स्वाध्याय स्वमन्थन स्वावलम्बन

उत्तर प्रदेश राजर्षि टण्डन मुक्त विश्वविद्यालय

(उत्तर प्रदेश सरकार द्वारा निर्गत अधिनियम संख्या 10, 1999 द्वारा स्थापित)

UGMM-06
अमूर्त बीजगणित

प्रथम-खण्ड
प्रारंभिक समूह सिद्धांत

इन्दिरा गाँधी राष्ट्रीय मुक्त विश्वविद्यालय

उत्तर प्रदेश राजर्षि टण्डन मुक्त विश्वविद्यालय

शान्तिपुरम् (सेक्टर-एफ), फाफामऊ, इलाहाबाद – 211013

उत्तर प्रदेश
राजर्षि टण्डन मुक्त विश्वविद्यालय

UGMM – 06

अमूर्त बीजगणित

खंड

1

प्रारंभिक समूह सिद्धांत

अमूर्त बीजगणित

शब्द "बीजगणितं" से तो आप सभी परिचित हैं ही। शायद आप जानते हों कि इसका अंग्रेज़ी अनुवाद अरबी शब्द "अल-जब्र" से आया है। पहले ज़माने में बीजगणित का संबंध समीकरणों का हल प्राप्त करने से था। फिर आया आधुनिक बीजगणित, जिसका संबंध चिरप्रतिष्ठित बीजगणित के अंतर्गत बारीक जाँचों से है। आजकल अमूर्त बीजगणित का अध्ययन होने लगा है, जो कि आधुनिक बीजगणित का व्यापकीकरण है। अमूर्त बीजगणित में हम उन बीजीय निकायों का अध्ययन करते हैं जिन्हें केवल अभिगृहीतों (axioms) से परिभाषित किया जाता है। सामान्यतः ये अभिगृहीत वास्तविक स्थितियों से विकसित होते हैं। रैखिक बीजगणित के पाठ्यक्रम से आप इस प्रकार के एक बीजीय निकाय, अर्थात् सदिश समष्टि के बारे में जानते हैं। जैसा कि आप जानते हैं, यूक्लिडीय समष्टि R^n को ध्यान में रखकर ही सदिश समष्टि को परिभाषित करने वाले अभिगृहीत विकसित किए गए।

इस पाठ्यक्रम में हम तीन अन्य आधारभूत बीजीय निकायों, अर्थात् समूह, वलय और क्षेत्र का अध्ययन करेंगे। पहले दो खंडों में हम आपको समूहों और उनके गुणों से परिचित कराएंगे, और शेष दो खंडों में हम वलय और क्षेत्र पर चर्चा करेंगे। पाठ्यक्रम की शुरुआत हम इकाई 1 से करेंगे, जिसमें हम समुच्चयों और फलनों की आधारभूत परिभाषाओं और परिणामों तथा पूर्णांकों की भाज्यता के गुणों का एक संक्षिप्त विवरण देंगे। इससे आप बाद में आने वाली संकल्पनाओं को आसानी से समझ सकेंगे।

आप शायद सोच रहे होंगे कि इस पाठ्यक्रम का अध्ययन क्यों करें? इस पाठ्यक्रम का अध्ययन करने के दौरान आप यह अनुभव करेंगे कि अमूर्त बीजगणित की विधियों से हम अनेक मिलते-जुलते बीजीय निकायों का अध्ययन केवल एक प्रतिनिधि निकाय का अध्ययन करके कर सकते हैं।

जो कुछ आप इस पाठ्यक्रम में पढ़ेंगे, उसके अनेक व्यावहारिक अनुप्रयोग हैं। आइए सबसे पहले हम समूह सिद्धांत के कुछ अनुप्रयोगों पर विचार करें। भौतिक विज्ञानी और रसायनज्ञ इस सिद्धांत का प्रयोग क्रिस्टल-विज्ञान, स्पेक्ट्रम-विज्ञान, व्यापक आपेक्षिकता, ठोस अवस्था भौतिकी और मूलकण भौतिकी में करते हैं। वास्तव में, समूह सिद्धांत के प्रयोग से ही वैज्ञानिकों ने ओमेगा ऋण कण के अस्तित्व का पूर्वानुमान लगाया था, जिसे 1964 में जाकर ही खोजा गया (पूर्वानुमान के कई सालों बाद)।

आइए, अब हम वलयों और क्षेत्रों के कुछ अनुप्रयोगों पर विचार करें। क्वांटम यांत्रिकी में बहुपद वलयों और आव्यूह वलयों का प्रयोग किया जाता है। आज आंकड़ा संचार क्षेत्र में त्रुटि का पता लगाने के लिए और त्रुटि-सुधार के लिए कार्यक्षम कोडों के निर्माण में क्षेत्र-सिद्धांत का प्रयोग किया जा रहा है। और, परिमित क्षेत्र सांख्यिकी में भी बहुत उपयोगी हैं।

हमने जिस प्रकार शिक्षण सामग्री को प्रस्तुत किया है, उसके बारे में भी हम दो शब्द कहना चाहेंगे। हमने यह मानकर इस पाठ्यक्रम को प्रस्तुत किया है कि आप रैखिक बीजगणित के पाठ्यक्रम में दी गई शिक्षण-सामग्री का अध्ययन कर चुके हैं। जैसा कि आप जानते हैं, जब भी हम आपको नई संकल्पनाओं से परिचित कराते हैं तो साथ में हम कई ठोस उदाहरण भी देते हैं जिससे कि आप संकल्पना को अच्छी तरह से समझ सकें। हमने रैखिक बीजगणित से कई उदाहरण लिए हैं। हम इस पाठ्यक्रम के खंड 4 में सदिश समष्टि के आधार के गुणों की जानकारी भी मानकर चलेंगे।

इस पाठ्यक्रम को चार खंडों में बांटा गया है। प्रत्येक खंड में हमने खंड की प्रस्तावना, खंड में पाए जाने वाले प्रतीकों की सूची और खंड की इकाइयाँ दी हैं। प्रत्येक इकाई में बीच-बीच में पाठ्यांश के साथ प्रश्न भी दिए गए हैं। ये प्रश्न इसलिए दिए गए हैं कि आप अपनी प्रगति की स्वयं जाँच कर सकें। इकाई में दिए गए प्रश्नों के हल/उत्तर इकाई के अंत में दिए गए हैं। जब आप किसी इकाई को पढ़ लें तो इकाई के प्रस्तावना में दिए गए उद्देश्यों को देखकर आप जांच कर लें कि आप कहां तक उद्देश्यों की पूर्ति में सफल हो पाए हैं। हर खंड के अंत में हमने एक शब्दावली दी है, जिसमें हमने खंड में पाए जाने वाले कुछ गणितीय पारिभाषिक शब्दों के अंग्रेज़ी अनुवाद दिए हैं।

अब हम संकेतन के बारे में कुछ कहेंगे। प्रत्येक इकाई को भागों में बांटा गया है। अलग-अलग इकाइयों में दी गई शिक्षण सामग्री एक-दूसरे से काफ़ी संबंधित है, इसलिए हमने संदर्भ का प्रयोग

किया है। इसके लिए हमने संकेत भाग x.y का प्रयोग किया है, जिसका अर्थ है इकाई x का भाग y।

इस पाठ्यक्रम के अध्ययन के दौरान हम आपको तीन सत्रीय कार्य भेजेंगे। ये शिक्षण-सहायक का भी काम करते हैं। आपके काउंसेलर पहले दो सत्रीय कार्यों का निर्धारण करेंगे और उपयुक्त टिप्पणियों के साथ आपको सत्रीय कार्य लौटा देंगे। तीसरे सत्रीय कार्द का मूल्यांकन कंप्यूटर द्वारा किया जाएगा।

यदि आप इस पाठ्यक्रम में दी गई शिक्षण-सामग्री का और अधिक अध्ययन करना चाहते हैं तो आप निम्नलिखित पुस्तकों को देख सकते हैं:

1 *प्रारंभिक आधुनिक बीजगणित*, डी. एन. मिश्र और एस. एन. माहेश्वरी (मध्य प्रदेश हिंदी ग्रंथ अकादमी)

2 *University Algebra* by N.S. Gopalakrishnan (Wiley-Eastern Ltd.).

3 *Topics in Algebra* by I.N. Herstein (Vikas)

4 *A Text Book of Modern Abstract Algebra* by Shanti Narayan.

5 *Basic Abstract Algebra* by Bhattacharya, Jain and Nagpaul (Cambridge University Press).

ये सभी पुस्तकें आपको अपने अध्ययन केन्द्र के पुस्तकालय में मिलेंगी।

आशा है कि आपको इस पाठ्यक्रम को पढ़ने में आनन्द आएगा।

खंड 1 प्रारंभिक समूह सिद्धांत

समूह एक बीजीय निकाय है, जिसमें एक समुच्चय होता है और साथ में उस पर परिभाषित एक द्वि-आधारी संक्रिया। दो सौ से भी अधिक वर्षों से गणितज्ञ समूह सिद्धांत का अध्ययन करते आ रहे हैं। उन्नीसवीं शताब्दी में समूह सिद्धांत के अंतर्गत क्रमचयों और प्रतिस्थापनों का अध्ययन होता था। धीरे-धीरे इस सिद्धांत ने विकसित होकर वर्तमान अमूर्त रूप धारण कर लिया।

वर्तमान समूह सिद्धांत की सहायता से आधारभूत गणितीय संरचनाओं का विश्लेषण किया जा सकता है। समूह सिद्धांत की विधियों और साधनों को लागू करके गणित की विभिन्न शाखाओं पर कार्य कर रहे गणितज्ञ अपने क्षेत्र का विकास कर सकते हैं। न केवल गणितज्ञ, बल्कि रसायनज्ञ और भौतिकी विज्ञानी भी अणुओं और क्रिस्टलों की संरचनाओं का विश्लेषण करने के लिए अथवा प्रौढ़ इलेक्ट्रॉनिकी के "ठोस परिपथों" के अध्ययन के लिए समूह सिद्धांत का प्रयोग करते हैं। डच भौतिकी विज्ञानी लॉरेंज़ द्वारा प्रस्तुत किया गया बीजीय रूपांतरण समूह ही था जिसका प्रयोग आइनस्टाइन ने विशिष्ट आपेक्षिकता का विश्लेषण करने में किया था। इसी रोचक और उपयोगी सिद्धांत के मूल तत्त्व हम आपको बताना चाहते हैं।

इस खंड की पहली इकाई में हम समुच्चयों, फलनों और संख्या सिद्धांत से संबंधित कुछ आधारभूत संकल्पनाओं का संक्षिप्त विवरण देंगे। साथ ही, कुछ ऐसे संकेतन को भी स्थापित करेंगे जिनका प्रयोग पूरे पाठ्यक्रम में किया जाएगा।

हम इकाई 2 में समूह सिद्धांत का अध्ययन शुरू करेंगे। इस इकाई में आप पढ़ेंगे कि समूह क्या होता है। आप यह भी देखेंगे कि पूर्णांकों और परिमेय संख्याओं के समुच्चय जैसे अनेक सुपरिचित समुच्चय योग-संक्रिया के सापेक्ष समूह होते हैं।

यहां हम तीन समूह — पूर्णांक माड्यूलो n का समूह, क्रमचय समूह और सम्मिश्र संख्या समूह — से भी आपको परिचित कराएंगे। इन समूहों को आप इस पाठ्यक्रम में प्रायः पाएंगे।

इकाई 3 में आप समूहों के उन उपसमुच्चयों का अध्ययन करेंगे जो स्वयं समूह हैं। इन्हें हम उपसमूह कहते हैं।

अंतिम इकाई में हम परिमित संख्या में अवयवों वाले समूहों से संबंधित एक प्रारंभिक प्रमेय पर चर्चा करेंगे। इस परिणाम का नामकरण गणितज्ञ लग्रांज के नाम पर किया गया है।

अगले खंड में आप समूह सिद्धांत का थोड़ी और गहराई से अध्ययन करेंगे। इसके लिए आपको उन सभी तथ्यों की जानकारी की आवश्यकता पड़ेगी, जिनका अध्ययन आप इस खंड में करेंगे। अतः आप इस खंड को ध्यान से पढ़िए। प्रत्येक प्रश्न को हल करने का प्रयास कीजिए और उसे हल करने के बाद ही आप आगे अध्ययन कीजिए।

संकेत और प्रतीक

$\{x \mid x, P$ को संतुष्ट करता है$\}$	ऐसे सभी x का समुच्चय जहां x गुण P को संतुष्ट करता हो
$\mathbf{N}$	प्राकृतिक संख्याओं का समुच्चय
$\mathbf{Z}(\mathbf{Z}^*)$	पूर्णांकों (शून्येतर पूर्णांकों) का समुच्चय
$\mathbf{Q}(\mathbf{Q}^*)$	परिमेय संख्याओं (शून्येतर परिमेय संख्याओं) का समुच्चय
$\mathbf{R}(\mathbf{R}^*)$	वास्तविक संख्याओं (शून्येतर वास्तविक संख्याओं) का समुच्चय
$\mathbf{C}(\mathbf{C}^*)$	सम्मिश्र संख्याओं (शून्येतर सम्मिश्र संख्याओं) का समुच्चय
$\mathbf{Z}_n$	माड्यूलो n पूर्णांकों का समुच्चय
ϕ	रिक्त समुच्चय
$\in$	का सदस्य है
$\notin$	का सदस्य नहीं है
$\subseteq (\subsetneq)$	का उपसमुच्चय है (का उचित उपसमुच्चय है)
$\not\subseteq$	का उपसमुच्चय नहीं है
$A \cup B$	समुच्चयों A और B का सम्मिलन
$A \cap B$	समुच्चयों A और B का प्रतिच्छेद
$A \setminus B$	A के उन अवयवों का समुच्चय जो B के अवयव नहीं हैं
A^c	A का पूरक
$A \times B$	A और B का कार्तीय गुणनफल
$\exists$	का अस्तित्व है
$\forall$	सभी के लिए
$\Longrightarrow$	निहित है
$\Longleftrightarrow$	निहित है और से निहित है (या यदि और केवल यदि)
$[a], \bar{a}$	a का तुल्यता-वर्ग
$f : A \to B$	समुच्चय A से समुच्चय B तक का फलन f
$f(S) \quad (f^{-1}(S))$	फलन f के अधीन समुच्चय S का प्रतिबिंब (प्रतिलोम प्रतिबिंब)
$f \circ g$	फलन f और फलन g का संयोजन
$a \mid b$	a, b को विभाजित करता है
$a \nmid b$	a, b को विभाजित नही करता
$a \equiv b \pmod{n}$	a और b समशेष हैं माड्यूलो n
$\pm a$	a या $(-a)$
x^{-1} या $-x$	अवयव x का प्रतिलोम
S_n	n प्रतीकों पर सममित समूह
$(i_1, i_2, \ldots, i_r)$	एक r-चक्र
$H \leq G$	H, G का उपसमूह है
$H \not\leq G$	H, G का उपसमूह नहीं है
$< S >$	समुच्चय S से जनित समूह
$< a >$	a से जनित चक्रीय समूह
$Hx, H + x$	उपसमूह H का दक्षिण सहसमुच्चय

A_n	n प्रतीकों का एकांतर समूह
Q_8	चतुष्टयी समूह
$Z(G)$	समूह G का केन्द्र
$o(G)$	समूह G की कोटि
$o(x)$	अवयव x की कोटि
	इसलिए

यूनानी अक्षर

α	ऐल्फ़ा
β	बीटा
γ	गामा
δ	डेल्टा
ε	एप्सिलॉन
ζ	ज़ीटा
η	ईटा
θ	थीटा
ι	आयोटा
κ	कापा
λ	लैम्डा
μ	म्यू
ν	न्यू
ξ	ज़ाइ
o	ओमिक्रॉन
$\pi(\Pi)$	पाइ (पाइ का बड़ा अक्षर)
ρ	रो
$\sigma(\Sigma)$	सिग्मा (सिग्मा का बड़ा अक्षर)
τ	टाओ
υ	अप्सिलॉन
ϕ	फ़ाइ
χ	काइ
ψ	साइ
ω	ओमेगा

इकाई 1 समुच्चय और फलन

इकाई की रूपरेखा

1.1 प्रस्तावना

इस इकाई में पहले हम समुच्चयों और फलनों से संबंधित कुछ आधारभूत संकल्पनाओं पर चर्चा करेंगे। ये संकल्पनाएं गणित की किसी भी शाखा के, विशेष रूप से बीजगणित के, अध्ययन में मौलिक हैं।

इस इकाई के अंतिम भाग में हम कुछ प्रारंभिक संख्या-सिद्धांत पर चर्चा करेंगे। इस भाग का मुख्य उद्देश्य कुछ ऐसे तथ्यों को एकत्रित करना है जिनकी आवश्यकता हमें पाठ्यक्रम के शेष भाग में पड़ेगी। हमें उम्मीद है कि आपको संख्या-सिद्धांत की सुन्दरता की झलक भी दिखा सकेंगे। इसी सुन्दरता की वजह से गणितज्ञ गाउस ने संख्या-सिद्धांत को "गणित की रानी" कहा था।

हम फिर कहना चाहेंगे कि इस इकाई में अति आधारभूत संकल्पनाओं पर विचार किया गया है। इनका प्रयोग पूरे पाठ्यक्रम में किया जाएगा। इसलिए इस इकाई को ध्यान से पढ़िए।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- समुच्चयों पर विभिन्न संक्रियाओं का प्रयोग कर सकेंगे;
- समुच्चयों पर कार्तीय गुणनफल परिभाषित कर सकेंगे;
- यह जांच कर सकेंगे कि संबंध एक तुल्यता संबंध है या नहीं, और तुल्यता-वर्ग को ज्ञात कर सकेंगे;
- आगमन नियम का कथन दे सकेंगे और उसका प्रयोग कर सकेंगे;
- विभाजन-कलन विधि और अद्वितीय अभाज्य गुणनखंडन प्रमेय का प्रयोग कर सकेंगे।

1.2 समुच्चय

आपने बातचीत के दौरान किसी संग्रह का वर्णन देते समय शब्द "समुच्चय" का प्रयोग कई बार किया होगा। गणित में शब्द **समुच्चय** का प्रयोग वस्तुओं के **सुपरिभाषित** संग्रह के वर्णन के लिए किया जाता है। अर्थात् प्रत्येक समुच्चय का वर्णन इस प्रकार होना चाहिए कि यदि कोई वस्तु दी हुई हो तो यह स्पष्ट होना चाहिए कि दी हुई वस्तु समुच्चय में है या नहीं।

उदाहरण के लिए, सभी प्राकृतिक संख्याओं का संग्रह सुपरिभाषित है। इसलिए यह एक समुच्चय है। लेकिन सभी धनी व्यक्तियों का संग्रह समुच्चय नहीं है, क्योंकि ऐसा कोई नियम नहीं है जिसे लागू करके हम कह सकें कि अमुक व्यक्ति धनी है या नहीं।

यूनानी अक्षर $\in$ "का सदस्य है" को प्रकट करता है। यह एक यूनानी शब्द का संक्षिप्त रूप है जिसका अर्थ है "है"।

यदि S एक समुच्चय हो तो संग्रह S की वस्तु a को S का **अवयव (element)** कहते हैं। इस तथ्य को हम प्रतीकों में $a \in S$ से व्यक्त करते हैं। (इसे a, S में है "या a, S का सदस्य है" पढ़ा जाता है।)

यदि a, S में नहीं है, तो हम $a \notin S$ लिखते हैं। उदाहरण के लिए, $3 \in \mathbf{R}$, वास्तविक संख्याओं का समुच्चय। परन्तु $\sqrt{-1} \notin \mathbf{R}$.

ऐसा समुच्चय, जिसमें कोई अवयव न हो, **रिक्त समुच्चय** (empty set) कहलाता है और इसे हम यूनानी अक्षर ϕ (फाइ) से प्रकट करते हैं। उदाहरण के लिए, 1 से कम सभी प्राकृतिक संख्याओं का समुच्चय ϕ है।

किसी अरिक्त समुच्चय का वर्णन करने की प्रायः दो विधियाँ हैं:
(1) सूची विधि (roster method), और
(2) समुच्चय निर्माण विधि (set builder method).

सूची विधि : इस विधि में हम समुच्चय के सभी अवयवों को कोष्ठक के अंदर लिखते हैं। उदाहरण के लिए, 48 के सभी धन भाजकों के संग्रह के अवयव 1, 2, 3, 4, 6, 8, 12, 16, 24 और 48 हैं। अतः इस समुच्चय को हम {1, 2, 3, 4, 6, 8, 12, 16, 24, 48} लिख सकते हैं।

समुच्चय के इस वर्णन में निम्नलिखित दो प्रथाएं अपनाई गई हैं:
प्रथा 1 : समुच्चय के अवयवों को लिखने के क्रम का कोई महत्व नहीं है।
प्रथा 2 : किसी भी अवयव को एक से अधिक बार नहीं लिखा जाता है, अर्थात् प्रत्येक अवयव को केवल एक बार ही लिखना चाहिए।

उदाहरण के लिए, $1\frac{1}{2}$ और $4\frac{1}{4}$ के बीच सभी पूर्णांकों का समुच्चय S लीजिए। स्पष्ट है कि ये पूर्णांक 2, 3 और 4 हैं। अतः हम $S = \{2, 3, 4\}$ लिख सकते हैं। हम $S = \{3, 2, 4\}$ भी लिख सकते हैं परन्तु हमें $S = \{2, 3, 2, 4\}$ नहीं लिखना चाहिए। क्यों? क्या प्रथा 2 इसका संकेत नहीं देती?

सूची विधि का प्रयोग कभी-कभी बड़े समुच्चय के अवयवों को सूचीबद्ध करने के लिए भी किया जाता है। इस स्थिति में हम समुच्चय के सभी अवयवों को शायद लिखना न चाहें। हम कुछ अवयवों को लिख देते हैं, जिनसे हमें शेष अवयवों का संकेत मिल जाए। उदाहरण के लिए, 0 और 100 के बीच सभी पूर्णांकों का समुच्चय $\{0, 1, 2, \ldots, 100\}$ है, और सभी पूर्णांकों का समुच्चय $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$ है।

समुच्चय का वर्णन करने की एक अन्य विधि है

समुच्चय निर्माण विधि : इस विधि में पहले हम उस गुण को मालूम करने की कोशिश करते हैं जो समुच्चय के अवयवों की विशेषता हो, अर्थात् हम एक ऐसा गुण P मालूम करना चाहते हैं, जो समुच्चय के सभी अवयवों में हो और जो किसी अन्य वस्तु में न हो। तब हम इस समुच्चय का वर्णन इस प्रकार करते हैं:

{x | x गुण P को संतुष्ट करता है}, या
{x : x गुण P को संतुष्ट करता है}.

इसे इस प्रकार पढ़ा जाता है "ऐसे सभी x का समुच्चय जहां x गुण P को संतुष्ट करता हो"। उदाहरण के लिए, सभी पूर्णांकों के समुच्चय को इस प्रकार भी लिखा जा सकता है:

Z = {x | x एक पूर्णांक है}.

अब हम कुछ अन्य समुच्चय देंगे, जिनसे शायद आप परिचित हैं:

Q, परिमेय संख्याओं का समुच्चय $= \left\{ \frac{a}{b} \mid a, b \in \mathbf{Z}, b \neq 0 \right\}$
R, वास्तविक संख्याओं का समुच्चय
C, सम्मिश्र संख्याओं का समुच्चय $= \{a + ib \mid a, b \in \mathbf{R}\}$ (यहां $i = \sqrt{-1}$.)

आइए अब हम देखें कि उपसमुच्चय क्या होते हैं।
उपसमुच्चय : समुच्चय $A = \{1, 3, 4\}$ और $B = \{1, 4\}$ लीजिए। यहां B का प्रत्येक अवयव, A का भी अवयव है। ऐसी स्थिति में, अर्थात् जब समुच्चय B का प्रत्येक अवयव समुच्चय A का अवयव हो, हम कहते हैं कि **B, A का एक उपसमुच्चय है,** और इसे $B \subseteq A$ के रूप में लिखते हैं।

यह स्पष्ट है कि यदि A कोई समुच्चय हो तो A का प्रत्येक अवयव निश्चय ही A का एक अवयव होगा। अतः प्रत्येक समुच्चय A के लिए $A \subseteq A$.

और किसी भी समुच्चय A के लिए, $\phi \subseteq A$.

अब समुच्चय $S = \{1, 3, 5, 15\}$ और $T = \{2, 3, 5, 7\}$ लीजिए। क्या $S \subseteq T$? इसका उत्तर है "नहीं", क्योंकि S का प्रत्येक अवयव T में नहीं है; उदाहरण के लिए, $1 \in S$ पर $1 \notin T$. ऐसी स्थिति में हम कहते हैं कि S, T का उपसमुच्चय नहीं है, और इसे $S \not\subseteq T$ से प्रकट करते हैं।

ध्यान दीजिए कि यदि B, A का एक उपसमुच्चय नहीं है, तो B का एक ऐसा अवयव अवश्य होगा जो A का अवयव नहीं है। इस तथ्य को हम गणितीय संकेतन पद्धति में '$\exists\, x \in B$ जिसके लिए $x \notin A$' लिखते हैं।

'$\exists$' "का अस्तित्व है" को प्रकट करता है।

अब हम कह सकते हैं कि **दो समुच्चय A और B बराबर हैं** (अर्थात् इनके ठीक-ठीक समान अवयव हैं) **यदि और केवल यदि $A \subseteq B$ और $B \subseteq A$.**

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कर सकते हैं।

E 1) नीचे दिए गए कथनों में से कौन-कौन से कथन सही हैं?

(क) $N \subseteq Z$, (ख) $Z \subseteq N$, (ग) $\{0\} \subseteq \{1, 2, 3\}$, (घ) $\{2, 4, 6\} \not\subseteq \{2, 4, 8\}$

आइए अब हम समुच्चयों पर की जाने वाली कुछ संक्रियाओं पर विचार करें। यहां हम समुच्चयों के सम्मिलन, प्रतिच्छेद और पूरकीकरण की संक्रियाओं पर संक्षेप में चर्चा करेंगे।

सम्मिलन : यदि A और B समुच्चय S के उपसमुच्चय हों तो हम दोनों समुच्चयों के अवयवों को इकट्ठा करके एक नया समुच्चय प्राप्त कर सकते हैं। यह समुच्चय A और B का सम्मिलन है। औपचारिक रूप में, **A और B का सम्मिलन** (union) S के उन सभी अवयवों का समुच्चय होता है जो A में या B में हैं। हम A और B के सम्मिलन को $A \cup B$ से प्रकट करते हैं। इस तरह,

$A \cup B = \{x \in S \mid x \in A$ या $x \in B\}$.

उदाहरण के लिए, यदि $A = \{1, 2\}$ और $B = \{4, 6, 7\}$, तब $A \cup B = \{1, 2, 4, 6, 7\}$.

और यदि $A = \{1, 2, 3, 4\}$ और $B = \{2, 4, 6, 8\}$ तो $A \cup B = \{1, 2, 3, 4, 6, 8\}$. यहां ध्यान दीजिए कि 2 और 4, A और B दोनों में हैं, परन्तु जब हम $A \cup B$ लिखते हैं तब हम प्रथा 2 के अनुसार इन अवयवों को केवल एक बार लिखते हैं।

क्या आप देख सकते हैं कि किसी समुच्चय A के लिए $A \cup A = A$?

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए। हल करते समय याद रखिए कि $A \subseteq B$ दिखाने के लिए आपको $x \in A \implies x \in B$ दिखाना होगा।

'$\implies$' 'निहित है' को दर्शाता है

E 2) मान लीजिए A, B, C समुच्चय S के उपसमुच्चय हैं, जहां $A \subseteq C$ और $B \subseteq C$। दिखाइए कि

क) $A \cup B \subseteq C$

ख) $A \cup B = B \cup A$

ग) $A \cup \phi = A$

अब हम सम्मिलन की परिभाषा का विस्तार करके दो से अधिक समुच्चयों का सम्मिलन परिभाषित करेंगे।

यदि $A_1, A_2, A_3, \ldots, A_k$ समुच्चय S के k उपसमुच्चय हों तो उनका सम्मिलन $A_1 \cup A_2 \cup \ldots \cup A_k$ उन अवयवों का समुच्चय है जो इन समुच्चयों में से कम से कम एक समुच्चय का सदस्य अवश्य है। अर्थात्

$A_1 \cup A_2 \cup \ldots \cup A_k = \{x \in S \mid x \in A_i$ किसी $i = 1, 2, \ldots, k$ के लिए $\}$.

व्यंजक $A_1 \cup A_2 \cup \ldots \cup A_k$ को हम संक्षेप में $\bigcup_{i=1}^{k} A_i$ लिख सकते हैं।

यदि $\wp$ समुच्चय S के उपसमुच्चयों का एक संग्रह हो तो हम $\wp$ के सभी सदस्यों के सम्मिलन को $\bigcup_{A \in \wp} A = \{x \in S \mid x \in A$ किसी $A \in \wp$ के लिए$\}$ से परिभाषित कर सकते हैं।

आइए अब हम दिए हुए दो या अधिक समुच्चयों से एक नया समुच्चय प्राप्त करने की एक अन्य वेधि पर विचार करें।

प्रतिच्छेद : यदि A और B समुच्चय S के दो उपसमुच्चय हों तो हम ऐसे अवयवों को इकट्ठा कर सकते हैं जो A और B दोनों में हों। हम इस समुच्चय को **A और B का प्रतिच्छेद** (intersection) कहते हैं, और इसे $A \cap B$ से प्रकट करते हैं। अतः

$A \cap B = \{x \in S \mid x \in A$ **और** $x \in B\}$.

इस तरह, यदि $P = \{1, 2, 3, 4\}$ और $Q = \{2, 4, 6, 8\}$, तो

$P \cap Q = \{2, 4\}$.

क्या आप देख सकते हैं कि किसी समुच्चय A के लिए $A \cap A = A$?

अब मान लीजिए $A = \{1, 2\}$ और $B = \{4, 6, 7\}$, बताइए कि $A \cap B$ क्या होगा? इस स्थिति में हम पाते हैं कि A और B का कोई प्रतिच्छेदी अवयव नहीं है। अतः $A \cap B = \phi$, यानि कि रिक्त समुच्चय।

जब दो समुच्चयों का प्रतिच्छेद ϕ होता है तो हम कहते हैं कि ये दो समुच्चय **असंयुक्त** (disjoint) (या **परस्पर असंयुक्त**) हैं। उदाहरण के लिए, समुच्चय $\{1, 4\}$ और $\{0, 5, 7, 14\}$ असंयुक्त हैं।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 3) मान लीजिए A और B समुच्चय S के उपसमुच्चय हैं। दिखाइए कि

क) $A \cap B = B \cap A$

ख) $A \subseteq A \implies A \cap B = A$

ग) $A \cap \phi = \phi$

प्रतिच्छेद की परिभाषा का विस्तार करके उसे अनेक समुच्चयों पर भी लागू किया जा सकता है। इस तरह, समुच्चय S के k उपसमुच्चयों $A_1, A_2, A_3, \ldots, A_k$ का प्रतिच्छेद है

$A_1 \cap A_2 \cap \ldots \cap A_k = \{x \in S \mid x \in A_i$, प्रत्येक $i = 1, 2, \ldots, k$ के लिए$\}$

हम व्यंजक $A_1 \cap A_2 \cap \ldots \cap A_k$ को संक्षेप में $\bigcap_{i=1}^{k} A_i$ लिख सकते हैं।

'$\forall$' 'प्रत्येक के लिए' को प्रकट करता है।

व्यापक रूप में, यदि $\wp$ समुच्चय S के उपसमुच्चयों का एक संग्रह हो तो $\wp$ के सभी सदस्यों के प्रतिच्छेद को

$\bigcap_{A \in \wp} A = \{x \in S \mid x \in A \ \forall A \in \wp\}$ से परिभाषित करते हैं।

नीचे दिए गए प्रश्नों में हमने समुच्चयों के सम्मिलन और प्रतिच्छेद के महत्वपूर्ण गुण दिए हैं।

E 4) समुच्चय S के उपसमुच्चयों A, B, C के लिए दिखाइए कि

क) $(A \cup B) \cup C = A \cup (B \cup C)$

ख) $(A \cap B) \cap C = A \cap (B \cap C)$

ग) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

घ) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

E 5) बताइए कि नीचे दिए गए कथन सत्य हैं अथवा असत्य। यदि कथन असत्य हैं तो प्रति-उदाहरण दीजिए।

क) यदि $A \subseteq B$ और $B \subseteq C$ तो $A \subseteq C$.

ख) यदि $A \not\subseteq B$ और $B \not\subseteq A$, तो A और B असंयुक्त हैं।

ग) $A \not\subseteq A \cup B$

घ) $B \subseteq A \cup B$

ङ) यदि $A \cup B = \phi$, तो $A = B = \phi$.

सम्मिलन और प्रतिच्छेद की संक्रियाओं के अतिरिक्त समुच्चयों पर एक अन्य संक्रिया है, अर्थात् अंतर लेने की संक्रिया।

अंतर : समुच्चय $A = \{1, 2, 3\}$ और $B = \{2, 3, 4\}$ लीजिए। अब A के उन सभी अवयवों का समुच्चय, जो B के अवयव नहीं हैं, $\{1\}$ है। हम इस समुच्चय को **अंतर** (difference) $A \setminus B$ कहते हैं। इसी प्रकार, अंतर $B \setminus A$, B के उन अवयवों का समुच्चय है जो A के अवयव नहीं हैं, अर्थात् $\{4\}$.

इस तरह, समुच्चय S के किन्हीं दो समुच्चयों A और B के लिए $A \setminus B = \{x \in S \mid x \in A$ और $x \notin B\}$

यदि हम एक ही समुच्चय X के अवयवों और उपसमुच्चयों पर विचार कर रहे हैं तो हम कहते हैं कि समुच्चय X **समष्टीय समुच्चय** (universal set) है। मान लीजिए X समष्टीय समुच्चय है और $A \subseteq X$. तब X के उन सभी अवयवों के समुच्चय को, जो A के सदस्य नहीं हैं, A का **पूरक** (complement) कहते हैं। इसे हम A', A^c या $X \setminus A$ से प्रकट करते हैं। इस तरह,

$A^c = \{x \in X \mid x \notin A\}$

उदाहरण के लिए, यदि $X = \{a, b, p, q, r\}$ और $A = \{a, p, q\}$, तो $A^c = \{b, r\}$.

अब आप नीचे दिए प्रश्न को हल करने का प्रयास कीजिए।

E 6) नीचे दिए गए कथन सत्य क्यों हैं?

क) A और A^c असंयुक्त हैं, अर्थात् $A \cap A^c = \phi$.

ख) $A \cup A^c = X$, जहां X समष्टीय समुच्चय है।

ग) $(A^c)^c = A$.

अब हम समुच्चय सिद्धांत की एक अति महत्वपूर्ण रचना पर विचार करेंगे।

1.3 कार्तीय गुणनफल (Cartesian Product)

दो दिए हुए समुच्चयों से हम एक रोचक समुच्चय बना सकते हैं, अर्थात् उनका **कार्तीय गुणनफल**, जोकि फ्रांसीसी दार्शनिक और गणितज्ञ रने देकार्त (1596-1650) के नाम पर रखा गया है। उन्होंने कार्तीय निर्देशांक पद्धति का आविष्कार भी किया था।

मान लीजिए A और B दो समुच्चय हैं। युग्म (a, b) लीजिए, जिसका पहला अवयव A में है और दूसरा अवयव B में है। तब (a, b) को **क्रमित युग्म** (ordered pair) कहते हैं। क्रमित युग्म में अवयवों के लिखने का क्रम महत्वपूर्ण है। इस तरह, (a, b) और (b, a) अलग-अलग क्रमित युग्म हैं। **दो क्रमित युग्मों (a, b) और (c, d) को बराबर (अथवा समान) कहते हैं यदि $a = c$ और $b = d$।**

परिभाषा : समुच्चयों A और B का **कार्तीय गुणनफल** $A \times B$ सभी संभव क्रमित युग्मों (a, b) का समुच्चय है, जहां $a \in A, b \in B$.

उदाहरण के लिए, यदि $A = \{1, 2, 3\}$ और $B = \{4, 6\}$, तो

$A \times B = \{(1, 4), (1, 6), (2, 4), (2, 6), (3, 4), (3, 6)\}$.

साथ ही ध्यान दीजिए कि

$B \times A = \{(4, 1), (4, 2), (4, 3), (6, 1), (6, 2), (6, 3)\}$

और $A \times B \neq B \times A$.

आइए अब हम कार्तीय गुणनफल के बारे में कुछ टिप्पणी दें।

टिप्पणी : i) $A \times B = \phi$ यदि और केवल यदि $A = \phi$ या $B = \phi$,

ii) यदि A में m अवयव हों और B में n अवयव हों तो $A \times B$ में mn अवयव होते हैं। $B \times A$ में भी mn अवयव होते हैं। परन्तु, यह आवश्यक नहीं है कि $B \times A$ और $A \times B$ के अवयव समान हों, जैसा कि आप अभी देख चुके हैं।

हम दो से अधिक समुच्चयों के कार्तीय गुणनफल की परिभाषा भी इसी प्रकार दे सकते हैं। इस तरह, यदि $A_1, A_2, \ldots, A_n$, n समुच्चय हों तो

$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, \ldots, a_n \in A_n\}$

उनका कार्तीय गुणनफल होगा। उदाहरण के लिए, यदि **R** सभी वास्तविक संख्याओं का समुच्चय हो, तो

$$\mathbf{R} \times \mathbf{R} = \{(a_1, a_2) \mid a_1 \in \mathbf{R}, a_2 \in \mathbf{R}\}$$

$$\mathbf{R} \times \mathbf{R} \times \mathbf{R} = \{(a_1, a_2, a_3) \mid a_i \in \mathbf{R} \ \forall\ i = 1, 2, 3\},$$

आदि-आदि। प्रायः $\mathbf{R} \times \mathbf{R}$ के लिए $\mathbf{R}^2$ और $\mathbf{R} \times \ldots \times \mathbf{R}$ (n बार) के लिए $\mathbf{R}^n$ लिखा जाता है

आप जानते हैं कि समतल के प्रत्येक बिन्दु के दो निर्देशांक होते हैं, x और y, और आप यह भी जानते हैं कि वास्तविक संख्याओं का प्रत्येक क्रमित युग्म (x, y) समतल के किसी बिन्दु के निर्देशांकों को परिभाषित करता है। इस तरह, हम कह सकते हैं कि $\mathbf{R}^2$ एक समतल को निरूपित करता है। वास्तव में, $\mathbf{R}^2$, x-अक्ष और y-अक्ष का कार्तीय गुणनफल है। इसी प्रकार, $\mathbf{R}^3$ एक त्रिविम समष्टि को निरूपित करता है और $\mathbf{R}^n$, जहां $n \geq 1$, एक n-विम समष्टि को निरूपित करता है। ध्यान दीजिए कि **R** एक रेखा को निरूपित करता है।

अब आप नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 7) यदि $A = \{2, 5\}$, $B = \{2, 3\}$, तो $A \times B$, $B \times A$ और $A \times A$ ज्ञात कीजिए।

E 8) यदि $A \times B = \{(7, 2), (7, 3), (7, 4), (2, 2), (2, 3), (2, 4)\}$, तो A और B ज्ञात कीजिए।

E 9) सिद्ध कीजिए कि $(A \cup B) \times C = (A \times C) \cup (B \times C)$, और $(A \cap B) \times C = (A \times C) \cap (B \times C)$.

आइए अब हम कार्तीय गुणनफलों के कुछ उपसमुच्चयों पर विचार करें।

1.4 संबंध

आप व्यक्तियों के बीच के संबंध की संकल्पना से परिचित हैं। उदाहरण के लिए, दो व्यक्तियों A और B में माता (पिता)—संतान का संबंध होता है यदि और केवल यदि A, B की संतान हो या B, A की संतान हो।

गणित में किसी समुच्चय S पर संबंध R का अर्थ है समुच्चय S के अवयवों में परस्पर संबंध। यदि इस संबंध से $a \in S$ और $b \in S$ संबंधित हो तो हम aRb या $(a, b) \in R$ लिखते हैं। संकेत $(a, b) \in R$ से हम पाते हैं कि $R \subseteq S \times S$. और ठीक इसी प्रकार से हम एक समुच्चय पर संबंध को परिभाषित करते हैं।

परिभाषा : समुच्चय S पर **संबंध** (relation) R, $S \times S$ का एक उपसमुच्चय होता है।

उदाहरण के लिए, यदि **N** प्राकृतिक संख्याओं का समुच्चय हो और R संबंध "का गुणज है" तो 15 R 5, परन्तु 5 R 15 नहीं। अर्थात् $(15, 5) \in R$ परन्तु $(5, 15) \notin R$, यहां $R \subseteq \mathbf{N} \times \mathbf{N}$.

और, यदि **Q** सभी परिमेय संख्याओं का समुच्चय हो और R संबंध "से बड़ा है" हो, तो 3 R 2 (क्योंकि $3 > 2$).

नीचे दिया गया प्रश्न इन्हीं संबंधों पर आधारित है।

E 10) मान लीजिए **N** सभी प्राकृतिक संख्याओं का समुच्चय है और R संबंध $\{(a, a^2) \mid a \in \mathbf{N}\}$ है। बताइए कि नीचे दिए गए कथन सत्य हैं अथवा असत्य।

क) 2 R 3, ख) 3 R 9, ग) 9 R 3.

अब हम कुछ विशेष प्रकार के संबंधों पर विचार करेंगे।

परिभाषा : समुच्चय S पर परिभाषित संबंध R को

i) **स्वतुल्य** (reflexive) कहते हैं यदि $a R a \ \forall \ a \in S$.

ii) **सममित** (symmetric) कहते हैं यदि $a R b \implies b R a \ \forall \ a, b \in S$.

iii) **संक्रामक** (transitive) कहते हैं यदि $a R b$ और $b R c \implies a R c \ \forall \ a, b, c \in S$.

इन संकल्पनाओं से अच्छी तरह से परिचित होने के लिए नीचे दिए गए उदाहरणों पर विचार कीजिए।

उदाहरण 1 : Z पर संबंध R लीजिए जो '$a R b$ यदि और केवल यदि $a > b$' से परिभाषित है। बताइए कि R स्वतुल्य, सममित और संक्रामक है या नहीं।

हल : चूंकि $a > a$ सत्य नहीं है, इसलिए $a R a$ सत्य नहीं होगा। अतः R स्वतुल्य नहीं है।

यदि $a > b$ तो निश्चय ही $b > a$ सत्य नहीं होगा। अर्थात् $a R b$, $b R a$ को निहित नहीं करता। अतः R सममित नहीं है।

अब, यदि $a > b$ और $b > c$ तो $a > c$. यानि कि $a R b$ और $b R c \implies a R c$. इस तरह, R संक्रामक है।

उदाहरण 2 : मान लीजिए S एक अरिक्त समुच्चय है। यह भी मान लीजिए कि $\wp(S)$, S के सभी उपसमुच्चयों के समुच्चय को प्रकट करता है, अर्थात्

$\wp(S) = \{A \mid A \subseteq S\}$.

$\wp(S)$ पर संबंध R को

$R = \{(A, B) \mid A, B \in \wp(S)$ और $A \subseteq B\}$

से परिभाषित कीजिए।

बताइए कि R स्वतुल्य, सममित या संक्रामक है या नहीं।

हल : चूंकि $A \subseteq A \ \forall A \in \wp(S)$, इसलिए R स्वतुल्य है।

यदि $A \subseteq B$, तो यह आवश्यक नहीं है कि B, A में आविष्ट हो। (वास्तव में, $A \subseteq B$ और $B \subseteq A \iff A = B$) इस तरह, हम यह पाते हैं कि R सममित नहीं है।

यदि $A \subseteq B$ और $B \subseteq C$, तो $A \subseteq C \ \forall A, B, C \in \wp(S)$. इस तरह हम पाते हैं कि R संक्रामक है।

अब शायद आप नीचे दिए गए प्रश्नों को हल करना चाहेंगे।

E 11) संबंध $R \subseteq N \times N$ निम्न रूप से परिभाषित है:

$(a, b) \in R$ यदि और केवल यदि 5, $(a - b)$ को विभाजित करता हो। क्या R स्वतुल्य है? सममित है? संक्रामक है?

E 12) कुछ उदाहरणों से बताइए कि E 10 का संबंध स्वतुल्य, सममित अथवा संक्रामक क्यों नहीं है।

E 11 का संबंध स्वतुल्य, सममित और संक्रामक है। ऐसे संबंध को **तुल्यता संबंध** (equivalence relation) कहते हैं।

समुच्चय S पर परिभाषित तुल्यता संबंध का एक अति महत्वपूर्ण गुण है कि यह S को अनेक परस्पर असंयुक्त उपसमुच्चयों में विभाजित करता है, अर्थात् यह S को विभाजित करता है। आइए देखें कि यह कैसे होता है?

मान लीजिए R समुच्चय S पर एक तुल्यता संबंध है। मान लीजिए $a \in S$. तब समुच्चय $\{b \in S \mid a R b\}$ को S में a का **तुल्यता-वर्ग** (equivalence class) कहते हैं। यह S के उन अवयवों का समुच्चय है जो a से संबंधित हैं। हम इसे [a] या $\bar{a}$ से प्रकट करते हैं।

उदाहरण के लिए, बताइए कि E 11 में दिए गए R के लिए तुल्यता-वर्ग क्या है?

यह है

$[1] = \{n \mid 1\ R\ n, n \in N\}$

$= \{n \mid n \in N$ और 5, $(1-n)$ को विभाजित करता है$\}$

$= \{n \mid n \in N$ और 5, $(n-1)$ को विभाजित करता है$\}$

$= \{1, 6, 11, 16, 21, \ldots\ldots\ldots\}$

इसी प्रकार

$[2] = \{n \mid n \in N$ और 5, $(n-2)$ को विभाजित करता है

$= \{2, 7, 12, 17, 22, \ldots\ldots\ldots\}$,

$[3] = \{3, 8, 13, 18, 23, \ldots\ldots\ldots\}$,

$[4] = \{4, 9, 14, 19, 24, \ldots\ldots\ldots\}$,

$[5] = \{5, 10, 15, 20, 25, \ldots\ldots\ldots\}$,

$[6] = \{1, 6, 11, 16, 21, \ldots\ldots\ldots\}$,

$[7] = \{2, 7, 12, 17, 22, \ldots\ldots\ldots\}$.

ध्यान दीजिए कि

i) [1] और [6] असंयुक्त नहीं हैं। वास्तव में, $[1] = [6]$. इसी प्रकार, $[2] = [7]$, आदि-आदि।

ii) $N = [1] \cup [2] \cup [3] \cup [4] \cup [5]$, और दाएं पक्ष के समुच्चय परस्पर असंयुक्त हैं।

अब हम इन तथ्यों को व्यापक रूप में निम्नलिखित प्रमेय में सिद्ध करेंगे।

प्रमेय 1 : मान लीजिए R समुच्चय S पर एक तुल्यता संबंध है। $a \in S$ के लिए मान लीजिए कि $[a]$, a के तुल्यता-वर्ग को प्रकट करता है। तो

'$\Longleftrightarrow$' "निहित है और से निहित है" को प्रकट करता है।

क) $a \in [a]$,

ख) $b \in [a] \Longleftrightarrow [a] = [b]$,

ग) $S = \bigcup_{a \in S} [a]$,

घ) $a, b \in S$ के लिए, $[a] \cap [b] = \phi$ या $[a] = [b]$.

उपपत्ति : क) R एक तुल्यता संबंध है, इसलिए यह स्वतुल्य है।

$\therefore a\,R\,a \;\forall a \in S. \quad \therefore a \in [a]$.

ख) सबसे पहले यह मान लीजिए कि $b \in [a]$. हम दिखाएंगे कि $[a] \subseteq [b]$ और $[b] \subseteq [a]$. इसके लिए मान लीजिए $x \in [a]$. तब $x\,R\,a$. हम यह भी जानते हैं कि $a\,R\,b$. इस तरह, R की संक्रामकता से $x\,R\,b$, अर्थात् $x \in [b]$. $\therefore [a] \subseteq [b]$.

इसी प्रकार हम दिखा सकते हैं कि $[b] \subseteq [a]$.

$\therefore [a] = [b]$.

विलोमतः, मान लीजिए कि $[a] = [b]$. तब $b \in [b] = [a]$.

$\therefore b \in [a]$.

ग) $[a] \subseteq S \;\forall a \in S$, इसलिए $\bigcup_{a \in S} [a] \subseteq S$ (देखिए E2).

विलोमतः, मान लीजिए $x \in S$. तब ऊपर के (क) के अनुसार $x \in [x]$. $[x]$ संग्रह के उन समुच्चयों में एक समुच्चय है, जिनका सम्मिलन $\bigcup_{a \in S} [a]$ है। अतः $x \in \bigcup_{a \in S} [a]$. इसलिए $S \subseteq \bigcup_{a \in S} [a]$.

इस तरह, $S \subseteq \bigcup_{a \in S} [a]$ और $\bigcup_{a \in S} [a] \subseteq S$, जिससे (ग) सिद्ध हो जाता है।

घ) मान लीजिए $[a] \cap [b] \neq \phi$. मान लीजिए $x \in [a] \cap [b]$. तब $x \in [a]$ और $x \in [b]$.

$\Longrightarrow [x] = [a]$ और $[x] = [b]$, ऊपर के (ख) के अनुसार।

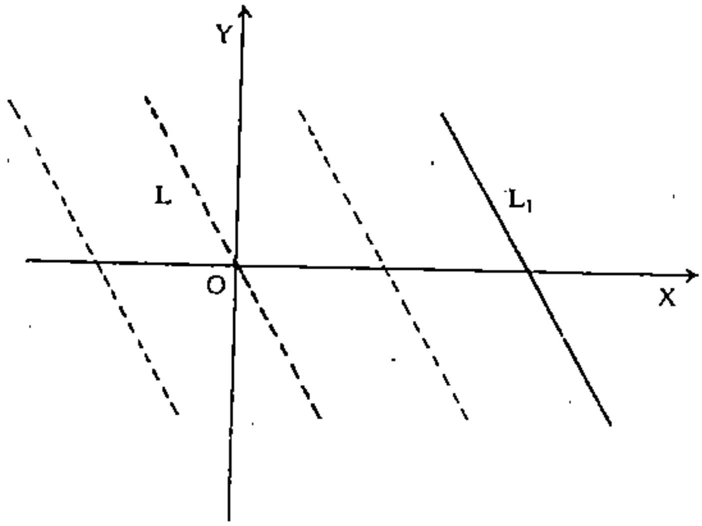
$\Longrightarrow [a] = [b]$.

ध्यान दीजिए कि प्रमेय 1 में (ग) के दाएं पक्ष के अलग-अलग समुच्चय (घ) के कारण परस्पर असंयुक्त हैं। अतः (ग) दिखाता है कि हम S को S के परस्पर असंयुक्त उपसमुच्चयों के सम्मिलन के रूप में कैसे व्यक्त कर सकते हैं। (ग) से हमें तुल्यता-वर्गों में S का एक विभाजन प्राप्त होता है।

आइए अब हम एक समुच्चय को तुल्यता-वर्गों में विभाजित करने से संबंधित कुछ और उदाहरणों पर विचार करें।

उदाहरण 3 : मान लीजिए S, $R \times R$ में सरल रेखाओं का एक समुच्चय है। S पर संबंध "$L_1 R L_2$ यदि और केवल यदि $L_1 = L_2$ या L_1, L_2 के समांतर हों" लीजिए और दिखाइए कि R एक तुल्यता संबंध है। S में तुल्यता-वर्ग कौन-कौन से हैं?

हल : R स्वतुल्य, सममित और संक्रामक है। इसलिए R एक तुल्यता संबंध है। अब एक रेखा L_1 लीजिए (देखिए चित्र1)।



चित्र 1 : L_1 का तुल्यता वर्ग

मान लीजिए L एक रेखा है जो (0, 0) से होकर जाती है और जो L_1 के समांतर है। तब $L \in [L_1]$. इस तरह, $[L] = [L_1]$. इस प्रकार, (0, 0) से होकर जाने वाली अलग-अलग रेखाओं से S के अलग-अलग तुल्यता वर्ग प्राप्त होते हैं। प्रत्येक तुल्यता वर्ग में वे सभी रेखाएं होती हैं, जो L के समांतर हैं।

अब एक प्रश्न आपके लिए!

E 13) दिखाइए कि 'a R b यदि और केवल यदि $|a| = |b|$', Z पर एक तुल्यता संबंध है। [0] और [1] क्या हैं?

अगले भाग में हम उस संकल्पना पर संक्षिप्त चर्चा करेंगे, जिससे आप पहले से ही परिचित हैं, अर्थात् फलन।

1.5 फलन

आपको याद होगा कि एक अरिक्त समुच्चय A से एक अरिक्त समुच्चय B तक का फलन f एक नियम है जो A के प्रत्येक अवयव के साथ B के ठीक एक अवयव का संबंध स्थापित करता है। इसे $f: A \to B$ के रूप में लिखा जाता है। यदि f, $a \in A$ के साथ B के अवयव b का संबंध स्थापित करता हो तो हम $f(a) = b$ लिखते हैं। A को f का **प्रांत** (domain) कहते हैं और समुच्चय $f(A) = \{f(a) \mid a \in A\}$ को f का **परिसर** (range) कहते हैं। f का परिसर B का एक उपसमुच्चय होता है, अर्थात् $f(A) \subseteq B$. B को f का **सहप्रांत** (codomain) कहते हैं।

ध्यान दीजिए कि

i) A के प्रत्येक अवयव के साथ हम B का कोई अवयव संबंधित करते हैं।

ii) A के प्रत्येक अवयव के साथ हम B का केवल एक ही अवयव संबंधित करते हैं।

iii) A के दो या अधिक अवयवों के साथ हम B का एक अवयव संबंधित कर सकते हैं।

उदाहरण के लिए, मान लीजिए $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. $f : A \to B$ को $f(1) = 1, f(2) = 4, f(3) = 9$ से परिभाषित कीजिए। तब f एक फलन होता है, जिसका प्रांत A है और परिसर $\{1, 4, 9\}$ है। इस स्थिति में हम प्रत्येक $x \in A$ के लिए $f(x) = x^2$ या $f : A \to B : f(x) = x^2$ भी लिख सकते हैं। प्रायः हम इस संकेत का प्रयोग किसी भी फलन को परिभाषित करने के लिए करेंगे।

यदि हम $g : A \to B$ को $g(1) = 1, g(2) = 1, g(3) = 4$ से परिभाषित करें तो g भी एक फलन है। g और f के प्रांत समान हैं, परन्तु g का परिसर $\{1, 4\}$ है।

टिप्पणी : हम फलन $f : A \to B$ को $A \times B$ का उपसमुच्चय $\{(a, f(a)) \mid a \in A\}$ भी मान सकते हैं।

"f एकैकी है" को 'f, 1-1 है' भी लिख सकते हैं

आइए हम कुछ विशेष गुणों वाले फलनों पर विचार करें।
परिभाषा : फलन $f : A \to B$ को **एकैकी** (one-one or injective) कहते हैं, यदि f, A के विभिन्न अवयवों को B के विभिन्न अवयवों के साथ संबंधित करता हो, अर्थात् यदि $a_1, a_2 \in A$ और $a_1 \neq a_2$, तो $f(a_1) \neq f(a_2)$. दूसरे शब्दों में, f, 1-1 है यदि $f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$.

ऊपर दिए गए उदाहरणों में फलन f एकैकी है। फलन g एकैकी फलन नहीं है क्योंकि 1 और 2, A के अलग-अलग अवयव हैं। परन्तु $g(1) = g(2)$.

अब आप समुच्चयों और फलनों से संबंधित एक अन्य उदाहरण पर विचार करें।

मान लीजिए $A = \{1, 2, 3\}$ और $B = \{p, q, r\}$. मान लीजिए $f : A \to B$, $f(1) = q, f(2) = r, f(3) = p$ से परिभाषित हैं। तब f एक फलन है। यहां f का परिसर = B = f का सहप्रांत। यह आच्छादक फलन का एक उदाहरण है, जैसा कि अब आप देखेंगे।
परिभाषा : फलन $f : A \to B$ को **आच्छादक** (onto or surjective) कहते हैं, यदि f का परिसर B हो, अर्थात् प्रत्येक $b \in B$ के लिए एक ऐसा $a \in A$ हो जिससे कि $f(a) = b$. दूसरे शब्दों में, f आच्छादक है यदि $f(A) = B$.

आच्छादक फलन के एक अन्य महत्वपूर्ण उदाहरण के लिए दो अरिक्त समुच्चय A और B लीजिए। हम एक फलन $\pi_1 : A \times B \to A : \pi_1((a, b)) = a$ को परिभाषित करते हैं। π_1 को A पर $A \times B$ का **प्रक्षेप** (projection) कहते हैं। आप यह भी देख सकते हैं कि π_1 का परिसर A है। अतः π_1 आच्छादक है। इसी प्रकार, $\pi_2 : A \times B \to B : \pi_2((a, b)) = b$, B पर $A \times B$ का प्रक्षेप है और एक आच्छादक फलन है।

यदि कोई फलन एकैकी और अच्छादक दोनों हो, तो उसे **एकैकी आच्छादक** (bijective) कहते हैं। आप इस प्रकार के फलन का प्रयोग इस पाठ्यक्रम के खंड 2 में काफ़ी करेंगे।

निम्नलिखित उदाहरण पर विचार कीजिए। इसका प्रयोग आप बार-बार करेंगे।

उदाहरण 4 : मान लीजिए A एक समुच्चय है। फलन $I_A : A \to A : I_A(a) = a$ को A पर **तत्समक फलन** (identity function) कहते हैं। दिखाइए कि I_A एकैकी आच्छादक है।

हल : किसी $a \in A$ के लिए $I_A(a) = a$. अतः I_A का परिसर A है। अर्थात् I_A आच्छादक है। I_A, 1-1 भी है क्योंकि यदि $a_1, a_2 \in A$ और $a_1 \neq a_2$ तो $I_A(a_1) \neq I_A(a_2)$.
इस तरह हम पाते हैं कि I_A एकैकी आच्छादक है।

यदि $f : A \to B$ एकैकी आच्छादक है। तो हम **समुच्चय A और B को तुल्य भी कहते हैं**। जो समुच्चय किसी $n \in N$ के लिए समुच्चय $\{1, 2, 3, \ldots, n\}$ के तुल्य है, **परिमित** (finite) समुच्चय कहलाता है। जो समुच्चय परिमित नहीं है, **अंनत** (infinite) समुच्चय कहलाता है।
प्रथा : रिक्त समुच्चय ϕ को परिमित समुच्चय माना जाता है।

अब आप नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 14) मान लीजिए $f : N \to N : f(n) = n + 5$ से परिभाषित है। सिद्ध कीजिए कि f एकैकी है, परन्तु आच्छादक नहीं।

E 15) मान लीजिए $f : Z \to Z : f(n) = n + 5$ से परिभाषित है। सिद्ध कीजिए कि f एकैकी आच्छादक है।

अगले प्रश्न में एक ऐसे फलन का उल्लेख किया गया है, जिसका प्रयोग आप बार-बार करेंगे। यह फलन है **अचर फलन** $f : A \to B : f(a) = c$, जहां c, B का एक नियत अवयव है।

E 16) यदि अचर फलन $f : X \to \{c\}$ एकैकी हो, तो X को कैसा होना चाहिए? क्या f आच्छादक है?

आइए, अब हम देखें कि फलन का प्रतिलोम प्रतिबिंब क्या होता है।

परिभाषा : मान लीजिए A और B दो समुच्चय हैं और $f : A \to B$ एक फलन है। तब B के किसी उपसमुच्चय S के लिए **f के अधीन S का प्रतिलोम प्रतिबिंब** समुच्चय $f^{-1}(S) = \{a \in A \mid f(a) \in S\}$ होता है।

उदाहरण के लिए, $I_A^{-1}(A) = \{a \in A \mid I_A(a) \in A\} = A$. और E 14 के फलन f के लिए

$f^{-1}(\{1, 2, 3\}) = \{n \in N \mid f(n) \in \{1, 2, 3\}\}$

$= \{n \in N \mid n + 5 \in \{1, 2, 3\}\}$

$= \phi$, यानि कि रिक्त समुच्चय।

परन्तु $f^{-1}(N) = \{6, 7, 8, \ldots\}$

अब हम फलन के प्रतिलोम प्रतिबिंब से संबंधित एक प्रमेय देंगे।

प्रमेय 2 : मान लीजिए $f : A \to B$ एक फलन है। तब,

क) B के किसी उपसमुच्चय S के लिए, $f(f^{-1}(S)) \subseteq S$.

ख) A के किसी उपसमुच्चय X के लिए, $X \subseteq f^{-1}(f(X))$.

उपपत्ति : हम (क) सिद्ध करेंगे और आप (ख) सिद्ध कर सकते हैं (देखिए E17)। मान लीजिए $b \in f(f^{-1}(S))$. तब परिभाषा के अनुसार, $\exists\ a \in f^{-1}(S)$ जिससे कि $b = f(a)$. परन्तु $a \in f^{-1}(S) \implies f(a) \in S$. अर्थात् $b \in S$.

इस तरह, $f(f^{-1}(S)) \subseteq S$.

E 17 को हल करने पर यह प्रमेय पूरी तरह से सिद्ध हो जाएगा।

E 17) प्रमेय 2 (ख) सिद्ध कीजिए।

E 18) यदि $f : A \to B$ और $S, T \subseteq B$, तो दिखाइए कि

क) $S \subseteq T \implies f^{-1}(S) \subseteq f^{-1}(T)$

ख) $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$

ग) $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$.

आइए अब हम दिए हुए फलनों से नए फलन प्राप्त करने की अतिमहत्वपूर्ण विधि पर विचार करें।

फलनों का संयोजन

यदि $f : A \to B$ और $g : C \to D$ फलन हों और यदि f का परिसर C का उपसमुच्चय हो, तो g और f को मिलाकर एक नया फलन $h : A \to D$ प्राप्त करने की एक सामान्य विधि है। आइए देखें कि यह क्या है।

प्रत्येक $x \in A$ के लिए $h(x)$ सूत्र

$h(x) = g(f(x))$

से परिभाषित होता है। ध्यान दीजिए कि $f(x)$, f के परिसर में है। इसलिए $f(x) \in C$. अतः $g(f(x))$ परिभाषित है और यह D का एक अवयव है। इस फलन h को हम **g और f का संयोजन** कहते हैं और इसे $g \circ f$ से दर्शाते हैं। $g \circ f$ का प्रांत A है और सहप्रांत D है। ज़्यादातर जिन स्थितियों का हम अध्ययन करेंगे उनमें $B = C$ होगा। आइए अब हम कुछ उदाहरण लें।

उदाहरण 5 : मान लीजिए $f : \mathbf{R} \to \mathbf{R}$ और $g : \mathbf{R} \to \mathbf{R}$, $f(x) = x^2$ और $g(x) = x + 1$ से परिभाषित हैं। $g_o f$ क्या है? $f_o g$ क्या है?

हल : हम पाते हैं कि f का परिसर g के प्रांत **R** का एक उपसमुच्चय है। अतः $g_o f$ परिभाषित है। परिभाषा के अनुसार $\forall\ x \in \mathbf{R}$

$g_o f(x) = g(f(x)) = f(x) + 1 = x^2 + 1.$

अब $f_o g$ को देखिए। आप देख सकते हैं कि $f_o g$ परिभाषित है और $\forall\ x \in \mathbf{R}$,

$f_o g(x) = f(g(x)) = (g(x))^2 = (x + 1)^2.$

इस तरह यह पाते हैं कि $f_o g$ और $g_o f$ दोनों ही परिभाषित हैं, परन्तु $g_o f \neq f_o g$. (उदाहरण के लिए, $g_o f(1) \neq f_o g(1)$.)

$f : A \to B$ और $g : C \to D$ बराबर हैं, यदि $A = C$ और $f(a) = g(a)\ \forall\ a \in A$.

उदाहरण 6 : मान लीजिए $A = \{1, 2, 3\}$, $B = \{p, q, r\}$ और $C = \{x, y\}$. मान लीजिए $f : A \to B$, $f(1) = p$, $f(2) = p$, $f(3) = r$ से परिभाषित है। मान लीजिए $g : B \to C$, $g(p) = x$, $g(q) = y$, $g(r) = y$ से परिभाषित है। क्या $f_o g$ और $g_o f$ परिभाषित किए जा सकते हैं?

हल : $f_o g$ परिभाषित हो, इसके लिए यह आवश्यक है कि g का परिसर f के प्रांत का उपसमुच्चय हो। इस उदाहरण में g का परिसर C है और f का प्रांत A है। और, चूंकि C, A का उपसमुच्चय नहीं है, इसलिए $f_o g$ को परिभाषित नहीं किया जा सकता।

अब f का परिसर, $\{p, r\}$, g के प्रांत B का उपसमुच्चय है। अतः हम पाते हैं कि $g_o f$ परिभाषित है, और $g_o f : A \to C$ ऐसा है कि

$g_o f(1) = g(f(1)) = g(p) = x,$

$g_o f(2) = g(f(2)) = g(p) = x,$

$g_o f(3) = g(f(3)) = g(r) = y.$

इस उदाहरण में ध्यान दें कि g आच्छादक है, और $g_o f$ भी आच्छादक है।

अब फलनों के संयोजन से संबंधित एक प्रश्न।

E 19) नीचे दिए गए प्रत्येक प्रश्न में f और g, **R** से **R** तक के फलन हैं। $f_o g$ और $g_o f$ परिभाषित कीजिए।

क) $f(x) = 5x$, $g(x) = x + 5$.

ख) $f(x) = 5x$, $g(x) = x/5$.

ग) $f(x) = |x|$, $g(x) = x^2$.

अब हम उस प्रमेय पर विचार करेंगे, जिसमें यह दिखाया गया है कि फलनों के संयोजन के प्रति तत्समक फलन का व्यवहार ठीक वैसा ही है, जैसा कि **R** में गुणन के प्रति संख्या 1 का। अर्थात् यदि हम उपयुक्त तत्समक फलन के साथ किसी फलन f का संयोजन लें तो हमें वही फलन f प्राप्त होता है।

प्रमेय 3 : मान लीजिए A एक समुच्चय है। प्रत्येक फलन $f : A \to A$ के लिए $f_o I_A = I_{A o} f = f$.

उपपत्ति : चूंकि f और I_A दोनों ही A से A तक परिभाषित हैं, इसलिए दोनों ही संयोजन $f_o I_A$ और $I_{A o} f$ परिभाषित हैं।

अब, $\forall\ x \in A$,

$f_o I_A(x) = f(I_A(x)) = f(x)$, इसलिए $f_o I_A = f$.

और, $\forall\ x \in A$, $I_{A o} f(x) = I_A(f(x))$, इसलिए $I_{A o} f = f$.

अब आप इस प्रमेय की उपपत्ति की तरह नीचे दिए गए प्रश्न को हल करने का प्रयास कर सकते हैं।

E 20) यदि A और B कोई समुच्चय हों और $g : B \to A$ हो, तो सिद्ध कीजिए कि $I_{A o} g = g$ और $g_o I_B = g$.

वास्तविक संख्याओं के संबंध में आप जानते हैं कि यदि कोई वास्तविक संख्या $x \neq 0$ दी हो तो ऐसी संख्या $y \neq 0$ है जिससे कि $xy = 1$. y को x का प्रतिलोम कहते हैं। इसी प्रकार हम फलनों के प्रतिलोम फलन परिभाषित कर सकते हैं।

परिभाषा : मान लीजिए $f : A \to B$ एक दिया हुआ फलन है। यदि एक ऐसे फलन $g : B \to A$ का **अस्तित्व हो जिससे कि** $f_\circ g = I_B$ **और** $g_\circ f = I_A$, तो हम कहते हैं कि g, f का **प्रतिलोम** है, और **हम** $g = f^{-1}$ **लिखते हैं।**

उदाहरण के लिए, $f(x) = x + 3$ से परिभाषित $f : R \to R$ लीजिए। यदि हम $g : R \to R$ को $g(x) = x - 3$ से परिभाषित करें, तो $f_\circ g\,(x) = f(g(x)) = g(x) + 3 = (x - 3) + 3 = x \; \forall x \in R$. **अतः** $f_\circ g = I_R$. आप यह भी सत्यापित कर सकते हैं कि $g_\circ f = I_R$. इसलिए $g = f^{-1}$.

ध्यान दीजिए कि इस उदाहरण में f, 3 को x में जोड़ता है और g इसका विपरीत कार्य करता है, **अर्थात्** g, 3 को x से घटाता है। इस तरह हम देखते हैं कि किसी दिए हुए फलन का प्रतिलोम ज्ञात **करने की विधि है:** $f(x)$ से x को प्राप्त करने का प्रयास कीजिए।

उदाहरण के लिए, मान लीजिए $f : R \to R : f(x) = 3x + 5$ से परिभाषित है। हम $3x + 5$ से x **कैसे** प्राप्त कर सकते हैं? इसका उत्तर है कि "पहले 5 घटाइए और फिर 3 से भाग दीजिए"।

अतः हम $g(x) = \dfrac{x-5}{3}$ लेते हैं और पाते हैं कि किसी $x \in R$ के लिए

$$g_\circ f\,(x) = g(f(x)) = \frac{f(x)-5}{3} = \frac{(3x+5)-5}{3} = x.$$

और $f_\circ g\,(x) = 3(g(x)) + 5 = 3\left(\dfrac{x-5}{3}\right) + 5 = x.$

आइए देखें कि फलन का प्रतिलोम प्राप्त करने की प्रक्रिया को आपने ठीक से समझ लिया है या नहीं।

E 21) $f : R \to R : f(x) = \dfrac{x}{3}$ का प्रतिलोम क्या है?

क्या सभी फलनों के प्रतिलोम होते हैं? नहीं, जैसा कि अगले उदाहरण से पता चलता है।

उदाहरण 7 : अचर फलन $f : R \to R : f(x) = 1$ लीजिए। f का प्रतिलोम क्या है?

हल : यदि f का प्रतिलोम $g : R \to R$ हो, तो $f_\circ g = I_R$, अर्थात् $\forall x \in R$, $f_\circ g\,(x) = x$. विशेष रूप से, $f_\circ g(5) = 5$, अर्थात् $f(g(5)) = 5$. परन्तु $f(g(5)) = 1$, क्योंकि $f(x) = 1 \; \forall x \in R$. इस तरह हमें एक अंतर्विरोध प्राप्त होता है। अतः f का कोई प्रतिलोम नहीं है।

इस उदाहरण को देखकर हमारे मन में एक स्वाभाविक प्रश्न उठ सकता है कि f के प्रतिलोम के अस्तित्व के लिए आवश्यक और पर्याप्त प्रतिबंध क्या है? इस प्रश्न का उत्तर निम्नलिखित प्रमेय से प्राप्त होता है।

प्रमेय 4 : फलन $f : A \to B$ का प्रतिलोम होता है यदि और केवल यदि f एकैकी आच्छादक हो।

उपपत्ति : सबसे पहले यह मान लीजिए कि f एकैकी आच्छादक है। हम एक फलन $g : B \to A$ को परिभाषित करेंगे और सिद्ध करेंगे कि $g = f^{-1}$. मान लीजिए $b \in B$. चूंकि f आच्छादक है, इसलिए ऐसा $a \in A$ होता है जिससे कि $f(a) = b$. चूंकि f एकैकी है, अतः केवल एक ही ऐसा $a \in A$ होगा। हम A के इस अद्वितीय अवयव a को $g(b)$ मानते हैं। अर्थात् यदि $b \in B$, तो हम $g(b) = a$ परिभाषित करते हैं, जहां $f(a) = b$.

ध्यान दीजिए कि f आच्छादक है, इसलिए $B = \{f(a) \mid a \in A\}$. तब हम केवल $g : B \to A$ को $g(f(a)) = a$ से परिभाषित कर रहे हैं। परिभाषा से ही हम देख सकते हैं कि $g_\circ f = I_A$.

अब मान लीजिए $b \in B$ **और** $g(b) = a$. तब g की परिभाषा के अनुसार $f(a) = b$. इसलिए $f_\circ g\,(b) = f(g(b)) = f(a) = b$. **अतः** $f_\circ g = I_B$.

इसलिए $f_\circ g = I_B$ **और** $g_\circ f = I_A$.
इससे सिद्ध होता है कि $g = f^{-1}$.

विलोमतः, मान लीजिए f का एक प्रतिलोम है और $g = f^{-1}$. हमें यह सिद्ध करना है कि f एकैकी और आच्छादक है।

मान लीजिए $f(a_1) = f(a_2)$. तब $g(f(a_1)) = g(f(a_2))$.

$g \circ f$, 1 − 1 है $\Longrightarrow$ f, 1 − 1 है।

$\Longrightarrow g \circ f(a_1) = g \circ f(a_2)$

$\Longrightarrow a_1 = a_2$, क्योंकि $g \circ f = I_A$.

अतः f एकैकी है।

अब, यदि $b \in B$ दिया हुआ हो, तो $f \circ g = I_B$, जिससे कि $f \circ g\,(b) = I_B\,(b) = b$.

$g \circ f$ आच्छादक है $\Longrightarrow$ g आच्छादक है।

अर्थात् $f(g(b)) = b$.

अर्थात् f आच्छादक है।

इस तरह, प्रमेय सिद्ध हो जाता है।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 22) निम्नलिखित फलन R से R तक हैं। प्रत्येक फलन के लिए मालूम कीजिए कि उसका प्रतिलोम है या नहीं, और यदि प्रतिलोम है तो उसे प्राप्त कीजिए।

क) $f(x) = x^2\ \forall\ x \in \mathbf{R}$.

ख) $f(x) = 0\ \forall\ x \in \mathbf{R}$.

ग) $f(x) = 11x + 7\ \forall\ x \in \mathbf{R}$.

आइए अब हम कुछ प्रारंभिक संख्या-सिद्धांत पर चर्चा करें।

1.6 संख्या-सिद्धांत के कुछ परिणाम

इस भाग में हम पूर्णांकों के गुणनखंड से संबंधित कुछ ऐसे गुणों पर विचार करेंगे, जिनका प्रयोग हम इस पाठ्यक्रम के दौरान करेंगे। इसके लिए हमें परिमित आगमन नियम को जानने की आवश्यकता है।

1.6.1 आगमन नियम (Principle of Induction)

पहले हम पूर्णांकों के एक अभिगृहीत (axiom) का कथन देंगे जिसका प्रयोग हम प्रायः करेंगे। यह है सुक्रमण सिद्धांत (well-ordering principle). हम एक परिभाषा से शुरू करते हैं।

परिभाषा : मान लीजिए S, **Z** का एक अरिक्त उपसमुच्चय है। अवयव $a \in S$ को S का **न्यूनतम अवयव** (least element, minimum element) कहते हैं यदि $a \leq b\ \forall\ b \in S$.

उदाहरण के लिए, 1, **N** का एक न्यूनतम अवयव है। परन्तु **Z** का कोई न्यूनतम अवयव नहीं है। वास्तव में, **Z** के अनेक उपसमुच्चयों, जैसे $2\mathbf{Z}$, $\{-1, -2, -3, \ldots\}$, आदि, के कोई न्यूनतम अवयव नहीं हैं।

नीचे दिए गए अभिगृहीत से हमें ऐसे कुछ समुच्चयों के बारे में पता चलता है, जिनके न्यूनतम अवयव हैं।

सुक्रमण सिद्धांत : **N** के प्रत्येक अरिक्त उपसमुच्चय का एक न्यूनतम अवयव होता है।

आपको जानकर शायद आश्चर्य होगा कि यह सिद्धांत परिमित आगमन नियम के तुल्य है, जिसका कथन हम अब दे रहे हैं।

प्रमेय 5 : मान लीजिए $S \subseteq \mathbf{N}$, जहां

i) $1 \in S$, और

ii) जब भी $k \in S$, तब, $k + 1 \in S$.

तब $S = \mathbf{N}$.

और, यह प्रमेय अगले प्रमेय के तुल्य है।

प्रमेय 6 : मान लीजिए $S \subseteq N$, जहां

i) $1 \in S$, और

ii) यदि $m \in S \; \forall \; m < k$, तब $k \in S$.

तब $S = N$.

इस पाठ्यक्रम में हम सुक्रमण सिद्धांत और प्रमेय 5 तथा प्रमेय 6 की तुल्यता को सिद्ध नहीं करेंगे, क्योंकि इसकी उपपत्ति कुछ जटिल है।

आइए अब हम प्रमेय 5 और प्रमेय 6 को उन रूपों में लिखें, जिनमें हम अक्सर उनका प्रयोग करेंगे।

प्रमेय 5': मान लीजिए $P(n)$ धन पूर्णांक n के बारे में एक कथन है, जहां

i) $P(1)$ सत्य है, और

ii) यदि किसी $k \in N$ के लिए $P(k)$ सत्य है, तो $P(k+1)$ भी सत्य होगा।

तब $P(n)$ सभी $n \in N$ के लिए सत्य होगा।

प्रमेय 6': मान लीजिए $P(n)$ धन पूर्णांक n के बारे में एक कथन है, जहां

i) $P(1)$ सत्य है, और

ii) यदि $P(n)$ सभी धन पूर्णांकों $m < k$ के लिए सत्य है तो $P(k)$ भी सत्य होगा।

तब $P(n)$ सभी $n \in N$ के लिए सत्य होगा।

ऊपर दिए गए तुल्य कथन बीजगणित के अनेक परिणामों को सिद्ध करने में काफी उपयोगी होते हैं। इस पाठ्यक्रम के दौरान हम आगमन नियम का प्रयोग प्रायः उस रूप में करेंगे, जिस रूप में हमें सुविधा होगी। आइए अब हम एक उदाहरण पर विचार करें।

उदाहरण 8 : सिद्ध कीजिए कि प्रत्येक $n \in N$ के लिए

$$1^3 + 2^3 + \ldots + n^3 = \frac{n^2(n+1)^2}{4}.$$

हल : मान लीजिए $S_n = 1^3 + 2^3 + \ldots + n^3$, और मान लीजिए कि

कथन $S_n = \frac{n^2(n+1)^2}{4}$, $P(n)$ है।

अब चूंकि $S_1 = \frac{1^2 \times 2^2}{4}$, इसलिए $P(1)$ सही है।

अब मान लीजिए $P(n-1)$ सही है, अर्थात् $S_{n-1} = \frac{(n-1)^2 n^2}{4}$.

$$\begin{aligned}
\text{तब } S_n &= 1^3 + \ldots + (n-1)^3 + n^3 \\
&= S_{n-1} + n^3 \\
&= \frac{(n-1)^2 n^2}{4} + n^3, \text{ क्योंकि } P(n-1) \text{ सत्य है।} \\
&= \frac{n^2[(n-1)^2 + 4n]}{4} \\
&= \frac{n^2(n+1)^2}{4}.
\end{aligned}$$

इस तरह $P(n)$ भी सत्य है। अतः आगमन नियम के अनुसार सभी $n \in N$ के लिए $P(n)$ सत्य है।

अब आप आगमन नियम का प्रयोग संख्याओं के निम्नलिखित गुण को सिद्ध करने के लिए कीजिए। इस गुण का प्रयोग आपने कई बार किया होगा।

E 23) $a, b \in R$ और $n \in N$ के लिए सिद्ध कीजिए कि $(ab)^n = a^n b^n$.

आइए अब हम पूर्णांकों के कुछ गुणनखंड गुणों पर विचार करें।

1.6.2 Z में भाज्यता

संख्या-सिद्धांत की एक मूलभूत संकल्पना पूर्णांकों की भाज्यता (divisibility) है।

परिभाषा : मान लीजिए $a, b \in Z$ और $a \neq 0$. तब हम कहते हैं कि **a, b को विभाजित करता है** यदि एक ऐसे पूर्णांक c का अस्तित्व है जिससे कि $b = ac$. इसे हम $a \mid b$ लिखते हैं, और कहते हैं कि **a, b का भाजक (या गुणनखंड) है, या b, a से भाज्य है, या b, a का गुणज है।**

यदि a, b को विभाजित न करता हो तो हम लिखते हैं $a \nmid b$.

हम निम्नलिखित प्रश्न में पूर्णांकों की भाज्यता से संबंधित कुछ गुण दे रहे हैं। इन्हें आप आसानी से सिद्ध कर सकते हैं।

E 24) मान लीजिए a, b, c शून्येतर पूर्णांक हैं, तब

क) $a \mid 0, \pm 1 \mid a, \pm a \mid a$.

ख) $a \mid b \Longrightarrow ac \mid bc$.

ग) $a \mid b$ और $b \mid c \Longrightarrow a \mid c$.

घ) $a \mid b$ और $b \mid a \Longleftrightarrow a = \pm b$.

ङ) $c \mid a$ और $c \mid b \Longrightarrow c \mid (ax + by) \; \forall \; x, y \in Z$.

अब हम एक परिणाम देंगे, जिसे सिद्ध करने के लिए हम प्रमेय 5′ का प्रयोग करेंगे।

प्रमेय 7 (विभाजन-कलन विधि): मान लीजिए $a, b \in Z, b > 0$. तब ऐसे अद्वितीय पूर्णांकों q, r का अस्तित्व है जिनसे कि $a = qb + r$, जहां $0 \le r < b$.

उपपत्ति : पहले हम सिद्ध करेंगे कि q और r का अस्तित्व है। इसके बाद हम दिखाएंगे कि ये अद्वितीय हैं। इनके अस्तित्व को सिद्ध करने के लिए हम तीन अलग-अलग स्थितियों को लेंगे : $a = 0$, $a > 0$, $a < 0$.

स्थिति 1 $(a = 0)$: $q = 0, r = 0$ लीजिए। तब $a = qb + r$.

स्थिति 2 $(a > 0)$: मान लीजिए P(n) यह कथन है कि $n = qb + r$, किसी $q, r \in Z$ के लिए, जहां $0 \le r < b$. आइए अब हम देखें कि P(1) सत्य है या नहीं।
यदि $b = 1$, तो हम $q = 1, r = 0$ ले सकते हैं, और इस तरह, $1 = 1.1 + 0$.
यदि $b > 1$, तब $q = 0, r = 1$ लीजिए, अर्थात् $1 = 0.b + 1$.

इस तरह P(1) सत्य है।

अब मान लीजिए $P(n - 1)$ सत्य है, अर्थात् किसी $q_1, r_1 \in Z$ के लिए, जहां $0 \le r_1 < b$,
$(n - 1) = q_1 b + r_1$. तब $r_1 \le b - 1$, अर्थात् $r_1 + 1 \le b$.
इसलिए

$$n = \begin{cases} q_1 b + (r_1 + 1), & \text{यदि } (r_1 + 1) < b \\ (q_1 + 1)b + 0, & \text{यदि } r_1 + 1 = b. \end{cases}$$

इससे पता चलता है कि P(n) सत्य है। अतः प्रमेय 5′ के अनुसार किसी $n \in N$ के लिए P(n) सत्य है। अर्थात् $a > 0$ के लिए

$a = qb + r$, जहां $q, r \in Z, 0 \le r < b$.
स्थिति 3 $(a < 0)$: यहां $(-a) > 0$. इसलिए स्थिति 2 के अनुसार हम
$(-a) = qb + r', 0 \le r' < b$. लिख सकते हैं।

अर्थात्

$$a = \begin{cases} (-q)b, & \text{यदि } r' = 0 \\ (-q - 1)b + (b - r'), & \text{यदि } 0 < r' < b. \end{cases}$$

इससे पूर्णांकों q, r का अस्तित्व सिद्ध हो जाता है।

अब मान लीजिए q', r' ऐसे पूर्णांक हैं, जिनसे कि $a = qb + r$ और $a = q'b + r'$, जहां $0 \leq r < b, 0 \leq r' < b$. तब $r - r' = b(q' - q)$. इस तरह, $b \mid (r - r')$. परन्तु $|r - r'| < b$. अतः $r - r' = 0$, अर्थात् $r = r'$ और फिर $q = q'$.

इस तरह, हमने q और r की अद्वितीयता को सिद्ध कर दिया है।

व्यंजक $a = qb + r$ $(0 \leq r < b)$ में r को **शेषफल** (remainder) कहते हैं जो a को b से भाग देने पर प्राप्त होता है।

आइए, अब हम गुणनखंडों पर फिर विचार करें।

परिभाषा : मान लीजिए $a, b \in \mathbf{Z}$. $c \in \mathbf{Z}$ को a और b का **सार्व भाजक** (common divisor) कहते हैं, यदि $c \mid a$ और $c \mid b$.

उदाहरण के लिए, 2 और 4 का एक सार्व भाजक 2 है। E 24 (क) से आप जानते हैं कि किसी $a, b \in Z$ के लिए, 1 और -1, a और b के सार्व भाजक हैं। इस तरह, आप देख सकते हैं कि दो पूर्णांकों के एक से अधिक सार्व भाजक होते हैं। इससे संबंधित हम एक परिभाषा देते हैं।

परिभाषा : पूर्णांक d को दो शून्येतर पूर्णांकों a और b का **महत्तम सार्व भाजक** (greatest common divisor) (संक्षेप में g.c.d.) कहते हैं, यदि

i) $d \mid a$ और $d \mid b$, और

ii) $c \mid a$ और $c \mid b \implies c \mid d$.

ध्यान दीजिए कि यदि a और b के दो g.c.d. d और d' हों तो (ii) के अनुसार $d \mid d'$ और $d' \mid d$. इस तरह, $d = \pm d'$ (देखिए E 24). इनमें से केवल एक ही धनात्मक होगा। **इस अद्वितीय धनात्मक g.c.d को (a, b) से प्रकट करते हैं।**

अब हम दिखाएंगे कि किन्हीं दो शून्येतर पूर्णांकों a और b के लिए (a, b) का अस्तित्व है। साथ ही आप सुक्रमण सिद्धांत की उपयोगिता भी देख सकेंगे।

प्रमेय 8 : दो शून्येतर पूर्णांकों a और b का g.c.d. होता है, और $(a, b) = ma + nb$ किन्हीं $m, n \in \mathbf{Z}$ के लिए।

उपपत्ति : मान लीजिए $S = \{xa + yb \mid x, y \in Z, (xa + yb) > 0\}$.
चूंकि $a^2 + b^2 > 0$, इसलिए $a^2 + b^2 \in S$. अर्थात् $S \neq \phi$. फिर सुक्रमण सिद्धांत के अनुसार S का एक न्यूनतम अवयव होगा, मान लीजिए d. अब $d = ma + nb$, किसी $m, n \in Z$ के लिए। हम दिखाएंगे कि $d = (a, b)$.

अब, चूंकि $d \in S$, इसलिए $d > 0$. अतः विभाजन-कलन विधि से हम $a = qd + r$, $0 \leq r < d$, लिख सकते हैं। इस तरह,

$r = a - qd = a - q(ma + nb) = (1 - qm)a + (-qn)b.$

अब, यदि $r \neq 0$, तो $r \in S$. लेकिन $r < d$ और d, S का न्यूनतम अवयव है। यह एक अंतर्विरोध है। अतः $r = 0$, अर्थात् $a = qd$. अर्थात् $d \mid a$. इसी प्रकार हम दिखा सकते हैं कि $d \mid b$. इस तरह d, a और b का एक सार्व भाजक है।

अब, मान लीजिए c एक पूर्णांक है जो a और b, दोनों का भाजक है।
तब, किसी $a_1, b_1 \in Z$ के लिए, $a = a_1c$, $b = b_1c$.
परन्तु, तब $d = ma + nb = ma_1c + nb_1c = (ma_1 + nb_1)c$.
अतः $c \mid d$.

