ... + a_nx^n$ पूर्णांक गुणांकों ($f(x) \in \mathbf{Z}[x]$) वाला एक एक बहुपद है। मान लें कि किसी अभाज्य संख्या p के लिये,

$p \mid a_o,\ p \mid a_1,\ p \mid a_2\ ...,\ p \mid a_{n-1},\ p \nmid a_n,\ p^2 \nmid a_o$

तो $f(x)$ परिमेयों की वलय $\mathbf{Q}$ पर अलघुकरणीय बहुपद है।

हम सर्वप्रथम सिद्ध कर लेते हैं।

लैमा (Lemma): यदि $f(x) \in \mathbf{Z}[x]$ आघक है एवं $f(x)$, $\mathbf{Z}$ कृ पर अलघुकरणीय हो तो f, $\mathbf{Q}$ पर अलघुकरणीय है।

प्रमाण: मान लेते हैं कि f, $\mathbf{Q}$ पर अलघुकरणीय नहीं है तो हम लिख सकते हैं कि $f = gh,\quad g, h \in \mathbf{Q}[x]$ युक्त $\deg g, \deg h > 0$

तो $g(x) \in \mathbf{Q}[x] \Rightarrow g = \frac{1}{\alpha} g_1(x)$ जहाँ $g_1(x) \in \mathbf{Z}[x]$

$h(x) \in \mathbf{Q}[x] \Rightarrow h = \frac{1}{\beta} h_1(x)$ जहाँ $h_1(x) \in \mathbf{Z}[x]$

(उदाहरणार्थ यदि $g(x) = \frac{2}{3}x^2 + \frac{1}{2}x + 1 \in \mathbf{Q}[x]$ तो $g(x) = \frac{1}{6}(4x^2 + 3x + 6)$ जहाँ तो $g_1(x) = 4x^2 + 3x + 6 \in \mathbf{Z}[x]$)।

पुनः $g_1(x) \in \mathbf{Z}[x] \Rightarrow g_1 = dg_1^*$ जहाँ g_1^* आघक है।

$h_1(x) \in \mathbf{Z}[x] \Rightarrow h_1 = d'h_1^*$ जहाँ h_1^* आघक है।

टिप्पणी

इस प्रकार $f = gh = \frac{1}{\alpha\beta}\ dd' g_1^* h_1^*$

$\Rightarrow \quad \alpha\beta f = dd' g_1^* h_1^*$

$\Rightarrow \quad c(\alpha\beta f) = c(dd' g_1^* h_1^*)$

चूँकि $f, \mathbf{Z}[x]$ में आघक बहुपद है, इसका अंश $\mathbf{Z}$ में एक ईकाई है एवं चूँकि $\mathbf{Z}$ में इकाइयाँ '1' अथवा -1 $c(f) = \pm 1$ हैं। इसी प्रकार $c(g_1^*), c(h_1^*), \pm 1$ हो सकती है।

दोनों ओर अंशों को समीकृत करने पर हम पाते हैं,

$\pm\alpha\beta = \pm dd'$

अर्थात् $\alpha\beta = \pm dd'$

तथा इसी कारण समीकरण $\alpha\beta f = dd' g_1^* h_1^*, f = \pm g_1^* h_1^*$ में घट (Reduce) हो जाता है।

अब $\deg(\pm g_1^*) = \deg g_1^* = \deg d g_1^* = \deg g_1$

$= \deg \frac{1}{\alpha} g_1 = \deg g > 0$

इसी प्रकार $\deg(h_1^*) > 0$

इस प्रकार हम $f = \pm g_1^* h_1^*$ लिख सकते हैं जहाँ $\pm g_1^*, h_1^*, \mathbf{Z}[x]$ में बहुपद हैं एवं इनमें धनात्मक श्रेणी है।

$\Rightarrow f, \mathbf{Z}$ पर परिवर्तक (Reducible) है जो कि एक विरोधाभास है।

इसी कारण लैमा सिद्ध हुआ।

हम अब प्रमुख प्रमेय के प्रमाण की ओर आते हैं।

हम दर्शाते हैं कि $f, \mathbf{Z}$ पर अलघुकरणीय है।

मान लेते हैं कि यह $\mathbf{Z}$ पर अलघुकरणीय न हो तो $\exists\, g, h \in \mathbf{Z}[x]$ इस प्रकार होगा कि $f = gh$ सहित $\deg g, \deg h > 0$

मान लें कि $g(x) \quad = b_o + b_1 x + ... + b_s x^s$

$h(x) = c_o + c_1 x + ... + c_t x^t$

तो $g(x)\, h(x) = b_o c_o + (b_1 c_o + b_o c_1) x + ...$

अतः $f = gh$

$\Rightarrow \quad a_o + a_1 x + ... = b_o c_o + (b_1 c_o + b_o c_1)\, x + ...$

$\Rightarrow \quad a_o = b_o c_o$

अब $p \mid a_o \Rightarrow p \mid b_o c_o \Rightarrow p \mid b_o$ or $p \mid c_o$ क्योंकि p अभाज्य है।

मान लेते हैं कि $p \mid b_0$ तो $p \nmid c_0$ क्योंकि $p^2 \nmid a_o$

$[p \mid b_0, p \mid c_0 \Rightarrow p^2 \mid b_0 c_0 \Rightarrow p^2 \mid a_0]$

पुनः p सभी $b_0, b_1, b_2, ..., b_s$ को विभाजित नहीं कर सकता क्योंकि यदि ऐसा होता तो p इस प्रकार के प्रत्येक पदों को विभाजित करता है।

$b_0c_0,\ b_1c_0 + b_0c_1,\ .....$

अर्थात् p समस्त $a_0, a_1, ..., a_n$ को विभाजित करता है।

किन्तु $p \nmid a_n$

मान लेते हैं कि k सबसे छोटा पूर्णांक है कि $p \nmid b_k, k \le s < n$

अतः $p \mid b_0, p \mid b_1, ..., p \mid b_{k-1}, p \nmid b_k$

अब $a_k = b_kc_0 + b_{k-1}c_1 + ... + b_oc_k$

$p \mid a_k$ दिए गए $k < n$ के अनुसार है।

$p \mid (b_{k-1}c_1 + b_{k-2}c_2 + ... + b_0c_k)$

$\Rightarrow\ p \mid b_kc_0 \Rightarrow p \mid b_k$ or $p \mid c_0$ भी

उक्त दोनों से विरोधाभास आता है। इसी कारण $f(x), \mathbf{Z}$ पर अलघुकरणीय है।

यदि $f(x)$ आघक हो तो यह लैमा द्वारा $\mathbf{Q}$ पर अलघुकरणीय होगा। यदि $f(x)$ आघक न हो तो हम $f = df_1$ लिख सकते हैं जहाँ f_1 आघक है एवं $d = c(f)$