इस तरह, हमने दिखाया है कि d, a और b का एक g.c.d. है। वास्तव में, यह अद्वितीय धनात्मक g.c.d. (a, b) है।

उदाहरण के लिए, 2 और 10 का g.c.d. $2 = 1.2 + 0.10$ है
और 2 तथा 3 का g.c.d $1 = (-1)2 + 1(3)$ है।

जिन पूर्णांक युग्मों का g.c.d. 1 हो, उनका एक विशेष नाम है, जिसे हम अब बताएंगे।

परिभाषा : यदि $(a, b) = 1$, तो पूर्णांकों a और b को एक-दूसरे के **सापेक्षतः अभाज्य** (relatively prime) या **असहभाज्य** (coprime) कहते हैं।

प्रमेय 8 का प्रयोग करके हम कह सकते हैं कि **a और b एक-दूसरे के असहभाज्य होते हैं यदि और केवल यदि ऐसे $m, n \in Z$ हों जिनसे कि $1 = ma + nb$.**

अगला प्रमेय हमें सापेक्षतः अभाज्य संख्याओं का एक रोचक गुण बताता है।

प्रमेय 9 : यदि $a, b, c \in Z$, $(a, b) = 1$ और $b \mid ac$, तो $b \mid c$.

उपपत्ति : हम जानते हैं कि $\exists\, m, n \in Z$ जिससे कि $1 = ma + nb$.

तब $c = c.1 = c(ma + nb) = mac + nbc$.

अब $b \mid ac$ और $b \mid bc$.

$\therefore$ $b \mid (mac + nbc)$ (E 24 (ग) से)

इस तरह, $b \mid c$.

आइए अब हम अभाज्य गुणनखंडन पर चर्चा करें।

परिभाषा : यदि प्राकृतिक संख्या $p(\neq 1)$ के भाजक केवल 1 और p हों, तो इसे **अभाज्य** (prime) कहते हैं। यदि प्राकृतिक संख्या $n(\neq 1)$ अभाज्य न हो, तो उसे **भाज्य संख्या** (composite number) कहते हैं।

उदाहरण के लिए, 2 और 3 अभाज्य संख्या हैं, जबकि 4 एक भाज्य संख्या है।

ध्यान दीजिए कि **यदि p अभाज्य है और $a \in Z$ जहां $p \nmid a$, तो $(p, a) = 1$.**

अब नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 25) यदि p अभाज्य है और $p \mid ab$, तो दिखाइए कि $p \mid a$ या $p \mid b$.

E 26) यदि p अभाज्य है और $p \mid a_1a_2 \ldots a_n$, तो दिखाइए कि किसी $i = 1, \ldots, n$ के लिए $p \mid a_i$.

अब संख्या 50 लीजिए। हम $50 = 2 \times 5 \times 5$ लिखते हैं, अभाज्यों के गुणनफल के रूप में। वास्तव में, हम किसी भी प्राकृतिक संख्या को अभाज्यों के गुणनफल के रूप में लिख सकते हैं। यही अद्वितीय अभाज्य गुणनखंड प्रमेय (unique prime factorisation theorem) का कथन है।

प्रमेय 10 (अद्वितीय अभाज्य गुणनखंडन प्रमेय) : प्रत्येक पूर्णांक $n > 1$ को $n = p_1p_2 \ldots p_n$ के रूप में लिखा जा सकता है, जहां $p_1, \ldots, p_n$ अभाज्य संख्याएं हैं। यह निरूपण अद्वितीय है, केवल अभाज्य गुणनखंडों को लिखने के क्रम को छोड़कर।

उपपत्ति : पहले हम इस प्रकार के गुणनखंडन का अस्तित्व सिद्ध करेंगे। मान लीजिए P(n) यह कथन है कि $(n + 1)$ अभाज्यों का गुणनफल है। P(1) सत्य है, क्योंकि 2 स्वयं अभाज्य संख्या है। अब मान लीजिए कि सभी धनात्मक पूर्णांकों $m < k$ के लिए P(m) सत्य है। हम यह दिखाना चाहते हैं कि P(k) सत्य है। यदि $k + 1$ अभाज्य है, तो P(k) सत्य है। यदि $k + 1$ अभाज्य नहीं है तो हम $k + 1 = m_1m_2$ लिख सकते हैं, जहां $1 < m_1 < k + 1$ और $1 < m_2 < k + 1$. परन्तु तब $P(m_1 - 1)$ और $P(m_2 - 1)$, दोनों ही सत्य हैं। इस तरह,

$m_1 = p_1p_2 \ldots p_r$, $m_2 = q_1q_2 \ldots q_s$, जहां

$p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ अभाज्य है।

इस तरह,

$k + 1 = p_1p_2 \ldots p_rq_1q_2 \ldots q_s$, अर्थात् P(k) सत्य है। अतः प्रमेय 6' के अनुसार प्रत्येक $n \in N$ के लिए P(n) सत्य है।

आइए अब हम दिखाएंगे कि यह गुणनखंडन अद्वितीय है।

मान लीजिए $n = p_1p_2 \ldots p_t = q_1q_2 \ldots q_s$, जहां

$p_1, p_2, \ldots, p_t, q_1, q_2, \ldots, q_s$ अभाज्य हैं।

अब हम t पर आगमन का प्रयोग करेंगे।

यदि $t = 1$, तो $p_1 = q_1q_2 \ldots q_s$. परन्तु p_1 अभाज्य है। इस तरह इसके गुणनखंड केवल 1 और स्वयं हैं। अतः $s = 1$ और $p_1 = q_1$.

अब मान लीजिए $t > 1$ और अद्वितीयता $(t - 1)$ अभाज्यों के किसी गुणनफल पर लागू होता है। अब $p_1 \mid q_1q_2 \ldots q_s$. इसलिए E 26 से, किसी i के लिए, $p_1 \mid q_i$. हम मान सकते हैं कि $p_1 \mid q_1$ (अगर ज़रूरी हो तो हम $q_1, \ldots, q_s$ का क्रम बदल सकते हैं)। परन्तु p_1 और q_1, दोनों ही अभाज्य हैं। इसलिए $p_1 = q_1$. परन्तु तब $p_2 \ldots p_t = q_2 \ldots q_s$. इसलिए, आगमन से $t - 1 = s - 1$ और प्रत्येक $i = 2, \ldots, t$ के लिए ऐसा j है जिससे कि $p_i = q_j$ और प्रत्येक $k = 2, \ldots, s$ के लिए ऐसा m है, जिससे कि $q_k = p_m$. इस तरह हमने गुणनखंडन की अद्वितीयता को सिद्ध कर दिया है।

किसी संख्या के अभाज्य गुणनखंडन में कोई अभाज्य संख्या दोहराई जा सकती है, जैसा कि 50 के गुणनखंडन $50 = 2 \times 5 \times 5$ में 5 दो बार आता है। यदि हम समान अभाज्य संख्याओं को इकट्ठा करें तो हम प्रमेय 10 की निम्नलिखित उपप्रमेय दे सकते हैं।

उपप्रमेय : किसी भी प्राकृतिक संख्या n को $n = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$ के रूप में अद्वितीयत: लिखा जा सकता है, जहां $i = 1, 2, \ldots, r$ के लिए प्रत्येक $m_i \in N$ और p_i एक अभाज्य संख्या है, जहां $1 < p_1 < p_2 < \ldots < p_r$

प्रमेय 10 के एक अनुप्रयोग के रूप में हम निम्नलिखित महत्वपूर्ण प्रमेय देते हैं, जिसे प्राचीन यूनानी गणितज्ञ यूक्लिड ने प्रस्तुत किया था।

प्रमेय 11 : अभाज्य संख्याओं की संख्या अपरिमित है।

उपपत्ति : मान लीजिए अभाज्य संख्याओं का समुच्चय P परिमित है, और $P = \{p_1, p_2, \ldots, p_n\}$. प्राकृतिक संख्या $n = p_1p_2 \ldots p_n + 1$ लीजिए।
अब मान लीजिए किसी $i = 1, \ldots, n$ के लिए $p_i \mid n$. तब $p_i \mid (n - p_1p_2 \ldots p_n)$. अर्थात् $p_i \mid 1$, जो एक अंतर्विरोध है। अत: कोई भी p_i, n को विभाजित नहीं करता। परन्तु, चूंकि $n > 1$, इसलिए प्रमेय 10 के अनुसार n का एक अभाज्य गुणनखंड अवश्य होगा। इस प्रकार हम एक अंतर्विरोध पर पहुंच गए हैं। इसलिए जो कथन हम मानकर चले थे, वह ग़लत है; अर्थात् अभाज्य संख्याओं का समुच्चय अपरिमित होगा।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 27) सिद्ध कीजिए कि किसी अभाज्य संख्या p के लिए $\sqrt{p}$ अपरिमेय है।

(**संकेत :** मान लीजिए $\sqrt{p}$ परिमेय है। तब $\sqrt{p} = \frac{a}{b}$, जहां $a, b \in Z$. हम मान सकते हैं कि $(a, b) = 1$ अब अभाज्य संख्याओं के जिन गुणों पर हमने चर्चा की है, उनका प्रयोग कीजिए।)

आइए अब देखें कि इस इकाई में हमने क्या किया है।

1.7 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों पर ग़ौर किया है:

1) समुच्चयों और उपसमुच्चयों के कुछ गुण।
2) समुच्चयों का सम्मिलन, प्रतिच्छेद, अंतर और पूरक।
3) समुच्चयों का कार्तीय गुणनफल।
4) व्यापक रूप में संबंध, और विशेष रूप से तुल्यता संबंध।
5) फलन, 1-1 फलन, आच्छादक फलन और एकैकी आच्छादक फलन की परिभाषा।
6) फलनों का संयोजन।
7) सुक्रमण सिद्धांत, जिसके अनुसार N के प्रत्येक उपसमुच्चय का एक न्यूनतम अवयव होता है।

8 परिमित आगमन नियम जिसके अनुसार, यदि $P(n)$ किसी $n \in N$ के बारे में एक कथन हो, जहां
   i) $P(1)$ सत्य है, और
   ii) यदि किसी $k \in N$ के लिए $P(k)$ सत्य है, तो $P(k+1)$ भी सत्य होगा,
   तब प्रत्येक $n \in N$ के लिए $P(n)$ सत्य होगा।

9) परिमित आगमन नियम का कथन इस प्रकार भी दिया जा सकता है
   यदि $P(n)$ किसी $n \in N$ के बारे में एक कथन हो, जहां
   i) $P(1)$ सत्य है और
   ii) यदि प्रत्येक धन पूर्णांक $m < k$ के लिए $P(m)$ सत्य है, तो $P(k)$ भी सत्य होगा,
   तब प्रत्येक $n \in N$ के लिए $P(n)$ सत्य होगा।
   ध्यान दीजिए कि सुक्रमण सिद्धांत और परिमित आगमन नियम तुल्य हैं।

10) Z में भाज्यता के कुछ गुण, जैसे विभाजन-कलन विधि और अद्वितीय अभाज्य गुणनखंडन।

1.8 हल/उत्तर

E 1) (क) सत्य (ख) असत्य (ग) असत्य (घ) सत्य

E 2) क) $x \in A \cup B \Rightarrow x \in A$ या $x \in B \Rightarrow x \in C$, क्योंकि $A \subseteq C$ और $B \subseteq C$.

ख) $x \in A \cup B \Leftrightarrow x \in A$ या $x \in B \Leftrightarrow x \in B$ या $x \in A \Leftrightarrow x \in B \cup A$.

$\therefore A \cup B = B \cup A$.

ग) $x \in A \cup \phi \Rightarrow x \in A$ या $x \in \phi \Rightarrow x \in A$,
क्योंकि ϕ का कोई अवयव नहीं होता।
$\therefore A \cup \phi \subseteq A$.
और $A \subseteq A \cup \phi$, क्योंकि $x \in A \Rightarrow x \in A \cup \phi$.
$\therefore A = A \cup \phi$.

E 3) क) आप इसे E 2 (ख) की तरह हल कर सकते हैं।

ख) $x \in A \cap B \Rightarrow x \in A$ और $x \in B \Rightarrow x \in A$, क्योंकि $A \subseteq B$.
$\therefore A \cap B \subseteq A$.
विलोमतः, $x \in A \Rightarrow x \in A$ और $x \in B$, क्योंकि $A \subseteq B$.
$\Rightarrow x \in A \cap B$.
$\therefore A \subseteq A \cap B$.
$\therefore A \cap B = A$.

ग) तथ्य $\phi \subseteq A$ का प्रयोग कीजिए।

E 4) क) $x \in (A \cup B) \cup C \Leftrightarrow x \in A \cup B$ या $x \in C$
$\Leftrightarrow x \in A$ या $x \in B$ या $x \in C$.
$\Leftrightarrow x \in A$ या $x \in B \cup C$
$\Leftrightarrow x \in A \cup (B \cup C)$
$\therefore (A \cup B) \cup C = A \cup (B \cup C)$

ख) आप (क) की तरह इसे हल करने का प्रयास कीजिए।

ग) $B \cap C \subseteq B \Rightarrow A \cup (B \cap C) \subseteq A \cup B$.
इसी प्रकार, $A \cup (B \cap C) \subseteq A \cup C$.
$\therefore A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.
विलोमतः, $x \in (A \cup B) \cap (A \cup C)$
$\Rightarrow x \in A \cup B$ और $x \in A \cup C$
$\Rightarrow x \in A$ या $x \in B$ और $x \in A$ या $x \in C$

$\Longrightarrow x \in A$ या $x \in B \cap C$

$\Longrightarrow x \in A \cup (B \cap C)$

$\therefore (A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

इस तरह, (ग) सिद्ध हो जाता है।

घ) (ग) की तरह इसे हल करने का प्रयास कीजिए।

E 5) क) सत्य।

ख) असत्य। उदाहरण के लिए, यदि $A = \{0, 1\}$ और $B = \{0, 2\}$, तो $A \not\subseteq B, B \not\subseteq A$ और $A \cap B = \{0\} \neq \phi$.

ग) असत्य। वास्तव में, किसी समुच्चय A के लिए, $A \subseteq A \cup B$.

घ) सत्य।

ङ) सत्य।

E 6) क) $x \in A$ यदि और केवल यदि $x \notin A^c$.

ख) चूंकि A और A^c, X के उपसमुच्चय हैं, इसलिए $A \cup A^c \subseteq X$.

विलोमतः, यदि $x \in X$ और $x \notin A$, तो $x \in A^c$.

$\therefore X \subseteq A \cup A^c$.

$\therefore X = A \cup A^c$.

ग) $x \in A \Longleftrightarrow x \notin A^c \Longleftrightarrow x \in (A^c)^c$. $\therefore A = (A^c)^c$.

E 7) $A \times B = \{(2, 2), (2, 3), (5, 2), (5, 3)\}$

$B \times A = \{(2, 2), (3, 2), (2, 5), (3, 5)\}$

$A \times A = \{(2, 2), (2, 5), (5, 2), (5, 5)\}$

E 8) पहले निर्देशांकों का समुच्चय A है। $\therefore A = \{7, 2\}$.

दूसरे निर्देशांकों का समुच्चय B है। $\therefore B = \{2, 3, 4\}$.

E 9) $(x, y) \in (A \cup B) \times C \Longleftrightarrow x \in A \cup B$ और $y \in C$

$\Longleftrightarrow x \in A$ या $x \in B$ और $y \in C$

$\Longleftrightarrow x \in A$ और $y \in C$ या $x \in B$ और $y \in C$

$\Longleftrightarrow (x, y) \in A \times C$ या $(x, y) \in B \times C$

$\Longleftrightarrow (x, y) \in (A \times C) \cup (B \times C)$.

इसी प्रकार, आप दिखा सकते हैं कि

$(A \cap B) \times C = (A \times C) \cap (B \times C)$.

E 10) क) असत्य ख) सत्य ग) असत्य

E 11) चूंकि $\forall a \in N, a - a = 0$ को 5 विभाजित करता है, इसलिए R स्वतुल्य है।

यदि $5 \mid (a - b)$, तो $5 \mid (b - a)$. $\therefore$ R सममित है।

यदि $5 \mid (a - b)$ और $5 \mid (b - c)$,

तो $5 \mid \{(a - b) + (b - c)\}$, अर्थात् $5 \mid (a - c)$.

$\therefore$ R संक्रामक है।

E 12) 2 R 2 असत्य है।

$(2, 4) \in R$, परन्तु $(4, 2) \notin R$.

$(2, 4) \in R, (4, 16) \in R$, परन्तु $(2, 16) \notin R$.

E 13) $|a| = |a| \ \forall a \in Z$. $\therefore$ R स्वतुल्य है

$|a| = |b| \Longrightarrow |b| = |a|$. $\therefore$ R सममित है।

$|a| = |b|$ और $|b| = |c| \Longrightarrow |a| = |c|$. $\therefore$ R संक्रामक है।

$\therefore$ R एक तुल्यता संबंध है।

$[0] = \{a \in \mathbf{Z} \mid aR0\} = \{a \in \mathbf{Z} \mid \; |a| = 0\} = \{0\}$.

$[1] = \{1, -1\}$.

E 14) $n, m \in N$ के लिए, $f(n) = f(m) \Longrightarrow n + 5 = m + 5 \Longrightarrow n = m$.

$\therefore$ f 1-1 है।

चूँकि $1 \notin f(N)$, $f(N) \neq N$ $\quad \therefore$ f आच्छादक नहीं है।

E 15) f, 1-1 है (जैसा कि E 14 में था)।

किसी $z \in \mathbf{Z}$ के लिए $f(z - 5) = z$.

$\therefore$ f आच्छादक है। अतः यह एकैकी आच्छादक है।

E 16) $f(x) = c \; \forall \; x \in X$.

मान लीजिए X में कम से कम दो अवयव x और y हैं।

तब $f(x) = c = f(y)$. परन्तु $x \neq y$ अर्थात् f, 1-1 नहीं है। इसलिए यदि :

X में केवल एक अवयव होगा।

चूँकि $f(X) = \{c\}$, इसलिए f आच्छादक है।

E 17) $x \in X \Longrightarrow f(x) \in f(X) \Longrightarrow x \in f^{-1}(f(X))$. $\quad \therefore X \subseteq f^{-1}(f(x))$

E 18) क) $x \in f^{-1}(S) \Longrightarrow f(x) \in S \subseteq T$.

$\Longrightarrow f(x) \in T$

$\Longrightarrow x \in f^{-1}(T)$.

$\therefore f^{-1}(S) \subseteq f^{-1}(T)$.

ख) $x \in f^{-1}(S \cup T) \Longleftrightarrow f(x) \in S \cup T$

$\Longleftrightarrow f(x) \in S$ या $f(x) \in T$

$\Longleftrightarrow x \in f^{-1}(S)$ या $x \in f^{-1}(T)$

$\Longleftrightarrow x \in f^{-1}(S) \cup f^{-1}(T)$

ग) इसे आप (ख) की तरह हल कीजिए।

E 19) सभी स्थितियों में $f \circ g$ और $g \circ f$, R से R तक के फलन हैं।

क) $f \circ g(x) = f(x + 5) = 5(x + 5) \; \forall \; x \in R$

$g \circ f(x) = g(5x) = 5x + 5 \; \forall \; x \in R$.

ख) $f \circ g(x) = g \circ f(x) = x \; \forall \; x \in R$.

$f \circ g(x) = x^2 = g \circ f(x) \; \forall \; x \in R$.

E 20) दिखाइए कि $I_A \circ g(b) = g(b)$ और $g \circ I_B(b) = g(b) \; \forall \; b \in B$

E 21) $g : \mathbf{R} \to \mathbf{R} : g(x) = 3x$.

E 22) क) f, 1-1 नहीं है, क्योंकि $f(1) = f(-1)$.

$\therefore f^{-1}$ का अस्तित्व नहीं है।

ख) f आच्छादक नहीं है, क्योंकि $f(\mathbf{R}) \neq \mathbf{R}$.

$\therefore f^{-1}$ का अस्तित्व नहीं है।

ग) f एकैकी आच्छादक है। $\quad \therefore$ f का अस्तित्व है।

$$f^{-1} : \mathbf{R} \to \mathbf{R} : f^{-1}(x) = \frac{x - 7}{11}.$$

E 23) मान लीजिए P(n) यह कथन है कि $(ab)^n = a^n b^n$.

P(1) सत्य है। मान लीजिए कि P(n − 1) सत्य है। तब

$$(ab)^n = (ab)^{n-1}(ab)$$
$$= (a^{n-1}b^{n-1})\,ab, \text{ क्योंकि } P(n-1) \text{ सत्य है।}$$
$$= a^{n-1}(b^{n-1}a)b$$
$$= a^{n-1}(ab^{n-1})b$$
$$= a^n b^n$$

$\therefore$ P(n) सत्य है।

$\therefore$ $\forall n \in N$, P(n) सत्य है।

E 24) क) क्योंकि $a.0 = 0$, $a \mid 0$

$(\pm 1)(\pm a) = a$. $\therefore \pm 1 \mid a$ और $\pm a \mid a$.

ख) $a \mid b \Rightarrow b = ad$, किसी $d \in Z$ के लिए।

$\Rightarrow bc = (ac)d$,

$\Rightarrow ac \mid bc$.

ग) $b = ad$, $c = be$, किन्हीं $d, e \in Z$ के लिए।

$\therefore c = ade$. $\therefore a \mid c$.

घ) $a \mid b \Rightarrow b = ad$, किसी $d \in Z$ के लिए।

$b \mid a \Rightarrow a = be$, किसी $e \in Z$ के लिए।

$\therefore a = ade \Rightarrow de = 1$, क्योंकि $a \neq 0$.

$\therefore e = \pm 1$. $\therefore a = \pm b$.

ङ) $c \mid a$ और $c \mid b \Rightarrow a = cd$, $b = ce$ किन्हीं $d, e \in Z$ के लिए।

$\therefore$ किसी $x, y \in Z$ के लिए, $ax + by = c(dx + ey)$.

$\therefore c \mid (ax + by)$.

E 25) मान लीजिए $p \nmid a$. तब $(p, a) = 1$.

$\therefore$ प्रमेय 9 के अनुसार $p \mid b$.

E 26) मान लीजिए P(n) यह कथन है कि

$p \mid a_1a_2 \ldots a_n \Rightarrow p \mid a_i$, किसी $i = 1, 2, \ldots, n$ के लिए।

P(1) सत्य है।

मान लीजिए $P(m-1)$ सत्य है।

अब मान लीजिए $p \mid a_1a_2 \ldots a_m$. तब $p \mid (a_1 \ldots a_{m-1})a_m$.

E 25 से, $p \mid a_1a_2 \ldots a_{m-1}$ या $p \mid a_m$.

$\therefore$ $p \mid a_i$ किसी $i = 1, \ldots, m$ के लिए (क्योंकि $P(m-1)$ सत्य है)

$\therefore$ P(m) सत्य है।

$\therefore$ $\forall n \in N$, P(n) सत्य है।

E 27) $\sqrt{p} = \frac{a}{b} \Rightarrow a^2 = pb^2 \Rightarrow p \mid a^2 \Rightarrow p \mid a$, क्योंकि p अभाज्य है।

मान लीजिए $a = pc$. तब $a^2 = pb^2 \Rightarrow p^2c^2 = pb^2 \Rightarrow pc^2 = b^2$

$\Rightarrow p \mid b^2 \Rightarrow p \mid b$.

$\therefore p \mid (a, b) = 1$, एक अंतर्विरोध।

$\therefore \sqrt{p}$ अपरिमेय है।

इकाई 2 समूह

इकाई की रूपरेखा

2.1 प्रस्तावना

इकाई 1 में हमने समुच्चयों और फलनों के कुछ आधारभूत गुणों पर चर्चा की है। इस इकाई में हम बीजीय संरचना वाले कुछ समुच्चयों पर चर्चा करेंगे। इन्हें हम समूह कहते हैं। समूह सिद्धांत अमूर्त बीजगणित की प्राचीनतम शाखाओं में से एक शाखा है। गणित और अन्य विज्ञानों में इसके अनेक अनुप्रयोग हैं। समूह सिद्धांत भौतिकी, रसायन विज्ञान और कंप्यूटर विज्ञान के विकास में काफी सहायक रहा है। इसकी जड़ें अठारहवीं शताब्दी के गणितज्ञ लग्रांज, रूफीनी और गाल्वा (Galois) के कार्यों में मिलती हैं।

इस इकाई में हम समूह सिद्धांत का अध्ययन शुरू करेंगे। हम समूहों को परिभाषित करेंगे और उनके कुछ उदाहरण देंगे। फिर हम समूह के अवयवों के कुछ गुणों पर चर्चा करेंगे। अंत में, हम तीन सुपरिचित एवं प्रायः इस्तेमाल होने वाले समूहों पर चर्चा करेंगे। बाद की इकाइयों में हम समूह सिद्धांत पर और चर्चा करेंगे।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- द्वि-आधारी संक्रिया की परिभाषा और इसके कुछ उदाहरण दे सकेंगे;
- आवेली और अन्-आवेली समूहों की परिभाषा और उदाहरण दे सकेंगे;
- विभिन्न समूहों के लिए निरसन नियम और घातांक नियम का प्रयोग कर सकेंगे;
- पूर्णांक माड्यूलो n, क्रमचय और संमिश्र संख्याओं के आधारभूत गुणों का प्रयोग कर सकेंगे।

2.2 द्वि-आधारी संक्रियाएं

आप R, Q और C में जोड़ तथा गुणा की सामान्य संक्रियाओं से परिचित हैं। ये संक्रियाएं द्वि-आधारी संक्रियाओं के उदाहरण हैं। ये कैसी संक्रियाएं हैं?

परिभाषा : मान लीजिए S एक अरिक्त समुच्चय है। किसी फलन $*: S \times S \to S$ को S पर **द्वि-आधारी संक्रिया** (binary operation) कहते हैं।

अतः द्वि-आधारी संक्रिया S के प्रत्येक क्रमित अवयव-युग्म के साथ S के एक अद्वितीय अवयव का संबंध स्थापित करती है।

S पर किसी द्वि-आधारी संक्रिया $*$ के लिए और किसी $(a, b) \in S \times S$ के लिए हम $*(a, b)$ को $a * b$ से प्रकट करते हैं।

हम द्वि-आधारी संक्रियाओं को प्रकट करने के लिए +, −, ×, ÷, o, • और △ जैसे प्रतीकों का प्रयोग करेंगे।

आइए, हम कुछ उदाहरणों पर विचार करें।

i) **Z** पर + और × द्वि-आधारी संक्रियाएं हैं। यहां $+(a, b) = a + b$ और $\times(a, b) = a \times b \ \forall \ a, b \in \mathbf{Z}$.
हम सामान्यतः $a \times b$ को ab से प्रकट करेंगे।

ii) मान लीजिए $\wp(S)$, S के सभी उपसमुच्चयों का समुच्चय है। तब $\wp(S)$ पर संक्रियाएं ∪ और ∩ द्वि-आधारी संक्रियाएं हैं, क्योंकि S के किन्हीं दो उपसमुच्चयों, A और B के लिए, $A \cup B$ और $A \cap B$ $\wp(S)$ में हैं।

iii) मान लीजिए X एक अरिक्त समुच्चय है और $\mathcal{F}(X)$, सभी फलनों $f : X \to X$ का समुच्चय है। तब फलनों का संयोजन $\mathcal{F}(X)$ पर एक द्वि-आधारी संक्रिया है, क्योंकि $f \circ g \in \ \in \mathcal{F}(x) \ \forall \ f, g \in \mathcal{F}(X)$.

अब हम द्वि-आधारी संक्रिया के कुछ गुणों को परिभाषित करेंगे।

परिभाषा : मान लीजिए • समुच्चय S पर एक द्वि-आधारी संक्रिया है। हम कहते हैं कि

i) S के उपसमुच्चय T पर • **संवृत** (closed) है, यदि $a \bullet b \in T \ \forall \ a, b \in T$.

ii) • **साहचर्य** (associative) है, यदि सभी $a, b, c \in S$ के लिए $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

iii) • **क्रमविनिमेय** (commutative) है, यदि सभी $a, b \in S$ के लिए $a \bullet b = b \bullet a$.

उदाहरण के लिए, **R** पर जोड़ और गुणा की संक्रियाएं क्रमविनिमेय हैं और साहचर्य भी। परन्तु **R** पर घटाने की संक्रिया न तो क्रमविनिमेय है और न ही साहचर्य। ऐसा क्यों?
क्या $a - b = b - a$ या $(a - b) - c = a - (b - c) \ \forall \ a, b, c \in \mathbf{R}$?
नहीं। उदाहरण के लिए, $1 - 2 \neq 2 - 1$ और $(1 - 2) - 3 \neq 1 - (2 - 3)$.
और, घटाने की संक्रिया $\mathbf{N} \subseteq \mathbf{R}$ पर संवृत नहीं है, क्योंकि $1 \in \mathbf{N}, 2 \in \mathbf{N}$, परन्तु $1 - 2 \notin \mathbf{N}$.

ध्यान दीजिए कि S पर द्वि-आधारी संक्रिया सदा ही S पर संवृत होती है, परन्तु संभव है कि यह S के उपसमुच्चय पर संवृत न हो।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 1) **R** पर परिभाषित निम्नलिखित द्वि-आधारी संक्रियाओं के लिए ज्ञात कीजिए कि ये क्रमविनिमेय अथवा साहचर्य हैं या नहीं। क्या ये N पर संवृत्त हैं?
सभी $x, y \in \mathbf{R}$ के लिए

क) $x \dotplus y = x + y - 5$

ख) $x \bullet y = 2(x + y)$

ग) $x \vartriangle y = \dfrac{x - y}{2}$

परिकलन के दौरान आप प्रायः निम्न तथ्य का प्रयोग अवश्य करते होंगे:
$a(b + c) = ab + ac$ और $(b + c)a = ba + ca \ \forall \ a, b, c \in \mathbf{R}$.
इस तथ्य से पता चलता है कि **R** में गुणन जोड़ पर वंटित है। व्यापक रूप में हम निम्नलिखित परिभाषा देते हैं।

परिभाषा : यदि ∘ और • समुच्चय S पर दो द्वि-आधारी संक्रियाएं हों, तो हम कहते हैं कि •, ∘ पर **वंटित (या वितरित)** है, यदि सभी $a, b, c \in S$ के लिए

$a \bullet (b \circ c) = (a \bullet b) \circ (a \bullet c)$ और
$(b \circ c) \bullet a = (b \bullet a) \circ (c \bullet a)$.

उदाहरण के लिए, मान लीजिए $a * b = \frac{a+b}{2}\ \forall\ a, b \in \mathbf{R}$. तब

$a(b * c) = a\left(\frac{b+c}{2}\right) = \frac{ab+ac}{2} = ab * ac$, और

$(b * c)a = \left(\frac{b+c}{2}\right)a = \frac{ba+ca}{2} = ba * ca\ \forall\ a, b, c \in \mathbf{R}$.

अत: गुणन $*$ पर बंटित है।

एक अन्य उदाहरण के रूप में इकाई 1 का प्रश्न E 4 लीजिए। क्या कहता है यह प्रश्न? यह कहता है कि समुच्चयों का प्रतिच्छेद समुच्चयों के सम्मिलन पर बंटित होता है और समुच्चयों का सम्मिलन समुच्चयों के प्रतिच्छेद पर बंटित होता है।

आइए अब हम कुछ द्वि-आधारी संक्रियाओं को ध्यान से देखें। आप जानते हैं कि किसी $a \in \mathbf{R}$ के लिए $a + 0 = a, 0 + a = a$ और $a + (-a) = (-a) + a = 0$. हम कहते हैं कि 0 जोड़ का तत्समक अवयव (identity element) है और $(-a)$, a का योज्य प्रतिलोम (additive inverse) या ऋणात्मक है। इसकी व्यापक परिभाषा निम्नलिखित है।

परिभाषा : मान लीजिए $*$ समुच्चय S पर एक द्वि-आधारी संक्रिया है। यदि एक ऐसा अवयव $e \in S$ हो जिससे कि $\forall\ a \in S$, $a * e = a$ और $e * a = a$, तो e को $*$ का **तत्समक अवयव** कहते हैं।

$a \in S$ के लिए हम कहते है कि $b \in S$, a का **प्रतिलोम** है, यदि $a * b = e$ और $b * a = e$. इस स्थिति में हम प्राय: $b = a^{-1}$ लिखते हैं।

तत्समक अवयवों और प्रतिलोमों के उदाहरणों के बारे में चर्चा करने से पहले निम्नलिखित परिणाम पर विचार कीजिए। इसमें हम $*$ के तत्समक अवयव की अद्वितीयता को और $*$ के सापेक्ष किसी अवयव के प्रतिलोम की अद्वितीयता को सिद्ध करेंगे, यदि प्रतिलोम हो तो।

प्रमेय 1 : मान लीजिए $*$ समुच्चय S पर एक द्वि-आधारी संक्रिया है। तब

क) यदि $*$ का एक तत्समक अवयव हो, तो यह अद्वितीय होगा।

ख) यदि $*$ साहचर्य हो और $s \in S$ का $*$ के सापेक्ष एक प्रतिलोम हो, तो यह अद्वितीय होगा।

उपपत्ति : क) मान लीजिए e और e', दोनों ही $*$ के तत्समक अवयव हैं। तब

$e = e * e'$, क्योंकि e' एक तत्समक अवयव है।

$= e'$, क्योंकि e एक तत्समक अवयव है।

अर्थात् $e = e'$. इस तरह हम पाते हैं कि तत्समक अवयव अद्वितीय है।

ख) मान लीजिए ऐसे $a, b \in S$ हैं, जिनसे कि $s * a = e = a * s$ और $s * b = e = b * s$, जहां e, $*$ का तत्समक अवयव है। तब

$a = a * e = a * (s * b)$

$= (a * s) * b$, क्योंकि $*$ साहचर्य है।

$= e * b$

$= b$.

अर्थात् $a = b$.

इस तरह, s का प्रतिलोम अद्वितीय है।

द्वि-आधारी संक्रिया का तत्समक अवयव हो सकता है और नहीं भी। उदाहरण के लिए, N पर जोड़ की संक्रिया का कोई तत्समक अवयव नहीं है।

इसी प्रकार, हो सकता है कि एक द्वि-आधारी संक्रिया के सापेक्ष किसी अवयव का प्रतिलोम न हो। उदाहरण के लिए, $2 \in \mathbf{Z}$ का $\mathbf{Z}$ पर गुणन के सापेक्ष कोई प्रतिलोम नहीं है।

आइए अब हम कुछ उदाहरणों पर विचार करें।

उदाहरण 1 : यदि $a \oplus b = a + b - 1$ से द्वि-आधारी संक्रिया $\oplus : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ परिभाषित हो, तो सिद्ध कीजिए कि $\oplus$ का एक तत्समक है। यदि $\oplus$ के सापेक्ष $x \in \mathbf{R}$ का प्रतिलोम हो, तो इसे ज्ञात कीजिए।

हल : हम ऐसा $e \in R$ प्राप्त करना चाहते हैं जिससे कि $a \oplus e = e = e \oplus a \; \forall a \in R$. अतः हम एक ऐसा $e \in R$ प्राप्त करना चाहते हैं जिससे कि $a + e - 1 = a \; \forall a \in R$. स्पष्ट है कि $e = 1$ इसे संतुष्ट करेगा। साथ ही $1 \oplus a = a \; \forall a \in R$. अतः 1, $\oplus$ का तत्समक अवयव है।
$x \in R$ के लिए, यदि x का प्रतिलोम b हो तो $b \oplus x = 1$ होना चाहिए। अर्थात् $b + x - 1 = 1$, अर्थात् $b = 2 - x$. वास्तव में $(2 - x) \oplus x = (2 - x) + x - 1 = 1$. और,
$x \oplus (2 - x) = x + 2 - x - 1 = 1$.

इसलिए $x^{-1} = 2 - x$

उदाहरण 2 : मान लीजिए S एक अरिक्त समुच्चय है। S के सभी उपसमुच्चयों का समुच्चय $\wp(S)$ लीजिए। क्या $\wp(S)$ पर $\cup$ और $\cap$ क्रमविनिमेय अथवा साहचर्य संक्रियाएं हैं? क्या इन संक्रियाओं के सापेक्ष तत्समक अवयव और $\wp(S)$ के अवयवों के प्रतिलोम का अस्तित्व है?

हल : चूंकि $A \cup B = B \cup A$ और $A \cap B = B \cap A \; \forall A, B \in \wp(S)$, इसलिए सम्मिलन और प्रतिच्छेद की संक्रियाएं क्रमविनिमेय हैं। इकाई 1 के E 4 के अनुसार, दोनों संक्रियाएं साहचर्य हैं। आप देख सकते हैं कि रिक्त समुच्चय ϕ और समुच्चय S क्रमशः सम्मिलन और प्रतिच्छेद की संक्रियाओं के तत्समक हैं।

चूंकि $S \neq \phi$, इसलिए ऐसा कोई $B \in \wp(S)$ नहीं है जिससे कि $S \cup B = \phi$. वास्तव में, किसी अरिक्त $A \in \wp(S)$ के लिए, A का सम्मिलन के सापेक्ष कोई प्रतिलोम नहीं है। इसी प्रकार, S के किसी उचित उपसमुच्चय का प्रतिच्छेद के सापेक्ष कोई प्रतिलोम नहीं है।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 2) क) E 1 में दी गई संक्रियाओं का तत्समक अवयव ज्ञात कीजिए, जहां भी इसका अस्तित्व हो।

ख) E 1 में दी गई संक्रियाओं में प्रत्येक के सापेक्ष $x \in R$ के लिए x^{-1} (यदि इसका अस्तित्व हो तो) प्राप्त कीजिए।

यदि विचाराधीन समुच्चय S छोटा हो तो हम S पर किसी द्वि-आधारी संक्रिया की क्रिया एक सारणी से दिखा सकते हैं।

चित्र 1 : आर्थर केली

संक्रिया सारणी

मान लीजिए S एक परिमित समुच्चय है और $*$, S पर एक द्वि-आधारी संक्रिया है। हम द्वि-आधारी संक्रिया को एक वर्ग सारणी से निरूपित कर सकते हैं। इस सारणी को संक्रिया सारणी या केली सारणी कहते हैं। केली सारणी का नामकरण सुप्रसिद्ध गणितज्ञ आर्थर केली (1821-1895) के नाम पर किया गया है।

इस सारणी को लिखने के लिए पहले हम S के अवयवों को एक ही क्रम में ऊपर से नीचे तथा बाएं से दाएं की ओर लिखते हैं। तब हम सारणी में $a * b$ को a से शुरू होने वाली पंक्ति और b के नीचे दिए गए स्तम्भ (कॉलम) के प्रतिच्छेद पर लिखते हैं।

उदाहरण के लिए, यदि $S = \{-1, 0, 1\}$ और द्वि-आधारी संक्रिया गुणन हो, जिसे $\cdot$ से प्रकट किया गया हो, तो इसे निम्नलिखित सारणी से निरूपित किया जा सकता है।

	-1	0	1
-1	$(-1).(-1)$ $=1$	$(-1).0$ $=0$	$(-1).1$ $=-1$
0	$0.(-1)$ $=0$	0.0 $=0$	0.1 $=0$
1	$1.(-1)$ $=-1$	1.0 $=0$	1.1 $=1$

विलोमतः, यदि हमें सारणी दी हुई हो, तो हम S पर एक द्वि-आधारी संक्रिया को परिभाषित कर सकते हैं। उदाहरण के लिए हम $S = \{1, 2, 3\}$ पर संक्रिया * को निम्नलिखित सारणी से परिभाषित कर सकते हैं।

*	1	2	3
1	1	2	3
2	3	1	2
3	2	3	1

इस सारणी से हम देख सकते हैं कि $1 * 2 = 2$ और $2 * 3 = 2$.

अब $2 * 1 = 3$ और $1 * 2 = 2$. $\therefore 2 * 1 \neq 1 * 2$. अर्थात् क्रमविनिमेय नहीं है।

और $(2 * 1) * 3 = 3 * 3 = 1$, $2 * (1 * 3) = 2$.

$\therefore (2 * 1) * 3 \neq 2 * (1 * 3)$.

$\therefore$ * साहचर्य नहीं है।

देखा, एक सारणी से कितनी जानकारी प्राप्त की जा सकती है!

नीचे दिए गए प्रश्न को हल करने से आपको केली सारणी बनाने का कुछ अभ्यास हो जाएगा।

E 3) समुच्चय $\wp(S)$ (देखिए उदाहरण 1) के लिए संक्रिया सारणी बनाइए, जहां $S = \{0, 1\}$ और संक्रिया $\cap$ है।

अब निम्नलिखित परिभाषा पर विचार कीजिए।

परिभाषा : मान लीजिए * एक अरिक्त समुच्चय S पर एक द्वि-आधारी संक्रिया है और मान लीजिए $a_1, a_2, \ldots, a_{k+1} \in S$. हम गुणनफल $a_1 * a_2 * \ldots * a_{k+1}$ को इस प्रकार परिभाषित करते हैं:
यदि $k = 1$, $a_1 * a_2$, S का एक सुपरिभाषित अवयव है।
यदि $a_1 * \ldots * a_k$ परिभाषित हो, तो

$$a_1 * a_2 * \ldots * a_{k+1} = (a_1 * \ldots * a_k) * a_{k+1}.$$

हम इस परिभाषा का प्रयोग निम्नलिखित परिणाम में करेंगे।

प्रमेय 2 : मान लीजिए $a_1, \ldots, a_{m+n}$ समुच्चय S के अवयव हैं और *, S पर एक साहचर्य द्वि-आधारी संक्रिया है। तब

$$(a_1 * \ldots * a_m) * (a_{m+1} * \ldots * a_{m+n}) = a_1 * \ldots * a_{m+n}.$$

उपपत्ति : हम n पर आगमन का प्रयोग करेंगे। अर्थात् हम दिखाएंगे कि $n = 1$ के लिए कथन सत्य है। फिर यह मानकर कि यह कथन $(n - 1)$ के लिए सत्य है, इसे n के लिए सिद्ध करेंगे।

यदि $n = 1$, तो ऊपर की परिभाषा से हमें

$$(a_1 * \ldots * a_m) * a_{m+1} = a_1 * \ldots * a_{m+1}$$

प्राप्त होता है।

अब मान लीजिए कि

$$(a_1 * \ldots . * a_m) * (a_{m+1} * \ldots . . * a_{m+n-1}) = a_1 * \ldots . * a_{m+n-1}.$$

तब

$$(a_1 * \ldots . * a_m) * (a_{m+1} * \ldots . . * a_{m+n})$$

$= (a_1 * \ldots . * a_m) * ((a_{m+1} * \ldots . . * a_{m+n-1}) * a_{m+n})$

$= ((a_1 * \ldots . * a_m) * (a_{m+1} * \ldots . . * a_{m+n-1})) * a_{m+n}$, क्योंकि * साहचर्य है।

$= (a_1 * \ldots . * a_{m+n-1}) * a_{m+n}$, आगमन से।

$= a_1 * \ldots . * a_{m+n}$, परिभाषा से।

इस तरह, परिणाम सभी n के लिए लागू होता है।

इस पाठ्यक्रम में हम प्रमेय 2 का प्रयोग प्रा- : करेंगे।

द्वि-आधारी संक्रियाओं की चर्चा के बाद आइए अब हम समूहों प चर्चा करें।

2.3 समूह क्या है?

इस भाग में हम एक बीजीय निकाय, यानि कि समूह के कुछ आधारभूत गुणों का अध्ययन करेंगे। इस बीजीय निकाय में एक समुच्चय होता है जिस पर एक द्वि-आधारी संक्रिया, परिभाषित होती है, जो भाग 2.2 में दिए गए कुछ गुणों को संतुष्ट करती है। आइए हम देखें कि यह निकाय क्या है।

परिभाषा : मान लीजिए G एक अरिक्त समुच्चय है और $*$, G पर एक द्वि-आधारी संक्रिया है। हम युग्म $(G, *)$ को एक **समूह** (group) कहते हैं, यदि

G 1) $*$ साहचर्य हो,

G 2) G में $*$ के ि एक तत्समक अव ेवा हो, और

G 3) G के प्रत्येक अवयव का $*$ के सापेक्ष G में एक प्रतिलोम होता हो।

$(G, *)$ को **सामिसमूह** (semigroup) कहते हैं यदि $*$ गुण G 1 को संतुष्ट करता हो। इस तरह, प्रत्येक समूह एक सामिसमूह होता है।

अब हम समूह के कुछ उदाहरण देंगे।

उदाहरण 3 : दिखाइए कि $(Z, +)$ एक समूह है, परन्तु $(Z, \cdot)$ समूह नहीं है।

हल : $+$, **Z** पर एक साहचर्य द्वि-आधारी संक्रिया है। $+$ के लिए तत्समक अवयव 0 है और किसी $n \in \mathbf{Z}$ का प्रतिलोम $(-n)$ है। इस तरह, $(\mathbf{Z}, +)$, G 1, G 2 और G 3 को संतुष्ट करता है। अतः यह एक समूह है।

Z में गुणन साहचर्य है और $1 \in \mathbf{Z}$ गुणन के लिए तत्समक है। लेकिन, क्या **Z** के प्रत्येक अवयव का एक गुणनात्मक प्रतिलोम होता है? नहीं। उदाहरण के लिए, $\cdot$ के सापेक्ष 0 और 2 के प्रतिलोम नहीं हैं। इसलिए $(\mathbf{Z}, \cdot)$ एक समूह नहीं है।

ध्यान दीजिए कि $(\mathbf{Z}, \cdot)$ एक सामिसमूह है क्योंकि यह G 1 को संतुष्ट करता है। अतः कुछ ऐसे सामिसमूह होते हैं, जो समूह नहीं होते।

नीचे दिए गए प्रश्न से आपको समूह के दो और उदाहरण प्राप्त होंगे।

E 4) दिखाइए कि $(\mathbf{Q}, +)$ और $(\mathbf{R}, +)$ समूह हैं।

वास्तव में, यह दिखाने के लिए कि $(G, *)$ एक समूह है, यह दिखाना ही काफी है कि $*$ निम्नलिखित अभिगृहीतों को संतुष्ट करता है।

G 1') $*$ साहचर्य है,

G 2') $\exists$ $e \in G$ जिससे कि $a * e = a \; \forall \; a \in G$, और

G 3') यदि $a \in G$, तो $\exists$ $b \in G$ जिससे कि $a * b = e$.

यहां हम कहना चाह रहे हैं कि अभिगृहीतों के दोनों समुच्चय तुल्य हैं। इनमें अंतर केवल यह है: अभिगृहीतों के पहले संग्रह में हमें यह सिद्ध करना होता है कि e एक दो-पक्षीय तत्समक है और $a \in G$ का प्रतिलोम b, $a * b = e$ और $b * a = e$, दोनों को संतुष्ट करता है। दूसरे, संग्रह में हमें केवल यह सिद्ध करना होता है कि e एक एक-पक्षीय तत्समक है और $a \in G$ का प्रतिलोम केवल $a * b = e$ को संतुष्ट करता है।

वास्तव में, ये अभिगृहीत निम्नलिखित के भी तुल्य हैं:

G 1'') $*$ साहचर्य है,

G 2'') $\exists$ $e \in G$ जिससे कि $e * a = a \; \forall \; a \in G$, और

G 3'') यदि $a \in G$, तो $\exists$ $b \in G$ जिससे कि $b * a = e$.

स्पष्ट है कि यदि $*$, G 1, G 2 और G 3 को संतुष्ट करता हो तो यह G 1', G 2', और G 3' को भी संतुष्ट करेगा। निम्नलिखित प्रमेय से हमें पता चलता है कि यदि $*$, G 1', G 2' और G 3' को संतुष्ट करता हो तो यह G 1, G 2 और G 3 को भी संतुष्ट करेगा।

प्रमेय 3 : मान लीजिए $(G, *)$, G 1′, G 2′ और G 3′ को संतुष्ट करता है। तब $e * a = a \; \forall \; a \in G$. और यदि $a \in G$ के लिए $\exists \; b \in G$ जिससे कि $a * b = e$, तो $b * a = e$. इस तरह, $(G, *)$ G 1, G 2 और G 3 को संतुष्ट करता है।

इस प्रमेय को सिद्ध करने के लिए हमें निम्नलिखित परिणाम की आवश्यकता है।

प्रमेयिका 1 : मान लीजिए $(G, *)$, G 1′, G 2′ और G 3′ को संतुष्ट करता है। यदि $\exists \; a \in G$ जिससे कि $a * a = a$, तब $a = e$.

उपपत्ति : G 3′ से हम जानते हैं कि $\exists \; b \in G$ जिससे कि $a * b = e$.

अब $(a * a) * b = a * b = e$.

और $a * (a * b) = a * e = a$.

इसलिए G 1′ से, $a = e$.

अब हम इस प्रमेयिका का प्रयोग प्रमेय 3 को सिद्ध करने के लिए करेंगे।

प्रमेय 3 की उपपत्ति : चूंकि G 1 और G 1′ एक ही अभिगृहीत हैं, इसलिए G 1 सत्य है। अब हम यह सिद्ध करेंगे कि G 3 सत्य है। मान लीजिए $a \in G$. G 3′ से $\exists \; b \in G$ जिससे कि $a * b = e$. हम दिखाएंगे कि $b * a = e$. अब,

$(b * a) * (b * a) = (b * (a * b)) * a = (b * e) * a = b * a$.

इसलिए प्रमेयिका 1 से, $b * a = e$. अतः G 3 सत्य है।

अब हम दिखाएंगे कि G 2 सत्य है। मान लीजिए $a \in G$. तब G 2′ के अनुसार, किसी भी $a \in G$ के लिए $a * e = a$. G 3 सत्य है, इसलिए $\exists \; b \in G$ जिससे कि $a * b = b * a = e$.

तब

$e * a = (a * b) * a = a * (b * a) = a * e = a$.

अर्थात् G 2 भी सत्य है।

इस तरह, हम यह पाते हैं कि $(G, *)$, G 1, G 2 और G 3 को संतुष्ट करता है।

आइए अब हम समूह के कुछ और उदाहरण लें।

उदाहरण 4 : मान लीजिए $G = \{\pm 1, \pm i\}$, $i = \sqrt{-1}$. मान लीजिए द्वि-आधारी संक्रिया गुणा है। दिखाइए कि $(G, \cdot)$ एक समूह है।

हल : संक्रिया $\cdot$ की सारणी है

	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

इस सारणी से पता चलता है कि $a \cdot 1 = a \; \forall \; a \in G$. अतः 1 तत्समक अवयव है। इससे यह भी पता चलता है कि $(G, \cdot)$, G 3′ को संतुष्ट करता है। इसलिए $(G, \cdot)$ एक समूह है।
ध्यान दीजिए कि $G = \{1, x, x^2, x^3\}$, जहां $x = i$

उदाहरण 4 से आप देख सकते हैं कि किसी निकाय को समूह सिद्ध करने के लिए हम प्रमेय 3 के प्रयोग से किस प्रकार अपना काम घटा सकते हैं।

ध्यान दीजिए कि उदाहरण 4 के समूह में केवल 4 अवयव हैं, जबकि उदाहरण 3 और E 4 के समूहों में अनंततः अनेक अवयव हैं। इस संबंध में हम निम्नलिखित परिभाषा देते हैं।

परिभाषा : यदि $(G, *)$ एक समूह हो, जहां G, n अवयवों वाला एक परिमित समुच्चय है, तो हम $(G, *)$ को **कोटि** (order) n **का परिमित समूह** कहते हैं। यदि G एक अनंत समुच्चय है तो हम $(G, *)$ को **अनंत समूह** कहते हैं।

चित्र 2 : एन. एच. आबेल (1802-1829)

यदि $*$ एक क्रमविनिमेय द्वि-आधारी संक्रिया हो, तो हम कहते हैं कि $(G, *)$ एक **क्रमविनिमेय समूह या आबेली समूह** है।

आबेली समूहों का नाम नॉर्वे के एक प्रतिभाशाली युवा गणितज्ञ नील्स हेनरीक आबेल के नाम पर रखा गया है।

इस तरह, उदाहरण 4 का समूह कोटि 4 का एक परिमित आबेली समूह है। उदाहरण 3 और E 4 के समूह अनंत आबेली समूह हैं।

आइए अब हम अक्रमविनिमेय (non-commutative) (या अन्-आबेली) समूह के एक उदाहरण पर विचार करें। इस उदाहरण को पढ़ने से पहले, याद कीजिए कि समुच्चय S पर $m \times n$ आव्यूह (matrix) समुच्चय S के अवयवों की m पंक्तियों और n स्तंभों में एक आयताकार व्यवस्था है।

उदाहरण 5 : मान लीजिए G शून्येतर सारणिक वाले सभी 2×2 आव्यूहों का समुच्चय है। अर्थात्

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \, a, b, c, d \in \mathbf{R}, ad - bc \neq 0 \right\}.$$

आव्यूह गुणन के साथ G को लीजिए। अर्थात्

G के अवयवों $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ और $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ के लिए,

$$A.P = \begin{bmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{bmatrix}.$$

दिखाइए कि $(G, \cdot)$ एक समूह है।

यदि $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, तो $ad - bc$ को A का सारणिक कहते हैं, और इसे $\det A$ या $|A|$ से प्रकट करते हैं।

हल : पहले हम दिखाएंगे कि $\cdot$ एक द्वि-आधारी संक्रिया है, अर्थात्
$A, P \in G \implies A.P \in G$. अब, $\det (AP) = \det A \cdot \det P \neq 0$,
क्योंकि $\det A \neq 0$, $\det P \neq 0$.
अतः G के सभी A, P के लिए, $A \cdot P \in G$.

$\det (AB) = (\det A) (\det B)$

हम यह भी जानते हैं कि आव्यूह गुणन साहचर्य है और

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ गुणनात्मक तत्समक है। अब, G के अवयव

$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ के लिए, आव्यूह

$$B = \begin{bmatrix} \dfrac{d}{ad - bc} & \dfrac{-b}{ad - bc} \\[2ex] \dfrac{-c}{ad - bc} & \dfrac{a}{ad - bc} \end{bmatrix},$$

ऐसा है कि $\det B = \dfrac{1}{ad - bc} \neq 0$ और $AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

इस तरह, $B = A^{-1}$. (ध्यान दीजिए कि हमने यहां अभिगृहीत G 3′ का प्रयोग किया है, न कि G 3 का।)

इससे पता चलता है कि $\mathbf{R}$ पर शून्येतर सारणिक वाले सभी 2×2 आव्यूहों का समुच्चय आव्यूह गुणन के सापेक्ष एक समूह है। चूंकि

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$$

और

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix},$$

इसलिए, यह समूह क्रमविनिमेय नहीं है।

इस समूह को प्राय: $GL_2(\mathbf{R})$ से प्रकट करते हैं, और इसे $\mathbf{R}$ पर कोटि 2 वाला **व्यापक रैखिक समूह** (general linear group) कहते हैं। हम इस समूह का प्रयोग खंड 2 और खंड 2 में उदाहरणों के लिए करेंगे।

आइए अब हम आबेली समूह के एक अन्य उदाहरण पर विचार करें।

उदाहरण 6 : $\mathbf{R}^2$ के सभी **स्थानांतरणों** (translations) का निम्नलिखित समुच्चय लीजिए:

$T = \{f_{a,b} : \mathbf{R}^2 \to \mathbf{R}^2 \mid f_{a,b}(x, y) = (x + a, y + b)$, नियत $a, b \in \mathbf{R}$ के लिए$\}$.

ध्यान दीजिए कि T के प्रत्येक अवयव $f_{a,b}$ को $\mathbf{R}^2$ के बिन्दु (a, b) से निरूपित किया जा सकता है। दिखाइए कि $(T, \circ)$ एक समूह है, जहां $\circ$ फलनों के संयोजन को प्रकट करता है।

हल : आइए अब हम देखें कि T पर $\circ$ द्वि-आधारी संक्रिया है या नहीं।

अब $f_{a,b} \circ f_{c,d}(x, y) = f_{a,b}(x + c, y + d) = (x + c + a, y + d + b)$

$= f_{a+c,b+d}(x, y)$, किसी भी $(x, y) \in \mathbf{R}^2$ के लिए।

$\therefore f_{a,b} \circ f_{c,d} = f_{a+c,b+d} \in T$.

इस तरह, $\circ$, T पर द्वि-आधारी संक्रिया है।

अब $f_{a,b} \circ f_{0,0} = f_{a,b} \; \forall f_{a,b} \in T$.

अतः $f_{0,0}$ तत्समक अवयव है।

साथ ही, $f_{a,b} \circ f_{-a,-b} = f_{0,0} \; \forall f_{a,b} \in T$. इसलिए $f_{a,b} \in T$ का प्रतिलोम $f_{-a,-b}$ है।

इस तरह, $(T, \circ)$, G 1', G 2' और G 3' को संतुष्ट करता है। इसलिए यह एक समूह है।

ध्यान दीजिए कि $f_{a,b} \circ f_{c,d} = f_{c,d} \circ f_{a,b} \; \forall f_{a,b}, f_{c,d} \in T$. इसलिए $(T, \circ)$ आबेली है।

अब आप नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 5) मान लीजिए $\mathbf{Q}^*$, $\mathbf{R}^*$ और $\mathbf{Z}^*$ शून्येतर परिमेय संख्याओं, वास्तविक संख्याओं और पूर्णांकों के समुच्चयों को प्रकट करते हैं। क्या नीचे दिए गए कथन सत्य हैं? यदि नहीं, तो कारण बताइए।

क) $(\mathbf{Q}^*, .)$ आबेली समूह है।

ख) $(\mathbf{R}^*, .)$ परिमित आबेली समूह है।

ग) $(\mathbf{Z}^*, .)$ एक समूह है।

घ) $(\mathbf{Q}^*, .)$, $(\mathbf{R}^*, .)$ और $(\mathbf{Z}^*, .)$ सामिसमूह हैं।

E 6) दिखाइए कि $(G, *)$ एक अन्-आबेली समूह है, जहां $G = \{(a, b) \mid a, b \in \mathbf{R}, a \neq 0\}$ और G पर $*$ $(a, b) * (c, d) = (ac, bc + d)$ से परिभाषित है।

अब हम समूह के अवयवों के कुछ गुणों पर विचार करेंगे।

2.4 समूह के गुण

इस भाग में हम समूह के अवयवों के गुणों से संबंधित कुछ प्रारंभिक परिणाम प्रस्तुत करेंगे। परन्तु पहले हम संकेतन की एक प्रथा का उल्लेख करेंगे।

प्रथा : आगे से, अपनी सुविधा के लिए हम **समूह $(G, *)$ को G से प्रकट करेंगे।** और हम $a, b \in G$ के लिए **$a * b$ को ab से प्रकट करेंगे,** और कहेंगे कि हम a और b का गुणा कर रहे हैं। अक्षर e समूह तत्समक को ही प्रकट करेगा।

आइए अब हम एक सरल परिणाम सिद्ध करें।

प्रमेय 4 : मान लीजिए G एक समूह है। फिर

क) $(a^{-1})^{-1} = a$, प्रत्येक $a \in G$ के लिए

ख) $(ab)^{-1} = b^{-1}a^{-1}$, सभी $a, b \in G$ के लिए

उपपत्ति : (क) प्रतिलोम की परिभाषा के अनुसार
$(a^{-1})^{-1}(a^{-1}) = e = (a^{-1})(a^{-1})^{-1}$.
साथ ही, $aa^{-1} = a^{-1}a = e$.

इस तरह, प्रमेय 1 (ख) के अनुसार, $(a^{-1})^{-1} = a$.
(ख) चूंकि $a, b \in G$, इसलिए $ab \in G$.
अतः $(ab)^{-1} \in G$. और यह वह अद्वितीय अवयव है जो
$(ab)(ab)^{-1} = (ab)^{-1}(ab) = e$ को संतुष्ट करता है। लेकिन

$$
\begin{aligned}
(ab)(b^{-1}a^{-1}) &= ((ab)b^{-1})a^{-1} \\
&= (a(bb^{-1})a^{-1}) \\
&= (ae)a^{-1} \\
&= aa^{-1} \\
&= e.
\end{aligned}
$$

इसी प्रकार, $(b^{-1}a^{-1})(ab) = e$.

इस तरह, प्रतिलोम की अद्वितीयता से हमें $(ab)^{-1} = b^{-1}a^{-1}$ प्राप्त होता है।

ध्यान दीजिए कि समूह G के लिए $(ab)^{-1} = a^{-1}b^{-1}$ केवल तब होता है, जबकि G आबेली हो।

आप जानते हैं कि $\mathbf{R}^*$ के a, b, c के लिए जब कभी $ba = ca$ या $ab = ac$, तब हम यह निष्कर्ष निकाल सकते हैं कि $b = c$. अर्थात् हम a का निरसन कर सकते हैं। यह बात सभी समूहों पर लागू होती है।

प्रमेय 5 : किसी समूह G के अवयवों a, b, c के लिए,

क) $ab = ac \Rightarrow b = c$. (इसे **वाम निरसन नियम** कहते हैं।)

ख) $ba = ca \Rightarrow b = c$. (इसे **दक्षिण निरसन नियम** कहते हैं।)

उपपत्ति : यहां हम केवल (क) को सिद्ध करेंगे और (ख) की उपपत्ति आप पर छोड़ देंगे (देखिए E 7)।

क) मान लीजिए $ab = ac$. दोनों पक्षों को बायीं ओर $a^{-1} \in G$ से गुणा करने पर हमें प्राप्त होता है

$$
\begin{aligned}
& a^{-1}(ab) = a^{-1}(ac) \\
\Rightarrow\ & (a^{-1}a)b = (a^{-1}a)c \\
\Rightarrow\ & eb = ec, \text{ जहां } e \text{ तत्समक अवयव है।} \\
\Rightarrow\ & b = c.
\end{aligned}
$$

ध्यान रखिए कि गुणा करने का अर्थ है संक्रिया $*$ को लागू करना।

E 7) प्रमेय 5 (ख) सिद्ध कीजिए।

अब प्रमेय 5 का प्रयोग नीचे दिए गए प्रश्न को हल करने में कीजिए।

E 8) यदि G एक समूह है और $g \in G$ ऐसा हो कि सभी $x \in G$ के लिए $gx = g$, तो दिखाइए कि $G = \{e\}$.

अब हम समूह के एक अन्य गुण को सिद्ध करेंगे।

प्रमेय 6 : समूह G के अवयवों a, b के लिए समीकरणों $ax = b$ और $ya = b$ के G में अद्वितीय हल होते हैं।

उपपत्ति : पहले हम दिखाएंगे कि इन रैखिक समीकरणों के G में हल हैं, और फिर दिखाएंगे कि हल अद्वितीय हैं।

$a, b \in G$ के लिए $a^{-1}b \in G$ लीजिए। तब

$a(a^{-1}b) = (aa^{-1})b = eb = b$. इस तरह, $a^{-1}b$ समीकरण $ax = b$ को संतुष्ट करता है, अर्थात् $ax = b$ का G में एक हल है।

लेकिन, क्या यही एक हल है? मान लीजिए G में $ax = b$ के दो हल x_1 और x_2 हैं। तब $ax_1 = b = ax_2$. वाम निरसन नियम लागू करने पर $x_1 = x_2$ प्राप्त होता है। अतः G में $a^{-1}b$ ही अद्वितीय हल है।

इसी प्रकार दक्षिण निरसन नियम लागू करके हम दिखा सकते हैं कि G में $ya = b$ का एक ही हल ba^{-1} है।

अब हम प्रमेय 6 में दिए गए गुण को प्रस्तुत करेंगे।

उदाहरण 7 : $GL_2(R)$ में $A = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 5 \\ 0 & 4 \end{bmatrix}$ लीजिए (देखिए उदाहरण 5)। $AX = B$ का हल ज्ञात कीजिए

हल : प्रमेय 6 से हम जानते हैं कि $X = A^{-1}B$. अब,

$$A^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} \text{ (देखिए उदाहरण 5)}$$

$$\therefore X = A^{-1}B = \begin{bmatrix} 2 & -2 \\ -1 & 3 \end{bmatrix}$$

अगले उदाहरणों में हम एक महत्वपूर्ण समूह पर विचार करेंगे।

उदाहरण 8 : मान लीजिए S एक अरिक्त समुच्चय है। **समनित अंतर** Δ की द्वि-आधारी संक्रिया के साथ $\wp(S)$ लीजिए (देखिए उदाहरण 2), जहां

$A \Delta B = (A \setminus B) \cup (B \setminus A) \; \forall A, B \in \wp(S)$.

दिखाइए कि $(\wp(S), \Delta)$ एक आबेली समूह है। समीकरण $Y \Delta A = B$ का अद्वितीय हल क्या है?

हल : Δ एक साहचर्य द्वि-आधारी संक्रिया है। यह बात निम्नलिखित तथ्यों के प्रयोग से दिखाई जा सकती है:

$A \setminus B = A \cap B^c$, $(A \cap B)^c = A^c \cup B^c$, $(A \cup B)^c = A^c \cap B^c$, और $\cup$ तथा $\cap$ क्रमविनिमेय और साहचर्य हैं।

Δ क्रमविनिमेय भी है, क्योंकि $A \Delta B = B \Delta A \; \forall A, B \in \wp(S)$. और ϕ तत्समक अवयव है, क्योंकि $A \Delta \phi = A \; \forall A \in \wp(S)$. तथा प्रत्येक अवयव स्वयं अपना प्रतिलोम है, क्योंकि $A \Delta A = \phi \; \forall A \in \wp(S)$.

इस तरह, $(\wp(S), \Delta)$ एक आबेली समूह है।

अब $(\wp(S), \Delta)$ के A, B के लिए हम $Y \Delta A = B$ हल करना चाहते हैं। हम जानते हैं कि A स्वयं अपना प्रतिलोम है। इसलिए प्रमेय 6 के अनुसार, $Y = B \Delta A^{-1} = B \Delta A$ अद्वितीय हल है। हमने यहां यह भी सिद्ध कर दिया है कि $\wp(S)$ के A, B के लिए $(B \Delta A) \Delta A = B$.

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 9) घटाने की द्वि-आधारी संक्रिया के साथ **Z** लीजिए। क्या $(\mathbf{Z}, -)$ एक समूह है? क्या आप $a - x = b \; \forall a, b \in \mathbf{Z}$ का एक हल प्राप्त कर सकते हैं?

आइए अब हम देखें कि किसी अवयव को स्वयं से बार-बार गुणा करने पर क्या प्राप्त होता है।

परिभाषा : मान लीजिए G एक समूह है। $a \in G$ के लिए हम निम्नलिखित परिभाषा देते हैं:

i) $a^0 = e$.

ii) $a^n = a^{n-1}.a$, यदि $n > 0$

iii) $a^{-n} = (a^{-1})^n$, $n > 0$ के लिए।

n को **पूर्णांकीय घात** (integral power) a^n का **घातांक** (exponent) कहते हैं। इस तरह, परिभाषा के अनुसार $a^1 = a$, $a^2 = a \cdot a$, $a^3 = a^2 \cdot a$, आदि-आदि।

टिप्पणी : जब द्वि-आधारी संक्रिया जोड़ हो, तो a^n, na हो जाएगा।
उदाहरण के लिए, किसी $a \in \mathbf{Z}$ के लिए,
यदि $n = 0$, तो $na = 0$;
यदि $n > 0$, तो $na = a + a + \ldots + a$ (n बार); और
यदि $n < 0$, तो $na = (-a) + (-a) + \ldots + (-a)$ ($-n$ बार)।

आइए अब हम समूह के अवयवों के लिए कुछ घातांक नियम सिद्ध करें।

प्रमेय 7 : मान लीजिए G एक समूह है। $a \in G$ और $m, n \in \mathbf{Z}$ के लिए,

क) $(a^n)^{-1} = a^{-n} = (a^{-1})^n$,

ख) $a^m . a^n = a^{m+n}$,

ग) $(a^m)^n = a^{mn}$.

उपपत्ति : हम यहां (क) और (ख) को सिद्ध करेंगे तथा (ग) की उपपत्ति आपके लिए छोड़ देंगे (देखिए E 10)।

क) यदि $n = 0$, स्पष्ट है कि $(a^n)^{-1} = a^{-n} = (a^{-1})^n$.
अब मान लीजिए $n > 0$. चूंकि $aa^{-1} = e$, इसलिए
$e = e^n = (a\,a^{-1})^n$
$= (a\,a^{-1})(a\,a^{-1})\ldots(a\,a^{-1})$ (n बार)
$= a^n (a^{-1})^n$, क्योंकि $a\,a^{-1} = a^{-1}\,a$.
$\therefore (a^n)^{-1} = (a^{-1})^n$.
और $(a^{-1})^n = a^{-n}$, परिभाषा के अनुसार।
$\therefore (a^n)^{-1} = (a^{-1})^n = a^{-n}$, यदि $n > 0$.
यदि $n < 0$, तो $(-n) > 0$ और
$(a^n)^{-1} = [a^{-(-n)}]^{-1}$
$= [(a^{-n})^{-1}]^{-1}$, $n > 0$ की स्थिति से
$= a^{-n}$.
और $(a^{-1})^n = (a^{-1})^{-(-n)} = [(a^{-1})^{-1}]^{-n}$, $n > 0$ की स्थिति से
$= a^{-n}$.
अतः इस स्थिति में भी $(a^n)^{-1} = a^{-n} = (a^{-1})^n$.

ख) यदि $m = 0$ या $n = 0$, तो $a^{m+n} = a^m \cdot a^n$. मान लीजिए $m \neq 0$ और $n \neq 0$.

हम 4 स्थितियों पर विचार करेंगे।

स्थिति 1 ($m > 0$ और $n > 0$) : हम इस कथन को n पर आगमन करके सिद्ध करेंगे।
यदि $n = 1$, तब $a^m \cdot a = a^{m+1}$, परिभाषा के अनुसार। अब मान लीजिए कि $a^m \cdot a^{n-1} = a^{m+n-1}$.
तब, $a^m \cdot a^n = a^m(a^{n-1} \cdot a) = (a^m \cdot a^{n-1})a = a^{m+n-1} \cdot a$
$= a^{m+n}$.

इस तरह, आगमन नियम के अनुसार, सभी $m > 0$ और $n > 0$ के लिए (क) लागू होता है।

स्थिति 2 ($m < 0$ और $n < 0$) : तब $(-m) > 0$ और $(-n) > 0$. इस तरह, स्थिति 1 से $a^{-n} \cdot a^{-m} = a^{-(n+m)} = a^{-(m+n)}$. दोनों पक्षों का प्रतिलोम लेने पर और (क) का प्रयोग करने पर हमें निम्नलिखित प्राप्त होता है।

$a^{m+n} = (a^{-n} \cdot a^{-m})^{-1} = (a^{-m})^{-1} \cdot (a^{-n})^{-1} = a^m \cdot a^n$.

स्थिति 3 ($m > 0$, $n < 0$ और $m + n \geq 0$) : तब स्थिति 1 से $a^{m+n} \cdot a^{-n} = a^m$. दोनों पक्षों की दायीं ओर $a^n = (a^{-n})^{-1}$ से गुणा करने पर हमें $a^{m+n} = a^m \cdot a^n$ प्राप्त होता है।

स्थिति 4 . ($m > 0, n < 0$ और $m + n < 0$) : स्थिति 2 से $a^{-m} \cdot a^{m+n} = a^n$. दोनों पक्षों की बायीं ओर $a^m = (a^{-m})^{-1}$ से गुणा करने पर $a^{m+n} = a^m \cdot a^n$ प्राप्त होता है।
स्थितियाँ, जबकि $m < 0$ और $n > 0$, स्थितियाँ 3 और 4 के समान हैं। इसलिए सभी $a \in G$ और $m, n \in \mathbf{Z}$ के लिए
$a^{m+n} = a^m.a^n$.

इस प्रमेय की उपपत्ति को पूरा करने के लिए E 10 हल कीजिए।

E 10) अब आप प्रमेय 7 का (ग) सिद्ध कर सकते हैं।
(**संकेत** : स्थिति $n > 0$ के लिए n पर आगमन करके सिद्ध कीजिए। फिर $n < 0$ के लिए कथन को सिद्ध कीजिए।)

अब हम तीन महत्वपूर्ण समूहों का अध्ययन करेंगे।

2.5 तीन समूह

इस भाग में हम तीन समूहों—पूर्णांक माड्यूलो n का समूह, सममित समूह और सम्मिश्र संख्याओं का समुच्चय – पर विचार करेंगे। इनका प्रयोग हम इस पूरे पाठ्यक्रम में उदाहरण के रूप में कई बार करेंगे।

2.5.1 पूर्णांक माड्यूलो n (Integers Modulo n)

पूर्णांक समुच्चय $\mathbf{Z}$ और $n \in \mathbf{N}$ लीजिए। हम $\mathbf{Z}$ पर समशेषता संबंध को "a, b माड्यूलो n के **समशेष** (congruent) है यदि n, a − b को विभाजित करता हो" से परिभाषित करते हैं। इसे हम **$a \equiv b \pmod n$** से प्रकट करते हैं। उदाहरण के लिए,
$4 \equiv 1 \pmod 3$, क्योंकि $3 \mid (4 - 1)$.
इसी प्रकार, $(-5) \equiv 2 \pmod 7$ और $30 \equiv 0 \pmod 6$.

$\equiv$ एक तुल्यता संबंध है (देखिए भाग 1.4). अतः यह $\mathbf{Z}$ को असंयुक्त तुल्यता वर्गों में विभाजित करता है, जिन्हें हम **तुल्यता वर्ग माड्यूलो n** कहते हैं। हम r को आविष्ट करने वाले वर्ग को $\bar{r}$ से प्रकट करते हैं। इस तरह,

$\bar{r} = \{m \in \mathbf{Z} \mid m \equiv r \pmod n\}$.
इसलिए किसी r $(0 \leq r < n)$ के लिए पूर्णांक m, $\bar{r}$ का सदस्य होता है यदि और केवल यदि $n \mid (r - m)$, अर्थात् यदि और केवल यदि किसी $k \in \mathbf{Z}$ के लिए $r - m = kn$.
$\therefore \bar{r} = \{r + kn \mid k \in \mathbf{Z}\}$.
अब, यदि $m \geq n$, तो विभाजन-कलन विधि के अनुसार किसी $q, r \in \mathbf{Z}$ के लिए $m = nq + r$, जहां $0 \leq r < n$. अर्थात् किसी $r = 0, \ldots, n-1$ के लिए $m \equiv r \pmod n$. इसलिए सभी समशेषता वर्ग माड्यूलो n, $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ हैं। मान लीजिए,
$\mathbf{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.
हम $\mathbf{Z}_n$ पर संक्रिया + को $\bar{a} + \bar{b} = \overline{a+b}$ से परिभाषित करते हैं।

लेकिन, क्या यह संक्रिया सुपरिभाषित है? इसकी जांच करने के लिए हमें देखना है कि यदि $\mathbf{Z}_n$ में $\bar{a} = \bar{b}$ और $\bar{c} = \bar{d}$, तो $\overline{a+b} = \overline{c+d}$.
अब, $a \equiv b \pmod n$ और $c \equiv d \pmod n$.
इसलिए, ऐसे पूर्णांक k_1 और k_2 हैं जिनसे कि $a - b = k_1n$ और $c - d = k_2n$. परंतु फिर
$(a + c) - (b + d) = (a - b) + (c - d) = (k_1 + k_2)n$
$\therefore \overline{a+c} = \overline{b+d}$.

इस तरह, $\mathbf{Z}_n$ पर + एक सुपरिभाषित द्वि-आधारी संक्रिया है। उदाहरण के लिए, $\mathbf{Z}_4$ में
$\bar{2} + \bar{2} = \bar{0}$, क्योंकि $2 + 2 = 4$ और $4 \equiv 0 \pmod 4$.
$\mathbf{Z}_n$ में जोड़ की संक्रिया को समझने के लिए नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 11) $\mathbf{Z}_4$ पर + के लिए नीचे दी गई संक्रिया सारणी को भरिए।

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$				
$\bar{1}$				
$\bar{2}$				
$\bar{3}$				

आइए अब हम दिखाएं कि
($\mathbf{Z}_n$, +) एक क्रमविनिमेय समूह है।

i) $\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}\ \forall\ \bar{a}, \bar{b} \in \mathbf{Z}_n$, अर्थात् $\mathbf{Z}_n$ में जोड़ क्रमविनिमेय है।

ii) $\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + (\overline{b+c}) = \overline{a+(b+c)}$
$= \overline{(a+b)+c} = (\overline{a+b}) + \bar{c} = (\bar{a} + \bar{b}) + \bar{c}\ \forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbf{Z}_n$,
अर्थात् $\mathbf{Z}_n$ में जोड़ साहचर्य है।

iii) $\bar{a} + \bar{0} = \bar{a} = \bar{0} + \bar{a}\ \forall\ \bar{a} \in \mathbf{Z}_n$,
अर्थात् $\bar{0}$ जोड़ का तत्समक है।

iv) $\bar{a} \in \mathbf{Z}_n$ के लिए $\exists\ \overline{n-a} \in \mathbf{Z}_n$ जिससे कि
$\bar{a} + \overline{n-a} = \bar{n} = \bar{0} = \overline{n-a} + \bar{a}$.

इस तरह, जोड़ के सापेक्ष $\mathbf{Z}_n$ के प्रत्येक अवयव का एक प्रतिलोम होता है।

(i) से (iv) तक के गुणों को देखने से पता चलता है कि ($\mathbf{Z}_n$, +) एक आबेली समूह है।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 12) संबंध "समशेषता माड्यूलो 5" से निर्धारित **Z** के विभाजन का वर्णन दीजिए।

वास्तव में, हम $\bar{a} \cdot \bar{b} = \overline{ab}$ से $\mathbf{Z}_n$ पर गुणन भी परिभाषित कर सकते हैं। तब,
$\bar{a}\,\bar{b} = \bar{b}\,\bar{a}\ \forall\ \bar{a}, \bar{b} \in \mathbf{Z}_n$ और
$(\bar{a}\,\bar{b})\,\bar{c} = \bar{a}\,(\bar{b}\,\bar{c})\ \forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbf{Z}_n$.

इस तरह, $\mathbf{Z}_n$ में गुणन एक क्रमविनिमेय और साहचर्य द्वि-आधारी संक्रिया है।

$\mathbf{Z}_n$ का एक गुणनात्मक तत्समक, अर्थात् $\bar{1}$ भी है। लेकिन ($\mathbf{Z}_n$, ·) एक समूह नहीं है। इसका कारण यह है कि $\mathbf{Z}_n$ के हर अवयव का, जैसे कि $\bar{0}$ का, प्रतिलोम नहीं है।

अब मान लीजिए कि हम $\mathbf{Z}_n$ के शून्येतर अवयव, अर्थात् ($\mathbf{Z}_n^*$, ·) लेते हैं। क्या यह एक समूह है? उदाहरण के लिए, $\mathbf{Z}_4^* = \{\bar{1}, \bar{2}, \bar{3}\}$ एक समूह नहीं है, क्योंकि $\mathbf{Z}_4^*$ पर · एक द्वि-आधारी संक्रिया नहीं है, क्योंकि $\bar{2} \cdot \bar{2} = \bar{0} \notin \mathbf{Z}_4^*$. परन्तु किसी अभाज्य p के लिए ($\mathbf{Z}_p^*$, ·) एक आबेली समूह है।

E 13) दिखाइए कि ($\mathbf{Z}_5^*$, .) एक आबेली समूह है।
(संकेत : इसकी संक्रिया सारणी बनाइए।)

आइए अब हम सममित समूह पर चर्चा करें।

2.5.2 सममित समूह (Symmetric Group)

अब हम सममित समूह पर संक्षेप में चर्चा करेंगे। इस समूह पर हम इकाई 7 में विस्तृत चर्चा करेंगे।

मान लीजिए X एक अरिक्त समुच्चय है। हम देख चुके हैं कि फलनों का संयोजन X से X तक के सभी फलनों के समुच्चय $\mathcal{F}(X)$ पर द्वि-आधारी संक्रिया परिभाषित करता है। यह द्वि-आधारी संक्रिया साहचर्य है। तत्समक फलन I_X, $\mathcal{F}(X)$ में तत्समक है।

अब $\mathcal{F}(X)$ का उपसमुच्चय S(X) लीजिए, जहां
$S(X) = \{f \in \mathcal{F}(X) \mid f$ एकैकी आच्छादक है$\}$.

अतः $f \in S(X)$ यदि और केवल यदि $f^{-1} : X \to X$ का अस्तित्व हो। याद रखिए कि $f \circ f^{-1} = f^{-1} \circ f = I_X$. इससे यह भी पता चलता है कि $f^{-1} \in S(X)$.
अब S(X) के सभी f, g के लिए,
$(g \circ f) \circ (f^{-1} \circ g^{-1}) = I_X = (f^{-1} \circ g^{-1}) \circ (g \circ f)$, अर्थात् $g \circ f \in S(X)$.

इस तरह, S(X) पर $\circ$ एक द्वि-आधारी संक्रिया है।

आइए अब हम जांच करें कि $(S(X), \circ)$ एक समूह है या नहीं।

i) $\circ$ साहचर्य है, क्योंकि $(f \circ g) \circ h = f \circ (g \circ h) \ \forall f, g, h \in S(X)$.

ii) I_X तत्समक अवयव है, क्योंकि $f \circ I_X = f = I_X \circ f \ \forall f \in S(X)$.

iii) $f \in S(X)$ के लिए, f^{-1}, f का प्रतिलोम है।

इस तरह, हम पाते हैं कि $(S(X), \circ)$ एक समूह है। इसे X पर **सममित समूह** कहते हैं।

यदि समुच्चय X परिमित हो, मान लीजिए $X = \{1, 2, 3, \ldots, n\}$, तो हम S(X) को S_n से प्रकट करते हैं, और प्रत्येक $f \in S_n$ को **n प्रतीकों पर एक क्रमचय** (permutation) कहते हैं।

मान लीजिए हम S_n में एक अवयव f का निर्माण करना चाहते हैं। पहले हम f(1) ले सकते हैं। f(1), n प्रतीकों $1, 2, \ldots, n$ में से कोई भी प्रतीक हो सकता है। f(1) को चुनने के बाद हम समुच्चय $\{1, 2, \ldots, n\} \setminus \{f(1)\}$ में से $(n-1)$ विधियों से f(2) चुन सकते हैं, क्योंकि f, 1 1 है। आगमन से f(i) चुनने के बाद हम $(n-i)$ विधियों से $f(i+1)$ चुन सकते हैं। इस तरह, $(1 \times 2 \times \ldots\ldots \times n) = n!$ विधियों से हम f को चुन सकते हैं, अर्थात् S_n में $n!$ अवयव हैं। अपनी सुविधा के लिए हम $f \in S_n$ को

$$\begin{pmatrix} 1 & 2 & \cdots\cdots & n \\ f(1) & f(2) & & f(n) \end{pmatrix}$$

से निरूपित करते हैं।

उदाहरण के लिए, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ फलन
$f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\} : f(1) = 2, f(2) = 4, f(3) = 3, f(4) = 1$
को निरूपित करता है।

ऊपरी पंक्ति में अवयवों को किसी भी क्रम में रखा जा सकता है, अगर नीचे की पंक्ति के अवयवों का क्रम भी तदानुसार बदला जाए। इस तरह,

$\begin{pmatrix} 2 & 1 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ भी फलन f को निरूपित करता है।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 14) 3 प्रतीकों पर सभी क्रमचयों का समुच्चय S_3 लीजिए। इसके $3! (= 6)$ अवयव होंगे। इनमें से एक तो तत्समक फलन I है। दूसरा $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ है। क्या आप अन्य 4 अवयव बता सकते हैं?

E 14 को हल करने के दौरान आपको एक अवयव $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ अवश्य प्राप्त हुआ होगा। यहां $f(1) = 2$, $f(2) = 3$ और $f(3) = 1$. ऐसे क्रमचय को चक्र कहते हैं। निम्नलिखित परिभाषा को देखिए।

परिभाषा : $f \in S_n$ को **संघाई r वाला चक्र** कहते हैं यदि $X = \{1, 2, \ldots, n\}$ में ऐसे $x_1, \ldots, x_r$ हों जिनके लिए $f(x_i) = x_{i+1}$, $1 \le i \le r - 1$ के लिए और $f(x_r) = x_1$, और $t \ne x_1, \ldots, x_r$ के लिए $f(t) = t$. इस स्थिति में f को $(x_1\ x_2 \ldots x_r)$ लिखते हैं।

उदाहरण के लिए, $f = (2\ 4\ 5\ 10) \in S_{10}$ का अर्थ है कि $f(2) = 4$, $f(4) = 5$, $f(5) = 10$, $f(10) = 2$ और $f(j) = j \ \forall \ j \ne 2, 4, 5, 10$ के लिए। अर्थात्

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 3 & 5 & 10 & 6 & 7 & 8 & 9 & 2 \end{pmatrix}$$

ध्यान दीजिए कि चक्र के संकेतन में हम क्रमचय द्वारा नियत किए गए अवयवों का उल्लेख नहीं करते हैं। इसी प्रकार क्रमचय $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$, S_5 में चक्र $(1\ 2\ 5\ 3\ 4)$ है।

$f \in S_n$ अवयव x को **नियत** करता है, यदि $f(x) = x$.

आइए अब हम देखें कि दो क्रमचयों के संयोजन का परिकलन किस तरह करते हैं। इसके लिए S_5 में निम्नलिखित उदाहरण लीजिए।

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha\beta(1) & \alpha\beta(2) & \alpha\beta(3) & \alpha\beta(4) & \alpha\beta(5) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \alpha(5) & \alpha(3) & \alpha(4) & \alpha(1) & \alpha(2) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (2\ 4),$$

क्योंकि 1, 3 और 5 नियत अवयव हैं।

नीचे दिए गए प्रश्नों से आपको S_n के अवयवों का गुणनफल ज्ञात करने का कुछ अभ्यास हो जाएगा।

E 15) S_3 में $(1\ 3) \circ (1\ 2)$ ज्ञात कीजिए।

E 16) S_3 में निम्नलिखित के प्रतिलोम लिखिए :

क) $(1\ 2)$

ख) $(1\ 3\ 2)$

दिखाइए कि $((1\ 2) \circ (1\ 3\ 2))^{-1} \ne (1\ 2)^{-1} \circ (1\ 3\ 2)^{-1}$
(इससे पता चलता है कि प्रमेय 4 (ख) में हम $(ab)^{-1} = a^{-1} b^{-1}$ नहीं लिख सकते हैं।)

आइए अब हम ऐसे समूह के बारे में बात करें, जिससे शायद आप परिचित हों, लेकिन यह न जानते हों कि वह एक समूह है।

2.5.3 संमिश्र संख्याएं (Complex Numbers)

इस उपभाग में हम दिखाएंगे कि संमिश्र संख्याओं का समुच्चय जोड़ के सापेक्ष एक समूह है। संभवत: आप में से कुछ लोग संमिश्र संख्याओं के कुछ आधारभूत गुणों से परिचित न हों। हमने इन गुणों को इस इकाई के परिशिष्ट में दिया है।

वास्तविक संख्याओं के सभी क्रमित युग्मों (x, y) का समुच्चय C लीजिए, अर्थात् $C = \mathbf{R} \times \mathbf{R}$. C में जोड़ + और गुणन (.) की परिभाषा इस प्रकार दीजिए:

C के (x_1, y_1) और (x_2, y_2) के लिए

$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, और

$(x_1, y_1) . (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$.