तो $f, \mathbf{Z}$ पर अलघुकरणीय है, $\mathbf{Z} \Rightarrow df_1, \mathbf{Z}$ पर अलघुकरणीय है।

$f_1, \mathbf{Z}$ पर अलघुकरणीय है।

$f_1, \mathbf{Q}$ पर अलघुकरणीय है (क्योंकि f_1 आधक है)।

$df_1, \mathbf{Q}$ पर अलघुकरणीय है।

$f, \mathbf{Q}$ पर अलघुकरणीय है।

इसी कारण प्रमेय सिद्ध हुआ।

ध्यान दें: चूँकि $f(x) = g(x)h(x) \Leftrightarrow f(x+1) = g(x+1)\ h(x+1)$।

हम पाते हैं कि $f(x)$ परिवर्तक योग्य (Reducible) (अलघुकरणीय या Irreducible) होगा यदि $f(x+1)$ परिवर्तक योग्य (अलघुकरणीय) हो। वस्तुतः 1 के स्थान पर कोई भी पूर्णांक लिया जा सकता है।

उदाहरण हेतु बहुपद $x^2 - 4x + 2, \mathbf{Q}$ पर अलघुकरणीय है क्योंकि यदि हम $p = 2$ मानें तो $p \mid 4, p \mid 2, p \nmid 1, p^2 \nmid 2$।

पुनः बहुपद $x^2 + 1 = f(x)$ का विचार करें।

चूँकि ऐसा कोई अभाज्य p नहीं है जो 1 को विभाजित करे, अतः हम आईसेण्टीन मापदंड को $f(x)$ पर लागू नहीं कर सकते।

$f(x+1) = (x+1)^2 + 1$

$= x^2 + 2x + 2$ $(a_o = 2, a_1 = 2, a_2 = 1)$ का विचार करें।

मान लें कि $p = 2$, तो $p \mid 2, p \nmid 1, p^2 \nmid 2$

टिप्पणी

टिप्पणी

इसी कारण $f(x+1)$ अलघुकरणीय है।

$\Rightarrow f(x)$ अलघुकरणीय है (पूर्ववर्ती टिप्पणियों (Remarks) के प्रयोग से)।

पुनः मान लें कि $f(x) = x^3 + x^2 - 2x - 1$

चूँकि ऐसा कोई अभाज्य नहीं है जो 1 को विभाजित करे अतः हम इस मापदंड को यहाँ प्रयोग नहीं कर सकते।

$f(x+1) = (x+1)^3 + (x+1)^2 - 2(x+1) - 1$

$= x^3 + 4x^2 + 3x - 1$ का विचार करें।

हमारे पास वही परिस्थिति है। आइए, विचार करें,

$f(x-1) = (x-1)^3 + (x-1)^2 - 2(x-1) - 1$

$= x^3 - 2x^2 - x - 1$

पुनः मापदंड को प्रयोग करना सम्भव नहीं हैं।

$f(x+2) = x^3 + 7x^2 + 14x + 7$ का विचार करें,

तो $p = 7$ यहाँ होगा क्योंकि यहाँ $a_0 = 7, a_1 = 14, a_2 = 7, a_3 = 1$ एवं $7 \mid 7$, $7 \mid 14$, $7 \mid 7$, $7 \nmid 1$, $7^2 \nmid 7$।

इस प्रकार मापदंड के अनुसार $f(x+2)$ हैं एवं इसीलिये $f(x)$ अलघुकरणीय है।

ध्यान दे: स्मरण रहे कि आईसेण्टीन की मापदंड बहुपदों की अलघुकरणीयता हेतु आवश्यक नहीं क्योंकि आप देख चुके हैं कि कोई अभाज्य p इस प्रकार विद्यमान् नहीं है कि $p \mid 1$ (भले ही बहुपद अलघुकरणीय हो सकता हो)। $x^3 - x + 1$, $\mathbf{Q}$ पर अलघुकरणीय है परन्तु यहां आईसेण्टीन मापदंड का प्रयोग नहीं हो सकता है।

बहुपद $f(x) = x^3 - x + 1$, $\mathbf{Q}$ पर अलघुकरणीय है क्योंकि मान लें कि यह परिवर्तक योग्य हो तो इसमें $\mathbf{Q}$ मूल (Root) है।

मान लें कि $\frac{m}{n}$ पूर्णांक $m, n, n \neq 0, (m, n) = 1$ मूल (Root) है।

तो $\frac{m^3}{n^3} - \frac{m}{m} + 1 = 0$

$\Rightarrow m^3 - mn^2 + n^3 = 0$

$\Rightarrow m^3 = n^2 (m - n)$

$\Rightarrow n^2 \mid m^3 \Rightarrow n \mid m^3 . 1 \Rightarrow n \mid 1$ as $(m, n) = 1$

$\Rightarrow n = \pm 1$

$\Rightarrow \frac{m}{n} = \pm m$

अथवा $m^3 - m + 1 = 0$

$\Rightarrow m(m^2 - 1) = -1$

$\Rightarrow m \mid 1$ अथवा $m = \pm 1$

$\Rightarrow \quad \frac{m}{n} = \pm 1, 1 - 1 + 1 = 0$ जिससे $x^3 - x + 1$ मिलता है जो कि सम्भव नहीं है।

इसी कारण $x^3 - x + 1, \mathbf{Q}$ पर परिवर्तक योग्य नहीं है।

टिप्पणी

उदाहरण 5.50: किसी अभाज्य p के लिये दर्शायें कि बहुपद $x^{p-1} + x^{p-2} + ... + x^2 + x + 1$ पर अलघुकरणीय है।

हल: मान लें कि $f(x) = x^{p-1} + x^{p-2} + ... + x^2 + x + 1$

$= \frac{x^p - 1}{x - 1}$ (G.P. का योगफल)

अब $f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + p_{c_1} x^{p-1} + ... + p_{c_r} x^{p-2} + ... + p_{c_p} - 1}{x}$

$= \frac{x^p + p_{c_1} x^{p-1} + ... + p_{c_{p-1}} x}{x}$

$= x^{p-1} + p_{c_1} x^{p-2} + ... + p_{c_{p-1}}$

चूँकि p एक अभाज्य संख्या है, सभी $1 \le r \le p-1$ के लिए $p \mid p_{c_r}$।

$p_{c_{p-1}} = p$ अथवा $p^2 \nmid p_{c_{p-1}}$ भी

इसी कारण आईसेण्टीन मापदंड से $f(x+1)$ एवं इसीलिये $f(x)$ अलघुकरणीय है।

अपनी प्रगति जांचिए

10. सोदाहरण दर्शाये कि युक्लिडीन डोमेन में a व b इन दो अवयवों को इस प्रकार ज्ञात करना सम्भव है कि $d(a) = d(b)$ परन्तु a, b संबद्ध नहीं हैं।
11. अद्वितीय गुणनखंड डोमेन से आपका क्या अभिप्राय है?
12. आईसेण्टीन मापदंड क्या है?

5.8 अपनी प्रगति जांचिए प्रश्नों के उत्तर

1. चूँकि $i = 0 + 1i + 0j + 0k$ से $j = 0 + 0i + 1j + 0k$ मिलता है, अतः हम पाते हैं कि D क्रमविनिमेय नहीं है एवं इसी कारण क्षेत्र नहीं है। D में ईकाई $1 = 1$ है।

   यदि $a + bi + cj + dk, D$ का कोई अशून्य अवयव हो (अर्थात् a, b, c, d के कम से कम एक पर अशून्य हो) तो $(a + bi + cj + dk)\frac{(a - bi - cj - dk)}{a^2 + b^2\ c^2 + d^2} = 1$

   इसी कारण D विभक्त वलय है परन्तु क्षेत्र नहीं है।

2. वलय R में अवयव e को महत्वपूर्ण कहा जाता है। यदि $e^2 = e$

टिप्पणी

3. मानचित्रण $\theta : R \to R'$ को समरूपता कहा जाता है यदि

$$\theta(a+b) = \theta(a) * \theta(b)$$
$$\theta(ab) = \theta(a)\ o\ \theta(b) \qquad a, b \in R$$

4. हमें विदित है कि $\mathbf{Z}_{30} \cong \frac{\mathbf{Z}}{(30)}$ एवं चूँकि $30 = 2 \times 3 \times 5$ वर्गमुक्त है, अतः $\frac{\mathbf{Z}}{(30)}$ अथवा $\mathbf{Z}_{30}$ में अशून्य महत्वपूर्ण अवयव नहीं हैं।

5. चूँकि $A \subseteq R$ सदा है, अतः हमें यह दर्शाने की आवश्यकता है कि $R \subseteq A$।

मान लेते हैं कि $r \in R$ कोई अवयव है।

चूँकि $1 \in A$ एवं A एक आदर्श है,

$r = 1 \,.\, r \in A$

$\Rightarrow \ R \subseteq A$ अथवा $A = R$

6. मान लेते हैं कि R एक विभक्त वलय है। A, R का कोई आदर्श इस प्रकार हो कि $A \neq \{0\}$ तो $\exists$ कम से कम $a \in A$ इस प्रकार है कि $a \neq 0$। R विभक्त वलय होने से $a^{-1} \in R$ व $aa^{-1} = 1$ है।

चूँकि $a \in A, a^{-1} \in R, aa^{-1} \in A$ (आदर्श की परिभाषा के अनुसार)।

$\Rightarrow 1 \in A$

$\Rightarrow A = R$

अर्थात् जिन आदर्शों में R हो सकता है वे R व $\{0\}$ ही हैं अथवा R एक सरल वलय है।

7. भागफल वलय समस्त समतुल्यता वर्गों की वलय है।

8. $(x+2) + I \in \frac{\mathbf{Z}_3[x]}{I}$ एवं $((x+2)+I)^2 = (x+2)^2 + I = (x^2 + 1.x + 1) + I$

का परन्तु $(x+2) + I$, $\frac{\mathbf{Z}_3[x]}{I}$ का शून्य नहीं है।

इसी कारण $\frac{\mathbf{Z}_3[x]}{I}$ जहाँ $I = < x^2 + x + 1 >$ एक समाकलित डोमेन नहीं है।

9. यदि $R[x]$ एक पीआईडी है तो R एक क्षेत्र है।

इसके विपरीत R को एक क्षेत्र मानें तो $R[x]$ एक युक्लिडीन डोमेन है।

$\Rightarrow \ R[x]$ एक पीआईडी है।

उपरोक्त प्रमेय को निम्नानुसार पुनर्कथित किया जा सकता है:

यदि R इकाईयुक्त एक समाकलित डोमेन हो जो कि क्षेत्र नहीं है तो $R[x]$ एक पीआईडी नहीं है।

10. $D = \{a + ib \mid a, b \in \mathbf{Z}\} = \mathbf{Z}[i]$ का विचार करें जो कि गॉसियन पूर्णांकों की वलय है जहाँ $d(a+ib) = a^2 + b^2$ तो D एक युक्लिडीन डोमेन है।

यहाँ $d(2+i3) = 13 = d(2-3i)$ परन्तु $2+3i$ व $2-3i$ संबद्ध नहीं हैं।

ध्यान दें: D की इकाइयाँ $\pm 1, \pm i$ हैं एवं इस प्रकार $2+3i$ का संबद्ध $(2+3i)1$, $(2+3i)(-1), (2+3i)i, (2+3i)(-i)$ हो सकता है,

अर्थात् $2+3i, -2-3i, 2i-3, 3-2i$

टिप्पणी

11. R को ईकाई युक्त समाकलित डोमेन मान लें तो R को अद्वितीय गुणनखंड डोमेन कहा जाता है यदि:

    (i) R के प्रत्येक अशून्य, गैर–ईकाई अवयव a को R के अलघुकरणीय अवयवों की परिमित संख्या के गुणन में रूप में व्यक्त किया जा सकता है।