खंड 3 में आप देखेंगे कि (C, + , ·) एक वलय और क्षेत्र भी है।

इससे एक बीजीय निकाय (C, + , ·) प्राप्त होता है जिसे सम्मिश्र संख्या निकाय कहते हैं। याद रखिए कि सम्मिश्र संख्याएं (x_1, y_1) और (x_2, y_2) बराबर होती हैं यदि और केवल यदि $x_1 = x_2$ और $y_1 = y_2$.

आप सत्यापित कर सकते हैं कि + और · क्रमविनिमेय और साहचर्य हैं। तथा

i) (0, 0) योज्य तत्समक है।

ii) C के (x, y) का योज्य प्रतिलोम $(-x, -y)$ है।

iii) (1, 0) गुणनात्मक तत्समक है।

iv) यदि C में $(x, y) \neq (0, 0)$, तो या तो $x^2 > 0$ या $y^2 > 0$ · अतः $x^2 + y^2 > 0$. तब

$$(x, y) \cdot \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right)$$
$$= \left(x \frac{x}{x^2 + y^2} - y \frac{-y}{x^2 + y^2}, x \frac{-y}{x^2 + y^2} + y \frac{x}{x^2 + y^2} \right)$$
$$= (1, 0)$$

इस तरह, $\left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2} \right)$, C में (x, y) का गुणनात्मक प्रतिलोम है।

इस तरह, (C, +) एक समूह है और (C^*, ·) एक समूह है। (हमेशा की तरह, यहां भी C^* शून्येतर सम्मिश्र संख्याओं के समुच्चय को प्रकट करता है।)

आइए अब हम देखें कि हमने इस इकाई में क्या किया है।

2.6 सारांश

इस इकाई में हमने

1) विभिन्न प्रकार की द्वि-आधारी संक्रियाओं पर चर्चा की है।

2) समूह की परिभाषा और उदाहरण दिए हैं।

3) समूह के अवयवों के लिए निरसन नियम और घातांक नियम को सिद्ध किया है तथा उनका प्रयोग किया है।

4) पूर्णांक माड्यूलो n के समूह, सममित समूह और सम्मिश्र संख्या समूह पर चर्चा की है।

हमने एक परिशिष्ट भी दिया है, जिसमें हमने सम्मिश्र संख्याओं के कुछ आधारभूत तथ्यों का उल्लेख किया है।

2.7 हल/उत्तर

E 1) क) $x \oplus y = y \oplus x \ \forall \ x, y \in \mathbf{R}$.

इसलिए $\oplus$ क्रमविनिमेय है।

$$(x \oplus y) \oplus z = (x + y - 5) \oplus z = (x + y - 5) + z - 5$$
$$= x + y + z - 10$$
$$= x \oplus (y \oplus z)$$

इसलिए $\oplus$ साहचर्य है।

N पर $\oplus$ संवृत नहीं है, क्योंकि $1 \oplus 1 \notin \mathbf{N}$.

ख) * क्रमविनिमेय है, साहचर्य नहीं है और N पर संवृत है।

ग) Δ क्रमविनिमेय नहीं है, साहचर्य नहीं है, N पर संवृत नहीं है।

E 2) क) $\oplus$ के सापेक्ष तत्समक अवयव 5 है।
मान लीजिए * के सापेक्ष e तत्समक अवयव है। तब

$x * e = x \implies 2(x+e) = x \implies e = \frac{-x}{2}$, जो x पर निर्भर करता है।

इसलिए **R** में ऐसा कोई नियत अवयव e नहीं है, जिसके लिए
$x * e = e * x = x \; \forall \, x \in \mathbf{R}$. अतः * का कोई तत्समक अवयव नहीं है।
इसी प्रकार, Δ का कोई तत्समक अवयव नहीं है।

ख) $\oplus$ के सापेक्ष x का प्रतिलोम $10 - x$ है। चूंकि अन्य संक्रियाओं के लिए कोई तत्समक नहीं है, इसलिए x^{-1} प्राप्त करने का कोई प्रश्न नहीं उठता।

E 3) $\wp(S) = \{\phi, \{0\}, \{1\}, \{0, 1\}\}$.
अतः सारणी है:

$\cap$	ϕ	$\{0\}$	$\{1\}$	S
ϕ	ϕ	ϕ	ϕ	ϕ
$\{0\}$	ϕ	$\{0\}$	ϕ	$\{0\}$
$\{1\}$	ϕ	ϕ	$\{1\}$	$\{1\}$
S	ϕ	$\{0\}$	$\{1\}$	S

E 4) जांच कीजिए कि दोनों ही G 1, G 2 और G 3 को संतुष्ट करते हैं।

E 5) क) और (घ) सत्य हैं।

ख) $\mathbf{R}^*$ अनंत आवेली समूह है।

ग) $(\mathbf{Z}^*, \cdot)$, G 1 और G 2 को संतुष्ट करता है, परन्तु G 3 को नहीं। ± 1 के अतिरिक्त, किसी भी पूर्णांक का गुणनात्मक प्रतिलोम नहीं होता।

E 6) $((a, b) * (c, d)) * (e, f)$
$= (ac, bc + d) * (e, f)$
$= (ace, (bc + d) * e, f)$
$= (a, b) * ((c, d) * (e, f))$
इस तरह, *, G 1' को संतुष्ट करता है।
$(a, b) * (1, 0) = (a, b) \; \forall \, (a, b) \in G.$
अतः G 3' लागू होता है।
इसलिए (G, *) एक समूह है।

E 7) $ba = ca \implies (ba)a^{-1} = (ca)a^{-1} \implies b = c.$

E 8) मान लीजिए $x \in G$. तब $gx = g = ge$. इसलिए प्रमेय 5 के अनुसार $x = e$.
$\therefore \; G = \{e\}$.

E 9) $(\mathbf{Z}, -)$ एक समूह नहीं है, क्योंकि G 1 संतुष्ट नहीं होता। किसी $a, b \in \mathbf{Z}$ के लिए
$a - (a - b) = b$. इसलिए किसी $a, b \in \mathbf{Z}$ के लिए $a - x = b$ का एक हल होता है।

E 10) स्पष्ट है कि $n = 0$ के लिए कथन सत्य है।
अब मान लीजिए $n > 0$. हम n पर आगमन लागू करेंगे। $n = 1$ के लिए कथन सत्य है।
अब मान लीजिए कि यह $n - 1$ के लिए सत्य है, अर्थात्, $(a^m)^{n-1} = a^{m(n-1)}$
तब, $(a^m)^n = (a^m)^{n-1+1} = (a^m)^{n-1} \cdot a^m$, (ख) से
$= a^{m(n-1)} \cdot a^m$
$= a^{m(n-1+1)}$, (ख) से
$= a^{mn}$.

इसलिए (ग) सत्य है $\forall\, n > 0$ और $\forall\, m \in Z$.
अब मान लीजिए $n < 0$. तब $(-n) > 0$.
$\therefore\ (a^m)^n = [(a^m)^{-n}]^{-1}$, (क) से
$= [a^{m(-n)}]^{-1}$, स्थिति $n > 0$ से
$= [a^{-mn}]^{-1}$
$= a^{mn}$, (क) से।
अतः $\forall\, m, n \in Z$, (ग) सत्य है।

E 11)

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

E 12) Z निम्नलिखित 5 तुल्यता वर्गों का असंयुक्त सम्मिलन है।
$\bar{0} = \{\ldots\ldots, -10, -5, 0, 5, 10, 15, \ldots\ldots\}$,
$\bar{1} = \{\ldots\ldots, -9, -4, 1, 6, 11, \ldots\ldots\}$,
$\bar{2} = \{\ldots\ldots, -8, -3, 2, 7, 12, \ldots\ldots\}$,
$\bar{3} = \{\ldots\ldots, -7, -2, 3, 8, 13, \ldots\ldots\}$,
$\bar{4} = \{\ldots\ldots, -6, -1, 4, 9, 14, \ldots\ldots\}$.

E 13) Z_5^* पर · की संक्रिया सारणी है:

	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

इससे पता चलता है कि Z_5^* पर · एक साहचर्य और क्रमविनिमेय द्वि-आधारी संक्रिया है, $\bar{1}$ गुणनात्मक तत्समक है और प्रत्येक अवयव का एक प्रतिलोम होता है।

इस तरह, $(Z_5^*, .)$ एक आबेली समूह है।

E 14) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

E 15) $f = (1\ 3)$, $g = (1\ 2)$.

तब $f \circ g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$,

$$= \begin{pmatrix} 1 & 2 & 3 \\ fg(1) & fg(2) & fg(3) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ f(2) & f(1) & f(3) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

लीजिए $f = (1\ \ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, केवल पंक्तियों का अदल-बदल करने पर।

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

$3\ \ 2)^{-1} = (2\ \ 3\ \ 1)$

$2) \circ (1\ \ 3\ \ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

तिलोम $\begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = (1\ 3)$ है।

परीत,

$(1\ \ 3\ \ 2)^{-1} = (1\ \ 2) \circ (1\ \ 2\ \ 3) = (2\ \ 3) \neq (1\ \ 3)$

: संमिश्र संख्याएं

श्र संख्या को वास्तविक संख्याओं के क्रमित युग्म से प्रकट किया जा सकता है।
श्र संख्याओं का समुच्चय है

$x, y \in \mathbf{R}\}.$

निरूपित करने की एक अन्य विधि $x + iy$ है, जहां $i = \sqrt{-1}$. हम x को $x + iy$ भाग (real part) और y को $x + iy$ का **अधिकल्पित भाग** (imaginary part) कहते

मिलते हैं, यदि हम $(x, 0)$ को x से और $(0, 1)$ को i से प्रकट करें। यह करने से

$0) + (0, 1)(y, 0)$

$0) + (0, y)$

$y).$

$(0,1) = (-1, 0) = -1.$

का प्रयोग करने के दौरान हम कभी-कभी संकेतन $x + iy$ का प्रयोग करेंगे, और तथ्य का प्रयोग करेंगे कि C के अवयवों को R^2 के बिन्दुओं से निरूपित किया जा

हैं कि

$$
\begin{aligned}
x_2 + iy_2) &= (x_1, y_1) + (x_2, y_2) \\
&= (x_1 + x_2, y_1 + y_2) \\
&= (x_1 + x_2) + i(y_1 + y_2), \text{ और}
\end{aligned}
$$

$$
\begin{aligned}
+ iy_2) &= (x_1, y_1)(x_2, y_2) \\
&= (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \\
&= (x_1x_2 - y_1y_2) + i(x_1y_2 + x_2y_1).
\end{aligned}
$$

मिश्र संख्या दी हुई हो तो हम उसका संयुग्मी परिभाषित करेंगे।

मिश्र संख्या $z = x + iy$ के लिए, संमिश्र संख्या $x + i(-y)$ को z का संयुग्मी कहते हैं। इसे $x - iy$ भी लिखते हैं और $\bar{z}$ से प्रकट करते हैं।

के निम्नलिखित गुण हैं:

एक वास्तविक संख्या है। वास्तव में, $z + \bar{z} = 2x$.

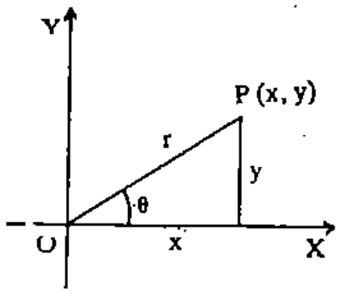
$x^2 + y^2$, एक ऋणेतर वास्तविक संख्या।

iii) किसी $z_1, z_2 \in C$ के लिए, $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$. ऐसा इसलिए है, क्योंकि

$$\begin{aligned}\overline{(x_1 + x_2) + i(y_1 + y_2)} &= (x_1 + x_2) - i(y_1 + y_2)\\ &= (x_1 - iy_1) + (x_2 - iy_2)\\ &= \bar{z}_1 + \bar{z}_2.\end{aligned}$$

iv) $\overline{z_1 z_2} = \bar{z}_1 . \bar{z}_2$, किसी भी $z_1, z_2 \in C$ के लिए

आइए अब हम संमिश्र संख्याओं को निरूपित करने की एक अन्य विधि पर विचार करें।



चित्र 3 : $x + iy$ का ज्यामितीय निरूपण

संमिश्र संख्याओं का ज्यामितीय निरूपण

हम जानते हैं कि संमिश्र संख्या $z = x + iy$ को समतल में बिन्दु (x, y) से निरूपित किया जाता है। यदि O बिन्दु $(0, 0)$ हो और $P, (x, y)$ हो (देखिए चित्र 3), तो हम जानते हैं कि दूरी $OP = \sqrt{x^2 + y^2}$. इसे संमिश्र संख्या z का **मापांक** (modulus) (या **निरपेक्ष मान**) कहते हैं और इसे $|z|$ से प्रकट करते हैं।

ध्यान दीजिए कि $\sqrt{x^2 + y^2} = 0$ यदि और केवल यदि $x = 0$ और $y = 0$.

आइए अब हम $|z|$ को r से और OP द्वारा धनात्मक x-अक्ष के साथ बनाए गए कोण को θ से प्रकट करें। तब θ को शून्येतर संमिश्र संख्या z का **एक कोणांक** (argument) कहते हैं। यदि θ, z का एक कोणांक हो, तो सभी $n \in Z$ के लिए $\theta + 2n\pi$ भी z का एक कोणांक होता है। लेकिन इन कोणांकों का एक अद्वितीय मान है, जो अंतराल $]-\pi, \pi]$ में स्थित होता है। इसे $x + iy$ का **मुख्य कोणांक** (principal argument) कहते हैं और **Arg (x + iy)** से प्रकट करते हैं।

चित्र 3 से आप देख सकते हैं कि,

$r = r\cos\theta$, $y = r\sin\theta$, अर्थात्

$z = (r\cos\theta, r\sin\theta) = r(\cos\theta + i\sin\theta) = re^{i\theta}$.

इसे संमिश्र संख्या $x + iy$ का **ध्रुवीय रूप** (polar form) कहते हैं।

अब, यदि $z_1 = r_1e^{i\theta_1}$ और $z_2 = r_2e^{i\theta_2}$, तब

$z_1z_2 = r_1r_2e^{i(\theta_1 + \theta_2)}$.

इस तरह, **z_1z_2 का एक कोणांक = z_1 का एक कोणांक + z_2 का एक कोणांक**

इसी प्रकार हम दिखा सकते हैं कि यदि $z_2 \neq 0$, तो

$\frac{z_1}{z_2}$ का एक कोणांक = z_1 का एक कोणांक − z_2 का एक कोणांक

विशेष रूप से, यदि $z (\neq 0)$ का कोणांक θ हो, तो $(-\theta)$, z^{-1} का एक कोणांक होगा।

संमिश्र संख्याओं से संबंधित एक महत्वपूर्ण प्रमेय का कथन देकर हम इस परिशिष्ट को समाप्त कर रहे हैं।

द मुआव्र (De Moivre) प्रमेय : यदि $z = r(\cos\theta + i\sin\theta)$ और $n \in N$, तो

$z^n = r^n(\cos n\theta + i\sin n\theta)$.

इकाई 3 उपसमूह

इकाई की रूपरेखा

3.1 प्रस्तावना

आप पूर्णांकों, परिमेय संख्याओं, वास्तविक संख्याओं और सम्मिश्र संख्याओं की बीजीय संरचनाओं के बारे में अध्ययन कर चुके हैं। आपने ध्यान दिया होगा कि न केवल $Z \subseteq Q \subseteq R \subseteq C$, बल्कि इन समुच्चयों में जोड़ और गुणा की संक्रियाएं भी समान होती हैं।

इस इकाई में आप समूहों के ऐसे उपसमुच्चयों से संबंधित कुछ और उदाहरणों का अध्ययन करेंगे, जो स्वयं समूह हैं। इस तरह की संरचना को उपसमूह कहते हैं। हम भाग 3.3 में इनके कुछ गुणों पर भी चर्चा करेंगे।

भाग 3.4 में हम कुछ ऐसी स्थितियों पर विचार करेंगे, जिनमें हम समूह के कुछ अवयवों से एक समूह प्राप्त करते हैं। विशेष रूप से हम ऐसे समूहों का अध्ययन करेंगे जिन्हें केवल एक अवयव से निर्मित किया जा सकता है।

आप इस इकाई को सावधानी से पढ़ें क्योंकि इसमें ऐसी आधारभूत संकल्पनाएं दी गई हैं जिनका प्रयोग इस पाठ्यक्रम के शेष भाग में बार-बार किया जाएगा।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- उपसमूह परिभाषित कर सकेंगे और इस बात की जांच कर सकेंगे कि दिए हुए समूह का उपसमुच्चय, समूह है या नहीं;
- जांच कर सकेंगे कि दो उपसमूहों का प्रतिच्छेद, सम्मिलन और गुणनफल एक समूह है या नहीं;
- चक्रीय समूह की संरचना और उसके गुणों की व्याख्या कर सकेंगे।

3.2 उपसमूह (Subgroup)

शायद आपने ध्यान दिया होगा कि समूह $(Z, +)$, $(Q, +)$ और $(R, +)$ सम्मिश्र संख्याओं के बड़े समूह $(C, +)$ में आविष्ट होते हैं। वे न केवल उपसमुच्चयों के रूप में, बल्कि समूहों के रूप में भी आविष्ट होते हैं। ये सभी समूह, उपसमूहों के उदाहरण हैं, जैसा कि आप देखेंगे।

परिभाषा : मान लीजिए $(G, *)$ एक समूह है। G के अरिक्त उपसमुच्चय H को G का उपसमूह कहते हैं, यदि

i) $a * b \in H \ \forall\ a, b \in H$, अर्थात् H पर $*$ एक द्वि-आधारी संक्रिया है; और

ii) $(H, *)$ स्वयं एक समूह है।

इस तरह, परिभाषा के अनुसार $(Q, +)$, $(R, +)$, और $(C, +)$, तीनों का एक उपसमूह $(Z, +)$, है।

अब यदि $(G, *)$ का एक उपसमूह $(H, *)$ हो, तो क्या $(H, *)$ का तत्समक अवयव $(G, *)$ के

तत्समक अवयव से भिन्न हो सकता है? आइएं, इस पर हम विचार करें। यदि $(H, *)$ का तत्समक h हो, तो किसी $a \in H$ के लिए $h * a = a * h = a$. साथ ही $a \in H \subseteq G$.

इसलिए $a * e = e * a = a$, जहां e, G का तत्समक है। अतः $h * a = e * a$.

G में दक्षिण निरसन करने पर हमें $h = e$ प्राप्त होता है।

इस तरह, जब कभी $(G, *)$ का एक उपसमूह $(H, *)$ हो, तो $e \in H$.

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कर सकते हैं।

E 1) यदि $(G, *)$ का उपसमुच्चय $(H, *)$ हो, तो क्या प्रत्येक $a \in H$ के लिए $a^{-1} \in H$?

E 1 तथा इससे पहले की गई चर्चा के आधार पर हम निम्नलिखित टिप्पणी दे सकते हैं।

टिप्पणी 1 : $(H, *)$ $(G, *)$ का एक उपसमूह होता है यदि और केवल यदि

i) $e \in H$,

ii) $a, b \in H \implies a * b \in H$, और

iii) $a \in H \implies a^{-1} \in H$.

यहां हम संकेतन के बारे में भी एक महत्वपूर्ण टिप्पणी देना चाहेंगे।

टिप्पणी 2 : यदि $(H, *)$, $(G, *)$ का एक उपसमूह हो तो हम केवल यही कहेंगे कि **H, G का एक उपसमूह है**, बशर्ते कि द्वि-आधारी संक्रियाओं के बारे में हमें कोई भ्रम न हो। इस तथ्य को हम $H \le G$ से भी प्रकट करेंगे।

अब हम एक उपसमुच्चय का उपसमूह होने के लिए एक महत्वपूर्ण आवश्यक और पर्याप्त प्रतिबंध पर चर्चा करेंगे।

प्रमेय 1 : मान लीजिए H समूह G का एक **अरिक्त** उपसमुच्चय है। तब H, G का एक उपसमूह होता है यदि और केवल यदि

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

उपपत्ति : आइए पहले हम मान लें कि $H \le G$. तब टिप्पणी 1 के अनुसार
$a, b \in H \implies a, b^{-1} \in H \implies ab^{-1} \in H$.

विलोमतः, $H \neq \phi$, इसलिए $\exists\, a \in H$. परन्तु तब $aa^{-1} = e \in H$.
और किसी $a \in H$ के लिए $ea^{-1} = a^{-1} \in H$.
अंत में, यदि $a, b \in H$, तो $a, b^{-1} \in H$.
तब $a(b^{-1})^{-1} = ab \in H$,

अर्थात् समूह की द्वि-आधारी संक्रिया के सापेक्ष H संवृत है।
अतः टिप्पणी 1 के अनुसार H एक उपसमूह है।

आइए अब हम उपसमूहों के कुछ उदाहरणों पर विचार करें। इन उदाहरणों को पढ़ते समय आप अनुभव करेंगे कि **आबेली समूह का उपसमूह आबेली** होता है।

उदाहरण 1 : समूह $(C^*, .)$ लीजिए। दिखाइए कि

$S = \{z \in C \mid |z| = 1\}$, $(C^*, .)$ का एक उपसमुच्चय है।

हल : चूंकि $1 \in S$, इसलिए $S \neq \phi$.
और $z_1, z_2 \in S$ के लिए

$|z_1 z_2^{-1}| = |z_1|\,|z_2^{-1}| = |z_1| \dfrac{1}{|z_2|} = 1$.

अतः $z_1 z_2^{-1} \in S$. इसलिए, प्रमेय 1 के अनुसार $S \le C^*$.

उदाहरण 2 : C पर सभी 2×3 आव्यूहों का समुच्चय $G = M_{2\times3}(C)$ लीजिए। सत्यापित कीजिए कि $(G, +)$ एक आबेली समूह है। दिखाइए कि

$S = \left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} \middle| a, b, c \in C \right\}$, G का एक उपसमूह है।

हल : हम G पर जोड़ को

$$\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} + \begin{bmatrix} p & q & r \\ s & t & u \end{bmatrix} = \begin{bmatrix} a+p & b+q & c+r \\ d+s & e+t & f+u \end{bmatrix}.$$

से परिभाषित करते हैं।

आप यह देख सकते हैं कि G पर + एक द्वि-आधारी संक्रिया है।

$O = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ योज्य तत्समक है और

$\begin{bmatrix} -a & -b & -c \\ -d & -e & -f \end{bmatrix}$, $\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix} \in G$

का प्रतिलोम है।

चूंकि $a + b = b + a \; \forall \; a, b \in C$, + आबेली भी है। इसलिए $(G, +)$ एक आबेली समूह है।

$H \leq (G, +) \Longleftrightarrow H \neq \phi$ और $a - b \in H \; \forall \; a, b \in H$.

अब चूंकि $O \in S$, इसलिए $S \neq \phi$. और

$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix}, \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} \in S$ के लिए

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} - \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} = \begin{bmatrix} 0 & a-d & b-e \\ 0 & 0 & c-f \end{bmatrix} \in S.$$

$\therefore S \leq G$

उदाहरण 3 : R पर सभी व्युत्क्रमणीय 3×3 आव्यूहों का समुच्चय $GL_3(R)$ लीजिए। अर्थात् $A \in GL_3(R)$ यदि और केवल यदि $\det(A) \neq 0$. दिखाइए कि $SL_3(R) = \{ A \in GL_3(R) \mid \det(A) = 1 \}$, $(GL_3(R), .)$ का एक उपसमूह है।

हल : 3×3 तत्समक आव्यूह $SL_3(R)$ में है। इसलिए $SL_3(R) \neq \phi$.
अब, $A, B \in SL_3(R)$ के लिए
$\det(AB^{-1}) = \det(A) \det(B^{-1}) = \det(A) \dfrac{1}{\det(B)} = 1,$
क्योंकि $\det(A) = 1$ और $\det(B) = 1$.
$\therefore AB^{-1} \in SL_3(R)$
$\therefore SL_3(R) \leq GL_3(R)$.

अब नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 2) दिखाइए कि किसी समूह G के संबंध में $\{e\}$ और G, G के उपसमूह हैं। ($\{e\}$ को तुच्छ उपसमूह (trivial subgroup) कहते हैं।)

अगला उदाहरण अति महत्वपूर्ण है, और इसका प्रयोग शायद आप कई बार करेंगे।

उदाहरण 4 : $(Z, +)$ का कोई भी अतुच्छ (non-trivial) उपसमूह mZ के रूप का होता है, जहां $m \in N$ और $mZ = \{ mt \mid t \in Z \} = \{ 0, \pm m, \pm 2m, \pm 3m, \ldots \}$.

हल : पहले हम दिखाएंगे कि mZ, Z का उपसमूह है। फिर हम दिखाएंगे कि यदि H, Z का एक उपसमूह है, $H \neq \{0\}$, तो किसी $m \in N$ के लिए $H = mZ$.

अब, $0 \in mZ$. इसलिए $mZ \neq \phi$. और $mr, ms \in mZ$ के लिए $mr - ms = m(r - s) \in mZ$.
इसलिए mZ, Z का एक उपसमूह है।

ध्यान दीजिए कि m, mZ का न्यूनतम धन पूर्णांक है।

अब, मान लीजिए $H \neq \{0\}$, Z का एक उपसमूह है और $S = \{i \mid i > 0, i \in H\}$. चूंकि $H \neq \{0\}$, इसलिए H में एक शून्येतर पूर्णांक k है। यदि $k > 0$, तो $k \in S$. यदि $k < 0$, तो $(-k) \in S$, क्योंकि $(-k) \in H$ और $(-k) > 0$.

इसलिए $S \neq \phi$.

स्पष्ट है कि $S \subseteq N$. अतः सुक्रमण सिद्धांत (भाग 1.6.1) के अनुसार S का एक न्यूनतम अवयव, मान लीजिए s, होता है। अर्थात् s, H का न्यूनतम धन पूर्णांक है।

अब $sZ \subseteq H$. आप बता सकते हैं कि ऐसा क्यों है? यह देखने के लिए कोई अवयव $st \in sZ$ लीजिए।

यदि $t = 0$, तो $st = 0 \in H$.
यदि $t > 0$, तो $st = s + s + \ldots + s$ (t बार) $\in H$.
यदि $t < 0$, तो $st = (-s) + (-s) + \ldots + (-s)$ ($-t$ बार) $\subseteq H$.

इसलिए $st \in H \ \forall \ t \in Z$. अर्थात् $sZ \in H$.

अब, मान लीजिए $m \in H$. विभाजनक-कलन विधि से (देखिए भाग 1.6.2) $\exists\, n, r \in Z, 0 \leq r < s$ जिनसे कि $m = ns + r$. इस तरह, $r = m - ns$.

लेकिन H, Z का उपसमूह है और $m, ns \in H$. इसलिए $r \in H$. अब S में s की न्यूनतमता से $r = 0$ होगा, अर्थात् $m = ns$. अतः $H \subseteq sZ$.

इस तरह, हमने सिद्ध कर लिया है कि $H = sZ$.

अगले उदाहरण को देखने से पहले, आइए हम देखें कि 1 के nवें मूल क्या हैं, अर्थात् कौन-सी सम्मिश्र संख्याएं z हैं, जिनके लिए $z^n = 1$.

इकाई 2 के परिशिष्ट से आप जानते हैं कि शून्येतर सम्मिश्र संख्या $z \in C$ का ध्रुवीय रूप $z = r(\cos\theta + i\sin\theta)$ होता है, जहां $r = |z|$ और θ, z का एक कोणांक है। और यदि z_1 का एक कोणांक θ_1 हो और z_2 का एक कोणांक θ_2 हो तो $\theta_1 + \theta_2$, $z_1 + z_2$ का एक कोणांक होता है। इस तथ्य की सहायता से हम 1 के nवें मूल ज्ञात करने का प्रयास करेंगे, जहां $n \in N$.

यदि $z = r(\cos\theta + i\sin\theta)$, 1 का nवां मूल हो, तो $z^n = 1$.

अतः, द मुआव्र प्रमेय के अनुसार

$1 = z^n = r^n(\cos n\theta + i\sin n\theta)$, अर्थात्

$$\cos(0) + i\sin(0) = r^n(\cos n\theta + i\sin n\theta). \qquad \ldots (1)$$

(1) के दोनों पक्षों के मापांकों की तुलना करने पर $r^n = 1$, अर्थात् $r = 1$ प्राप्त होता है।

(1) के दोनों पक्षों के कोणांकों की तुलना करने पर हम पाते हैं कि $0 + 2\pi k$ $(k \in Z)$ और $n\theta$ एक ही सम्मिश्र संख्या के कोणांक हैं। इस तरह, $2\pi k, k \in Z$, में से कोई भी मान $n\theta$ धारण कर सकता है। क्या इसका अर्थ है कि k के अलग-अलग मानों के लिए और $\theta = \frac{2\pi k}{n}$ के अलग-अलग मानों के लिए हमें 1 के अलग-अलग nवें मूल प्राप्त होते हैं? आइए इस सवाल का जवाब ढूंढें।

अब,

$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = \cos\frac{2\pi m}{n} + i\sin\frac{2\pi m}{n}$ यदि और केवल यदि किसी $t \in Z$ के लिए

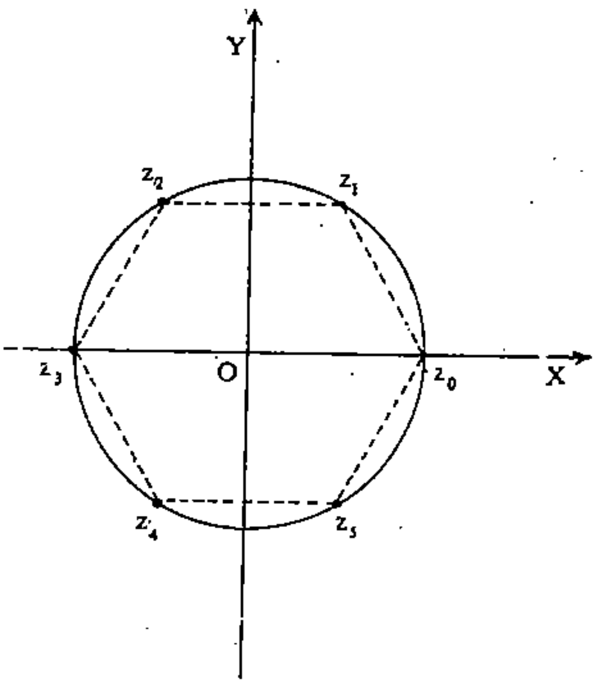
$\frac{2\pi k}{n} - \frac{2\pi m}{n} = 2\pi t$, यह तभी होता है यदि और केवल यदि $k = m + nt$, अर्थात्

$k \equiv m \pmod n$.

इस तरह, Z_n के प्रत्येक $\bar{r}$ के संगत हमें 1 का nवां मूल

$z = \cos \frac{2\pi r}{n} + i \sin \frac{2\pi r}{n}$ $(0 \leq r < n)$ प्राप्त होता है। ये ही 1 के सभी n वें मूल हैं।

उदाहरण के लिए, यदि $n = 6$, तो हमें 1 के 6वें मूल z_0, z_1, z_2, z_3, z_4 और z_5 प्राप्त होते हैं, जहां $z_j = \cos \frac{2\pi j}{6} + i \sin \frac{2\pi j}{6}$, $j = 0, 1, ..., 5$. चित्र 1 में आप देख सकते हैं कि ये सभी मूल उस वृत्त पर स्थित हैं, जिसकी त्रिज्या 1 है और केन्द्र (0, 0) पर है। ये एक सम-षट्भुज के शीर्ष हैं।



चित्र 1 : 1 के 6 वें मूल

अब, मान लीजिए $\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. तब 1 के सभी n मूल $1, \omega, \omega^2, ..., \omega^{n-1}$ होंगे, क्योंकि (द मुआव्र प्रमेय के अनुसार)

ω यूनानी अक्षर ओमेगा है।

$0 \leq j \leq n - 1$ के लिए $\omega^j = \cos \frac{2\pi j}{n} + i \sin \frac{2\pi j}{n}$.

मान लीजिए $U_n = \{1, \omega, \omega^2, ..., \omega^{n-1}\}$.

नीचे दिए गए प्रश्न में आपको U_n के अवयवों का एक रोचक गुण मिलेगा।

E 3) यदि $n > 1$ और $\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, तो दिखाइए कि
$1 + \omega + \omega^2 + ... + \omega^{n-1} = 0$.

अब हम C^* का एक परिमित उपसमूह प्राप्त करने की स्थिति में हैं।

उदाहरण 5 : दिखाइए कि $U_n \leq (C^*, .)$.

हल : स्पष्ट है कि $U_n \neq \phi$

अब, मान लीजिए $\omega^i, \omega^j \in U_n$.

तब, विभाजन-कलन विधि से हम $i + j = qn + r$ लिख सकते हैं, जहां $q, r \in \mathbf{Z}$ और $0 \leq r \leq n - 1$. परन्तु, तब $\omega^i . \omega^j = \omega^{i+j} = \omega^{qn+r} = (\omega^n)^q . \omega^r = \omega^r \in U_n$, क्योंकि $\omega^n = 1$. इस तरह, गुणन के सापेक्ष U_n संवृत है।

अंत में, यदि $\omega^i \in U_n$, तब $0 \le n - i \le n - 1$, और $\omega^i . \omega^{n-i} = \omega^n = 1$, अर्थात् सभी $1 \le i < n$ के लिए ω^i का प्रतिलोम ω^{n-i} है। अतः U_n, C^* का एक उपसमूह है।

ध्यान दीजिए कि U_n **कोटि n वाला एक परिमित समूह है और अनंत समूह C^* का एक उपसमूह है।** अतः प्रत्येक प्राकृतिक संख्या n के लिए हमें C^* का कोटि n वाला एक परिमित उपसमूह प्राप्त होता है।

इस भाग को समाप्त करने से पहले हम आपको एक और उपसमूह से परिचित कराएंगे।

परिभाषा : मान लीजिए कि G एक समूह है। तब समुच्चय
$Z(G) = \{ g \in G \mid xg = gx \ \forall \ x \in G \}$ को **G का केन्द्र** कहते हैं।

इस तरह, Z(G), G के उन अवयवों का समुच्चय है, जिनका G के प्रत्येक अवयव के साथ क्रमविनिमेय होता है।

उदाहरण के लिए, यदि G आबेली है, तो $Z(G) = G$.

अब हम दिखाएंगे कि $Z(G) \le G$.

प्रमेय 2 : किसी समूह G का केन्द्र G का उपसमूह होता है।

उपपत्ति : चूंकि $e \in Z(G)$, इसलिए $Z(G) \ne \phi$. अब

$a \in Z(G) \implies ax = xa \ \forall \ x \in G.$
$\implies x = a^{-1}xa \ \forall \ x \in G$, a^{-1} से पूर्व-गुणन करने पर।
$\implies xa^{-1} = a^{-1}x \ \forall \ x \in G$, a^{-1} से पश्च-गुणन करने पर।
$\implies a^{-1} \in Z(G)$.

और किन्हीं $a, b \in Z(G)$ और $x \in G$ के लिए
$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$.
$\therefore \ ab \in Z(G)$.

इस तरह, Z(G), G का एक उपसमूह है।

नीचे दिए गए प्रश्न को हल करने से आपको समूह का केन्द्र प्राप्त करने का कुछ अभ्यास हो जाएगा।

E 4) दिखाइए कि $Z(S_3) = \{ I \}$.
(संकेत : S_3 की संक्रिया सारणी लिखिए।)

आइए अब हम उपसमूहों के कुछ गुणों पर विचार करें।

3.3 उपसमूहों के गुण

आइए पहले हम दिखाएं कि संबंध "का उपसमूह है" संक्रामक है। इसकी उपपत्ति काफ़ी सरल है।

प्रमेय 3 : मान लीजिए G एक समूह है, H, G का उपसमूह है और K, H का उपसमूह है। तब K, G का उपसमूह होगा।

उपपत्ति : चूंकि $K \le H$, इसलिए $K \ne \phi$ और $ab^{-1} \in K \ \forall \ a, b \in K$. इसलिए $K \le G$.

आइए अब हम प्रमेय 3 के संदर्भ में Z के उपसमूहों पर विचार करें।

उदाहरण 6 : उदाहरण 4 में हम देख चुके हैं कि Z का कोई भी उपसमूह किसी $m \in N$ के लिए mZ के रूप का होता है। मान लीजिए mZ और kZ, Z के दो उपसमूह हैं। दिखाइए कि mZ, kZ का उपसमूह होता है, यदि और केवल यदि $k \mid m$.

हल : यहां हमें केवल यह दिखाना है कि $mZ \subseteq kZ \Longleftrightarrow k \mid m$.

अब $mZ \subseteq kZ \implies m \in mZ \subseteq kZ \implies m \in kZ \implies m = kr$, किसी $r \in Z$ के लिए।
$\implies k \mid m$.

विलोमतः, मान लीजिए $k \mid m$.

तब किसी $r \in Z$ के लिए $m = kr$. अब कोई $n \in mZ$ लीजिए और मान लीजिए कि $t \in Z$ जिससे कि $n = mt$. तब $n = mt = (kr)t = k(rt) \in kZ$.

अतः $mZ \subseteq kZ$.

इस तरह, $mZ \subseteq kZ$ यदि और केवल यदि $k \mid m$.

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E5) 9Z, Z के किन उपसमूहों का उपसमूह है?

अब हम प्रतिच्छेद और सम्मिलन की संक्रियाओं के सापेक्ष उपसमूहों के व्यवहारों के बारे में चर्चा करेंगे।

प्रमेय 4 : यदि H और K समूह G के दो उपसमूह हों, तो $H \cap K$ भी G का एक उपसमूह होता है।

उपपत्ति : चूंकि $e \in H$ और $e \in K$, जहां e, G का तत्समक है, इसलिए $e \in H \cap K$
इस तरह, $H \cap K \neq \phi$.

अब मान लीजिए $a, b \in H \cap K$. तब प्रमेय 1 के अनुसार यह दिखाना ही काफ़ी होगा कि $ab^{-1} \in H \cap K$. अब, चूंकि $a, b \in H$, इसलिए $ab^{-1} \in H$. इसी प्रकार, चूंकि $a, b \in K$, इसलिए $ab^{-1} \in K$. इस तरह, $ab^{-1} \in H \cap K$.

अतः $H \cap K$ समूह G का एक उपसमूह है।

यदि हम दो उपसमूहों के स्थान पर प्रमेय 4 में तीन या अधिक उपसमूह लें, तब भी उपपत्ति में दिए गए सभी तर्क लागू होते हैं। इस तरह, हमें निम्नलिखित परिणाम प्राप्त होता है।

प्रमेय 4 : यदि $\{H_i\}_{i \in I}$ समूह G के उपसमूहों का एक समुच्चय हो, तो $\bigcup_{i \in I} H_i$ भी G का एक समूह होता है।

क्या आप समझते हैं कि दो (या अधिक) उपसमूहों का सम्मिलन भी एक उपसमूह होता है? Z के दो उपसमूह 2Z और 3Z लीजिए। मान लीजिए $S = 2Z \cup 3Z$. अब $3 \in 3Z \subseteq S$, $2 \in 2Z \subseteq S$. परन्तु $1 = 3 - 2$, न तो 2Z में है और न ही 3Z में।

अतः S, (Z, +) का एक उपसमूह नहीं है। इस तरह, यदि A और B, G के उपसमूह हों तो यह आवश्यक नहीं है कि $A \cup B$ भी G का एक उपसमूह होगा। पर, यदि $A \subseteq B$, तो $A \cup B = B$, G का एक उपसमूह होगा। नीचे दिए गए प्रश्न से यह पता चलता है कि केवल यही एक स्थिति है जिसमें $A \cup B$, G का एक उपसमूह है।

E 6) मान लीजिए कि A और B समूह G के दो उपसमूह हैं। सिद्ध कीजिए कि $A \cup B$, G का एक उपसमूह होता है यदि और केवल यदि $A \subseteq B$ या $B \subseteq A$.

(संकेत : मान लीजिए $A \not\subseteq B$ और $B \not\subseteq A$. अब $a \in A \setminus B$ और $b \in B \setminus A$ लीजिए। तब दिखाइए कि $ab \notin A \cup B$. अतः $A \cup B \nleq G$. ध्यान दीजिए कि इसे सिद्ध करने से $A \cup B \leq G \implies A \subseteq B$ या $B \subseteq A$ सिद्ध हो जाता है।)

"$\nleq$ का उपसमूह नहीं है" को प्रकट करता है।

आइए अब हम समूह G के दो उपसमुच्चयों के गुणनफल पर विचार करें।

परिभाषा : मान लीजिए G एक समूह है और A, B समूह G के अरिक्त समुच्चय हैं। **A और B का गुणनफल समुच्चय** $AB = \{ab \mid a \in A, b \in B\}$ है। उदाहरण के लिए,

$$
\begin{aligned}
(2Z)(3Z) &= \{(2m)(3n) \mid m, n \in Z\} \\
&= \{6mn \mid m, n \in Z\} \\
&= 6Z.
\end{aligned}
$$

इस उदाहरण में हम देखते हैं कि दो उपसमूहों का गुणनफल एक उपसमूह है। लेकिन क्या यह बात हमेशा लागू होती है? इसके लिए समूह

$S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ और इसके उपसमूह $H = \{I, (1\ 2)\}$ और $K = \{I, (1\ 3)\}$ लीजिए। (आपको याद होगा कि (1 2), क्रमचय $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ है और (1 2 3) क्रमचय $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ है।)

$$
\begin{aligned}
\text{अब } HK &= \{I \circ I, I \circ (1\ 3), (1\ 2) \circ I, (1\ 2) \circ (1\ 3)\} \\
&= \{I, (1\ 3), (1\ 2), (1\ 3\ 2)\}
\end{aligned}
$$

अब $(1\ 3) \circ (1\ 2) = (1\ 2\ 3) \notin HK$. अर्थात् संयोजन के सापेक्ष HK संवृत नहीं है। इसलिए HK, G का एक उपसमूह नहीं होगा,

तो प्रश्न यह उठता है कि दो उपसमूहों का गुणनफल एक उपसमूह कब होगा? नीचे दिए गए परिणाम से इस प्रश्न का उत्तर प्राप्त हो जाता है।

प्रमेय 5 : मान लीजिए H और K, समूह G के उपसमूह हैं। तब HK समूह G का एक उपसमूह होता है यदि और केवल यदि $HK = KH$.

उपपत्ति : पहले मान लीजिए कि $HK \le G$. हम $HK = KH$ दिखाएंगे।

मान लीजिए $hk \in HK$. तब $(hk)^{-1} = k^{-1}h^{-1} \in HK$, क्योंकि $HK \le G$. इसलिए किसी $h_1 \in H$ और $k_1 \in K$ के लिए $k^{-1}h^{-1} = h_1k_1$. परन्तु तब $hk = (k^{-1}h^{-1})^{-1} = k_1^{-1}h_1^{-1} \in KH$. इस तरह, $HK \subseteq KH$.

अब हम दिखाएंगे कि $KH \subseteq HK$.

इसके लिए मान लीजिए $kh \in KH$. तब $(kh)^{-1} = h^{-1}k^{-1} \in HK$. परन्तु $HK \le G$. इसलिए $((kh)^{-1})^{-1} \in HK$, अर्थात् $kh \in HK$. इस तरह, $KH \subseteq HK$.

इस तरह, हमने दिखाया है कि $HK = KH$.

विलोमतः, मान लीजिए $HK = KH$. तब हमें सिद्ध करना है कि $HK \le G$. चूंकि $e = e^2 \in HK$, इसलिए $HK \ne \phi$. अब मान लीजिए $a, b \in HK$. तब किन्हीं $h, h_1 \in H$ और $k, k_1 \in K$ के लिए $a = hk$ और $b = h_1k_1$. तब
$ab^{-1} = (hk)(k_1^{-1}h_1^{-1}) = h[(kk_1^{-1})h_1^{-1}]$.
अब $(kk_1^{-1})h_1^{-1} \in KH = HK$. इसलिए $\exists\, h_2k_2 \in HK$ जिससे कि $(kk_1^{-1})h_1^{-1} = h_2k_2$. तब
$ab^{-1} = h(h_2k_2) = (hh_2)k_2 \in HK$.

इस तरह, प्रमेय 1 के अनुसार, $HK \le G$.

नीचे दिया गया परिणाम प्रमेय 5 का एक उपप्रमेय है।

उपप्रमेय : यदि H और K एक आबेली समूह G के उपसमूह हों, तो HK समूह G का एक उपसमूह होता है।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 7) क्या AB, S_4 का एक उपसमूह है, जहां $A = \{I, (1\ 4)\}$ और $B = \{I, (1\ 2)\}$?

अब हम जनक समुच्चयों पर विचार करेंगे।

3.4 चक्रीय समूह (Cyclic Group)

इस भाग में हम जनक समुच्चयों पर संक्षेप में चर्चा करेंगे, और फिर चक्रीय समूहों के बारे में विस्तार से बताएंगे।

मान लीजिए G एक समूह है और S, G का एक उपसमुच्चय है। G के उन सभी उपसमूहों का कुल $\mathcal{F}$ लीजिए जो S को आविष्ट करते हों, अर्थात्

$\mathcal{F} = \{H \mid H \leq G$ और $S \subseteq H\}$.

हमारा दावा है कि $\mathcal{F} \neq \phi$. ऐसा क्यों? क्या $G, \mathcal{F}$ में नहीं है? अब, प्रमेय 4 के अनुसार, $\bigcap_{H \in \mathcal{F}} H$, G का एक उपसमूह है।

ध्यान दीजिए कि

i) $S \subseteq \bigcap_{H \in \mathcal{F}} H$.

ii) $\bigcap_{H \in \mathcal{F}} H$, S को आविष्ट करने वाले G के उपसमूहों में से सबसे छोटा है। (क्योंकि, यदि K, G का एक उपसमूह हो जो S को आविष्ट करता हो, तो $K \in \mathcal{F}$, इसलिए $\bigcap_{H \in \mathcal{F}} \subseteq K$.)

इस टिप्पणी से हमें निम्नलिखित परिभाषा प्राप्त होती है।

परिभाषा : मान लीजिए S समूह G का एक उपसमुच्चय है। S को आविष्ट करने वाले G के उपसमूहों में से सबसे छोटे उपसमूह को **समूह S द्वारा जनित उपसमूह** कहते हैं। इसे $< S >$ से प्रकट करते हैं। इस तरह, $< S > = \cap \{H \mid H \leq G, S \subseteq H\}$.

यदि $S = \phi$, तब $< S > = \{e\}$.

यदि $< S > = G$, तो हम कहते हैं कि G **समुच्चय S से जनित होता है** और S, G **का जनक समुच्चय है।**

यदि समुच्चय S परिमित है, तो हम कहते हैं कि G **परिमिततः जनित** (finitely generated) है।

उदाहरण देने से पहले हम $< S >$ का वर्णन करने की एक और विधि देंगे। पिछली परिभाषा की तुलना में प्रयोग के लिए यह परिभाषा अधिक सरल है।

प्रमेय 6 : यदि S समूह G का एक अरिक्त उपसमुच्चय हो, तो
$< S > = \{a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \mid a_i \in S, 1 \leq i \leq k$ के लिए और $n_1, \dots n_k \in Z$ के लिए $\}$.

उपपत्ति : मान लीजिए

$A = \{a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \mid a_i \in S, 1 \leq i \leq k$ के लिए और $n_1, \dots, n_k \in Z$ के लिए$\}$.

अब क्योंकि $a_1, \dots, a_k \in S \subseteq < S >$ और $< S >$, G का एक उपसमूह है, इसलिए $a_i^{n_i} \in < S > \forall i, = 1, \dots, k$ अतः $a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \in < S >$. अर्थात् $A \subseteq < S >$.

आइए अब हम देखें कि क्यों $< S > \subseteq A$. हम दिखाएंगे कि A एक उपसमूह है जो S को आविष्ट करता है। तब, $< S >$ की परिभाषा के अनुसार $< S > \subseteq A$.

चूंकि किसी भी $a \in S$ के लिए $a = a^1 \in A$, इसलिए $S \subseteq A$. और चूंकि $S \neq \phi$, इसलिए $A \neq \phi$.

अब मान लीजिए $x, y \in A$.

तब $x = a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}, y = b_1^{m_1} b_2^{m_2} \dots b_r^{m_r}, a_i, b_j \in S$
$1 \leq i \leq k$ और $1 \leq j \leq r$ के लिए।
तब $xy^{-1} = (a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}) (b_1^{m_1} b_2^{m_2} \dots b_r^{m_r})^{-1}$
$= (a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}) (b_r^{-m_r} \dots b_1^{-m_1}) \in A$.

इस तरह, प्रमेय 1 के अनुसार A, G का एक उपसमूह है। अतः A, G का एक उपसमूह है, जो S को आविष्ट करता है। इसलिए, $< S > \subseteq A$. इससे पता चलता है कि $< S > = A$.

ध्यान दीजिए कि यदि $(G, +)$, S द्वारा जनित एक समूह हो, तो G का कोई भी अवयव $n_1a_1 + n_2a_2 + \dots + n_ra_r$ के रूप का होता है, जहां $a_1, \dots, a_r \in S$ और $n_1, n_2, \dots, n_r \in \mathbf{Z}$.

उदाहरण के लिए, $\mathbf{Z}$ विषम पूर्णांकों के समुच्चय $S = \{\pm 1, \pm 3, \pm 5, \dots\}$ से जनित है। ऐसा क्यों? यह देखने के लिए मान लीजिए $m \in \mathbf{Z}$. तब $m = 2^r s$, जहां $r \geq 0$ और $s \in S$. इस तरह, $m \in \langle S \rangle$. और इसलिए $\langle S \rangle = \mathbf{Z}$.

अब नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 8) दिखाइए कि $S = \{1\}$, $\mathbf{Z}$ को जनित करता है।

E 9) दिखाइए कि N का कोई उपसमुच्चय S सभी पूर्णांकों के समूह $\mathbf{Z}$ को जनित करता है यदि और केवल यदि S में ऐसे $s_1, \dots, s_k$ हों और $\mathbf{Z}$ में ऐसे $n_1, \dots, n_k$ हों जिनसे कि $n_1s_1 + \dots + n_ks_k = 1$.
(**संकेत** : प्रमेय 6 लागू कीजिए।)

E 10) दिखाइए कि यदि S समूह G को जनित करता हो और $S \subseteq T \subseteq G$, तो $G = \langle T \rangle$.

E 10 से पता चलता है कि एक समूह के अनेक जनक समुच्चय हो सकते हैं।
E 8 से ऐसे समूह का उदाहरण प्राप्त होता है, जो केवल एक ही अवयव से जनित होता है। इस प्रकार के समूह को हम एक विशेष नाम देते हैं।

परिभाषा : समूह G को **चक्रीय समूह** कहते हैं, यदि किसी $a \in G$ के लिए $G = \langle \{a\} \rangle$. हम प्राय: $\langle \{a\} \rangle$ को $\langle a \rangle$ लिखते हैं।

ध्यान दीजिए कि $\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$.

समूह G के उपसमूह H को **चक्रीय उपसमूह** कहते हैं, यदि वह चक्रीय समूह हो। इस तरह, $\langle (1\ 2) \rangle$, S_3 का एक चक्रीय उपसमूह है और $2\mathbf{Z} = \langle 2 \rangle$, $\mathbf{Z}$ का एक चक्रीय उपसमूह है।

इस संबंध में हम यहां एक टिप्पणी देना चाहेंगे।
टिप्पणी 3 : i) यदि $K \leq G$ और $a \in K$, तो $\langle a \rangle \subseteq K$. (क्योंकि $\langle a \rangle$, G का लघुतम उपसमूह है, जो a को आविष्ट करता है)।

ii) यह ज़रूरी नहीं कि $\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$ के सभी अवयव अलग-अलग हों। उदाहरण के लिए, $a = (1\ 2) \in S_3$ लीजिए। तब $\langle (1\ 2) \rangle = \{I, (1\ 2)\}$ क्योंकि $(1\ 2)^2 = I$, $(1\ 2)^3 = (1\ 2)$, आदि-आदि।

अब आप नीचे दिए गए सरल प्रश्नों को हल करने का प्रयास कर सकते हैं।

E 11) दिखाइए कि यदि $G \neq \{e\}$, तो $G \neq \langle e \rangle$.

E 12) दिखाइए कि $a \in G$ के लिए $\langle a \rangle = \langle a^{-1} \rangle$.

अब हम चक्रीय समूहों का एक गुण सिद्ध करेंगे।

प्रमेय 7 : प्रत्येक चक्रीय समूह आबेली होता है।

उपपत्ति : मान लीजिए $G = \langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$.
तब G के किसी x, y के लिए ऐसे $m, n \in \mathbf{Z}$ हैं जिनके लिए $x = a^m$, $y = a^n$. तब
$xy = a^m.a^n = a^{m+n} = a^{n+m} = a^n.a^m = yx$.
इस तरह G के सभी x, y के लिए $xy = yx$. अर्थात् G आबेली है।

ध्यान दीजिए कि प्रमेय 7 के अनुसार, प्रत्येक चक्रीय समूह आबेली होता है। परन्तु, इसका यह अर्थ नहीं है कि प्रत्येक आबेली समूह चक्रीय होता है। नीचे दिया गया उदाहरण लीजिए।

उदाहरण 7 : समुच्चय $K_4 = \{e, a, b, ab\}$ लीजिए और नीचे की सारणी द्वारा दी गई K_4 पर द्वि-आधारी संक्रिया लीजिए।

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

चित्र 2 : फ़ीलिक्स क्लाइन (1849-1925)

सारणी से पता चलता है कि $(K_4, .)$ एक समूह है। इस समूह को **क्लाइन 4-समूह** कहते हैं, जिसे पथप्रदर्शक जर्मन समूह सिद्धांतकार फ़ीलिक्स क्लाइन के नाम पर रखा गया है।

दिखाइए कि K_4 आबेली है, परन्तु चक्रीय नहीं।

हल : सारणी से हमें पता चलता है कि K_4 आबेली है। यदि यह चक्रीय होता तो यह e, a, b या ab से जनित होता। अब, $< e > = \{ e \}$ और $a^1 = a, a^2 = e, a^3 = a$, आदि-आदि।
इसलिए $< a > = \{ e, a \}$. इसी प्रकार $< b > = \{ e, b \}$ और $< ab > = \{ e, ab \}$.
अतः K_4 को e, a, b या ab जनित नहीं करता।
इस तरह, K_4 चक्रीय नहीं है।

प्रमेय 7 की सहायता से नीचे दिए गए प्रश्न को हल कीजिए।

E 13) दिखाइए कि S_3 चक्रीय नहीं है।

आइए अब चक्रीय समूहों के एक अन्य उपयोगी गुण पर विचार करें।

प्रमेय 8 : चक्रीय समूह का उपसमूह भी चक्रीय होता है।

उपपत्ति : मान लीजिए $G = < x >$ एक चक्रीय समूह है और H एक उपसमूह है।
यदि $H = \{ e \}$, तो $H = < e >$. अतः H चक्रीय होगा।
अब मान लीजिए $H \neq \{ e \}$. तब $\exists\, n \in Z$ जिससे कि $x^n \in H, n \neq 0$. चूंकि H एक उपसमूह है, इसलिए $(x^n)^{-1} = x^{-n} \in H$. अतः एक ऐसे धन पूर्णांक m (अर्थात् n या $-n$) का अस्तित्व होता है, जिसके लिए $x^m \in H$. इसलिए समुच्चय $S = \{ t \in N \mid x^t \in H \}$ रिक्त नहीं है। सुक्रमण सिद्धांत के अनुसार (देखिए भाग 1.6.1) S का एक न्यूनतम अवयव, मान लीजिए k, होता है। हम $H = < x^k >$ सिद्ध करेंगे।

अब क्योंकि $x^k \in H$, इसलिए $< x^k > \subseteq H$.

विलोमतः, मान लीजिए x^n, H का कोई अवयव है। विभाजन-कलन विधि से $n = mk + r$, जहां $m, r \in Z$ और $0 \leq r \leq k - 1$. परन्तु तब $x^r = x^{n-mk} = x^n . (x^k)^{-m} \in H$ क्योंकि $x^n, x^k \in H$.
परन्तु k न्यूनतम धन पूर्णांक है जिससे कि $x^k \in H$. अतः x^r, H में केवल तब हो सकता है, जबकि $r = 0$. और तब $n = mk$ और $x^n = (x^k)^m \in < x^k >$. इस तरह $H \subseteq < x^k >$. अतः $H = < x^k >$, अर्थात् H चक्रीय है।

प्रमेय 8 की सहायता से हम उदाहरण 4 के कथन को तुरन्त सिद्ध कर सकते हैं।

अब, प्रमेय 8 के कथनानुसार चक्रीय समूह का प्रत्येक उपसमूह चक्रीय होता है। परन्तु, इसका विलोम सत्य नहीं है। अर्थात् हम ऐसे समूह प्राप्त कर सकते हैं, जिनके सभी उचित उपसमूह तो चक्रीय होते हैं, परन्तु समूह चक्रीय नहीं होता। इसका एक उदाहरण लीजिए।

H, G का एक उचित उपसमूह होता है, यदि $H \subset G$ और H

3 प्रतीकों पर सभी क्रमचयों का समूह S_3 लीजिए। इसके उचित उपसमूह हैं :

$A = < I >$
$B = < (1\ 2) >$
$C = < (1\ 3) >$
$D = < (2\ 3) >$
$E = < (1\ 2\ 3) >$

जैसा कि आप देख सकते हैं, ये सभी चक्रीय हैं। परन्तु E 13 से आप जानते हैं कि S_3 चक्रीय नहीं है।

अब हम प्रमेय 8 के उपप्रमेय का कथन देंगे, जिसमें हम प्रमेय 8 की उपपत्ति में दिए गए महत्वपूर्ण तथ्य का उल्लेख करेंगे।

उपप्रमेय : मान लीजिए $H \neq \{e\}$, $< a >$ का एक उपसमूह है। तब $H = < a^n >$, जहां n ऐसा न्यूनतम धन पूर्णांक है, जिससे कि $a^n \in H$.

अब आप नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 14) दिखाइए कि प्रत्येक अनु-आबेली समूह का $\{e\}$ के अतिरिक्त एक अन्य उचित उपसमूह होता है।

E 15) Z_4 के सभी उपसमूह प्राप्त कीजिए। ध्यान दीजिए कि $Z_4 = < \bar{1} >$.

आइए अब हम देखें कि इस इकाई में हमने क्या किया है।

3.5 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों की चर्चा की है।

1) उपसमूह की परिभाषा और कुछ उदाहरण।
2) उपसमूहों का प्रतिच्छेद एक उपसमूह होता है।
3) दो उपसमूहों H और K का सम्मिलन एक उपसमूह होता है यदि और केवल यदि $H \subseteq K$ या $K \subseteq H$.
4) दो उपसमूहों H और K का गुणनफल एक उपसमूह होता है यदि और केवल यदि $HK = KH$
5) जनक समुच्चय की परिभाषा।
6) चक्रीय समूह आबेली होता है, परन्तु यह आवश्यक नहीं है कि विलोम भी सही हो।
7) चक्रीय समूह का कोई भी उपसमूह चक्रीय होता है, परन्तु आवश्यक नहीं है कि विलोम भी सही हो।

3.6 हल/उत्तर

E 1) हां, क्योंकि H स्वयं एक समूह है।

E 2) $\{e\} \neq \phi$ और $ee^{-1} = e \in \{e\}$.
$\therefore$ प्रमेय 1 के अनुसार $\{e\} \leq G$
$G \neq \phi$ और $x \in G$ के लिए $x^{-1} \in G$
$\therefore$ $a, b \in G$ के लिए $a, b^{-1} \in G$.
$\therefore$ $ab^{-1} \in G$. $\therefore$ $G \leq G$.

E 3) चूंकि $\omega^n = 1$, $(1 - \omega^n) = 0$, अर्थात्
$(1 - \omega)(1 + \omega + \omega^2 + \ldots + \omega^{n-1}) = 0$.
चूंकि $\omega \neq 1$, $1 + \omega + \omega^2 + \ldots + \omega^{n-1} = 0$.

E 4) इकाई 2 के E 14 से S_3 के अवयव याद कीजिए। S_3 की संक्रिया-सारणी लिखने पर आप पाएंगे कि केवल I ही S_3 के प्रत्येक क्रमचय के साथ क्रमविनिमेय करता है।

E 5) 9 के भाजक 1, 3 और 9 हैं।
इस तरह, 9Z केवल Z, 3Z और स्वयं का उपसमूह होगा।

E 6) हम जानते हैं कि यदि $A \subseteq B$ या $B \subseteq A$, तब $A \cup B$, A या B होगा। अतः यह G का एक उपसमूह होगा।

विलोमतः, हम मान लेंगे कि $A \not\subseteq B$ और $B \not\subseteq A$, और यह निष्कर्ष निकाल लेंगे कि $A \cup B \not\leq G$.

चूँकि $A \not\subseteq B$, इसलिए ऐसा $a \in A$ है, जिससे कि $a \notin B$. चूँकि $B \not\subseteq A$, इसलिए ऐसा $b \in B$ है, जिससे कि $b \notin A$. अब यदि $ab \in A$, तब $ab = c$, किसी $c \in A$ के लिए। तब $b = a^{-1}c \in A$, जो एक अंतर्विरोध है।

$\therefore ab \notin A$. इसी प्रकार $ab \notin B$. $\therefore ab \notin A \cup B$. लेकिन $a \in A \cup B$ और $b \in A \cup B$. इसलिए $A \cup B \not\leq G$.

E 7) $AB = \{I, (1\ 4), (1\ 2), (1\ 2\ 4)\}$.
परन्तु, $(1\ 2) \circ (1\ 4) = (1\ 4\ 2) \notin AB$. $\therefore AB \not\leq S_4$.

E 8) किसी $n \in Z$ के लिए $n = n \cdot 1 \in < \{1\} >$. $\therefore Z = < \{1\} >$.

E 9) पहले मान लीजिए कि $Z = < S >$. तब $1 \in < S >$.
$\therefore \exists\ s_1, ..., s_k \in S$ और $n_1, ..., n_k \in Z$ जिससे कि $n_1s_1 + ... + n_ks_k = 1$.
विलोमतः, मान लीजिए कि $\exists\ s_1, ..., s_k \in S$ और $n_1, ..., n_k \in Z$ जिससे कि $n_1s_1 + ... + n_ks_k = 1$.
तब $n \in Z$ के लिए $n = n \cdot 1 = nn_1s_1 + ... + nn_ks_k \in < S >$. $\therefore Z = < S >$.

E 10) हम जानते हैं कि $G = < S >$. इसलिए किसी भी $g \in G$ के लिए $\exists\ s_1, ..., s_k \in S$ और $n_1, ..., n_k \in Z$ जिससे कि $g = s_1^{n_1} ... s_k^{n_k}$. क्योंकि $S \subseteq T$, इसलिए $s_i \in T\ \forall\ i = 1, ..., k$.
$\therefore$ प्रमेय 6 के अनुसार $G = < T >$.

E 11) चूँकि $G \neq \{e\}$, इसलिए $\exists\ a \in G, a \neq e$.
चूँकि $a \neq e$, इसलिए $a \neq e^r$ किसी भी $r \in Z$ के लिए।
$\therefore a \notin < e >$. $\therefore G \neq < e >$.

E 12) हम दिखाएंगे कि $< a > \subseteq < a^{-1} >$ और $< a^{-1} > \subseteq < a >$.
अब $< a >$ का कोई अवयव है $a^n = (a^{-1})^{-n}$, $n \in Z$ के लिए।
$\therefore a^n \in < a^{-1} >$. $\therefore < a > \subseteq < a^{-1} >$.
इसी प्रकार, $< a^{-1} > \subseteq < a >$.
$\therefore < a > = < a^{-1} >$.

E 13) चूँकि S_3 आबेली नहीं है (उदाहरण के लिए $(1\ 3) \circ (1\ 2) \neq (1\ 2) \circ (1\ 3)$)
इसलिए प्रमेय 7 के अनुसार S_3 चक्रीय नहीं हो सकता।

E 14) मान लीजिए G एक अन्-आबेली समूह है। तब $G \neq \{e\}$.
$\therefore \exists\ a \in G, a \neq e$. तब $< a > \leq G$, $G \neq < a >$, क्योंकि G अन्-आबेली है।
$\therefore < a > \subsetneq G$.

E 15) चूँकि Z_4 चक्रीय है, इसलिए इसके सभी उपसमूह चक्रीय होंगे। इस तरह, इसके उपसमूह Z_4, $< \bar{2} >$, $< \bar{3} >$ और $\{\bar{0}\}$ हैं।

इकाई 4 लग्रांज प्रमेय

इकाई की रूपरेखा

4.1 प्रस्तावना

पिछली इकाई में हमने विभिन्न उपसमूहों की चर्चा की है। इस इकाई में हम देखेंगे कि किस प्रकार से एक उपसमूह एक समूह को तुल्यता-वर्गों में विभाजित कर सकता है। इसके लिए हमें सहसमुच्चयों की संकल्पना की आवश्यकता है।

भाग 4.3 में हम उपसमूह के अवयवों की संख्या से संबंधित एक अति उपयोगी परिणाम को सिद्ध करने के लिए सहसमुच्चयों का प्रयोग करेंगे। इस परिणाम से संबंधित प्रथम उल्लेख सुप्रसिद्ध गणितज्ञ लग्रांज (Lagrange) द्वारा बीजीय समीकरणों की साधनीयता पर लिखे गए शोध पत्र में मिलता है। आज इस प्रारंभिक प्रमेय को लग्रांज प्रमेय के नाम से जाना जाता है, हालांकि लग्रांज ने इसे केवल S_n के उपसमूहों के लिए सिद्ध किया था।

इस पाठ्यक्रम के खंड 2 का अध्ययन करने के दौरान आप लग्रांज प्रमेय का प्रयोग बार-बार करेंगे। इसलिए इस इकाई को ध्यान से पढ़ें।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- उपसमूह के वाम या दक्षिण सहसमुच्चय प्राप्त कर सकेंगे;
- समूह को उपसमूह के असंयुक्त समुच्चयों में विभाजित कर सकेंगे;
- लग्रांज प्रमेय को सिद्ध कर सकेंगे और उसका प्रयोग कर सकेंगे।

4.2 सहसमुच्चय (Cosets)

भाग 3.3 में हमने समूह के दो उपसमुच्चयों के गुणनफल को परिभाषित किया था। अब हम उस स्थिति पर विचार करेंगे, जिसमें दोनों में से एक उपसमुच्चय में केवल एक अवयव हो। वास्तव में हम स्थिति $H\{x\} = \{hx \mid h \in H\}$ पर विचार करेंगे, जहां H समूह G का एक उपसमूह है। हम $H\{x\}$ को Hx से प्रकट करेंगे।

परिभाषा : मान लीजिए H समूह G का एक उपसमूह है और मान लीजिए $x \in G$. हम समुच्चय

$Hx = \{hx \mid h \in H\}$

को G में H का दक्षिण सहसमुच्चय कहते हैं। अवयव x, Hx का एक प्रतिनिधि है।

इसी प्रकार हम वाम सहसमुच्चय

$xH = \{xh \mid h \in H\}$

को परिभाषित कर सकते हैं।

ध्यान दीजिए कि यदि समूह संक्रिया + हो, तो $x \in G$ से निरूपित $(G, +)$ में H के दक्षिण और वाम सहसमुच्चय क्रमशः

$H + x = \{h + x \mid h \in H\}$ और $x + H = \{x + h \mid h \in\}$ हैं।

आइए अब हम कुछ उदाहरणों पर विचार करें।

उदाहरण 1 : दिखाइए कि समूह G के उपसमूह H का G में एक दक्षिण एवं वाम सहसमुच्चय H है।

हल : G के तत्समक e से निरूपित G में H का दक्षिण सहसमुच्चय लीजिए। तब
$He = \{ he \mid h \in H \} = \{ h \mid h \in H \} = H.$
इसी प्रकार, $eH = H$.
इस तरह, समूह G में H का एक दक्षिण एवं वाम सहसमुच्चय H है।

उदाहरण 2 : Z में 4Z के दक्षिण सहसमुच्चय कौन-कौन से हैं?

हल : अब $H = 4Z = \{ ..., -8, -4, 0, 4, 8, 12, ... \}$.
H के दक्षिण सहसमुच्चय निम्नलिखित हैं :
$H + 0 = H$, उदाहरण 1 से।
$H + 1 = \{ ..., -11, -7, -3, 1, 5, 9, 13, ... \}$
$H + 2 = \{ ..., -10, -6, -2, 2, 6, 10, 14, ... \}$
$H + 3 = \{ ..., -9, -5, -1, 3, 7, 11, 15, ... \}$
$H + 4 = \{ ..., -8, -4, 0, 4, 8, 12, ... \} = H$

इसी प्रकार आप देख सकते हैं कि $H + 5 = H + 1, H + 6 = H + 2$, आदि-आदि।

आप यह भी देख सकते हैं कि $H - 1 = H + 3, H - 2 = H + 2, H - 3 = H + 1$, आदि-आदि।

इस तरह, अलग-अलग दक्षिण सहसमुच्चय $H, H + 1, H + 2$ और $H + 3$ हैं।

व्यापक रूप में, **Z में H (= nZ) के अलग-अलग दक्षिण सहसमुच्चय $H, H + 1, ..., H + (n - 1)$ हैं।** इसी प्रकार, Z में H = (nZ) के अलग-अलग वाम सहसमुच्चय $H, 1 + H, 2 + H, ..., (n - 1) + H$ हैं।

सहसमुच्चयों से संबंधित और उदाहरण देने से पहले आइए हम सहसमुच्चयों के कुछ गुणों पर चर्चा करें।

प्रमेय 1 : मान लीजिए H समूह G का एक उपसमूह है और मान लीजिए $x, y \in G$. तब
क) $x \in Hx$.

ख) $Hx = H \Longleftrightarrow x \in H$.

ग) $Hx = Hy \Longleftrightarrow xy^{-1} \in H$.

उपपत्ति : क) $x = ex$ और $e \in H$, इसलिए $x \in Hx$.

ख) आइए पहले हम मान लें कि $Hx = H$. तब, क्योंकि $x \in Hx$, इसलिए $x \in H$.

विलोमत:, मान लीजिए कि $x \in H$. हम दिखाएंगे कि $Hx \subseteq H$ और $H \subseteq Hx$. हम जानते हैं कि Hx का कोई भी अवयव hx के रूप का होता है, जहां $h \in H$. यह H में है, क्योंकि $h \in H$ और $x \in H$. इस तरह, $hx \subseteq H$.

अब मान लीजिए कि $h \in H$. तब $h = (hx^{-1})x \in Hx$, क्योंकि $hx^{-1} \in H$.

$\therefore H \subseteq Hx$.
$\therefore H = Hx$.

ग) $Hx = Hy \implies Hxy^{-1} = Hyy^{-1} = He = H \implies xy^{-1} \in H$, (ख) से।

विलोमत:, $xy^{-1} \in H \implies Hxy^{-1} = H \implies Hxy^{-1}y = Hy \implies Hx = Hy$. इस तरह, (ग) सिद्ध हो जाता है।

प्रमेय 1 में दिए गए गुण केवल दक्षिण सहसमुच्चयों के लिए सत्य नहीं होते। वे वाम सहसमुच्चयों के लिए भी सत्य हैं। इस संबंध में हम निम्नलिखित टिप्पणी दे रहे हैं।

टिप्पणी : प्रमेय 1 की उपपत्ति की तरह, हम सिद्ध कर सकते हैं कि यदि H, G का एक समूह हो और $x, y \in G$, तो

क) $x \in xH$

ख) $xH = H \Longleftrightarrow x \in H$

ग) $xH = yH \Longleftrightarrow x^{-1}y \in H$.

आइए अब हम समुच्चयों के कुछ और उदाहरण देखें।

उदाहरण 3 : मान लीजिए $G = S_3 = \{ I, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2) \}$ और H, $(1\,2\,3)$ से जनित G का चक्रीय उपसमूह है। G में H के वाम सहसमुच्चय प्राप्त कीजिए।

H, A_3 है, जो 3 प्रतीकों पर एकांतर समूह है।

हल : दो सहसमुच्चय हैं
$H = \{ I, (1\,2\,3), (1\,3\,2) \}$ और
$(1\,2)H = \{ (1\,2), (1\,2) \circ (1\,2\,3), (1\,2) \circ (1\,3\,2) \}$
$= \{ (1\,2), (2\,3), (1\,3) \}$.
अन्य सहसमुच्चयों को पाने के लिए आप प्रमेय 1 लागू करके देख सकते हैं कि
$(1\,2)H = (2\,3)H = (1\,3)H$, और
$(1\,2\,3)H = H = (1\,3\,2)H$.
इस तरह, H के अलग-अलग वाम सहसमुच्चय H और $(1\,2)H$ हैं।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए!

E 1) S_3 में $H = \langle (1\,2) \rangle$ के वाम और दक्षिण सहसमुच्चय प्राप्त कीजिए। दिखाइए कि किसी $x \in S_3$ के लिए $Hx \neq xH$.

आइए अब हम एक महत्वपूर्ण समूह, अर्थात् चतुष्टयी समूह (quaternion group) के सहसमुच्चयों पर विचार करें।

उदाहरण 4 : C पर 8, 2×2 आव्यूहों का निम्नलिखित समुच्चय लीजिए :
$Q_8 = \{ \pm I, \pm A, \pm B, \pm C \}$, जहां
$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $C = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ और $i = \sqrt{-1}$.

आप सत्यापित कर सकते हैं कि Q_8 के अवयवों के बीच निम्नलिखित संबंध लागू होते हैं:

$I^2 = I, A^2 = B^2 = C^2 = -I,$
$AB = C = -BA, BC = A = -CB, CA = B = -AC.$

अतः आव्यूह गुणन के सापेक्ष Q_8 एक अन्-आबेली समूह है। दिखाइए कि उपसमूह $H = \langle A \rangle$ के Q_8 में केवल दो अलग-अलग दक्षिण सहसमुच्चय हैं।

हल : $H = \langle A \rangle = \{ I, A, A^2, A^3 \} = \{ I, A, -I, -A \}$, क्योंकि $A^4 = I, A^5 = A$, आदि-आदि।
अतः ऊपर दिए गए संबंधों का प्रयोग करने पर
$HB = \{ B, C, -B, -C \}$.

प्रमेय 1 (ख) को लागू करने पर हम पाते हैं कि

$H = HI = HA = H(-I) = H(-A)$.

प्रमेय 1 (ग) को लागू करने पर हम पाते हैं कि

$HB = HC = H(-B) = H(-C)$.

अतः Q_8 में H के केवल दो अलग-अलग सहसमुच्चय हैं, H और HB.

नीचे दिए गए प्रश्न को हल करने से आप Q_8 को और अच्छी तरह से समझ सकेंगे।

E 2) दिखाइए कि $K = \{I, -I\}$, Q_8 का एक उपसमूह है। Q_8 में इसके सभी दक्षिण सहसमुच्चय प्राप्त कीजिए।

अब हम दिखाएंगे कि प्रत्येक समूह को इसके किसी भी उपसमूह के असंयुक्त सहसमुच्चयों के सम्मिलन के रूप में लिखा जा सकता है। इसके लिए हम G के अवयवों पर एक संबंध परिभाषित करते हैं।

परिभाषा : मान लीजिए H समूह G का एक उपसमूह है। हम G पर संबंध '$\sim$' को '$x \sim y$ यदि और केवल यदि $xy^{-1} \in H$' से परिभाषित करते हैं।

अतः प्रमेय 1 से हम पाते हैं कि $x \sim y$ यदि और केवल यदि $Hx = Hy$.

अब हम सिद्ध करेंगे कि यह संबंध एक तुल्यता संबंध है (देखिए इकाई 1)।

प्रमेय 2 : मान लीजिए H समूह G का एक उपसमूह है। तब '$x \sim y$ यदि और केवल यदि $xy^{-1} \in H$' से परिभाषित संबंध '$\sim$' एक तुल्यता संबंध है, और तुल्यता वर्ग समूह G में H के दक्षिण सहसमुच्चय हैं।

उपपत्ति : हमें सिद्ध करना है कि $\sim$ स्वतुल्य, सममित और संक्रामक है। सबसे पहले, किसी भी $x \in G$ के लिए $xx^{-1} = e \in H$.

$\therefore$ $x \sim x$, अर्थात् $\sim$ स्वतुल्य है।

इसके बाद, यदि $x, y \in G$ के लिए $x \sim y$, तो $xy^{-1} \in H$.

$\therefore$ $(xy^{-1})^{-1} = yx^{-1} \in H$. इस तरह, $y \sim x$, अर्थात् $\sim$ सममित है।

अंत में, यदि $x, y, z \in G$ ऐसे हों कि $x \sim y$ और $y \sim z$, तो $xy^{-1} \in H$ और $yz^{-1} \in H$.

$\therefore$ $(xy^{-1})(yz^{-1}) = x(y^{-1}y)z^{-1} = xz^{-1} \in H$. $\therefore$ $x \sim z$ अर्थात् $\sim$ संक्रामक है।

इस तरह, $\sim$ एक तुल्यता संबंध है।

$x \in G$ से निर्धारित तुल्यता-वर्ग है

$[x] = \{ y \in G \mid y \sim x \} = \{ y \in G \mid xy^{-1} \in H \}$.

अब, हम दिखाएंगे कि $[x] = Hx$.

इसके लिए, मान लीजिए $y \in [x]$.

तब प्रमेय 1 के अनुसार $Hy = Hx$.
और, क्योंकि $y \in Hy$, इसलिए $y \in Hx$.
अतः $[x] \subseteq Hx$.
अब Hx का कोई अवयव hx लीजिए। तब
$x(hx)^{-1} = x(x^{-1}h^{-1}) = (xx^{-1})h^{-1} = h^{-1} \in H$.
इसलिए $hx \sim x$, अर्थात् $hx \in [x]$. यह किसी भी $hx \in Hx$ के लिए सत्य है। इसलिए $Hx \subseteq [x]$.
इस तरह, हमने दिखाया है कि $[x] = Hx$.

प्रमेय 2 और इकाई 1 के प्रमेय 1 (घ) की सहायता से हम निम्नलिखित टिप्पणी दे सकते हैं।

टिप्पणी : यदि Hx और Hy समूह G के उपसमूह H के दो दक्षिण सहसमुच्चय हों, तो

$Hx = Hy$ या $Hx \cap Hy = \phi$.

ध्यान दीजिए कि प्रमेय 2 और ऊपर दी गई टिप्पणी के अनुसार समूह G का कोई उपसमूह H, G को असंयुक्त दक्षिण सहसमुच्चयों में विभाजित करता है।

ठीक ऊपर की तरह हम सिद्ध कर सकते हैं कि

i) G में H के कोई भी दो वाम सहसमुच्चय समान या असंयुक्त होते है, और

ii) G में H के अलग-अलग वाम सहसमुच्चयों का असंयुक्त सम्मिलन G है।

उदाहरण के लिए, $S_3 = <(1\ 2\ 3)> \cup (1\ 2) <(1\ 2\ 3)>$ (उदाहरण 3 की सहायता से)।

अब शायद आप नीचे दिए गए प्रश्नों को हल करना चाहेंगे।

E 3) मान लीजिए H समूह G का एक उपसमूह है। दिखाइए कि H के अवयवों और H के दक्षिण अथवा वाम सहसमुच्चय के अवयवों में एकैकी संगति होती है।
(**संकेत** : दिखाइए कि फलन $f : H \longrightarrow Hx : f(h) = hx$ एकैकी आच्छादक है।)

E 4) Z को 5Z के असंयुक्त सहसमुच्चयों के सम्मिलन के रूप में लिखिए।

E 3 को ध्यान में रखकर हम कह सकते हैं कि यदि H समूह G का एक परिमित उपसमूह हो, तो **H के प्रत्येक सहसमुच्चय में अवयवों की संख्या वही होती है जो H में अवयवों की संख्या है।**

हम अगले भाग में इस तथ्य का प्रयोग परिमित समूह के उपसमूह के सहसमुच्चयों की संख्या से संबंधित प्रारंभिक प्रमेय को सिद्ध करने में करेंगे।

4.3 लग्रांज प्रमेय

इस भाग में पहले हम परिमित समूह की कोटि को परिभाषित करेंगे और फिर दिखाएंगे कि उपसमूह की कोटि समूह की कोटि को विभाजित करती है।

आइए एक परिभाषा से शुरू करें।

परिभाषा : परिमित समूह G की **कोटि** (order) समूह G के अवयवों की संख्या होती है। इसे $o(G)$ से प्रकट किया जाता है।

उदाहरण के लिए, $o(S_3) = 6$ और $o(A_3) = 3$. (आपको याद होगा कि
$A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$!)
आप यह भी देख सकते हैं कि $o(Z_n) = n$ और भाग 2.5.2 से आप जानते हैं कि $o(S_n) = n!$

अब मान लीजिए G एक परिमित समूह है और H समूह G का एक उपसमूह है। हम G में H के दक्षिण सहसमुच्चयों के समुच्चय और G में H के वाम सहसमुच्चयों के समुच्चय के बीच के फलन f को
$f : \{Hx \mid x \in G\} \longrightarrow \{yH \mid y \in G\} : f(Hx) = x^{-1}H$
से परिभाषित करते हैं।
अब E 5 हल कीजिए।

E 5) सत्यापित कीजिए कि f एकैकी आच्छादक है।

E 5 से हमें पता चलता है कि G में H के दक्षिण सहसमुच्चयों और वाम सहसमुच्चयों के बीच एकैकी संगति है। इसलिए G में H के अलग-अलग दक्षिण सहसमुच्चयों की संख्या और G में H के अलग-अलग वाम सहसमुच्चयों की संख्या बराबर होती है।

परिभाषा : मान लीजिए H परिमित समूह G का एक उपसमूह है। हम G में H के अलग-अलग सहसमुच्चयों की संख्या को G में H का **सूचकांक** (index) कहते हैं और इसे $|G : H|$ से प्रकट करते हैं।

इस तरह, उदाहरण 3 से हम देखते हैं कि $|S_3 : A_3| = 2$.

ध्यान दीजिए कि यदि हम $H = \{e\}$ लें, तो
$|G : \{e\}| = o(G)$, क्योंकि $\{e\}g = \{g\} \ \forall\ g \in G$ और $\{e\}g \neq \{e\}g'$ यदि $g \neq g'$.

आइए अब हम उपसमूहों की कोटि पर विचार करें। भाग 3.4 में आपने देखा था कि S_3 के उपसमूहों की कोटियां 1, 2, 3 और 6 हैं। ये सभी संख्याएं $o(S_3) = 6$ को विभाजित करती हैं। यह तथ्य परिमित समूहों से संबंधित एक मूलभूत प्रमेय की विशेष स्थिति है। इसकी शुरुआत हमें 1770 में सुप्रसिद्ध फ्रांसिसी गणितज्ञ लग्रांज द्वारा लिखे गए शोध पत्र में मिलती है। उन्होंने इस परिणाम को केवल क्रमचय समूहों के लिए सिद्ध किया था। व्यापक परिणाम को शायद सुप्रसिद्ध गणितज्ञ एवरीस्त गाल्वा ने 1830 में सिद्ध किया था।

चित्र 1 : जोसेफ़ लुई लग्रांज
(1736-1813)

प्रमेय 3 (लग्रांज) : मान लीजिए H परिमित समूह G का एक उपसमूह है। तब
$o(G) = o(H)|G : H|$.

इस तरह, $o(H)$, $o(G)$ को विभाजित करता है, और $|G : H|$, $o(G)$ को विभाजित करता है।

उपपत्ति : आप जानते हैं कि हम G को H के असंयुक्त दक्षिण सहसमुच्चयों के सम्मिलन के रूप में लिख सकते हैं। मान लीजिए कि
$Hx_1, Hx_2, ..., Hx_r$ समूह G में H के सभी अलग-अलग सहसमुच्चय हैं। तब

$$G = Hx_1 \cup Hx_2 \cup ... \cup Hx_r \qquad ... (1)$$

और $|G : H| = r$.

E 3 से हम जानते हैं कि

$$|Hx_1| = |Hx_2| = ... = |Hx_r| = o(H).$$

इस तरह, (1) के दाएं पक्ष के सम्मिलन में अवयवों की कुल संख्या है

$$o(H) + o(H) + ... + o(H) \text{ (r बार)} = ro(H).$$

इसलिए (1) के अनुसार $o(G) = ro(H)$
$= o(H)|G : H|$.

जब हम परिमित समूह के सभी उपसमूहों को प्राप्त करना चाहेंगे तब आप लग्रांज प्रमेय के महत्व को समझ सकेंगे।

उदाहरण के लिए, मान लीजिए हमें कोटि 35 वाले समूह G के सभी उपसमूह ज्ञात करने के लिए कहा गया हो। तब संभव उपसमूह केवल कोटि 1, 5, 7 और 35 वाले होंगे। इसलिए हमें कोटि 2 या 4 वाले उपसमूहों को पता लगाने में समय बरबाद करने की आवश्यकता नहीं।

वास्तव में, हम लग्रांज प्रमेय की सहायता से कई सुंदर परिणाम प्राप्त कर सकते हैं। आइए हम अवयवों की कोटि से संबंधित कुछ परिणाम सिद्ध करें। इसके लिए पहले हम "अवयव की कोटि" को परिभाषित करेंगे।

परिभाषा : मान लीजिए G एक समूह है और $g \in G$. तब **g की कोटि** चक्रीय उपसमूह $<g>$ की कोटि होती है, यदि $<g>$ परिमित हो तो। इस परिमित संख्या को हम $o(g)$ से प्रकट करते हैं।

यदि $<g>$, G का अनंत उपसमूह हो, तो हम कहते हैं कि **g की कोटि** अपरिमित है।

अब किसी परिमित कोटि वाले $g \in G$ को लें। तब समुच्चय $\{e, g, g^2, ...\}$ परिमित होगा। अतः g के सभी घात अलग-अलग नहीं हो सकते। इसलिए किसी $r > s$ के लिए $g^r = g^s$.

तब $g^{r-s} = e$ और $r - s \in N$.

इस तरह, समुच्चय $\{t \in N \mid g^t = e\}$ अरिक्त है। अतः सुक्रमण सिद्धांत के अनुसार इसका न्यूनतम अवयव होगा। मान लीजिए n ऐसा न्यूनतम धन पूर्णांक है जिससे कि $g^n = e$. तब $<g> = \{e, g, g^2, ..., g^{n-1}\}$.

इसलिए $o(g) = o(<g>) = n$.

अर्थात् $o(g)$ ऐसा न्यूनतम धन पूर्णांक है जिससे कि $g^n = e$. (ध्यान दीजिए कि यदि $g \in (G, +)$, तो $o(g)$ ऐसा न्यूनतम धन पूर्णांक n है, जिससे कि $ng = e$.)