    (ii) यदि $a = p_1 p_2 \ldots\ldots p_m$
    $a = q_1 q_2 \ldots\ldots q_n$

    जहाँ p_i व q_j, R में अलघुकरणीय हों तो $m = n$ एवं प्रत्येक p_i किसी q_j का संबद्ध है।

12. आईसेण्टीन मापदंड इस प्रकार है,

    मान लें कि $f(x) = a_o + a_1 x + a_2 x^2 + \ldots\ldots + a_n x^n$ पूर्णांक गुणांकों युक्त बहुपद है (अर्थात् $f(x) \in \mathbf{Z}[x]$)। मान लें कि किसी अभाज्य संख्या p के लिये,
    $p \mid a_o,\ p \mid a_1,\ p \mid a_2 \ldots, p \mid a_{n-1},\ p \nmid a_n,\ p^2 \nmid a_o$
    तो $f(x)$, $\mathbf{Q}$ (परिमेयों की वलय) पर अलघुकरणीय बहुपद है।

5.9 सारांश

- समूह ऐसी प्रणाली है जिसमें एक गैर–रिक्त समुच्चय व द्विआधारी संरचना होती है।
- दो द्विआधारी संरचना + व . के साथ एक गैर–रिक्त समुच्चय R से वलय का निर्माण होता माना जाता है यदि निम्नांकित अभिगृहीत की पूर्ति हो रही हो:
    1. सभी $a, b, c \in R$ के लिए $a + (b + c) = (a + b) + c$
    2. $a, b \in R$ के लिए $a + b = b + a$
    3. R में $\exists$ कोई अवयव 0 (शून्य कहलाने वाला) इस प्रकार कि सभी $a \in R$ के लिए $a + 0 = 0 + a = a$
    4. प्रत्येक $a \in R$, के लिए $\exists$ अवयव $(-a) \in R$ इस प्रकार कि $a + (-a) = (-a) + a = 0$
    5. सभी $a, b, c \in R$ के लिए $a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$
    6. सभी $a, b, c \in R$ के लिए $a \,.\, (b + c) = a \,.\, b + a \,.\, c$

       $(b + c) \,.\, a = b \,.\, a + c \,.\, a$
- वलय R को क्रमविनिमेय वलय कहा जाता है यदि सभी $a, b \in R$ के लिए $ab = ba$। पुनः यदि $\exists$ अवयव $e \in R$ इस प्रकार है कि समस्त $a \in R$ हेतु $ae = ea = a$

टिप्पणी

- मान लें कि $\mathbf{Z}$ पूर्णांकों का समुच्चय हो तो $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$ से सम्मिश्रण संख्याओं $a + ib$ के सामान्य योग व गुणन के अधीन वलय का निर्माण होता है जहाँ $a, b \in \mathbf{Z}$ को गुआसियान पूर्णांक कहा जाता है एवं $\mathbf{Z}[i]$ को गॉसियन पूर्णांकों की वलय कहते हैं।
- R को वलय मान लेते हैं। अवयव $0 \neq a \in R$ को शून्य भाजक कहा जाता है यदि $\exists$ अवयव $0 \neq b \in R$ इस प्रकार है कि $ab = 0$ अथवा $ba = 0$।
- क्रमविनिमेय वलय R को समाकलित डोमेन कहा जाता है यदि $ab = 0$ में $R \Rightarrow a = 0$ अथवा $b = 0$। अन्य शब्दों में क्रमविनिमेय वलय R को समाकलित डोमेन कहा जाता है यदि R में शून्य भाजक न हों।
- समाकलित डोमेन का स्पष्ट उदाहरण पूर्णांकों की वलय $< \mathbf{Z}, +, \cdot >$ है जबकि आव्यूहों के वलय उस वलय का उदाहरण है जो कि समाकलित डोमेन नहीं है।
- ईकाई युक्त वलय R में अवयव a को गुणन के सन्दर्भ में व्युत्क्रम (अथवा ईकाई) कहा जाता है यदि $\exists$ कोई $b \in R$ इस प्रकार हो कि $ab = 1 = ba$।
- ईकाई युक्त वलय R को विभक्त वलय अथवा तिरछा क्षेत्र कहा जाता है यदि R के अशून्य अवयवों से गुणन के सन्दर्भ में समूह का निर्माण होता हो।
- क्रमविनिमेय विभक्त वलय को क्षेत्र कहा जाता है।
- वास्तविक संख्याओं से क्षेत्र का निर्माण होता है जबकि पूर्णांकों से नहीं, सामान्य योग व गुणन के अधीन।
- क्षेत्र एक समाकलित डोमेन है।

  मान लें कि एक क्षेत्र $< R, +, . >$ है तो R एक क्रमविनिमेय वलय है।
- अशून्य परिमित समाकलित डोमेन एक क्षेत्र है।

  मान लें कि R अशून्य परिमित समाकलित डोमेन है।
- वलय R को बूलियन वलय कहा जाता है यदि सभी $x \in R$ के लिए $x^2 = x$ हो।
- वलय R के गैर–रिक्त उपसमुच्चय S को R की उपवलय कहा जाता है यदि S से R के द्विआधारी रचना के अधीन वलय का निर्माण होता हो।
- पूर्णांकों की वलय $< \mathbf{Z}, +, \cdot >$ वास्तविक संख्याओं की वलय $\mathrm{R}, +, \cdot >$ की उपवलय है।
- यदि R एक वलय हो तो $\{0\}$ व R सदैव R की उपवलय होंगी जिन्हें S के नगण्य उपवलय कहा जाता है।
- वलय R का गैर–रिक्त उपसमुच्चय S, R के उपवलय है यदि $a, b \in S \Rightarrow ab$, $a - b \in S$।
- क्षेत्र F के गैर–रिक्त उपसमुच्चय S को उपक्षेत्र कहा जाता है यदि S से F में संक्रियाओं के अधीन क्षेत्र का निर्माण होता हो। इसी प्रकार हम विभक्त वलय की उपविभक्त वलय को परिभाषित कर सकते हैं।