$o(g) = 1$ यदि और केवल यदि $g = e$.

अब मान लीजिए कि $g \in G$ अपरिमित कोटि का है। तब $m \neq n$ के लिए $g^m \neq g^n$.
(क्योंकि यदि $g^m = g^n$, तो $g^{m-n} = e$, अर्थात् $< g >$ परिमित समूह है।)

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास करें।

E 6) निम्नलिखित अवयवों की कोटियां क्या हैं?

(क) $(1\ 2) \in S_3$

(ख) $I \in S_4$

(ग) $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in Q_8$

(घ) $\bar{3} \in Z_4$

(ङ) $1 \in R$

आइए अब हम अवयव की कोटि के संबंध में एक महत्वपूर्ण परिणाम सिद्ध करें।

प्रमेय 4 : मान लीजिए G एक समूह है और $g \in G$ कोटि n का है। तब $m \in N$ के लिए $g^m = e$ होता है यदि और केवल यदि $n \mid m$.

उपपत्ति : पहले हम दिखाएंगे कि $g^m = e \implies n \mid m$. इसके लिए समुच्चय
$S = \{ r \in Z \mid g^r = e \}$ लीजिए।
अब $n \in S$. और यदि $a, b \in S$, तो
$g^a = e = g^b$. अतः $g^{a-b} = g^a (g^b)^{-1} = e$. इसलिए $a - b \in S$. इस तरह, $S \leq Z$.

अतः इकाई 3 के उदाहरण 4 से हम पाते हैं कि $S = nZ$. याद रहे कि n, S में न्यूनतम धन पूर्णांक है।

अब यदि किसी $m \in N$ के लिए $g^m = e$, तो $m \in S = nZ$. इसलिए $n \mid m$.

आइए अब हम दिखाएँ कि $n \mid m \implies g^m = e$.
चूंकि $n \mid m$, इसलिए किसी $t \in Z$ के लिए $m = nt$. तब $g^m = g^{nt} = (g^n)^t = e^t = e$. इस तरह, प्रमेय सिद्ध हो जाता है।

अब हम चक्रीय समूह में अवयवों की कोटियों से संबंधित परिणाम को सिद्ध करने के लिए प्रमेय 4 का प्रयोग करेंगे।

प्रमेय 5 : मान लीजिए $G = < g >$ एक चक्रीय समूह है।

क) यदि g अपरिमित कोटि का हो, तो प्रत्येक $m \in Z$ के लिए g^m भी अपरिमित कोटि का होगा।

ख) यदि $o(g) = n$, तो

$$o(g^m) = \frac{n}{(n, m)} \ \forall \ m = 1, \ldots, n-1$$ ((n, m), n और m का g.c.d. है।)

उपपत्ति : क) कोई अवयव अपरिमित कोटि का होता है यदि और केवल यदि इसके सभी घात अलग-अलग हों। हम जानते हैं कि g के सभी घात अलग-अलग हैं। हमें दिखाना है कि g^m के सभी घात अलग-अलग हैं। यदि संभव हो, तो मान लीजिए कि $(g^m)^t = (g^m)^w$. तब $g^{mt} = g^{mw}$ पर तब $mt = mw$. अतः $t = w$. इससे पता चलता है कि g^m के सभी घात अलग-अलग हैं। इसलिए g^m अपरिमित कोटि का है।

ख) चूंकि $o(g) = n$, $G = \{ e, g, \ldots, g^{n-1} \}$.
चूंकि $< g^m >$, G का एक उपसमूह है, इसलिए यह परिमित कोटि का होगा। इस तरह, हम पाते हैं कि g^m परिमित कोटि का है। मान लीजिए $o(g^m) = t$. हम दिखाएंगे कि $t = \frac{n}{(n, m)}$.

अब, $g^{mt} = (g^m)^t = e \implies n \mid tm$, प्रमेय 4 के अनुसार।

मान लीजिए $d = (n, m)$. तब हम $n = n_1 d, m = m_1 d$ लिख सकते हैं, जहां $(m_1, n_1) = 1$.

तब $n_1 = \frac{n}{d} = \frac{n}{(n, m)}$.

अब, $n \mid tm \implies n \mid tm_1 d \implies n_1 d \mid tm_1 d \implies n_1 \mid tm_1$.
लेकिन $(n, m_1) = 1$. इसलिए, $n_1 \mid t$. ... (1)
और, $(g^m)^{n_1} = g^{m_1 d n_1} = g^{m_1 n} = (g^n)^{m_1} = e^{m_1} = e$.

इस तरह, $o(g^m)$ की परिभाषा और प्रमेय 4 से हमें
$t \mid n_1$
प्राप्त होता है। (1) और (2) बताते हैं कि ... (2)

$t = n_1 = \frac{n}{(n, m)}$,

अर्थात् $o(g^m) = \frac{n}{(n, m)}$.

इस परिणाम का प्रयोग करने पर हम पाते हैं कि

Z_{12} में $o(\bar{4})$, $\frac{12}{(12, 4)} = 3$ है।

अगले प्रश्न को हल करने से आपको प्रमेय 5 का प्रयोग करने का कुछ अभ्यास हो जाएगा।

E 7) $\bar{2}, \bar{4}$ और $\bar{5} \in Z_{18}$ की कोटियां ज्ञात कीजिए।

अगला प्रश्न लग्राज़ प्रमेय का एक नतीजा है।

E 8) मान लीजिए G एक परिमित समूह है और $x \in G$. तब दिखाइए कि $o(x)$, $o(G)$ को विभाजित करता है। विशेष रूप से दिखाइए कि $x^{o(G)} = e$.

हम परिमित समूह सिद्धांत के एक सरल, लेकिन महत्वपूर्ण, परिणाम को सिद्ध करने के लिए E 8 में दिए गए परिणाम का प्रयोग करेंगे।

प्रमेय 6 : अभाज्य कोटि वाला प्रत्येक समूह चक्रीय होता है।

उपपत्ति : मान लीजिए G अभाज्य कोटि p वाला एक समूह है। क्योंकि $p \neq 1$, इसलिए $\exists\, a \in G$ जहां $a \neq e$. अब E 8 और प्रमेय 4 से $o(a) \mid p$. इसलिए

$o(a) = 1$ या $o(a) = p$. क्योंकि $a \neq e$, इसलिए $o(a) \geq 2$. इस तरह, $o(a) = p$, अर्थात् $o(< a >) = p$. इसलिए $< a > \leq G$ और $o(< a >) = o(G)$.

अतः $< a > = G$, अर्थात् G चक्रीय है।

प्रमेय 3 और प्रमेय 6 से हम तुरन्त कह सकते हैं कि किसी कोटि 35 वाले समूह के सभी उचित उपसमूह चक्रीय होंगे।

आइए अब हम भाज्य कोटि वाले समूहों पर विचार करें।

प्रमेय 7 : यदि G ऐसा परिमित समूह हो कि $o(G)$ न तो 1 हो और न ही कोई अभाज्य, तो G के अतुच्छ उचित उपसमूह होते हैं।

उपपत्ति : यदि G चक्रीय नहीं है, तो कोई भी $a \in G$, $a \neq e$ एक उचित अतुच्छ उपसमूह $< a >$ को जनित करता है।

अब, मान लीजिए कि G चक्रीय है और $G = < x >$, जहां $o(x) = mn$ $(m, n \neq 1)$.

तब $(x^m)^n = x^{mn} = e$. इस तरह, प्रमेय 4 से
$o(x^m) \leq n < o(G)$.

इस तरह, $< x^m >$, G का एक उचित अतुच्छ उपसमूह है।

अब आप निम्नलिखित प्रश्न को हल करने के लिए प्रमेय 7 का प्रयोग कर सकते हैं।

E 9) Z_4 के दो अतुच्छ उचित उपसमूह ज्ञात कीजिए।

अब हम लग्रांज प्रमेय की सहायता से संख्या-सिद्धांत के कुछ महत्वपूर्ण परिणाम सिद्ध करेंगे। और आगे पढ़ने से पहले भाग 1.6.2 से "सापेक्षतः अभाज्य" की परिभाषा को दोहरा लें।

हम पहले ऑयलर फ़ाइ-फलन की परिभाषा देंगे, जो कि स्विट्ज़रलैण्डवासी गणितज्ञ लियोनार्ड ऑयलर (1707-1783) के नाम पर है।

परिभाषा : हम ऑयलर फ़ाई-फलन $\phi : N \longrightarrow N$ को निम्न रूप से परिभाषित करते हैं :

$\phi(1) = 1$ और $\phi(n)$ = उन प्राकृतिक संख्याओं की संख्या जो n से कम हैं और n के सापेक्षतः अभाज्य हैं, $n \geq 2$ के लिए।

उदाहरण के लिए, $\phi(2) = 1$ और $\phi(6) = 2$ (क्योंकि केवल 1 और 5 ही ऐसे धन पूर्णांक हैं जो 6 से कम हैं और 6 के सापेक्षतः अभाज्य हैं)।

अब हम एक प्रमेयिका सिद्ध करेंगे जिसकी सहायता से हम इसके बाद दिए गए प्रमेय को सिद्ध करेंगे। इस प्रमेयिका से प्रत्येक $n \geq 2$ के लिए Z_n के उपसमूहों के उदाहरण भी प्राप्त होते हैं।

प्रमेयिका 1: मान लीजिए $G = \{\bar{r} \in Z_n \mid (r, n) = 1\}$, जहां $n \geq 2$. तब $(G, .)$ एक समूह है, जहां $\bar{r} . \bar{s} = \overline{rs}$ $\forall$ $\bar{r}, \bar{s} \in Z_n$ और $o(G) = \phi(n)$.

उपपत्ति : पहले हम दिखाएंगे कि गुणन के सापेक्ष G संवृत है.
अब, $\bar{r}, \bar{s} \in G \Longrightarrow (r, n) = 1$ और $(s, n) = 1 \Longrightarrow (rs, n) = 1. \Longrightarrow \overline{rs} \in G$. इसलिए G पर $\cdot$ एक द्वि-आधारी संक्रिया है। $\bar{1} \in G$ और तत्समक है।

अब किसी $\bar{r} \in G$ के लिए $(r, n) = 1$.

$\Longrightarrow ar + bn = 1$, किसी $a, b \in Z$ के लिए (इकाई 1 के प्रमेय 8 के अनुसार)
$\Longrightarrow n \mid ar - 1$
$\Longrightarrow ar \equiv 1 \pmod n$,
$\Longrightarrow \bar{a}\,\bar{r} = \bar{1}$
$\Longrightarrow \bar{a} = \bar{r}^{-1}$
और $\bar{a} \in G$, क्योंकि यदि a और n का 1 के अतिरिक्त एक अन्य सार्व गुणनखंड हो, तो यह गुणनखंड $ar + bn = 1$ को भाग देगा। पर यह संभव नहीं है।
इस तरह, G के प्रत्येक अवयव का एक प्रतिलोम होता है।
इसलिए $(G, \cdot)$ एक समूह है। वास्तव में, यह Z_n के उन अवयवों का समूह है जिनके गुणनात्मक प्रतिलोम हैं।

चूंकि G ऐसे सभी $\bar{r} \in Z_n$ का समुच्चय है जिनके लिए $r < n$ और $(r, n) = 1$, इसलिए $o(G) = \phi(n)$.

प्रमेयिका 1 और लग्रांज प्रमेय से हमें तुरंत निम्नलिखित परिणाम प्राप्त हो जाता है। इस परिणाम को गणितज्ञ ऑयलर और पीएर फ़र्मा ने प्राप्त किया था।

प्रमेय 8 (ऑयलर-फर्मा) : मान लीजिए $a \in N$ और $n \geq 2$ ऐसे हैं कि $(a, n) = 1$.
तब $a^{\phi(n)} \equiv 1 \pmod n$.

उपपत्ति : क्योंकि $\bar{a} \in Z_n$ और $(a, n) = 1$, इसलिए $\bar{a} \in G$ (प्रमेयिका 1 का समूह)। क्योंकि $o(G) = \phi(n)$, इसलिए हमें E 8 के प्रयोग से $\bar{a}^{\phi(n)} = \bar{1}$ प्राप्त होता है।

इस तरह, $a^{\phi(n)} \equiv 1 \pmod n$

अब आप प्रमेय 8 की सहायता से नीचे दिए गए प्रश्नों को हल कर सकते हैं।

E 10) 3^{47} को 23 से भाग देने पर कितना शेषफल बचता है? (ध्यान दीजिए कि $\phi(23) = 22$, क्योंकि 1, 2, ..., 22 में से प्रत्येक संख्या 23 के सापेक्षतः अभाज्य है।)

E 11) मान लीजिए $a \in N$ और p एक अभाज्य संख्या है। दिखाइए कि $a^{p-1} \equiv 1 \pmod p$. (इस परिणाम को **फ़र्मा का छोटा प्रमेय** कहते हैं। इसे सिद्ध करने के लिए आपको तथ्य $\phi(p) = p - 1$ का प्रयोग करना पड़ेगा।)

आप जान ही गए होंगे कि लग्रांज प्रमेय कितना महत्वपूर्ण है। अब बताइए कि क्या यह सच है कि यदि $m \mid o(G)$ तो G का कोटि m वाला एक उपसमूह होगा? इकाई 7 में हम आपको दिखाएंगे कि S_4 के उपसमूह

$A_4 = \{ I, (1\,2\,3), (1\,2\,4), (1\,3\,2), (1\,3\,4), (1\,4\,2), (1\,4\,3), (2\,3\,4), (2\,4\,3), (1\,2)\,(3\,4), (1\,3)\,(2\,4), (1\,4)\,(2\,3) \}$

का कोई कोटि 6 वाला उपसमूह नहीं है, हालांकि $6 \mid 12 = o(A_4)$.

आइए अब हम इस इकाई में किए गए शिक्षा सामग्री का संक्षिप्त विवरण दें।

4.4 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों की चर्चा की है।

1) उपसमूह के दक्षिण और वाम सहसमुच्चयों की परिभाषा और उदाहरण।
2) उपसमूह के दो वाम (दक्षिण) सहसमुच्चय असंयुक्त अथवा समान होते हैं।
3) कोई भी उपसमूह, समूह को उपसमूह के असंयुक्त वाम (अथवा दक्षिण) सहसमुच्चयों में विभाजित करता है।
4) समूह की कोटि और समूह के अवयव की कोटि की परिभाषा।
5) लग्रांज प्रमेय की उपपत्ति, जिसका कथन है कि यदि H समूह G का एक उपसमूह हो, तो $o(G) = o(H) \mid G : H \mid$. लेकिन यह ज़रूरी नहीं है कि यदि $m \mid o(G)$, तो G का कोटि m वाला एक उपसमूह हो।
6) लग्रांज प्रमेय के निम्नलिखित परिणाम :
   i) अभाज्य कोटि वाला प्रत्येक समूह चक्रीय होता है।
   ii) $a^{\phi(n)} \equiv 1 \pmod n$, जहां $a, n \in N$, $(a, n) = 1$ और $n \geq 2$.

4.5 हल/उत्तर

E 1) $H = \{ I, (1\,2) \}$.
इसके वाम सहसमुच्चय $H, (1\,2)H, (1\,3)H, (2\,3)H, (1\,2\,3)H, (1\,3\,2)H$.
इस तरह, S_3 में H के अलग-अलग वाम सहसमुच्चय $H, (1\,3)H, (2\,3)H$ हैं।

अब $(1\,2)H = H$,
$(1\,2\,3)H = (1\,3)H$

इसी प्रकार, S_3 में H के अलग-अलग दक्षिण सहसमुच्चय $H, H(1\,3), H(2\,3)$ हैं।

अब, $(1\,3)H = \{ (1\,3), (1\,2\,3) \}$ और $H(1\,3) = \{ (1\,3), (1\,3\,2) \}$.
$\therefore (1\,3)H \neq H(1\,3)$.

आप $(2\,3)H \neq H(2\,3)$ भी देख सकते हैं।

E 2) क्योंकि $ab^{-1} \in K \;\forall\; a, b \in K$, इसलिए हम इकाई 3 के प्रमेय 1 को लागू करके कह सकते हैं कि $K \leq Q_8$.

अब, $K = KI = K(-I)$, $KA = K(-A) = \{ A, -A \}$,
$KB = K(-B) = \{ B, -B \}$, $KC = K(-C) = \{ C, -C \}$.

E 3) मान लीजिए Hx, G में H का एक सहसमुच्चय है। फलन $f : H \longrightarrow Hx : f(h) = hx$ लीजिए। अब, $h, h' \in H$ के लिए $hx \implies h'x \implies h = h'$, निरसन से। इसलिए f, 1-1 है।

स्पष्ट है कि f आच्छादक है। इस तरह, f एकैकी आच्छादक है।
अतः H के अवयवों और Hx के अवयवों के बीच एकैकी संगति है।
इसी प्रकार, फलन $f : H \longrightarrow xH : f(h) = xh$ एकैकी आच्छादक है।
अतः H के अवयव और xH के अवयव एकैकी संगति में हैं।

E 4) $\mathbf{Z}$ में $5\mathbf{Z}$ के अलग-अलग सहसमुच्चय $5\mathbf{Z}, 5\mathbf{Z}+1, 5\mathbf{Z}+2, 5\mathbf{Z}+3, 5\mathbf{Z}+4$ हैं।
$\therefore\ \mathbf{Z} = 5\mathbf{Z} \cup 5\mathbf{Z}+1 \cup 5\mathbf{Z}+2, \cup 5\mathbf{Z}+3 \cup 5\mathbf{Z}+4.$

E 5) f सुपरिभाषित है, क्योंकि $Hx = Hy \implies xy^{-1} \in H \implies (xy^{-1})^{-1} \in H$
$\implies f(Hx) = f(Hy). \implies (y^{-1})^{-1}x^{-1} \in H \implies x^{-1}H = y^{-1}H.$
f, 1-1 है क्योंकि $f(Hx) = f(Hy) \implies x^{-1}H = y^{-1}H$
$\implies yx^{-1} \in H \implies xy^{-1} \in H \implies Hx = Hy.$
f आच्छादक है क्योंकि G में H का कोई भी वाम सहसमुच्चय $yH = f(Hy^{-1})$ है। इसलिए f एकैकी आच्छादक है।

E 6) क) $(1\ 2) \neq I, (1\ 2)^2 = (1\ 2) \circ (1\ 2) = I. \quad \therefore \circ((12)) = 2$

ख) $I^1 = I. \quad \therefore o(I) = 1.$

ग) 2

घ) $\bar{3} \neq \bar{0}, 2.\bar{3} = \bar{6} = \bar{2}, 3.\bar{3} = \bar{9} = \bar{1}, 4.\bar{3} = \overline{12} = \bar{0}. \quad \therefore o(\bar{3}) = 4.$

ङ) $<1> = \mathbf{R}$ अनंत है। इसलिए 1 अपरिमित कोटि का है।

E 7) $\mathbf{Z}_{18} = <\bar{1}>$
इस तरह, प्रमेय 5 को लागू करने पर हम पाते हैं कि

$o(\bar{r}) = o(r.\bar{1}) = \dfrac{18}{(18, r)}$ किसी $\bar{r} \in \mathbf{Z}_{18}$ के लिए।

$\therefore o(\bar{2}) = 9, o(\bar{4}) = 9, o(\bar{5}) = 18.$

E 8) चूंकि $o(x) = o(<x>)$ और $o(<x>) \mid o(G), o(x) \mid o(G)$. इस तरह, प्रमेय 4 को लागू करने पर $x^{o(G)} = e$.

E 9) $o(\mathbf{Z}_8) = 8 = 2 \times 4.$
$\bar{2} \in \mathbf{Z}_8$ और $o(\bar{2}) = 4$. अतः $<\bar{2}> \lneq \mathbf{Z}_8$.
इसी प्रकार, $\bar{4} \in \mathbf{Z}_8$ और $o(\bar{4}) = 2. \quad \therefore <\bar{4}> \leq \mathbf{Z}_8.$

E 10) हम जानते हैं कि $\mathbf{Z}_{23}$ में $(\bar{3})^{\phi(23)} = \bar{1}$,
अर्थात् $\bar{3}^{22} = \bar{1} \quad \therefore \bar{3}^{44} = \bar{1}$
$\therefore \bar{3}^{47} = \bar{3}^3.\bar{3}^{44} = \bar{3}^3 = \overline{27}$

अतः $3^{47} \equiv 27 \pmod{23}$.

इसलिए 3^{47} को 23 से भाग देने पर हमें शेषफल 27 प्राप्त होता है।

E 11) प्रमेय 8 और $\phi(p) = p - 1$ का प्रयोग करके हमें परिणाम तुरंत प्राप्त हो जाता है।

शब्दावली

अद्वितीय	unique
अधिकल्पित भाग	imaginary part
अभिगृहीत	axiom
अनु-आबेली	non-abelian
अनंत समूह	infinite group
अभाज्य कोटि	prime order
अभाज्य गुणनखंडन	prime factorisation
अवयव	element
असंयुक्त	disjoint
असहभाज्य	coprime
आगमन	induction
आबेली	abelian
आच्छादक	surjective, onto
उपपत्ति	proof
उपप्रमेय	corollary
उपसमुच्चय	subset
उपसमूह	subgroup
एकांतर समूह	alternating group
एकैकी	one-one, injective
एकैकी आच्छादक	bijective
एकैकी संगति	one-to-one correspondenc
कार्तीय गुणनफल	Cartesian product
क्रमचय	permutation
क्रमविनिमेय	commutative
क्रमित युग्म	ordered pair
कोटि	order
कोणांक	argument
घातांक	power, exponent, index
चक्र	cycle
चक्रीय उपसमूह	cyclic subgroup
चक्रीय समूह	cyclic group
चतुष्टयी समूह	quaternion group
जनक समुच्चय	generating set
तत्समक	identity
तुच्छ उपसमूह	trivial subgroup
तुल्यता	equivalence relation
तुल्यता वर्ग	equivalence class

द्वि-आधारी संक्रिया	binary operation
ध्रुवीय रूप	polar form
निरसन नियम	cancellation law
परिमित समूह	finite group
परिसर	range
पूरक	complement
प्रतिच्छेद	intersection
प्रतिलोम	inverse
प्रमेय	theorem
प्रमेयिका	lemma
प्रांत	domain
भाज्य कोटि	composite order
भाज्यता	divisibility
मापांक	modulus
योज्य प्रतिलोम	additive inverse
रिक्त समुच्चय	empty set
विभाजन-कलन विधि	division algorithm
संक्रामक	transitive
संक्रिया	operation
संख्या-सिद्धांत	number theory
संबंध	relation
संमिश्र संख्या	complex number
संमिश्र संयुग्मी	complex conjugate
संयोजन	composition
संवृत	closed
सममित	symmetric
सममित समूह	symmetric group
समशेषता	congruence
सम-षट्भुज	regular hexagon
सम्मिलन	union
समुच्चय	set
समूह	group
सहप्रांत	co-domain
सहसमुच्चय	coset
सापेक्षतः अभाज्य	relatively prime
सामिसमूह	semigroup
सार्व भाजक	common divisor
साहचर्य	associative

सुक्रमण सिद्धांत	well-ordering principle
सूचकांक	index
स्थानांतरण	translation
स्वतुल्य	reflexive

NOTES

उत्तर प्रदेश
राजर्षि टण्डन मुक्त विश्वविद्यालय

UGMM – 06
अमूर्त बीजगणित

खंड

2

समूह सिद्धांत के कुछ और विषय

समूह सिद्धांत के कुछ और विषय

यह खंड, खंड 1 की ही निरंतरता में है। पिछले खंड में हम विभिन्न समूहों और उनके उपसमूहों पर चर्चा कर चुके हैं। इस खंड में सबसे पहले हम एक विशेष प्रकार के उपसमूह, जिसे प्रसामान्य उपसमूह कहते हैं, का अध्ययन करेंगे। इकाई 5 का अध्ययन करने पर आपको पता चल जाएगा कि इन उपसमूहों का इतना अधिक महत्व क्यों है।

इस खंड की दूसरी इकाई में हम आपको बीजीयतः समान निकायों की संकल्पना से परिचित कराएंगे। इस प्रकार के निकायों को तुल्याकारी कहते हैं। इस शब्द का प्रयोग सबसे पहले 1870 में गणितज्ञ कमील जोर्दां ने ऐसे दो समूहों के लिए किया था, जो बराबर तो नहीं होते हैं, परन्तु उनका बीजीय व्यवहार समान होता है। तुल्याकारिता विशेष स्थिति है समाकारिता की, जो समूहों के बीच ऐसा फलन है जिसके अधीन प्रांत की बीजीय संरचना बनी रहती है। इकाई 6 में हम समाकारिताओं, तुल्याकारिताओं और महत्वपूर्ण समाकारिता के मूल प्रमेय का अध्ययन करेंगे।

इकाई 7 में हम क्रमचयों के समूहों का अध्ययन करेंगे, जो भाग 2.5.2 में दी गई पाठ्य-सामग्री का विस्तृत अध्ययन है। क्रमचय समूह अमूर्त समूह सिद्धांत का, जिसका अध्ययन आप कर रहे हैं, एक ठोस आधार प्रदान करता है। ये समूह इसलिए भी महत्वपूर्ण हैं, क्योंकि, जैसा कि आप देखेंगे, प्रत्येक समूह क्रमचय समूह के तुल्याकारी होता है।

इस खंड की अंतिम इकाई में आप कुछ परिमित समूहों की, विशेष रूप से 1 से 10 तक की कोटि के समूहों की, बीजीय संरचना का अध्ययन करेंगे। इसके लिए हम गणितज्ञ सीलो द्वारा सिद्ध किए गए कुछ परिणामों को लागू करेंगे। हमें समूहों के अनुलोम गुणनफलों की संकल्पना की भी आवश्यकता पड़ेगी। अतः हम इकाई में इस पर भी चर्चा करेंगे।

इस खंड के साथ हम समूह सिद्धांत का अध्ययन समाप्त कर रहे हैं। अगले दो खंडों में आप अन्य बीजीय निकायों, अर्थात् वलयों (rings) और क्षेत्रों (fields) का अध्ययन करेंगे। आप देखेंगे कि ये निकाय भी समूह हैं। अतः इस खंड में तथा पिछले खंड में आपने जिन संकल्पनाओं का अध्ययन किया है, उनका प्रयोग आप आगे के अध्ययन में भी करते रहेंगे।

इस खंड को पढ़ने के बाद आप सत्रीय कार्य 1 को कीजिए, जिसमें इस पाठ्यक्रम के खंड 1 और खंड 2 से संबंधित प्रश्न हैं।

संकेत और प्रतीक

xHy	$\{ xhy \mid h \in H \}$
$H \trianglelefteq G$	H, G का प्रसामान्य उपसमूह है
A_n	n प्रतीकों पर एकान्तर समूह
S_n	n प्रतीकों पर सममित समूह
D_{2n}	कोटि $2n$ वाला द्वितल समूह
G/H	H के संगत G का विभाग समूह
Ker f	समाकारिता f की अष्टि
$[x, y]$	$x^{-1} y^{-1} xy$, x और y का क्रमविनिमयक
$[G, G]$	G का क्रमविनिमयक उपसमूह
$\simeq$	के तुल्याकारी है
Aut G	G की स्वाकारिताओं का समूह
Inn G	G की आंतरिक स्वाकारिताओं का समूह
$Z(G)$	G का केन्द्र
$(i_1\, i_2 \ldots\, i_r)$	एक r-चक्र
$G \times G'$	समूहों G और G' का बाह्य अनुलोम गुणनफल
$H \times K$	उपसमूहों H और K का आंतरिक अनुलोम गुणनफल

खंड 1 में दिए गए संकेतों को भी देखिए।

इकाई 5 प्रसामान्य उपसमूह

इकाई की रूपरेखा

5.1 प्रस्तावना

खंड 1 में आप उपसमूहों और सहसमुच्चयों के बारे में पढ़ चुके हैं। इस इकाई में सबसे पहले आप एक विशेष प्रकार के उपसमूह, अर्थात् प्रसामान्य उपसमूह, के बारे में अध्ययन करेंगे। आप देखेंगे कि उपयुक्त रूप से परिभाषित एक संक्रिया के सापेक्ष ऐसे उपसमूह के सहसमुच्चयों से एक समूह प्राप्त होता है। इस समूह को विभाग समूह कहते हैं। भाग 5.3 में हम इस पर विस्तार से चर्चा करेंगे।

यदि आप प्रसामान्य उपसमूहों और विभाग समूहों को समझ लें, तो अगली इकाई में दी गई संकल्पनाओं और परिणामों को समझने में आपको काफ़ी आसानी हो जाएगी। अतः अगली इकाई का अध्ययन करने से पहले आप इस बात से सुनिश्चित हो जाएं कि आपने नीचे दिए गए उद्देश्यों को पूरा कर लिया है।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- सत्यापित कर सकेंगे कि कोई उपसमूह प्रसामान्य है कि नहीं;
- किसी दिए हुए प्रसामान्य उपसमूह का संगत विभाग समूह प्राप्त कर सकेंगे।

5.2 प्रसामान्य उपसमूह (Normal Subgroup)

इकाई 4 के E 1 में आपने देखा कि यह आवश्यक नहीं कि उपसमूह H के वाम सहसमुच्चय aH और दक्षिण सहसमुच्चय Ha बराबर ही हों। परन्तु कुछ ऐसे उपसमूह H होते हैं, जिनके लिए दक्षिण सहसमुच्चय Hx और वाम सहसमुच्चय xH समूह के सभी x के लिए समान होते हैं। समूह-सिद्धांत में इस प्रकार के उपसमूह का काफ़ी महत्व है। अतः इस प्रकार के उपसमूह को हम एक विशेष नाम देते हैं।

परिभाषा : समूह G के उपसमूह N को G का एक **प्रसामान्य उपसमूह** कहते हैं, यदि $Nx = xN \ \forall \ x \in G$, और इस तथ्य को हम $N \trianglelefteq G$ से दर्शाते हैं।

उदाहरण के लिए, किसी भी समूह G के दो प्रसामान्य उपसमूह, अर्थात् $\{e\}$ और स्वयं G, होते हैं। क्या आप बता सकते हैं कि ऐसा क्यों है? इसका कारण है कि किसी $x \in G$ के लिए $\{e\}x = \{x\} = x\{e\}$, और किसी $x \in G$ के लिए $Gx = G = xG$.

आइए अब हम एक और उदाहरण लें।

उदाहरण 1 : दिखाइए कि **Z** का प्रत्येक उपसमूह **Z** में प्रसामान्य होता है।

हल : इकाई 3 के उदाहरण 4 से आप जानते हैं कि यदि H, **Z** का एक उपसमूह हो, तो किसी $m \in \mathbf{Z}$ के लिए $H = m\mathbf{Z}$. अब, किसी $z \in \mathbf{Z}$ के लिए,

$$H + z = \{..., -3m + z, -2m + z, -m + z, z, m + z, 2m + z, ...\}$$
$$= \{..., z - 3m, z - 2m, z - m, z, z + m, z + 2m, ...\} \text{ (क्योंकि + क्रमविनिमेय है)}$$
$$= z + H.$$

$\therefore H \trianglelefteq \mathbf{Z}$.

ध्यान दीजिए कि उदाहरण 1 निम्नलिखित तथ्य की एक विशेष स्थिति है

क्रमविनिमेय समूह का प्रत्येक उपसमूह प्रसामान्य उपसमूह होता है।
इसे हम आगे प्रमेय 2 में सिद्ध करेंगे।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 1) दिखाइए कि $A_3 \trianglelefteq S_3$ (इकाई 4 का उदाहरण 3 देखिए)।

आइए अब हम एक परिणाम को सिद्ध करें, जो हमें उन तुल्य प्रतिबंधों के बारे में बताता है जिनके अधीन उपसमूह प्रसामान्य उपसमूह होता है।

प्रमेय 1 : मान लीजिए H समूह G का एक उपसमूह है। नीचे दिए गए कथन तुल्य हैं।

(क) H, G में प्रसामान्य है।

$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$

(ख) $g^{-1}Hg \subseteq H \; \forall \; g \in G$.

(ग) $g^{-1}Hg = H \; \forall \; g \in G$.

उपपत्ति : हम दिखाएंगे कि
(क) $\Rightarrow$ (ख) $\Rightarrow$ (ग) $\Rightarrow$ (क).

इससे पता चल जाएगा कि तीनों कथन तुल्य हैं।

(क) $\Rightarrow$ (ख) : चूंकि (क) सत्य है, इसलिए $Hg = gH \; \forall \; g \in G$. अब हम (ख) सिद्ध करेंगे। इस संबंध में $g \in G$ के लिए $g^{-1}Hg$ लीजिए।

मान लीजिए $g^{-1}hg \in g^{-1}Hg$. चूंकि $hg \in Hg = gH$, $\exists \; h_1 \in H$ जिससे कि $hg = gh_1$.

$\therefore \; g^{-1}hg = g^{-1}gh_1 = h_1 \in H$.

अतः (ख) सत्य है।

(ख) $\Rightarrow$ (ग) : हम जानते हैं कि (ख) सत्य है, अर्थात् $g \in G$ के लिए $g^{-1}Hg \subseteq H$.

यहाँ हम दिखाना चाहते हैं कि $H \subseteq g^{-1}Hg$.
मान लीजिए $h \in H$. तब,

$$\begin{aligned} h = ehe &= (g^{-1}g)\,h\,(g^{-1}g) \\ &= g^{-1}(ghg^{-1})\,g \\ &= g^{-1}\{(g^{-1})^{-1}hg^{-1}\}\,g \in g^{-1}Hg, \text{ क्योंकि } (g^{-1})^{-1}hg^{-1} \in (g^{-1})^{-1}H(g^{-1}) \subseteq H. \end{aligned}$$

$\therefore \; H \subseteq g^{-1}Hg$.

$\therefore \; g^{-1}Hg = H \; \forall \; g \in G$.

(ग) $\Rightarrow$ (क) : हम जानते हैं कि किसी भी $g \in G$ के लिए $g^{-1}Hg = H$.

$Ha = Hb \Leftrightarrow Hac = Hbc$ किन्हीं $a, b, c \in G$ के लिए।

$\therefore \; g(g^{-1}Hg) = gH$, अर्थात् $Hg = gH$.
$\therefore \; H \trianglelefteq G$, अर्थात् (क) सत्य है।

यहाँ हम प्रमेय 1 के संबंध में एक टिप्पणी देना चाहेंगे।

टिप्पणी : प्रमेय 1 के अनुसार $H \trianglelefteq G \Leftrightarrow g^{-1}Hg = H \; \forall \; g \in G$. **इसका अर्थ यह नहीं कि** $g^{-1}hg = h \; \forall \; h \in H$ और $g \in G$.
उदाहरण के लिए, आपने E 1 में दिखाया है कि $A_3 \trianglelefteq S_3$. अतः प्रमेय 1 के अनुसार $(1\,2)^{-1}A_3(1\,2) = A_3$. परन्तु,
$(1\,2)^{-1}(1\,3\,2)(1\,2) \neq (1\,3\,2)$. वास्तव में, यह $(1\,2\,3)$ है।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 2) $GL_2(\mathbf{R})$ का उपसमूह $SL_2(\mathbf{R}) = \{A \in GL_2(\mathbf{R}) \mid \det(A) = 1\}$ लीजिए (इकाई 2 का

उदाहरण 5 देखिए)। तथ्यों $\det(AB) = \det(A)\det(B)$ और $\det(A^{-1}) = \frac{1}{\det(A)}$ की सहायता से सिद्ध कीजिए कि $SL_2(R) \trianglelefteq GL_2(R)$.

अब हम उदाहरण 1 के बाद दिए गए परिणाम को सिद्ध करेंगे। वास्तव में, यह परिणाम प्रमेय 1 का एक उपप्रमेय है।

प्रमेय 2 : क्रमविनिमेय समूह का प्रत्येक उपसमूह प्रसामान्य होता है।

उपपत्ति : मान लीजिए G एक आबेली समूह है और $H \leq G$. किसी $g \in G$ और $h \in H$ के लिए

$g^{-1}hg = (g^{-1}g)h = h \in H$. $\therefore g^{-1}Hg \subseteq H$. इस तरह, $H \trianglelefteq G$.

प्रमेय 2 के अनुसार यदि G आबेली है तो इसके सभी उपसमूह प्रसामान्य होंगे। किन्तु, इस प्रमेय का विलोम सत्य नहीं है, अर्थात् कुछ ऐसे अन्-आबेली समूह होते हैं जिनके सभी उपसमूह प्रसामान्य होते हैं। इस संबंध में एक उदाहरण हम प्रमेय 3 के बाद देंगे। आइए पहले हम प्रसामान्य उपसमूह के एक अन्य उदाहरण पर विचार करें।

उदाहरण 2 : इकाई 3 के उदाहरण 7 में दिया गया क्लाइन 4-समूह K_4 लीजिए। दिखाइए कि इसके दोनों उपसमूह $< a >$ और $< b >$ प्रसामान्य हैं।

हल : इकाई 3 के उदाहरण 7 में दी गई संक्रिया सारणी लीजिए। ध्यान दीजिए कि a और b कोटि 2 के अवयव हैं। इसलिए $a = a^{-1}$ और $b = b^{-1}$. और यह भी ध्यान दीजिए कि $ba = ab$.

अब, मान लीजिए $H = < a > = \{e, a\}$. हम सत्यापित करेंगे कि $H \trianglelefteq K_4$, अर्थात्
$g^{-1}hg \in H \; \forall \; g \in K_4$ और $h \in H$.

अब, $g^{-1}eg = e \in H \; \forall \; g \in K_4$.

और, $e^{-1}ae = a \in H$, $a^{-1}aa = a \in H$, $b^{-1}ab = bab = a \in H$
और $(ab)^{-1}a(ab) = b^{-1}(a^{-1}aa)b = bab = a \in H$.

$\therefore H \trianglelefteq K_4$.

इसी प्रकार, हम सिद्ध कर सकते हैं कि $< b > \trianglelefteq K_4$.

उदाहरण 2 में $< a >$ और $< b >$, दोनों ही K_4 में सूचकांक 2 वाले उपसमूह हैं। निम्नलिखित प्रमेय ऐसे उपसमूहों से ही संबंधित है।

प्रमेय 3 : समूह G का प्रत्येक सूचकांक 2 वाला उपसमूह G में प्रसामान्य होता है।

उपपत्ति : मान लीजिए $N \leq G$ ऐसा है कि $|G : N| = 2$.
मान लीजिए N के दोनों दक्षिण सहसमुच्चय N और Nx हैं और दोनों वाम सहसमुच्चय N और yN हैं।

अब, $G = N \cup yN$ और $x \in G$. $\therefore x \in N$ या $x \in yN$.
चूंकि $N \cap Nx = \phi$, $x \notin N$. $\therefore x \in yN$. $\therefore xN = yN$.
$N \trianglelefteq G$ दिखाने के लिए हमें $Nx = xN$ दिखाना है।
अब किसी $n \in N$ के लिए $nx \in G = N \cup xN$. इसलिए $nx \in N$ या $nx \in xN$.
परन्तु, $nx \notin N$, क्योंकि $x \notin N$.
$\therefore nx \in xN$.

इस तरह, $Nx \subseteq xN$.

इसी प्रकार, हम दिखा सकते हैं कि $xN \subseteq Nx$.

$\therefore Nx = xN$ और $N \trianglelefteq G$.

हम इस प्रमेय का प्रयोग इकाई 7 में यह दिखाने के लिए करेंगे कि किसी $n \geq 2$ के लिए एकान्तर समूह A_n, S_n का एक प्रसामान्य उपसमूह होता है।

वास्तव में, यदि आप भाग 4.3 के अंतिम अंश को पढ़ें, तो आप पाएंगे कि $A_4 \trianglelefteq S_4$, क्योंकि लग्रांज प्रमेय के अनुसार

$$|S_4 : A_4| = \frac{o(S_4)}{o(A_4)} = \frac{4!}{12} = 2.$$

अब हम एक ऐसा उदाहरण देंगे, जिससे सिद्ध हो जाता है कि प्रमेय 2 का विलोम सत्य नहीं है।

चतुष्टयी समूह Q_8 लीजिए जिसकी चर्चा हम इकाई 4 के उदाहरण 4 में कर चुके हैं। इस समूह के निम्नलिखित 6 उपसमूह हैं :

$H_0 = \{I\}, H_1 = \{I, -I\}, H_2 = \{I, -I, A, -A\}, H_3 = \{I, -I, B, -B\},$
$H_4 = \{I, -I, C, -C\}, H_5 = Q_8.$

आप जानते हैं कि H_0 और H_5, Q_8 में प्रसामान्य हैं। प्रमेय 3 की सहायता से आप देख सकते हैं कि H_2, H_3 और H_4, Q_8 में प्रसामान्य हैं।

गुणा करके आप देख सकते हैं कि

$g^{-1}H_1g \subseteq H_1 \forall\, g \in Q_8. \therefore\ H_1 \trianglelefteq Q_8.$

अत: Q_8 के सभी उपसमूह प्रसामान्य हैं।

परन्तु, आप जानते हैं कि Q_8 अनु-आबेली है (उदाहरण के लिए, $AB = -BA$)।

अभी तक हमने प्रसामान्य उपसमूहों के उदाहरण दिए हैं। आइए अब हम एक ऐसे उपसमूह का उदाहरण लें, जो प्रसामान्य नहीं है।

उदाहरण 3 : दिखाइए कि S_3 का उपसमूह $<(1\ 2)>$ प्रसामान्य नहीं है।

हल : हमें एक ऐसा $g \in S_3$ ज्ञात करना है जिससे कि $g^{-1}(1\ 2)g \notin <(1\ 2)>$. चलिए हम $g = (1\ 2\ 3)$ लेकर देखते हैं।

$$\begin{aligned} g^{-1}(1\ 2)g &= (3\ 2\ 1)(1\ 2)(1\ 2\ 3) \\ &= (3\ 2\ 1)(2\ 3) = (1\ 3) \notin <(1\ 2)> \end{aligned}$$

अत: S_3 में $<(1\ 2)>$ प्रसामान्य नहीं है।

अब आप नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 3) गुणन के प्रति $\mathbf{R}^*$ के सभी 2×2 विकर्ण आव्यूहों (diagonal matrices) का समूह लीजिए। इसके कितने उपसमूह प्रसामान्य हैं?

E 4) दिखाइए कि G का केन्द्र Z(G), G में प्रसामान्य है। (याद कीजिए कि $Z(G) = \{x \in G \mid xg = gx \forall g \in G\}$.)

E 5) दिखाइए कि $<(2\ 3)>$, S_3 में प्रसामान्य नहीं है।

इकाई 3 में हमने सिद्ध किया था कि यदि $H \leq G$ और $K \leq H$, तो $K \leq G$. अर्थात् '$\leq$' एक संक्रामक संबंध है। परन्तु "$\trianglelefteq$" संक्रामक संबंध नहीं है। अर्थात्, यदि $H \trianglelefteq N$ और $N \trianglelefteq G$, तो यह आवश्यक नहीं है कि $H \trianglelefteq G$ हो। इससे संबंधित एक उदाहरण हम इकाई 7 में देंगे। लेकिन, इकाई 3 के प्रमेय 4 में दिए गए उपसमूहों के गुण के संगत हम निम्नलिखित परिणाम सिद्ध करेंगे।

प्रमेय 4 : मान लीजिए H और K समूह G के प्रसामान्य उपसमूह हैं। तब $H \cap K \trianglelefteq G$.

उपपत्ति : इकाई 3 के प्रमेय 4 से हम जानते हैं कि $H \cap K \leq G$. हमें दिखाना है कि $g^{-1}xg \in H \cap K \forall\, x \in H \cap K$ और $g \in G$.

अब, मान लीजिए कि $x \in H \cap K$ और $g \in G$. तब $x \in H$ और $H \trianglelefteq G$. $\therefore g^{-1}xg \in H$.

इसी प्रकार, $g^{-1}xg \in K$. $\therefore g^{-1}xg \in H \cap K$.

इस तरह, $H \cap K \trianglelefteq G$.

नीचे दिए गए प्रश्न में हम आपको प्रसामान्य उपसमूहों का एक महत्वपूर्ण गुण सिद्ध करने के लिए कह रहे हैं।

E 6) (क) सिद्ध कीजिए कि यदि $H \trianglelefteq G$ और $K \leq G$, तो $HK \leq G$.
(संकेत : इकाई 3 का प्रमेय 5 लागू कीजिए।)

(ख) सिद्ध कीजिए कि यदि $H \trianglelefteq G$ और $K \trianglelefteq G$, तो $HK \trianglelefteq G$.

अब एक महत्वपूर्ण समूह लीजिए, जो दो उपसमूहों का गुणनफल है जिनमें से केवल एक प्रसामान्य है।

उदाहरण 4 : मान लीजिए G,
$\{x, y \mid x^2 = e, y^4 = e, xy = y^{-1}x\}$ से जनित एक समूह है।

मान लीजिए $H = \langle x \rangle$ और $K = \langle y \rangle$. तब दिखाइए कि $K \trianglelefteq G$, $H \ntrianglelefteq G$ और $G = HK$.

"$\ntrianglelefteq$" ''का प्रसामान्य उपसमूह नहीं है'' को प्रकट करता है।

हल : ध्यान दीजिए कि G के अवयव x^iy^j के रूप के हैं, जहाँ $i = 0, 1$ और $j = 0, 1, 2, 3$.
$\therefore G = \{e, x, xy, xy^2, xy^3, y, y^2, y^3\}$.
$\therefore |G : K| = 2$. इस तरह, प्रमेय 3 के अनुसार $K \trianglelefteq G$.

ध्यान दीजिए कि यहां हम प्रमेय 2 लागू नहीं कर सकते, क्योंकि G अन्-आबेली है (क्योंकि $xy = y^{-1}x$ और $y \neq y^{-1}$).

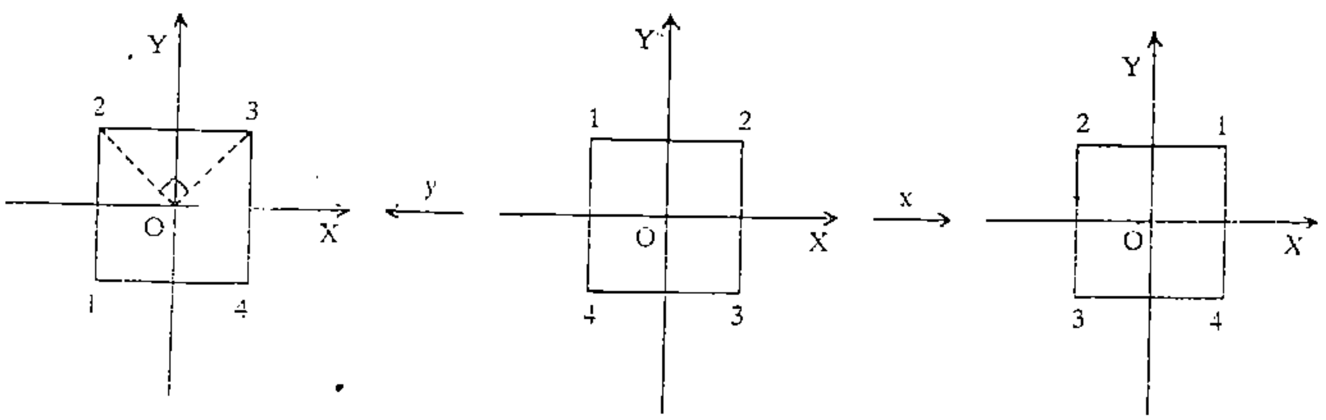
आइए अब हम देखें कि $H \trianglelefteq G$ है कि नहीं।

इसके लिए $y^{-1}xy$ लीजिए। अब $y^{-1}xy = xy^2$, क्योंकि $y^{-1}x = xy$.

यदि $xy^2 \in H$, तो $xy^2 = e$ या $xy^2 = x$. (याद रखिए कि $o(x) = 2$, जिससे कि $x^{-1} = x$.)
अब, $xy^2 = e \implies y^2 = x^{-1} = x$
$\implies y^3 = xy = y^{-1}x$
$\implies y^4 = x$
$\implies e = x$, जो एक अंतर्विरोध है।
और, $xy^2 = x \implies y^2 = e$, एक अंतर्विरोध।
$\therefore y^{-1}xy = xy^2 \notin H$, और इसलिए, $H \ntrianglelefteq G$.

अंत में, G की परिभाषा से आप देख सकते हैं कि $G = HK$.

समूह G की कोटि 8 है और इसे **द्वितल समूह** (dihedral group) D_8 कहते हैं। यह वर्ग के सममितियों का समूह है। अर्थात् इसके अवयव उन अलग-अलग विधियों को निरूपित करते हैं जिनसे वर्ग की दो प्रतियों को इस तरह रखा जा सकता हो कि एक प्रति दूसरी प्रति को ढक ले। इसके जनकों की ज्यामितीय व्याख्या इस प्रकार है (देखिए चित्र 1):



चित्र 1 : D_8 के जनकों का ज्यामितीय निरूपण

y मूल बिन्दु के प्रति कोण $\frac{\pi}{2}$ से यूक्लिडीय समतल का घूर्णन है और x ऊर्ध्वाधर अक्ष के प्रति परावर्तन है।

हम $n \geq 2$ के लिए D_8 को द्वितल समूह में व्यापकीकृत कर सकते हैं।

$D_{2n} = \langle \{x, y \mid x^2 = e, y^n = e, xy = y^{-1}x\} \rangle$

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 7) D_6 की व्याख्या और इसका ज्यामितीय अर्थ बताइए।

आइए अब हम नई बीजीय संरचनाएं प्राप्त करने के लिए प्रसामान्य उपसमूहों का प्रयोग करें।

5.3 विभाग समूह (Quotient Group)

इस भाग में हम प्रसामान्य उपसमूहों की सहायता से एक नया समूह प्राप्त करेंगे। यह समूह रैखिक बीजगणित के पाठ्यक्रम में दी गई विभाग समष्टियों (quotient spaces) की संकल्पना के अनुरूप है।

मान लीजिए H समूह G का एक प्रसामान्य उपसमूह है। तब प्रत्येक $g \in G$ के लिए $gH = Hg$. समूह G में H के सभी सहसमुच्चयों का संग्रह लीजिए। (ध्यान दीजिए कि $H \trianglelefteq G$. इसलिए हमें "वाम सहसमुच्चय" अथवा "दक्षिण सहसमुच्चय" लिखने की आवश्यकता नहीं है, केवल "सहसमुच्चय" लिखना ही काफी है।) हम इस समुच्चय को G/H से प्रकट करते हैं। अब, $x, y \in H$ के लिए

$(Hx)(Hy) = H(xH)y$, सहचारिता का प्रयोग करने पर।

$= HHxy$, H की प्रसामान्यता से।

$= Hxy$, क्योंकि $HH = H$, क्योंकि H एक उपसमूह है।

हम G/H के दो सहसमुच्चयों Hx और Hy के गुणनफल को
$(Hx)(Hy) = Hxy$ से परिभाषित करते हैं, जहाँ $x, y \in G$.

ऐसा लगता है कि हमारी परिभाषा इस बात पर निर्भर करती है कि हम किस तरह से सहसमुच्चय को निरूपित करते हैं। आइए इस कथन को समझें। मान लीजिए, C_1 और C_2 दो समुच्चय हैं। मान लीजिए $C_1 = Hx$ और $C_2 = Hy$. तब $C_1C_2 = Hxy$. परन्तु C_1 और C_2 को Hx और Hy के रूप में कई तरीकों से लिखा जा सकता है। अतः आप पूछ सकते हैं कि क्या C_1C_2, C_1 और C_2 के लिखने की विशेष विधि पर निर्भर करता है? अर्थात् यदि $C_1 = Hx = Hx_1$, और $C_2 = Hy = Hy_1$, तब क्या $C_1C_2 = Hxy$ या $C_1C_2 = Hx_1y_1$? वास्तव में, हम आपको दिखाएंगे कि $Hxy = Hx_1y_1$, अर्थात् **सहसमुच्चयों का गुणनफल सुपरिभाषित है।**

चूंकि $Hx = Hx_1$ और $Hy = Hy_1$

इसलिए $xx_1^{-1} \in H$ और $yy_1^{-1} \in H$.

$\therefore (xy)(x_1y_1)^{-1} = (xy)(y_1^{-1}x_1^{-1}) = x(yy_1^{-1})x_1^{-1}$

$= x(yy_1^{-1})x^{-1}(xx_1^{-1}) \in H$, क्योंकि $xx_1^{-1} \in H$ और $H \trianglelefteq G$.

अर्थात् $(xy)(x_1y_1)^{-1} \in H$.

$\therefore Hxy = Hx_1y_1$.

इस तरह, हमने आपको दिखाया है कि G/H पर गुणन एक सुपरिभाषित द्वि-आधारी संक्रिया है।

अब हम दिखाएंगे कि (G/H,.) एक समूह है।

प्रमेय 5 : मान लीजिए H समूह G का एक प्रसामान्य उपसमूह है और G/H, G में H के सभी सहसमुच्चयों के समुच्चय को प्रकट करता है। तब, $Hx.Hy = Hxy$, $x, y \in G$, से परिभाषित गुणन के प्रति G/H एक समूह होता है। सहसमुच्चय $H = He$, G/H का तत्समक है और Hx का प्रतिलोम सहसमुच्चय Hx^{-1} है।

उपपत्ति : हमने देखा कि दो सहसमुच्चयों का गुणनफल एक सहसमुच्चय होता है।

यह गुणन साहचर्य भी है, क्योंकि

$$
\begin{aligned}
((Hx)(Hy))(Hz) &= (Hxy)(Hz) \\
&= Hxyz, \text{ क्योंकि } G \text{ में गुणनफल साहचर्य है।} \\
&= Hx(yz) \\
&= (Hx)(Hyz) \\
&= (Hx)((Hy)(Hz)),\ x, y, z \in G \text{ के लिए}
\end{aligned}
$$

अब, यदि e, G का तत्समक हो, तो प्रत्येक $x \in G$ के लिए $Hx.He = Hxe = Hx$ और $He.Hx = Hex = Hx$.

इस तरह, $He = H$, G/H का तत्समक अवयव है। और, किसी $x \in G$ के लिए $Hx.Hx^{-1} = Hxx^{-1} = He = Hx^{-1}x = Hx^{-1}.Hx$. अतः Hx का प्रतिलोम Hx^{-1} होगा।

इस तरह, हमने सिद्ध किया है कि G के प्रसामान्य उपसमूह H के सभी सहसमुच्चयों का समुच्चय G/H से $Hx.Hy = Hxy$ द्वारा परिभाषित गुणन के प्रति एक समूह प्राप्त होता है। इस समूह को H के सापेक्ष G का **विभाग समूह** कहते हैं।

ध्यान दीजिए कि विभाग समूह G/H की कोटि, G में H का सूचकांक है। अतः लग्रांज प्रमेय के अनुसार यदि G एक परिमित समूह हो तो

$$o(G/H) = \frac{o(G)}{o(H)}.$$

यह भी ध्यान दीजिए कि यदि $(G, +)$ एक आबेली समूह हो और $H \leq G$, तो $H \trianglelefteq G$. और $(H + x) + (H + y) = H + (x + y)$ से G/H पर संक्रिया परिभाषित होती है।

आइए अब हम विभाग समूहों के कुछ उदाहरण देखें।

उदाहरण 5 : समूह G/H प्राप्त कीजिए, जहाँ $G = S_3$ और $H = A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$.

हल : पहले तो ध्यान दीजिए कि $A_3 \trianglelefteq S_3$, क्योंकि $|S_3 : A_3| = 2$. इकाई 4 के उदाहरण 3 से आपको मालूम हो गया है कि G/H कोटि 2 वाला एक समूह है जिसके अवयव H और $(1\ 2)H$ हैं।

उदाहरण 6 : दिखाइए कि समूह Z/nZ की कोटि n है।

हल : Z/nZ के अवयव $a + nZ = \{a + kn \mid k \in Z\}$ के रूप के हैं। इस तरह, Z/nZ के अवयव मॉड्यूलो n समशेषता वर्ग ही हैं, अर्थात् Z_n के अवयव हैं (देखिए भाग 2.5.1)। इस तरह, $Z/nZ = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.

$\therefore o(Z/nZ) = n.$

ध्यान दीजिए कि Z/nZ में जोड़ $\bar{a} + \bar{b} = \overline{a+b}$ से परिभाषित होता है।

अब आप नीचे दिए गए सरल प्रश्नों को हल करने का प्रयास कीजिए।

E 8) किसी समूह G के लिए {e} और G के संगत विभाग समूह ज्ञात कीजिए।

E 9) दिखाइए कि चक्रीय समूह का विभाग समूह चक्रीय होता है।
(संकेत : यदि $G = \langle x \rangle$, तो दिखाइए कि $G/H = \langle Hx \rangle$.)

अब बताइए कि क्या G और G/H के सदा ही समान बीजीय गुण होते हैं? नीचे दिए गए प्रश्नों को हल करने पर आप पाएंगे कि यदि G आबेली है तो G/H भी आबेली होगा। परन्तु यह आवश्यक नहीं है कि इसका विलोम भी सही हो। अर्थात् यदि G/H आबेली हो तो यह आवश्यक नहीं है कि G भी आबेली हो। इस तरह, यह आवश्यक नहीं है कि G और G/H के समान बीजीय गुण हों।

E 10) दिखाइए कि यदि समूह G क्रमविनिमेय हो और $H \trianglelefteq G$, तो G/H भी क्रमविनिमेय होगा।

E 11) उदाहरण 4 का समूह D_8 लीजिए। दिखाइए कि D_8 के अन्-आबेली होने के बावजूद D_8/K आबेली है।

शायद आपको यह जानकर आश्चर्य होगा कि हम किसी भी समूह G का एक ऐसा प्रसामान्य उपसमूह H परिभाषित कर सकते हैं जिससे कि G/H आबेली हो। यह उपसमूह क्रमविनिमयक उपसमूह है।

परिभाषा : मान लीजिए G एक समूह है और $x, y \in G$. तब $x^{-1}y^{-1}xy$ को x और y का **क्रमविनिमयक** (commutator) कहते हैं। इसे $[x, y]$ से प्रकट करते हैं।

सभी क्रमविनिमयकों के समुच्चय से जनित G के उपसमूह को G का **क्रमविनिमयक उपसमूह** (commutator subgroup) कहते हैं। इसे **[G, G]** से प्रकट करते हैं।

उदाहरण के लिए, यदि G एक क्रमविनिमेय समूह हो, तो $x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = e \ \forall\ x, y \in G$.
$\therefore [G, G] = \{e\}$.

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 12) [G, G] प्राप्त कीजिए, जहाँ G चक्रीय है।

आइए अब हम क्रमविनिमयक उपसमूह के संगत विभाग समूह की क्रमविनिमेयता सिद्ध करें।

प्रमेय 6 : मान लीजिए G एक समूह है। तब [G, G], G का एक प्रसामान्य उपसमूह होता है। और G/[G, G] क्रमविनिमेय होता है।

उपपत्ति : हमें दिखाना है कि किसी क्रमविनिमयक $x^{-1}y^{-1}xy$ और किसी $g \in G$ के लिए $g^{-1}(x^{-1}y^{-1}xy)g \in [G, G]$.

अब, $g^{-1}(x^{-1}y^{-1}xy)g = (g^{-1}xg)^{-1}(g^{-1}yg)^{-1}(g^{-1}xg)(g^{-1}yg) \in [G, G]$.
$\therefore [G, G] \trianglelefteq G$.

शेष उपपत्ति में हम सुविधा के लिए [G, G] को H से प्रकट करेंगे।

अब, $x, y \in G$ के लिए

$$HxHy = HyHx \Longleftrightarrow Hxy = Hyx \Longleftrightarrow (xy)(yx)^{-1} \in H$$
$$\Longleftrightarrow xyx^{-1}y^{-1} \in H.$$

अतः, चूँकि $xyx^{-1}y^{-1} \in H \ \forall\ x, y \in G$, इसलिए $HxHy = HyHx \ \forall\ x, y \in G$. अर्थात् G/H आबेली है।

ध्यान दीजिए कि हमारे लिए विभाग समूह G/H की परिभाषा केवल तभी अर्थपूर्ण है, जबकि $H \trianglelefteq G$. परन्तु, यदि $H \ntrianglelefteq G$, तब भी G में H के सभी वाम (या दक्षिण) सहसमुच्चयों का समुच्चय G/H परिभाषित है। लेकिन, इस स्थिति में G/H एक समूह नहीं होगा। नीचे दिए गए प्रश्न में आपको एक उदाहरण मिलेगा।

E 13) $G = S_3$ और $H = \langle (1\ 2) \rangle$ के लिए दिखाइए कि G/H में दक्षिण सहसमुच्चयों का गुणनफल सुपरिभाषित नहीं है।
(**संकेत** : दिखाइए कि $H(1\ 2\ 3) = H(2\ 3)$ और $H(1\ 3\ 2) = H(1\ 3)$, लेकिन $H(1\ 2\ 3)(1\ 3\ 2) \neq H(2\ 3)(1\ 3)$.)

E 13 से संबंधित हम निम्नलिखित टिप्पणी देते हैं।

टिप्पणी : यदि H, G का एक उपसमूह हो, तो H के सहसमुच्चयों का गुणनफल केवल तभी परिभाषित होता है जबकि $H \trianglelefteq G$. ऐसा इसलिए है, क्योंकि यदि $HxHy = Hxy \ \forall\ x, y \in G$, तो विशेष रूप से $Hx^{-1}Hx = Hx^{-1}x = He = H \ \forall\ x \in G$.

इसलिए, किसी $h \in H$ के लिए $x^{-1}hx = ex^{-1}hx \in Hx^{-1}Hx = H$.
अर्थात् किसी $x \in G$ के लिए $x^{-1}Hx \subseteq H$.
$\therefore H \trianglelefteq G$.

आइए अब हम संक्षेप में देखें कि हमने इस इकाई में क्या किया है।

5.4 सारांश

इस इकाई में हमने निम्नलिखित बातों पर चर्चा की :

1. प्रसामान्य उपसमूह की परिभाषा और उदाहरण।
2. आबेली समूह का प्रत्येक उपसमूह प्रसामान्य होता है।
3. सूचकांक 2 वाला प्रत्येक उपसमूह प्रसामान्य होता है।
4. यदि H और K समूह G के प्रसामान्य उपसमूह हों, तो $H \cap K$ भी प्रसामान्य होगा।
5. दो प्रसामान्य उपसमूहों का गुणनफल प्रसामान्य उपसमूह होगा।
6. यदि $H \trianglelefteq N$ और $N \trianglelefteq G$, तो यह आवश्यक नहीं है कि H, G में प्रसामान्य हो।
7. विभाग समूह की परिभाषा और उदाहरण।
8. यदि G आबेली हो, तो G का प्रत्येक विभाग समूह आबेली होता है। इसका विलोम सत्य नहीं है।
9. क्रमविनिमयक उपसमूह का संगत विभाग समूह क्रमविनिमेय होता है।
10. G में H के वाम (या दक्षिण) सहसमुच्चयों का समुच्चय एक समूह होता है यदि और केवल यदि $H \trianglelefteq G$.

5.5 हल/उत्तर

E 1) $S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

$A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$

आप जांच कर सकते हैं कि

$A_3I = A_3 = IA_3$, $A_3(1\ 2) = (1\ 2)\, A_3$, आदि आदि।

$\therefore A_3 \trianglelefteq S_3$.

E 2) किसी $A \in GL_2(\mathbf{R})$ और $B \in SL_2(\mathbf{R})$ के लिए

$$\det(A^{-1}BA) = \det(A^{-1})\det(B)\det(A)$$

$$= \frac{1}{\det(A)}\det(A), \text{ क्योंकि } \det(B) = 1$$

$$= 1$$

$\therefore A^{-1}BA \in SL_2(\mathbf{R})$

$\therefore SL_2(\mathbf{R}) \trianglelefteq GL_2(\mathbf{R})$.

E 3) सभी, क्योंकि यह समूह आबेली है।

E 4) मान लीजिए, $g \in G$ और $x \in Z(G)$. तब

$g^{-1}xg = g^{-1}gx$, क्योंकि $x \in Z(G)$

$= x \in Z(G)$

$\therefore g^{-1}Z(G)g \subseteq Z(G) \;\forall\; g \in G$.

$\therefore Z(G) \trianglelefteq G$

E 5) चूंकि $(1\ 2\ 3)^{-1}(2\ 3)(1\ 2\ 3) = (1\ 2) \notin \langle (2\ 3) \rangle$, $\langle (2\ 3) \rangle \ntrianglelefteq S_3$.

E 6) क) कोई अवयव $hk \in HK$ लीजिए। चूंकि $H \trianglelefteq G$, इसलिए $k^{-1}hk \in H$. मान लीजिए

$k^{-1}hk = h_1$. तब $hk = kh_1 \in KH$.

$\therefore hk \in KH \;\forall\; hk \in HK \therefore HK \subseteq KH$

ऐसे ही, किसी $kh \in KH$ के लिए $khk^{-1} \in H$.

मान लीजिए $khk^{-1} = h_2$ तब $kh = h_2k \in HK$.

$\therefore kh \in HK \;\forall\; kh \in KH$

$\therefore KH \subseteq HK$

इस तरह, हमने दिखाया है कि $HK = KH$.

$\therefore\ HK \leq G$.

ख) (क) से हम जानते हैं कि $HK \leq G$. $HK \trianglelefteq G$ दिखाने के लिए, $g \in G$ और $hk \in HK$ लीजिए। तब,

$g^{-1}hkg = g^{-1}h(gg^{-1})kg = (g^{-1}hg)(g^{-1}kg) \in HK$, क्योंकि $H \trianglelefteq G$, $K \trianglelefteq G$.

$\therefore\ g^{-1}HKg \subseteq HK\ \forall\ g \in G$.

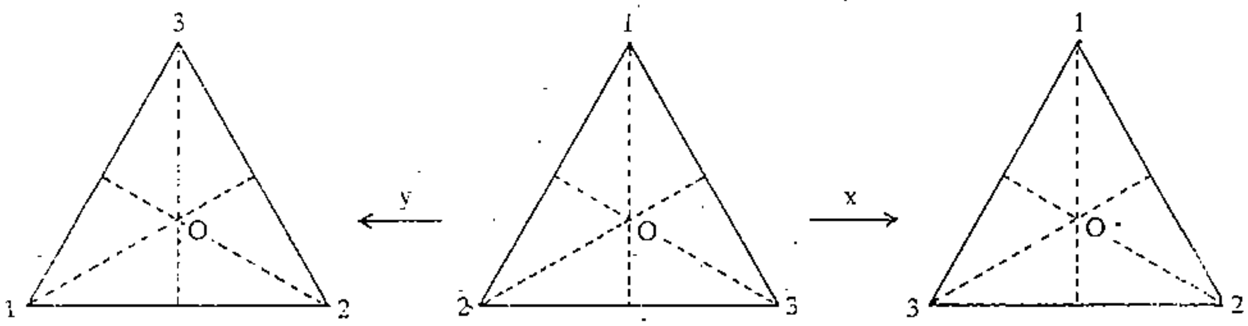
$\therefore\ HK \trianglelefteq G$.

E 7) D_6, x और y से जनित होता है, जहाँ

$x^2 = e$, $y^3 = e$ और $xy = y^{-1}x$.

$\therefore\ D_6 = \{e, x, y, y^2, xy, xy^2\}$.

यह समबाहु त्रिभुज की सममितियों का समूह है। इसके जनक x और y हैं, जहां x नियत शीर्ष से गुज़रने वाली शीर्षलंब (altitude) के प्रति परावर्तन के संगत है और y केन्द्रक (centroid) के प्रति $120°$ के घूर्णन के संगत हैं (देखिए चित्र 2)।



चित्र 2 : D_6 के जनक

E 8) $G/\{e\} = \{\{e\}g \mid g \in G\} = \{\{g\} \mid g \in G\}$

$G/G = \{Gg \mid g \in G\} = \{G\}$, क्योंकि $Gg = G\ \forall\ g \in G$.

तो, G/G में केवल एक अवयव, अर्थात् तत्समक होता है।

E 9) मान लीजिए $G = \langle x \rangle$ और G/H, G का एक विभाग समूह है। G/H का कोई भी अवयव $Hx^n = (Hx)^n$ के रूप का होता हैं, क्योंकि G का कोई भी अवयव x^n के रूप का होता है। $\therefore\ G/H = \langle Hx \rangle$.

E 10) G/H में किन्हीं दो अवयवों Hx और Hy के लिए

$(Hx)(Hy) = Hxy = Hyx$, क्योंकि G आबेली है।

$\qquad = (Hy)(Hx)$.

$\therefore\ G/H$ आबेली है।

E 11) $D_8/K = \{K, Kx\}$. आप जांच कर सकते हैं कि यह आबेली है। आप देख चुके हैं कि $xy \neq yx$.

$\therefore\ D_8$ आबेली नहीं है।

E 12) G चक्रीय है, इसलिए यह आबेली है।

$\therefore\ [G, G] = \{e\}$.

E 13) अब $(1\ 2\ 3)(1\ 3\ 2) = I$, $(2\ 3)(1\ 3) = (1\ 2\ 3)$.

$\therefore\ H(1\ 2\ 3)(1\ 3\ 2) = HI = H = \{I, (1\ 2)\}$, और

$H(2\ 3)(1\ 3) = H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\}$.

इसलिए $H(1\ 2\ 3) = H(2\ 3)$ और $H(1\ 3\ 2) = H(1\ 3)$, लेकिन

$H(1\ 2\ 3)(1\ 3\ 2) \neq H(2\ 3)(1\ 3)$.

इकाई 6 समूह समाकारिताएँ

इकाई की रूपरेखा

6.1 प्रस्तावना

इस पाठ्यक्रम में हमने एक समूह से दूसरे समूह तक के फलनों के बारे में अभी तक चर्चा नहीं की है। शायद आपने सोचा हो कि हमने इकाई 1 में फलनों के विभिन्न पहलुओं को क्यों दोहराया था। इस इकाई को पढ़ने पर आप इसका कारण जान जाएंगे।

भाग 6.2 में हम समूहों के बीच उन फलनों के विभिन्न गुणों पर चर्चा करेंगे, जो अपने प्रांत-समूहों की बीजीय संरचना को बनाए रखते हैं। ऐसे फलन को समूह समाकारिता कहते हैं। इस नाम का प्रयोग सबसे पहले गणितज्ञ क्लाइन ने 1893 में किया था। यह संकल्पना सदिश समष्टि समाकारिता की संकल्पना के अनुरूप है, जिसका अध्ययन आप रैखिक बीजगणित के पाठ्यक्रम में कर चुके हैं।

भाग 6.3 में हम आपको एक अति-महत्वपूर्ण गणितीय संकल्पना, अर्थात् तुल्याकारिता से परिचित कराएंगे। आप देखेंगे कि तुल्याकारिता एकैकी आच्छादक समाकारिता होती है। तुल्याकारिताओं का महत्व इस बात में है कि दो समूह तुल्याकारी होते हैं यदि और केवल यदि उनके सारे बीजीय गुण समान हों।

भाग 6.4 में हम समूह सिद्धांत के एक मौलिक प्रमेय, अर्थात् समाकारिता के मूल प्रमेय को सिद्ध करेंगे। हम इसके कुछ महत्वपूर्ण परिणाम भी बताएंगे।

अंत मे, अर्थात् भाग 6.5 में हम स्वाकारिताओं के बारे में चर्चा करेंगे। ये फलन किसी समूह से स्वयं तक की तुल्याकारिताएं हैं। हम विशेष रूप से आंतर स्वाकारिताओं के समूह पर विचार करेंगे। इस समूह की सहायता से हमें किसी समूह G के लिए विभाग समूह G/Z(G) की संरचना के बारे में जानकारी मिलती है, जहां Z(G), G का केन्द्र है।

हमारी सलाह है कि इस इकाई को पढ़ने से पहले आप भाग 1.5 और इकाई 5 को दोहरा लें।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- सत्यापित कर सकेंगे कि समूहों के बीच का कोई फलन समाकारिता है कि नहीं;
- किसी भी समाकारिता की अष्टि और परिसर प्राप्त कर सकेंगे;
- जांच कर सकेंगे कि समूहों के बीच का कोई फलन तुल्याकारिता है या नहीं;
- समाकारिता के मूल प्रमेय का कथन दे सकेंगे, उसे सिद्ध कर सकेंगे तथा उसका प्रयोग कर सकेंगे;
- सिद्ध कर सकेंगे कि किसी समूह G के लिए $\text{Inn } G \trianglelefteq \text{Aut } G$ और $G/Z(G) \simeq \text{Inn } G$.

6.2 समाकारिता , (Homomorphism)

हम एक समूह से दूसरे समूह तक के फलनों के अध्ययन की शुरूआत एक उदाहरण से करेंगे।

समूह $(\mathbf{Z}, +)$ और $(\{1, -1\}, .)$ लीजिए। यदि हम

$f : \mathbf{Z} \longrightarrow \{1, -1\}$ को

$$f(n) = \begin{cases} 1, & \text{यदि } n \text{ सम हो} \\ -1, & \text{यदि } n \text{ विषम हो,} \end{cases}$$

से परिभाषित करें तो आप देख सकते हैं कि

$f(a + b) = f(a).f(b) \; \forall \; a, b \in \mathbf{Z}$.

इसका अर्थ है कि फलन f अपने प्रांत की बीजीय संरचना को बनाए रखता है, अर्थात् f समाकारिता का एक उदाहरण है।

परिभाषा : मान लीजिए $(G_1, *_1)$ और $(G_2, *_2)$ दो समूह हैं। किसी फलन $f : G_1 \longrightarrow G_2$ को **समूह समाकारिता** (या केवल **समाकारिता**) कहते हैं, यदि

$f(x *_1 y) = f(x) *_2 f(y) \; \forall \; x, y \in G_1$.

ध्यान दीजिए कि G_1 से G_2 तक की समाकारिता, G_1 के किसी गुणनफल $x *_1 y$ को G_2 के गुणनफल $f(x) *_2 f(y)$ में प्रतिचित्रित करती है।

उदाहरणों पर चर्चा करने से पहले आइए हम किसी दी हुई समाकारिता से संबंधित दो समुच्चयों को परिभाषित करें।

परिभाषा : मान लीजिए $(G_1, *_1)$ और $(G_2, *_2)$ दो समूह हैं और $f : G_1 \longrightarrow G_2$ एक समाकारिता है। तब

i) f का **परिसर** (image) समुच्चय
   $\text{Im } f = \{f(x) \mid x \in G_1\}$ है।

ii) f की **अष्टि** (kernel) समुच्चय
   $\text{Ker } f = \{x \in G_1 \mid f(x) = e_2\}$ है, जहाँ e_2, G_2 का तत्समक है।

ध्यान दीजिए कि $\text{Im } f \subseteq G_2$ और $\text{Ker } f = f^{-1}(\{e_2\}) \subseteq G_1$.

आइए अब हम कुछ उदाहरण लें।

उदाहरण 1 : समूह $(\mathbf{R}, +)$ और $(\mathbf{R}^*, .)$ लीजिए। दिखाइए कि फलन $\exp : (\mathbf{R}, +) \longrightarrow (\mathbf{R}^*, .) : \exp(r) = e^r$ एक समूह समाकारिता है। Im exp और Ker exp भी ज्ञात कीजिए।

हल : किन्हीं $r_1, r_2 \in \mathbf{R}$ के लिए हम जानते हैं कि

$e^{r_1 + r_2} = e^{r_1}.e^{r_2}$.

$\therefore \exp(r_1 + r_2) = \exp(r_1).\exp(r_2)$.

अतः exp $(\mathbf{R}, +)$ से $(\mathbf{R}^*, .)$ तक की एक समाकारिता है।

अब $\text{Im exp} = \{\exp(r) \mid r \in \mathbf{R}\} = \{e^r \mid r \in \mathbf{R}\}$.

और $\text{Ker exp} = \{r \in \mathbf{R} \mid e^r = 1\} = \{0\}$.

ध्यान दीजिए कि exp, **R** के तत्समक 0 को $\mathbf{R}^*$ के तत्समक 1 में प्रतिचित्रित करता है। और exp, r के योज्य प्रतिलोम $(-r)$ को exp (r) के गुणनात्मक प्रतिलोम में प्रतिचित्रित करता है।

उदाहरण 2 : समूह $(\mathbf{R}, +)$ और $(\mathbf{C}, +)$ लीजिए और $f : (\mathbf{C}, +) \longrightarrow (\mathbf{R}, +)$ को $f(x + iy) = x$ से परिभाषित कीजिए, अर्थात् f किसी सम्मिश्र संख्या को उसके वास्तविक भाग में प्रतिचित्रित करता है। दिखाइए कि f एक समाकारिता है। Im f और Ker f क्या हैं?

हल : **C** के कोई दो अवयव $a + ib$ और $c + id$ लीजिए। तब,

$$\begin{aligned} f((a + ib) + (c + id)) &= f((a + c) + i(b + d)) = a + c \\ &= f(a + ib) + f(c + id). \end{aligned}$$

अतः f एक समूह समाकारिता है।

$\text{Im } f = \{ f(x + iy) \mid x, y \in \mathbf{R} \} = \{x \mid x \in \mathbf{R}\} = \mathbf{R}$.

इसलिए f आच्छादक फलन है (देखिए भाग 1.5)।

$\text{Ker } f = \{ x + iy \in \mathbf{C} \mid f(x + iy) = 0 \} = \{ x + iy \in \mathbf{C} \mid x = 0 \}$

$= \{ iy \mid y \in \mathbf{R} \}$, शुद्धतः अधिकल्पित संख्याओं का समुच्चय।

ध्यान दीजिए कि f, C के योज्य तत्समक को R के योज्य तत्समक में, और किसी $z \in \mathbf{C}$ के लिए, $(-z)$ को $-f(z)$ में प्रतिचित्रित करता है।

नीचे दिए गए प्रश्नों को हल करने की कोशिश कीजिए। इससे आपको पता चल जाएगा कि अभी तक जो कुछ पढ़ाया गया है, उसे आपने अच्छी तरह से समझ लिया है कि नहीं।

E 1) दिखाइए कि $f : (\mathbf{R}^*, .) \rightarrow (\mathbf{R}, +) : f(x) = \ln x$, x का प्राकृतिक लघुगणक, समूह समाकारिता है। Ker f और Im f भी ज्ञात कीजिए।

E 2) क्या $f : (GL_n(\mathbf{R}), .) \rightarrow (\mathbf{R}^*, .) : f(A) = \det(A)$ एक समाकारिता है? यदि है, तो Ker f और Im f ज्ञात कीजिए।

उदाहरण 1 और उदाहरण 2 में हमने देखा है कि समाकारिताएं तत्समक को तत्समक में और प्रतिलोम को प्रतिलोम में प्रतिचित्रित करती हैं। ये तथ्य किसी भी समूह समाकारिता के लिए सिद्ध किए जा सकते हैं।

प्रमेय 1 : मान लीजिए $f : (G_1, *_1) \rightarrow (G_2, *_2)$ एक समूह समाकारिता है। तब

क) $f(e_1) = e_2$, जहां e_1, G_1 का तत्समक है और e_2, G_2 का तत्समक है।

ख) $f(x^{-1}) = [f(x)]^{-1} \forall x \in G_1$.

उपपत्ति : (क) मान लीजिए $x \in G_1$. तब $e_1 *_1 x = x$. इसलिए
$f(x) = f(e_1 *_1 x) = f(e_1) *_2 f(x)$, क्योंकि f एक समाकारिता है।
लेकिन $f(x) = e_2 *_2 f(x)$, G_2 में।
इस तरह, $f(e_1) *_2 f(x) = e_2 *_2 f(x)$
इसलिए, G_2 में निरसन नियम से, $f(e_1) = e_2$.

(ख) अब किसी $x \in G_1$ के लिए,
$f(x) *_2 f(x^{-1}) = f(x *_1 x^{-1}) = f(e_1) = e_2$.

इसी प्रकार, $f(x^{-1}) *_2 f(x) = e_2$.

अतः $f(x^{-1}) = [f(x)]^{-1} \forall x \in G_1$.

ध्यान दीजिए कि प्रमेय 1 का विलोम सत्य नहीं है। अर्थात् यदि $f : G_1 \rightarrow G_2$ एक ऐसा फलन हो जिसके लिए $f(e_1) = e_2$ और $[f(x)]^{-1} = f(x^{-1}) \forall x \in G_1$, तो f का समाकारिता होना ज़रूरी नहीं। उदाहरण के लिए, $f : \mathbf{Z} \rightarrow \mathbf{Z} : f(0) = 0$ और

$$f(n) = \begin{cases} n + 1 \ \forall \ n > 0 \\ n - 1 \ \forall \ n < 0 \end{cases}$$ लीजिए। तब $f(1 + 1) \neq f(1) + f(1)$.

इसलिए f समाकारिता नहीं है। परन्तु $f(e_1) = e_2$ और $f(-n) = -f(n) \forall n \in \mathbf{Z}$.

आइए अब हम समाकारिताओं के कुछ और उदाहरण लें। विभाग समूहों से हम समाकारिताओं का एक महत्वपूर्ण वर्ग प्राप्त कर सकते हैं।

उदाहरण 3 : मान लीजिए $H \trianglelefteq G$. फलन $p : G \rightarrow G/H : p(x) = Hx$ लीजिए। दिखाइए कि p एक समाकारिता है। (p को प्राकृतिक या विहित समूह समाकारिता कहते हैं।) यह भी दिखाइए कि p आच्छादक है। Ker p क्या है?

हल : $x, y \in G$ के लिए $p(xy) = Hxy = Hx\,Hy = p(x)\,p(y)$. इसलिए p एक समाकारिता है।
अब, $\text{Im } p = \{ p(x) \mid x \in G\} = \{ Hx \mid x \in G \} = G/H$.
अतः p आच्छादक है।

$\text{Ker } p = \{ x \in G \mid p(x) = H \}$ (आपको याद होगा कि H, G/H का तत्समक है।
$= \{ x \in G \mid Hx = H \}$
$= \{ x \in G / x \in H \}$, इकाई 4 के प्रमेय 1 से।
$= H$.

इस उदाहरण में आप देख सकते हैं कि $\text{Ker}\, p \trianglelefteq G$. आप यह भी देख सकते हैं कि यहाँ प्रमेय 1 सत्य है।

और उदाहरणों पर विचार करने से पहले नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 3) S_3 से S_3/A_3 तक प्राकृतिक समाकारिता p की परिभाषा दीजिए। क्या $(1\ 2) \in \text{Ker}\, p$? क्या $(1\ 2) \in \text{Im}\, p$?

E 4) मान लीजिए $S = \{z \in C \mid |z| = 1\}$. (इकाई 3 का उदाहरण 1 देखिए)। $f : (R, +) \longrightarrow (S, .) : f(x) = e^{inx}$ परिभाषित कीजिए, जहाँ n एक नियत धन पूर्णांक है। क्या f समाकारिता है? यदि है, तो Ker f ज्ञात कीजिए।

E 5) मान लीजिए G एक समूह है और $H \trianglelefteq G$. एक ऐसा समूह G_1 और समाकारिता $f : G \longrightarrow G_1$ प्राप्त कीजिए जिससे कि $\text{Ker}\, f = H$.
(संकेत : क्या उदाहरण 3 से आपको सहायता मिलेगी?)

समाकारिताओं के उदाहरणों का एक और वर्ग आविष्टि प्रतिचित्र से संबंधित है।

उदाहरण 4 : मान लीजिए H समूह G का एक उपसमूह है। दिखाइए कि फलन $i : H \longrightarrow G : i(h) = h$ एक समाकारिता है। इस फलन को **आविष्टि प्रतिचित्र** कहते हैं।

हल : चूंकि $i(h_1h_2) = h_1h_2 = i(h_1)i(h_2) \ \forall\ h_1, h_2 \in H$, इसलिए i एक समूह समाकारिता है।

आइए हम सममित समूहों के संदर्भ में आविष्टि प्रतिचित्र पर संक्षेप में विचार करें। दो वास्तविक संख्याएं m और n लीजिए, जहाँ $m \leq n$. तब हम S_m को S_n का उपसमूह मान सकते हैं, जहाँ

σ यूनानी अक्षर सिग्मा है।

$$\begin{pmatrix} 1 & 2 & \ldots & m \\ \sigma(1) & \sigma(2) & \ldots & \sigma(m) \end{pmatrix}$$

के रूप में लिखे गए $\sigma \in S_m$ को हम

$$\begin{pmatrix} 1 & 2 & \ldots & m & m+1 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(m) & m+1 & \ldots & n \end{pmatrix} \in S_n$$

के समान मानते हैं। अर्थात् $\sigma(k) = k \ \forall\ k = m+1, \ldots, n$.

तब हम आविष्टि प्रतिचित्र $i : S_m \longrightarrow S_n$ परिभाषित कर सकते हैं।

उदाहरण के लिए, $i : S_3 \rightarrow S_4$ के अधीन

$(1\ 2)$, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ में प्रतिचित्रित होता है।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 6) प्रतिचित्र $i : 3Z \longrightarrow Z$ की अष्टि और प्रतिबिंब क्या है?

अब हम समाकारिताओं से संबंधित कुछ परिणामों को सिद्ध करेंगे। सुविधा के लिए आगे से हम द्वि-आधारी संक्रिया के संकेत का प्रयोग नहीं करेंगे, और $a*b$ के स्थान पर केवल ab लिखेंगे।

आइए अब हम दो समाकारिताओं के संयोजन पर विचार करें। क्या यह भी समाकारिता होगा? आइए देखें।

प्रमेय 2 : यदि $f : G_1 \longrightarrow G_2$ और $g : G_2 \longrightarrow G_3$ दो समूह समाकारिताएं हों तो इनका संयोजन $g \circ f : G_1 \longrightarrow G_3$ भी समूह समाकारिता होगा।

उपपत्ति : मान लीजिए $x, y \in G_1$. तब

$g \circ f(xy) = g(f(xy))$
$= g(f(x)f(y))$, क्योंकि f एक समाकारिता है।
$= g(f(x))\, g(f(y))$, क्योंकि g एक समाकारिता है।
$= g \circ f(x) \cdot g \circ f(y)$.

अतः $g \circ f$ एक समाकारिता है।

अब आप प्रमेय 2 की सहायता से नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 7) मान लीजिए $n \in N$. दिखाइए कि $f : \mathbf{Z} \to \mathbf{Z} : f(x) = nx$ और $g : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} : g(x) = \bar{x}$ का संयोजन एक समाकारिता है। Ker $g \circ f$ और Im$(g \circ f)$ क्या हैं?

अभी तक आपने देखा है कि समाकारिता की अष्टि और परिसर समुच्चय हैं। और अभी तक दिए गए उदाहरणों में शायद आपने नोट किया होगा कि ये उपसमूह हैं। अब हम सिद्ध करेंगे कि समाकारिता की अष्टि एक प्रसामान्य उपसमूह होती है और परिसर एक उपसमूह होता है।

प्रमेय 3 : मान लीजिए $f : G_1 \to G_2$ एक समूह समाकारिता है। तब

क) Ker f, G_1 का एक प्रसामान्य उपसमूह है।

ख) Im f, G_2 का एक उपसमूह है।

उपपत्ति : (क) चूंकि $f(e_1) = e_2$, इस लिए $e_1 \in$ Ker f.
$\therefore$ Ker f $\neq \phi$.

अब, यदि $x, y \in$ Ker f, तो $f(x) = e_2$ और $f(y) = e_2$.
$\therefore f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)\, [f(y)]^{-1} = e_2$.
$\therefore xy^{-1} \in$ Ker f.

इसलिए, इकाई 3 के प्रमेय 1 के अनुसार, Ker f $\leq G_1$.
अब, किसी $y \in G_1$ और $x \in$ Ker f के लिए
$f(y^{-1}xy) = f(y^{-1})\, f(x) f(y)$
$= [f(y)]^{-1} e_2 f(y)$, क्योंकि $f(x) = e_2$ और प्रमेय 1 के अनुसार।
$= e_2$.

$\therefore$ Ker f $\trianglelefteq G_1$.

ख) Im f $\neq \phi$, क्योंकि $f(e_1) \in$ Im f.
अब, मान लीजिए $x_2, y_2 \in$ Im f. तब $\exists\, x_1, y_1 \in G_1$ जिनसे कि $f(x_1) = x_2$ और $f(y_1) = y_2$.
$\therefore x_2 y_2^{-1} = f(x_1)\, f(y_1^{-1}) = f(x_1 y_1^{-1}) \in$ Im f.
$\therefore$ Im f $\leq G_2$.

इस परिणाम को लागू करके हम उदाहरण 2 से तुरंत देख सकते हैं कि शुद्धतः अधिकल्पित संख्याओं का समुच्चय C का एक प्रसामान्य उपसमूह है।

आइए अब हम एक और उदाहरण लें, जो E 4 की एक विशेष स्थिति है (जब n = 1)।

$\phi : (\mathbf{R}, +) \to (\mathbf{C}^*, .) : \phi(x) = \cos x + i \sin x$ लीजिए। हम जानते हैं कि $\phi(x + y) = \phi(x)\,\phi(y)$, अर्थात् ϕ एक समूह समाकारिता है। अब $\phi(x) = 1$ यदि और केवल यदि किसी $n \in \mathbf{Z}$ के लिए $x = 2\pi n$. इस तरह, प्रमेय 3 के अनुसार Ker $\phi = \{2\pi n \mid n \in \mathbf{Z}\}$, $(\mathbf{R}, +)$ का एक प्रसामान्य उपसमूह है। नोट कीजिए कि यह चक्रीय है, और 2π एक जनक है।

इसी प्रकार, हम देख सकते हैं कि Im ϕ, $\mathbf{C}^*$ का एक उपसमूह है। यह निरपेक्ष मान 1 वाले सभी सम्मिश्र संख्याओं का समुच्चय है, अर्थात् यह 1 इकाई त्रिज्या वाले और केन्द्र (0, 0) वाले वृत्त पर पड़ने वाले सभी सम्मिश्र संख्याओं का समुच्चय है।

आपने देखा होगा कि कभी तो समाकारिता की अष्टि {e} होती है (जैसा कि उदाहरण 1 में), और कभी-कभी एक बड़ा उपसमूह होती है (जैसा कि उदाहरण 2 में)। क्या अष्टि के आमाप से कुछ पता चलता है? हम सिद्ध करेंगे कि समाकारिता 1-1 होती है यदि और केवल यदि इसकी अष्टि {e} हो।

प्रमेय 4 : मान लीजिए $f : G_1 \longrightarrow G_2$ एक समूह समाकारिता है। तब f एकैकी होता है यदि और केवल यदि $\text{Ker } f = \{e_1\}$, जहाँ e_1 समूह G_1 का तत्समक अवयव है।

उपपत्ति : पहले तो मान लीजिए कि f एकैकी है। मान लीजिए कि $x \in \text{Ker } f$. तब $f(x) = e_2$, अर्थात् $f(x) = f(e_1)$. लेकिन f, 1-1 है। अतः $x = e_1$.
इस प्रकार, $\text{Ker } f = \{e_1\}$.

विलोमतः मान लीजिए कि $\text{Ker } f = \{e_1\}$. मान लीजिए कि $x, y \in G_1$ ऐसे हैं कि $f(x) = f(y)$. तब,

$$f(xy^{-1}) = f(x)\, f(y^{-1})$$
$$= f(x)\, [f(y)]^{-1} = e_2.$$

$\therefore xy^{-1} \in \text{Ker } f = \{e_1\}$. $\therefore xy^{-1} = e_1$ और $x = y$.

इससे पता चलता है कि f एकैकी है।

इस प्रकार प्रमेय 4 और उदाहरण 4 का प्रयोग करके हम तुरंत कह सकते हैं कि कोई भी आविष्टि $i : H \longrightarrow G$, 1-1 है, क्योंकि $\text{Ker } i = \{e\}$.

आइए हम एक और उदाहरण लें।

उदाहरण 5 : $\mathbf{R}^2$ के स्थानांतरणों का समूह T लीजिए (इकाई 2 का उदाहरण 6)। हम प्रतिचित्र $\phi : (\mathbf{R}^2, +) \longrightarrow (T, \circ)$ को $\phi(a, b) = f_{a,b}$ से परिभाषित करते हैं। दिखाइए कि ϕ एक आच्छादक समाकारिता है, जो 1-1 भी है।

हल : $\mathbf{R}^2$ के $(a, b), (c, d)$ के लिए हमने देखा है कि

$$f_{a+c,b+d} = f_{a,b} \circ f_{c,d}$$

$\therefore \phi((a, b) + (c, d)) = \phi(a, b) \circ \phi(c, d)$

अतः ϕ समूहों की एक समाकारिता है।

अब, T का कोई भी अवयव $f_{a,b} = \phi(a, b)$ के रूप का है। इसलिए ϕ आच्छादक है।

अब हम दिखाएंगे कि ϕ एकैकी भी है।

मान लीजिए कि $(a, b) \in \text{Ker } \phi$. तब $\phi(a, b) = f_{0,0}$, अर्थात्

$f_{a,b} = f_{0,0}$

$\therefore f_{a,b}(0, 0) = f_{0,0}(0, 0)$, अर्थात्

$(a, b) = (0, 0)$

$\therefore \text{Ker } \phi = \{ (0, 0) \}$

$\therefore \phi$, 1-1 है।

इस तरह हमने सिद्ध किया कि ϕ एक समाकारिता है जो एकैकी आच्छादक है।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 8) किसी $n > 1$ के लिए $\mathbf{Z}_n$ और $\mathbf{U}_n$ (इकाई 3 के उदाहरण 5 में दिए गए 1 के nवें मूलों का समूह) लीजिए। मान लीजिए ω, 1 के ऐसे nवें मूल को प्रकट करता है, जो U_n को जनित करता है। तब $U_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$ अब फलन $f : \mathbf{Z}_n \longrightarrow U_n : f(\bar{r}) = \omega^r$ लीजिए। दिखाइए कि f एक समूह समाकारिता है। क्या f, 1-1 है? क्या f आच्छादक है?

आइए अब हम एक आच्छादक समाकारिता के एक उपयोगी गुण पर विचार करें।

प्रमेय 5 : यदि $f : G_1 \longrightarrow G_2$ एक आच्छादक समूह समाकारिता हो और S, G_1 को जनित करने वाला एक उपसमुच्चय हो, तो $f(S)$, G_2 को जनित करता है।

उपपत्ति : हम जानते हैं कि

$G_1 = \langle S \rangle = \{ x_1^{r_1} x_2^{r_2} \ldots x_m^{r_m} \mid m \in \mathbf{N}$ और $x_i \in S, r_i \in \mathbf{Z} \; \forall \; i\}$.

हम दिखाएंगे कि $G_2 = \langle f(S) \rangle$.

मान लीजिए कि $x \in G_2$. चूंकि f आच्छादक है, इसलिए ऐसा $y \in G_1$ है जिससे कि $f(y) = x$.

चूंकि $y \in G_1$, इसलिए किसी $m \in \mathbf{N}$ के लिए
$y = x_1^{r_1} \dots x_m^{r_m}$, जहाँ $x_i \in S$ और $r_i \in Z$, $1 \le i \le m$ के लिए। इस तरह,
$x = f(y) = f(x_1^{r_1} \dots x_m^{r_m})$
$= (f(x_1))^{r_1} \dots (f(x_m))^{r_m}$, क्योंकि f समाकारिता है।
$\Rightarrow x \in < f(S) >$, क्योंकि प्रत्येक $i = 1, 2, \dots, r$ के लिए $f(x_i) \in f(S)$.

इस प्रकार, $G_2 = < f(S) >$.

नीचे दिए गए प्रश्न में हमने चक्रीय समूहों के एक महत्वपूर्ण गुण का उल्लेख किया है जिसे आप प्रमेय 5 की सहायता से सिद्ध कर सकते हैं।

E 9) दिखाइए कि चक्रीय समूह का समाकारी प्रतिबिंब (homomorphic image) चक्रीय होता है, अर्थात् यदि G एक चक्रीय समूह हो और $f : G \to G'$ एक समाकारिता हो, तो $f(G)$ चक्रीय होगा।

E 9 को हल करने पर आप तुरंत कह सकते हैं कि **चक्रीय समूह का कोई भी विभाग समूह चक्रीय होता है।**

अभी तक आपने विभिन्न प्रकार की समाकारिताओं—एकैकी, आच्छादक और एकैकी आच्छादक के उदाहरण देखे हैं। आइए अब हम विशेष रूप से एकैकी आच्छादक समाकारिताओं पर विचार करें।

6.3 तुल्याकारिता (Isomorphism)

इस भाग में हम उन समाकारिताओं पर विचार करेंगे जो 1-1 और आच्छादक हैं। हम कुछ परिभाषाओं से शुरू करते हैं।

परिभाषाएं : मान लीजिए G_1 और G_2 दो समूह हैं। समाकारिता $f : G_1 \to G_2$ को **तुल्याकारिता** कहते हैं, यदि f, 1-1 और आच्छादक हो।

इस स्थिति में हम कहते हैं कि **समूह G_1 समूह G_2 के तुल्याकारी** (isomorphic) है या G_1 और G_2 तुल्याकारी हैं। हम इसे $G_1 \simeq G_2$ से प्रकट करते हैं।

समूह G से स्वयं तक की तुल्याकारिता को G की **स्वाकारिता** (automorphism) कहते हैं। उदाहरण के लिए, तत्समक फलन $I_G : G \to G : I_G(x) = x$ एक स्वाकारिता है।

आइए हम तुल्याकारिता के एक अन्य उदाहरण पर विचार करें।

उदाहरण 6 : समुच्चय $G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| a, b \in \mathbf{R} \right\}$ लीजिए।
तब, G आव्यूह योग के प्रति एक समूह होता है। दिखाइए कि
$f : G \to C : f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + ib$ एक तुल्याकारिता है।

हल : आइए पहले हम सत्यापित करें कि f एक समाकारिता है।
अब, G के किन्हीं दो अवयवों $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ और $\begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ के लिए,

$$f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right) = f\left(\begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix}\right) = (a+c) + i(b+d)$$

$$= (a + ib) + (c + id)$$

$$= f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) + f\left(\begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right)$$

इसलिए f एक समाकारिता है।

अब, $\text{Ker} f = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| \, a + ib = 0 \right\} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \middle| \, a = 0, b = 0 \right\} = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$.

अतः प्रमेय 4 के अनुसार f, 1-1 है।
अंत में, चूंकि Im $f = C$, इसलिए f आच्छादक है।

अतः f एक तुल्याकारिता है।

अब हम एक महत्वपूर्ण टिप्पणी देना चाहेंगे।

टिप्पणी : यदि G_1 और G_2 तुल्याकारी समूह हों, तो उनकी समान बीजीय संरचना होगी और वे समान बीजीय गुणों को संतुष्ट करेंगे। उदाहरण के लिए, किसी परिमित समूह के तुल्याकारी कोई भी समूह परिमित होगा और समान कोटि की होगी। इस तरह, दो **तुल्याकारी समूह बीजीयतः अभिन्न तंत्र होते हैं।**

नीचे दिया गया प्रमेय तुल्याकारी समूहों का बीजीयतः समान होने का एक परिणाम है।

प्रमेय 6 : यदि $f : G \longrightarrow H$ एक समूह तुल्याकारिता हो और $x \in G$, तो $< x > \simeq < f(x) >$. इसलिए

i) यदि x परिमित कोटि का हो, तो $o(x) = o(f(x))$.

ii) यदि x अपरिमित कोटि का हो, तो $f(x)$ भी अपरिमित कोटि का होगा।

उपपत्ति : यदि हम G के किसी उपसमूह K तक f का संकुचन करें तो हमें फलन $f|_K : K \longrightarrow f(K)$ प्राप्त होता है। चूंकि f एकैकी आच्छादक है, इसलिए इसका संकुचन $f|_K$ भी एकैकी आच्छादक होगा। अतः G के किसी भी उपसमूह K के लिए $K \simeq f(K)$. विशेष रूप से, किसी $x \in G$ के लिए, $<x> \simeq f(<x>) = <f(x)>$, E 9 के अनुसार।

अब, यदि x परिमित कोटि का हो, तो $o(x) = o(< x >) = o(< f(x) >) = o(f(x))$. जिससे (i) सिद्ध हो जाता है।

(ii) को सिद्ध करने के लिए मान लीजिए x अपरिमित कोटि का है। तब $< x >$ एक अनंत समूह होगा। इसलिए $<f(x)>$ एक अनंत समूह होगा। अतः $f(x)$ अपरिमित कोटि का होगा। इस तरह हमने (ii) सिद्ध कर दिया है।

अब आप नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 10) दिखाइए कि नियत पूर्णांक n के लिए, $Z \simeq nZ$.
(संकेत : $f : (Z, +) \longrightarrow (nZ, +) : f(k) = nk$ लीजिए।)

E 11) क्या $f : Z \longrightarrow Z : f(x) = 0$ समाकारिता है? तुल्याकारिता है?

अगले दो प्रश्न तुल्याकारिता के व्यापक गुणों से संबंधित हैं। E 12 तुल्याकारिताओं के लिए प्रमेय 2 के अनुरूप है। E 13 इस तथ्य को प्रमाणित करता है कि तुल्याकारी समूहों के बीजीय गुण समान होते हैं।

E 12) यदि $\phi : G \longrightarrow H$ और $\theta : H \longrightarrow K$ समूहों की दो तुल्याकारिताएं हैं, तो दिखाइए कि $\theta \circ \phi$, G से K तक की एक तुल्याकारिता है।

E 13) यदि $f : G \longrightarrow H$ समूहों की एक तुल्याकारिता है और G आबेली है, तो दिखाइए कि H भी आबेली होगा।

अभी तक हमने तुल्याकारी समूहों के कई उदाहरण दिए हैं। अब आप नीचे दिए गए उदाहरण पर विचार कीजिए।

उदाहरण 7 : दिखाइए कि $(\mathbf{R}^*, .)$, $(\mathbf{C}^*, .)$ के तुल्याकारी नहीं है।

हल : मान लीजिए ये तुल्याकारी हैं और $f : C^* \to R^*$ एक तुल्याकारिता है। तब प्रमेय 6 के अनुसार $o(i) = o(f(i))$. अब $o(i) = 4$. $\therefore$ $o(f(i)) = 4$.

लेकिन, ± 1 के अलावा किसी भी वास्तविक संख्या की कोटि अपरिमित होती है और $o(1) = 1$, $o(-1) = 2$.

इस प्रकार, हमें एक अंतर्विरोध प्राप्त होता है। अतः जो हम मानकर चले थे, वह सही नहीं है। अर्थात् R^* और C^* तुल्याकारी नहीं हैं।

अब आप नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 14) दिखाइए कि $(C^*, .)$, $(R, +)$ के तुल्याकारी नहीं है।

E 15) क्या किसी $n \neq 1$ के लिए $Z \simeq Z/nZ$?

आपने देखा होगा कि तुल्याकारिता की परिभाषा से केवल इस बात का पता चलता है कि यह फलन एकैकी आच्छादक है, अर्थात् इसके प्रतिलोम का अस्तित्व होता है। लेकिन, इससे हमें प्रतिलोम के किसी गुण के बारे में कुछ पता नहीं चलता। नीचे दिया गया परिणाम इसी से संबंधित है।

प्रमेय 7 : यदि $f : G_1 \to G_2$ समूहों की एक तुल्याकारिता हो, तो $f^{-1} : G_2 \to G_1$ भी एक तुल्याकारिता होगी।

उपपत्ति : इकाई 1 से हम जानते हैं कि f^{-1} एकैकी आच्छादक है। अतः यहाँ हमें केवल यह दिखाने की आवश्यकता है कि f^{-1} एक समाकारिता है। मान लीजिए $a', b' \in G_2$ और $a = f^{-1}(a')$, $b = f^{-1}(b')$. तब $f(a) = a'$ और $f(b) = b'$. इसलिए $f(ab) = f(a)\, f(b) = a'b'$.

f^{-1} लागू करने पर हमें निम्नलिखित प्राप्त होता है :
$f^{-1}(a'b') = f^{-1}(a')\, f^{-1}(b')$. इस प्रकार,
$f^{-1}(a'b') = f^{-1}(a')\, f^{-1}(b')$ सभी $a', b' \in G_2$ के लिए। अतः f^{-1} एक तुल्याकारिता है।

उदाहरण 5 और प्रमेय 7 से हम तुरंत कह सकते हैं कि

$\phi^{-1} : T \to R^2 : \phi^{-1}(f_{a,b}) = (a, b)$ एक तुल्याकारिता है।

प्रमेय 7 के अनुसार, यदि $G_1 \simeq G_2$, तो $G_2 \simeq G_1$. हम इस परिणाम का प्रयोग अक्सर करेंगे (उदाहरण के लिए, प्रमेय 9 को सिद्ध करने में)।

आइए, अब हम समूह सिद्धांत के एक अति-महत्वपूर्ण प्रमेय पर विचार करें। खंड 3 में आप वलय सिद्धांत में इसके अनुरूप का अध्ययन करेंगे और रैखिक बीजगणित के पाठ्यक्रम में आप रैखिक रूपांतरणों के लिए इसके अनुरूप का अध्ययन कर चुके हैं।

6.4 तुल्याकारिता प्रमेय

इस भाग में हम समाकारिताओं और विभाग समूहों के बीच के संबंध के बारे में कुछ परिणाम सिद्ध करेंगे। पहला परिणाम समूहों के लिए समाकारिता का मूल प्रमेय (Fundamental Theorem of Homomorphism) है। इस प्रमेय को "मूल" इसलिए माना जाता है, क्योंकि समूह-सिद्धांत का काफ़ी भाग इस परिणाम पर निर्भर करता है। इस परिणाम को प्रथम तुल्याकारिता प्रमेय भी कहते हैं।

प्रमेय 8 (समाकारिता का मूल प्रमेय) : मान लीजिए कि G_1 और G_2 दो समूह हैं और $f : G_1 \to G_2$ एक समूह समाकारिता है। तब, $G_1/\text{Ker } f \simeq \text{Im } f$.
विशेष रूप से, यदि f आच्छादक हो, तो $G_1/\text{Ker } f \simeq G_2$.

उपपत्ति : मान लीजिए $\text{Ker } f = H$. ध्यान दीजिए कि $H \trianglelefteq G_1$. आइए हम फलन
$\psi : G_1/H \to \text{Im } f : \psi(Hx) = f(x)$.
परिभाषित करें।

इसे देखने पर ऐसा मालूम पड़ता है कि ψ की परिभाषा सहसमुच्चय के प्रतिनिधि पर निर्भर करती है। लेकिन हम दिखाएंगे कि यदि $x, y \in G_1$ ऐसे हों कि $Hx = Hy$, तब $\psi(Hx) = \psi(Hy)$. इससे यह सिद्ध हो जाएगा कि ψ एक सुपरिभाषित फलन है।

अब, $Hx = Hy \implies xy^{-1} \in H = \text{Ker } f \implies f(xy^{-1}) = e_2$, G_2 का तत्समक।

$$\implies f(x)[f(y)]^{-1} = e_2 \implies f(x) = f(y).$$

$$\implies \psi(Hx) = \psi(Hy).$$

अतः ψ एक सुपरिभाषित फलन है।

आइए अब हम सत्यापित करें कि ψ एक समाकारिता है। $Hx, Hy \in G_1/H$ के लिए

$\psi((Hx)(Hy)) = \psi(Hxy)$

$= f(xy)$

$= f(x)\, f(y)$, क्योंकि f एक समाकारिता है।

$= \psi(Hx)\, \psi(Hy)$.

अतः ψ एक समूह समाकारिता है।

चलिए अब देखें कि ψ एकैकी आच्छादक है कि नहीं।

अब, G_1/H में Hx, Hy के लिए

$\psi(Hx) = \psi(Hy)$

$\implies f(x) = f(y)$

$\implies f(x)\,[f(y)]^{-1} = e_2$

$\implies f(xy^{-1}) = e_2$

$\implies xy^{-1} \in \text{Ker } f = H.$

$\implies Hx = Hy$

$\therefore\ \psi$, 1-1 है।

और $\text{Im } f$ का कोई भी अवयव $f(x) = \psi(Hx)$ के रूप का है, जहाँ $x \in G_1$.

$\therefore\ \text{Im } \psi = \text{Im } f.$

इस तरह हमने सिद्ध किया है कि ψ एकैकी आच्छादक है। अतः यह एक तुल्याकारिता है।

इस तरह, $G_1/\text{Ker } f \simeq \text{Im } f$. अब, यदि f आच्छादक हो, तो $\text{Im } f = G_2$.

अतः इस स्थिति में $G_1/\text{Ker } f \simeq G_2$.

हमने प्रमेय 8 की स्थिति को नीचे दिए गए आरेख में दर्शाया है।

$$\begin{tikzcd}
G_1 \arrow[rr, "f"] \arrow[dr, "p"'] & & \text{Im } f \leq G_2 \\
& G_1/\text{Ker } f \arrow[ur, dotted, "\psi"'] &
\end{tikzcd}$$

यहां p प्राकृतिक समाकारिता है (देखिए उदाहरण 3)।

आरेख को देखने से पता चलता है कि यदि आप G_1 के अवयवों पर पहले p लागू करें और फिर ψ लागू करें तो परिणाम वही होता है जो कि उन पर f लागू करने से होता है। अर्थात्

$\psi \circ p = f.$

साथ ही, ध्यान दीजिए कि प्रमेय 8 के अनुसार f के प्रति G_1 के दो अवयवों का समान प्रतिबिंब होता है यदि और केवल यदि वे $\text{Ker } f$ के समान सहसमुच्चय के सदस्य हों।

आइए अब हम कुछ उदाहरणों पर विचार करें। एक सरल स्थिति $I_G : G \to G$ है। यहाँ प्रमेय 8 को लागू करने पर हम पाते हैं कि $G/\{e\} \simeq G$. इस कारण हम $G/\{e\}$ और G को कई बार एक ही मानेंगे।

आइए अब हम कुछ अतुच्छ उदाहरण लें।

उदाहरण 8 : सिद्ध कीजिए कि $C/R \simeq R$.

हल : $f : C \longrightarrow R : f(a + ib) = b$ परिभाषित कीजिए। तब f एक समाकारिता है, $Ker\, f = R$ और $Im = R$. इसलिए प्रमेय 8 लागू करने पर हम पाते हैं कि $C/R \simeq R$.

उदाहरण 9 : फलन $f : Z \longrightarrow (\{1, -1\}, .) : f(n) = \begin{cases} 1, & \text{यदि } n \text{ सम हो} \\ -1, & \text{यदि } n \text{ विषम हो} \end{cases}$

लीजिए। भाग 6.2 के शुरू में आपने देखा था कि f एक समाकारिता है। Ker f और Im f प्राप्त कीजिए। इस स्थिति में प्रमेय 8 के अनुसार क्या होता है?

हल : मान लीजिए Z_e और Z_o क्रमशः सम पूर्णांकों और विषम पूर्णांकों के समुच्चयों को प्रकट करते हैं। तब,

$Ker\, f = \{ n \in Z \mid f(n) = 1 \} = Z_e$,
$Im\, f = \{ f(n) \mid n \in Z \} = \{ 1, -1 \}$.
इस तरह, प्रमेय 8 के अनुसार $Z/Z_e \simeq \{ 1, -1 \}$.
इससे यह भी पता चलता है कि $o(Z/Z_e) = 2$.
Z में Z_e के दो सहसमुच्चय Z_e और Z_o हैं।
$\therefore \{ Z_e, Z_o \} \simeq \{ 1, -1 \}$.

उदाहरण 10 : दिखाइए कि $GL_2(R)/SL_2(R) \simeq R^*$, जहाँ
$SL_2(R) = \{A \in GL_2(R) \mid \det(A) = 1 \}$.

हल : हम जानते हैं कि फलन
$f : GL_2(R) \longrightarrow R^* : f(A) = \det(A)$ एक समाकारिता है। अब, $Ker\, f = SL_2(R)$.

और $Im\, f = R^*$, क्योंकि किसी $r \in R^*$ को $\det\left(\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix}\right)$ के रूप में लिखा जा सकता है।

इस प्रकार, प्रमेय 8 लागू करने पर $GL_2(R)/SL_2(R) \simeq R^*$.

अब आप नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 16) उदाहरण 1 की स्थिति लीजिए। दिखाइए कि $(R, +) \simeq (R^+, .)$ धन वास्तविक संख्याओं का समूह।

E 17) मान लीजिए U_4, 1 के चौथे मूलों का गुणनात्मक समूह है।
$f : Z \longrightarrow U_4 : f(n) = i^n$ परिभाषित कीजिए। प्रमेय 8 लागू करके दिखाइए कि $Z_4 \simeq U_4$.
(यहां $i = \sqrt{-1}$.)

अब हम एक ऐसे महत्वपूर्ण परिणाम को सिद्ध करने के लिए समाकारिता के मूल प्रमेय का प्रयोग करेंगे, जिससे सभी चक्रीय समूहों का वर्गीकरण होता है।

प्रमेय 9 : कोई भी चक्रीय समूह $(Z, +)$ या $(Z_n, +)$ के तुल्याकारी होता है।

उपपत्ति : मान लीजिए $G = < x >$ एक चक्रीय समूह है।
$f : Z \longrightarrow G : f(n) = x^n$ परिभाषित कीजिए।

f एक समाकारिता है, क्योंकि
$f(n + m) = x^{n+m} = x^n . x^m = f(n) f(m)$.

और यह भी ध्यान दीजिए कि $Im\, f = G$.

अब Ker f की दो संभावनाएं हो सकती हैं— $Ker\, f = \{0\}$ या $Ker\, f \neq \{0\}$

स्थिति ($Ker\, f = \{0\}$) : इस स्थिति में f, 1-1 है। इसलिए f एक तुल्याकारिता है। अतः प्रमेय 7 के अनुसार f^{-1} एक तुल्याकारिता है। अर्थात् $G \simeq (Z, +)$.

स्थिति 2 ($Ker\, f \neq \{0\}$) : चूंकि $Ker\, f \leq Z$, इसलिए इकाई 3 के उदाहरण 4 से हम जानते हैं कि

किसी $n \in \mathbf{N}$ के लिए $\text{Ker } f = n\mathbf{Z}$. अतः समाकारिता के मूल प्रमेय से $\mathbf{Z}/n\mathbf{Z} \simeq G$.

$\therefore\ G \simeq \mathbf{Z}/n\mathbf{Z} \simeq (\mathbf{Z}_n, +)$

यहाँ नोट कीजिए, चूँकि $< x > \simeq \mathbf{Z}_n$, $o(x) = n$. अतः कोई भी परिमित चक्रीय समूह, $\mathbf{Z}_n$ के तुल्याकारी है, जहाँ n समूह की कोटि है।

प्रमेय 9 के प्रयोग से हम कह सकते हैं कि कोटि 4 वाले सभी चक्रीय समूह तुल्याकारी होते हैं, क्योंकि ये सभी $\mathbf{Z}_4$ के तुल्याकारी हैं। इसी प्रकार, सभी अनंत चक्रीय समूह तुल्याकारी होते हैं।

अब आप नीचे दिए गए परिणाम को सिद्ध कर सकते हैं।

E 18) मान लीजिए S वृत्त समूह $\{ z \in \mathbf{C} \mid |z| = 1 \}$ है। दिखाइए कि $\mathbf{R}/\mathbf{Z} \simeq S$.
(संकेत : $f: \mathbf{R} \longrightarrow S : f(x) = e^{2\pi i x}$ परिभाषित कीजिए। दिखाइए कि f एक आच्छादक **समाकारिता है और** $\text{Ker } f = \mathbf{Z}$.)

अब हम समाकारिता के मूल प्रमेय की सहायता से दूसरा तुल्याकारिता प्रमेय सिद्ध करेंगे। इसका संबंध उपसमूहों के प्रतिच्छेद और गुणनफल से है। इस प्रमेय को सिद्ध करने के लिए हमें नीचे के प्रश्न में दिए गए परिणाम की आवश्यकता होगी। तब क्यों न आप पहले इसी प्रश्न को हल कर लें!

E 19) मान लीजिए G एक समूह है, $H \leq G$ और $K \trianglelefteq G$. तब

क) $H \cap K \trianglelefteq H$, और

ख) यदि $A \leq G$ ऐसा है $K \subseteq A$, तो $K \trianglelefteq A$.

आइए अब हम प्रमेय पर विचार करें।

प्रमेय 10 : यदि H और K समूह G के उपसमूह हों, जहाँ K, G में प्रसामान्य है, तो
$H/(H \cap K) \simeq (HK)/K$.

उपपत्ति : पहले हम सत्यापित करेंगे कि विभाग समूह $H/(H \cap K)$ और $(HK)/K$ सुपरिभाषित हैं। E 19 से हम जानते हैं कि $H \cap K \trianglelefteq H$.

इकाई 5 के E 6 से हम जानते हैं कि $HK \leq G$ और E 19 से हम जानते हैं कि $K \trianglelefteq HK$. इस प्रकार, हम पाते हैं कि दिए हुए विभाग समूह अर्थपूर्ण हैं।

अब हमें अष्टि $H \cap K$ वाला एक आच्छादक समाकारिता $f : H \longrightarrow (HK)/K$ प्राप्त करना है। और तब समाकारिता का मूल प्रमेय लागू करके हम परिणाम प्राप्त कर सकेंगे। हम
$f : H \longrightarrow (HK)/K : f(h) = hK$ परिभाषित करते हैं।

अब, $x, y \in H$ के लिए
$f(xy) = xy\, K = (xK)\,(yK) = f(x)\, f(y)$.
अतः f एक समाकारिता है।

$\text{Im } f = \{ f(h) \mid h \in H \} = \{ hK \mid h \in H \}$.
हम दिखाएंगे कि $\text{Im } f = (HK)/K$. इसके लिए एक अवयव $hK \in \text{Im } f$ लीजिए। चूँकि $h \in H$, इसलिए $h \in HK$.
$\therefore\ hK \in (HK)/K.\ \therefore\ \text{Im } f \subseteq (HK)/K$.

दूसरी ओर, $(HK)/K$ का कोई अवयव $hk\, K$ लीजिए। तब

$\quad = f(h) \in \text{Im } f$.
$\therefore\ (HK)/K \subseteq \text{Im } f$.
$\therefore\ \text{Im } f = (HK)/K$.

अंत में, $\text{Ker } f = \{ h \in H \mid f(h) = K \} = \{ h \in H \mid hK = K \}$
$= \{ h \in H \mid h \in K \}$
$= H \cap K.$

अतः मूल प्रमेय लागू करने पर हमें $H/(H \cap K) \simeq (HK)/K$ प्राप्त होता है।

अब हम एक टिप्पणी देना चाहेंगे।

टिप्पणी : यदि H और K, (G, +) के उपसमूह हों, तो प्रमेय 10 के अनुसार
$(H + K)/K \simeq H/(H \cap K)$.

अब आप नीचे दिए गए प्रश्नों को हल करने के लिए प्रमेय 10 का प्रयोग कर सकते हैं।

E 20) मान लीजिए H और K परिमित समूह G के उपसमूह हैं, और $H \trianglelefteq G$. दिखाइए कि
$$o(HK) = \frac{o(H)\, o(K)}{o(H \cap K)}$$

E 21) दिखाइए कि $3\mathbf{Z}/12\mathbf{Z} \simeq \mathbf{Z}_4$.
(संकेत : $H = 3\mathbf{Z}, K = 4\mathbf{Z}$) लीजिए।)

और अब तीसरे समाकारिता प्रमेय पर विचार करें। यह भी प्रमेय 8 का एक उपप्रमेय है।

प्रमेय 11 : मान लीजिए H और K समूह G के प्रसामान्य उपसमूह हैं और $K \subseteq H$. तब,

$(G/K)/(H/K) \simeq G/H.$

उपपत्ति : हम G/K से G/H तक एक आच्छादक समाकारिता परिभाषित करेंगे, जिसकी अष्टि H/K होगी।

$f : G/K \to G/H : f(Kx) = Hx$ लीजिए। f सुपरिभाषित है, क्योंकि $x, y \in G$ के लिए
$Kx = Ky \Rightarrow xy^{-1} \in K \subseteq H \Rightarrow xy^{-1} \in H \Rightarrow Hx = Hy \Rightarrow f(Kx) = f(Ky).$

उपपत्ति का शेष भाग हम आप पर छोड़ रहे हैं (नीचे दिए गए प्रश्न को देखिए)।

E 22) दिखाइए कि f एक आच्छादक समाकारिता है और $\text{Ker } f = H/K$.

आइए अब हम किसी समूह से स्वयं तक की तुल्याकारिताओं पर विचार करें।

6.5 स्वाकारिता (Automorphism)

इस भाग में पहले हम दिखाएंगे कि किसी समूह की सभी स्वाकारिताओं का समुच्चय एक समूह है। फिर हम इस समूह के एक विशेष उपसमूह को परिभाषित करेंगे।

मान लीजिए G एक समूह है। निम्नलिखित समुच्चय लीजिए :

$\text{Aut } G = \{ f : G \to G \mid f$ एक तुल्याकारिता है $\}$.

आप देख चुके हैं कि तत्समक फलन $I_G \in \text{Aut } G$. E 12 से आप जानते हैं कि संयोजन की द्वि-आधारी संक्रिया के सापेक्ष Aut G संवृत है। और, प्रमेय 7 के अनुसार, यदि $f \in \text{Aut } G$, तो $f^{-1} \in \text{Aut } G$. हम इस चर्चा को संक्षेप में निम्नलिखित प्रमेय के रूप में प्रस्तुत करते हैं।

प्रमेय 12 : मान लीजिए G एक समूह है। तब Aut G, G की स्वाकारिताओं का समुच्चय, एक समूह है।

आइए अब हम Aut G के एक उदाहरण को देखें।

उदाहरण 11 : दिखाइए कि Aut $\mathbf{Z} \simeq \mathbf{Z}_2$.

हल : मान लीजिए $f : \mathbf{Z} \to \mathbf{Z}$ एक स्वाकारिता है। मान लीजिए $f(1) = n$. अब हम दिखाएंगे कि $n = 1$ या -1.
चूंकि f आच्छादक है और $1 \in \mathbf{Z}$, इसलिए $\exists\ m \in \mathbf{Z}$ जिसके लिए $f(m) = 1$,
अर्थात् $mn = 1$.
$\therefore\ n = 1$ या $n = -1$.

इस प्रकार, Aut $\mathbf{Z}$ में केवल दो अवयव हैं, I और $-$ I.
इसलिए Aut $\mathbf{Z} = \langle -I \rangle \simeq \mathbf{Z}_2$.

अब समूह G के कोई दिए हुए अवयव के संगत हम G की एक स्वाकारिता परिभाषित करेंगे। एक नियत अवयव $g \in G$ लीजिए।
$f_g : G \to G : f_g(x) = gxg^{-1}$ परिभाषित कीजिए।

हम दिखाएंगे कि f_g, G की एक स्वाकारिता है।

i) f_g एक समाकारिता है : यदि $x, y \in G$, तो

$$\begin{aligned} f_g(xy) &= g(xy)g^{-1} \\ &= gx(e)yg^{-1}, \text{ जहाँ } e, G \text{ का तत्समक है।} \\ &= gx(g^{-1}g)yg^{-1} \\ &= (gxg^{-1})(gyg^{-1}) \\ &= f_g(x)\,f_g(y). \end{aligned}$$

ii) f_g, 1-1 है : $x, y \in G$, के लिए

$$\begin{aligned} f_g(x) = f_g(y) &\Rightarrow gxg^{-1} = gyg^{-1} \\ &\Rightarrow x = y, \text{ G में निरसन नियम लागू करने पर।} \end{aligned}$$

iii) f_g आच्छादक है : यदि $y \in G$, तो

$$\begin{aligned} y &= (gg^{-1})\,y(gg^{-1}) \\ &= g(g^{-1}yg)\,g^{-1} \\ &= f_g(g^{-1}yg) \in \operatorname{Im} f_g. \end{aligned}$$

इस प्रकार हम पाते हैं कि f_g, G की एक स्वाकारिता है। हम इस स्वाकारिता को एक विशेष नाम देते हैं।

परिभाषा : f_g को G के अवयव g **द्वारा प्रेरित G की आंतर स्वाकारिता** (inner automorphism) कहते हैं। G की सभी आंतर स्वाकारिताओं से बना Aut G के उपसमुच्चय को **Inn G** से प्रकट करते हैं।

उदाहरण के लिए, S_3 लीजिए। आइए हम $f_g(I)$, $f_g(1\ 3)$ और $f_g(1\ 2\ 3)$ का परिकलन करें, जहाँ $g = (1\ 2)$. ध्यान दीजिए कि $g^{-1} = (1\ 2) = g$.
अब, $f_g(I) = g \circ I \circ g^{-1} = I$,
$f_g(1\ 3) = (1\ 2)(1\ 3)(1\ 2) = (2\ 3)$,
$f_g(1\ 2\ 3) = (1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2)$.

नीचे दिए गए प्रश्न से आपको आंतर स्वाकारिताओं को प्राप्त करने का कुछ अभ्यास हो जाएगा।

E 23) $f_g \in$ Inn G का परिसर प्राप्त कीजिए, जहाँ

क) $G = GL_2(\mathbf{R})$ और $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

ख) $G = \mathbf{Z}$ और $g = 3$.

ग) $G = \mathbf{Z}/5\mathbf{Z}$ और $g = \bar{4}$.

अब आप देखेंगे कि Inn G, Aut G का एक प्रसामान्य उपसमूह है।

प्रमेय 13 : मान लीजिए G एक समूह है। तब Inn G, Aut G का एक प्रसामान्य उपसमूह होता है।

उपपत्ति : Inn G अरिक्त है, क्योंकि $I_G = f_e \in$ Inn G, जहाँ e, G में तत्समक है।

आइए अब हम देखें कि $g, h \in G$ के लिए $f_g \circ f_h \in$ Inn G या नहीं।

किसी $x \in G$ के लिए

$$\begin{aligned} f_g \circ f_h(x) &= f_g(hxh^{-1}) \\ &= g(hxh^{-1})g^{-1} \\ &= (gh)\ x\ (gh)^{-1} \\ &= f_{gh}(x) \end{aligned}$$

इस तरह, $f_{gh} = f_g \circ f_h$, अर्थात् संयोजन के सापेक्ष Inn G संवृत है।

और $f_e = I_G$, Inn G में है। अब, $f_g \in$ Inn G के लिए, $\exists\, f_{g^{-1}} \in$ Inn G,
जिससे कि $f_g \circ f_{g^{-1}} = f_{gg^{-1}} = f_e = I_G$.
इसी प्रकार, $f_{g^{-1}} \circ f_g = I_G$.

इस तरह, $f_{g^{-1}} = (f_g)^{-1}$, अर्थात् Inn G के प्रत्येक अवयव का Inn G में एक प्रतिलोम होता है।

इससे यह सिद्ध हो जाता है कि Inn G, Aut G का एक उपसमूह है।

अब Inn G $\trianglelefteq$ Aut G सिद्ध करने के लिए मान लीजिए कि $\phi \in$ Aut G और $f_g \in$ Inn G.
तब $x \in G$ के लिए

$$\begin{aligned} \phi^{-1} \circ f_g \circ \phi(x) &= \phi^{-1} \circ f_g(\phi(x)) \\ &= \phi^{-1}(g\phi(x)g^{-1}) \\ &= \phi^{-1}(g)\ \phi^{-1}(\phi(x))\ \phi^{-1}(g^{-1}) \\ &= \phi^{-1}(g)\ x[\phi^{-1}(g)]^{-1} \\ &= f_{\phi^{-1}(g)}(x). \end{aligned}$$ (ध्यान दें कि $\phi^{-1}(g) \in G$.)

$\therefore\ \phi^{-1} \circ f_g \circ \phi = f_{\phi^{-1}(g)} \in$ Inn G $\forall\ \phi \in$ Aut G और $f_g \in$ Inn G.
$\therefore$ Inn G $\trianglelefteq$ Aut G.

अब कुछ प्रश्न! E 23 से शायद आपको E 24 में दिए गए उपयोगी परिणाम का संकेत प्राप्त हो गया होगा।

E 24) दिखाइए कि समूह G क्रमविनिमेय होता है यदि और केवल यदि Inn G = $\{I_G\}$.

E 25) दिखाइए कि यदि $x \in G$ ऐसा हो कि $f_g(x) = x\ \forall\ g \in G$, तो $\langle x \rangle \trianglelefteq G$.

अब हम एक रोचक परिणाम सिद्ध करेंगे, जो समूह G के केन्द्र के सहसमुच्चयों का Inn G के साथ संबंध स्थापित करता है। आपको याद होगा कि G का केन्द्र $Z(G) = \{x \in G \mid xg = gx\ \forall\ g \in G\}$.

प्रमेय 14 : मान लीजिए G एक समूह है। तब $G/Z(G) \simeq$ Inn G.

उपपत्ति : हम इस परिणाम को सिद्ध करने के लिए शक्तिशाली समाकारिता के मूल प्रमेय का प्रयोग करेंगे।

हम $f : G \longrightarrow$ Aut G : $f(g) = f_g$ परिभाषित करते हैं।
पहले तो, f एक समाकारिता है क्योंकि $g, h \in G$ के लिए

$$\begin{aligned} f(gh) &= f_{gh} \\ &= f_g \circ f_h \end{aligned}$$ (प्रमेय 13 की उपपत्ति देखिए)
$$= f(g) \circ f(h).$$

इसके बाद Im f = $\{f_g \mid g \in G\}$ = Inn G.

अंत में,
$$\begin{aligned} \text{Ker } f &= \{g \in G \mid f_g = I_G\} \\ &= \{g \in G \mid f_g(x) = x\ \forall\ x \in G\} \\ &= \{g \in G \mid gxg^{-1} = x\ \forall\ x \in G\} \\ &= \{g \in G \mid gx = xg\ \forall\ x \in G\} \\ &= Z(G). \end{aligned}$$

अतः मूल प्रमेय के अनुसार,

$G/Z(G) \simeq \text{Inn } G.$

अब आप नीचे दिए गए प्रश्न को प्रमेय 14 के प्रयोग से हल कर सकते हैं।

E 26) दिखाइए कि $S_3 \simeq \text{Inn } S_3$.

आइए अब देखें कि हमने इस इकाई में क्या किया है।

6.6 सारांश

इस इकाई में हमने निम्नलिखित बातों पर चर्चा की है।

1. समूह समाकारिता की परिभाषा और उदाहरण।
2. मान लीजिए $f: G_1 \longrightarrow G_2$ एक समूह समाकारिता है। तब $f(e_1) = e_2$, $[f(x)]^{-1} = f(x^{-1})$, $\text{Im } f \leq G_2$, $\text{Ker } f \trianglelefteq G_1$.
3. समाकारिता 1-1 होती है यदि और केवल यदि उसकी अष्टि तुच्छ उपसमूह हो।
4. समूह तुल्याकारिता की परिभाषा और उदाहरण।
5. दो समूह तुल्याकारी होते हैं यदि और केवल यदि उनके बिल्कुल समान बीजीय संरचनाएं हों।
6. समूह समाकारिताओं (तुल्याकारिताओं) का संयोजन एक समूह समाकारिता (तुल्याकारिता) है।
7. समाकारिता के मूल प्रमेय की उपपत्ति, जिसके अनुसार यदि $f: G_1 \longrightarrow G_2$ एक समूह समाकारिता हो, तो $G_1/\text{Ker } f \simeq \text{Im } f$.
8. कोई भी अनंत चक्रीय समूह $(\mathbf{Z}, +)$ के तुल्याकारी होता है। कोटि n वाला परिमित चक्रीय समूह $(\mathbf{Z}_n, +)$ के तुल्याकारी होता है।
9. मान लीजिए G एक समूह है, $H \leq G$, $K \trianglelefteq G$. तब $H/(H \cap K) \simeq (HK)/K$.
10. मान लीजिए G एक समूह है, $H \trianglelefteq G$, $K \trianglelefteq G$, $K \subseteq H$. तब $(G/K)/(H/K) \simeq G/H$.
11. समूह G की स्वाकारिताओं का समुच्चय, Aut G फलनों के संयोजन के सापेक्ष एक समूह है।
12. किसी समूह G के लिए $\text{Inn } G \trianglelefteq \text{Aut } G$.
13. किसी समूह G के लिए $G/Z(G) \simeq \text{Inn } G$.

6.7 हल/उत्तर

E 1) $x, y \in \mathbf{R}^*$ के लिए $f(x\,y) = \ln(xy) = \ln x + \ln y$.

$\therefore$ f एक समाकारिता है।

$\text{Ker } f = \{ x \in \mathbf{R}^* \mid f(x) = 0 \} = \{1\}$.

$\text{Im } f = \{ f(x) \mid x \in \mathbf{R}^* \} = \{ \ln x \mid x \in \mathbf{R}^* \}$.

E 2) $A, B \in GL_3(\mathbf{R})$ के लिए

$f(AB) = \det(AB) = \det(A)\det(B) = f(A)\,f(B)$.

$\therefore$ f एक समाकारिता है।

$\text{Ker } f = \{ A \in GL_3(\mathbf{R}) \mid f(A) = 1 \} = \{ A \in GL_3(\mathbf{R}) \mid \det(A) = 1 \}$

$= SL_3(\mathbf{R})$, कोटि 3 वाला विशेष रैखिक समूह।

$\text{Im } f = \{ \det(A) \mid A \in GL_3(\mathbf{R}) \} = \mathbf{R}^*$ (क्योंकि किसी भी $r \in \mathbf{R}^*$ के लिए

$$\exists\ A = \begin{bmatrix} r & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in GL_3(\mathbf{R}) \text{ जिससे कि } \det(A) = r.$$

E 3) $p : S_3 \longrightarrow S_3/A_3 : p(x) = A_3x.$
ध्यान दीजिए कि $A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$.
अब, $\text{Ker}\ p = A_3$. $\therefore (1\ 2) \notin \text{Ker}\ p$.
$\text{Im}\ p = \{A_3x \mid x \in S_3\}$. $\therefore (1\ 2) \notin \text{Im}\ p$.

E 4) $x, y \in \mathbf{R}$ के लिए
$f(x + y) = e^{in(x+y)} = e^{inx} \cdot e^{iny} = f(x) \cdot f(y)$.
$\therefore$ f एक समाकारिता है।
$\text{Ker}\ f = \{x \in \mathbf{R} \mid f(x) = 1\} = \{x \in \mathbf{R} \mid e^{inx} = 1\}$

$$= \{x \in \mathbf{R} \mid nx \in 2\pi \mathbf{Z}\} = \frac{2\pi}{n}\mathbf{Z}.$$

E 5) उदाहरण 3 से हम जानते हैं कि यदि हम $G_1 = G/H$ लें और f को G से G/H पर प्राकृतिक समाकारिता मान लें, तो $\text{Ker}\ f = H$.

E 6) $i : 3\mathbf{Z} \longrightarrow \mathbf{Z} : i(3n) = 3n$.
$\text{Ker}\ i = \{3n \mid 3n = 0\} = \{0\}$
$\text{Im}\ i = 3\mathbf{Z}$.

E 7) $g \circ f : \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z} : g \circ f(x) = \overline{nx} = \overline{0}$.
तब, किन्हीं $x, y \in \mathbf{Z}$ के लिए
$g \circ f(x + y) = \overline{0} = \overline{0} + \overline{0} = g \circ f(x) + g \circ f(y)$.
$\therefore g \circ f$ एक समाकारिता है।

E 8) किन्हीं $\overline{r}, \overline{s} \in \mathbf{Z}_n$ के लिए
$f(\overline{r} + \overline{s}) = f(\overline{r + s}) = \omega^{r+s} = \omega^r . \omega^s = f(\overline{r}) . f(\overline{s})$.
$\therefore$ f एक समाकारिता है।
f, 1-1 है, क्योंकि
$f(\overline{r}) = 1 \implies \omega^r = 1$
$\implies r \mid o(\omega) = n$ (देखिए इकाई 4)
$\implies \overline{r} = \overline{0}$
$\therefore \text{Ker}\ f = \{\overline{0}\}$.
f आच्छादक है क्योंकि U_n का कोई अवयव ω^r है, $0 \le r \le n - 1$, के लिए, और $\omega^r = f(\overline{r})$.

E 9) मान लीजिए $G = \langle x \rangle$ और $f : G \longrightarrow G'$ एक समाकारिता है। तब $f : G \longrightarrow f(G)$ एक आच्छादक समाकारिता है। इसलिए प्रमेय 5 के अनुसार $f(G) = \langle f(x) \rangle$, अर्थात् f(G) चक्रीय है।

E 10) क) फलन $f : \mathbf{Z} \longrightarrow n\mathbf{Z} : f(k) = nk$ एक सुपरिभाषित फलन है।
अब, $f(m + k) = n(m + k) = nm + nk = f(m) + f(k)\ \forall\ m, k \in \mathbf{Z}$.
$\therefore$ f एक समाकारिता है।
$\text{Ker}\ f = \{0\}$. $\therefore$ f, 1-1 है।
$\text{Im}\ f = n\mathbf{Z}$. $\therefore$ f आच्छादक है।
$\therefore$ f एक तुल्याकारिता है और $\mathbf{Z} \simeq n\mathbf{Z}$.

E 11) f एक समाकारिता है, परन्तु 1-1 नहीं है।
अत: f एक तुल्याकारिता नहीं है।

E 12) प्रमेय 2 के अनुसार $\theta \circ \phi$ एक समाकारिता है। अब मान लीजिए $x \in \text{Ker}\ (\theta \circ \phi)$
तब,
$(\theta \circ \phi)(x) = 0 \implies \theta(\phi(x)) = 0$
$\implies \phi(x) = 0$, क्योंकि θ, 1-1 है।
$\implies x = 0$, क्योंकि ϕ, 1-1 है।

$\therefore \text{Ker}\ (\theta \circ \phi) = \{0\}$. $\therefore \theta \circ \phi$, 1-1 है।

अंत में, कोई $k \in K$ लीजिए। तब किसी $h \in H$ के लिए $k = \theta(h)$, क्योंकि θ आच्छादक है। अब किसी $g \in G$ के लिए $h = \phi(g)$, क्योंकि ϕ आच्छादक है।

$\therefore$ $k = \theta_o\phi(g)$. $\therefore$ $\theta_o\phi$ आच्छादक है।
$\therefore$ $\theta_o\phi$ एक तुल्याकारिता है।

E 13) मान लीजिए $a, b \in H$. तब $\exists$ $x, y \in G$ जिससे कि $a = f(x)$, $b = f(y)$.
अब, $ab = f(x) f(y) = f(xy)$.
$= f(yx)$, क्योंकि G आवेली है।
$= f(y) f(x)$
$= ba$.
$\therefore$ H आवेली है।

E 14) मान लीजिए $C^* \simeq R$ और $f : C^* \longrightarrow R$ एक तुल्याकारिता है। तब $o(f(i)) = 4$. लेकिन, 0 को छोड़कर $(\mathbf{R}, +)$ का प्रत्येक अवयव अपरिमित कोटि का है; और $o(0) = 1$. इस तरह, हमें एक अंतर्विरोध प्राप्त होता है।

$\therefore$ C^* और **R** तुल्याकारी नहीं हैं।

E 15) चूंकि **Z** अनंत है और **Z**/n**Z** परिमित है, इसलिए ये दो समूह तुल्याकारी नहीं हो सकते।

E 16) $\operatorname{Im} \exp = \{ e^r \mid r \in \mathbf{R} \} = \mathbf{R}^*$.
$\operatorname{Ker} \exp = \{ 0 \}$.
इस तरह, समाकारिता के मूल प्रमेय के अनुसार $\mathbf{R} \simeq \mathbf{R}^*$.

E 17) $U_4 = \{ 1, i, i^2, i^3 \} = \{ \pm 1, \pm i \}$.
f एक समाकारिता है, $\operatorname{Ker} f = \{ n \mid i^n = 1 \} = 4\mathbf{Z}$,
$\operatorname{Im} f = U_4$.
$\therefore$ $\mathbf{Z}/4\mathbf{Z} \simeq U_4$
इकाई 5 में हमने देखा है कि $\mathbf{Z}/4\mathbf{Z}$ और $\mathbf{Z}_4$ समान हैं।
$\therefore$ $\mathbf{Z}_4 \simeq U_4$.

E 18) $f(x + y) = e^{2\pi i(x+y)} = e^{2\pi ix}.e^{2\pi iy} = f(x)f(y)$.

$\therefore$ f एक समाकारिता है।

अब S का कोई भी अवयव $\cos\theta + i \sin\theta$

$= \cos 2\pi \dfrac{\theta}{2\pi} + i \sin 2\pi \dfrac{\theta}{2\pi} = f\left(\dfrac{\theta}{2\pi}\right)$.

के रूप का होता है। इसलिए f आच्छादक है।
साथ ही,
$\operatorname{Ker} f = \{ x \in \mathbf{R} \mid e^{2\pi ix} = 1 \}$
$= \{ x \in \mathbf{R} \mid \cos 2\pi x + i \sin 2\pi x = 1 \}$
$= \mathbf{Z}$, क्योंकि $\cos\theta + i \sin\theta = 1$ यदि और केवल यदि $\theta \in 2\pi\mathbf{Z}$.

इसलिए समाकारिता के मूल प्रमेय के अनुसार $\mathbf{R}/\mathbf{Z} \simeq S$.

E 19) क) आप जानते हैं कि $H \cap K \leq H$. अब मान लीजिए $h \in H$ और $x \in H \cap K$.
तब, $h^{-1}xh \in H$, क्योंकि $h, x \in H$.
और $h^{-1}xh \in K$, क्योंकि $x \in K$ और $K \trianglelefteq G$.
$\therefore$ $h^{-1}xh \in H \cap K$. $\therefore$ $H \cap K \trianglelefteq H$.

ख) चूंकि $K \leq G$, इसलिए $K \leq A$. और किसी भी $a \in A$ के लिए $a \in G$.
अतः, चूंकि $K \trianglelefteq G$, $a^{-1}Ka = K$. $\therefore$ $K \trianglelefteq A$.

E 20) प्रमेय 10 के अनुसार $(HK)/H \simeq K/(H \cap K)$.

$\therefore$ $\dfrac{o(HK)}{o(H)} = \dfrac{o(K)}{o(H \cap K)}$, अर्थात् $o(HK) = \dfrac{o(H)\, o(K)}{o(H \cap K)}$

E 21) मान लीजिए $H = 3\mathbf{Z}$, और $K = 4\mathbf{Z}$. प्रमेय 10 के अनुसार $(H + K)/K \simeq H/(H \cap K)$.

अब, $H + K = 3\mathbf{Z} + 4\mathbf{Z} = \mathbf{Z}$ (इकाई 3 के E 9 का और तथ्य $1 = 4 - 3$ का प्रयोग करें।)

और $H \cap K = 3Z \cap 4Z = 12Z$ (क्योंकि $x \in 3Z \cap 4Z$ यदि और केवल यदि $3 | x$ और $4 | x$.)

इस प्रकार, प्रमेय 10 के अनुसार $Z/4Z \simeq 3Z/12Z$.
आप यह भी जानते हैं कि $Z/4Z \simeq Z_4$.
$\therefore 3Z/12Z \simeq Z_4$.

E 22) G/K के किन्हीं Kx, Ky के लिए
$f((Kx)(Ky)) = f(Kxy) = Hxy = (Hx)(Hy) = f(Kx) f(Ky)$.
$\therefore$ f एक समाकारिता है।

अब G/H का कोई अवयव Hx के रूप का है। और $Hx = f(Kx) \in \text{Im } f$.
$\therefore \text{Im } f = G/H$.
अंत में,

$$\begin{aligned} \text{Ker } f &= \{ Kx \in G/K \mid f(Kx) = H \} \\ &= \{ Kx \in G/K \mid Hx = H \} \\ &= \{ Kx \in G/K \mid x \in H \} \\ &= H/K \end{aligned}$$

इसलिए प्रमेय 8 के अनुसार $(G/K)/(H/K) \simeq G/H$.

E 23) क) $f_g : GL_2(R) \to GL_2(R) : f_g\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = g\begin{bmatrix} a & b \\ c & d \end{bmatrix} g^{-1}$

अब, $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \therefore g^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

$$\therefore g\begin{bmatrix} a & b \\ c & d \end{bmatrix}g^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$$

$$\therefore f_g(GL_2(R)) = \left\{ \begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \middle| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(R) \right\}.$$

ख) $f_g : Z \to Z : f_g(x) = g + x + (-g) = x$.
$\therefore f_g = I. \quad \therefore f_g(Z) = Z$.

ग) यहाँ भी, चूंकि G आबेली है, इसलिए $f_g = I$.

E 24) पहले मान लीजिए कि G आबेली है। तब $f_g \in \text{Inn } G$ के लिए
$f_g(x) = gxg^{-1} = gg^{-1}x = x \; \forall \; x \in G$.
$\therefore f_g = I_G$.
$\therefore \text{Inn } G = \{ I_G \}$.

विलोमतः मान लीजिए कि $\text{Inn } G = \{I_G\}$.
तब किन्हीं $x, y \in G$ के लिए $f_x(y) = y$.
$\Rightarrow xyx^{-1} = y \Rightarrow xy = yx$.

अर्थात् G के किन्हीं दो अवयव x, y के लिए, $xy = yx$. अतः G आबेली है।

E 25) $g^{-1} < x > g = < x > \forall \; g \in G$ दिखाने के लिए यह दिखाना काफ़ी होगा कि
$g^{-1}xg \in < x > \forall \; g \in G$.
अब किसी $g \in G$ के लिए हमें दिया हुआ है कि
$f_{g^{-1}}(x) = x$
$\Rightarrow g^{-1}x(g^{-1})^{-1} = x$
$\Rightarrow g^{-1}xg = x$.
$\therefore g^{-1} < x > g = < x >. \quad \therefore < x > \trianglelefteq G$.

E 26) हम जानते हैं कि $S_3/Z(S_3) \simeq \text{Inn } S_3$.
लेकिन $Z(S_3) = \{ I \}$. $\therefore S_3 \simeq \text{Inn } S_3$.

इकाई 7 क्रमचय समूह

इकाई की रूपरेखा

7.1 प्रस्तावना

इस इकाई में हम उस समूह के बारे में विस्तार से चर्चा करेंगे जिसका अध्ययन आप भाग 2.5.2 में कर चुके हैं। यह सममित समूह है। जैसा कि आप पिछली इकाइयों में देख चुके हैं, सममित समूह S_n और इसके उपसमूहों से हमें अनेक उदाहरण प्राप्त हुए हैं। सममित समूहों और उनके उपसमूहों को क्रमचय समूह कहते हैं। क्रमचय समूहों और रूपांतरणों के समूहों के अध्ययन से ही समूह-सिद्धांत का आधार बना है।

इस इकाई में हम क्रमचय समूहों के बारे में पहले दी गई जानकारी को दोहराने के साथ-साथ उनके बारे में और अधिक जानकारी भी देंगे। हम क्रमचयों की संरचना पर चर्चा करेंगे और विशेष रूप से सम क्रमचयों पर विचार करेंगे। हम दिखाएंगे कि सम क्रमचयों का समुच्चय एक समूह होता है जिसे एकांतर समूह कहते हैं। अंत में हम गणितज्ञ केली द्वारा दिए गए परिणाम को सिद्ध करेंगे जिसके अनुसार प्रत्येक समूह किसी क्रमचय समूह के तुल्याकारी होता है। इसी परिणाम की वजह से क्रमचय समूहों का इतना महत्व है।

हमारी सलाह है कि आप इस इकाई को ध्यान से पढ़ें क्योंकि इससे आपको समूह-सिद्धांत के अध्ययन के लिए एक ठोस आधार प्राप्त होता है। हमारा सुझाव है कि इस इकाई की पढ़ाई शुरू करने से पहले आप भाग 2.5.2 को दोहरा लीजिए।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- S_n के किसी क्रमचय को असंयुक्त चक्रों के गुणनफल के रूप में व्यक्त कर सकेंगे;
- मालूम कर सकेंगे कि S_n का कोई अवयव विषम है अथवा सम;
- सिद्ध कर सकेंगे कि कोटि n वाला एकांतर समूह S_n में प्रसामान्य होता है और कोटि $\frac{n!}{2}$ का होता है;
- केली प्रमेय सिद्ध कर सकेंगे और इसका प्रयोग कर सकेंगे।

7.2 सममित समूह

भाग 2.5.2 से आप जानते हैं कि अरिक्त समुच्चय X पर **क्रमचय** एक X से X तक का एकैकी आच्छादक फलन है। हम X पर के सभी क्रमचयों के समुच्चय को S(X) से प्रकट करते हैं।

आइए हम भाग 2.5.2 में दिए गए कुछ तथ्यों को दोहरा लें।

मान लीजिए X, n अवयवों वाला एक परिमित समुच्चय है। सरलता के लिए हम इन अवयवों को 1, 2, ... , n, मान लेते हैं। इन n प्रतीकों पर सभी क्रमचयों के समुच्चय को S_n से प्रकट करते हैं। हम किसी $f \in S_n$ को दो रेखाओं के रूप में निम्न प्रकार से निरुपित करते हैं :

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

अब $f(1)$ के लिए n संभावनाएं हैं, अर्थात् $1, 2, \ldots, n$. एक बार $f(1)$ निर्धारित हो जाए तो $f(2)$ के लिए $(n-1)$ संभावनाएं हैं, अर्थात् $\{1, 2, \ldots, n\} \setminus \{f(1)\}$ क्योंकि f, 1-1 है। इस तरह, $f(1)$ और $f(2)$ को $n(n-1)$ तरीकों से चुना जा सकता है। इसी प्रक्रिया को जारी रखने पर हम पाते हैं कि f को परिभाषित करने के $n!$ अलग-अलग विधियाँ हैं। अतः S_n के $n!$ अवयव हैं।

आइए अब हम किसी समुच्चय X के लिए S(X) की बीजीय संरचना पर विचार करें। क्रमचयों का संयोजन S(X) पर एक द्वि-आधारी संक्रिया है। आपको क्रमचयों के संयोजन का परिकलन करने का कुछ अभ्यास हो जाए, इसके लिए एक उदाहरण लीजिए।

मान लीजिए $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ और $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$ S_4 में हैं।

तब $f_o g$ प्राप्त करने के लिए पहले हम g लागू करते हैं और फिर f लागू करते है।

$\therefore\ f_o g(1) = f(g(1)) = f(4) = 3.$

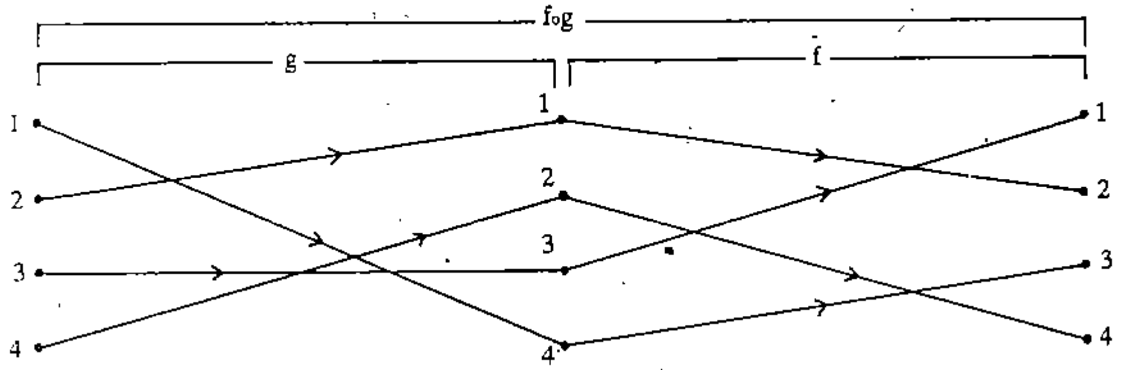
$f_o g(2) = f(g(2)) = f(1) = 2.$

$f_o g(3) = f(g(3)) = f(3) = 1.$

$f_o g(4) = f(g(4)) = f(2) = 4.$

$f_o g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

हमने इस प्रक्रिया को चित्र 1 में एक आरेख के रूप में प्रस्तुत किया है।



चित्र 1 : S_4 में (1 2 4 3) o (1 4 2)

आइए अब हम किसी भी समुच्चय X के लिए S(X) पर विचार करें। भाग 2.5.2 में हमने निम्नलिखित परिणाम सिद्ध किया है।

प्रमेय 1 : मान लीजिए X एक अरिक्त समुच्चय है। तब निकाय (S(X), o) एक समूह है जिसे X का **सममित समूह** कहते हैं।

इस तरह, S_n कोटि $n!$ वाला एक समूह है। हम S_n को **कोटि n वाला सममित समूह** कहते हैं। ध्यान दीजिए कि यदि $f \in S_n$, तो

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \ldots & f(n) \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

अब, पिछली इकाइयों से प्राप्त अनुभव के आधार पर नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 1) दिखाइये कि $n \geq 3$ के लिए, (S_n, o) एक अक्रमविनिमेय समूह है।

(संकेत : सत्यापित कीजिए कि $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ और $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ में क्रमविनिमेय नहीं होता।)

हम यहां पर शब्दावली और संकेतन के बारे में एक टिप्पणी देना चाहेंगे।

टिप्पणी : आगे से हम क्रमचयों के संयोजन को क्रमचयों का गुणन कहेंगे। और हम संयोजन का संकेतन भी प्रयोग नहीं करेंगे। अर्थात् हम **$f_o g$ के लिए केवल fg लिखेंगे।**

क्रमचयों के लिए जिस दो रेखाओं वाले संकेतन का हम अब तक प्रयोग करते रहे हैं वह कुछ बोझिल है। अगले भाग में हम आपको क्रमचयों के लिए संक्षिप्त संकेतन बताएंगे।

7.3 चक्रीय वियोजन

इस भाग में हम पहले क्रमचयों को लिखने के एक सुविधाजनक तरीके पर विचार करेंगे। इस तरीके में किसी भी क्रमचय को चक्रों के गुणनफल के रूप में लिखा जाता है। आइए पहले हम देखें कि चक्र क्या होता है।

क्रमचय $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ लीजिए। इन में से कोई एक प्रतीक, मान लीजिए 1, लीजिए।

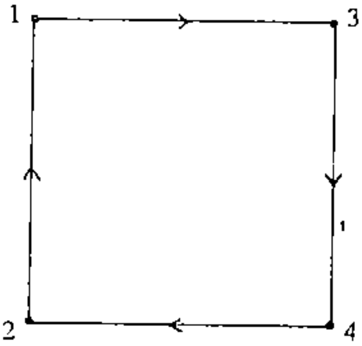
अब हम पहले एक वाम कोष्ठक लगाते हैं। और उसके बाद 1 लिखते हैं : (1

चूंकि f, 1 को 3 में प्रतिचित्रित करता है, इसलिए हम 1 के बाद 3 लिखते हैं : (1 3

चूंकि f, 3 को 4 में प्रतिचित्रित करता है, इसलिए हम 3 के बाद 4 लिखते हैं : (1 3 4

चूंकि f, 4 को 2 में प्रतिचित्रित करता है, इसलिए हम 4 के बाद 2 लिखते हैं : (1 3 4 2

चूंकि f, 2 को 1 में प्रतिचित्रित करता है, और प्रतीक 1 से हमने शुरू किया था इसलिए प्रतीक 2 के बाद हम कोष्ठक बंद कर देते हैं : (1 3 4 2)



चित्र 2 : (1 3 4 2)

इस प्रकार हम f = (1 3 4 2) लिखते हैं। इसका अर्थ यह है कि कोष्ठक में अंतिम प्रतीक को छोड़कर अन्य सभी प्रतीकों को f उनकी दायीं ओर के प्रतीक में प्रतिचित्रित करता है और अंतिम प्रतीक को पहले प्रतीक में प्रतिचित्रित करता है।

यदि हम प्रतीक 3 से शुरू करें तो हमें f = (3 4 2 1) प्राप्त होगा। यह व्यंजक (1 3 4 2) के बराबर ही है, क्योंकि दोनों ही उस क्रमचय को प्रकट करते हैं जिसे हमने चित्र 2 में दर्शाया है।

इस प्रकार के क्रमचय को **4-चक्र** या **लंबाई 4 वाला चक्र** कहते हैं। चित्र 2 को देखने से आपको इस बात का पता चल जाएगा कि हमने यह नाम क्यों दिया है।

आइए अब हम एक परिभाषा दें।

परिभाषा : क्रमचय $f \in S_n$ को **r-चक्र** (या **लंबाई r का चक्र**) कहते हैं यदि 1 और n के बीच ऐसे r अलग-अलग पूर्णांक $i_1, i_2, \ldots, i_r$ हैं जिनसे कि

$f(i_1) = i_2, f(i_2) = i_3, \ldots, f(i_{r-1}) = i_r, f(i_r) = i_1$ और $f(k) = k \; \forall \; k \notin \{i_1, i_2, \ldots, i_r\}$.

तब हम $f = (i_1 \; i_2 \ldots i_r)$. लिखते हैं।

विशेष रूप से, 2-चक्र को **पक्षांतरण** (transposition) कहते हैं।

उदाहरण के लिए, क्रमचय $f = (2 \;\; 3) \in S_3$ एक पक्षांतरण है। यहां $f(1) = 1$, $f(2) = 3$ और $f(3) = 2$.

इस भाग में आगे जाकर आप देखेंगे कि क्रमचय सिद्धांत में पक्षांतरण एक अति-महत्वपूर्ण भूमिका निभाता है।

अब, S_n में कोई 1-चक्र (i) लीजिए। यह केवल तत्समक क्रमचय $I = \begin{pmatrix} 1 & 2 & \ldots\ldots & n \\ 1 & 2 & \ldots\ldots & n \end{pmatrix}$ है, क्योंकि यह i को i में प्रतिचित्रित करता है और अन्य (n − 1) प्रतीकों को उन्हीं में प्रतिचित्रित करता है।

आइए, अब हम S_3 में चक्रों के कुछ उदाहरण लें। (1 2 3) एक 3-चक्र है जो 1 को 2 में 2 को 3 में और 3 को 1 में प्रतिचित्रित करता है। S_3 में 3 पक्षांतरण हैं, अर्थात् (1 2), (1 3) और (2 3).

नीचे दिए प्रश्न को हल करने पर आपको पता चल जाएगा कि आप चक्र का अर्थ समझ पाए हैं या नहीं।

E 2) S_5 में दो पक्षांतरण, दो 3-चक्र और एक 5-चक्र लिखिए।

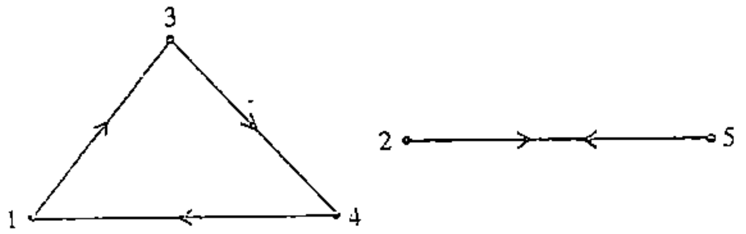
अब बताइए कि क्या हम किसी भी क्रमचय को चक्र के रूप में लिख सकते हैं? नहीं। S_5 से निम्नलिखित उदाहरण लीजिए।

क्रमचय $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$ लीजिए।

यदि हम प्रतीक 1 से शुरू करें और g पर चक्र प्राप्त करने की प्रक्रिया को लागू करें तो तीन चरणों के बाद हमें $(1\ 3\ 4)$ प्राप्त होता है। चूंकि g, 4 को 1 में प्रतिचित्रित करता है, इसलिए हम कोष्ठक बंद कर देते हैं, हालांकि अब तक हमने g में आने वाले सभी प्रतीकों को नहीं लिखा है। अब हम एक ऐसा प्रतीक लेते हैं जो अभी तक लिखा न गया हो, मान लीजिए 2.और चक्र लिखने की प्रक्रिया को फिर से शुरू करते हैं। इस तरह हमें एक अन्य चक्र $(2\ 5)$ प्राप्त होता है। अब g के सभी प्रतीक समाप्त हो गए हैं।

$\therefore\ g = (1\ 3\ 4)\ (2\ 5)$

हम g के इस व्यंजक को एक 3-चक्र और एक पक्षांतरण का **गुणनफल** कहते हैं। चित्र 3 में हमने g को एक आरेख मे निरूपित किया है जिसमें 3-चक्र और 2-चक्र स्पष्ट रूप से दिखाई पड़ते हैं।



चित्र 3 : (1 3 4) (2 5)

चूंकि प्रत्येक चक्र को हम किसी भी प्रतीक से शुरू कर सकते हैं, इसलिए g को अनेक विधियों से व्यक्त किया जा सकता है। उदाहरण के लिए,

$g = (4\ 1\ 3)\ (2\ 5) = (2\ 5)\ (1\ 3\ 4) = (5\ 2)\ (3\ 4\ 1).$

अर्थात गुणनफल में हम अलग चक्रों को किसी भी क्रम में लिख सकते हैं। और प्रत्येक चक्र में प्रारंभिक अवयव का चुनाव भी कई तरीकों से किया जा सकता है।

इस तरह, हम पाते हैं कि हम g को एक चक्र के रूप में नहीं लिख सकते हैं; यह असंयुक्त चक्रों का एक गुणनफल है।

परिभाषा : हम दो चक्रों को **असंयुक्त** कहते हैं, यदि उनमें कोई प्रतिच्छेदी प्रतीक न हो। इस तरह, असंयुक्त चक्र अवयवों के असंयुक्त समुच्चयों को गतिमान करता है। (ध्यान दीजिए कि $f \in S_n$ प्रतीक i को **गतिमान** करता है यदि $f(i) \neq i$. हम कहते हैं कि f, i को **नियत** रखता है यदि $f(i) = i$.)

उदाहरण के लिए, S_4 में चक्र $(1\ 2)$ और $(3\ 4)$ असंयुक्त हैं। लेकिन $(1\ 2)$ और $(1\ 4)$ असंयुक्त नहीं हैं, क्योंकि दोनों 1 को गतिमान करते हैं।

ध्यान दीजिए कि यदि f और g **असंयुक्त** हैं, तो $fg = gf$, क्योंकि f और g प्रतीकों के असंयुक्त समुच्चयों को गतिमान करते हैं।

आइए अब हम एक और उदाहरण को देखें।

मान लीजिए h, S_5 का क्रमचय

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$ है।

असंयुक्त चक्रों के गुणनफल में लिखने की प्रक्रिया को लागू करने पर हमें

$h = (1\ 4\ 5)\ (2)\ (3)$

प्राप्त होता है, क्योंकि h दोनों प्रतीकों 2 और 3 को नियत रखता है। प्रथानुसार हम h के व्यंजक में 1-चक्र (2) और (3) को तब तक शामिल नहीं करते जब तक कि इन पर विशेष ध्यान न देना हो, क्योंकि ये केवल तत्समक क्रमचय को ही निरूपित करते हैं। इस प्रकार, हम केवल $h = (1\ 4\ 5)$ लिखते हैं।

यदि आपने अभी तक की गई चर्चा को समझ लिया है, तो आप नीचे दिए गए प्रश्नों को हल कर सकेंगे।

E 3) नीचे दिए गए प्रत्येक क्रमचय को ऊपर बतायी गई विधि से असंयुक्त चक्रों के गुणनफल के रूप में व्यक्त कीजिए।

क) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$

ख) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 7 & 2 & 1 & 3 & 6 & 5 \end{pmatrix}$

ग) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$

E 4) क्या चक्रों (1 3) और (1 5 6) में क्रम-विनिमय होता है? क्यों?

जो आपने E 3 में देखा है वह व्यापक रूप में सत्य होता है। निम्नलिखित परिणाम को देखिए।

प्रमेय 2 : प्रत्येक क्रमचय $f \in S_n$, $f \neq I$, को असंयुक्त चक्रों के गुणनफल के रूप में व्यक्त किया जा सकता है।

इस कथन की उपपत्ति काफ़ी बोझिल है। प्रक्रिया वही है जिसे आपने E 3 में लागू किया है। अत: उपपत्ति हम यहां नहीं देंगे।

अब हम कुछ प्रश्न दे रहे हैं जिनमें हमने क्रमचयों के कुछ रोचक गुणों का उल्लेख किया है।

E 5) दिखाइए कि S_n में प्रत्येक क्रमचय एक चक्र होता है यदि और केवल यदि $n < 4$.

E 6) यदि $f = (i_1\ i_2 \ldots i_r) \in S_n$, तो दिखाइए कि
$f^{-1} = (i_r\ i_{r-1} \ldots i_2\ i_1)$.

E 7) यदि f एक r-चक्र है तो दिखाइए कि $o(f) = r$, अर्थात् $f^r = I$ और $f^s \neq I$, यदि $s < r$.
(संकेत : यदि $f = (i_1\ i_2 \ldots i_r)$, तो $f(i_1) = i_2$, $f^2(i_1) = i_3, \ldots, f^{r-1}(i_1) = i_r$)

आइए अब हम देखें कि हम किसी चक्र को पक्षांतरणों के गुणनफल के रूप में कैसे लिख सकते हैं। S_5 में चक्र (1 5 3 4 2) लीजिए। आप सत्यापित कर सकते हैं कि यह गुणनफल (1 2) (1 4) (1 3) (1 5) के बराबर है। ध्यान दीजिए कि ये पक्षांतरण असंयुक्त नहीं हैं। इनमें से सभी पक्षांतरण अवयव 1 को गतिमान करते हैं।

$(i_1\ i_2 \ldots i_r) = (i_1\ i_r)\ (i_1\ i_{r-1}) \ldots (i_1\ i_2)$

जिस प्रक्रिया को अभी हमने लागू किया है, वह किसी भी चक्र पर लागू की जा सकती है। अर्थात् किसी भी r-चक्र $(i_1\ i_2 \ldots i_r)$ को पक्षांतरणों के गुणनफल $(i_1\ i_r)\ (i_1\ i_{r-1}) \ldots (i_1\ i_2)$, के रूप में लिखा जा सकता है। ध्यान दीजिए कि चूंकि पक्षांतरण असंयुक्त नहीं है, इसलिए इनमें क्रम-विनिमय होना आवश्यक नहीं।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 8) निम्नलिखित चक्रों को पक्षांतरणों के गुणनफल के रूप में व्यक्त कीजिए:
क) (1 3 5), ख) (5 3 1), ग) (2 4 5 3).

अब हम प्रमेय 2 की सहायता से एक परिणाम देंगे जिससे यह पता चलता है कि क्रमचय सिद्धांत में पक्षांतरणों का इतना महत्व क्यों है।

प्रमेय 3 : S_n $(n \geq 2)$ में प्रत्येक क्रमचय को पक्षांतरणों के गुणनफल के रूप में लिखा जा सकता है।

उपपत्ति : उपपत्ति काफ़ी सरल है। प्रमेय 2 के अनुसार, I के अतिरिक्त प्रत्येक क्रमचय असंयुक्त चक्रों का गुणनफल होता है। और अभी-अभी आपने देखा है कि प्रत्येक चक्र पक्षांतरणों का गुणनफल होता है। अतः I के अतिरिक्त प्रत्येक क्रमचय पक्षांतरणों का गुणनफल होता है। साथ ही, $I = (1\ 2)(1\ 2)$. इस प्रकार, I भी पक्षांतरणों का गुणनफल है। इस तरह प्रमेय सिद्ध हो जाता है।

आइए देखें कि प्रमेय 3 का प्रयोग कैसे करते हैं। E 3 (क) का क्रमचय $(1\ 5\ 3\ 2\ 4)$ है। यह $(1\ 4)(1\ 2)(1\ 3)(1\ 5)$ के बराबर है।

इसी प्रकार क्रमचय $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 2 & 5 \end{pmatrix}$

$= (1\ 3\ 4)(2\ 6\ 5) = (1\ 4)(1\ 3)(2\ 5)(2\ 6)$.

अब आप प्रक्रिया को लागू करने की कोशिश कर सकते हैं।

E 9) E 3(ख) के क्रमचय को पक्षांतरणों के गुणनफल के रूप में लिखिए।

E 10) दिखाइए कि $(1\ 2 \ldots 10) = (1\ 2)(2\ 3) \ldots (9\ 10)$.

प्रमेय 3 में दिए गए वियोजन से संबंधित हमें S_n का एक उपसमूह प्राप्त होता है। अब हम इस पर विचार करेंगे।

7.4 एकांतर समूह

आपने देखा है कि S_n के किसी क्रमचय को पक्षांतरणों के गुणनफल के रूप में लिखा जा सकता है। E 10 से आप यह भी देख सकते हैं कि गुणनफल के गुणनखंड अद्वितीयतः निर्धारित नहीं होते। परंतु सभी निरूपणों में एक बात देखने को मिलती है—यदि ऐसे एक निरूपण में S_n का क्रमचय पक्षांतरणों का विषम संख्या में गुणनफल हो, तो यह इस प्रकार के किसी भी निरूपण में पक्षांतरणों का विषम संख्या में गुणनफल होगा। इसी प्रकार, यदि एक निरूपण में $f \in S_n$ पक्षांतरणों का सम संख्या में गुणनफल हो, तो इस प्रकार के किसी भी निरूपण में f पक्षांतरणों का सम संख्या में गुणनफल होगा। इस तथ्य को सिद्ध करने के लिए हमें चिह्नक या चिह्न फलन की संकल्पना की ज़रूरत है।

परिभाषा : $f \in S_n$ $(n \geq 2)$ का चिह्नक (signature)

$$\text{sign } f = \prod_{i<j} \frac{f(j) - f(i)}{j - i}$$

से परिभाषित है।

$\prod_{i=1}^{n} \alpha_i = \alpha_1 \alpha_2 \ldots \alpha_n.$

उदाहरण के लिए, $f = (1\ 2\ 3) \in S_3$ के लिए

$$\text{sign } f = \frac{f(2) - f(1)}{2 - 1} \cdot \frac{f(3) - f(1)}{3 - 1} \cdot \frac{f(3) - f(2)}{3 - 2}$$

$$= \left(\frac{3-2}{1}\right)\left(\frac{1-2}{2}\right)\left(\frac{1-3}{1}\right) = 1$$

इसी प्रकार, यदि $f = (1\ 2) \in S_3$, तो

$$\text{sign } f = \frac{f(2) - f(1)}{2 - 1} \cdot \frac{f(3) - f(1)}{3 - 1} \cdot \frac{f(3) - f(2)}{3 - 2}$$

$$= \left(\frac{1-2}{1}\right)\left(\frac{3-2}{2}\right)\left(\frac{3-1}{1}\right) = -1.$$

आगे से जब भी हम sign f के बारे में बात करेंगे, हम यह मान कर चलेंगे कि $f \in S_n$, जहां $n \geq 2$.

अब आप नीचे दिए गए सरल प्रश्न को हल करने का प्रयास कीजिए।

E 11) $I \in S_n$ का चिह्नक क्या है?

क्या आपने इस बात की ओर ध्यान दिया है कि चिह्नक एक फलन sign : $S_n \to \mathbf{Z}$ को परिभाषित करता है? अब हम दिखाएंगे कि यह फलन एक समाकारिता है।

प्रमेय 4 : मान लीजिए $f, g \in S_n$, तब

$\text{sign}(f \circ g) = (\text{sign } f)(\text{sign } g)$.

उपपत्ति : परिभाषा के अनुसार

$$\text{sign}(f \circ g) = \prod_{\substack{i,j=1 \\ i<j}}^{n} \frac{f(g(j)) - f(g(i))}{j - i}$$

$$= \prod_{i,j} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} \quad \prod_{i,j} \frac{g(j) - g(i)}{j - i}.$$

अब जैसे-जैसे i और j, 1 से n तक के सभी संभव अलग-अलग मानों के युग्म लेते हैं, वैसे-वैसे g(i) और g(j) भी सभी अलग-अलग मानों के युग्म लेंगे, क्योंकि g एकैकी आच्छादक है।

$\therefore \prod_{i<j} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} = \text{sign } f.$

$\therefore \text{sign}(f \circ g) = (\text{sign } f)(\text{sign } g)$.

अब हम दिखाएंगे कि $\text{Im (sign)} = \{1, -1\}$.

प्रमेय 5 : क) यदि $t \in S_n$ एक पक्षांतरण है, तो $\text{sign } t = -1$.

ख) $\text{sign } f = 1$ या $-1 \ \forall f \in S_n$

ग) $\text{Im (sign)} = \{1, -1\}$.

उपपत्ति : क) मान लीजिए $t = (p\ q)$, जहां $p < q$. अब sign t के केवल एक गुणनखंड में p और q दोनों होते हैं, अर्थात्

$$\frac{t(q) - t(p)}{q - p} = \frac{p - q}{q - p} = -1.$$

sign t का प्रत्येक गुणनखंड, जिसमें p या q नहीं आता, 1 के बराबर होता है, क्योंकि

$$\frac{t(i) - t(j)}{i - j} = \frac{i - j}{i - j} = 1, \text{ यदि } i, j \neq p, q.$$

शेष गुणनखंडों में या तो p होता है या q होता है, पर दोनों नहीं होते। इनके जोड़ों को लेकर हमें निम्नलिखित गुणनफलों में से एक गुणनफल प्राप्त होता है :

$$\frac{t(i) - t(p)}{i - p} \frac{t(i) - t(q)}{i - q} = \frac{i - q}{i - p} \frac{i - p}{i - q} = 1, \text{ यदि } i > q,$$

$$\frac{t(i) - t(p)}{i - p} \frac{t(q) - t(i)}{q - i} = \frac{i - q}{i - p} \frac{p - i}{q - i} = 1, \text{ यदि } q > i > p,$$

$$\frac{t(p) - t(i)}{p - i} \frac{t(q) - t(i)}{q - i} = \frac{q - i}{p - i} \frac{p - i}{q - i} = 1, \text{ यदि } i < p.$$

sign t के सभी गुणनखंडों के मान लेकर हम देखते हैं कि $\text{sign } t = -1$.

ख) मान लीजिए $f \in S_n$. प्रमेय 3 से हम जानते हैं कि

$f = t_1 t_2 \ldots t_r$, S_n के किन्हीं पक्षांतरणों $t_1, t_2, \ldots, t_r$ के लिए

$\therefore \text{sign } f = \text{sign}(t_1 t_2 \ldots t_r)$

$= (\text{sign } t_1)(\text{sign } t_2) \ldots (\text{sign } t_r)$, प्रमेय 4 से।

$= (-1)^r$, ऊपर दिए गए (क) से।

$\therefore \text{sign } f = 1$ या -1.

ग) हम जानते हैं कि $\text{Im (sign)} \subseteq \{1, -1\}$.