टिप्पणी

- यह सिद्ध किया जा सकता है कि S, F की उपक्षेत्र होगा यदि $a, b \in S$, $b \neq 0 \Rightarrow a - b, ab^{-1} \in S$
- R को वलय S का उपसमुच्चय मानें तो R युक्त S की सबसे छोटी उपवलय को S द्वारा उत्पन्न उपवलय कहा जाता है।
- R एक वलय हो तो $Z(R)$ = समुच्चय (सभी $r \in R$ के लिए $x \in R \mid xr = rx$) को वलय का केन्द्र कहा जाता है।
- $< \mathbf{Z}, +, . >$ में ईकाई '1' है परन्तु सम पूर्णांकों की इसकी उपवलय $< \mathbf{E}, +, . >$ में ईकाई नहीं होती।
- $< \mathbf{Z}, +, . >$ में वही ईकाई '1' है जो इसकी मूल वलय $< \mathbf{Q}, +, . >$ में है।
- R को कोई वलय मानें। यदि धनात्मक पूर्णांक n इस प्रकार विद्यमान् हो कि सभी $a \in R$ के लिए $na = 0$ तो R को परिमित अभिलक्षण युक्त कहा जाता है एवं ऐसे धनात्मक सबसे छोटे पूर्णांक को R का अभिलक्षण कहते हैं।
- R के अभिलक्षण को R अथवा ch, R से इंगित किया जाता है।
- सम्मिश्रित, वास्तविक, परिमेय संख्याओं, सम पूर्णांकों, पूर्णांकों की वलय, ये सभी ch, 0 की हैं।
- यदि R एक (अशून्य) परिमित वलय है तो $\text{ch}\, R \neq 0$। माना $o(R) = m > 1$ चूँकि $\langle R, + \rangle$ एक समूह $ma = 0 \ \forall \ a \in R$ है। इसी कारण $\text{ch}\, R \neq 0$ है।
- R को ईकाई युक्त वलय मानें। यदि '1' योज्य कोटि n का हो तो $\text{ch}\, R = n$। यदि '1' योज्य अपरिमित कोटि का है तो ch R, 0 है।
- यदि '1' में योग के अधीन अपरिमित कोटि हो तो $\exists, n$ इस प्रकार कि $n \,.\, 1 = 0$ एवं इस प्रकार $\text{ch}\, R = 0$।
- यदि R ईकाई युक्त वलय हो तो R में $n > 0$ है यदि n सबसे छोटा धनात्मक पूर्णांक इस प्रकार हो कि $n \,.\, 1 = 0$।
- यदि D एक समाकलित डोमेन हो तो D का अभिलक्षण या तो शून्य है अथवा अभाज्य संख्या है।
- परिमित क्षेत्र की कोटि किसी अभाज्य p के लिये p^n है।
- ऐसा कोटि युक्त समाकलित डोमेन नहीं हो सकता जो दो सुनिश्चित अभाज्यों द्वारा विभाज्य हो (अर्थात् हमारे पास कोटि n युक्त समाकलित डोमेन नहीं हो सकता जहाँ n को एक से अधिक अभाज्यों के गुणन के रूप में व्यक्त किया जा सकता हो)।
- परिमित समाकलित डोमेन में ch होता है जबकि अपरिमित समाकलित डोमेन परिमित अथवा ch, 0 हो सकता है।

टिप्पणी

- R_1 व R_2 को दो वलय मानें।

  मान लेते हैं कि $R = \{(a, b) \mid a \in R_1, b \in R_2\}$ तो यह सरलता से सत्यापित किया जा सकता है कि R से योग व गुणन के अधीन निम्नपरिभाषित अनुसार वलय का निर्माण होता है,

  $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

  $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$

- मान लें कि $< R, +, \cdot >, < R', *, o >$ दो वलय हों। मानचित्रण $\theta : R \to R'$ को समरूपता कहते हैं यदि,

  $\theta(a + b) = \theta(a) * \theta(b)$

  $\theta(ab) = \theta(a)\ o\ \theta(b) \qquad a, b \in R$

- मान लें कि $f: R \to R'$ समरूपता है, हम f के आधारभूत को इस प्रकार परिभाषित करते हैं,

  $\text{Ker}\, f = \{x \in R \mid f(x) = 0'\}$

  जहाँ $0', R'$ का शून्य है।

- यदि हम मानचित्र $f: \mathbf{Z} \to \mathbf{E}$ का विचार करें जहाँ $\mathbf{E}$ = सम पूर्णांकों की वलय है, $f(x) = 0$ द्वारा परिभाषित अनुसार सभी x के लिए हम पाते हैं कि $\mathbf{E}$ में इकाइयाँ नहीं है जबकि '1' $\mathbf{Z}$ की इकाइयाँ है।

- मानचित्र $f: \mathbf{Z} \to \mathbf{E}$ इस प्रकार है कि $f(x) = 2x$ एक समूह तुल्याकारिता है। इस प्रकार $\mathbf{Z}$ व $\mathbf{E}$ समूहों के रूप में तुल्याकारिक हैं जबकि $\mathbf{Z}$ व $\mathbf{E}$ वलयो के रूप में तुल्याकारिक नहीं हैं। वस्तुतः $\mathbf{Z}$ में इकाइयाँ है परन्तु $\mathbf{E}$ में इकाइयाँ नहीं है। वस्तुतः f वलय समरूपता नहीं होगी।

- यदि $f: R \to R'$ आच्छादक समरूपता है तो R', R की भागफल वलय से तुल्याकारिक है। वस्तुतः $R' \cong \dfrac{R}{\text{Ker}\, f}$ ।

- यदि N वलय R का आदर्श हो तो R के समस्त आदर्श के समुच्चय के मध्य एक–एक आच्छादक मानचित्रण विद्यमान् है जिसमें N है एवं R/N के आदर्श का समुच्चय अंतर्विष्ट है।

- यदि N वलय R का आदर्श है तो R/N का कोई आदर्श प्रकार A/N का है जहाँ A, R का आदर्श है जिसमें N अंतर्विष्ट है।