हम यह भी जानते हैं कि किसी पक्षांतरण t के लिए

sign $t = -1$, और sign $I = 1$.
$\therefore \{1, -1\} \subseteq \text{Im (sign)}$.
$\therefore \text{Im (sign)} = \{1, -1\}$.

अब हम इस भाग के प्रारंभ में दिए गए कथन को सिद्ध करने की स्थिति में हैं।

प्रमेय 6 : मान लीजिए $f \in S_n$ और मान लीजिए कि
$f = t_1 t_2 \ldots . t_r = t_1' t_2' \ldots . t_s'$
पक्षांतरणों के गुणनफल के रूप में f के दो गुणनखंड हैं। तब दोनों r और s सम पूर्णांक होते हैं या दोनों विषम पूर्णांक होते हैं।

उपपत्ति : हम फलन sign : $S_n \to \{1, -1\}$ को $f = t_1 t_2 \ldots . t_r$ पर लागू करते हैं। प्रमेय 5 से हम जानते हैं कि
sign $f = (\text{sign } t_1)(\text{sign } t_2) \ldots (\text{sign } t_r) = (-1)^r$.
sign $(t_1' t_2' \ldots t_s') = (-1)^s$, f के लिए $t_1' t_2' \ldots t_s'$ प्रतिस्थापित करने पर।
अर्थात् $(-1)^s = (-1)^r$.
यह तभी संभव है जबकि s और r दोनों ही या तो सम हो या विषम।

इस तरह, हमने दिखाया है कि $f \in S_n$ के लिए, f के पक्षांतरणों के किसी गुणनखंड में आने वाले गुणनखंडों की संख्या सदा ही सम है या सदा ही विषम है। अतः नीचे दी गई परिभाषा भी अर्थपूर्ण है।

परिभाषा : क्रमचय $f \in S_n$ को **सम** (even) कहते हैं यदि इसे सम संख्या में पक्षांतरणों के गुणनफल के रूप में लिखा जा सकता है। f को **विषम** (odd) कहते हैं, यदि इसे विषम संख्या में पक्षांतरणों के गुणनफल के रूप में लिखा जा सकता है।

sign $f = 1$ यदि और केवल यदि f सम हो।

उदाहरण के लिए, $(1\ 2) \in S_3$ एक विषम क्रमचय है। वास्तव में, कोई भी पक्षांतरण विषम क्रमचय होता है। इसके विपरीत कोई भी 3-चक्र एक सम क्रमचय होता है, क्योंकि
$(i\ j\ k) = (i\ k)(i\ j)$

अब आप देखिए कि आप सम क्रमचय और विषम क्रमचय का मतलब समझ गए हैं कि नहीं।

E 12) E 8 और E 9 में कौन से क्रमचय विषम हैं?

E 13) यदि $f, g \in S_n$ विषम हैं, तो क्या $f \circ g$ भी विषम होगा?

E 14) तत्समक क्रमचय विषम है या सम?

अब हम S_n के एक महत्वपूर्ण उपसमुच्चय को परिभाषित करेंगे। यह है
$A_n = \{f \in S_n \mid f \text{ सम है}\}$.

हम दिखाएंगे कि $A_n \trianglelefteq S_n$, और $n \geq 2$ के लिए $o(A_n) = \frac{n!}{2}$.

प्रमेय 7 : S_n के सम क्रमचयों का समुच्चय कोटि $\frac{n!}{2}$ वाला S_n का एक प्रसामान्य उपसमूह है।
उपपत्ति : चिह्नक फलन
sign : $S_n \to \{1, -1\}$
लीजिए। ध्यान दीजिए कि $\{1, -1\}$ गुणन के प्रति एक समूह है। अब प्रमेय 4 के अनुसार sign एक समूह समाकारिता है और प्रमेय 5 के अनुसार Im (sign) $= \{1, -1\}$. आइए अब हम Ker (sign) प्राप्त करें।

$$\text{Ker (sign)} = \{f \in S_n \mid \text{sign } f = 1\}$$
$$= \{f \in S_n \mid f \text{ सम है}\}$$
$$= A_n.$$

$\therefore A_n \trianglelefteq S_n$.

अब समाकारिता के मूल प्रमेय के अनुसार
$S_n/A_n \simeq \{1, -1\}$.

$\therefore o(S_n/A_n) = 2$, अर्थात्, $\frac{o(S_n)}{o(A_n)} = 2$.

$\therefore o(A_n) = \frac{o(S_n)}{2} = \frac{n!}{2}$.

ध्यान दीजिए कि इस प्रमेय के कथनानुसार S_n के सम क्रमचयों की संख्या S_n के विषम क्रमचयों की संख्या के बराबर होती है।

प्रमेय 7 से हमें निम्नलिखित परिभाषा प्राप्त होती है।

परिभाषा : S_n के सम क्रमचयों के समूह A_n को **कोटि n का एकांतर समूह** (alternating group of degree n) कहते हैं।

आइए अब हम एक उदाहरण पर विचार करें जिसे आप पिछली इकाइयों में देख चुके हैं, अर्थात् A_3. अब, प्रमेय 7 के अनुसार

$o(A_3) = \frac{3!}{2} = 3$.

चूंकि $(1\ 2\ 3) = (1\ 3)(1\ 2)$, इसलिए $(1\ 2\ 3) \in A_3$.
इसी प्रकार $(1\ 3\ 2) \in A_3$ और $I \in A_3$ तो है ही।
$\therefore A_3 = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$.

ऊपर के उदाहरण में हमने निम्नलिखित तथ्य का प्रयोग किया है :
r-चक्र विषम होता है यदि r सम हो और सम होता है यदि r विषम हो।
ऐसा इसलिए है क्योंकि r-चक्र

$(i_1\ i_2 \ldots i_r) = (i_1\ i_r)(i_1\ i_{r-1}) \ldots (i_1\ i_2)$,

$(r-1)$ पक्षांतरणों का गुणनफल। इस तथ्य की सहायता से आप नीचे दिए गए प्रश्न को हल कीजिए।

E 15) A_4 के सभी अवयव लिखिए।

अब थोड़ी देर के लिए आइए हम इकाई 4 में दिए गए लग्रांज प्रमेय को फिर से देखें। इस प्रमेय के अनुसार परिमित समूह के उपसमूह की कोटि समूह की कोटि को विभाजित करता है। वहां हमने यह भी कहा था कि यदि $n \mid o(G)$ तो यह आवश्यक नहीं है कि G का कोटि n वाला कोई उपसमूह हो। अब, क्योंकि आप A_4 से परिचित हो चुके हैं, इसलिए हम इस कथन को उदाहरण द्वारा स्पष्ट कर सकते हैं।

हम दिखाएंगे कि A_4 का कोटि 6 वाला कोई उपसमूह नहीं है, हालांकि $6 \mid o(A_4)$. मान लीजिए A_4 का ऐसा एक उपसमूह H है। तब $o(H) = 6$, $o(A_4) = 12$.
$\therefore |A_4 : H| = 2$. $\therefore H \trianglelefteq A_4$ (इकाई 5 का प्रमेय 3 देखिए)।
अब, क्योंकि A_4/H कोटि 2 वाला एक समूह है, इसलिए इकाई 4 के E 8 के अनुसार
$(Hg)^2 = H \ \forall\ g \in A_4$.
(याद रखिए कि H, A_4/H का तत्समक है।)
$\therefore g^2 \in H \ \forall\ g \in A_4$.
अब, $(1\ 2\ 3) \in A_4$. $\therefore (1\ 2\ 3)^2 = (1\ 3\ 2) \in H$.
इसी प्रकार, $(1\ 3\ 2)^2 = (1\ 2\ 3) \in H$.
इसी तर्क के अनुसार हम कह सकते हैं कि $(1\ 4\ 2), (1\ 2\ 4), (1\ 4\ 3), (1\ 3\ 4), (2\ 3\ 4), (2\ 4\ 3)$ भी H के अलग-अलग अवयव हैं, और $I \in H$. तो हैं ही।

इस तरह हम पाते हैं कि H में कम से कम 9 अवयव हैं।
$\therefore o(H) \geq 9$. यह हमारी इस बात का अंतर्विरोध करता है कि $o(H) = 6$. अतः A_4 का कोटि 6 वाला कोई उपसमूह नहीं है।

हम A_4 का प्रयोग एक और उदाहरण के लिए भी करेंगे। (देखा A_4 कितना उपयोगी है!) इकाई 5 में हमने कहा था कि यदि $H \trianglelefteq N$ और $N \trianglelefteq G$ तो यह आवश्यक नहीं है कि G में H का प्रसामान्य हो। तो लीजिए, एक उदाहरण।

A_4 का, उप समुच्चय $V_4 = \{I, (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\}$ लीजिए।

E 16) सत्यापित कीजिए कि $(V_4, \circ)$, A_4 का प्रसामान्य उपसमूह है।.

अब मान लीजिए $H = \{I, (1\ 2)(3\ 4)\}$. तब H, V_4 में सूचकांक 2 वाला एक उपसमूह है।
$\therefore H \trianglelefteq V_4$.
इसलिए $H \trianglelefteq V_4$, $V_4 \trianglelefteq A_4$. लेकिन $H \ntrianglelefteq A_4$ क्यों? क्योंकि $(1\ 2\ 3) \in A_4$ ऐसा है कि
$(1\ 2\ 3)^{-1}(1\ 2)(3\ 4)(1\ 2\ 3) = (1\ 3)(2\ 4) \notin H$.

और आइए अब हम देखें कि समूह सिद्धांतों में क्रमचय समूह का इतना महत्व क्यों है।

7.5 केली प्रमेय

गणित में पहले प्रकट होने वाले अधिकांश परिमित समूह क्रमचय समूह थे। अंग्रेज़ गणितज्ञ केली ने ही पहले इस बात का अनुभव किया था कि प्रत्येक समूह की बीजीय संरचना किसी समुच्चय X के लिए S(X) के किसी उपसमूह की बीजीय संरचना के समान है। इस भाग में हम केली के परिणाम और उसके कुछ अनुप्रयोगों ~~का वर्णन~~ करेंगे।

प्रमेय 8 (केली) : कोई भी समूह G सममित समूह S(G) के किसी उपसमूह के तुल्याकारी होता है।

उपपत्ति : $a \in G$ के लिए हम निम्नलिखित वाम गुणन फलन परिभाषित करते हैं :

$f_a : G \to G : f_a(x) = ax$.
f_a, 1-1, है, क्योंकि
$f_a(x) = f_a(y) \implies ax = ay \implies x = y \;\forall\, x, y \in G$.
f_a आच्छादक है, क्योंकि कोई भी $x \in G$, $f_a(a^{-1}x)$ के बराबर है।
$\therefore f_a \in S(G) \;\forall\, a \in G$.
अब हम फलन $f : G \to S(G)$:
$f(a) = f_a$ परिभाषित करते हैं।

ध्यान दीजिए कि S(G) समुच्चय G पर सममित समूह है।

हम दिखाएंगे कि f एक एकैकी समाकारिता है। इसके लिए ध्यान दीजिए कि
$(f_a \circ f_b)(x) = f_a(bx) = abx = f_{ab}(x) \;\forall\, a, b \in G$
$\therefore f(ab) = f_{ab} = f_a \circ f_b = f(a) \circ f(b) \;\forall\, a, b \in G$.
अर्थात् f एक समाकारिता है।

अब, $\operatorname{Ker} f = \{a \in G \mid f_a = I_G\}$
$= \{a \in G \mid f_a(x) = x \;\forall\, x \in G\}$
$= \{a \in G \mid ax = x \;\forall\, x \in G\}$
$= \{e\}$.

इस प्रकार, समाकारिता के मूल प्रमेय के अनुसार
$G/\operatorname{Ker} f \simeq \operatorname{Im} f \leq S(G)$.
अर्थात् G, S(G) के किसी उपसमूह के तुल्याकारी है।

केली प्रमेय के एक उदाहरण के रूप में हम दिखाएंगे कि क्लाइन 4-समूह K_4 (इकाई 3 का उदाहरण 7 देखिए) S_4 के उपसमूह V_4 के तुल्याकारी है। K_4 की गुणन सारणी है

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

E 17) सत्यापित कीजिए कि $f_e = I$, $f_a = (e\ a)(b\ c)$, $f_b = (e\ b)(a\ c)$, $f_c = (e\ c)(a\ b)$.

E 17 हल करने पर आप देख सकते हैं कि

$K_4 \simeq \{I, (c\ a)(b\ c), (c\ b)(a\ c), (c\ c)(a\ b)\}$.

अब, प्रतीकों c, a, b, c के स्थान पर 1, 2, 3, 4 प्रतिस्थापित करने पर हमें V_4 प्राप्त हो जाता है।

$\therefore K_4 \simeq V_4$.

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 18) S_4 का वह उपसमूह प्राप्त कीजिए जो Z_4 के तुल्याकारी है। क्या $Z_4 \simeq A_4$?

तो आइए देखें कि इस इकाई में हमने क्या किया है।

7.6 सारांश

इस इकाई में हमने निम्नलिखित बातों पर चर्चा की है।

1. किसी समुच्चय X के लिए सममित समूह S(X), और विशेष रूप से समूह S_n.
2. चक्रों और पक्षांतरणों की परिभाषाएं और कुछ गुण।
3. S_n में तत्समक के अलावा प्रत्येक क्रमचय को चक्रों के असंयुक्त गुणनफल के रूप में लिखा जा सकता है।
4. S_n (जहां $n \geq 2$) में किसी भी क्रमचय को पक्षांतरणों के गुणनफल के रूप में लिखा जा सकता है।
5. समाकारिता $\text{sign}: S_n \to \{1, -1\}$, जहां $n \geq 2$.
6. विषम और सम क्रमचय।
7. S_n (जहां $n \geq 2$) में सम क्रमचयों का समुच्चय A_n कोटि $\frac{n!}{2}$ वाला S_n का एक प्रसामान्य उपसमूह है।
8. कोई भी समूह किसी क्रमचय समूह के तुल्याकारी होता है।

7.7 हल/उत्तर

E 1) क्योंकि $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ और

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

इसलिए ये दो क्रमचय क्रमविनिमेय नहीं करते।

$\therefore S_3$ अन्-आबेली है।

इकाई 6 में (उदाहरण 4 के बाद) हमने दिखाया है कि कैसे

$S_3 \leq S_n \ \forall\ n \geq 3$.

अतः सभी $n \geq 3$ के लिए S_n अन्-आबेली होगा।

E 2) इसके अनेक उत्तर हो सकते हैं। हमारा उत्तर है

(1 2), (2 4), (1 3 5), (1 2 3), (2 5 1 4 3).

E 3) क) (1 5 3 2 4)

ख) (1 8 5) (2 4) (3 7 6)

ग) (1 4) (2 5)

E 4) नहीं, क्योंकि

$$(1\ 3)(1\ 5\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} = (1\ 5\ 4\ 3), \text{ और}$$

$$(1\ 5\ 4)(1\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} = (1\ 3\ 5\ 4).$$

E 5) आप जानते हैं कि S_1, S_2 और S_3 के सभी अवयव चक्र हैं। इसलिए यदि $n < 4$, तो S_n में प्रत्येक क्रमचय चक्रीय होता है।
विलोमतः, हम दिखाएंगे कि यदि $n \geq 4$, तो S_n में एक ऐसा क्रमचय होता है जो चक्र नहीं है। अवयव (1 2) (3 4) लीजिए। सभी $n \geq 4$ के लिए यह S_n का एक अवयव है, पर यह चक्र नहीं है।

E 6) $(i_1\ i_2 \ldots i_r)(i_r\ i_{r-1} \ldots i_2\ i_1) = I$
$= (i_r\ i_{r-1} \ldots i_2\ i_1)(i_1\ i_2 \ldots i_r)$,
$\therefore (i_1\ i_2 \ldots i_r)^{-1} = (i_r\ i_{r-1} \ldots i_2\ i_1)$.

E 7) मान लीजिए $f = (i_1\ i_2 \ldots i_r)$.
तब $f(i_1) = i_2, f(i_2) = i_3, \ldots, f(i_{r-1}) = i_r, f(i_r) = i_1$.
$\therefore f^2(i_1) = f(i_2) = i_3, f^3(i_1) = f(i_3) = i_4, \ldots, f^r(i_1) = f(i_r) = i_1$.
इसी प्रकार $f^r(i_k) = i_k \forall k = 2, \ldots, r$.
$\therefore f^r = I$.
और $s < r$ के लिए $f^s(i_1) = i_{s+1} \neq i_1$. $\therefore f^s \neq I$.
$\therefore o(f) = r$.

E 8) क) (1 5) (1 3)
ख) (5 1) (5 3)
ग) (2 3) (2 5) (2 4)

E 9) (1 5) (1 8) (2 4) (3 6) (3 7)

E 10) किन्हीं तीन प्रतीकों i, j और k के लिए
$(i\ j)(j\ k) = (i\ j\ k)$.
तब यदि m एक अन्य प्रतीक हो, तो
$(i\ j\ k)(k\ m) = (i\ j\ k\ m)$, आदि-आदि।
$\therefore (1\ 2)(2\ 3) \ldots (9\ 10)$
$= (1\ 2\ 3)(3\ 4) \ldots (9\ 10)$
$= (1\ 2\ 3\ 4) \ldots (9\ 10)$
$= (1\ 2\ 3 \ldots 10)$

E 11) $\text{sign } I = \prod_{\substack{i,j=1 \\ i<j}}^{n} \frac{I(j) - I(i)}{j - i} = \prod_{\substack{i,j=1 \\ i<j}}^{n} \frac{j - i}{j - i} = 1.$

E 12) E 8(ग) और E 9 के क्रमचय विषम हैं।

E 13) $\text{sign}(f) = \text{sign}(g) = -1$.
$\therefore \text{sign}(f \circ g) = (-1)(-1) = 1$
$\therefore f \circ g$ सम है।

E 14) $\text{sign } I = 1$. $\therefore I$ सम है।

E 15) हम जानते हैं कि $o(A_4) = \frac{4!}{2} = 12$. तब $I \in A_4$. साथ ही, सभी 3-चक्र A_4 में होंगे। वे हैं:

(1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3).
और फिर दो पक्षांतरणों के सभी संभव असंयुक्त गुणनफल भी हैं :
वे हैं : (1 2) (3 4), (1 3) (4 2), (1 4) (2 3).
इस प्रकार हमें A_4 के सभी 12 अवयव प्राप्त हो गए हैं।

E 16) गुणा करके आप देख सकते हैं कि V_4, $\circ$ के सापेक्ष संवृत है और V_4 का प्रत्येक अवयव स्वयं अपना प्रतिलोम होता है।

$\therefore V_4 \leq A_4$.
और गुणा करके ही आप देख सकते हैं कि
$f^{-1}gf \in V_4 \; \forall f \in A_4$ और $g \in V_4$.
$\therefore V_4 \trianglelefteq A_4$.

E 17) $f_e(x) = ex = x \; \forall x \in K_4$. $\therefore f_e = I$
अब $f_a(e) = a, f_a(a) = e, f_a(b) = c, f_a(c) = b$.
$\therefore f_a = (e\ a)\ (b\ c)$.
इसी प्रकार, $f_b = (e\ b)\ (a\ c)$ और $f_c = (e\ c)\ (a\ b)$.

E 18) हम जानते हैं कि $Z_4 = < \bar{1} >$ और $o(\bar{1}) = 4$. इसलिए S_4 का जो उपसमूह Z_4 के तुल्याकारी है, कोटि 4 वाला चक्रीय समूह होगा।
यह क्रमचय $f_{\bar{1}}$ से जनित होगा।
अब $f_{\bar{1}}(x) = \bar{1} + x \; \forall x \in Z_4$.
$\therefore f_{\bar{1}} = (\bar{1}\ \bar{2}\ \bar{3}\ \bar{4})$, जो $(1\ 2\ 3\ 4)$ के बराबर है।
$\therefore Z_4 \simeq <(1\ 2\ 3\ 4)>$, जोकि निश्चित ही A_4 के तुल्याकारी नहीं है।

इकाई 8 परिमित समूह

इकाई की रूपरेखा

8.1 प्रस्तावना

अब तक आप विभिन्न परिमित और अपरिमित समूहों तथा उनके उपसमूहों से परिचित हो चुके हैं। इस इकाई में हम कुछ परिमित समूहों पर विशेष ध्यान देंगे और उनकी संरचनाओं पर चर्चा करेंगे। उदाहरण के लिए, आप देखेंगे कि कोटि 6 वाला कोई समूह या तो चक्रीय होता है या S_3 के तुल्याकारी होता है।

परिमित समूह की संरचना को समझने के लिए हमें समूहों के अनुलोम गुणनफल की थोड़ी जानकारी की आवश्यकता है। भाग 8.2 में हम बाह्य और आंतरिक अनुलोम गुणनफलों के बारे में चर्चा करेंगे।

भाग 8.3 में हम सुप्रसिद्ध गणितज्ञ सीलो (1832-1918) द्वारा प्राप्त किए गए कुछ परिणामों के अनुप्रयोगों पर चर्चा करेंगे। इन प्रमेयों और कौशी के एक प्रमेय की सहायता से हम कुछ परिमित समूहों के विभिन्न उपसमूह प्राप्त कर सकते हैं।

अंत में, अर्थात् भाग 8.4 में हम भाग 8.2 और भाग 8.3 से प्राप्त जानकारी का प्रयोग अनेक परिमित समूहों की संरचनाओं को ज्ञात करने में करेंगे। विशेष रूप से हम कोटि 10 से कम या उसके बराबर की कोटि वाले समूहों पर चर्चा करेंगे।

इस इकाई के साथ हम समूह-सिद्धांत पर अपनी चर्चा समाप्त करते हैं। अगले खंड में आप वलय-सिद्धांत के बारे में अध्ययन शुरू करेंगे। आपने पहले दो खंडों में जो कुछ भी पढ़ा है उसका प्रयोग आप करते रहेंगे क्योंकि, जैसा कि आप देखेंगे, प्रत्येक वलय एक समूह भी होता है।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- परिमित संख्या में समूहों का अनुलोम गुणनफल प्राप्त कर सकेंगे;
- जांच कर सकेंगे कि कोई समूह अपने उपसमूहों का अनुलोम गुणनफल है अथवा नहीं;
- परिमित समूहों की संरचनाओं और संभव उपसमूहों को प्राप्त करने के लिए सीलो प्रमेयों का प्रयोग कर सकेंगे;
- कोटि p, p^2 या pq वाले समूहों का वर्गीकरण कर सकेंगे, जहां p और q ऐसी अभाज्य संख्याएं हैं कि $p > q$ और $q \nmid p-1$.

8.2 समूहों का अनुलोम गुणनफल

इस भाग में हम दिए हुए समूहों का प्रयोग करके नए समूह प्राप्त करने की एक अति महत्वपूर्ण विधि पर चर्चा करेंगे। पहले हम देखेंगे कि किस प्रकार से दो समूहों का संयोजन करके हम एक दूसरा समूह प्राप्त कर सकते हैं। इसके बाद हम देखेंगे कि किस प्रकार से एक समूह के दो उपसमूहों के संयोजन से हम एक अन्य उपसमूह प्राप्त कर सकते हैं।

8.2.1 बाह्य अनुलोम गुणनफल

इस उपभाग में हम दिए हुए दो या अधिक समूहों से एक नया समूह प्राप्त करेंगे।

मान लीजिए $(G_1, *_1)$ और $(G_2, *_2)$ दो समूह हैं। इनका कार्तीय गुणनफल (देखिए भाग 1.3) $G = G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}$ लीजिए। क्या हम G_1 और G_2 पर परिभाषित संक्रियाओं की सहायता से G पर एक द्वि-आधारी संक्रिया परिभाषित कर सकते हैं? इसके लिए एक विधि स्पष्ट है, अर्थात् संगत घटकों को गुणा करने की विधि। अर्थात् हम G पर संक्रिया $*$ को

$(a, b) * (c, d) = (a *_1 c, b *_2 d) \; \forall a, c \in G_1, b, d \in G_2$
से परिभाषित करते हैं।

जिस ढंग से हमने संक्रिया $*$ को परिभाषित किया है उससे स्पष्ट है कि यह एक द्वि-आधारी संक्रिया है।

यह सत्यापित करने के लिए कि $(G, *)$ एक समूह है अथवा नहीं, आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 1) दिखाइए कि G पर द्वि-आधारी संक्रिया $*$ साहचर्य है। इसका तत्समक अवयव और G में किसी अवयव (x, y) का व्युत्क्रम ज्ञात कीजिए।

इस तरह, आपने सिद्ध कर दिया है कि $*$ के सापेक्ष $G = G_1 \times G_2$ एक समूह है। हम G को $(G_1, *_1)$ और $(G_2, *_2)$ का **बाह्य अनुलोम गुणनफल** (external direct product) कहते हैं।

उदाहरण के लिए, $\mathbf{R}^2$, R का स्वयं के साथ बाह्य अनुलोम गुणनफल है।

एक अन्य उदाहरण है अनुलोम गुणनफल $(\mathbf{Z}, +) \times (\mathbf{R}^*, \cdot)$, जिसमें संक्रिया
$(m, x) * (n, y) = (m + n, xy)$
से दी जाती है।

इसी तरह हम 3, 4 या अधिक समूहों का बाह्य अनुलोम गुणनफल भी परिभाषित कर सकते हैं।

परिभाषा : मान लीजिए $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$ समूह हैं। इनका **बाह्य अनुलोम गुणनफल** समूह $(G, *)$ है, जहां
$G = G_2 \times G_2 \times \ldots \times G_n$ और
$(x_1, x_2, \ldots, x_n) * (y_1, y_2, \ldots, y_n) = (x_1 *_1 y_1, x_2 *_2 y_2, \ldots, x_n *_n y_n) \; \forall x_i, y_i \in G_i$.
इस प्रकार, $\mathbf{R}^n$, R की n प्रतियों का बाह्य अनुलोम गुणनफल है।

यहां हम संकेतन के बारे में एक टिप्पणी देना चाहेंगे।

टिप्पणी 1 : आगे से हम यह मानकर चलेंगे कि सभी संक्रियाएं $*, *_1, \ldots, *_n$ गुणन संक्रिया हैं, जब तक कि कोई विशेष उल्लेख न किया जाए। इस तरह $G = G_1 \times G_2 \times \ldots \times G_n$ पर संक्रिया

$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n) \; \forall a_i, b_i \in G_i$

से दी जाएगी।

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 2) दिखाइए कि किन्हीं दो समूहों G_1 और G_2 के लिए $G_1 \times G_2 \simeq G_2 \times G_1$.

E 2 की वजह से हम 2 (या n) समूहों के अनुलोम गुणनफल में इनके क्रम की चिंता नहीं करते।

अब, मान लीजिए G बाह्य अनुलोम गुणनफल $G_1 \times G_2$ है। प्रक्षेप प्रतिचित्र (projection map)

$\pi_1 : G_1 \times G_2 \to G_1 : \pi_1 (x, y) = x$ लीजिए। π_1 एक समूह समाकारिता है क्योंकि

$$\pi_1 ((a, b) (c, d)) = \pi_1 (ab, cd)$$
$$= ab$$
$$= \pi_1(a, b)\, \pi_1 (c, d).$$

π_1 आच्छादक भी है, क्योंकि कोई भी $x \in G_1$, $\pi_1 (x, e_2)$ होता है।

आइए अब हम Ker π_1 पर विचार करें।

$$\text{Ker } \pi_1 = \{(x, y) \in G_1 \times G_2 \mid \pi_1 (x, y) = e_1\}$$
$$= \{(e_1, y) \mid y \in G_2\} = \{e_1\} \times G_2.$$

$\therefore \{e_1\} \times G_2 \trianglelefteq G_1 \times G_2.$

साथ ही, समाकारिता के मूल प्रमेय के अनुसार

$(G_1 \times G_2)/(\{e_1\} \times G_2) \simeq G_1.$

इसी प्रकार हम सिद्ध कर सकते हैं कि

$G_1 \times \{e_2\} \trianglelefteq G_1 \times G_2$ और $(G_1 \times G_2)/(G_1 \times \{e_2\}) \simeq G_2.$

नीचे दिए गए प्रश्नों में हमने समूहों के बाह्य अनुलोम गुणनफलों से संबंधित व्यापक तथ्य प्रस्तुत किए हैं।

E 3) दिखाइए कि $G_1 \times G_2$ अपने प्रसामान्य उपसमूहों $H = G_1 \times \{e_2\}$ और $K = \{e_1\} \times G_2$ का गुणनफल है। यह भी दिखाइए कि
$(G_1 \times \{e_2\}) \cap (\{e_1\} \times G_2) = \{(e_1, e_2)\}.$

E 4) सिद्ध कीजिए कि $Z(G_1 \times G_2) = Z(G_1) \times Z (G_2)$, जहां $Z(G)$, G के केन्द्र को प्रकट करता है (इकाई 3 का प्रमेय 2 देखिए)।

E 5) मान लीजिए A और B क्रमशः कोटि m और n वाले चक्रीय समूह हैं, जहां $(m, n) = 1$. सिद्ध कीजिए कि $A \times B$ कोटि mn वाला चक्रीय समूह है।
(**संकेत :** $f : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n : f(r) = (r + m\mathbf{Z}, r + n\mathbf{Z})$ परिभाषित कीजिए। तब समाकारिता का मूल प्रमेय लागू करके दिखाइए कि $\mathbf{Z}_m \times \mathbf{Z}_n \simeq \mathbf{Z}_{mn}$.)

परिमित चक्रीय समूहों का अनुलोम गुणनफल चक्रीय होता है यदि और केवल यदि उनकी कोटियां सापेक्षतः अभाज्य हों।

अभी तक हमने दो समूहों G_1 और G_2 से $G_1 \times G_2$ प्राप्त करने की विधि देखी है। अब हम देखेंगे कि किन प्रतिबंधों के अधीन हम किसी समूह को उसके उपसमूहों के अनुलोम गुणनफल के रूप में व्यक्त कर सकते हैं।

8.2.2 आंतरिक अनुलोम गुणनफल

आइए हम पहले इकाई 5 से याद करें कि यदि H और K समूह G के प्रसामान्य उपसमूह हों, तो HK समूह G का प्रसामान्य उपसमूह होगा। हमारी रुचि उस स्थिति में है जबकि HK पूरा का पूरा G हो। इस संबंध में हम एक परिभाषा दे रहे हैं।

परिभाषा : मान लीजिए H और K समूह G के प्रसामान्य उपसमूह हैं। हम G को H और K का **आंतरिक अनुलोम गुणनफल** (internal direct product) कहते हैं, यदि $G = HK$ और $H \cap K = \{e\}$. इसे हम $G = H \times K$ लिखते हैं।

उदाहरण के लिए, आइए हम परिचित क्लाइन 4-समूह $K_4 = \{e, a, b, ab\}$ लें, जहां $a^2 = e, b^2 = e$ और $ab = ba$.

मान लीजिए $H = \langle a \rangle$ और $K = \langle b \rangle$. तब

$H \cap K = \{e\}$. साथ ही $G = HK$.

$\therefore G = H \times K.$

ध्यान दीजिए कि $H \simeq \mathbf{Z}_2$ और $K \simeq \mathbf{Z}_2 \therefore G \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$.

एक अन्य उदाहरण के रूप में $\mathbf{Z}_{10}$ को लीजिए। यह अपने उपसमूहों $H = \{\bar{0}, \bar{5}\}$ और $K = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ का आंतरिक अनुलोम गुणनफल है। ऐसा इसलिए है क्योंकि

i) $Z_{10} = H + K$, क्योंकि Z_{10} का कोई भी अवयव H के किसी अवयव और K के किसी अवयव का योगफल होता है, और

ii) $H \cap K = \{\bar{0}\}$.

अब बताइए कि क्या कोई बाह्य अनुलोम गुणनफल आंतरिक अनुलोम गुणनफल भी हो सकता है? आइए इस प्रश्न का उत्तर ढूंढने के लिए हम E 3 को देखें। इसके अनुसार $G_1 \times G_2$ का बाह्य गुणनफल आंतरिक गुणनफल $(G_1 \times \{e_2\}) \times (\{e_1\} \times G_2)$ होता है।

इस संबंध में यहां हम एक टिप्पणी देना चाहते हैं।

टिप्पणी 2 : मान लीजिए H और K समूह G के प्रसामान्य उपसमूह हैं। तब H और K का आंतरिक अनुलोम गुणनफल H और K के बाह्य अनुलोम गुणनफल के तुल्याकारी होता है। यही कारण है कि जब हम उपसमूहों के आंतरिक अनुलोम गुणनफल के बारे में चर्चा कर रहे होते हैं तो हम "आंतरिक" शब्द का प्रयोग नहीं करते और केवल "उपसमूहों का अनुलोम गुणनफल" कहते हैं।

आइए अब हम दो उपसमूहों के आंतरिक अनुलोम गुणनफल की परिभाषा को अनेक उपसमूहों के आंतरिक अनुलोम गुणनफल में विस्तृत करें।

परिभाषा : समूह G अपने प्रसामान्य उपसमूहों $H_1, H_2, \ldots, H_n$ का **आंतरिक अनुलोम गुणनफल** होता है यदि

i) $G = H_1H_2 \ldots H_n$, और

ii) $H_i \cap H_1 \ldots H_{i-1} H_{i+1} \ldots H_n = \{e\} \; \forall \, i = 1, \ldots, n$.

उदाहरण के लिए, {a, b, c} से जनित समूह G पर विचार कीजिए, जहां $a^2 = e = b^2 = c^2$ और $ab = ba, ac = ca, bc = cb$. यह $< a >, < b >$ और $< c >$ का आंतरिक अनुलोम गुणनफल है। अर्थात्

$G \simeq Z_2 \times Z_2 \times Z_2$.

अब बताइए कि क्या प्रत्येक समूह को उसके दो या अधिक उचित प्रसामान्य उपसमूहों के आंतरिक अनुलोम गुणनफल के रूप में लिखा जा सकता है? समूह **Z** लीजिए। मान लीजिए $Z = H \times K$, जहां H, K, **Z** के उपसमूह हैं। इकाई 3 के उदाहरण 4 से आप जानते हैं कि $H = < m >$ और $K = < n >$, किन्हीं $m, n \in Z$ के लिए। तब $mn \in H \cap K$. परन्तु यदि $H \times K$ अनुलोम गुणनफल है, तो $H \cap K = \{0\}$. इस तरह, हमें एक अंतर्विरोध प्राप्त होता है। अतः **Z** को दो उपसमूहों के आंतरिक अनुलोम गुणनफल के रूप में नहीं लिखा जा सकता।

इसी तर्क के प्रयोग से हम कह सकते हैं कि **Z** को $H_1 \times H_2 \times \ldots \times H_n$ के रूप में नहीं लिखा जा सकता है, जहां $H_i \leq Z \; \forall \, i = 1, 2, \ldots, n$.

जब कोई समूह अपने उपसमूहों का आंतरिक अनुलोम गुणनफल होता है तब वह निम्नलिखित प्रमेय को संतुष्ट करता है।

प्रमेय 1 : मान लीजिए समूह G अपने उपसमूहों H और K का आंतरिक अनुलोम गुणनफल है। तब,

क) प्रत्येक $x \in G$ को $x = hk$ के रूप में **अद्वितीयतः** व्यक्त किया जा सकता है, जहां $h \in H$ और $k \in K$; और

ख) $hk = kh \; \forall \, h \in H, k \in K$.

उपपत्ति : (क) हम जानते हैं कि $G = HK$. अतः यदि $x \in G$, तो किसी $h \in H$ और $k \in K$ के लिए $x = hk$. अब मान लीजिए कि $x = h_1k_1$ भी है, जहां $h_1 \in H$ और $k_1 \in K$. तब
$hk = h_1k_1$. $\therefore h_1^{-1}h = k_1k^{-1}$. अब $h_1^{-1}h \in H$.
साथ ही, क्योंकि $h_1^{-1}h = k_1k^{-1} \in K$, इसलिए $h_1^{-1}h \in K$.
$\therefore h_1^{-1}h \in H \cap K = \{e\}$.
$\therefore h_1^{-1}h = e$, जिसका अर्थ है कि $h_1 = h$.
इसी प्रकार, $k_1 k^{-1} = e$, जिसका अर्थ है कि $k_1 = k$.

इस तरह, H के एक अवयव और K के एक अवयव के गुणनफल के रूप में x का निरूपण अद्वितीय है।

ख) दो अवयवों x और y में क्रमविनिमेयता दिखाने का सबसे अच्छा तरीका है कि हम दिखाएं कि उनका क्रमविनिमयक $x^{-1}y^{-1}xy$ तत्समक है। अतः मान लीजिए कि $h \in H$ और $k \in K$, और $h^{-1}k^{-1}hk$ लीजिए। चूंकि
$K \trianglelefteq G$, $h^{-1}k^{-1}h \in K$, अतः $h^{-1}k^{-1}hk \in K$.
इसी तर्क के प्रयोग से $h^{-1}k^{-1}hk \in H$.
$\therefore h^{-1}k^{-1}hk \in H \cap K = \{e\}$
$\therefore h^{-1}k^{-1}hk = e$, अर्थात् $hk = kh$.

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 6) मान लीजिए H और K समूह G के प्रसामान्य उपसमूह हैं, जो प्रमेय 1 (क) को संतुष्ट करते हैं। दिखाइए कि
$G = H \times K$.

आइए अब हम आंतरिक अनुलोम गुणनफलों और विभाग समूहों के संबंध के बारे में विचार करें।

प्रमेय 2 : मान लीजिए कि H और K समूह G के ऐसे प्रसामान्य उपसमूह हैं जिनसे कि $G = H \times K$. तब $G/H \simeq K$ और $G/K \simeq H$.

उपपत्ति : हम इस परिणाम को सिद्ध करने के लिए इकाई 6 के प्रमेय 8 को लागू करेंगे।
अब $G = HK$ और $H \cap K = \{e\}$. इसलिए
$G/H = HK/H \simeq K/(H \cap K) = K/\{e\} \simeq K$.
इसी प्रकार हम सिद्ध कर सकते हैं कि $G/K \simeq H$.

अब हम एक परिणाम दे रहे हैं जो प्रमेय 2 से तुरंत प्राप्त हो जाता है और जिसका प्रयोग भाग 8.4 में किया जाएगा।

प्रमेय 3 : मान लीजिए कि G एक परिमित समूह है और H और K उसके ऐसे उपसमूह हैं कि $G = H \times K$. तब
$o(G) = o(H)\, o(K)$

इसकी उपपत्ति हम आपके लिए छोड़ रहे हैं (नीचे दिया गया प्रश्न देखिए)।

E 7) प्रमेय 2 की सहायता से प्रमेय 3 सिद्ध कीजिए।

आइए अब हम किसी परिमित समूह की संरचना से संबंधित कुछ आधारभूत परिणामों पर चर्चा करें।

8.3 सीलो प्रमेय

इकाई 4 में हमने लग्रांज प्रमेय सिद्ध किया था, जिसके अनुसार किसी परिमित समूह के उपसमूह की कोटि समूह की कोटि को विभाजित करती है। हमने वहां यह भी कहा था कि यदि G एक **परिमित चक्रीय समूह** हो और $m \mid o(G)$, तो G का कोटि m वाला एक उपसमूह होता है। लेकिन, यदि G चक्रीय नहीं है तो यह आवश्यक नहीं है कि यह कथन सही ही हो, जैसा कि आप पिछली इकाई में देख चुके हैं। इस संदर्भ में गणितज्ञ कौशी (Cauchy) ने 1845 में निम्नलिखित उपयोगी परिणाम सिद्ध किया था।

प्रमेय 4 : यदि अभाज्य p परिमित समूह G की कोटि को विभाजित करता हो, तो G कोटि p वाले एक अवयव को आविष्ट करता है।

इस परिणाम की उपपत्ति के लिए समूह सिद्धांत की ऐसी जानकारी आवश्यक है जोकि हम इस पाठ्यक्रम में नहीं दे रहे हैं। अतः हम उपपत्ति नहीं देंगे। इस परिणाम से हमें निम्नलिखित परिणाम तुरंत प्राप्त होता है।

प्रमेय 5 : यदि अभाज्य p परिमित समूह G की कोटि को विभाजित करता हो, तो G कोटि p वाले एक उपसमूह को आविष्ट करता है।

उपपत्ति : कोटि p वाले अवयव से जनित चक्रीय उपसमूह लीजिए। इस अवयव का अस्तित्व प्रमेय 4 के अनुसार होता है।

इस तरह, प्रमेय 5 से हम जानते हैं कि किसी कोटि 30 वाले समूह के कोटि 2 वाला एक उपसमूह, कोटि 3 वाला एक उपसमूह और कोटि 5 वाला एक उपसमूह होगा।

1872 में नार्वे के गणितज्ञ लुडविग सीलो (Ludwig Sylow) ने कौशी के परिणाम के एक असाधारण विस्तार को सिद्ध किया। यह परिणाम, जिसे प्रथम सीलो प्रमेय कहते हैं, परिमित समूह सिद्धांत का आधार सिद्ध हुआ है। उदाहरण के लिए, इस परिणाम की सहायता से हम कह सकते हैं कि कोटि 100 वाले किसी समूह के कोटि 2, 4, 5 और 25 वाले उपसमूह होते हैं। आइए हम देखें कि आखिर यह शक्तिशाली प्रमेय है क्या।

प्रमेय 6 (प्रथम सीलो प्रमेय) : मान लीजिए कि G एक परिमित समूह है, जहां $o(G) = p^n m$, p अभाज्य है, $n \geq 1$ और $(p, m) = 1$. तब G कोटि p^k वाला उपसमूह आविष्ट करता है, सभी $k = 1, \ldots, n$ के लिए।

हम न तो इस परिणाम को और न ही अगले दो सीलो प्रमेयों को सिद्ध करेंगे। परंतु इन परिणामों का कथन देकर हम दिखाएंगे कि ये परिणाम कितने उपयोगी हैं।

अगले प्रमेय में संयुग्मिता (conjugacy) और सीलो p-उपसमूह की संकल्पनाओं का प्रयोग होता है, जिनकी परिभाषा हम अब दे रहे हैं।

परिभाषा : समूह G के दो उपसमूह H और K, **G में संयुग्मी** होते हैं यदि $\exists\, g \in G$ जिससे कि $K = g^{-1}Hg$, और तब K को G में H का संयुग्मी कहते हैं।

क्या अब आप नीचे दिए गए प्रश्न को हल कर सकते हैं?

E 8) दिखाइए कि $H \trianglelefteq G$ यदि और केवल यदि G में H का संयुग्मी केवल H ही है।

अब हम सीलो p-उपसमूह परिभाषित करेंगे।

परिभाषा : मान लीजिए G एक परिमित समूह है और p एक ऐसा अभाज्य है जिससे कि $n \geq 1$ के लिए $p^n \mid o(G)$ पर $p^{n+1} \nmid o(G)$. तब समूह G के कोटि p^n वाले उपसमूह को G का **सीलो p-उपसमूह** कहते हैं।

अतः, यदि $o(G) = p^n m$, $(p, m) = 1$, तो कोटि p^n वाले G का उपसमूह एक सीलो p-उपसमूह होगा। प्रमेय 6 के अनुसार ऐसा उपसमूह सदा ही होता है। परन्तु एक समूह के एक से अधिक सीलो p-उपसमूह हो सकते हैं। अगले परिणाम से हमें पता चलता है कि एक समूह के दो सीलो p-उपसमूहों के बीच का संबंध क्या है।

प्रमेय 7 (द्वितीय सीलो प्रमेय) : मान लीजिए G एक समूह है, जहां $o(G) = p^n m$, $(p, m) = 1$ और p अभाज्य है। तब G के कोई भी दो सीलो p-उपसमूह G में संयुग्मी होते हैं।

आइए अब हम देखें कि एक समूह के कितने सीलो p-उपसमूह हो सकते हैं।

प्रमेय 8 (तृतीय सीलो प्रमेय) : मान लीजिए G कोटि $p^n m$ वाला एक समूह है, जहां $(p, m) = 1$ और p एक अभाज्य है। तब G के अलग-अलग सीलो p-उपसमूहों की संख्या $n_p = 1 + kp$ होती है, किसी $k \geq 0$ के लिए। इसके अतिरिक्त, $n_p \mid o(G)$.

यहां हम प्रमेय 8 को लागू करने के संबंध में एक टिप्पणी देना चाहेंगे।

टिप्पणी 3 : प्रमेय 8 के अनुसार $n_p \equiv 1 \pmod p$ (देखिए भाग 2.5.1)। $\therefore (n_p, p^n) = 1$ साथ ही, चूंकि $n_p \mid o(G)$, इकाई 1 के प्रमेय 9 से, $n_p \mid m$. इस तथ्य से हमें n_p की संभावनाओं को कम करने में सहायता मिलती है, जैसा कि आप नीचे दिए गए उदाहरणों में देखेंगे।

उदाहरण 1 : दिखाइए कि कोटि 15 वाला कोई भी समूह चक्रीय होता है।

हल : मान लीजिए G कोटि $15 = 3 \times 5$ वाला एक समूह है। प्रमेय 6 के अनुसार G का एक सीलो 3-उपसमूह है। और प्रमेय 8 के अनुसार ऐसे उपसमूहों की संख्या 15 को अवश्य विभाजित करेगी और वह 1 (mod 3) के समशेष होगी। टिप्पणी 3 के अनुसार ऐसे उपसमूहों की संख्या 5 को अवश्य विभाजित करेगी और वह 1 (mod 3) के समशेष होगी। इस तरह, हम पाते हैं कि

संभावना केवल 1 है। इसलिए G का केवल एक ही सीलो 3-उपसमूह है, मान लीजिए H. अतः प्रमेय 7 और E 8 से हम जानते हैं कि $H \trianglelefteq G$. चूंकि H अभाज्य कोटि वाला है, इसलिए यह चक्रीय है।

इसी प्रकार, हम जानते हैं कि G का एक कोटि 5 वाला उपसमूह है। ऐसे उपसमूहों की कुल संख्या 1, 6 या 11 है और वह 3 को अवश्य विभाजित करेगी। इस प्रकार, हम पाते हैं कि इस संख्या की संभावना केवल 1 है। इसलिए G का कोटि 5 वाला केवल एक ही समूह है, मान लीजिए K. तब $K \trianglelefteq G$ और K चक्रीय है।

आइए अब हम $H \cap K$ पर विचार करें। मान लीजिए $x \in H \cap K$. तब $x \in H$ और $x \in K$.
$\therefore o(x) \mid o(H)$ और $o(x) \mid o(K)$ (इकाई 4 के E 8 के अनुसार), अर्थात् $o(x) \mid 3$ और $o(x) \mid 5$.
$\therefore o(x) = 1$. $\therefore x = e$.
अर्थात् $H \cap K = \{e\}$.

साथ ही; $o(HK) = \dfrac{o(H)\, o(K)}{o(H \cap K)} = 15 = o(G)$.

$\therefore G = HK$.
अतः $G = H \times K \simeq \mathbf{Z}_3 \times \mathbf{Z}_5 \simeq \mathbf{Z}_{15}$, E 5 के अनुसार।

उदाहरण 2 : दिखाइए कि किसी कोटि 30 वाले समूह G का या तो कोटि 5 वाला एक प्रसामान्य उपसमूह होता है या कोटि 3 वाला एक प्रसामान्य उपसमूह होता है।

हल : चूंकि $30 = 2 \times 3 \times 5$, इसलिए G का एक सीलो 2-उपसमूह, एक सीलो 3-उपसमूह और एक सीलो 5-उपसमूह होता है। सीलो 5-उपसमूहों की संख्या $1 + 5k$ के रूप की होती है और 6 को (टिप्पणी 3 के अनुसार) विभाजित करती है। इसलिए यह 1 या 6 हो सकती है। यदि यह 1 है तो सीलो 5-उपसमूह G में प्रसामान्य है।

इसके विपरीत, मान लीजिए सीलो 5-उपसमूहों की संख्या 6 है। इन उपसमूहों में से प्रत्येक उपसमूह कोटि 5 वाले अलग-अलग चक्रीय समूह हैं, जिनमें केवल एक ही प्रतिच्छेदी अवयव e है। अतः ये उपसमूह समूह के $24 + 1 = 25$ अवयव आविष्ट करते हैं। इस तरह समूह के 5 ऐसे अवयव बचते हैं जो या तो कोटि 2 वाले हैं या कोटि 3 वाले। अब, सीलो 3-उपसमूहों की संख्या 1 या 10 हो सकती है। परन्तु, 10 सीलो 3-उपसमूह नहीं हो सकते, क्योंकि हमारे पास समूह के अधिक से अधिक 5 अवयव हैं जोकि कोटि 3 वाले हैं। अतः यदि समूह के 6 सीलो 5-उपसमूह हों तो इसका केवल 1 सीलो 3-उपसमूह होगा। यह G में प्रसामान्य होगा।

अब आप नीचे दिए गए प्रश्नों को हल करने का प्रयास कीजिए।

E 9) दिखाइए कि कोटि 20 वाले प्रत्येक समूह का एक उचित प्रसामान्य अतुच्छ उपसमूह होता है।

E 10) $\mathbf{Z}_{24}$ के सभी सीलो p-उपसमूह ज्ञात कीजिए, जहां p, 24 को विभाजित करने वाले सभी अभाज्यों के मान लेता है।

E 11) दिखाइए कि किसी कोटि 255 ($= 3 \times 5 \times 17$) वाले समूह का या तो 1 या 51 सीलो 5-उपसमूह होते हैं। इसके कितने सीलो 3-उपसमूह हो सकते हैं?

आइए अब हम 1 से 10 तक की कोटि वाले समूहों का वर्गीकरण करने के लिए शक्तिशाली सीलो प्रमेयों को लागू करें। इसके दौरान हम आपको अनेक प्रकार के परिमित समूहों की बीजीय संरचना से परिचित कराएंगे।

8.4 कोटि 1 से कोटि 10 तक के समूह

इस भाग में हम कुछ परिमित समूहों का अध्ययन करने के लिए पिछले भाग में प्राप्त परिणामों को लागू करेंगे। विशेष रूप से हम तुल्याकारिता तक 1 से 10 तक की कोटि वाले सभी समूहों की सूची देंगे।

सबसे पहले हम एक अति उपयोगी परिणाम को सिद्ध करेंगे।

प्रमेय 9 : मान लीजिए G एक ऐसा समूह है कि $o(G) = pq$, जहां p, q ऐसे अभाज्य हैं कि $p > q$ और $q \nmid p-1$. तब G चक्रीय होता है।

उपपत्ति : मान लीजिए P, G का एक सीलो p-उपसमूह है और Q, G का एक सीलो q-उपसमूह है। तब $o(P) = p$ और $o(Q) = q$. अब, क्योंकि अभाज्य कोटि वाला समूह चक्रीय होता है, इसलिए किन्हीं $x, y \in G$ के लिए $P = \langle x \rangle$ और $Q = \langle y \rangle$.

तृतीय सीलो प्रमेय के अनुसार कोटि p वाले उपसमूहों की संख्या n_p, $1, 1+p, 1+2p, \ldots$ हो सकती है, और यह q को अवश्य विभाजित करेगी। परन्तु $p > q$, इसलिए n_p की संभावना केवल 1 है। इस तरह, हम पाते हैं कि G का केवल एक ही सीलो p-उपसमूह है, अर्थात् P.और द्वितीय सीलो प्रमेय के अनुसार $P \trianglelefteq G$.

अब G के अलग-अलग सीलो q-उपसमूहों की संख्या $n_q = 1 + kq$ होती है, किसी k के लिए, और $n_q \mid p$. चूंकि p अभाज्य है इसलिए इसके गुणनखंड केवल 1 और p होंगे। $\therefore n_q = 1$ या $n_q = p$.अब, यदि $1 + kq = p$ तो $q \mid p - 1$. लेकिन, शुरू में हम यह मानकर चले थे कि $q \nmid p - 1$. इस तरह हमें एक अंतर्विरोध प्राप्त होता है। अतः $n_q = 1$ ही होगा। इस प्रकार, G में सीलो q-उपसमूह Q प्रसामान्य है।

अब हम दिखाना चाहते हैं कि $G = P \times Q$. इसके लिए आइए हम $P \cap Q$ लें। क्योंकि $P \cap Q$ के किसी भी अवयव की कोटि p और q को विभाजित करती है, इसलिए यह $(p, q) = 1$ को भी विभाजित करेगी। $\therefore P \cap Q = \{e\}$.

$\therefore o(PQ) = o(P)\, o(Q) = pq = o(G)$. $\therefore G = PQ$.

इस तरह हम पाते हैं कि

$G = P \times Q \simeq Z_p \times Z_q \simeq Z_{pq}$, E 5 से।

इसलिए G कोटि pq वाला चक्रीय समूह है।

प्रमेय 9 लागू करके हम तुरंत कह सकते हैं कि कोटि 15 वाला कोई भी समूह चक्रीय होता है (उदाहरण 1)। इसी प्रकार, यदि $o(G) = 35$, तो G चक्रीय होगा।

अब, यदि $q \mid p - 1$ और $o(G) = pq$, तो क्या G चक्रीय होगा? इसके लिए S_3 लीजिए। आप जानते हैं कि $o(S_3) = 6 = 2.3$, परन्तु S_3 चक्रीय नहीं है। इस संबंध में हम निम्नलिखित परिणाम दे रहे हैं।

प्रमेय 10 : मान लीजिए G एक ऐसा समूह है कि $o(G) = 2p$, जहां p एक विषम अभाज्य है। तब या तो G चक्रीय होता है, या G कोटि 2p वाले द्वितल समूह (dihedral group) D_{2p} के तुल्याकारी होता है। (आपको याद होगा कि

$D_{2p} = \langle \{x, y \mid x^p = e, y^2 = e$ और $yx = x^{-1}y\} \rangle$.)

उपपत्ति : प्रमेय 9 की उपपत्ति की तरह, यहां भी G का एक कोटि p वाला उपसमूह $P = \langle x \rangle$ होगा, और एक कोटि 2 वाला उपसमूह $Q = \langle y \rangle$ होगा, और $P \trianglelefteq G$ क्योंकि $p > 2$. और चूंकि $(2, p) = 1$, इसलिए $P \cap Q = \{e\}$.

$\therefore o(PQ) = o(G)$.

$\therefore G = PQ$.

अब दो स्थितियां है, अर्थात् जब $Q \trianglelefteq G$ और जब $Q \ntrianglelefteq G$.

यदि $Q \trianglelefteq G$, तो $G = P \times Q$, और तब $G = \langle xy \rangle$.

यदि G में Q प्रसामान्य नहीं है, तो G अवश्य अन्-आबेली होगा। (आपको याद होगा कि आबेली समूह का प्रत्येक उपसमूह प्रसामान्य होता है।)

$\therefore xy \neq yx$. $\therefore y^{-1}xy \neq x$.

अब, चूंकि $P = \langle x \rangle \trianglelefteq G$, $y^{-1}xy \in P$.

अतः किसी $r = 2, \ldots, p-1$ के लिए $y^{-1}xy = x^r$.

इसलिए, $y^{-2}xy^2 = y^{-1}(y^{-1}xy)y = y^{-1}x^ry = (y^{-1}xy)^r = (x^r)^r = x^{r^2}$.

$\Longrightarrow x = x^{r^2}$, क्योंकि $o(y) = 2$.

$\Longrightarrow x^{r^2} - 1 = e$.

लेकिन $o(x) = p$, इसलिए इकाई 4 के प्रमेय 4 के अनुसार
$p \mid (r^2 - 1)$, अर्थात् $p \mid (r-1)(r+1)$
$\Rightarrow p \mid (r-1)$ या $p \mid (r+1)$.
परन्तु $2 \leq r \leq p-1$. $\therefore p = r+1$,
अर्थात् $r = p-1$.
अतः हम पाते हैं कि
$y^{-1}xy = x^r = x^{p-1} = x^{-1}$.
इसलिए, $G = PQ = < \{x, y \mid x^p = e, y^2 = e, y^{-1}xy = x^{-1}\} >$,
जिसकी बीजीय संरचना ठीक वही है जोकि D_{2p} की है।
$\therefore G \simeq D_{2p} = \{e, x, x^2, \ldots, x^{p-1}, y, xy, x^2y, \ldots, x^{p-1}y\}$.

आप नीचे दिए गए उदाहरण से प्रमेय 10 की उपयोगिता समझ सकेंगे।

उदाहरण 3 : किसी कोटि 6 वाले समूह की संभव बीजीय संरचनाएं क्या हैं?

हल : मान लीजिए G कोटि 6 वाला एक समूह है। तब प्रमेय 10 के अनुसार $G \simeq Z_6$ या $G \simeq D_6$. इकाई 5 के E 7 में आप देख ही चुके हैं कि $S_3 \simeq D_6$. इसलिए यदि G चक्रीय नहीं है, तो $G \simeq S_3$.

अब आप नीचे दिए गए प्रश्न को हल करने का प्रयास कर सकते हैं।

E 12) दिखाइए कि यदि G कोटि 10 वाला समूह है, तो
$G \simeq Z_{10}$ या $G \simeq D_{10}$.

अब, इकाई 4 के प्रमेय 6 से हम जानते हैं कि यदि $o(G)$ अभाज्य है, तो G चक्रीय होता है। इस प्रकार, कोटि 2, 3, 5 और 7 वाले समूह चक्रीय होते हैं। उदाहरण 3 और E 12 के साथ इस तथ्य को लागू करके हम उन सभी समूहों का वर्गीकरण कर सकते हैं जिनकी कोटियां 1, 2, 3, 5, 6, 7 या 10 हैं। कोटि $4 = 2^2$ और $9 = 3^2$ वाले समूहों की संरचना के बारे में आप क्या कह सकते हैं? ऐसे समूहों पर निम्नलिखित परिणाम लागू होता है।

प्रमेय 11 : यदि G कोटि p^2 वाला एक समूह हो, जहां p अभाज्य है, तो G आबेली होता है।

यहां हम इस प्रमेय को सिद्ध नहीं करेंगे क्योंकि इसकी उपपत्ति इस पाठ्यक्रम के क्षेत्र से बाहर है। परन्तु इस प्रमेय को लागू करके हम कोटि p^2 वाले समूहों का वर्गीकरण आसानी से कर सकते हैं।

प्रमेय 12 : मान लीजिए G एक ऐसा समूह है कि $o(G) = p^2$, जहां, p एक अभाज्य है। तब या तो G चक्रीय होता है या $G \simeq Z_p \times Z_p$, कोटि p वाले दो चक्रीय समूहों का अनुलोम गुणनफल।

उपपत्ति : मान लीजिए G का कोटि p^2 वाला एक अवयव a है। तब $G = < a >$

इसके विपरीत, मान लीजिए कि G का कोटि p^2 वाला कोई भी अवयव नहीं है। तब, किसी $x \in G$ के लिए $o(x) = 1$ या $o(x) = p$ (लग्रांज प्रमेय लागू करने पर)।

मान लीजिए $x \in G, x \neq e$ और $H = < x >$
क्योंकि $x \neq e$, इसलिए $o(H) \neq 1$.
$\therefore o(H) = p$.

इसलिए ऐसा $y \in G$ होगा जिससे कि $y \notin H$. तब ऊपर वाले तर्क द्वारा हम कह सकते हैं कि $K = < y >$ की कोटि p है। चूंकि G आबेली है (प्रमेय 11 के अनुसार), इसलिए H और K दोनों ही G में प्रसामान्य हैं।

हम दिखाना चाहते हैं कि $G = H \times K$. इसके लिए $H \cap K$ लीजिए। अब,
$H \cap K \leq H$. $\therefore o(H \cap K) \mid o(H) = p$. $\therefore o(H \cap K) = 1$ या $o(H \cap K) = p$.
यदि $o(H \cap K) = p$, तो $H \cap K = H$, और इसी तर्क से हम कह सकते हैं कि $H \cap K = K$.
परन्तु, तब $H = K$. $\therefore y \in H$, जो एक अंतर्विरोध है।
$\therefore o(H \cap K) = 1$, अर्थात् $H \cap K = \{e\}$.

इसलिए, $H \trianglelefteq G$, $K \trianglelefteq G$, $H \cap K = \{e\}$ और $o(HK) = p^2 = o(G)$.
$\therefore\ G = H \times K \simeq \mathbf{Z}_p \times \mathbf{Z}_p$.

अब, आप नीचे दिए गए प्रश्न को हल करने का प्रयास कीजिए।

E 13) कोटि 4 और कोटि 9 वाले समूहों की संभव बीजीय संरचनाएं क्या हैं?

अभी तक हमने कोटि 8 वाले समूहों को छोड़कर 1 से 10 तक की कोटि वाले समूहों की बीजीय संरचनाएं प्रदर्शित की हैं। अब हम कोटि 8 वाले समूहों के वर्गीकरण की (उपपत्ति बिना) सूची देंगे।

यदि G कोटि 8 वाला आबेली समूह हो, तो

i) $G \simeq \mathbf{Z}_8$, कोटि 8 वाला चक्रीय समूह, या

ii) $G \simeq \mathbf{Z}_4 \times \mathbf{Z}_2$, या

iii) $G \simeq \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

यदि G कोटि 8 वाला अन्-आबेली समूह हो, तो

i) $G \simeq Q_8$, चतुष्टयी समूह, जिस पर हम इकाई 4 के उदाहरण 4 में चर्चा कर चुके हैं; या

ii) $G \simeq D_8$, द्वितल समूह जिस पर हम इकाई 5 के उदाहरण 4 में चर्चा कर चुके हैं।

इस तरह, हमने कोटि 1, 2, ... , 10 वाले समूहों की बीजीय संरचना को देख लिया है। हम बता चुके हैं कि यह वर्गीकरण **तुल्याकारिता** तक ही है। अतः, उदाहरण के लिए, कोटि 10 वाला कोई भी समूह $\mathbf{Z}_{10}$ या $\mathbf{D}_{10}$ के **तुल्याकारी** होता है; यह आवश्यक नहीं है कि यह $\mathbf{Z}_{10}$ या $\mathbf{D}_{10}$ के बराबर हो।

आइए अब हम इस इकाई में दी गई पाठ्य-सामग्री का संक्षिप्त विवरण दें।

8.5 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों पर चर्चा की है।

1. समूहों के बाह्य अनुलोम गुणनफलों की परिभाषा और उदाहरण।
2. प्रसामान्य उपसमूहों के आंतरिक अनुलोम गुणनफलों की परिभाषा और उदाहरण।
3. यदि $(m, n) = 1$, तो $\mathbf{Z}_m \times \mathbf{Z}_n \simeq \mathbf{Z}_{mn}$.
4. $o(H \times K) = o(H)\,o(K)$.
5. सीलो प्रमेयों के कथन और अनुप्रयोग। इन प्रमेयों के अनुसार मान लीजिए G कोटि $p^n m$ वाला एक परिमित समूह है, जहां p एक अभाज्य है और $p \nmid m$. तब
   i) G कोटि p^k वाले उपसमूह को आविष्ट करता है $\forall\ k = 1, \ldots, n$;
   ii) G में कोई भी दो सीलो p-उपसमूह संयुग्मी होते हैं;
   iii) G के अलग-अलग सीलो p-उपसमूहों की संख्या 1(mod p) के समशेष होती है और $o(G)$ को विभाजित करती है (वास्तव में, यह m को विभाजित करती है)।
6. मान लीजिए $o(G) = pq$, जहां p एक अभाज्य है, $p > q$, $q \nmid p - 1$. तब G चक्रीय होता है।
7. मान लीजिए $o(G) = p^2$, जहां p एक अभाज्य है। तब
   i) G आबेली है।
   ii) G चक्रीय है या $G \simeq \mathbf{Z}_p \times \mathbf{Z}_p$.

8. 1 से 10 तक की कोटि वाले समूहों का वर्गीकरण, जिसे हम नीचे की सारणी में दे रहे हैं।

o(G)	बीजीय संरचना
1	$\{e\}$
2	$\mathbf{Z}_2$
3	$\mathbf{Z}_3$
4	$\mathbf{Z}_4$ या $\mathbf{Z}_2 \times \mathbf{Z}_2$
5	$\mathbf{Z}_5$
6	$\mathbf{Z}_6$ या S_3
7	$\mathbf{Z}_7$
8	$\mathbf{Z}_8$ या $\mathbf{Z}_4 \times \mathbf{Z}_2$ या $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ (यदि G आबेली है) Q_8 या D_8 (यदि G अन्-आबेली है)
9	$\mathbf{Z}_9$ या $\mathbf{Z}_3 \times \mathbf{Z}_3$
10	$\mathbf{Z}_{10}$ या D_{10}

8.6 हल/उत्तर

E 1) • साहचर्य है : मान लीजिए $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$.
$((a_1, b_1) * (a_2, b_2)) * (a_3, b_3) = (a_1, b_1) * ((a_2, b_2) * (a_3, b_3))$.
को सिद्ध करने के लिए, इस तथ्य को लागू कीजिए कि $*_1$ और $*_2$ साहचर्य हैं। G का तत्समक अवयव (e_1, e_2) है, जहां e_1 और e_2 क्रमशः G_1 और G_2 के तत्समक हैं।
$(x, y) \in G$ का व्युत्क्रम (x^{-1}, y^{-1}) है।

E 2) $f: G_1 \times G_2 \to G_2 \times G_1 : f(a, b) = (b, a)$ परिभाषित कीजिए। तब f, 1-1, आच्छादक और समाकारिता है। अर्थात् f एक तुल्यकारिता है।
$\therefore G_1 \times G_2 \simeq G_2 \times G_1$.

E 3). हमें दिखाना है कि $G_1 \times G_2$ का कोई भी अवयव hk के रूप का होता है, जहां $h \in H$ और $k \in K$. अब $G_1 \times G_2$ का कोई भी अवयव $(x, y) = (x, e_2)(e_1, y)$ होता है और $(x, e_2) \in H, (e_1, y) \in K$.
$\therefore G_1 \times G_2 = HK$.
आइए अब हम $H \cap K$ पर विचार करें। मान लीजिए $(x, y) \in H \cap K$. क्योंकि $(x, y) \in H$, इसलिए $y = e_2$. क्योंकि $(x, y) \in K$, इसलिए $x = e_1$.
$\therefore (x, y) = (e_1, e_2)$. $\therefore H \cap K = \{(e_1, e_2)\}$.

E 4) अब, $(x, y) \in Z(G_1 \times G_2)$.
$\Longleftrightarrow (x, y)(a, b) = (a, b)(x, y) \ \forall \ (a, b) \in G_1 \times G_2$
$\Longleftrightarrow (xa, yb) = (ax, by) \ \forall \ a \in G_1, b \in G_2$
$\Longleftrightarrow xa = ax \ \forall \ a \in G_1$ और $yb = by \ \forall \ b \in G_2$
$\Longleftrightarrow x \in Z(G_1)$ और $y \in Z(G_2)$
$\Longleftrightarrow (x, y) \in Z(G_1) \times Z(G_2)$
$\therefore Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$

E 5) मान लीजिए $A = \langle x \rangle$ और $B = \langle y \rangle$, जहां $o(x) = m, o(y) = n$.
तब $A \simeq \mathbf{Z}_m$ और $B \simeq \mathbf{Z}_n$.
यदि हम सिद्ध कर दें कि $\mathbf{Z}_m \times \mathbf{Z}_n \simeq \mathbf{Z}_{mn}$, तब हम यह सिद्ध कर देंगे कि $A \times B \simeq \mathbf{Z}_{mn}$, अर्थात् $A \times B$ कोटि mn वाला चक्रीय समूह है। तो आइए अब हम सिद्ध करें कि यदि $(m, n) = 1$, तो $\mathbf{Z}_{mn} \simeq \mathbf{Z}_m \times \mathbf{Z}_n$.
$f: \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n : f(r) = (r + m\mathbf{Z}, r + n\mathbf{Z})$.
परिभाषित कीजिए।
(आपको याद होगा कि किसी $s \in \mathbf{N}$ के लिए $\mathbf{Z}_s = \mathbf{Z}/s\mathbf{Z}$.)
अब f एक समाकारिता है, क्योंकि

$$\begin{aligned} f(r+s) &= ((r+s) + m\mathbf{Z}, (r+s) + n\mathbf{Z}) \\ &= (r + m\mathbf{Z}, r + n\mathbf{Z}) + (s + m\mathbf{Z}, s + n\mathbf{Z}) \\ &= f(r) + f(s). \end{aligned}$$

$$\text{Ker } f = \{r \in \mathbf{Z} \mid r \in m\mathbf{Z} \cap n\mathbf{Z}\}$$
$$= \{r \in \mathbf{Z} \mid r \in mn\mathbf{Z}\}$$
$$= mn\mathbf{Z}.$$

अंत में हम दिखाएंगे कि f आच्छादक है। अब कोई अवयव $(u + m\mathbf{Z}, v + n\mathbf{Z}) \in \mathbf{Z}_m \times \mathbf{Z}_n$ लीजिए। क्योंकि $(m, n) = 1$, $\exists\, s, t \in \mathbf{Z}$ जिससे कि $ms + nt = 1$ (देखिए भाग 1.6)। इस समीकरण से हम पाते हैं कि $f(u(1 - ms) + v(1 - nt)) = (u + m\mathbf{Z}, v + n\mathbf{Z})$. इस तरह, f आच्छादक है।
अब समाकारिता का मूल प्रमेय लागू करने पर हम पाते हैं कि $\mathbf{Z}/\text{Ker } f \simeq \text{Im } f$,
अर्थात् $\mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}_m \times \mathbf{Z}_n$,
अर्थात् $\mathbf{Z}_{mn} \simeq \mathbf{Z}_m \times \mathbf{Z}_n$.
$\therefore$ $A \times B$ कोटि mn वाला चक्रीय समूह है।

E 6) हम जानते हैं कि प्रत्येक $x \in G$ को hk के रूप में व्यक्त किया जा सकता है, जहां $h \in H$ और $k \in K$.
$\therefore$ $G = HK$
अब हमें दिखाना है कि $H \cap K = \{e\}$.
मान लीजिए $x \in H \cap K$. तब $x \in H$ और $x \in K$.
$\therefore$ $xe \in HK$ और $ex \in HK$.
अतः H के एक अवयव और K के एक अवयव के गुणनफल के रूप में x के दो निरुपण xe और ex हैं। परन्तु हम यह मानकर चले हैं कि प्रत्येक अवयव का इस प्रकार का केवल एक निरुपण होना चाहिए। अतः दोनों निरुपण xe और ex संपाती होंगे, अर्थात् $x = e$.
$\therefore$ $H \cap K = \{e\}$.
$\therefore$ $G = H \times K$.

E 7) $G = H \times K \implies G/H \simeq K \implies o(G/H) = o(K) \implies o(G)/o(H) = o(K)$.
$\implies o(G) = o(H)\, o(K)$.

E 8) $H \trianglelefteq G \iff g^{-1}Hg = H \;\forall g \in G$
$\iff$ G में H का संयुग्मी केवल H है।

E 9) मान लीजिए G कोटि 20 वाला एक समूह है। चूंकि $20 = 2^2 \times 5$, इसलिए G का एक सीलो 5-उपसमूह होगा। ऐसे उपसमूहों की संख्या 1(mod 5) के समशेष है और 4 को विभाजित करती है। इस प्रकार हम पाते हैं कि संख्या 1 है। अतः G का सीलो 5-उपसमूह G में प्रसामान्य है, और यही इच्छित उपसमूह है।

E 10) $o(\mathbf{Z}_{24}) = 24 = 2^3 \times 3$.
$\therefore$ $\mathbf{Z}_{24}$ का एक सीलो 2-उपसमूह और एक सीलो 3-उपसमूह है। सीलो 2-उपसमूहों की संख्या 1 या 3 है और सीलो 3-उपसमूहों की संख्या 1 या 4 है। अब, यदि $\mathbf{Z}_{24}$ का केवल 1 सीलो 2-उपसमूह हो, तो इसमें समूह के 8 अवयव हैं। इस प्रकार, कोटि 3 वाले 16 अवयव बचते हैं। परन्तु यह संभव नहीं है, क्योंकि हमारे पास अधिक से अधिक 4 अलग-अलग सीलो 3-उपसमूह (अर्थात् कोटि 3 वाले 8 अवयव) हो सकते हैं। इस तरह हमें एक अंतर्विरोध प्राप्त होता है।
$\therefore$ $\mathbf{Z}_{24}$ के 3 सीलो 2-उपसमूह होने चाहिए। और तब इसका केवल 1 सीलो 3-उपसमूह होगा। ये ही $\mathbf{Z}_{24}$ के सभी सीलो p-उपसमूह हैं।

E 11) $255 = 3 \times 15 \times 17 = 5 \times 51$.
सीलो 5-उपसमूहों की संख्या 1 (mod 5) के समशेष है और यह 51 को विभाजित करेगी। इस तरह यह 1 या 51 है।
क्योंकि $255 = 3 \times 85$, इसलिए G के सीलो 3-उपसमूहों की संख्या 1 (mod 3) के समशेष है और यह 85 को विभाजित करेगी।
इस तरह, यह 1 या 85 है।

E 12) यहां हम प्रमेय 10 लागू कर सकते हैं।

E 13) प्रमेय 12 लागू करने पर हम पाते हैं कि

i) $o(G) = 4 \implies G \simeq \mathbf{Z}_4$ या $G \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$.

ii) $o(G) = 9 \implies G \simeq \mathbf{Z}_9$ या $G \simeq \mathbf{Z}_3 \times \mathbf{Z}_3$.

शब्दावली

अनुलोम गुणनफल	direct product
अष्टि	kernel
आंतर स्वाकारिता	inner automorphism
आंतरिक अनुलोम गुणनफल	internal direct product
आविष्टि प्रतिचित्र	inclusion map
एकांतर समूह	alternating group
केन्द्रक	centroid
कौशी	Cauchy
क्रमचय	permutation
क्रमविनिमयक	commutator
घूर्णन	rotation
चक्रीय	cyclic
चक्रीय वियोजन	cyclic decomposition
चिह्नक	signature
चिह्न फलन	sign function
तुल्याकारिता	isomorphism
तुल्याकारी	isomorphic
द्वितल समूह	dihedral group
पक्षांतरण	transposition
परावर्तन	reflection
प्रसामान्य उपसमूह	normal subgroup
प्राकृतिक समाकारिता	natural homomorphism
प्रेरित	induced
बाह्य अनुलोम गुणनफल	external direct product
वर्ग	square
विभाग समूह	quotient group
विषम संख्या	odd number
शीर्ष लंब	altitude
संकुचन	restriction
संयुग्मी	conjugate
समबाहु त्रिभुज	equilateral triangle
सममित समूह	symmetric group
सम संख्या	even number
समाकारिता	homomorphism
समाकारी	homomorphic
सहचारिता	associativity
सीलो	Sylow
स्वाकारिता	automorphism

NOTES

उत्तर प्रदेश
राजर्षि टण्डन मुक्त विश्वविद्यालय

UGMM – 06
अमूर्त बीजगणित

खंड

3

प्रारंभिक वलय सिद्धांत

खंड 3 प्रारंभिक वलय सिद्धांत

इस पाठ्यक्रम के पहले दो खंडों में हमने समूह सिद्धांत के विभिन्न पहलुओं से आपको परिचित कराया है। इस खंड की तीन इकाइयों में हम एक अन्य बीजीय संरचना से आपको परिचित कराएंगे। इस संरचना में एक समुच्चय होता है और उस पर परिभाषित दो द्वि-आधारी संक्रियाएँ होती हैं। यदि ऐसा निकाय कुछ अभिगृहीतों (axioms) को संतुष्ट करता हो, जिन्हें हमने इकाई 9 में दिया है, तो हम इसे वलय कहेंगे।

गणितज्ञ रिचर्ड डेडेकिण्ड (1831-1916) और लियोपोल्ड क्रॉनेकर (1823-1891) ने सबसे पहले वलय की संकल्पना प्रस्तुत की। क्रॉनेकर ने इस प्रकार के निकाय को "कोटि" कहा था। अमूर्त वलय की जो परिभाषा आज दी जा रही है, एमी नोयथर की देन लगती है। उन्होंने 1921 में प्रकाशित अपने शोध पत्र में इसका काफ़ी प्रयोग किया था।

इस खंड को पढ़ते समय आप देखेंगे कि वलय एक आबेली समूह है, जिसमें कुछ विशेष गुण भी हैं। आप देखेंगे कि समूह सिद्धांत की अनेक संकल्पनाओं के अनुरूप वलय सिद्धांत में होते हैं। इसलिए समूहों के बारे में जो कुछ भी आपने पढ़ा है, वह इस खंड तथा अगले खंड का अध्ययन करते समय सहायक सिद्ध होगा।

हम वलय सिद्धांत का प्रस्तुतीकरण ठीक उसी तरह करेंगे जैसे हमने आपको समूह सिद्धांत से परिचित कराने के लिए किया था। सबसे पहले हम विभिन्न प्रकार के वलयों की परिभाषा देंगे। इसके बाद हम आपको उपवलयों (जो कि उपसमूहों के अनुरूप हैं) और गुणजावलियों (जो कि प्रसामान्य उपसमूहों के अनुरूप हैं) से परिचित कराएँगे। इकाई 5 की तरह इससे हमें विभाग समूहों के अनुरूप विभाग वलय प्राप्त होंगे। इस खंड की अंतिम इकाई में हम वलय समाकारिताओं और तुल्याकारिताओं पर चर्चा करेंगे। आप देखेंगे कि समूहों से संबंधित अति उपयोगी तुल्याकारिता प्रमेयों के अनुरूप वलय सिद्धांत में लागू होते हैं। इनसे हमें वलयों की संरचना का विश्लेषण करने में बहुत सहायता मिलती है।

पिछले खंडों की तरह इस खंड में भी हमने अनेक उदाहरण और प्रश्न दिए हैं जिससे आप पाठ्य सामग्री को आसानी से समझ सकें। इकाई में दिए गए प्रश्नों का उतना ही महत्व है जितना कि शेष पाठ्य सामग्री का। इसलिए जब भी आप किसी प्रश्न पर पहुँचते हैं, आप उसे हल करके ही आगे बढ़ें।

संकेत और प्रतीक

$a \equiv b \pmod{n}$	a और b समशेष हैं माड्यूलो n
$\wp(X)$	X के सभी उपसमुच्चयों का समुच्चय
$A \triangle B$	$(A \setminus B) \cup (B \setminus A)$
R/I	I के सापेक्ष R का विभाग वलय
$< a >$	a द्वारा जनित मुख्य गुणजावली
$< a_1, \ldots\ldots, a_n >$	$a_1, a_2, \ldots\ldots, a_n$ द्वारा जनित गुणजावली
$\operatorname{Ker} f$	समाकारिता f के अष्टि
$\simeq$	के तुल्याकारी है

आभार
डॉ॰ माणिक पटवर्धन और डॉ॰ सुजाता वर्मा को उनके सुझावों के लिए।

इकाई 9 वलय

इकाई की रूपरेखा

9.1 प्रस्तावना

इस इकाई के साथ हम ऐसे बीजीय निकायों का अध्ययन शुरू करते हैं जिन पर कुछ गुणों को संतुष्ट करने वाली दो द्वि-आधारी संक्रियाएं परिभाषित हैं। Z, Q और R इस प्रकार के निकाय के उदाहरण हैं। इस निकाय को हम वलय कहेंगे।

अब, आप जानते हैं कि दोनों योग और गुणन Z पर द्वि-आधारी संक्रियाएं हैं। आप यह भी जानते हैं कि योग के सापेक्ष Z एक आबेली समूह है। हालांकि गुणन के सापेक्ष यह एक आबेली समूह नहीं है, Z में गुणन साहचर्य होता है। साथ ही, योग और गुणन निम्नलिखित बंटन — नियमों से संबंधित हैं :

$a(b + c) = ab + ac$, और
$(a + b)c = ac + bc$
$\forall a, b, c \in Z$.

हम द्वि-आधारी संक्रियाओं के इन्हीं गुणों को किसी भी वलय की परिभाषा देने के लिए व्यापक रूप में प्रस्तुत करेंगे। यह परिभाषा सुप्रसिद्ध बीजगणितज्ञ एमी नोयथर की देन है।

चित्र 1 : एमी नोयथर (1882-1935)

वलयों को परिभाषित करने के बाद हम वलयों के अनेक उदाहरण देंगे। हम परिभाषा से ही प्राप्त वलयों के कुछ परिभाषित गुण भी बताएंगे। अंत में हम वलय पर परिभाषित 'गुणन' पर और अधिक प्रतिबंध लागू करने पर प्राप्त कुछ प्रकार के वलयों की चर्चा करेंगे।

जैसा कि इस इकाई के विषयों से पता चलता है, यह इकाई इस पाठ्यक्रम के शेष अध्ययन की बुनियाद है। अतः यह आवश्यक है कि अगली इकाई को शुरू करने से पहले आप नीचे दिए गए उद्देश्यों को पढ़ ले।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- वलय की परिभाषा और उदाहरण दे सकेंगे;
- वलय के पारिभाषिक अभिगृहीतों से वलय के कुछ प्रारंभिक गुण प्राप्त कर सकेंगे;
- क्रमविनिमेय वलय, तत्समकी वलय और तत्समकी क्रमविनिमेय वलय की परिभाषा और उदाहरण दे सकेंगे।

9.2 वलय क्या है ?

आप पूर्णांक समुच्चय Z से परिचित हैं ही। आप यह भी जानते है कि योग के सापेक्ष यह एक समूह है। क्या यह गुणन के सापेक्ष भी एक समूह है ? नहीं। परन्तु गुणन साहचर्य है और योग पर बंटित होता है। पूर्णांकों के योग और गुणन के इन गुणों के कारण हम कहते हैं कि निकाय (Z, +, .) एक वलय है। लेकिन वलय से हम क्या समझते है ?

परिभाषा : किसी भी अरिक्त समुच्चय R को, जिस पर दो द्वि-आधारी संक्रियाएं योग (+) और गुणन (·) परिभाषित हैं, हम **वलय** कहेंगे यदि वह निम्नलिखित अभिगृहीतों को संतुष्ट करे :

R1) R के सभी a, b के लिए
$a+b = b+a$,
अर्थात् योग क्रमविनिमेय है।

R2) R के सभी a, b, c के लिए
$(a+b)+c = a+(b+c)$,
अर्थात् योग साहचर्य है।

R3) R में एक अवयव है (जिसे 0 से प्रकट करते हैं) जिससे कि R के सभी a के लिए
$a+0 = a = 0+a$,
अर्थात् R का एक योज्य तत्समक है।

R4) R के प्रत्येक a के लिए R में एक अवयव x है जिससे कि $a + x = 0 = x + a$, अर्थात् R के प्रत्येक अवयव का एक योज्य प्रतिलोम होता है।

R5) R के सभी a, b, c के लिए
$(a.b).c = a.(b.c)$,
अर्थात् गुणन साहचर्य है।

R6) R के सभी a, b, c के लिए
$a.(b+c) = a.b+a.c$, और
$(a+b).c = a.c + b.c$,
अर्थात् बांयी ओर से तथा दांयी ओर से गुणन योग पर बंटित होता है।

R1 से R4 तक के अभिगृहीतों के अनुसार (R, +) एक आबेली समूह है। अभिगृहीत R5 के अनुसार गुणन साहचर्य है। अतः हम कह सकते हैं कि निकाय (R, +, .) एक वलय होता है यदि

i) (R, +) एक आबेली समूह हो,
ii) (R, .) एक सामिसमूह (semi-group) हो, और
iii) R के सभी a, b, c के लिए

$a.(b+c) = a.b+a.c$, और
$(a+b).c = a.c+b.c$

इकाई 2 से आप जानते हैं कि योज्य तत्समक 0 अद्वितीय होता है और R के प्रत्येक अवयव a का एक अद्वितीय योज्य प्रतिलोम होता है, जिसे $-a$ से प्रकट करते हैं। हम अवयव 0 को वलय का **शून्य अवयव** कहते हैं।

प्रथानुसार, हम $a+(-b)$ को $a-b$ लिखते हैं।

आइए अब हम वलयों के कुछ उदाहरणों पर विचार करें। आप देख चुके हैं कि **Z** एक वलय है। लेकिन, क्या समुच्चय **Q** और **R** वलय हैं? क्या (**Q**, +, .) और (**R**, +, .) R1 से R6 तक के अभिगृहीतों को संतुष्ट करते हैं? हां, करते हैं। इसलिए ये निकाय वलय हैं।

नीचे दिए गए उदाहरण से हमें वलयों के अनेक उदाहरण प्राप्त होते हैं।

उदाहरण 1 : दिखाइए कि (n**Z**, +, .) एक वलय है, जहां $n \in \mathbf{Z}$.

हल : आप जानते हैं कि $n\mathbf{Z} = \{nm \mid m \in \mathbf{Z}\}$
योग के सापेक्ष एक आबेली समूह है। आप यह भी जानते हैं कि n**Z** में गुणन साहचर्य होता है और दांयी ओर से तथा बांयी ओर से योग पर बंटित होता है। अतः साधारण योग और गुणन के सापेक्ष n**Z** एक वलय है।

वलय (R, +, .) का **अधःस्थ समुच्चय** R है।

अभी तक हमने जो **उदाहरण** लिए हैं वे **अनंत वलय** थे, अर्थात् उनके अधःस्थ समुच्चय (underlying sets) अनंत समुच्चय थे। आइए अब हम एक परिमित वलय पर विचार करें, अर्थात् ऐसे वलय (R, +, .) पर जहां R एक परिमित समुच्चय है। यहां हमारा उदाहरण समुच्चय $\mathbf{Z}_n$ है जिसका अध्ययन आप इकाई 2 (भाग 2.5.1) में कर चुके हैं। आइए हम अवशेष वर्ग माड्यूलो n के समुच्चय $\mathbf{Z}_n$ की रचना को संक्षेप में दोहरा लें।

पूर्णांकों a और b के लिए हम कहते हैं कि a और b समशेष (congruent) हैं, माड्यूलो n यदि $a - b$ पूर्णांक n से विभाज्य हो: प्रतीकों में $a \equiv b \pmod n$ यदि $n \mid a - b$. संबंध 'समशेषता माड्यूलो n' **Z** में एक तुल्यता संबंध होता है। पूर्णांक a वाला तुल्यता वर्ग

$$\begin{aligned}\bar{a} &= \{b \in \mathbf{Z} \mid a-b, \text{ n से विभाज्य है}\} \\ &= \{a+mn \mid m \in \mathbf{Z}\}\end{aligned}$$

होता है।

इसे **माड्यूलो n,a का समशेपता वर्ग** (congruence class) या **माड्यूलो n,a का अवशेष वर्ग** (residue class) **कहते हैं। सभी तुल्यता वर्गों के समुच्चय को $\mathbf{Z}_n$ से प्रकट करते हैं।**

अतः $\mathbf{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

हम वर्गों के योग और गुणन को उनके प्रतिनिधियों के पदों में निम्न प्रकार से परिभाषित करते हैं :

$\bar{a} + \bar{b} = \overline{a+b}$, और

$\bar{a}.\bar{b} = \overline{ab}\ \ \forall\ \bar{a}, \bar{b} \in Z_n$.