- वलय R में आदर्श का संकेतन समूहों में सामान्य उपसमूह की अवधारणा के समानान्तर है। सामान्य उपसमूहों से भागफल समूह का निर्माण सामने आता है, आदर्श काम आते हैं जब हम भागफल वलय को परिभाषित कर रहे होते हैं। कई अनुरूपों से परिणाम आता है जिसके साथ हम आरम्भ कर सकते हैं।

टिप्पणी

- वलय R के गैर–रिक्त उपसमुच्चय I को R का दायाँ आदर्श कहा जाता है यदि,

  $(i)\ a, b \in I \Rightarrow a - b \in I$

  $(ii)\ a \in I, r \in r \Rightarrow ar \in I.$

  I को R का बायाँ आदर्श कहते हैं यदि,

  $(i)\ a, b \in I \Rightarrow a - b \in I$

  $(ii)\ a \in I, r \in R \Rightarrow ra \in I$

- हो सकता है कि उपवलय आदर्श न हो।

  हमें विदित है कि $< \mathbf{Z}, +, \cdot >, < \mathbf{Q}, +, \cdot >$ की उपवलय है जहाँ $\mathbf{Z}$ पूर्णांक, $\mathbf{Q}$ = परिमेय।

  $3 \in \mathbf{Z}, \frac{1}{5} \in \mathbf{Q}$ किन्तु $3.\frac{1}{5} \notin \mathbf{Z}$

  इस प्रकार $\mathbf{Z}$ आदर्श नहीं है।

- यदि A व B के दो आदर्श हों तो $A + B, R$ का आदर्श है जिसमें A व B दोनों अंतर्विष्ट हैं।
- वस्तुतः $< S >, \mathrm{R}$ के समस्त आदर्श का प्रतिच्छेद या सर्वनिष्ठ होगा जिसमें S है एवं यह S युक्त सबसे छोटा आदर्श है। यदि S परिमित है तो हम कहते हैं कि $A = < S >$ परिमित रूप से उत्पन्न है।
- यदि $S = \varphi,\ \{0\}$ तो चूँकि R युक्त $S = \varphi, < S > \subseteq \{0\}$ का आदर्श है एवं इसलिये $< S > = \{0\}$।
- यदि A व B वलय R के दो आदर्श हों तो $A + B = < A \cup B >$ है।
- वलय AB के किन्हीं दो आदर्श A व B का गुणन R, R का एक आदर्श है।
- वलय $R \neq \{0\}$ को सरल वलय कहते हैं यदि R में कोई आदर्श न हो, R व $\{0\}$ को छोड़कर।
- विभक्त वलय एक सरल वलय है।
- यदि $S, < R, + >$ को कोई उपसमूह हो तो $S, (a \in S \subseteq R, r \in R \Rightarrow ar = 0 \in S)$ का दायाँ आदर्श होगा। दिए गए पदानुसार R में दो ही दायें आदर्श हैं, R व $\{0\}$। इस प्रकार $< R, + >$ में दो ही उपसमूह हो सकते हैं: R व $\{0\}$।
- R को कोई वलय मानें एवं I, R का आदर्श हो। चूँकि $a, b \in I \Rightarrow a - b \in I,$ हम पाते हैं कि $I, < R, + >$ का उपसमूह है। पुनः चूँकि $< R, + >$ एबेलियन है अतः $I,$ R का सामान्य उपसमूह होगा एवं इस प्रकार हम भागफल समूह $\frac{R}{I}$ की चर्चा कर सकते हैं $\frac{R}{I} = \{r + I \mid r \in R\}, R$ में I के समस्त सहसमुच्चय का समुच्चय (स्पष्टतया बायें अथवा दायें सहसमुच्चय समतुल्य हैं)।

टिप्पणी

- अमूर्त बीजगणित में समाकलित डोमेन की भिन्नों के क्षेत्र अथवा क्षेत्र भागफल सबसे छोटे क्षेत्र है जिसमें समाकलित डोमेन समा सके।
- समाकलित डोमेन R की भिन्नों के क्षेत्र के अवयवों में प्रकार a/b होता है एवं R और b 0 में a, b सहित। वलय R की भिन्नों के क्षेत्र को Quot(R) अथवा Frac(R) द्वारा इंगित किया जाता है। इसे भागफल क्षेत्र अथवा भिन्नों के क्षेत्र अथवा भिन्न क्षेत्र कहते हैं।
- R को कोई वलय मानें। R पर बहुपद से हमारा आशय प्रकार $f(x) = a_o + a_1x + a_2x^2 + ... + a_mx^m$, $a_i \in R$ के व्यंजक से है।
- बहुपदों $f(x)$ व $g(x)$ के योग को इस प्रकार परिभाषित किया जाता है,

  $f(x) + g(x) = (a_o + b_o) + (a_1 + b_1)\, x + (a_2 + b_2)\, x^2 + ...$
- $R, R[x]$ की समरूपता प्रतिबिंब है एवं इसी कारण इसमें ईकाई है, ईकाई युक्त वलय की समरूपता प्रतिबिंब के रूप में एक ईकाई युक्त वलय है। वस्तुतः $\theta\,(e(x)), R$ की ईकाई होगी जहाँ $e(x), R[x]$ की ईकाई है।
- यदि R समाकलित डोमेन हो तो चूँकि $a_m \neq 0, b_n \neq 0$, इसीलिये $a_mb_n \neq 0$ एवं इस कारण $c_{m+n} = a_mb_n \neq 0$ दर्शा रहा है कि $\deg(f(x)g(x)) = m + n$ है।
- यदि R एक वलय है, हम बहुपदों की संगत वलय $R[x]$ प्राप्त करते हैं। चूँकि $R[x]$ एक वलय है, हम इसी प्रकार $R[x, y]$ के बहुपदों की संगत वलय $R[x]$ प्राप्त करते हैं एवं संक्रिया को विस्तारित किया जा सकता है।
- यदि F क्षेत्र हो तो $F[x]$ ईकाई युक्त वलय है एवं इसी प्रकार $F[x, y]$ ईकाई युक्त वलय होगी।
- यदि F क्षेत्र हो तो $F[x]$ एक युक्लिडीन डोमेन है।
- यदि F एक क्षेत्र है, $F[x]$ में प्रत्येक आदर्श सिद्धांत है।
- परिमेय क्षेत्र में भिन्न a/b होते हैं जहाँ a व b पूर्णांक हैं एवं $b \neq 0$।
- प्रकार $a_mx^m + a_{m-1}\, x^{m-1} + \ldots\ldots + a_1x + a_0 = 0$ के समीकरण जहाँ m एक धनात्मक पूर्णांक है व a's परिमेय क्षेत्र के अवयव उन्हें x में बहुपद समीकरण कहा जाता है।
- समाकलित डोमेन R को युक्लिडीन डोमेन (अथवा युक्लिडीन वलय) कहा जाता है यदि सभी $a \in R$ के लिए $a \neq 0$, स्पष्ट (–ve) अऋणात्मक पूर्णांक $d(a)$ इस प्रकार है कि,