भाग 2.5.1 में आपने देखा है कि ये संक्रियाएं Z_n में सुपरिभाषित हैं। Z_n में जोड़ और गुणा करने के अभ्यास के लिए आप Z_5 के लिए निम्नलिखित केली सारणियों पर विचार करें।

Z_5 में जोड़

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Z_5 में गुणा

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

उपरोक्त को पढ़ने के बाद आइए अब हम परिमित वलय पर विचार करें।

उदाहरण 2 : दिखाइए कि $(Z_n, +, .)$ एक वलय है।

हल : आप जानते हैं कि $(Z_n, +)$ एक आबेली समूह है, और Z_n में गुणन साहचर्य है। हमें देखना है कि अभिगृहीत R6 संतुष्ट होता है कि नहीं।

किन्हीं $\bar{a}, \bar{b}, \bar{c}, \in Z_n$ के लिए

$$\begin{aligned}\bar{a}.(\bar{b}+\bar{c}) &= \overline{a.(b+c)}\\ &= \overline{a.b + a.c}\\ &= \overline{a.b} + \overline{a.c}\\ &= \bar{a}.\bar{b} + \bar{a}.\bar{c}.\end{aligned}$$

इस तरह $\bar{a}.(\bar{b}+\bar{c}) = \bar{a}.\bar{b} + \bar{a}.\bar{c}$.

इसी प्रकार $(\bar{a}+\bar{b}).\bar{c} = \bar{a}.\bar{c} + \bar{b}.\bar{c}\ \ \forall\ \bar{a}, \bar{b}, \bar{c} \in Z_n$.

अतः $(Z_n, +, \cdot)$, R1 से R6 तक के अभिगृहीतों को संतुष्ट करता है। अतः यह एक वलय है।

अब आप इस प्रश्न को हल कीजिए।

E1) Z_6^* में अर्थात् Z_6 के शून्येतर अवयवों के समुच्चय में, योग और गुणन की केली सारणियां लिखिए। क्या $(Z_6^*, +, \cdot)$ एक वलय है ? क्यों ?

आइए अब हम एक ऐसा वलय लें जिसका आधारस्थ समुच्चय C का एक उपसमुच्चय है।

उदाहरण 3 : समुच्चय

$Z + iZ = \{m + in \mid m$ और n पूर्णांक हैं $\}$

लीजिए, जहां $i^2 = -1$.

हम $Z + iZ$ में + और · को संमिश्र संख्याओं पर परिभाषित सामान्यतः योग और गुणन ही लेते हैं। इस तरह $Z + iZ$ में $m+in$ और $s+it$ के लिए

$(m+in) + (s+it) = (m+s) + i(n+t)$, और

$(m+in).(s+it) = (ms-nt) + i(mt+ns)$.

सत्यापित कीजिए कि सम योग और गुणन के सापेक्ष $\mathbf{Z}+i\mathbf{Z}$ एक वलय है। (इस वलय को गाउसीय पूर्णांकों (Gaussian integers) का वलय कहते हैं जो कि गणितज्ञ कार्ल फ्रेड्रिक गाउस के नाम पर रखा गया है।).

हल : सत्यापित कीजिए कि $(\mathbf{Z}+i\mathbf{Z},+)$, $(\mathbf{C},+)$ का एक उपसमूह है। इस तरह, R1 से R4 तक के अभिगृहीत संतुष्ट हो जाते हैं। आप यह भी सत्यापित कर सकते हैं कि

$$((a+ib).(c+id)).(m+in) = (a+ib).((c+id).(m+in))$$
$$\forall\, a+ib,\ c+id,\ m+in \in \mathbf{Z}+i\mathbf{Z}.$$

इससे यह पता चलता है कि R5 भी संतुष्ट हो जाता है।

अंत में आप सत्यापित कर सकते हैं कि दक्षिण बंटन नियम लागू होता है, अर्थात् किन्हीं $a+ib$, $c+id$, $m+in \in \mathbf{Z}+i\mathbf{Z}$ के लिए

$$((a+ib)+(c+id)).(m+in) = (a+ib).(m+in)+(c+id).(m+in).$$

इसी प्रकार आप सत्यापित कर सकते हैं कि $\mathbf{Z}+i\mathbf{Z}$ में वाम बंटन नियम लागू होता है। अतः $(\mathbf{Z}+i\mathbf{Z},+,\cdot)$ एक वलय है।

अगला उदाहरण इकाई 2 के उदाहरण 8 से संबंधित है। इसमें हम जिन संक्रियाओं को लेते हैं वे सामान्य योग और गुणन संक्रियाएं नहीं हैं।

उदाहरण 4 : मान लीजिए X एक अरिक्त समुच्चय है, $\wp(X)$, X के सभी उपसमुच्चयों का संग्रह है और $\triangle$ सममित अंतर (symmetric difference) संक्रिया को प्रकट करता है। दिखाइए कि $(\wp(X), \triangle, \cap)$ एक वलय है।

हल : X के किन्हीं दो उपसमुच्चयों A और B के लिए $A\triangle B = (A\setminus B) \cup (B\setminus A)$.

इकाई 2 के उदाहरण 8 में हमने दिखाया है कि $(\wp(X), \triangle)$ एक आबेली समूह है। आप यह भी जानते हैं कि $\cap$ साहचर्य है। आइए अब हम देखें कि $\triangle$ पर $\cap$ बंटित है कि नहीं।

मान लीजिए $A, B, C \in \wp(X)$. तब

$$\begin{aligned} A\cap(B\triangle C) &= A\cap[(B\setminus C)\cup(C\setminus B)] \\ &= [A\cap(B\setminus C)]\cup[A\cap(C\setminus B)] \quad (\text{क्योंकि } \cap, \cup \text{ पर बंटित है।}) \\ &= [(A\cap B)\setminus(A\cap C)]\cup[(A\cap C)\setminus(A\cap B)] \quad (\text{क्योंकि } \cap, \text{ पूरकीकरण पर बंटित है।}) \\ &= [(A\cap B)\ \triangle\ (A\cap C)] \end{aligned}$$

अतः वाम बंटन नियम लागू होता है।

और, $(B\triangle C)\cap A = A\cap(B\triangle C)$, क्योंकि $\cap$ क्रमविनिमेय है।

$$\begin{aligned} &= (A\cap B)\ \triangle\ (A\cap C) \\ &= (B\cap A)\ \triangle\ (C\cap A). \end{aligned}$$

इस तरह, दक्षिण बंटन नियम भी लागू होता है।

अतः $(\wp(X),\triangle,\cap)$ एक वलय है।

अभी तक आपने वलय के ऐसे उदाहरण देखे हैं जिनमें वलय पर परिभाषित दोनों संक्रियाएं क्रमविनिमेय रही हैं। यह बात अगले उदाहरण में नहीं है।

उदाहरण 5 : समुच्चय

$$\mathbf{M_2(R)} = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \middle|\ a_{11}, a_{12}, a_{21} \text{ और } a_{22} \text{ वास्तविक संख्याएँ हैं} \right\}$$

लीजिए। दिखाइए कि $\mathbf{M_2(R)}$ आव्यूहों के योग और गुणन के सापेक्ष एक वलय है।

हल : जिस तरह हमने इकाई 3 के उदाहरण 2 को हल किया है, उसी तरह आप सत्यापित कर सकते हैं कि $(\mathbf{M_2(R)},+)$ एक आबेली समूह है। आप गुणन के साहचर्य गुण को भी सत्यापित कर सकते हैं। (इकाई 2 के उदाहरण 5 को भी देखिए।) अब हम दिखाएंगे कि $\mathbf{M_2(R)}$ के A, B, C के लिए

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

$$A.(B+C) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \left(\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} \right)$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11}+c_{11} & b_{12}+c_{12} \\ b_{21}+c_{21} & b_{22}+c_{22} \end{bmatrix}.$$

$$= \begin{bmatrix} a_{11}(b_{11}+c_{11}) + a_{12}(b_{21}+c_{21}), & a_{11}(b_{12}+c_{12}) + a_{12}(b_{22}+c_{22}) \\ a_{21}(b_{11}+c_{11}) + a_{22}(b_{21}+c_{21}) & a_{21}(b_{12}+c_{12}) + a_{22}(b_{22}+c_{22}) \end{bmatrix}$$

$$= \begin{bmatrix} (a_{11}b_{11}+a_{12}b_{21}) + (a_{11}c_{11}+a_{12}c_{21}) & (a_{11}b_{12}+a_{12}b_{22}) + (a_{11}c_{12}+a_{12}c_{22}) \\ (a_{21}b_{11}+a_{22}b_{21}) + (a_{21}c_{11}+a_{22}c_{21}) & (a_{21}b_{12}+a_{22}b_{22}) + (a_{21}c_{12}+a_{22}c_{22}) \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{bmatrix} \begin{bmatrix} a_{11}c_{11}+a_{12}c_{21} & a_{11}c_{12}+a_{12}c_{22} \\ a_{21}c_{11}+a_{22}c_{21} & a_{21}c_{12}+a_{22}c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

$= A.B. + A.C.$

इसी प्रकार हम दूसरा वंटन नियम, अर्थात्

$(A+B).C = A.C+B.C \quad \forall A, B, C \in M_2(R)$ प्राप्त कर सकते हैं।

इस तरह, आव्यूह योग और आव्यूह गुणन के सापेक्ष $M_2(R)$ एक वलय है।

ध्यान दीजिए कि $M_2(R)$ पर गुणन क्रमविनिमेय नहीं है। अतः हम यह नहीं कह सकते हैं कि यदि वाम वंटन नियम लागू होता हो तो दक्षिण वंटन नियम भी लागू होगा।

अब आप नीचे दिए गए प्रश्नों को हल कीजिए।

E2) दिखाइए कि वास्तविक संख्याओं के योग और गुणन के सापेक्ष समुच्चय
$Q + \sqrt{2}\,Q = \{p + \sqrt{2}\,q \mid p, q \in Q\}$ एक वलय है।

E3) मान लीजिए $R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| \right.$ a, b वास्तविक संख्याएं हैं $\left.\right\}$

दिखाइए कि आव्यूह योग और आव्यूह गुणन के सापेक्ष R एक वलय है।

E4) मान लीजिए $R = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \middle| \right.$ a, b वास्तविक संख्याएं हैं $\left.\right\}$

सिद्ध कीजिए कि आव्यूह योग और आव्यूह गुणन के सापेक्ष R एक वलय है।

E5) $(\wp(X), \cup, \cap)$ वलय क्यों नहीं है ?

आइए अब हम ऐसे वलयों पर विचार करें जिनके अवयव फलन हैं।

उदाहरण 6 : संवृत अंतराल [0,1] पर परिभाषित सभी संतत वास्तविक मान फलनों वाला वर्ग लीजिए। हम इस वर्ग को C[0,1] से प्रकट करते हैं। यदि f और g अंतराल [0,1] पर दो संतत फलन हों, तो हम f+g और fg को निम्न-रूप से परिभाषित करते हैं :

प्रत्येक $x \in [0,1]$ के लिए

$(f+g)(x) = f(x)+g(x)$ (अर्थात् बिंदुशः योग)

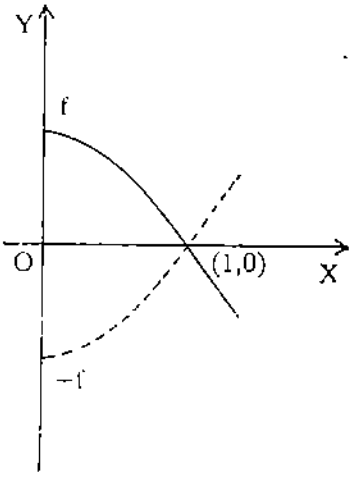
और $(f.g)(x) = f(x).g(x)$ (अर्थात् बिंदुशः गुणन)

कलन पाठ्यक्रम से आप जानते हैं कि अंतराल $[0,1]$ पर फलन $f+g$ और fg परिभाषित और संतत होते हैं, अर्थात् यदि f और $g \in C[0,1]$ तो $f+g$ और fg दोनों ही $C[0,1]$ में होते हैं। दिखाइए कि $+$ और $\cdot$ के सापेक्ष $C[0,1]$ एक वलय है।

हल : क्योंकि **R** में योग साहचर्य और क्रमविनिमेय होता है, इसलिए $C[0,1]$ में योग साहचर्य और क्रमविनिमेय होगा। $C[0,1]$ का योज्य तत्समक शून्य फलन है। $f \in C[0,1]$ का योज्य प्रतिलोम $(-f)$ है, जहां $(-f)(x) = -f(x)$ $\forall\, x \in [0,1]$. $(-f)$ के चित्रीय निरूपण के लिए चित्र 2 देखिए। इस तरह $(C[0,1], +)$ एक आवेली समूह है। साथ ही, क्योंकि **R** में गुणन साहचर्य है, इसलिए $C[0,1]$ में गुणन साहचर्य होगा।

आइए अब हम देखें कि अभिगृहीत R6 लागू होता है कि नहीं।

$f.(g+h) = f.g + f.h$ को सिद्ध करने के लिए हम $[0,1]$ में किसी x के लिए $[f.(g+h)](x)$ लेते हैं।



चित्र 2

अब,

$$
\begin{aligned}
(f.(g+h))(x) &= f(x)\,(g+h)(x) \\
&= f(x)(g(x) + h(x)) \\
&= f(x)\,g(x) + f(x)\,h(x), \text{ क्योंकि } \mathbf{R} \text{ में } .\,,+ \text{ पर बंटित होता है।} \\
&= (f.g)(x) + (f.h)(x) \\
&= (f.g + f.h)(x)
\end{aligned}
$$

अतः $f.(g+h) = f.g + f.h$.

चूंकि $C[0,1]$ में गुणन क्रमविनिमेय है, इसलिए दूसरा बंटन नियम भी लागू होता है। इस तरह, $C[0,1]$, R6 को संतुष्ट करता है। अतः $(C[0,1], +, .)$ एक वलय है।

इस वलय को **[0.1] पर संतत फलनों का वलय** कहते हैं।

अगला उदाहरण भी फलनों से संबंधित है।

समूह G की **अंतराकारिता** (endomorphism) G से G पर एक समाकारिता होती है।

उदाहरण 7 : मान लीजिए $(A, +)$ एक आवेली समूह है। A की सभी अंतराकारिताओं का समुच्चय है

$\text{End } A = \{ f : A \to A \mid f(a+b) = f(a) + f(b)\ \forall\, a, b \in A \}$.

$f, g \in \text{End } A$ के लिए हम $f+g$ और $f.g$ को निम्न प्रकार से परिभाषित करते हैं :

$$
\left.
\begin{aligned}
(f+g)(a) &= f(a) + g(a), \text{ और} \\
(f.g)(a) &= f \circ g\,(a) = f(g(a))\ \forall\, a \in A
\end{aligned}
\right\} \cdots\cdots\cdots\cdots (1)
$$

दिखाइए कि $(\text{End } A, +, .)$ एक वलय है। (इस वलय को A का **अंतराकारिता वलय** कहते हैं।)

हल : आइए पहले हम देखें कि (1) द्वारा परिभाषित $+$ और $.$, End A पर द्वि-आधारी संक्रियाएं हैं कि नहीं।

सभी $a, b \in A$ के लिए

$$
\begin{aligned}
(f+g)(a+b) &= f(a+b) + g(a+b) \\
&= (f(a)+f(b)) + (g(a)+g(b)) \\
&= (f(a)+g(a)) + (f(b)+g(b)) \\
&= (f+g)(a) + (f+g)(b), \text{ और}
\end{aligned}
$$

$$
\begin{aligned}
(f.g)(a+b) &= f(g(a+b)) \\
&= f(g(a) + g(b)) \\
&= f(g(a)) + f(g(b)) \\
&= (f.g)(a) + (f.g)(b)
\end{aligned}
$$

इस तरह $f+g$ और $f.g \in \text{End } A$.

आइए अब हम देखें कि $(\text{End } A, +, .)$ R1 से R6 तक के अभिगृहीतों को संतुष्ट करता है कि नहीं।

चूंकि आवेली समूह A में $+$ साहचर्य और क्रमविनिमेय है, इसलिए End A में भी $+$ साहचर्य और क्रमविनिमेय होगा। A पर शून्य समाकारिता End A का योज्य प्रतिलोम है। $(-f)$, $f \in \text{End } A$ का योज्य प्रतिलोम है। इस तरह, $(\text{End } A, +)$ एक आवेली समूह है।

आप यह भी जानते हैं कि फलनों का संयोजन End A पर एक साहचर्य संक्रिया है।

अंत में यह देखने के लिए कि R6 संतुष्ट होता है कि नहीं हम किन्हीं $f, g, h \in \text{End } A$ के लिए $f.(g+h)$ पर विचार करते हैं।

अब, किसी $a \in A$ के लिए

$$\begin{aligned}[f.(g+h)](a) &= f((g+h)(a)) \\ &= f(g(a)+h(a)) \\ &= f(g(a))+f(h(a)) \\ &= (f.g)(a)+(f.h)(a) \\ &= (f.g+f.h)(a)\end{aligned}$$

$\therefore f.(g+h) = f.g + f.h.$

इसी प्रकार हम सिद्ध कर सकते हैं कि

$(f+g).h = f.h + g.h.$

इस तरह, End A, R1 से R6 तक के अभिगृहीतों को संतुष्ट करता है। अतः (End A, +, .) एक वलय है।

ध्यान दीजिए कि . क्रमविनिमेय नहीं है, क्योंकि यह आवश्यक नहीं है कि सभी $f, g \in$ End A के लिए $f \circ g$, $g \circ f$ के बराबर हो।

अब आप इन प्रश्नों को हल करने की कोशिश कीजिए।

E6) मान लीजिए X एक अरिक्त समुच्चय है और (R, +, .) एक वलय है। X से R तक के सभी फलनों का समुच्चय
Map (X, R) लीजिए। अर्थात्
$Map(X,R) = \{f \mid f: X \to R\}$.
बिंदुशः योग और बिंदुशः गुणन से Map(X, R) में + और. परिभाषित कीजिए। दिखाइए कि (Map (X, R), +, .) एक वलय है।

E7) दिखाइए कि वास्तविक संख्याओं का समुच्चय **R** निम्नलिखित प्रकार से परिभाषित योग और गुणन के सापेक्ष एक वलय है : सभी $a, b \in \mathbf{R}$ के लिए
$a \oplus b = a + b + 1$, और
$a \odot b = a.b + a + b$,
जहां + और . वास्तविक संख्याओं के सामान्य योग और गुणन को प्रकट करते हैं।

E7 को हल करने पर आपने इस बात की ओर अवश्य ध्यान दिया होगा कि एक दिया हुआ समुच्चय अनेक अलग-अलग वलयों का अधःस्थ समुच्चय हो सकता है।

आइए अब हम वलयों के कार्तीय गुणनफल पर विचार करें।

उदाहरण 8 : मान लीजिए (A, +, .) और, (B, $\boxplus$, $\boxdot$) दो वलय हैं। दिखाइए कि निम्न प्रकार से परिभाषित $\oplus$ और * के सापेक्ष इनका कार्तीय गुणनफल $A \times B$ एक वलय है :
$A \times B$ के सभी $(a, b), (a', b')$ के लिए $(a,b) \oplus (a',b') = (a+a', b \boxplus b')$ और
$(a, b) * (a', b') = (a . a', b \boxdot b')$.

हल : हमने $A \times B$ में योग और गुणन को संगत घटकों के योग और गुणन से परिभाषित किया है। $A \times B$ का शून्य अवयव (0,0) है। (a,b) का योज्य प्रतिलोम $(-a, \boxminus b)$ है, जहां $\boxminus b$, $\boxplus$ के सापेक्ष b के प्रतिलोम को प्रकट करता है।

क्योंकि A और B में गुणन साहचर्य होते हैं, इसलिए $A \times B$ में * साहचर्य होगा। और इस बात को प्रयोग करके कि A और B पर R6 लागू होता है, हम दिखा सकते हैं कि $A \times B$ पर R6 लागू होता है। इस तरह, हम पाते हैं कि $(A \times B, \oplus, *)$ एक वलय है।

यदि आप इस उदाहरण को समझ गए हैं तो आप नीचे दिए गए प्रश्न को हल कर सकेंगे।

E8) $Z_2 \times Z_3$ की योग सारणी और गुणन सारणी लिखिए।

आगे बढ़ने से पहले हम संकेत परंपरा के बारे में एक टिप्पणी देना चाहेंगे। समूहों के संबंध में, सुविधा के लिए हमने (G,) के लिए संकेत G का प्रयोग किया है। यहां भी सुविधा के लिए आगे से हम (R, +, .) के लिए संकेत R का प्रयोग करेंगे। इस तरह, हम मानकर चलेंगे कि + और · ज्ञात हैं। और हम दो वलय अवयवों a और b के गुणनफल $a \cdot b$ के स्थान पर केवल ab लिखेंगे।

तो आइए अब हम वलयों के विभिन्न गुणों का अध्ययन शुरू करें।

9.3 प्रारंभिक गुण

इस भाग में हम वलयों के कुछ सरल लेकिन महत्वपूर्ण गुणों को सिद्ध करेंगे जो कि वलय की परिभाषा ही से प्राप्त हो जाते हैं। अध्ययन के दौरान आपको यह बात हमेशा ध्यान में रखनी चाहिए कि किसी वलय R के लिए (R, +) एक आबेली समूह होता है। अतः पिछली इकाइयों में समूहों के लिए प्राप्त किए गए परिणाम आबेली समूह (R, +) पर लागू होते हैं। विशेष रूप से,

i) शून्य अवयव 0, और किसी अवयव का योज्य प्रतिलोम अद्वितीय होता है।

ii) योग के सापेक्ष निरसन नियम (cancellation law) लागू होता है, अर्थात्

$\forall a, b, c \in R, a+c=b+c \Rightarrow a = b.$

जैसा कि हम पहले बता चुके हैं, हम $a, b \in R$ के लिए $a+(-b)$ के स्थान पर $a-b$ और $a.b$ के स्थान पर ab लिखेंगे।

तो आइए, अब हम मुख्यतः अभिगृहीत R6 से प्राप्त कुछ गुणों पर विचार करें।

प्रमेय 1 : मान लीजिए R एक वलय है। तब, किन्हीं $a, b, c \in R$ के लिए

i) $a0 = 0 = 0a$,

ii) $a(-b) = (-a)b = -(ab)$,

iii) $(-a)(-b) = ab$,

iv) $a(b-c) = ab - ac$, और,

v) $(b-c)a = ba - ca$.

उपपत्ति : i) अब, $0+0=0$

$\Rightarrow a(0+0) = a0$

$\Rightarrow a0+a0=a0$, बंटन नियम लागू करने पर।

$=a0+0$, क्योंकि 0 योज्य तत्समक है।

$\Rightarrow a0 = 0$, $(R, +)$ के निरसन नियम के अनुसार।

इसी प्रकार दूसरा बंटन नियम लागू करके हम दिखा सकते हैं कि $0a = 0$. इस तरह, सभी $a \in R$ के लिए $a0=0=0a$.

ii) योज्य प्रतिलोम की परिभाषा से हम जानते हैं कि $b+(-b)=0$.

अब, $0 = a\,0$, (i) से

$= a(b+(-b))$, क्योंकि $0=b+(-b)$

$= ab + a(-b)$, बंटन नियम के अनुसार।

अब $ab + [-(ab)] = 0$. और $ab + a(-b) = 0$. परन्तु आप जानते हैं कि अवयव का योज्य प्रतिलोम अद्वितीय होता है।

अतः हमें $-(ab) = a(-b)$ प्राप्त होता है।

इसी प्रकार $a + (-a) = 0$ लेकर हम $-(ab)=(-a)b$ प्राप्त कर सकते हैं।

इस तरह, सभी $a, b \in R$ के लिए
$a(-b) = (-a)b = -(ab)$.

iii) $a, b \in R$ के लिए

$(-a)(-b) = -a(-b)$, (ii) से

$= a(-(-b))$, (vi) से

$= ab$, क्योंकि $b, (-b)$ का योज्य प्रतिलोम है।

iv) $a, b, c \in R$ के लिए

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

$= ab+a(-c)$, बंटन नियम के अनुसार।

$= ab+[-(ac)]$, (ii) से

$= ab-ac$.

इसी प्रकार हम (v) सिद्ध कर सकते हैं।

अब आप इन प्रश्नों को हल करने की कोशिश कीजिए.

E9) दिखाइए कि $\{0\}$ सामान्य योग और गुणन के सापेक्ष एक वलय है। (इसे तुच्छ वलय (trivial ring) कहते हैं।) और यह भी दिखाइए कि यदि कोई एकल (singleton) वलय हो, तो वह $\{0\}$ ही होगा।

E10) सिद्ध कीजिए कि यदि वलय R में दोनों संक्रियाएं बराबर होती हैं, (अर्थात् $a+b=ab \ \forall a, b \in R$) तो R तुच्छ वलय होगा।

आइए अब हम वलय के तीन या अधिक अवयवों के योगफल और गुणनफल पर विचार करें। इन्हें हम पुनरावर्ती रूप में परिभाषित करेंगे, जैसा कि हम समूहों के संबंध में कर चुके हैं (देखिए इकाई 2)।

यदि $k(\geq 2)$ एक ऐसा पूर्णांक हो कि वलय R के k अवयवों का योगफल परिभाषित हो, तो हम क्रम में लिए गए R के $(k+1)$ अवयवों $a_1, a_2, \ldots, a_{k+1}$ के योगफल को
$a_1 + \ldots + a_{k+1} = (a_1 + \ldots + a_k) + a_{k+1}$ से परिभाषित करते हैं।

इसी प्रकार यदि k एक ऐसा धन पूर्णांक हो कि R के k अवयवों का गुणनफल परिभाषित हो, तो (क्रम में लिए गए) $(k+1)$ अवयवों $a_1, a_2, \ldots, a_{k+1}$ के गुणनफल को $a_1 . a_2 . \ldots . a_{k+1} = (a_1 . a_2 . \ldots . a_k) . a_{k+1}$ से परिभाषित करते हैं।

जैसे हमने समूहों के लिए किया था, वैसे ही वलयों के लिए भी हम + और · के सापेक्ष घातांक नियम प्राप्त कर सकते हैं। वास्तव में, किसी भी वलय R के लिए निम्नलिखित परिणाम सही हैं।

i) यदि m और n धन पूर्णांक हों और $a \in R$, तो $a^m . a^n = a^{m+n}$, और $(a^m)^n = a^{mn}$.

ii) यदि m और n कोई भी पूर्णांक हों और $a, b \in R$ तो

$(n+m)a = na + ma$,
$(nm)a = n(ma) = m(na)$,
$n(a+b) = na + nb$,
$m(ab) = (ma)\,b = a(mb)$, और
$(ma)\,(nb) = mn\,(ab) = (mna)b$.

iii) यदि $a_1, a_2, \ldots, a_m, b_1, \ldots, b_n \in R$, तो

$(a_1 + \ldots + a_m)(b_1 + \ldots + b_n)$
$= a_1b_1 + \ldots + a_1b_n + a_2b_1 + \ldots + a_2b_n + \ldots + a_mb_1 + \ldots + a_mb_n$

अब आप इस सरल प्रश्न को हल कीजिए।

E11) यदि R एक वलय हो और $a, b \in R$ ऐसे हों कि $ab = ba$, तो $n \in N$ पर आगमन नियम लागू करके निम्नलिखित **द्विपद प्रसार** (binomial expansion) प्राप्त करें।

$$(a+b)^n = a^n + {}^nC_1a^{n-1}b + \ldots + {}^nC_ka^{n-k}b^k + \ldots + {}^nC_{n-1}ab^{n-1} + b^n,$$

जहाँ $${}^nC_k = \frac{n!}{k!\,(n-k)!}.$$

वलय के अनेक अन्य गुण हैं जिन पर हम इस खंड में चर्चा करेंगे। फ़िलहाल हम दो प्रकार के वलयों को ध्यान से देखेंगे। इन्हें इन पर परिभाषित गुणन के व्यवहार के अनुसार वर्गीकृत किया गया है।

9.4 दो प्रकार के वलय

वलय की परिभाषा से हम जानते हैं कि वलय पर परिभाषित द्वि-आधारी संक्रिया गुणन साहचर्य है और, + के साथ, बंटन नियमों को संतुष्ट करता है। गुणन के गुणों के संबंध में इससे अधिक नहीं कहा गया है। यदि हम इस संक्रिया पर कुछ प्रतिबंध लागू करें तो हमें अनेक प्रकार के वलय प्राप्त होते हैं। आइए अब हम आपको दो प्रकार के वलयों से परिचित कराएं।

परिभाषा : हम कहते हैं कि वलय $(R, +, .)$ **क्रमविनिमेय** होता है यदि · क्रमविनिमेय हो, अर्थात् सभी $a, b \in R$ के लिए $ab = ba$.

उदाहरण के लिए, **Z**, **Q** और **R** क्रमविनिमेय वलय हैं।

परिभाषा : हम कहते हैं कि वलय $(R, +, .)$ **तत्समकी वलय** (ring with identity) होता है, यदि गुणन के सापेक्ष R का एक तत्समक अवयव हो, अर्थात् यदि R में एक ऐसे अवयव e का अस्तित्व हो जिससे कि सभी $a \in R$ के लिए $a . e = e . a = a$.

क्या आप इस प्रकार के वलय का उदाहरण दे सकते हैं ? क्या **Z**, **Q** और **R** तत्समकी वलय नहीं हैं ?

अगली परिभाषा पर विचार करने से पहले इस प्रश्न को हल कीजिए।

E12) सिद्ध कीजिए कि यदि गुणन के सापेक्ष वलय R का एक तत्समक अवयव हो, तो यह अद्वितीय होता है। (हम तत्समकी वलय में इस अद्वितीय तत्समक अवयव को प्रतीक 1 से प्रकट करते हैं।)

आइए अब हम पिछली दो परिभाषाओं को मिलाकर देखें।

परिभाषा : एक वलय $(R, +, .)$ को **तत्समकी क्रमविनिमेय वलय** कहते हैं, यदि यह एक क्रमविनिमेय वलय हो और इसमें गुणनात्मक तत्समक अवयव 1 हो।

इस तरह, वलय **Z**, **Q** और **R** तत्समकी क्रमविनिमेय वलय हैं। इन सभी वलयों में पूर्णांक 1 गुणनात्मक तत्समक है।

तत्समकी वलय के गुणनात्मक तत्समक को हम केवल तत्समक कहेंगे।

हम ऐसे भी क्रमविनिमेय वलय प्राप्त कर सकते हैं जो तत्समकी वलय नहीं हैं। उदाहरण के लिए, सभी सम पूर्णांकों का वलय $2\mathbf{Z}$ क्रमविनिमेय है। परंतु इसका कोई गुणनात्मक तत्समक नहीं है।

इसी प्रकार हम तत्समकी वलय प्राप्त कर सकते हैं जो क्रमविनिमेय नहीं हैं। उदाहरण के लिए, $M_2(\mathbf{R})$ का तत्समक $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ है। पर यह क्रमविनिमेय नहीं है। उदाहरण के लिए,

यदि $A = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$ और $B = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix}$, तो

$$AB = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} \text{ और}$$

$$BA = \begin{bmatrix} 0 & 1 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 4 & 0 \end{bmatrix}$$

इस तरह, $AB \neq BA$.

अब आप नीचे दिया गया प्रश्न हल कीजिए।

E13) उदाहरण 1, 2, 3, 4, 5, 6, 7 में दिए गए कौन से वलय क्रमविनिमेय हैं और कौन से तत्समकी हैं ? जहां कहीं भी तत्समक का अस्तित्व हो, उसे प्रस्तुत कीजिए।

अब बताइए कि क्या तुच्छ वलय तत्समकी वलय हो सकता है ? चूँकि $0.0 = 0$, इसलिए इस वलय के लिए 0 गुणनात्मक तत्समक भी है। अतः $(\{0\}, +, .)$ तत्समकी वलय है जिसमें योज्य तत्समक और गुणनात्मक तत्समक समान होते हैं। परंतु यदि R तुच्छ वलय नहीं है, तो हमें निम्नलिखित परिणाम प्राप्त होता है।

प्रमेय 2 : मान लीजिए R तत्समकी वलय है। यदि $R \neq \{0\}$, तो अवयव 0 और 1 अलग-अलग होते हैं।

उपपत्ति : चूंकि $R \neq \{0\}$, $\exists\, a \in R$, $a \neq 0$. अब मान लीजिए $0 = 1$. तब $a = a . 1 = a . 0 = 0$ (प्रमेय 1 के अनुसार)। अर्थात् $a = 0$, जो कि एक अंतर्विरोध है। इस तरह हम जो मानकर चले थे वह सही नहीं है। अर्थात् $0 \neq 1$.

आइए अब हम उदाहरण 8 पर फिर से विचार करें। $A \times B$ किस स्थिति में क्रमविनिमेय होगा ? $A \times B$ क्रमविनिमेय होता है यदि और केवल यदि दोनों वलय A और B क्रमविनिमेय हों। आइए देखें कि ऐसा क्यों है। सुविधा के लिए तीनों वलय A, B और $A \times B$ में संक्रियाओं को + और . से प्रकट करेंगे।

मान लीजिए (a,b) और $(a', b') \in A \times B$.

तब $(a,b).(a',b') = (a',b').(a,b)$

$\Longleftrightarrow (a.a', b.b') = (a'.a, b'.b)$

$\Longleftrightarrow a.a' = a'.a$ और $b.b' = b'.b$.

इस तरह हम पाते हैं कि $A \times B$ क्रमविनिमेय होता है यदि और केवल यदि A और B दोनों ही क्रमविनिमेय वलय हों।

इसी प्रकार हम दिखा सकते हैं कि $A \times B$ तत्समकी वलय होता है यदि और केवल A और B तत्समकी वलय हों। यदि A और B के तत्समक क्रमशः e_1 और e_2 हों तो $A \times B$ का तत्समक (e_1, e_2) होगा।

अब तत्समकी क्रमविनिमेय वलयों से संबंधित कुछ प्रश्न।

E14) दिखाइए कि E7 में दिया गया वलय तत्समकी क्रमविनिमेय वलय है।

E15) दिखाइए कि आव्यूहों का समुच्चय $\left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} \middle| x \in \mathbf{R} \right\}$ तत्समकी क्रमविनिमेय वलय है।

E16) मान लीजिए R एक बूलीय वलय (Boolean ring) है, अर्थात् $a^2 = a \;\forall\; a \in R$. दिखाइए कि $a = -a \;\forall\; a \in R$ और फलस्वरूप R क्रमविनिमेय होगा।

अब हम तत्समकी अ-क्रमविनिमेय वलय का एक महत्वपूर्ण उदाहरण देंगे। यह वास्तविक चतुष्टयियों (quaternions) का वलय है। इसका वर्णन पहले पहल आयरलैण्डवासी गणितज्ञ विलियम रोवन हैमिल्टन (1805-1865) ने किया था। यह वलय ज्यामिति, संख्या सिद्धांत और यांत्रिकी के अध्ययन में एक महत्वपूर्ण भूमिका निभाता है।

उदाहरण 9 : मान लीजिए $\mathbf{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{R}\}$, जहां i, j, k प्रतीक हैं जो संबंध $i^2 = -1 = j^2 = k^2$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$ संतुष्ट करते हैं।

हम **H** में योग और गुणन को निम्न प्रकार से परिभाषित करते हैं :

$(a+bi+cj+dk) + (a_1 + b_1i + c_1j + d_1k) = (a+a_1) + (b+b_1)i + (c+c_1)j + (d+d_1)k$, और

$(a+bi+cj+dk)\,(a_1 + b_1i + c_1j + d_1k) = (aa_1 - bb_1 - cc_1 - dd_1) + (ab_1 + ba_1 + cd_1 - dc_1)i$
$+ (ac_1 - bd_1 + ca_1 + db_1)j + (ad_1 + bc_1 - cb_1 + da_1)k.$

(देखने में यह गुणन जटिल लग सकता है। लेकिन ऐसा नहीं है। इसे i, j और k के संबंधों को ध्यान में रखकर बहुपदों के गुणन की तरह हल करते हैं।)

दिखाइए कि H एक वलय है।

हल : ध्यान दीजिए कि $\{\pm 1, \pm i, \pm j, \pm k\}$ समूह Q_8 है (इकाई 4 का उदाहरण 8)।

अब आप सत्यापित कर सकते हैं कि $(\mathbf{H}, +)$ एक आवेली समूह है जिसमें योज्य तत्समक $0 = 0 + 0i + 0j + 0k$ है, **H** में गुणन साहचर्य है, बंटन नियम लागू होते हैं और $1 = 1 + 0i + 0j + 0k$, **H** में तत्समक है।

क्या आप मानते हैं कि H क्रमविनिमेय वलय नहीं है? याद करें कि, $ij \neq ji$.

इस इकाई में अभी तक हमने विभिन्न प्रकार के वलयों पर चर्चा की है। हमने क्रमविनिमेय और अक्रमविनिमेय वलयों के उदाहरण देखे हैं। हालांकि अक्रमविनिमेय वलय महत्वपूर्ण हैं, परंतु आगे से हम सरलता के लिए केवल क्रमविनिमेय वलयों पर ही विचार करेंगे। इस तरह, आगे से **हमारे लिए वलय का अर्थ होगा क्रमविनिमेय वलय**। याद रखें कि क्रमविनिमेय वलय में + और · दोनों ही क्रमविनिमेय होते हैं।

आइए अब हम संक्षिप्त में देखें कि हमने इस इकाई में क्या किया है।

9.5 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों पर चर्चा की है।

1) वलय की परिभाषा और उदाहरण।
2) वलय के कुछ गुण जैसे वलय R में सभी a, b, c के लिए

   $a \cdot 0 = 0 = 0 \cdot a,$
   $a(-b) = -(ab) = (-a)b,$
   $(-a)(-b) = ab,$
   $a(b-c) = ab - ac,$
   $(b-c)a = ba - ca.$

3) योग और गुणन के लिए घातांक नियम और व्यापकीकृत बंटन नियम।
4) क्रमविनिमेय वलय, तत्समकी वलय और तत्समकी क्रमविनिमेय वलय।

आगे से यदि कोई विशेष उल्लेख न हो तो हम मानकर चलेंगे कि सभी वलय क्रमविनिमेय हैं।

9.6 हल/उत्तर

E1) Z_6^* में योग

+	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Z_6^* में गुणन

.	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

सारणियों से आप देख सकते हैं कि Z_6^* पर न तो योग और न ही गुणन द्वि-आधारी संक्रियाएं हैं, क्योंकि $\bar{0} \notin Z_6^*$. अतः $(Z_6^*, +, .)$ वलय नहीं हो सकता।

E2) हम $Q + \sqrt{2}\,Q$ में योग और गुणन को निम्न प्रकार से परिभाषित करते हैं :

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

$(a+\sqrt{2}\,b) \cdot (c+\sqrt{2}\,d) = (ac+2bd) + \sqrt{2}\,(ad+bc)\ \forall\, a, b, c, d \in Q.$

चूंकि **R** में + साहचर्य और क्रमविनिमेय है, इसलिए $Q + \sqrt{2}\,Q$ में + साहचर्य और क्रमविनिमेय है।

$0 = 0 + \sqrt{2}\,0$ योज्य तत्समक है और $(-a) + \sqrt{2}\,(-b)$, $a + \sqrt{2}\,b$ का योज्य प्रतिलोम है।

चूंकि **R** में गुणन साहचर्य है, इसलिए R5 भी लागू होता है। क्योंकि **R** में योग पर गुणन बंटित होता है, इसलिए यही बात $Q + \sqrt{2}\,Q$ में भी लागू होती है। अतः $(Q + \sqrt{2}\,Q, +, .)$ एक वलय है।

E3) R पर + और . सुपरिभाषित द्वि-आधारी संक्रियाएं हैं। R1, R2, R5 और R6 लागू होते हैं, क्योंकि ये गुण $M_2(R)$ के लिए सही हैं (उदाहरण 5)।

शून्य अवयव $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ है। $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ का योज्य प्रतिलोम $\begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix}$ है।

अतः R एक वलय है।

E4) R पर + और · द्वि-आधारी संक्रियाएं हैं। आप सत्यापित कर सकते हैं कि (R, + , .), R1 से R6 तक के अभिगृहीतों को संतुष्ट करता है।

E5) $\wp(X)$ पर $\cup$ और $\cap$ सुपरिभाषित द्वि-आधारी संक्रियाएं हैं। आइए देखें कि R1 से R6 तक के अभिगृहीतों में से कौन-कौन से अभिगृहीत $(\wp(X), \cup, \cap)$ से संतुष्ट नहीं होते। क्योंकि $\cup$ आबेली है, इसलिए R1 संतुष्ट हो जाता है। क्योंकि $\cup$ साहचर्य है, इसलिए R2 संतुष्ट हो जाता है। और, किसी $A \subseteq X$ के लिए $A \cup \phi = A$. अतः $\cup$ के सापेक्ष ϕ तत्समक है।

इस तरह, R3 संतुष्ट हो जाता है। अब, किसी भी $A \subseteq X$, $A \neq \phi$ के लिए ऐसा कोई $B \subseteq X$ नहीं है जिससे कि $A \cup B = \phi$. अतः R4 संतुष्ट नहीं होता।

इसलिए $(\wp(X), \cup, \cap)$ एक वलय नहीं है।

E6) क्योंकि R1, R2, R5 और R6 को R संतुष्ट करता है इसलिए इन्हें $M_{ap}(X,R)$ भी संतुष्ट करता है।

शून्य अवयव $0 : X \to R : 0(x) = 0$ है।

$f : X \to R$ का योज्य प्रतिलोम $(-f) : X \to R$ है। अतः $(M_{ap}(X, R), +, .)$ एक वलय है।

E7) पहले तो, $\mathbf{R}$ पर $\oplus$ और $\odot$ सुपरिभाषित द्वि-आधारी संक्रियाएं हैं। फिर, आइए देखें कि $(\mathbf{R}, \oplus, \odot)$, R1 – R6 को संतुष्ट करता है कि नहीं।

सभी $a, b, c \in \mathbf{R}$ के लिए

R1 : $a \oplus b = a+b+1 = b+a+1 = b \oplus a.$

R2 : $(a \oplus b) \oplus c = (a+b+1) \oplus c = a+b+1+c+1$

$= a+(b+c+1)+1 = a \oplus (b \oplus c)$

R3 : $a \oplus (-1) = a-1+1 = a \ \forall\ a \in \mathbf{R}.$

अतः $\oplus$ के सापेक्ष (-1) तत्समक है।

R4 : $a \oplus (-a-2) = a+(-a-2)+1 = -1$. अतः $\oplus$ के सापेक्ष a का प्रतिलोम $-a-2$ है।

R5 : $(a \odot b) \odot c = (ab+a+b) \odot c = (ab+a+b)c + (ab+a+b) + c$

$= a(bc+b+c) + a+(bc+b+c) = a \odot (b \odot c).$

R6 : $a \odot (b \oplus c) = a \odot (b+c+1) = a(b+c+1) + a+(b+c+1)$

$= (ab+a+b) + (ac+a+c) + 1$

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

अतः $(\mathbf{R}, \oplus, \odot)$ एक वलय है।

E8) $Z_2 = \{\bar 0, \bar 1\}, Z_3 = \{\bar 0, \bar 1, \bar 2\}$

$\therefore Z_2 \times Z_3 = \{(\bar 0,\bar 0), (\bar 0,\bar 1), (\bar 0,\bar 2), (\bar 1,\bar 0), (\bar 1,\bar 1), (\bar 1,\bar 2)\}$. अतः सारणियां हैं—

+	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 2)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$	$(\bar 1,\bar 2)$
$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 2)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$	$(\bar 1,\bar 2)$
$(\bar 0,\bar 1)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 2)$	$(\bar 0,\bar 0)$	$(\bar 1,\bar 1)$	$(\bar 1,\bar 2)$	$(\bar 1,\bar 0)$
$(\bar 0,\bar 2)$	$(\bar 0,\bar 2)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 1,\bar 2)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$
$(\bar 1,\bar 0)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$	$(\bar 1,\bar 2)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 2)$
$(\bar 1,\bar 1)$	$(\bar 1,\bar 1)$	$(\bar 1,\bar 2)$	$(\bar 1,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 2)$	$(\bar 0,\bar 0)$
$(\bar 1,\bar 2)$	$(\bar 1,\bar 2)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$	$(\bar 0,\bar 2)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$

	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 2)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$	$(\bar 1,\bar 2)$
$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$
$(\bar 0,\bar 1)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 2)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 2)$
$(\bar 0,\bar 2)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 2)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 2)$	$(\bar 0,\bar 1)$
$(\bar 1,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 0)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 0)$
$(\bar 1,\bar 1)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 1)$	$(\bar 0,\bar 2)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 1)$	$(\bar 1,\bar 2)$
$(\bar 1,\bar 2)$	$(\bar 0,\bar 0)$	$(\bar 0,\bar 2)$	$(\bar 0,\bar 1)$	$(\bar 1,\bar 0)$	$(\bar 1,\bar 2)$	$(\bar 1,\bar 1)$

E9) ध्यान दीजिए कि $\{0\}$ पर + और · द्वि-आधारी संक्रियाएं हैं। और R_1 से R_6 तक के गुण संतुष्ट हो जाते हैं। अब मान लीजिए एकल $\{a\}$ एक वलय है। तब इसमें योज्य तत्समक 0 अवश्य होगा। अतः $\{a\} = \{0\}$.

E10) हम जानते हैं कि $a+0=a \ \forall a \in \mathbf{R}$. क्योंकि $a+0=a.0$, हम पाते हैं कि $a.0=a \forall a \in \mathbf{R}$. परंतु प्रमेय 1 से हम जानते हैं कि $a.0=0$. इसलिए $a=0 \ \forall a \in \mathbf{R}$, अर्थात् $R = \{0\}$.

E11) क्योंकि $(a+b)' = a'+b'$, इसलिए $n=1$ के लिए यह कथन सत्य है। मान लीजिए कि $n=m$ के लिए कथन सत्य है, अर्थात्

$$(a+b)^m = a^m + {}^mC_1 a^{m-1}b + \ldots + {}^mC_{m-1} ab^{m-1} + b^m.$$

अब, $(a+b)^{m+1} = (a+b)(a+b)^m = (a+b) \left(\sum_{k=0}^{m} {}^mC_k a^{m-k} b^k\right)$

$= (a^{m+1} + {}^mC_1 a^{m+1-1}b + {}^mC_2 a^{m+1-2}b^2 + \ldots + {}^mC_m ab^m)$

$+ ({}^mC_0 a^m b + {}^mC_1 a^{m-1}b^2 + \ldots + {}^mC_{m-1} ab^m + b^{m+1})$, बंटन नियम से।

$= a^{m+1} + ({}^mC_1 + {}^mC_0)a^{m+1-1}b + \ldots + ({}^mC_k + {}^mC_{k-1})a^{m+1-k}b^k + \ldots + b^{m+1}$.

$= a^{m+1} + {}^{m+1}C_1 a^{m+1-1}b + \ldots + {}^{m+1}C_k a^{m+1-k}b^k + \ldots + {}^{m+1}C_m ab^m + b^{m+1}$

(क्योंकि ${}^mC_k + {}^mC_{k-1} = {}^{m+1}C_k$) इस तरह $n=m+1$ के लिए भी कथन सत्य है। अतः आगमन नियम के अनुसार यह n के लिए सत्य है।

E12) मान लीजिए e और e', R के दो गुणनात्मक तत्समक अवयव हैं।

तब $e = e.e'$, क्योंकि e' एक गुणनात्मक तत्समक है।

$= e'$ क्योंकि e एक गुणनात्मक तत्समक है। अतः $e=e'$, अर्थात् R का गुणनात्मक तत्समक अद्वितीय है।

E13) $n=1$ के लिए $n\mathbf{Z} = \mathbf{Z}$, तत्समक 1 वाला क्रमविनिमेय वलय है।

$\forall n>1$, $n\mathbf{Z}$ क्रमविनिमेय है परंतु इसका कोई तत्समक नहीं है।

$\mathbf{Z}_n$	तत्समक 1 वाला क्रमविनिमेय वलय है।
$\mathbf{Z}+i\mathbf{Z}$	तत्समक $1+i0$ वाला क्रमविनिमेय वलय है।
$\wp(X)$	तत्समक X वाला क्रमविनिमेय वलय है, क्योंकि $A \cap X = A \ \forall A \subseteq X$.
C[0,1]	तत्समक $1 : [0,1] \to \mathbf{R} : 1(x) = 1$ वाला क्रमविनिमेय वलय है।
End A	क्रमविनिमेय नहीं है। इसका तत्समक $I_A : A \to A : I_A(x) = x$ है।

E14) क्योंकि $a \odot b = b \odot a \ \forall a, b \in \mathbf{R}$, इसलिए $\odot$ क्रमविनिमेय है। और $a \odot 0 = a \ \ \forall a \in \mathbf{R}$. अतः 0 गुणनात्मक तत्समक है।

E15) पहले आप को यह जांच कर लेनी चाहिए कि दिया हुआ समुच्चय R1 – R6 को संतुष्ट करता है कि नहां।

ध्यान दीजिए कि $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ योज्य तत्समक है।

फिर आपको यह सत्यापित करना चाहिए कि किन्हीं दो अवयवों A और B के लिए $AB = BA$. अतः वलय क्रमविनिमेय है। इसका तत्समक $\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ है।

E16) किसी $a \in R$ के लिए $a^2=a$.

विशेष रूप से, $(2a)^2 = 2a \Rightarrow 4a^2=2a \Rightarrow 4a=2a \Rightarrow 2a=0$

$\Rightarrow a = -a$.

अब, $a, b \in R$ के लिए $a+b \in R$.

$\therefore (a+b)^2 = a+b \Rightarrow a^2 + ab + ba + b^2 = a + b$

$\Rightarrow a + ab + ba + b = a + b$, क्योंकि $a^2 = a$ और $b^2 = b$.

$\Rightarrow ab = -ba$

$\Rightarrow ab = ba$, क्योंकि $-ba = ba$.

अतः R क्रमविनिमेय है।

इकाई 10 उपवलय और गुणजावली

इकाई की रूपरेखा

10.1 प्रस्तावना

स इकाई में हम वलय सिद्धांत की विभिन्न संकल्पनाओं का अध्ययन करेंगे। ये संकल्पनाएं खंड 1 और 2 में दिए ए समूह सिद्धांत की संकल्पनाओं के अनुरूप हैं। हम उपवलय की संकल्पना से शुरू करेंगे जो कि उपसमूह की कल्पना के अनुरूप है, जैसा कि आप समझ गए होंगे।

सके बाद हम एक विशेष प्रकार के उपवलय, अर्थात् गुणजावली पर विचार करेंगे। आप देखेंगे कि किसी वलय में गजावली की भूमिका वही है जो कि किसी समूह में प्रसामान्य उपसमूह की। अर्थात् हम इनका प्रयोग विभाग वलय की कल्पना की परिभाषा देने के लिए करते हैं, जो कि वलय सिद्धांत में विभाग समूह की संकल्पना के अनुरूप है।

भाग वलयों की परिभाषा देने के बाद हम इस प्रकार के वलयों के अनेक उदाहरणों पर विचार करेंगे। परंतु आप वलयों का महत्व केवल आगे की इकाइयों को पढ़ने के बाद ही जान सकेंगे।

आशा करते हैं कि इस इकाई के निम्नलिखित उद्देश्यों को आप पूरा कर सकेंगे, क्योंकि केवल तब ही आप आगे इकाइयों को आसानी से समझ सकेंगे।

श्य

इकाई को पढ़ने के बाद आप

कुछ परिचित वलयों के उपवलयों और गुणजावलियों के उदाहरण दे सकेंगे;

देख सकेंगे कि किसी वलय का उपसमुच्चय उपवलय है कि नहीं;

देख सकेंगे कि किसी वलय का उपसमुच्चय गुणजावली है कि नहीं;

विभाग वलय की परिभाषा और उदाहरण दे सकेंगे।

.2 उपवलय (Subring)

ई 3 में हम आपको समूह के उपसमूहों की संकल्पना से परिचित करा चुके हैं। इस भाग में हम आपको वलय ांत में इस संकल्पना के अनुरूप संकल्पना से परिचित कराएंगे। याद रखिए कि हमारे लिए वलय का अर्थ है विनिमेय वलय।

नी इकाई में आपने देखा है कि न केवल $Z \subseteq Q$, बल्कि Z और Q समान संक्रियाओं के सापेक्ष वलय हैं। पता चलता है कि Z, Q का एक उपवलय है, जैसा कि आप अभी देखेंगे।

ाषा : मान लीजिए $(R, +, .)$ एक वलय है और S, R का एक उपसमुच्चय है। हम S को R का **उपवलय** हैं यदि $(S, +, .)$ स्वयं एक वलय हो, अर्थात् R पर परिभाषित संक्रियाओं के सापेक्ष S एक वलय हो।

रण के लिए, इकाई 9 के उदाहरण 1 के प्रयोग से हम कह सकते हैं कि सम पूर्णांकों का समुच्चय 2Z, Z का उपवलय है।

उदाहरण देने से पहले आइए हम उपवलय की परिभाषा का विश्लेषण करें। परिभाषा के अनुसार वलय R का उपवलय R पर परिभाषित संक्रियाओं के सापेक्ष एक वलय है। अब, वंटन नियम, क्रमविनिमेय नियम और य नियम R में लागू होते हैं इसलिए वे R के किसी उपसमुच्चय में भी लागू होते हैं। अतः यह सिद्ध करने के

लिए कि R का उपसमुच्चय S एक वलय है, हमें S के लिए R1 से R6 तक के सभी अभिगृहीतों की जांच करने की आवश्यकता नहीं है। इसके लिए यह जांच करना ही काफ़ी होगा कि

(i) + और . के सापेक्ष S संवृत है,

(ii) $0 \in S$, और

(iii) प्रत्येक $a \in S$ के लिए $-a \in S$.

यदि S इन तीन प्रतिबंधों को संतुष्ट करता हो तो S, R का एक उपवलय होता है। अतः हम उपवलय की एक और परिभाषा दे सकते हैं।

परिभाषा : मान लीजिए S वलय $(R, +, .)$ का एक उपसमुच्चय है। S को R का **उपवलय** कहते हैं यदि

(i) + और . के सापेक्ष S संवृत हो, अर्थात् जब भी $a, b \in S$, तब $a+b, a.b \in S$.

(ii) $0 \in S$, और

(iii) प्रत्येक $a \in S$ के लिए $-a \in S$.

इस परिभाषा को भी सुधारा जा सकता है। यह देखने के लिए, आप इकाई 3 से याद कीजिए कि $(S, +) \leqslant (R, +)$ यदि $a, b \in S \Rightarrow a-b \in S$. इस टिप्पणी की सहायता से हम आसानी से सत्यापित किए जाने वाले प्रतिबंध दे सकते हैं जिनके अंतर्गत उपसमुच्चय उपवलय होता है।

प्रमेय 1 : मान लीजिए S, $(R, +, .)$ का एक अरिक्त उपसमुच्चय है। तब S, R का एक उपवलय होता है यदि और केवल यदि

(क) $x-y \in S \ \forall \ x, y \in S$, और

(ख) $xy \in S \ \forall \ x, y \in S$,

उपपत्ति : हमें दिखाना है कि हमारी परिभाषा के अनुसार S, R का एक उपवलय होता है यदि और केवल यदि S (क) और (ख) को संतुष्ट करता हो।

अब S, R का एक उपवलय होता है यदि और केवल यदि $(S, +) \leqslant (R, +)$ और गुणन के सापेक्ष S संवृत हो, अर्थात् यदि और केवल यदि (क) और (ख) लागू होते हों।

इस तरह हमने प्रमेय सिद्ध कर लिया है।

इस प्रमेय की सहायता से हम आसानी से जांच कर सकते हैं कि कोई उपसमुच्चय उपवलय है कि नहीं। आइए हम कुछ उदाहरण लें।

हमने देखा है कि **Z, Q** का एक उपवलय है। वास्तव में आप प्रमेय 1 को लागू करके सत्यापित कर सकते हैं कि **Z**, वलयों **R, C** और $Z+iZ$ का उपवलय है। आप यह भी सत्यापित कर सकते हैं कि **Q** वलयों **R, C** और $Q + \sqrt{2}Q = \{\alpha+\sqrt{2}\beta \mid \alpha, \beta \in Q\}$ का उपवलय है।

नीचे दिए गए प्रश्न से आपको उपवलयों के कुछ और उदाहरण प्राप्त होंगे।

E1) दिखाइए कि **R**, **C** का उपवलय है, **Z+iZ,C** का उपवलय है और $\mathbf{Q} + \sqrt{2}\ \mathbf{Q}$, **R** का उपवलय है।

आइए अब हम संख्या समुच्चयों के अतिरिक्त उपवलयों के कुछ और उदाहरणों पर विचार करें।

उदाहरण 1 : माड्यूलो 6 के सापेक्ष पूर्णांकों का वलय Z_6 लीजिए। दिखाइए कि $3Z_6 = \{3.\overline{0}, 3.\overline{1}, \ldots\ldots, 3.\overline{5}\}$, Z_6 का उपवलय है।

हल : पहले तो, बताइए कि क्या आप मानते हैं कि $3Z_6 = \{\overline{0}, \overline{3}\}$? याद रखें कि $\overline{6}=\overline{0}, \overline{9}=\overline{3}$, आदि। और $\overline{0}-\overline{3} = -\overline{3} = \overline{3}$. इस तरह, $x-y \in 3Z_6 \forall x, y \in 3Z_6$. आप यह भी सत्यापित कर सकते हैं कि $xy \in 3Z_6 \forall x, y \in 3Z_6$. अतः प्रमेय 1 के अनुसार $3Z_6$, Z_6 का एक उपवलय है।

उदाहरण 2 : इकाई 9 के उदाहरण 4 में दिया गया वलय $\wp(X)$ लीजिए। दिखाइए कि $S = \{\phi, X\}$, $\wp(X)$ का उपवलय है।

हल : ध्यान दें कि $A \Delta A = \phi \forall A \in \wp(X)$ $\therefore$ $\wp(X)$ में $A = -A$.

अब, प्रमेय 1 को लागू करने के लिए पहले हम यह नोट करते हैं कि S अरिक्त है। इसके बाद,

$\phi \Delta \phi = \phi \in S$, $X \Delta X = \phi \in S$,

$\phi \Delta X = X \in S$, $\phi \cap \phi = \phi \in S$, $X \cap X = X \in S$, $\phi \cap X = \phi \in S$.

अतः प्रमेय 1 के अनुसार, S, $\wp(X)$ का एक उपवलय है।

अब आप एक संबंधित प्रश्न को हल कीजिए।

E2) मान लीजिए $A \subseteq X$, $A \neq \phi$. दिखाइए कि $S = \{\phi, A, A^c, X\}$, $\wp(X)$ का एक उपवलय है।

E2 से पता चलता है कि X के प्रत्येक उचित उपसमुच्चय के लिए हमें $\wp(X)$ का एक उपवलय प्राप्त होता है। इस तरह हम देखते हैं कि वलय के अनेक उपवलय हो सकते हैं। आइए हम वलय **Z** के दो उपवलयों पर विचार करें।

उदाहरण 3 : दिखाइए कि $S = \{(n,0) \mid n \in \mathbf{Z}\}$, $\mathbf{Z} \times \mathbf{Z}$ का एक उपवलय है। यह भी दिखाइए कि $D = \{(n,n) \mid n \in \mathbf{Z}\}$, $\mathbf{Z} \times \mathbf{Z}$ का एक उपवलय है।

हल : आप इकाई 9 के उदाहरण 8 से $\mathbf{Z}^2$ की वलय संरचना को दोहरा सकते हैं। दोनों S और D अरिक्त हैं। दोनों ही प्रमेय 1 के (क) और (ख) को संतुष्ट करते हैं। इस तरह, S और D दोनों ही **Z** के उपवलय हैं।

यहां हम एक टिप्पणी देना चाहेंगे जो कि अभी तक दिए गए उपवलयों के उदाहरणों पर आधारित है।

टिप्पणी : i) यदि R तत्समकी वलय हो, तो ज़रूरी नहीं कि R का हर उपवलय तत्समकी हो। उदाहरण के लिए, वलय **Z** तत्समकी है, परंतु इसका उपवलय $n\mathbf{Z} (n \geq 2)$ तत्समकी नहीं है।

ii) यदि उपवलय तत्समकी हो, तो यह ज़रूरी नहीं है कि उसका तत्समक वलय के तत्समक के समान हो। उदाहरण के लिए, वलय $\mathbf{Z} \times \mathbf{Z}$ का तत्समक (1,1) है। लेकिन इसके उपवलय $\mathbf{Z} \times \{0\}$ का तत्समक (1,0) है।

अब आप नीचे दिया गया प्रश्न हल कीजिए।

E3) दिखाइए कि

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in \mathbf{Z} \right\}$$

$$R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in \mathbf{R} \right\}$$

का उपवलय है। क्या S तत्समकी है ? यदि है, तो क्या इसका तत्समक और R का तत्समक बराबर है ?

आइए अब हम एक ऐसा उदाहरण लें, जिससे किसी वलय के अनेक उपवलय प्राप्त होते हैं।

उदाहरण 4 : मान लीजिए R एक वलय है और $a \in R$. दिखाइए कि समुच्चय $aR = \{ax \mid x \in R\}$, R का उपवलय है।

हल : क्योंकि $R \neq \phi$, इसलिए $aR \neq \phi$. अब, aR के किन्हीं दो अवयवों ax और ay के लिए

$ax - ay = a(x-y) \in aR$ और

$(ax)(ay) = a(xay) \in aR$.

अतः प्रमेय 1 के अनुसार, aR, R का एक उपवलय है।

उदाहरण 4 की सहायता से हम तुरंत कह सकते हैं कि सभी $\bar{m} \in \mathbf{Z}_n$ के लिए $\bar{m}\mathbf{Z}_n$, $\mathbf{Z}_n$ का उपवलय है। इससे यह भी पता चलता है कि सभी $n \in \mathbf{Z}$ के लिए $n\mathbf{Z}$, **Z** का उपवलय है।

अब आप नीचे दिए गए प्रश्नों को हल कीजिए।

E4) दिखाइए कि किसी वलय R के लिए {0} और R इसके उपवलय हैं।

E5) दिखाइए कि यदि A, B का उपवलय हो और B, C का उपवलय हो, तो A, C का उपवलय होगा।

E6) **Z** के एक ऐसे उपसमुच्चय का उदाहरण दीजिए जो कि उपव[illegible]

E5 काफ़ी उपयोगी है। उदाहरण के लिए E_1 और E_5 से हमें पता चलता है कि **Q** + [illegible] 2**Q**, **C** का एक उपवलय है।

आइए अब हम उपवलयों के कुछ गुणों पर विचार करें। इकाई 3 से आप जानते हैं कि दो या अधिक उपसमूहों का प्रतिच्छेद एक उपसमूह होता है। नीचे दिए गए परिणाम के अनुसार यही बात उपवलयों के लिए भी सही है।

प्रमेय 2 : मान लीजिए S_1 और S_2 वलय R के उपवलय हैं। तब $S_1 \cap S_2$ भी R का उपवलय होगा।

उपपत्ति : क्योंकि $0 \in S_1$ और $0 \in S_2$, $0 \in S_1 \cap S_2$. इसलिए $S_1 \cap S_2 \neq \phi$. अब मान लीजिए $x, y \in S_1 \cap S_2$. तब $x, y \in S_1$ और $x, y \in S_2$. अतः प्रमेय 1 के अनुसार, $x-y$ और xy, S_1 और S_2 दोनों में हैं, अर्थात् ये $S_1 \cap S_2$ में स्थित हैं। अतः $S_1 \cap S_2$, R का उपवलय है।

ऊपर दी गई उपपत्ति की तरह ही हम सिद्ध कर सकते हैं कि **वलय R के उपवलयों के किसी संग्रह का प्रतिच्छेद R का उपवलय होता है।**

आइए अब वलय के उपवलयों के सम्मिलन पर विचार करें। क्या आपके अनुसार सम्मिलन एक उपवलय होगा ? इस संबंध में नीचे दिया गया प्रश्न लीजिए।

E7) आप जानते हैं कि $Z + iZ$ और Q, C के उपवलय हैं। क्या इनका सम्मिलन C का उपवलय है ? क्यों ?

आइए अब हम उपवलयों के कार्तीय गुणनफल पर विचार करें।

प्रमेय 3 : मान लीजिए S_1 और S_2 क्रमशः वलय R_1 और वलय R_2 के उपवलय हैं। तब $S_1 \times S_2$, $R_1 \times R_2$ का उपवलय होगा।

उपपत्ति : चूँकि S_1 और S_2, R_1 और R_2 के उपवलय हैं, $S_1 \neq \phi$ और $S_2 \neq \phi$. इसलिए $S_1 \times S_2 \neq \phi$. अब, मान लीजिए (a, b) और $(a', b') \in S_1 \times S_2$. तब $a, a' \in S_1$ और $b, b' \in S_2$. तब, क्योंकि S_1 और S_2 उपवलय हैं, इसलिए $a - a'$, $aa' \in S_1$ और $b - b'$, $bb' \in S_2$.

(यहाँ हम सुविधा के लिए R_1 और R_2 दोनों के लिए + और . का प्रयोग कर रहे हैं।)

अतः

$(a, b) - (a', b') = (a - a', b - b') \in S_1 \times S_2$, और

$(a, b) . (a', b') = (aa', bb') \in S_1 \times S_2$.

इस तरह, प्रमेय 1 के अनुसार, $S_1 \times S_2$, $R_1 \times R_2$ का उपवलय है।

आप इस परिणाम का प्रयोग नीचे दिए गए प्रश्न को हल करने के लिए कर सकते हैं।

E8) $Z \times R$ के दो उचित अतुच्छ उपवलय, अर्थात् ऐसे उपवलय जो न तो शून्य हैं और न ही पूरा वलय, प्राप्त कीजिए।

आइए अब हम उपवलयों के एक महत्वपूर्ण वर्ग पर विचार करें।

10.3 गुणजावली (Ideal)

खंड 2 में आप प्रसामान्य उपसमूहों का अध्ययन कर चुके हैं और यह भी देख चुके हैं कि समूह सिद्धांत में वे क्या भूमिका निभाते हैं। आप देख चुके हैं कि प्रसामान्य उपसमूहों के अस्तित्व का सबसे महत्वपूर्ण कारण है कि इनकी सहायता से हम विभाग समूह परिभाषित कर सकते हैं। वलय सिद्धांत में हम इसी प्रकार की संकल्पना, अर्थात् विभाग वलय परिभाषित करना चाहते हैं। इस भाग में हम ऐसे उपवलयों पर चर्चा करेंगे जिनकी सहायता से हम विभाग वलय को परिभाषित कर सकते हैं। इन उपवलयों को गुणजावली कहते हैं। बीजीय संख्या सिद्धांत की छानबीन करने के दौरान 19 वीं शताब्दी के गणितज्ञ डेडेकिण्ड, क्रॉनिकर तथा अन्य गणितज्ञों ने इस संकल्पना का विकास किया। आइए देखें कि इसकी सहायता से हम विभाग वलय को कैसे परिभाषित कर सकते हैं।

एक वलय $(R, +, .)$ और इसका एक उपवलय I लीजिए। चूँकि $(R, +)$ एक आबेली समूह है, इसलिए $(R, +)$ में उपसमूह I प्रसामान्य होगा। अतः R में I के सभी सहसमुच्चयों का समुच्चय

$R/I = \{a + I \mid a \in R\}$

द्वि-आधारी संक्रिया + के सापेक्ष एक समूह होगा, जहाँ हम + को निम्न प्रकार से परिभाषित करते हैं :

सभी $a + I$, $b + I \in R/I$ के लिए,

$$(a + I) + (b + I) = (a + b) + I \qquad \ldots\ldots (1)$$

हम R/I पर · परिभाषित करना चाहते हैं जिससे कि R/I एक वलय बन जाए। आप शायद सोचें कि निम्न परिभाषा से यह हो जाएगा :

$$(a + I) . (b + I) = ab + I \;\forall\; a + I, b + I \in R/I \qquad \ldots\ldots (2)$$

लेकिन, क्या यह सुपरिभाषित है ? हर स्थिति में नहीं। उदाहरण के लिए, **R** का उपवलय **Z** लीजिए और **R** में **Z** के सहसमुच्चयों का समुच्चय लीजिए। अब, क्योंकि $1=1-0 \in Z$, इसलिए $1+Z=0+Z$. लेकिन इसका मतलब होगा कि $(\sqrt{2}+Z).(1+Z)=(\sqrt{2}+Z).(0+Z)$, अर्थात् $\sqrt{2}+Z=0+Z$, अर्थात् $\sqrt{2} \in Z$, जो एक अंतर्विरोध है। अतः समुच्चय **R/Z** पर गुणन की हमारी परिभाषा लागू नहीं होती।

लेकिन, यदि हम I पर कुछ प्रतिबंध लगाएँ, तो R/I पर परिभाषा (2) लागू होती है। ऐसे कौन से प्रतिबंध होने चाहिए ? इस प्रश्न का उत्तर प्राप्त करने के लिए, मान लीजिए कि (2) में दिया गुणन सुपरिभाषित है।

तब, सभी $r \in R$ के लिए $(r+I).(0+I) = r.0+I = 0+I = I$. अब, आप जानते हैं कि, यदि $x \in I$, तो $x+I=0+I=I$. चूँकि हमने यह मान लिया है कि . सुपरिभाषित है, हम देखते हैं कि

$(r+I).(x+I) = (r+I).(0+I) = 0+I$, जब भी $r \in R$, $x \in I$.

अर्थात् $rx+I = I$, जब भी $r \in R$, $x \in I$.

इस तरह, $rx \in I$, जब भी $r \in R$, $x \in I$.

अतः, यदि · सुपरिभाषित हो, तो उपवलय I एक और प्रतिबंध को अवश्य संतुष्ट करेगा। यह है $rx \in I$ जब भी $r \in R$ और $x \in I$.

भाग 10.4 में हम सिद्ध करेंगे कि I पर लगाया गया यह अतिरिक्त प्रतिबंध संक्रिया · को सुपरिभाषित बनाने के लिए और $(R/I, +, .)$ को एक वलय बनाने के लिए काफ़ी है। इस भाग में हम R के उन उपवलयों I पर विचार करेंगे जिन पर हम यह प्रतिबंध लगाते हैं कि

$rx \in I$ जब भी $r \in R$ और $x \in I$.

परिभाषा : वलय $(R, +, .)$ के अरिक्त उपसमुच्चय I को वलय R की **गुणजावली** कहते हैं, यदि

i) सभी $a, b \in I$ के लिए $a-b \in I$, और

ii) सभी $r \in R$ और $a \in I$ के लिए $ra \in I$.

यहां हम एक टिप्पणी देना चाहेंगे कि हम सदा ही अपने वलय को क्रमविनिमेय मान रहे हैं। यदि वलय अक्रमविनिमेय हो तो गुणजावली की परिभाषा में थोड़ा परिवर्तन आ जाता है। परिवर्तित परिभाषा है :

अक्रमविनिमेय वलय R का अतिरिक्त उपसमुच्चय I एक गुणजावली होता है, यदि

i) $a-b \in I \ \forall\ a, b \in I$, और

ii) $ra \in I$ और $ar \in I \ \forall\ a \in I, r \in R$.

आइए अब हम क्रमविनिमेय वलयों को लौट चलें। परिभाषा से हम देखते हैं कि **वलय R का उपवलय I, R की एक गुणजावली होता है यदि और केवल यदि $ra \in I \ \forall\ r \in R$ और $a \in I$.**

आइए हम कुछ उदाहरण लें। E4 में आपने देखा है कि किसी भी वलय R के लिए समुच्चय {0} एक उपवलय होता है। वास्तव में, यह R की एक गुणजावली है जिसे R की **तुच्छ गुणजावली** कहते हैं। यदि R में अन्य गुणजावली हो तो उसे R की **अतुच्छ गुणजावली** कहते हैं।

आप यह भी सत्यापित कर सकते हैं कि प्रत्येक वलय स्वयं की गुणजावली होती है। यदि वलय R की गुणजावली I ऐसी हो कि $I \neq R$, तो I को R की **उचित गुणजावली** कहते हैं।

उदाहरण के लिए, यदि $n \neq 0, 1$, तो उपवलय $nZ = \{nm \mid m \in Z\}$, Z की एक उचित अतुच्छ गुणजावली होती है। ऐसा इसलिए है, क्योंकि $z \in Z$ और $nm \in nZ$ के लिए $z(nm) = n(zm) \in nZ$.

अब आप यह प्रश्न हल कीजिए।

E 9) दिखाइए कि $\{\bar{0}, \bar{3}\}$ और $\{\bar{0}, \bar{2}, \bar{4}\}$, Z_6 की उचित गुणजावलियां हैं।

आइए अब हम गुणजावलियों के कुछ और उदाहरण लें।

उदाहरण 5 : मान लीजिए X एक अनंत समुच्चय है। X के सभी परिमित उपसमुच्चयों का वर्ग I लीजिए। दिखाइए कि I, $\wp(X)$ की एक गुणजावली है।

हल : $I = \{A \mid A, X$ का एक परिमित उपसमुच्चय है $\}$

ध्यान दीजिए कि

i) $\phi \in I$, अर्थात् $\wp(X)$ का शून्य अवयव I में है।

ii) $A-B = A+(-B) = A+B$, क्योंकि $\wp(X)$ में $B=-B$,

$= A \triangle B$.

इस तरह, यदि $A, B \in I$, तो $A-B$ भी X का परिमित उपसमुच्चय होगा। अतः $A-B \in I$.

iii) $AB = A \cap B$. अब, यदि A, X का परिमित उपसमुच्चय हो और B, $\wp(X)$ का कोई अवयव हो, तो $A \cap B$, X का एक परिमित उपसमुच्चय होगा। इस तरह, $A \in I$ और $B \in \wp(X) \Rightarrow AB \in I$.

अतः I, $\wp(X)$ की एक गुणजावली है।

उदाहरण 6 : मान लीजिए X एक समुच्चय है और Y, X का एक अरिक्त उपसमुच्चय है। दिखाइए कि $I = \{A \in \wp(X) \mid A \cap Y = \phi\}$, $\wp(X)$ की एक गुणजावली है। विशेष रूप से, यदि हम $Y = \{x_0\}$ लें, जहाँ x_0, X का एक नियत अवयव हो, तो

$I = \{A \in \wp(X) \mid x_0 \notin A\}$, $\wp(X)$ की एक गुणजावली है।

हल : सबसे पहले, $\phi \in I$. इसके बाद, $\forall$ A, B $\in$ I,

$(A-B) \cap Y = (A \triangle B) \cap Y = (A \cap Y) \triangle (B \cap Y) = \phi \triangle \phi = \phi$, जिससे कि $A-B \in I$.

अंत में $A \in I$ और $B \in \wp(X)$ के लिए

$(A-B) \cap Y = (A \cap B) \cap Y = (A \cap Y) \cap B = \phi \cap B = \phi$, जिसके कि $AB \in I$.

अतः I, $\wp(X)$ की एक गुणजावली है।

उदाहरण 7 : इकाई 9 के उदाहरण 6 में दिया गया वलय C[0,1] लीजिए।

मान लीजिए $M = \{f \in C[0,1] \mid f(\frac{1}{2})=0\}$. दिखाइए कि M, C[0,1] की एक गुणजावली है।

हल : सभी $x \in [0,1]$ के लिए $\mathbf{0} = (x)0$ से परिभाषित फलन **0**, C[0,1] का शून्य अवयव है। क्योंकि $\mathbf{0}(\frac{1}{2}) = 0$, $\mathbf{0} \in M$.

और, यदि $f, g \in M$, तो $(f-g)(\frac{1}{2}) = f(\frac{1}{2}) - g(\frac{1}{2}) = 0-0 = 0$.

इसलिए $f-g \in M$.

और फिर, यदि $f \in M$ और $g \in C[0,1]$, तो

$(fg)(\frac{1}{2}) = f(\frac{1}{2})\, g(\frac{1}{2}) = 0 \,.\, g(\frac{1}{2}) = 0$.

इसलिए $fg \in M$.

अतः M, C[0,1] की एक गुणजावली है।

जब आप इकाई 11 पढ़ेंगे आप देखेंगे कि M समाकारिता $\phi : C[0,1] \to R : \phi(f) = f(\frac{1}{2})$ की अष्टि है।

अब आप एक प्रश्न हल कर सकते हैं जो उदाहरण 7 का व्यापकीकरण है।

E10) मान लीजिए $a \in [0,1]$. दिखाइए कि समुच्चय

$I_a = \{f \in C[0,1] \mid f(a)=0\}$, C[0,1] की एक गुणजावली है।

अगले प्रश्न में हम आप से उदाहरण 4 के उपवलय पर विचार करने के लिए कहते हैं।

E11) मान लीजिए R एक वलय है और $a \in R$. दिखाइए कि Ra, R की एक गुणजावली है।

यदि आपने E11 हल कर लिया है, तो आप E9 को तुरंत हल कर सकते हैं। आइए देखें कि E11 का व्यापकीकरण किया जा सकता है कि नहीं।

उदाहरण 8 : किसी वलय R और $a_1, a_2 \in R$ के लिए दिखाइए कि

$Ra_1 + Ra_2 = \{x_1a_1 + x_2a_2 \mid x_1, x_2 \in R\}$, R की एक गुणजावली है।

हल : सबसे पहले, $0 = 0a_1 + 0a_2$ $\therefore$ $0 \in Ra_1 + Ra_2$.

इसके बाद, $\forall\, x_1, x_2, y_1, y_2 \in R$,

$(x_1a_1 + x_2a_2) - (y_1a_1 + y_2a_2) = (x_1-y_1)a_1 + (x_2-y_2)a_2 \in Ra_1 + Ra_2$.

अंत में $r \in R$ और $x_1a_1 + x_2a_2 \in Ra_1+Ra_2$ के लिए

$r(x_1a_1+x_2a_2) = rx_1a_1+rx_2a_2 \in Ra_1+Ra_2$.

अतः Ra_1+Ra_2, R की एक गुणजावली है।

गुणजावली प्राप्त करने की इस विधि का विस्तार करके हम R के नियत अव्ययवों $a_1, a_2, \ldots, a_n$ के लिए $\{x_1a_1+x_2a_2+\ldots+x_na_n | x_i \in R\}$ के रूप की गुणजावली प्राप्त कर सकते हैं। वलय सिद्धांत में इस प्रकार की गुणजावलियाँ बार-बार दिखती हैं। हम इन्हें एक विशेष नाम देते हैं।

परिभाषा : मान लीजिए $a_1, \ldots, a_n$ वलय R के नियत अवयव हैं। तब हम

$Ra_1 + Ra_2 + \ldots + Ra_n = \{x_1a_1 + x_2a_2 + \ldots + x_na_n \mid x_i \in R\}$

को **$a_1, \ldots, a_n$ से जनित गुणजावली** कहते हैं।

$a_1, \ldots, a_n$ को इस गुणजावली के **जनक** (generators) कहते हैं। हम इस गुणजावली को $<a_1, a_2, \ldots, a_n>$ से भी प्रकट करते हैं।

जब $n=1$, हम इस गुणजावली को **मुख्य गुणजावली** (principal ideal) कहते हैं। इस तरह, यदि $a \in R$, तो $Ra = <a>$, R की मुख्य गुणजावली है। अगले खंड में आप मुख्य गुणजावलियों का काफ़ी प्रयोग करेंगे।

अब मुख्य गुणजावलियों पर दो प्रश्न।

E12) मान लीजिए R एक तत्समकी वलय है। दिखाइए कि $<1> = R$.

E13) $\bar{3}$ से और $\bar{5}$ से जनित Z_{10} की मुख्य गुणजावलियाँ ज्ञात कीजिए।

अब हम वलय की एक विशेष गुणजावली पर विचार करेंगे। लेकिन इसके लिए हमें एक परिभाषा देनी होगी।

परिभाषा : वलय R के अवयव a को शून्यंभावी (nilpotent) कहते हैं यदि किसी धन पूर्णांक n के लिए $a^n=0$.

उदाहरण के लिए, $\bar{3}$ और $\bar{6}$, Z_9 के शून्यंभावी अवयव हैं क्योंकि $\bar{3}^2 = \bar{9} = \bar{0}$ और $\bar{6}^2 = \overline{36} = \bar{0}$ और ज़ाहिर है कि किसी भी वलय R में 0 एक शून्यंभावी अवयव होता है।

अब निम्नलिखित उदाहरण लीजिए।

उदाहरण 9 : मान लीजिए R एक वलय है। दिखाइए कि R के शून्यंभावी अवयवों का समुच्चय, R की एक गुणजावली है। इस गुणजावली को R की शून्य करणी (nil radical) कहते हैं।

हल : मान लीजिए $N = \{a \in R | a^n = 0$, किसी धनपूर्णांक n के लिए $\}$.
तब $0 \in N$.
और, यदि $a, b \in N$, तो किन्हीं धन पूर्णांकों m और n के लिए $a^n = 0$ और $b^m = 0$.
अब, $(a-b)^{m+n} = \sum_{r=0}^{m+n} {}^{m+n}C_r a^r (-b)^{m+n-r}$ (इकाई 9 का E11 देखिए)

प्रत्येक $r=0,1,\ldots,m+n$ के लिए या तो $r \geq n$, या $m+n-r \geq m$. अतः या तो $a^r=0$ या $b^{m+n-r}=0$.
इस तरह, पद $a^r(-b)^{m+n-r}=0$. इसलिए $(a-b)^{m+n} = 0$.
इस तरह, $a-b \in N$ जब भी $a, b \in N$.
अंत में, यदि $a \in N$ तो किसी धन पूर्णांक n के लिए $a^n=0$. अतः किसी $r \in R$ के लिए $(ar)^n = a^n r^n = 0$,
अर्थात् $ar \in N$. इसलिए N, R की एक गुणजावली है।

आइए देखें कि कुछ परिचित वलयों की शून्य करणियाँ क्या हैं। वलय **Z, Q, R** या **C** के लिए $N=\{0\}$, क्योंकि इन वलयों के किसी शून्येतर अवयव का घात शून्येतर ही होता है।

Z_4 के लिए $N = \{\bar{0}, \bar{2}\}$.

अब आप नीचे दिए गए प्रश्नों को हल कीजिए।

E14) Z_8 और $\wp(X)$ की शून्य करणियाँ ज्ञात कीजिए।

E15) मान लीजिए R एक वलय है और $a \in R$. दिखाइए कि $I = \{r \in R | ra = 0\}$, R की एक गुणजावली है।
(इस गुणजावली को a का शून्यकारी (annihilator) कहते हैं।)

अब तक आप गुणजावली की संकल्पना से परिचित हो गए होंगे। आइए अब हम गुणजावलियों से संबंधित कुछ परिणाम प्राप्त करें।

प्रमेय 4: मान लीजिए R तत्समक 1 वाला एक वलय है। यदि I, R की गुणजावली हो और $1 \in I$, तो $I = R$.

उपपत्ति : हम जानते हैं कि $I \subseteq R$. हम सिद्ध करना चाहते हैं कि $R \subseteq I$. मान लीजिए $r \in R$. क्योंकि $1 \in I$ और I, R की गुणजावली है, इसलिए $r = r.1 \in I$. अतः $R \subseteq I$. इसलिए $I = R$.

इस परिणाम की सहायता से हम तुरंत कह सकते हैं कि $\mathbf{Z}$, $\mathbf{Q}$ की गुणजावली नहीं है। क्या इस परिणाम से यह भी पता चलता है कि $\mathbf{Q}$, $\mathbf{R}$ की गुणजावली है कि नहीं ? बिल्कुल। क्योंकि $1 \in \mathbf{Q}$ और $\mathbf{Q} \neq \mathbf{R}$, इसलिए $\mathbf{Q}$, $\mathbf{R}$ की गुणजावली नहीं हो सकता।

आइए अब हम गुणजावलियों की बीजावली (algebra) पर विचार करें। पिछले भाग में हमने सिद्ध किया है कि उपवलयों का प्रतिच्छेद एक उपवलय होता है। यहाँ हम दिखाएंगे कि गुणजावलियों का प्रतिच्छेद एक गुणजावली होता है। हम यह भी दिखाएंगे कि गुणजावलियों का योगफल एक गुणजावली होता है और उचित रूप से परिभाषित गुणजावलियों का गुणनफल एक गुणजावली होता है।

प्रमेय 5 : यदि I और J वलय R की गुणजावलियाँ हों, तो

(क) $I \cap J$,

(ख) $I + J = \{a + b \mid a \in I$ और $b \in J\}$, और

(ग) $IJ = \{x \in R \mid x$ एक परिमित योगफल $a_1b_1 + \ldots + a_mb_m$ है, जहाँ $a_i \in I$ और $b_i \in J\}$ R की गुणजावलियाँ हैं।

उपपत्ति : (क) प्रमेय 2 से आप जानते हैं कि $I \cap J$, R का एक उपवलय है। अब, यदि $a \in I \cap J$, तो $a \in I$ और $a \in J$. अतः R के सभी x के लिए $ax \in I$ और $ax \in J$. इसलिए सभी $a \in I \cap J$ और $x \in R$ के लिए $ax \in I \cap J$. इस तरह, $I \cap J$, R की एक गुणजावली है।

(ख) सबसे पहले, क्योंकि $0 = 0 + 0 \in I \cap J$, इसलिए $I + J \neq \phi$. इसके बाद, यदि $x, y \in I + J$, तो किन्हीं $a_1, a_2 \in I$ और $b_1, b_2 \in J$ के लिए $x = a_1 + b_1$ और $y = a_2 + b_2$. इसलिए $x - y = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$. अंत में, मान लीजिए $x \in I + J$ और $r \in R$. तब किसी $a \in I$ और $b \in J$ के लिए $x = a + b$. अब $xr = (a + b)r = ar + br \in I + J$, क्योंकि $r \in R$, $a \in I \Rightarrow ar \in I$ और $r \in R$, $b \in J \Rightarrow br \in J$.
अतः $I + J$, R की एक गुणजावली है।

(ग) सबसे पहले, क्योंकि $I \neq \phi$ और $J \neq \phi$, इसलिए $IJ \neq \phi$.
इसके बाद, मान लीजिए $x, y \in IJ$. तब किन्हीं
$a_1, \ldots, a_m, a_1', \ldots, a_n' \in I$ और
$b_1, \ldots, b_m, b_1', \ldots, b_n' \in J$ के लिए
$x = a_1b_1 + \ldots + a_mb_m$ और $y = a_1'b_1' + \ldots + a_n'b_n'$.

$$\therefore x - y = (a_1b_1 + \ldots + a_mb_m) - (a_1'b_1' + \ldots + a_n'b_n')$$
$$= a_1b_1 + \ldots + a_mb_m + (-a_1')b_1' + \ldots + (-a_n')b_n'$$

जो ab के रूप के अवयवों का परिमित योगफल है, जहाँ $a \in I$ और $b \in J$. इसलिए $x - y \in IJ$.

अंत मे, मान लीजिए $x \in IJ$ और $x = a_1b_1 + \ldots + a_nb_n$ जहाँ $a_i \in I$ और $b_i \in J$. तब, किसी $r \in R$ के लिए
$xr = (a_1b_1 + \ldots + a_nb_n)r = a_1(b_1r) + \ldots + a_n(b_nr)$,
जो ab के रूप के अवयवों का परिमित योगफल है जहाँ $a \in I$ और $b \in J$. (ध्यान दीजिए कि R के सभी r के लिए $b_i \in J \Rightarrow b_ir \in J$.) अतः IJ, R की एक गुणजावली है।

यहाँ हम कहना चाहेंगे कि यदि हम $IJ = \{ab \mid a \in I, b \in J\}$ परिभाषित करें, तो गुणजावली की बात छोड़िए, हो सकता है कि IJ उपवलय ही न हो। इसका कारण है कि यदि $x, y \in IJ$, तो IJ की इस परिभाषा के अनुसार यह आवश्यक नहीं है कि $x - y \in IJ$.