  (i) सभी $a, b \in R, a \neq 0, b \neq 0$ के लिए $d(a) \leq d(ab)$

  (ii) सभी $a, b \in R, a \neq 0, b \neq 0$ के लिए $\exists\ t$ एवं R में r इस प्रकार $a = tb + r$

  जहाँ या तो $r = 0$ अथवा $d(r) < d(b)$।
- ऐसा आदर्श A जिसमें अवयव a_o के गुणज हैं, a_o के R सहित उसे R का आदर्श सिद्धांत कहा जाता है, a_o द्वारा उत्पन्न। हम इसे $A = (a_o)$ से इंगित करते हैं।

टिप्पणी

- R के सबसे छोटे आदर्श जिसमें a_o होता है तथा a_o द्वारा उत्पन्न सिद्धांत आदर्श कहा जाता है।
- युक्लिडीन डोमेन में प्रत्येक आदर्श सिद्धांत आदर्श है। युक्लिडीन डोमेन में ईकाई है।
- ईकाई युक्त समाकलित डोमेन R को आदर्श सिद्धांत डोमेन कहते हैं यदि R का प्रत्येक आदर्श सिद्धांत आदर्श हो।
- R को ईकाई युक्त क्रमविनिमेय वलय मानें। अवयव $p \in R$ को अभाज्य अवयव कहा जाता है यदि,
  (i) $p \neq 0, p$ एक ईकाई नहीं है।
  (ii) किसी भी a के लिए $b \in R$ यदि $p \mid ab$ तो $p \mid a$ या $p \mid b$।
- ईकाई युक्त समाकलित डोमेन में प्रत्येक अभाज्य अवयव अलघुकरणीय है। इसका विलोम वास्तविक नहीं।
- UFD में अवयव R अभाज्य है यदि यह अलघुकरणीय है।
- यदि R ईकाई युक्त समाकलित डोमेन हो जिसमें प्रत्येक अशून्य, गैर–ईकाई अवयव अलघुकरणीय अवयवों का परिमित गुणन है एवं प्रत्येक अलघुकरणीय अवयव अभाज्य है तो R एक यूएफ़डी है।
- ईकाई युक्त समाकलित डोमेन R एक यूएफ़डी है यदि और केवल यदि प्रत्येक अशून्य, गैर–ईकाई अवयव अलघुकरणीय अवयवों का एक परिमित गुणन है एवं प्रत्येक अलघुकरणीय अवयव अभाज्य है।
- ईकाई युक्त समाकलित डोमेन R एक यूएफ़डी है यदि प्रत्येक अशून्य, गैर–ईकाई अवयव अभाज्यों का परिमित गुणन है।
- वलय R में आदर्श $A_1 \subseteq A_2 \subseteq A_3 \subseteq .....$ की आरोही शृंखला का संघ R का आदर्श है।
- R एक यूएफ़डी है तो $R[x]$ में दो आघक बहुपदों का गुणन एक आघक बहुपद है।
- यदि $f(x)g(x)$, $R[x]$ में आघक बहुपद है, R यूएफ़डी है तो इसलिये (x) व $g(x)$ हैं।
- यदि R ईकाई युक्त समाकलित डोमेन है एवं R, का अलघुकरणीय अवयव है तो a, $R[x]$ का अलघुकरणीय अवयव है।
- R को ईकाई युक्त समाकलित डोमेन मानें। धनात्मक श्रेणी (अर्थात् $\deg \geq 1$) के बहुपद $f(x) \in R[x]$ को R पर अलघुकरणीय बहुपद कहा जाता है यदि इसे धनात्मक श्रेणी के दो बहुपदों के गुणन के रूप में व्यक्त न किया जा सके।
- धनात्मक श्रेणी का बहुपद जो कि अलघुकरणीय न हो R पर परिवर्तक योग्य कहलाता है।
- यदि F एक क्षेत्र हो तो $F[x]$ में आदर्श $< p(x) > \neq \{0\}$ महत्तम है यदि $p(x)$, $F[x]$ में अलघुकरणीय है।

टिप्पणी

- यदि R यूएफ़डी है एवं $p(x)$, $R[x]$ में आघक बहुपद तो इसे $R[x]$ के अलघुकरणीय अवयवों के गुणन के रूप में अनोखे प्रकार से गुणनखंड किया जा सकता है।
- यदि $f(x) \in R[x]$, $R[x]$ का अलघुकरणीय अवयव व आघक दोनों हो तो $f(x)$, $K[x]$ का अलघुकरणीय अवयव है।
- यदि $f(x) \in \mathbf{Z}[x]$ आघक हो एवं $f(x)$, $\mathbf{Z}$ पर अलघुकरणीय हो तो f, $\mathbf{Q}$ पर अलघुकरणीय है।

5.10 मुख्य शब्दावली

- **वलय** : यह एक बीजगणितीय संरचना है जिसमें योग व गुणन के रूप में दो द्विआधारी संरचना के साथ समुच्चय अंतर्विष्ट होता है जहाँ समुच्चय योग के अधीन एक एबेलियन समूह है एवं गुणन के अधीन एकाभ इस प्रकार है कि गुणन योग पर वितरित है।
- **क्रमविनिमेय वलय** : यह एक वलय R है यदि सभी $a, b \in R$ के लिए $ab = ba$ है।
- **विभक्त वलय** : ईकाई युक्त वलय को विभक्त वलय अथवा तिरछा क्षेत्र कहते हैं यदि वलय के अशून्य अवयवों से गुणन के सन्दर्भ में समूह का निर्माण होता है।
- **मापांक** : यह एक बीजगणितीय विषय है जिसमें गुणांकों को गुणित करते हुए वस्तुओं को एकसाथ क्रमविनिमय रूप से जोड़ा जा सकता है एवं जिसमें सदिश–परिचालन के अधिकांश नियम हैं।
- **क्षेत्र** : क्रमविनिमेय विभक्त वलय को क्षेत्र कहा जाता है।

5.11 स्व–मूल्यांकन प्रश्न एवं अभ्यास

लघु–उत्तरीय प्रश्न

1. वलय सिद्धांत क्या है?
2. बूलियन वलयों को परिभाषित करें।
3. उपवलय क्या हैं?
4. वलयो के अभिलक्षण बतायें।
5. मानचित्रण को कब समरूपता कहा जाता है?
6. आदर्श वलय क्या हैं?
7. दो आदर्शों के योगफल को आप कैसे परिभाषित करेंगे? उदाहरणों सहित प्रस्तुत करें।
8. दो आदर्शों के गुणन को उदाहरणों सहित परिभाषित करें।

9. भागफल वलयों के विशेषताओं को परिभाषित करें।
10. बहुपद वलयो की व्याख्या इनकी विशेषताओं सहित करें।
11. क्या हम क्रमविनिमेय वलयो पर बहुपद वलयो को परिभाषित कर सकते हैं? कैसे?
12. समाकलित डोमेन की विषेशताएँ लिखें।
13. युक्लिडीन डोमेन क्या है?
14. 'अद्वितीय गुणनखंड डोमेन' एवं 'आदर्श सिद्धांत डोमेन' शब्द समूहों की व्याख्या करें।

टिप्पणी

दीर्घ–उत्तरीय प्रश्न

1. उदाहरण सहित सिद्ध करें कि वलय R क्रमविनिमेय है।
2. यदि वलय R में समस्त x हेतु $x^2 = x$ तो दर्शायें कि $2x = 0$ व $x + y = 0 \Rightarrow x = y$।
3. यदि R ईकाई युक्त वलय हो एवं सभी $a, b \in R$ के लिए $(ab)^2 = (ba)^2$ एवं $2x = 0$

   $\Rightarrow x = 0$ तो दर्शायें कि R क्रमविनिमेय है।
4. **R** को वास्तविक संख्याओं का समुच्चय मानें। दर्शायें कि **R**×**R** से योग व गुणन के अधीन क्षेत्र का निर्माण निम्नपरिभाषानुसार होता है,

   $(a, b) + (c, d) = (a + c, b + d)$

   $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$
5. R को ईकाई युक्त क्रमविनिमेय वलय मान लेते हैं। दर्शायें कि,

   (i) a एक ईकाई है यदि a^{-1} एक ईकाई है।

   (ii) a, b इकाइयां हैं यदि ab ईकाई है।
6. दर्शायें कि ईकाई युक्त क्रमविनिमेय वलय में समस्त इकाइयों के समुच्चय से एक एबेलियन समूह बनता है।
7. अक्रमविनिमेय वलय R का उदाहरण प्रस्तुत करें जिसमें समस्त $x, y \in R$ हेतु $(xy)^2 = x^2y^2$ है।
8. यदि $< R, +, \cdot >$ ऐसी प्रणाली हो जिसमें ईकाई युक्त वलय की परिभाषा के सभी पद पूर्ण हो रहे हों ($a + b = b + a$ को छोड़कर) तो दर्शायें कि यह पद भी पूर्ण हो रही है, सभी $a, b \in R$ के लिए $(a + b)^2 = a^2 + b_2 + 2ab$ है।
9. यह दर्शाने हेतु उदाहरण प्रस्तुत करें कि दो उपवलयों का संघ हो सकता है कि उपवलय न हो। सिद्ध करें कि दो उपवलय का संघ एक उपवलय है यदि यह एक दूसरे में अंतर्विष्ट हो।
10. सिद्ध करें कि दो आदर्शों का संघ एक आदर्श होता है यदि इनमें से एक दूसरे में अंतर्विष्ट हों।

टिप्पणी

11. मान लें कि $f: R \to R'$ में एक समरूपता हो एवं R को A का आदर्श मानें। दर्शायें कि $f(A) = \{x \in R' | \exists\ a \in A, x = f(a)\}$, $f(R)$ का आदर्श है।

12. समाकलित डोमेन $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$. की भागफलों के क्षेत्र ज्ञात करें।

13. यदि A, B, C पीआईडी (PID) R में आदर्श हों तो सिद्ध करें कि:

    (i) $A \cap (B + C) = A \cap B + A \cap C$

    (ii) $A + (B \cap C) = (A + B) \cap (A + C)$

14. यदि R एक यूएफ़डी (UFD) है एवं $f(x) \in R[x]$ तो $f(x) = ag(x), a \in R$ लिखना सम्भव है, $g(x) \in R[x]$ आधक है। दर्शायें कि यदि $f(x) = ag(x) = bh(x), a, b \in R, g, h$ आधक हों तो a, b संबंद्धता हैं एवं इसलिये $g(x)$ व $h(x)$ हैं।

5.12 सहायक पाठ्य सामग्री

Sharma, Dr Anil and Jitendra Saini. 2016. *Abstract Algebra* (अमूर्त बीजगणित) Jaipur (Rajasthan): RBD Publisher.

Pathak, Dr H. K. 2017. *Abstract Algebra* (अमूर्त बीजगणित). Kolkata (West Bengal): Siksha Sahitya Prakashan.

Herstein, I. N. 1975. *Topics in Algebra*, 2nd Edition. New York: John Wiley and Sons.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. UK: Cambridge University Press (Indian Edition).

Khanna, V. K. and S. K. Bhambari. 2016. *A Course in Abstract Algebra*, 5th Edition. New Delhi: Vikas Publishing House Pvt. Ltd.

Clark, Allan. 2012. *Elements of Abstract Algebra*. Chelmsford: Courier Corporation.

Gilbert, Linda. 2008. *Elements of Modern Algebra*. Boston: Cengage Learning.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

Childs, Lindsay N. 2008. *A Concrete Introduction to Higher Algebra*. Berlin: Springer Science & Business Media.