आइए अब हम प्रमेय 5 में प्राप्त गुणजावलियों के परस्पर संबंध पर विचार करें। इसके लिए आइए हम पहले निम्नलिखित विशेष स्थिति पर विचार करें :

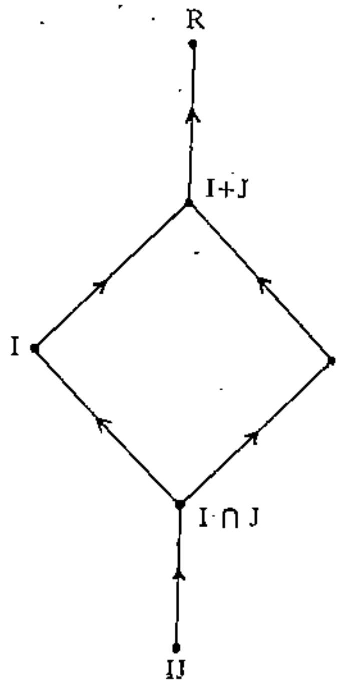
$R = \mathbf{Z}$, $I = 2\mathbf{Z}$ और $J = 10\mathbf{Z}$. तब, क्योंकि $J \subseteq I$, इसलिए $I \cap J = J$ और, $I + J$ का कोई भी अवयव $x = 2n + 10m$ के रूप का होता है, जहाँ $n, m \in \mathbf{Z}$. इस तरह, $x = 2(n + 5m) \in 2\mathbf{Z}$. साथ ही, $2\mathbf{Z} = I \subseteq I + J$

इस तरह, $I+J=\langle 2,10\rangle = \langle 2\rangle$.

इसी प्रकार आप देख सकते हैं कि $IJ = \langle 20\rangle$.

ध्यान दीजिए कि $IJ \subseteq I\cap J \subseteq I \subseteq I+J$.

वास्तव में, ये संबंध किन्हीं भी I और J के लिए सत्य होते हैं (देखिए E16)। हमने इसे चित्र 1 में दिखाया है।



चित्र 1 : गुणजावली पदानुक्रम

E16) यदि I और J वलय R की गुणजावलियाँ हों, तो दिखाइए कि

(क) $IJ \subseteq I\cap J \subseteq I \subseteq I+J$,
और $IJ \subseteq I\cap J \subseteq J \subseteq I+J$;

(ख) $I+J$ उन गुणजावलियों में से सबसे छोटी है जिनमें दोनों गुणजावलियाँ I और J आविष्ट होती हैं, अर्थात् यदि A, R की एक गुणजावली हो जो I और J दोनों को आविष्ट करती हो, तो A, $I+J$ को अवश्य आविष्ट करेगी;

(ग) $I\cap J$ उन गुणजावलियों में से सबसे बड़ी है जो I और J दोनों में आविष्ट होती है;

(घ) यदि $1 \in R$ और $I+J=R$, तो $IJ=I\cap J$, अर्थात् यदि चित्र 1 में दिए गए ऊपर के दो वलय समान हों, तो नीचे के दो वलय भी समान होंगे।

आइए अब हम उस बात पर विचार करें जो हमने इस भाग के शुरू में कही थी, यानि कि गुणजावली का महत्व।

10.4 विभाग वलय (Quotient Ring)

इकाई 5 में आप विभाग समूहों का अध्ययन कर चुके हैं। आप जानते हैं कि यदि किसी समूह G का प्रसामान्य उपसमूह N दिया हो, तो N के सभी सहसमुच्चयों का समुच्चय एक समूह होता है और इसे प्रसामान्य उपसमूह N का संगत विभाग समूह कहते हैं। गुणजावलियों के प्रयोग से अब हम वलयों के संबंध में इसी प्रकार की संकल्पना परिभाषित करेंगे। भाग 10.3 के शुरू में हमने कहा था कि यदि $(R, +, .)$ एक वलय हो और I, R का ऐसा उपवलय हो कि $(R/I, +, .)$ एक वलय है, जहाँ + और ·

$$(x+I)+(y+I) = (x+y)+I, \text{ और}$$

$$(x+I)\cdot(y+I)=xy+I \quad \forall x+I,\ y+I \in R/I$$

परिभाषित हैं, तो उपवलय I को एक और प्रतिबंध संतुष्ट करना चाहिए कि $rx \in I$ जब भी $r \in R$ और $x \in I$. अर्थात् I को एक गुणजावली होना चाहिए। अब हम दिखाएंगे कि यदि I इस अतिरिक्त प्रतिबंध को संतुष्ट करता हो, तो R/I पर परिभाषित संक्रियाएँ सुपरिभाषित हैं।

समूह सिद्धांत से हम जानते हैं कि $(R/I, +)$ एक आवेली समूह है। अतः हमें केवल यह सत्यापित करना है कि सुपरिभाषित है, अर्थात् यदि

$a+I=a'+I$, $b+I=b'+I$, तब $ab+I=a'b'+I$.

अब क्योंकि $a+I=a'+I$, इसलिए $a-a'\in I$.

मान लीजिए $a-a'=x$.

इसी प्रकार $b-b'\in I$, मान लीजिए $b-b'=y$.

तब $ab=(a'+x)(b'+x)=a'b' + (xb'+a'x+x^2)$.

$\therefore$ $ab-a'b'\in I$, क्योंकि $x\in I$ और I, R की एक गुणजावली है।

$\therefore$ $ab+I=a'b'+I$.

अतः $\cdot$ R/I पर सुपरिभाषित है।

अब नीचे दिए गए परिणाम को सिद्ध करना हमारा उद्देश्य है।

प्रमेय 6 : मान लीजिए R एक वलय है और I,R की एक गुणजावली है। तब

$(x+I) + (y+I) = (x+y) +I$, और

$(x+I) . (y+I) = xy + I \; \forall \; x, y \in R$.

से परिभाषित योग और गुणन के सापेक्ष R/I एक वलय होता है।

उपपत्ति : जैसा कि हम पहले कह चुके हैं, $(R/I, +)$ एक आवेली समूह है। अतः R/I को वलय सिद्ध करने के लिए हमें केवल यह देखना है कि $\cdot$ क्रमविनिमेय है, साहचर्य है और + पर वंटित है।

अब,

i) $\cdot$ क्रमविनिमेय है : सभी $a+I, b+I \in R/I$ के लिए

$(a+I).(b+I) = ab+I=ba+I = (b+I) . (a+I)$

ii) साहचर्य है: $\forall a,b,c \in R$

$$\begin{aligned}((a+I).(b+I)).(c+I) &= (ab+I).(c+I)\\ &= (ab)c + I\\ &= a(bc) + I\\ &= (a+I).((b+I).(c+I))\end{aligned}$$

iii) वंटन नियमः मान लीजिए $a+I, b+I, c+I \in R/I$. तब

$$\begin{aligned}(a+I).((b+I)+(c+I)) &= (a+I) [(b+c)+I]\\ &= a(b+c) + I\\ &= (ab+ac) + I\\ &= (ab+I) + (ac + I).\\ &= (a+I).(b+I)+(a+I).(c+I)\end{aligned}$$

अतः R/I एक वलय है। इस वलय को **गुणजावली I के सापेक्ष R का विभाग वलय कहते हैं।**

आइए अब हम कुछ उदाहरण लें। पहले हम वह उदाहरण लेंगे जिसकी वजह से शब्द '**R माड I**' का प्रयोग होता है।

उदाहरण 10 : मान लीजिए $R=\mathbf{Z}$ और $I=n\mathbf{Z}$. R/I क्या होगा ?

हल : भाग 10.3 में आपने देखा है कि $n\mathbf{Z}$, $\mathbf{Z}$ की गुणजावली है, और इकाई 2 में आपने देखा कि

$$\begin{aligned}\mathbf{Z}/n\mathbf{Z} &= \{n\mathbf{Z}, 1+n\mathbf{Z}, \ldots, (n-1)+n\mathbf{Z}\}\\ &= \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}\text{, जो कि}\end{aligned}$$

माड्यूलो n के सापेक्ष तुल्यता वर्गों के समुच्चय के बराबर हैं। अतः R/I वलय $\mathbf{Z}_n$ है।

आइए अब हम $\mathbf{Z}_n$ की एक गुणजावली पर विचार करें, जहाँ n ...

उदाहरण 11 : मान लीजिए $R=\mathbf{Z}_8$. दिखाइए कि $I=\{\bar{0},\bar{4}\}$, R की एक गुणजावली है। R/I में + और $\cdot$ की केली सारणियाँ लिखिए।

हलः $I=\bar{4}R$. अतः I, R की गुणजावली है। समूह सिद्धांत से आप जानते हैं कि R/I में अवयवों की संख्या

$$= O\,(R/I) = \frac{O(R)}{O(I)} = \frac{8}{2} = 4.$$

आप देख सकते हैं कि ये अवयव हैं

$0+I=\{\bar{0},\bar{4}\}$, $1+I=\{\bar{1},\bar{5}\}$, $2+I=\{\bar{2},\bar{6}\}$, $3+I=\{\bar{3},\bar{7}\}$.

R/I में + और · की केली सारणियाँ हैं:

$+$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$		$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{0}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$	$\bar{0}+I$	$\bar{0}+I$	$\bar{0}+I$	$\bar{0}+I$	$\bar{0}+I$
$\bar{1}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{2}+I$	$\bar{2}+I$	$\bar{3}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{0}+I$	$\bar{2}+I$	$\bar{0}+I$	$\bar{2}+I$
$\bar{3}+I$	$\bar{3}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$	$\bar{0}+I$	$\bar{3}+I$	$\bar{2}+I$	$\bar{1}+I$

अब आप नीचे दिए गए प्रश्न को हल कीजिए।

E17) दिखाइए कि यदि R एक तत्समकी वलय है, तो R की किसी गुणजावली I के लिए R/I तत्समकी वलय होगा।

E18) यदि R तत्समक 1 वाला वलय हो और I, R की एक गुणजावली हो जो 1 आविष्ट करती हो, तो R/I किस प्रकार दिखाई पड़ेगा ?

E19) मान लीजिए N, R की शून्य करणी है। दिखाइए कि R/N में कोई शून्येतर शून्यंभावी अवयव नहीं है।

जब हम अगली इकाई में समाकारिताओं की चर्चा कर लेंगे और जब हम खंड 4 में बहुपद वलयों पर चर्चा करेंगे तब आप विभाग वलयों की उपयोगिता और महत्व समझ सकेंगे।

आइए अब हम संक्षेप में देखें कि हमने इस इकाई में क्या किया है।

10.5 सारांश

इस इकाई में हम यह मानकर चले हैं कि सभी वलय क्रमविनिमेय हैं। इसमें हमने निम्नलिखित तथ्यों पर चर्चा की है।

1. उपवलय की परिभाषा और उसके उदाहरण।
2. इस तथ्य की उपपत्ति और प्रयोग कि वलय R का अरिक्त उपसमुच्चय S, वलय R का एक उपवलय होता है यदि और केवल यदि $x-y \in S$ और $xy \in S$ $\forall x, y \in S$.
3. किसी वलय के उपवलयों का प्रतिच्छेद वलय का एक उपवलय होता है।
4. उपवलयों का कार्तीय गुणनफल संगत वलयों के कार्तीय गुणनफल का उपवलय होता है।
5. गुणजावली की परिभाषा और उसके उदाहरण।
6. n अवयवों द्वारा जनित गुणजावली की परिभाषा।
7. वलय के शून्यंभावी अवयवों का समुच्चय वलय की एक गुणजावली होता है।
8. यदि I तत्समकी वलय R की गुणजावली हो और $1 \in I$, तो $I = R$.
9. यदि I और J वलय R की गुणजावलियां हों, तो $I \cap J$, $I+J$ और IJ भी R की गुणजावलियां हैं।
10. विभाग वलय की परिभाषा और उसके उदाहरण।

10.6 हल/उत्तर

E1) $\forall x, y \in R$, $x-y \in R$ और $xy \in R$. इस तरह R, C का एक उपवलय है। इसी तरह आप अन्य दो स्थितियों की जांच कर सकते हैं।

E2) स्पष्ट है कि S अरिक्त है।
और किन्हीं $x, y \in S$ के लिए $x-y = x \,\Delta\, (-y) = x \,\Delta\, y$. (जैसा कि उदाहरण 2 में दिया गया है)।

आप यह भी जांच कर सकते हैं कि $x \triangle y \in S \ \forall x, y \in S$. साथ ही किन्हीं $x, y \in S$ के लिए $x.y = x \cap y \in S$, जिसकी जांच आप कर सकते हैं। इस तरह, $S, \wp(X)$ का एक उपवलय है।

E3) सबसे पहले $S \neq \phi$. इसके बाद, S में किसी

$$A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \text{ और } C = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \text{ के लिए}$$

$$A - C = \begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in S \text{ और } AC = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S.$$

इस तरह S, R का एक उपवलय है।

S का तत्समक $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ है, जो कि R का तत्समक भी है।

E4) {0} और R दोनों ही अरिक्त हैं और प्रमेय 1 के (क) और (ख) को संतुष्ट करते हैं।

E5) क्योंकि A, B का एक उपवलय है, $A \neq \phi$ और $\forall x, y \in A$, $x - y \in A$ और $xy \in A$. यहाँ योग और गुणन वही हैं जो कि B पर परिभाषित योग और गुणन हैं। लेकिन ये वही हैं जो कि C पर परिभाषित हैं, क्योंकि B, C का उपवलय है। इस तरह A प्रमेय 1 को संतुष्ट करता है। इसलिए यह C का उपवलय है।

E6) इसके अनेक उदाहरण हैं। हम {1} लेते हैं। वास्तव में, {0} को छोड़कर **Z** का कोई भी परिमित समुच्चय एक उदाहरण होगा।

E7) $1+i$ और $\frac{1}{2}$ सम्मिलन के अवयव हैं।

परंतु $1+i-\frac{1}{2} = \frac{1}{2} + i \notin \mathbf{Z}+i\,\mathbf{Z} \cup \mathbf{Q}$. अतः

$\mathbf{Z}+i\mathbf{Z} \cup \mathbf{Q}$, **C** का उपवलय नहीं है।

E8) $2\mathbf{Z} \times \mathbf{R}$, $3\mathbf{Z} \times \{0\}$, अनंततः अनेक उदाहरणों में से दो हैं।

E9) ध्यान दीजिए कि ये दो समुच्चय $\bar{3}\mathbf{Z}_6$ और $\bar{2}\mathbf{Z}_6$ हैं।

उदाहरण 4 के अनुसार ये समुच्चय $\mathbf{Z}_6$ के उपवलय हैं। अब अवयवों का गुणन करके आप देख सकते हैं कि $rx \in \bar{3}\mathbf{Z}_6 \ \forall r \in \mathbf{Z}_6$ और $x \in \bar{3}\mathbf{Z}_6$.

(उदाहरण के लिए, $\bar{5}.\bar{3} = \overline{15} = \bar{3} \in \bar{3}\,\mathbf{Z}_6$)

इसी प्रकार आप देख सकते हैं कि $rx \in \bar{3}\mathbf{Z}_6 \ \forall r \in \mathbf{Z}_6, x \in \bar{2}\mathbf{Z}_6$.

अतः $\bar{3}\mathbf{Z}_6$ और $\bar{2}\mathbf{Z}_6$, $\mathbf{Z}_6$ की गुणजावलियाँ हैं।

E10) $I_a \neq \phi$, क्योंकि $\mathbf{0} \in I_a$.

$f, g \in I_a \Rightarrow (f-g)(a) = f(a) - g(a) = 0 \Rightarrow f - g \in I_a$.

$f \in I_a$, $g \in C[0,1] \Rightarrow (fg)(a) = f(a)\ g(a) = 0.g(a) = 0 \Rightarrow fg \in I_a$.

$\therefore I_a$, $C[0,1]$ की गुणजावली है।

E11) Ra, R का एक उपवलय है (देखिए उदाहरण 4)। आगे, $r \in R$ और $xa \in Ra$ के लिए $r(xa) = (rx)a \in Ra$.

$\therefore$ Ra, R की गुणजावली है।

E12) हम जानते हैं कि $<1> \subseteq R$. हमें दिखाना है कि $R \subseteq <1>$. अब, किसी $r \in R$ के लिए $r = r.1 \in <1>$

अतः $R \subseteq <1>$. $\therefore R = <1>$.

E13) $\bar{3}\mathbf{Z}_{10} = \{\bar{3}x \mid x \in \mathbf{Z}_{10}\} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}\}$

$= \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{2}, \bar{5}, \bar{8}, \bar{1}, \bar{4}, \bar{7}\}$

$= \mathbf{Z}_{10}$.

$\bar{5}\mathbf{Z}_{10} = \{\bar{0}, \bar{5}\}$.

E14) मान लीजिए $\mathbf{Z}_8$ की शून्यकरणी N है। तब $\bar{0} \in N$.

$\bar{1} \notin N$ क्योंकि सभी n के लिए $\bar{1}^n = \bar{1} \neq \bar{0}$

$\bar{2}^3 = \bar{0} \Rightarrow \bar{2} \in N$.

$\bar{3}^n \neq \bar{0} \ \forall n$. $\therefore \bar{3} \notin N$.

इसी प्रकार आप दिखा सकते हैं कि $\bar{4}, \bar{6} \in N$ और $\bar{5}, \bar{7} \notin N$.

$\therefore N = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$.

किसी $A \in \wp(X)$ के लिए, $A^n = A \cap A \cap \ldots \cap A = A \; \forall \; n$.

इस तरह, $A^n = \phi$ यदि और केवल यदि $A = \phi$.

अतः $\wp(X)$ की शून्य करणी $\{\phi\}$ है।

E15) सबसे पहले, $I \neq \phi$, क्योंकि $0 \in I$.

इसके बाद, $r, s \in I \Rightarrow ra = 0 = sa \Rightarrow (r-s)a = 0 \Rightarrow r-s \in I$.

अंत में, $r \in I$ और $x \in R \Rightarrow (rx)a = x(ra) = x0 = 0 \Rightarrow rx \in I$.

अतः I, R की एक गुणजावली है।

E16) (क) किसी $a \in I$ और $b \in J$ के लिए $ab \in I$ और $ab \in J$.

अतः $ab \in I \cap J$. क्योंकि $I \cap J$ एक गुणजावली है, इसलिए ऐसे अवयवों का परिमित योगफल भी $I \cap J$ में होगा। अतः $IJ \subseteq I \cap J$.

स्पष्ट है कि $I \cap J \subseteq I$, $I \cap J \subseteq J$,

$I \subseteq I + J$ और $J \subseteq I + J$.

(ख) मान लीजिए A, R की एक गुणजावली है जिसमें I और J आविष्ट हैं। तब निश्चय ही $I + J \subseteq A$.

इस तरह, (ख) सिद्ध हो जाता है।

(ग) मान लीजिए B, R की एक ऐसी गुणजावली है कि $B \subseteq I$ और $B \subseteq J$. तब निश्चय ही $B \subseteq I \cap J$.

इस तरह, (ग) सिद्ध हो जाता है।

(घ) हम दिखाना चाहते हैं कि $I \cap J \subseteq IJ$.

मान लीजिए $x \in I \cap J$. तब $x \in I$ और $x \in J$.

चूंकि $1 \in R = I + J$, इसलिए किसी $i \in I$ और $j \in J$ के लिए $1 = i + j$.

$\therefore x = x.1 = xi + xj = ix + xj \in IJ$.

अतः $I \cap J \subseteq IJ$.

E17) $1 + I$, R/I का तत्समक है।

E18) प्रमेय 4 के अनुसार $I = R$.

$\therefore R/I = \{\bar{0}\}$.

E19) मान लीजिए $x + N \in R/N$ एक शून्यंभावी अवयव है।

तब $(x+N)^n = N$ किसी धन पूर्णांक n के लिए।

$\Rightarrow x^n \in N$ किसी धन पूर्णांक n के लिए।

$\Rightarrow (x^n)^m = 0$ किसी धन पूर्णांक m के लिए

$\Rightarrow x^{nm} = 0$ किसी धन पूर्णांक nm के लिए

$\Rightarrow x \in N$

$\Rightarrow x + N = 0 + N$, R/N का शून्य अवयव।

अतः R/N का कोई शून्येतर शून्यंभावी अवयव नहीं है।

इकाई 11 वलय समाकारिताएं

इकाई की रूपरेखा

11.1 प्रस्तावना

इकाई 6 में आप समूहों के बीच ऐसे फलनों का अध्ययन कर चुके हैं जो द्वि-आधारी संक्रिया को बनाए रखते हैं। वहां आपने यह भी देखा है कि समूह की संरचना का अध्ययन करने में ये फलन कितने उपयोगी होते हैं। इस इकाई में हम वलयों के बीच ऐसे फलनों पर चर्चा करेंगे जो दोनों द्वि-आधारी संक्रियाओं को बनाए रखते हैं। ऐसे फलनों को वलय समाकारिता कहते हैं। आप देखेंगे कि समाकारिताओं की सहायता से हम वलय की बीजीय प्रकृति की जांच कैसे कर सकते हैं।

यदि समाकारिता एकैकी आच्छादक हो, तो इसे तुल्याकारिता कहते हैं। समूह सिद्धांत की तरह, वलय सिद्धांत में भी तुल्याकारिता की भूमिका बीजीयतः समान निकायों को पहचानना है। इसी कारण से ये महत्वपूर्ण हैं। इस इकाई में हम इन फलनों पर भी चर्चा करेंगे।

अंत में हम वलय समाकारिता, गुणजावली और विभाग वलय के परस्पर संबंध आपको दिखाएंगे।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- यह जांच कर सकेंगे कि कोई फलन वलय समाकारिता है कि नहीं;
- किसी भी समाकारिता की अष्टि और प्रतिबिंब प्राप्त कर सकेंगे;
- वलय समाकारिताओं और तुल्याकारिताओं के उदाहरण दे सकेंगे;
- वलय समाकारिता के कुछ गुण सिद्ध कर सकेंगे और उनका प्रयोग कर सकेंगे;
- वलयों के संबंध में समाकारिता के मूल प्रमेय का कथन दे सकेंगे, उसे सिद्ध कर सकेंगे और उसे लागू कर सकेंगे।

11.2 समाकारिता

समूह समाकारिता की संकल्पना के अनुरूप है वलय समाकारिता की संकल्पना। आपको याद होगा कि समूह समाकारिता अपने प्रांत की समूह संक्रिया को बनाए रखती है। अतः स्वाभाविक है कि हम वलय समाकारिता से आशा करें कि वह भी अपने प्रांत की वलय संरचना को बनाए रखे। निम्नलिखित परिभाषा को लीजिए।

परिभाषा : मान लीजिए $(R_1, +, .)$ और $(R_2, +, .)$ दो वलय है और $f: R_1 \to R_2$ एक फलन है। हम f को **वलय समाकारिता** (ring homomorphism) कहते हैं, यदि R_1 के सभी a,b के लिए

$f(a+b)=f(a)+f(b)$, और

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

ध्यान दीजिए कि परिभाषा के समीकरणों के वाम पक्ष में दिए गए + और . , R_1 पर परिभाषित हैं, जबकि दक्षिण पक्ष में दिए गए + और ·, R_2 पर परिभाषित हैं।

अतः हम कह सकते हैं कि $f: R_1 \to R_2$ एक समाकारिता है, यदि

i) योगफल का प्रतिबिंब, प्रतिबिंबों का योगफल हो, और

ii) गुणनफल का प्रतिबिंब, प्रतिबिंबों का गुणनफल हो।

इस तरह वलय समाकारिता f समूह $(R_1, +)$ से समूह $(R_2, +)$ तक एक समूह समाकारिता भी है।

इकाई 6 की तरह आइए यहां भी हम समाकारिताओं के कुछ उदाहरण देने से पहले समाकारिता की अष्टि और प्रतिबिंब की परिभाषा दे दें। जैसी अपेक्षा की जा सकती है, ये परिभाषाएं इकाई 6 में दी गई परिभाषाओं के अनुरूप हैं।

परिभाषा : मान लीजिए R_1 और R_2 दो वलय हैं और $f: R_1 \to R_2$ एक वलय समाकारिता है। तब

i) **f का प्रतिबिंब** (image) समुच्चय $\text{Im} f = \{f(x) \mid x \in R_1\}$ है।

ii) **f की अष्टि** (kernel) समुच्चय $\text{Ker} f = \{x \in R_1 \mid f(x) = 0\}$ है।

ध्यान दीजिए कि $\text{Im} f \subseteq R_2$ और $\text{Ker} f \subseteq R_1$. यदि $\text{Im} f = R_2$, तो f को **आच्छादक समाकारिता** (epimorphism) कहते हैं, और तब R_2 को R_1 का **समाकारी प्रतिबिंब** (homomorphic image) कहते हैं।

आइए अब हम कुछ उदाहरण लें।

उदाहरण 1 : मान लीजिए R एक वलय है। दिखाइए कि तत्समक फलन I_R एक वलय समाकारिता है। $\text{Ker}\, I_R$ और $\text{Im} I_R$ क्या होंगे ?

हल : मान लीजिए $x, y \in R$. तब

$I_R(x+y) = x+y = I_R(x) + I_R(y)$, और

$I_R(xy) = xy = I_R(x)\, I_R(y)$.

अतः I_R एक वलय समाकारिता है।

$$\begin{aligned}\text{Ker}\, I_R &= \{x \in R \mid I_R(x) = 0\}\\ &= \{x \in R \mid x = 0\}\\ &= \{0\}\\ \text{Im}\, I_R &= \{I_R(x) \mid x \in R\}\\ &= \{x \mid x \in R\}\\ &= R.\end{aligned}$$

इस तरह, I_R आच्छादक है। अतः यह एक आच्छादक समाकारिता है।

उदाहरण 2 : मान लीजिए $B \in N$. दिखाइए कि सभी $m \in Z$ के लिए $f(m) = \overline{m}$ से परिभाषित फलन $f: Z \to Z_s$ एक समाकारिता है। Ker f और Im f भी ज्ञात कीजिए।

हल : किन्हीं $m, n \in Z$ के लिए

$f(m+n) = \overline{m+n} = \overline{m} + \overline{n} = f(m) + f(n)$, और

$f(mn) = \overline{mn} = \overline{m}\,\overline{n} = f(m)\, f(n)$.

अतः f एक वलय समाकारिता है।

$$\begin{aligned}\text{अब, Ker} f &= \{m \in Z \mid f(m) = \overline{0}\}\\ &= \{m \in Z \mid \overline{m} = \overline{0}\}\\ &= \{m \in Z \mid m \equiv 0 (\text{mod } s)\}\\ &= sZ.\\ \text{Im} f &= \{f(m) \mid m \in Z\}\\ &= \{\overline{m} \mid m \in Z\}\\ &= Z_s.\end{aligned}$$

अतः f एक आच्छादक समाकारिता है।

उदाहरण 3 : फलन $f: Z_6 \to Z_3 : f(n \,(\text{mod } 6)) = n \,(\text{mod } 3)$ लीजिए। दिखाइए कि f एक वलय समाकारिता है। Ker f क्या होगा ?

हल : सबसे पहले, किन्हीं $n, m \in Z$ के लिए

$$\begin{aligned}f(n(\text{mod } 6) + m(\text{mod } 6)) &= f((n+m)\,(\text{mod } 6)) = (n+m)\,(\text{mod } 3)\\ &= n(\text{mod } 3) + m(\text{mod } 3)\\ &= f(n(\text{mod } 6)) + f(m(\text{mod } 6))\end{aligned}$$

इसी प्रकार आप दिखा सकते हैं कि

$f(n(\text{mod } 6)\cdot m(\text{mod } 6)) = f(n(\text{mod } 6))\cdot f(m(\text{mod } 6))$. अतः f एक वलय समाकारिता है।

$\text{Ker } f = \{n(\text{mod } 6) \mid n \equiv 0(\text{mod } 3)\} = \{n(\text{mod } 6) \mid n \in 3Z\} = \{\bar{0}, \bar{3}\}$, जहां उपर लगाया गया दंड 'mod 6' को प्रकट करता है।

कुछ और उदाहरणों पर विचार करने से पहले हम पारिभाषिक शब्दों के संबंध में एक टिप्पणी देना चाहेंगे। आगे से हम 'वलय समाकारिता' के स्थान पर केवल 'समाकारिता' का प्रयोग करेंगे। आपको याद होगा कि हमने समूह समाकारिताओं के लिए भी यही किया था।

अब कुछ प्रश्न।

E1) यदि S वलय R का एक उपवलय हो, तो R की संक्रियाएं + और · के सापेक्ष S एक वलय होता है। दिखाइए कि आविष्टि फलन $i: S \to R: i(x) = x$ एक समाकारिता है। Ker i और Im i क्या होंगे?

E2) मान लीजिए R_1 और R_2 दो वलय हैं। $f: R_1 \to R_2: f(x) = 0$ परिभाषित कीजिए। दिखाइए कि f एक समाकारिता है। Ker f और Im f भी ज्ञात कीजिए। (इस फलन को **तुच्छ समाकारिता** (trivial homomorphism) कहते हैं।)

E3) क्या $f: Z \to 2Z: f(x) = 2x$ एक समाकारिता है? क्यों?

ध्यान दें कि E1 की सहायता से हम कह सकते हैं कि $f(n) = n$ से परिभाषित $f: Z \to Q$ (या **R**, या **C**, या $Z + iZ$) एक समाकारिता है।

आइए अब हम कुछ और उदाहरणों पर विचार करें।

ϕ को बिंदु $x = \frac{1}{2}$ पर **मानांकन फलन** (evaluation map) कहते हैं।

उदाहरण 4 : संवृत अंतराल [0,1] पर परिभाषित सभी वास्तविक मान संतत फलनों का वलय C[0,1] लीजिए। $\phi: C[0,1] \to \mathbf{R} : \phi(f) = f(\frac{1}{2})$ परिभाषित कीजिए। दिखाइए कि ϕ एक समाकारिता है।

हल : मान लीजिए f और $g \in C[0,1]$.

तब, सभी $x \in C[0,1]$ के लिए

$(f+g)(x) = f(x) + g(x)$, और

$(fg)(x) = f(x)\, g(x)$.

अब, $\phi(f+g) = (f+g)(\frac{1}{2}) = f(\frac{1}{2}) + g(\frac{1}{2}) = \phi(f) + \phi(g)$, और

$\phi(fg) = (fg)(\frac{1}{2}) = f(\frac{1}{2})\, g(\frac{1}{2}) = \phi(f)\, \phi(g)$.

अतः ϕ समाकारिता है

उदाहरण 5 : आव्यूह योग और गुणन के सापेक्ष

वलय $R = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \;\middle|\; a, b \in \mathbf{R} \right\}$ लीजिए। दिखाइए कि फलन $f: \mathbf{Z} \to \mathbf{R} : f(n) = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$ एक समाकारिता है।

हल : ध्यान दीजिए कि $f(n) = n\,I$, जहां I कोटि 2 वाला तत्समक आव्यूह है। अब आप जांच कर सकते हैं कि

$f(n+m) = f(n) + f(m)$, और

$f(nm) = f(n)\, f(m)\ \forall\ n, m \in \mathbf{Z}$.

अतः f एक समाकारिता है।

उदाहरण 6 : इकाई 9 के उदाहरण 4 का वलय $\wp(X)$ लीजिए। मान लीजिए Y, X का एक अरिक्त उपसमुच्चय है। $f: \wp(X) \to \wp(Y) : f(A) = A \cap Y$ परिभाषित कीजिए। दिखाइए कि f एक समाकारिता है। क्या $Y^c \in \text{Ker } f$? Im f क्या होगा?

हल : $\wp(X)$ के किन्हीं A और B के लिए

$$f(A \triangle B) = f((A \setminus B) \cup (B \setminus A)).$$
$$= ((A \setminus B) \cap Y) \cup ((B \setminus A) \cap Y).$$
$$= ((A \cap Y) \setminus (B \cap Y)) \cup ((B \cap Y) \setminus (A \cap Y))$$
$$= (f(A) \setminus f(B)) \cup (f(B) \setminus f(A))$$
$$= f(A) \triangle f(B), \text{ और}$$

$$f(A \cap B) = (A \cap B) \cap Y$$
$$= (A \cap B) \cap (Y \cap Y)$$
$$= (A \cap Y) \cap (B \cap Y), \text{ क्योंकि } \cap \text{ साहचर्य और क्रमविनिमेय है।}$$
$$= f(A) \cap f(B).$$

इसलिए $f. \wp(X)$ से $\wp(Y)$ तक एक वलय समाकारिता है। अब $\wp(Y)$ का शून्य अवयव ϕ है। इसलिए

$\text{Ker } f = \{A \in \wp(X) \mid A \cap Y = \phi\}$. $\therefore Y^C \in \text{Ker } f$.

हम दिखाएंगे कि f आच्छादक है।

अब, $\text{Im } f = \{A \cap Y \mid A \in \wp(X)\}$.

अतः $\text{Im } f \subseteq \wp(Y)$.

यह दिखाने के लिए कि $\wp(Y) \subseteq \text{Im } f$, कोई $B \in \wp(Y)$ लीजिए। तब, $B \in \wp(X)$ और $f(B) = B \cap Y = B$.

इस तरह $B = \text{Im } f$. इसलिए $\text{Im } f = \wp(Y)$.

अतः f एक आच्छादक समाकारिता है।

नीचे दिए गए प्रश्नों से आपको समाकारिताओं के कुछ और उदाहरण मिल जाएंगे।

E4) मान लीजिए A और B दो वलय हैं। दिखाइए कि प्रक्षेप फलन $p : A \times B \to A : p(x,y) = x$ एक समाकारिता है। Ker p और Im p क्या होंगे ?

E5) क्या $f : Z + \sqrt{2}Z \to Z + \sqrt{2}\,Z : f(a + \sqrt{2}b) = a - \sqrt{2}b$ एक समाकारिता है ?

E6) दिखाइए कि फलन $\phi : C[0,1] \to R \times R : \phi(f) = (f(0), f(1))$ एक समाकारिता है।

अनेक उदाहरणों पर चर्चा करने के बाद आइए अब हम वलय समाकारिताओं से संबंधित कुछ आधारभूत परिणाम प्राप्त करें।

11.3 समाकारिताओं के गुण

आइए पहले हम कुछ ऐसे गुणों को देखें जो दिखाते हैं कि कोई समाकारिता किस तरह अपने प्रांत की संरचना बनाए रखती है। नीचे दिया गया परिणाम इकाई 6 के प्रमेय 1 का केवल एक पुनर्कथन है।

प्रमेय 1 मान लीजिए $f : R_1 \to R_2$ वलय R_1 से वलय R_2 तक एक समाकारिता है। तब

(क) $f(0) = 0$,

(ख) $f(-x) = -f(x) \; \forall \; x \in R_1$, और

(ग) $f(x-y) = f(x) - f(y) \; \forall \; x, y \in R_1$.

उपपत्ति : चूंकि f, $(R_1, +)$ से $(R_2, +)$ तक एक समूह समाकारिता है, इसलिए परिणाम प्राप्त करने के लिए हम इकाई 6 के प्रमेय 1 को लागू कर सकते हैं।

नीचे दिए गए प्रश्न में हम आपसे समाकारिताओं के एक अन्य गुण को सिद्ध करने के लिए कह रहे हैं।

E7) मान लीजिए $f : R_1 \to R_2$ एक आच्छादक वलय समाकारिता है। यदि R_1 तत्समक 1 सहित हो, तो दिखाइए कि R_2 तत्समक f(1) सहित है।

आइए अब हम समाकारिताओं के सापेक्ष उपवलयों के प्रतिबिंबों और प्रतिलोम प्रतिबिंबों (inverse images) पर विचार करें। (प्रतिलोम प्रतिबिंब की परिभाषा के लिए भाग 1.5 देखिए।)

प्रमेय 2 : मान लीजिए $f: R_1 \to R_2$ एक वलय समाकारिता है। तव

(क) यदि S, R_1 का एक उपवलय है, तो $f(S), R_2$ का एक उपवलय होता है।

(ख) यदि T, R_2 का एक उपवलय हो, तो $f^{-1}(T), R_1$ का एक उपवलय होता है।

उपपत्ति : हम (ख) को सिद्ध करेंगे और (क) की उपपत्ति आप पर छोड़ रहे हैं (देखिए E8)। आइए हम इकाई 10 के प्रमेय 1 का प्रयोग करें।

सवसे पहले, क्योंकि $T \neq \phi$, इसलिए $f^{-1}(T) \neq \phi$. इसके वाद, मान लीजिए $a, b \in f^{-1}(T)$. तव $f(a), f(b) \in T$.

$\Rightarrow f(a) - f(b) \in T$ और $f(a) f(b) \in T$.

$\Rightarrow f(a-b) \in T$ और $f(ab) \in T$.

$\Rightarrow a-b \in f^{-1}(T)$ और $ab \in f^{-1}(T)$

$\Rightarrow f^{-1}(T)$ एक उपवलय है।

प्रमेय 2 की उपपत्ति को पूरा करने के लिए E8 हल कीजिए।

E8) प्रमेय 2 का (क) सिद्ध कीजिए।

अव, स्वाभाविक है कि हम यह आशा करें कि प्रमेय 2 के अनुरूप ही गुणजावलियों से संवंधित प्रमेय भी होगा। लेकिन आविष्टि $i: \mathbf{Z} \to \mathbf{R}: i(x) = x$ लीजिए। आप जानते हैं कि $2\mathbf{Z}, \mathbf{Z}$ की गुणजावली है। लेकिन क्या $i(2\mathbf{Z})$ (अर्थात् $2\mathbf{Z}$) $\mathbf{R}$ की गुणजावली है ? नहीं। उदाहरण के लिए, $2 \in 2\mathbf{Z}$, $\frac{1}{4} \in \mathbf{R}$, परन्तु $2 \cdot \frac{1}{4} = \frac{1}{2} \notin 2\mathbf{Z}$. अतः **यह आवश्यक नहीं है कि गुणजावली का समाकारी प्रतिविंव भी एक गुणजावली हो।** लेकिन निराश न होइए। अभी भी हमारे पास नीचे दिया गया उपयोगी परिणाम है।

प्रमेय 3 : मान लीजिए $f: R_1 \to R_2$ एक वलय समाकारिता है।

क) यदि f आच्छादक है और I, R_1 की एक गुणजावली है, तो $f(I), R_2$ की एक गुणजावली होती है।

ख) यदि I, R_2 की एक गुणजावली है, तो $f^{-1}(I), R_1$ की एक गुणजावली होती है और $\text{Ker } f \subseteq f^{-1}(I)$.

उपपत्ति : यहाँ हम (क) सिद्ध करेंगे और (ख) को आप पर छोड़ देंगे (देखिए E9)।

सवसे पहले, क्योंकि I, R_1 का उपवलय है, इसलिए $f(I), R_2$ का उपवलय होगा।

इसके वाद, $f(x) \in f(I)$ और $r \in R_2$ लीजिए। चूंकि f आच्छादक है $\exists s \in R_1$ जिससे कि $f(s) = r$. तव $rf(x) = f(s) f(x) = f(sx) \in f(I)$, क्योंकि $sx \in I$. अतः $f(I), R_2$ की एक गुणजावली है।

उपपत्ति को पूरा करने के लिए E9 हल कीजिए।

E9) प्रमेय 3 का (ख) सिद्ध कीजिए।

अव, आच्छादक समाकारिता $f: R \to S$ लीजिए और R की गुणजावली I लीजिए। प्रमेय 3 से आप जानते हैं कि $f(I)$, S की गुणजावली है और $f^{-1}(f(I))$, R की गुणजावली है। I और $f^{-1}(f(I))$ का संवंध क्या है ? स्पष्ट है कि $I \subseteq f^{-1}(f(I))$. क्या $f^{-1}(f(I))$, $R \setminus I$ के अवयवों को आविष्ट कर सकता है ? याद रखें कि $\text{Ker } f \subseteq f^{-1}(f(I))$. अतः $I + \text{Ker } f \subseteq f^{-1}(f(I))$. वास्तव में $I + \text{Ker } f = f^{-1}(f(I))$. आइए देखें क्यों।

मान लीजिए $x \in f^{-1}(f(I))$. तव $f(x) \in f(I)$. इसलिए किसी $y \in I$ के लिए $f(x) = f(y)$. तव $f(x-y) = 0$.

$\therefore x - y \in \text{Ker } f$, अर्थात् $x \in y + \text{Ker } f \subseteq I + \text{Ker } f$.

$\therefore f^{-1}(f(I)) \subseteq I + \text{Ker } f$.

इस तरह, $f^{-1}(f(I)) = I + \text{Ker } f$.

इससे पता चलता है कि यदि $\text{Ker } f \subseteq I$, तो $f^{-1}(f(I)) = I$ (क्योंकि $\text{Ker } f \subseteq I \Rightarrow I + \text{Ker } f = I$.)

अव आप एक सरल प्रश्न को हल करना चाहेंगे ?

E10) मान लीजिए $f: R \to S$ एक आच्छादक वलय समाकारिता है। दिखाइए कि यदि J, S की एक गुणजावली है, तो $f(f^{-1}(J)) = J$.

अभी तक की गई चर्चा से हमें निम्नलिखित प्रमेय प्राप्त होता है।

प्रमेय 4 : मान लीजिए $f: R \to S$ एक आच्छादक वलय समाकारिता है। तब

(क) यदि I, R की एक गुणजावली हो जो Ker f को आविष्ट करती हो तो $I = f^{-1}(f(I))$.

(ख) Ker f को आविष्ट करने वाली R की गुणजावलियों के समुच्चय और S की गुणजावलियों के समुच्चय के बीच प्रतिचित्रण $I \to f(I)$ एक एकैकी संगति (one-to-one correspondence) को परिभाषित करता है।

उपपत्ति : ऊपर की चर्चा में हम (क) सिद्ध कर चुके हैं। आइए अब हम (ख) सिद्ध करें।

मान लीजिए A, Ker f को आविष्ट करने वाली R की गुणजावलियों का समुच्चय है और B, S की गुणजावलियों का समुच्चय है।

$\phi : A \to B : \phi(I) = f(I)$ परिभाषित कीजिए।

हम दिखाना चाहते हैं कि ϕ एकैकी और आच्छादक है।

ϕ आच्छादक है : यदि $J \in B$ तो प्रमेय 3 के अनुसार $f^{-1}(J) \in A$ और $\text{Ker } f \subseteq f^{-1}(J)$. अब

$\phi(f^{-1}(J)) = f(f^{-1}(J)) = J$, E10 की सहायता से।

ϕ एकैकी है : यदि I_1 और I_2, Ker f को आविष्ट करने वाली R की गुणजावलियां हों, तो

$$\begin{aligned}\phi(I_1) = \phi(I_2) &\Rightarrow f(I_1) = f(I_2)\\ &\Rightarrow f^{-1}(f(I_1)) = f^{-1}(f(I_2))\\ &\Rightarrow I_1 = I_2, \text{(क) के अनुसार}\end{aligned}$$

अतः ϕ एकैकी आच्छादक है।

इस परिणाम की सहायता से नीचे दिए गए प्रश्न हल कीजिए।

E11) समाकारिता $f : Z \to Z_{12} : f(z) = \bar{z}$ की अष्टि ज्ञात कीजिए। Z_{12} की गुणजावलियां भी ज्ञात कीजिए।

E12) दिखाइए कि समाकारिता $f: Z \to Z \times Z : f(n) = (n, n)$ आच्छादक नहीं है। $Z \times Z$ की एक ऐसी गुणजावली ज्ञात कीजिए जो $f(I)$ के रूप की नहीं है, जहां I, Z की एक गुणजावली है।

आइए अब हम किसी वलय समाकारिता f के लिए समुच्चयों Ker f और Im f को ध्यान से देखें। इकाई 6 में हम सिद्ध कर चुके हैं कि यदि $f: G_1 \to G_2$ एक समूह समाकारिता है, तो Ker f, G_1 का एक प्रसामान्य उपसमूह होता है और Im f, G_2 का एक उपसमूह होता है। इसी परिणाम के अनुरूप वलय समाकारिताओं के लिए परिणाम हैं, जिनका अंदाज़ा आपको अभी तक अध्ययन किए गए उदाहरणों से हो गया होगा।

प्रमेय 5 : मान लीजिए $f: R_1 \to R_2$ एक वलय समाकारिता है। तब

(क) Ker f, R_1 की गुणजावली है।

(ख) Im f, R_2 का उपवलय है।

उपपत्ति : (क) क्योंकि $\{0\}$, R_2 की गुणजावली है, इसलिए प्रमेय 3 (ख) के अनुसार $f^{-1}(\{0\})$, R_1 की गुणजावली होगी। परन्तु $f^{-1}(\{0\}) = \text{Ker } f$. इस तरह हमने दिखाया है कि Ker f, R_1 की गुणजावली है।

(ख) क्योंकि R_1, R_2 का उपवलय है, इसलिए प्रमेय 2 (क) के अनुसार $f(R_1)$, R_2 का उपवलय होगा। अतः Im f, R_2 का उपवलय है।

कुछ समुच्चयों की गुणजावली सिद्ध करने के लिए यह परिणाम काफ़ी उपयोगी है। उदाहरण के लिए, प्रमेय 5 और उदाहरण 3 से आप तुरंत यह निष्कर्ष निकाल सकते हैं कि $\{\bar{0}, \bar{3}\}$, Z_6 की गुणजावली है। जैसे-जैसे हम आगे बढ़ते जाएंगे आप प्रमेय 5 के इस प्रयोग के और उदाहरण देखेंगे।

आइए अब हम समाकारिता की अष्टि को करीब से देखें। हम इकाई 6 के प्रमेय 4 के अनुरूप एक परिणाम सिद्ध करेंगे।

एकैकी समाकारिता को **एकक समाकारिता** (Monomorphism) कहते हैं

प्रमेय 6 : मान लीजिए $f: R_1 \to R_2$ एक समाकारिता है। तब, f एकैकी होता है, यदि और केवल यदि $\text{Ker } f = \{0\}$.

उपपत्ति : f एकैकी होता है यदि और केवल यदि f, $(R_1, +)$ से $(R_2, +)$ तक एक एकैकी समूह समाकारिता हो। इकाई 6 के प्रमेय 4 के अनुसार यह सत्य होता है यदि और केवल यदि $\text{Ker } f = \{0\}$.

इस तरह हमारा परिणाम सिद्ध हो जाता है।

प्रमेय 6 की सहायता से नीचे दिया गया प्रश्न हल कीजिए।

E13) उदाहरण 1 से उदाहरण 6 तक के समाकारिताओं में से कौन से 1-1 हैं?

अभी तक हमने देखा है कि यदि कोई वलय समाकारिता $f: R \rightarrow S$ दी हुई हो, तो हम R की एक गुणजावली, अर्थात् Ker f प्राप्त कर सकते हैं। अब बताइए कि यदि वलय R की कोई गुणजावली I दी हुई हो, तो क्या हम एक ऐसी समाकारिता f परिभाषित कर सकते हैं, जिससे कि Ker f = I ?

नीचे दिए गए प्रमेय से इस प्रश्न का उत्तर प्राप्त हो जाता है। इस प्रमेय का अध्ययन करने से पहले आप इकाई 10 में दी गई विभाग वलय की परिभाषा को दोहरा लीजिए।

प्रमेय 7 : यदि I वलय R की एक गुणजावली है, तो एक ऐसी वलय समाकारिता $f: R \rightarrow R/I$ का अस्तित्व होता है जिसकी अष्टि I है।

उपपत्ति : आइए हम $f: R \rightarrow R/I : f(a) = a+I$ परिभाषित करें। आइए देखें कि f एक समाकारिता है कि नहीं। इसके लिए $a, b \in R$ लीजिए। तब

$$f(a+b) = (a+b)+I = (a+I) + (b+I) = f(a) + f(b), \text{ और}$$

$$f(ab) = ab + I = (a+I)(b+I) = f(a) f(b).$$

अतः f एक समाकारिता है।

और, $\text{Ker } f = \{a \in R \mid f(a) = 0+I\} = \{a \in R \mid a+I = I\}$
$= \{a \in R \mid a \in I\} = I.$

इस तरह, प्रमेय सिद्ध हो जाता है।

यहां यह भी ध्यान दीजिए कि समाकारिता f आच्छादक है।

ऊपर की उपपत्ति में परिभाषित समाकारिता को R से R/I पर **विहित (या प्राकृतिक) समाकारिता** (canonical or natural homomorphism) कहते हैं।

अब आप इस सरल प्रश्न को हल कीजिए।

E14) मान लीजिए S वलय R का एक उपवलय है। क्या हम हमेशा एक ऐसी वलय समाकारिता को परिभाषित कर सकते हैं जिसका प्रांत R हो और जिसकी अष्टि S हो? क्यों?

आइए अब हम समाकारिताओं के संयोजन पर विचार करें। निश्चय ही नीचे दिए गए परिणाम से आपको हैरानी होगी।

प्रमेय 8 : मान लीजिए R_1, R_2 और R_3 वलय हैं और $f: R_1 \rightarrow R_2$ तथा $g: R_2 \rightarrow R_3$ वलय समाकारिताएं हैं। तब इनका संयोजन $g \circ f: R_1 \rightarrow R_3 : (g \circ f)(x) = g(f(x))$ एक वलय समाकारिता है।

इस परिणाम की उपपत्ति वैसी ही है जैसी कि इकाई 6 में दिए गए इसके संगत परिणाम की उपपत्ति। इसे हम आपके लिए छोड़ रहे हैं (नीचे दिया गया प्रश्न देखिए)।

E15) प्रमेय 8 सिद्ध कीजिए।

E16) प्रमेय 8 की स्थिति में सिद्ध कीजिए कि

(क) यदि $g \circ f$, 1−1 है, तो f भी 1−1 है।

(ख) यदि $g \circ f$ आच्छादक है, तो g भी आच्छादक है।

E17) प्रमेय 8 की सहायता से दिखाइए कि फलन $h: Z \times Z \rightarrow Z_2 : h(n, m) = \bar{m}$ एक समाकारिता है।

आइए अब हम देखें कि वलय सिद्धांत में समूह तुल्याकारिता का अनुरूप क्या है।

11.4 तुल्याकारिता प्रमेय

काई 6 में हम समूह तुल्याकारिताओं और इनसे संबंधित अनेक परिणामों पर चर्चा कर चुके हैं। इस भाग में यही ात वलयों के लिए करेंगे। आइए पहले हम वलय तुल्याकारिता (ring isomorphism) को परिभाषित करें।

ारिभाषा : मान लीजिए R_1 और R_2 दो वलय हैं। फलन $f: R_1 \rightarrow R_2$ को **वलय तुल्याकारिता** (या केवल तुल्याकारिता) कहते हैं यदि

) f एक वलय समाकारिता हो,

i) f, 1 – 1 हो, और

ii) f आच्छादक हो।

इस तरह, हम पाते हैं कि तुल्याकारिता एक एकैकी आच्छादक समाकारिता होती है।

किसी वलय R से स्वयं तक की तुल्याकारिता को R की **स्वाकारिता** (automorphism) कहते हैं।

यदि $f: R_1 \rightarrow R_2$ एक तुल्याकारिता है तो हम कहते हैं कि R_1 और R_2 **तुल्याकारी** (isomorphic) हैं, और इसे $R_1 \simeq R_2$ से प्रकट करते हैं।

यहां हम एक टिप्पणी देना चाहेंगे।

टिप्पणी : दो वलय तुल्याकारी होते हैं यदि और केवल यदि वे बीजीयतः अभिन्न हों। यानि कि तुल्याकारी वलयों के बिल्कुल एक जैसे ही बीजीय गुण होने चाहिए। इस तरह, यदि R_1 तत्समकी वलय हो तो यह तत्समक के बिना किसी वलय के तुल्याकारी नहीं हो सकता। इसी प्रकार, यदि R_1 की गुणजावलियाँ केवल {0} और स्वयं हों, तो R_1 के तुल्याकारी किसी वलय में भी यह गुण अवश्य होगा।

अब, नीचे दिए गए प्रश्नों को हल कीजिए। इन्हें हल करने से आप तुल्याकारिताओं से और अधिक परिचित हो जाएंगे।

E18) निम्नलिखित फलनों में से कौन से फलन तुल्याकारिताएं हैं।

(क) $f: \mathbf{Z} \rightarrow \mathbf{R} : f(n) = n$

(ख) $f: \mathbf{Z} \rightarrow 5\mathbf{Z} : f(n) = 5n$

(ग) $f: \mathbf{C} \rightarrow \mathbf{C} : f(z) = \bar{z}$, z का संमिश्र संयुग्मी।

E19) मान लीजिए $\phi: R_1 \rightarrow R_2$ एक वलय तुल्याकारिता है। तब $\phi^{-1}: R_2 \rightarrow R_1$ एक सुपरिभाषित फलन है क्योंकि ϕ एकैकी आच्छादक है। दिखाइए कि ϕ^{-1} भी एक तुल्याकारिता है।

$R_1 \simeq R_2$ यदि और केवल यदि $R_2 \simeq R_1$.

E20) दिखाइए कि तुल्याकारिताओं का संयोजन एक तुल्याकारिता है।

और आइए अब थोड़ी देर के लिए इकाई 6 की ओर लौट चलें। वहां हमने समूहों के लिए समाकारिता के मूल प्रमेय को सिद्ध किया था। इसके अनुसार समूह G का समाकारी प्रतिबिंब G के किसी विभाग समूह के तुल्याकारी होता है। अब हम इसी प्रकार का परिणाम वलयों के लिए सिद्ध करेंगे। अर्थात् हम वलयों के लिए प्रथम तुल्याकारिता प्रमेय (या समाकारिता का मूल प्रमेय) सिद्ध करेंगे।

प्रमेय 9 (समाकारिता का मूल प्रमेय) : मान लीजिए $f: R \rightarrow S$ एक वलय समाकारिता है। तब $R/\text{Ker } f \simeq \text{Im } f$. विशेष रूप से, यदि f आच्छादक है, तो $R/\text{Ker } f \simeq S$.

उपपत्ति : सबसे पहले ध्यान दीजिए कि $R/\text{Ker } f$ एक सुपरिभाषित विभाग वलय है, क्योंकि Ker f, R की एक गुणजावली है। हम सुविधा के लिए $\text{Ker } f = I$ लेंगे।

आइए हम $\psi: R/I \rightarrow S : \psi(x+I) = f(x)$ परिभाषित करें। इकाई 6 के प्रमेय 8 की तरह हमें यहां भी सत्यापित करना होगा कि ψ सुपरिभाषित है, अर्थात् यदि $x+I = y+I$ तो $\psi(x+I) = \psi(y+I)$.

अब, $x+I = y+I \Rightarrow x-y \in I = \text{Ker } f \Rightarrow f(x-y) = 0 \Rightarrow f(x) = f(y) \Rightarrow \psi(x+I) = \psi(y+I)$.

अतः ψ सुपरिभाषित है।

आइए अब हम देखें कि ψ एक तुल्याकारिता है कि नहीं।

i) ψ एक समाकारिता है : मान लीजिए $x, y \in R$. तब

$$\psi((x+I)+(y+I)) = \psi(x+y+I) = f(x+y) = f(x) + f(y)$$
$$= \psi(x+I) + \psi(y+I), \text{ और}$$
$$\psi((x+I)(y+I)) = \psi(xy+I) = f(xy) = f(x)\, f(y)$$
$$= \psi(x+I)\, \psi(y+I).$$

अतः ψ एक वलय समाकारिता है।

ii) $\text{Im}\, \psi = \text{Im}\, f$: चूंकि $\psi(x+I) = f(x) \in \text{Im}\, f\ \forall x \in R$, इसलिए $\text{Im}\, \psi \subseteq \text{Im}\, f$. साथ ही $\text{Im}\, f$ का कोई भी अवयव किसी $x \in R$ के लिए $f(x) = \psi(x+I)$ के रूप का होता है। इस तरह, $\text{Im}\, f \subseteq \text{Im}\, \psi$. इसलिए $\text{Im}\, \psi = \text{Im}\, f$.

iii) ψ, 1−1 है : इसे दिखाने के लिए मान लीजिए $x, y \in R$ जहां $\psi(x+I) = \psi(y+I)$. तब $f(x) = f(y)$, जिससे कि $f(x-y) = 0$, अर्थात् $x-y \in \text{Ker}\, f = I$ अर्थात् $x+I = y+I$.

अतः ψ, 1−1 है।

इस तरह, हमने दिखाया है कि $R/\text{Ker}\, f \simeq \text{Im}\, f$.

अतः यदि f आच्छादक है, तो $\text{Im}\, f = S$ और $R/\text{Ker}\, f \simeq S$.

ध्यान दीजिए कि इस परिणाम के अनुसार f संयोजन $\psi_\circ \eta$ है, जहां η विहित समाकारिता $\eta : R \to R/I : \eta(a) = a+I$ है। इसे चित्रीय रूप में निम्न प्रकार से दिखाया जा सकता है।

आइए अब हम मूल प्रमेय के प्रयोग के कुछ उदाहरणों पर विचार करें।

$p : \mathbf{Z} \to \mathbf{Z}_m : p(n) = \bar{n}$ लीजिए। p एक आच्छादक समाकारिता है और

$\text{Ker}\, p = \{n \mid \bar{n} = \bar{0}, \mathbf{Z}_m \text{ में}\} = m\mathbf{Z}$.

इसलिए $\mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}_m$.

(ध्यान दीजिए कि हमने इस बात का प्रयोग कई बार किया है कि $\mathbf{Z}/m\mathbf{Z}$ और $\mathbf{Z}_m$ समान हैं।)

एक अन्य उदाहरण के लिए प्रक्षेप फलन (projection map) $p : R_1 \times R_2 \to R_1 : p(a,b) = a$ लीजिए, जहाँ R_1 और R_2 वलय हैं। तब p आच्छादक है, और इसकी अष्टि $\{(0,b) \mid b \in R_2\}$ है, जो R_2 के तुल्याकारी है।

इसलिए $(R_1 \times R_2)/R_2 \simeq R_1$

अब आप इस प्रश्न को हल कीजिए।

E21) उदाहरण 1 से उदाहरण 6 तक की प्रत्येक स्थिति में समाकारिता का मूल प्रमेय क्या कहता है ?

आइए अब हम प्रमेय 9 को लागू करके सिद्ध करें कि किसी वलय R से Z तक की आच्छादक वलय समाकारिता अपनी अष्टि से अद्वितीयतः निर्धारित हो जाती है। यानि कि R से Z तक की समान अष्टि वाली दो अलग-अलग आच्छादक वलय समाकारिताएं नहीं हो सकतीं। (ध्यान दीजिए कि यह बात समूह समाकारिताओं के लिए सही नहीं है। उदाहरण के लिए, आप जानते हैं कि I_Z और $-I_Z$, Z से स्वयं तक की समान अष्टि $\{0\}$ वाली दो अलग-अलग आच्छादक समाकारिताएं हैं।) इस कथन को सिद्ध करने के लिए हमें निम्नलिखित परिणाम की आवश्यकता है।

प्रमेय 10 : Z से स्वयं तक की केवल एक अतुच्छ वलय समाकारिता है, अर्थात् $I_{\mathbf{Z}}$.

उपपत्ति : मान लीजिए $f : \mathbf{Z} \to \mathbf{Z}$ एक अतुच्छ वलय समाकारिता है। मान लीजिए n एक धन पूर्णांक है। तब

$n = 1+1+\ldots+1.$ (n बार)

इसलिए,

$f(n) = f(1)+f(1)+\ldots+f(1)$ (n बार) $= nf(1)$.

और, यदि n एक ऋण पूर्णांक है, तो $-n$ धन पूर्णांक होगा। इसलिए $f(-n)=(-n)f(1)$, क्योंकि f एक समाकारिता है। अतः इस स्थिति में भी $f(n) = nf(1)$.

और $f(0) = 0 = 0\, f(1)$.

अतः $f(n) = nf(1)\ \forall\ n \in Z$ ..... (1)

अब, क्योंकि f एक अतुच्छ समाकारिता है, इसलिए किसी $m \in Z$ के लिए $f(m) \neq 0$.

तब, $f(m) = f(m.1) = f(m)\, f(1)$.

दोनों ओर $f(m)$ का निरसन करने पर हमें $f(1) = 1$ प्राप्त होता है। इसलिए (1) से हम पाते हैं कि

$f(n) = n \forall n \in Z$, अर्थात् $f = I_Z$.

इस प्रमेय का एक महत्वपूर्ण उपप्रमेय है।

उपप्रमेय : मान लीजिए कोई वलय R, **Z** के तुल्याकारी है। यदि f और g, R से **Z** तक की दो आच्छादक समाकारिताएं हों, तो $f = g$.

उपपत्ति : संयोजन $f \circ g^{-1}$, **Z** से स्वयं तक की एक तुल्याकारिता है। इसलिए, प्रमेय 10 के अनुसार, $f \circ g^{-1} = I_Z$, अर्थात् $f = g$.

अब हम निम्नलिखित परिणाम को सिद्ध कर सकते हैं।

प्रमेय 11 : मान लीजिए R एक वलय है और f तथा g, R से Z तक की ऐसी समाकारिताएं हैं कि $\text{Ker } f = \text{Ker } g$. तब $f = g$.

उपपत्ति : प्रमेय 9 के अनुसार, तुल्याकारिताएं $\psi_f : R/\text{Ker } f \to \mathbf{Z}$ और $\psi_g : R/\text{Ker } g \to \mathbf{Z}$, परिभाषित हैं। क्योंकि $\text{Ker } f = \text{Ker } g$, इसलिए ψ_f और ψ_g एक ही वलय से **Z** तक की तुल्याकारिताएं हैं। अतः ऊपर के उपप्रमेय के अनुसार, $\psi_f = \psi_g$.

साथ ही, क्योंकि $\text{Ker } f = \text{Ker } g$, इसलिए विहित फलन

$\eta_f : R \to R/\text{Ker } f$ और $\eta_g : R \to R/\text{Ker } g$ समान हैं।

$\therefore f = \psi_f \circ \eta_f = \psi_g \circ \eta_g = g$

अब हम आपको प्रमेय 9 के दो अनुप्रयोगों को सिद्ध करने का मौका दे रहे हैं। ये अनुप्रयोग इकाई 6 के प्रमेय 10 और प्रमेय 11 के अनुरूप हैं।

E22) (द्वितीय समाकारिता प्रमेय) मान लीजिए S वलय R का एक उपवलय है और I, R की एक गुणजावली है। दिखाइए कि $(S+I)/I \simeq S/(S \cap I)$.

E23) (तृतीय तुल्याकारिता प्रमेय) मान लीजिए I और J वलय R की ऐसी गुणजावलियां हैं कि $J \subseteq I$. दिखाइए कि I/J वलय R/J की गुणजावली है और $(R/J)/(I/J) \simeq R/I$.

आइए अब हम समाकारिताओं पर अपनी चर्चा को यहीं रोकें और जो इस इकाई में हमने किया है, उसे संक्षेप में दोहराएं। इन फलनों की चर्चा हम अगली इकाइयों में करते रहेंगे।

1.5 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों पर चर्चा की है।

वलय समाकारिता, इसकी अष्टि और इसके प्रतिबिंब की परिभाषा और अनेक उदाहरण।

किसी समाकारिता के सापेक्ष उपवलय का प्रतिबिंब या प्रतिलोम प्रतिबिंब एक उपवलय होता है।

यदि $f : R \to S$ एक वलय समाकारिता है, तो

i) $\text{Im } f$, S का उपवलय है,

ii) $\text{Ker } f$, R की गुणजावली है,

iii) S की प्रत्येक गुणजावली I के लिए $f^{-1}(I)$, R की गुणजावली होती है।

iv) यदि f आच्छादक है, तो $f(I)$, S की गुणजावली होती है।

4 समाकारिता एकैकी होती है यदि और केवल यदि इसकी अष्टि $\{0\}$ हो।

5 समाकारिताओं का संयोजन एक समाकारिता है।

6 वलय तुल्याकारिता की परिभाषा और उसके उदाहरण।

7 समाकारिता के मूल प्रमेय की उपपत्ति और उसके अनुप्रयोग।
इस प्रमेय के अनुसार, यदि $f: R \to S$ एक वलय समाकारिता है, तो $R/\text{Ker } f \simeq \text{Im } f$.

11.6 हल/उत्तर

E1) $x, y \in S$ के लिए

$i(x+y) = x+y = i(x)+i(y)$, और

$i(xy) = xy = i(x)\, i(y)$

$\therefore$ i एक समाकारिता है।

$\text{Ker } i = \{x \in S \mid i(x) = 0\} = \{0\}$

$\text{Im } i = \{i(x) \mid x \in S\} = S$.

E2) किन्हीं $x, y \in R_1$ के लिए

$f(x+y) = 0 = 0+0 = f(x)+f(y)$, और

$f(xy) = 0 = 0 \cdot 0 = f(x) \cdot f(y)$.

$\therefore$ f एक समाकारिता है।

$\text{Ker } f = \{x \in R_1 \mid f(x) = 0\} = R_1$

$\text{Im } f = \{0\}$.

E3) $f(2.3) = f(6) = 12$, लेकिन $f(2).f(3) = 4.6 = 24$.

अतः $f(2.3) \neq f(2)\, f(3)$.

$\therefore$ f एक समाकारिता नहीं है।

E4) किन्हीं $(a,b), (c,d) \in A \times B$ के लिए

$p((a,b)+(c,d)) = p(a+c, b+d) = a+c = p(a,b)+p(c,d)$.

$p((a,b)\,(c,d)) = p(ac, bd) = ac = p(a,b)\, p(c,d)$.

$\text{Ker } p = \{(a,b) \in A \times B \mid a=0\} = \{0\} \times B$.

$\text{Im } p = \{p(a,b) \mid (a,b) \in A \times B\} = \{a \mid (a,b) \in A \times B\} = A$.

E5) हां, आप इसकी जांच कर सकते हैं।

E6) $f, g \in C[0,1]$ के लिए

$$\begin{aligned}
\phi(f+g) &= ((f+g)(0), (f+g)(1)) \\
&= (f(0), f(1)) + (g(0), g(1)) \\
&= \phi(f) + \phi(g), \text{ और} \\
\phi(fg) &= (fg(0), fg(1)) = (f(0), g(0))\,(f(1), g(1)) \\
&= \phi(f)\, \phi(g).
\end{aligned}$$

$\therefore$ ϕ एक समाकारिता है।

E7) मान लीजिए $x \in R_2$, क्योंकि f आच्छादक है, इसलिए $\exists\, r \in R_1$ जिससे कि $f(r) = x$.

क्योंकि $r \cdot 1 = r$, इसलिए $f(r)\, f(1) = f(r)$.

अतः $x f(1) = x$. यह बात किसी भी $x \in R_2$ के लिए सत्य है।

$\therefore$ $f(1)$, R_2 का तत्समक है।

) फिर से इकाई 10 के प्रमेय 4 को लागू कीजिए।

i) $S \neq \phi \Rightarrow f(S) \neq \phi$.

ii) मान लीजिए $a', b' \in f(S)$, तब $\exists\, a, b \in S$ जिससे कि $f(a)=a'$, $f(b)=b'$.

अब $a'-b' = f(a)-f(b) = f(a-b) \in f(S)$, क्योंकि $a-b \in S$.

और $a'b' = f(a)f(b) = f(ab) \in f(S)$ क्योंकि $ab \in S$.

$\therefore f(S)$, R_2 का एक उपवलय है।

) क्योंकि I, R_2 का उपवलय है, इसलिए $f^{-1}(I)$, R_1 का उपवलय है। अब, मान लीजिए, $a \in f^{-1}(I)$ और $r \in R_1$.

हम दिखाना चाहते हैं कि $ar \in f^{-1}(I)$.

क्योंकि $a \in f^{-1}(I)$, $f(a) \in I$. $\therefore f(a)f(r) \in I$, अर्थात्

$f(ar) \in I$. $\therefore ar \in f^{-1}(I)$.

अतः $f^{-1}(I)$, R_1 की गुणजावली है।

और, यदि $x \in \text{Ker } f$, तो $f(x)=0 \in I$.

$\therefore x \in f^{-1}(I)$.

$\therefore \text{Ker } f \subseteq f^{-1}(I)$.

) मान लीजिए $x \in f(f^{-1}(J))$, तब $x=f(y)$, जहां $y \in f^{-1}(J)$, अर्थात् $f(y) \in J$, अर्थात् $x \in J$, इस तरह, $f(f^{-1}(J)) \subseteq J$.

अब, मान लीजिए $x \in J$, क्योंकि f आच्छादक है $\exists\, y \in R$ जिससे कि $f(y)=x$.

तब $y \in f^{-1}(x) \subseteq f^{-1}(J)$.

$\therefore x = f(y) \in f(f^{-1}(J))$.

अतः $J \subseteq f(f^{-1}(J))$.

इस तरह, परिणाम सिद्ध हो जाता है।

$\text{Ker } f = \{n \in Z \mid n \equiv 0 \pmod{12}\} = 12Z$.

अब, आप जानते हैं कि Z की कोई भी गुणजावली Z का एक उपवलय होती है। अतः यह किसी $n \in N$ के लिए nZ होगी। इस तरह Ker f को अन्तर्विष्ट करने वाली Z की गुणजावलियाँ वे सभी nZ होंगी जिनके लिए $n/12$, अर्थात् Z, 2Z, 3Z, 4Z, 6Z, 12Z. इस तरह, प्रमेय 4 (ख) के अनुसार, Z_{12} की गुणजावलियां हैं, Z_{12}, $\bar{2}Z_{12}$, $\bar{3}Z_{12}$, $\bar{4}Z_{12}$, $\bar{6}Z_{12}$ और $\{\bar{0}\}$.

उदाहरण के लिए, $(0,1) \in \text{Im } f$.

Z की किसी गुणजावली I के लिए, $f(I) = I \times I$.

इस तरह, $Z \times Z$ की गुणजावली $Z \times \{0\}$, Z की किसी भी गुणजावली I के लिए $f(I)$ के रूप में नहीं हो सकती।

उदाहरण 1 और 5 की समाकारिताएं।

नहीं। उदाहरण के लिए, Q का उपवलय Z लीजिए। क्योंकि Z, Q की गुणजावली नहीं है, इसलिए यह Q से किसी अन्य वलय तक की किसी समाकारिता की अष्टि नहीं हो सकती।

किन्हीं $x, y \in R_1$ के लिए

$$\begin{aligned} g\circ f(x+y) &= g(f(x+y)) = g(f(x)+f(y)) \\ &= g\circ f(x) + g\circ f(y), \text{ और} \\ g\circ f(xy) &= g(f(xy)) = g(f(x)\,f(y)) \\ &= g\circ f(x)\; g\circ f(y), \text{ और} \end{aligned}$$

इस तरह, $g\circ f$ एक समाकारिता है।

क) $x \in \text{Ker } f \Rightarrow f(x) = 0 \Rightarrow g\circ f(x) = 0 \Rightarrow x=0$,

क्योंकि $g\circ f$, 1−1 है।

$\therefore \text{Ker } f = \{0\}$.

$\therefore f$, 1−1 है।

(ख) मान लीजिए $x \in R_3$. क्योंकि $g_o f$ आच्छादक है, $\exists\ y \in R_1$ जिससे कि $g_o f\,(y) = x$, अर्थात् $g(f(y)) = x$. अतः g आच्छादक है।

E17) h प्रक्षेप फलन $p : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z} : p(n,m) = m$ और फलन $f : \mathbf{Z} \to \mathbf{Z}_2 : f(r) = \bar{r}$ का संयोजन है। p और f दोनों ही वलय समाकारिताएं हैं। $\therefore$ h एक वलय समाकारिता है।

E18) (क) f आच्छादक नहीं है। इसलिए यह तुल्याकारिता नहीं है।

(ख) f समाकारिता नहीं है।

(ग) C के अवयवों के गुणों के लिए इकाई 2 का परिशिष्ट देखिए। तब आप आसानी से सिद्ध कर सकते हैं कि f एक तुल्याकारिता है।

E19) मान लीजिए $x, y \in R_2$ और $\phi^{-1}(x) = r$, $\phi^{-1}(y) = s$. तब $x = \phi(r)$ और $y = \phi(s)$. इसलिए

$x + y = \phi(r) + \phi(s) = \phi(r+s)$ और $xy = \phi(rs)$.

$\therefore\ \phi^{-1}(x+y) = r+s = \phi^{-1}(x) + \phi^{-1}(y)$, और

$\phi^{-1}(xy) = rs = \phi^{-1}(x)\,\phi^{-1}(y)$.

अतः ϕ^{-1} एक समाकारिता है।

आप पहले से जानते हैं कि यह एकैकी आच्छादक है।

अतः ϕ^{-1} एक तुल्याकारिता है।

E20) मान लीजिए $f : R_1 \to R_2$ और $g : R_2 \to R_3$ वलय समाकारिताएं हैं। प्रमेय 8 से आप जानते हैं कि $g_o f$ एक समाकारिता है। शेष भाग के लिए आप वही प्रक्रिया अपनाइए जो कि इकाई 6 के E12 में आपने अपनाई थी।

E21) उदाहरण 1 : $R \simeq R$

उदाहरण 2 : अभी हमने ऊपर जो कुछ किया है, अर्थात् $\mathbf{Z}/s\,\mathbf{Z} \simeq \mathbf{Z}_s$.

उदाहरण 3 : $\mathbf{Z}_6/\{\bar{0}, \bar{3}\} \simeq \mathbf{Z}_3$

उदाहरण 4 : $\text{Ker}\ \phi = \{f \in C[0,1] \mid f(\frac{1}{2}) = 0\}$

$\text{Im}\ \phi = \mathbf{R}$ (क्योंकि यदि कोई $r \in \mathbf{R}$ दिया हो तो हम अचर फलन $f_r : [0,1] \to \mathbf{R} : f_r(x) = r$ परिभाषित कर सकते हैं। तब $f_r(\frac{1}{2}) = r$.

इस तरह, $r = \phi(f_r) \in \text{Im}\,\phi$.)

उदाहरण 5 : $\mathbf{Z} \simeq \{nI \mid n \in \mathbf{Z}\}$

उदाहरण 6 : $\wp(X)/\text{Ker}\ f \simeq \wp(Y)$

E22) क्योंकि I, R की एक गुणजावली है और $I \subseteq S+I$, इसलिए यह $S+I$ की एक गुणजावली है।

इस तरह, $(S+I)/I$ एक सुपरिभाषित वलय है।

$f : S \to (S+I)/I : f(x) = x + I$ परिभाषित कीजिए।

तब आप जांच कर सकते हैं कि

$f(x+y) = f(x) + f(y)$, और

$f(xy) = f(x)\,f(y)\ \forall\ x, y \in S$.

जैसा कि आपने इकाई 6 के प्रमेय 10 में किया था, उसी प्रक्रिया से आप यहां भी जांच कर सकते हैं कि f आच्छादक है और $\text{Ker}\ f = S \cap I$. इस तरह $S/(S \cap I) \simeq (S+I)/I$.

E23) $f : R/J \to R/I : f(r+J) = r + I$ परिभाषित कीजिए। जैसा कि आपने इकाई 6 के प्रमेय 11 में किया था, यहां भी आप जांच कर सकते हैं कि f सुपरिभाषित है, f आच्छादक है और $\text{Ker}\ f = I/J$. इस तरह, I/J, R/J की एक गुणजावली है और $(R/J)/(I/J) \simeq R/I$

व्दावली

तुच्छ गुणजावली	non-trivial ideal
तुच्छ समाकारिता	non-trivial homomorphism
तराकारिता	endomorphism
धःस्थ समुच्चय	underlying set
भिगृहीत	axiom
वशेष वर्ग	residue class
ष्टि	kernel
च्छादक समाकारिता	epimorphism
चित गुणजावली	proper ideal
पवलय	subring
कल	singleton
कैक समाकारिता	monomorphism
मविनिमेय वलय	commutative ring
गुणजावली	ideal
तुष्टयी	quaternion
नक	generator
तसमकी वलय	ring with identity
तुच्छ गुणजावली	trivial ideal
तुच्छ वलय	trivial ring
द्वि-आधारी संक्रिया	binary operation
द्विपद प्रसार	binomial expansion
प्रक्षेप फलन	projection map
बंटन (या वितरण) नियम	distributive law
बिंदुशः	pointwise
बीजावली	algebra
बूलीय वलय	Boolean ring
मुख्य गुणजावली	principal ideal
योज्य प्रतिलोम	additive inverse
वलय	ring
वलय सिद्धान्त	ring theory
विभाग वलय	quotient ring
विहित समाकारिता	canonical homomorphism
शून्य करणी	nil radical
शून्यकारी	annihilator
शून्यंभावी	nilpotent
संतत	continuous
संवृत अंतराल	closed interval
समाकारिता का मूल प्रमेय	Fundamental theorem of homomorphism
समाकारी प्रतिबिंब	homomorphic map
समशेषता	congruence
साहचर्य	associativity
स्वाकारिता	automorphism

NOTES

NOTES

उत्तर प्रदेश
राजर्षि टण्डन मुक्त विश्वविद्यालय

UGMM – 06
अमूर्त बीजगणित

खंड

4

पूर्णांकीय प्रांत और क्षेत्र

पूर्णांकीय प्रांत और क्षेत्र

इस खंड में हम वलय सिद्धांत पर अपनी चर्चा जारी रखेंगे। खंड के प्रारंभ में दो विशेष प्रकार के वलयों-पूर्णांकीय प्रांत और क्षेत्र, से हम आपका परिचय कराएंगे। फिर हम इनके गुणों पर विस्तार से चर्चा करेंगे।

इस खंड की दूसरी इकाई में हम उन वलयों की चर्चा करेंगे जिनके अवयवों-एक चर में बहुपद— से शायद आप परिचित हों। हम किसी भी पूर्णांकीय प्रांत या क्षेत्र पर बहुपदों के विभिन्न गुणों पर चर्चा करेंगे। गणित के अलावा बहुपदों के सिद्धांत का अनेक क्षेत्रों में अनुप्रयोग होता है। वास्तव में, इसी कारण आर्यभट्ट-I, श्रीधर, भास्कर-II और अन्य प्राचीन भारतीय गणितज्ञों ने **Q** पर रैखिक और द्विघात बहुपदों का गहराई से अध्ययन किया और इससे संबंधित सिद्धांत को विकसित किया। आजकल इस सिद्धांत का कूटलेखन सिद्धांत तथा सामाजिक विज्ञान व रासायनिक विज्ञान की समस्याओं के गणितीय निदर्श बनाने में प्रयोग होता है।

इस पाठ्यक्रम की तीसरी इकाई में हम आपका परिचय तीन प्रकार के पूर्णांकीय प्रांतों से कराएंगे, जिनके सबसे जाने-पहचाने उदाहरण हैं **Z** और किसी क्षेत्र पर बहुपद वलय। ये प्रांत हैं यूक्लिडीय प्रांत, मुख्य गुणजावली प्रांत और अद्वितीय गुणनखंडन प्रांत। हम इनके कुछ गुणों की विस्तार से चर्चा करेंगे और बताएंगे कि ये प्रांत किस प्रकार परस्पर संबद्ध हैं।

इस पाठ्यक्रम की अंतिम इकाई में हम **Q** पर उन बहुपदों पर विचार करेंगे जिनके उचित गुणनखंड नहीं होते। ऐसे बहुपद के प्रयोग से हम **Q** के क्षेत्र विस्तार प्राप्त कर सकते हैं। इस इकाई में इन्हीं व अन्य क्षेत्र विस्तारों के साथ-साथ उपक्षेत्र पर भी चर्चा करेंगे। फिर हम परिमित क्षेत्र व उनके गुणों पर विचार करेंगे। कूटलेखन सिद्धांत में इनकी महत्वपूर्ण भूमिका होती है।

इस खंड के साथ ही हम इस पाठ्यक्रम को समाप्त करते हैं। आशा है कि इकाई 15 समाप्त कर लेने के बाद प्रत्येक इकाई में दिए गए उद्देश्यों को आपने हासिल कर लिया होगा।

संकेत और प्रतीक

C [0,1]	[0, 1] से **R** तक के संतत फलनों का वलय
$\wp(X)$	X के सभी उपसमुच्चयों का समुच्चय
$\mathbf{Z}_n$	मॉड्यूलो n पूर्णांकों का वलय
char R	वलय R का अभिलक्षणिक
Ra, <a>	a द्वारा जनित R की मुख्य गुणजावली
R[x]	R पर एक चर वाले बहुपदों का वलय
deg f(x)	बहुपद f(x) की घात
$\max(a_1, \ldots, a_n)$	पूर्णांकों $a_1, a_2, \ldots, a_n$ में महत्तम पूर्णांक
$a \mid b$	a, b को विभाजित करता है
$a \nmid b$	a, b को विभाजित नहीं करता
g c d	महत्तम सार्व भाजक
(a,b)	a और b का महत्तम सार्व भाजक
l c m	लघुतम सार्व गुणज

पिछले खंडों में दिए गए संकेतों को भी देखिए।

आभार

डॉ. माणिक पटवर्धन और डॉ. सुजाता वर्मा को उनके उपयोगी सुझावों के लिए

इकाई 12 आधारभूत तथ्य

इकाई की रूपरेखा

12.1 प्रस्तावना

इकाई 9 में पहले हमने आपको वलयों से और फिर विशेष वलयों से परिचित कराया था, जिनकी विशेषता उनके गुणन संबंधी गुणों में है। इस इकाई में हम आपको एक अन्य प्रकार के वलय, अर्थात् पूर्णांकीय प्रांत से परिचित कराएंगे। आप देखेंगे कि पूर्णांकीय प्रांत एक ऐसा तत्समकी वलय है जिसमें दो शून्येतर अवयवों का गुणनफल शून्येतर होता है। हम ऐसे वलयों के विभिन्न गुणों पर चर्चा करेंगे।

इसके बाद हम **Q**, **R**, **C** और $\mathbf{Z}_p$ (जहां p एक अभाज्य संख्या है) जैसे वलयों पर विचार करेंगे। इन वलयों के शून्येतर अवयवों से गुणन के सापेक्ष आबेली समूह प्राप्त होते हैं। ऐसे वलयों को क्षेत्र कहते हैं। ये संरचनाएं काफ़ी उपयोगी होती हैं, जिसका एक कारण यह है कि हम उनमें "भाग" दे सकते हैं।

पूर्णांकीय प्रांतों और क्षेत्रों से संबंधित कुछ विशेष गुणजावलियां होती हैं जिन्हें अभाज्य गुणजावली और उच्चिष्ठ गुणजावली कहते हैं। इस इकाई में हम इन गुणजावलियों और इनके संगत विभाग वलयों के बारे में भी चर्चा करेंगे।

अंत में हम किसी दिए हुए पूर्णांकीय प्रांत को आविष्ट करने वाले सबसे छोटे क्षेत्र को प्राप्त करने की विधि बताएंगे। ठीक इसी तरीके से ही **Z** से **Q** प्राप्त किया जाता है। हम इस प्रकार के क्षेत्र को दिए हुए पूर्णांकीय प्रांत का विभाग क्षेत्र कहते हैं।

इस इकाई में हमने आपको अनेक नई संकल्पनाओं से परिचित कराने की कोशिश की है। इन्हें समझने में आपको कुछ समय लग सकता है। घबराइए नहीं। जितना समय लगता है, लगने दीजिए। लेकिन इस इकाई को समाप्त करने पर आपको विश्वास हो जाना चाहिए कि आपने नीचे दिए उद्देश्यों को प्राप्त कर लिया है। केवल तब ही आप इस पाठ्यक्रम की शेष इकाइयों को आसानी से समझ सकेंगे।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- जांच कर सकेंगे कि कोई बीजीय निकाय पूर्णांकीय प्रांत है कि नहीं;
- किसी वलय का अभिलक्षणिक प्राप्त कर सकेंगे;
- जांच कर सकेंगे कि कोई बीजीय निकाय क्षेत्र है कि नहीं;
- अभाज्य गुणजावलियों और उच्चिष्ठ गुणजावलियों को परिभाषित कर सकेंगे और उन्हें पहचान सकेंगे;
- पूर्णांकीय प्रांतों और क्षेत्रों के साधारण गुणों को सिद्ध कर सकेंगे और उनका प्रयोग कर सकेंगे; और
- किसी पूर्णांकीय प्रांत के विभाग क्षेत्र को प्राप्त कर सकेंगे या उसे पहचान सकेंगे।

12.2 पूर्णांकीय प्रांत (Integral Domain)

आप जानते हैं कि दो शून्येतर पूर्णांकों का गुणनफल एक शून्येतर पूर्णांक होता है, अर्थात् यदि $m, n \in \mathbf{Z}$ ऐसे हों कि $m \neq 0, n \neq 0$ तो $mn \neq 0$. अब वलय Z_6 लीजिए। हम देखते हैं कि $\overline{2} \neq \overline{0}$ और $\overline{3} \neq \overline{0}$, परन्तु $\overline{2} \cdot \overline{3} = \overline{0}$. इस तरह हम देखते हैं कि $\mathbf{Z}_6$ के शून्येतर अवयवों $\overline{2}$ और $\overline{3}$ का गुणनफल शून्य है। जैसा कि आप देखेंगे, इससे पता चलता है कि $\overline{2}$ (और $\overline{3}$) शून्य का भाजक है, अर्थात् $\overline{2}$ (और $\overline{3}$) से $\overline{0}$ भाज्य है।

तो आइए देखें कि शून्य का भाजक क्या होता है ?

परिभाषा : वलय R के शून्येतर अवयव a को **R में शून्य का भाजक** (zero divisor) कहते हैं यदि R में ऐसा शून्येतर अवयव b है जिससे कि $ab = 0$.

(ध्यान दीजिए कि b भी एक शून्य का भाजक होगा।)

क्या अब आप मानते हैं कि Z_6 में $\overline{2}$ शून्य का भाजक है ? अब बताइए कि Z_4 में $\overline{3}$ शून्य का भाजक है या नहीं ? चूंकि Z_4 में प्रत्येक शून्येतर x के लिए $\overline{3} \cdot x \neq \overline{0}$, इसलिए $\overline{3}$, Z_4 में शून्य का भाजक नहीं है।

इस चर्चा के बाद आप नीचे दिया गया प्रश्न हल कर सकते हैं।

E1) मान लीजिए $n \in \mathbf{N}$ और $m|n, 1 < m < n$. तो दिखाइए कि Z_n में $\overline{m}$ शून्य का भाजक है।

आइए अब हम $C[0,1]$ में शून्य के भाजक के एक उदाहरण पर विचार करें। फलन $f \in C[0,1]$ लीजिए जो

$$f(x) = \begin{cases} x - \frac{1}{2}, & 0 \leq x \leq 1/2 \\ 0, & 1/2 \leq x \leq 1 \end{cases}$$

से परिभाषित है।

आइए हम $g : [0,1] \to \mathbf{R}$ को

$$g(x) = \begin{cases} 0, & 0 \leq x \leq 1/2 \\ x - 1/2, & 1/2 \leq x \leq 1 \end{cases}$$

से परिभाषित करें।

तब $g \in C[0,1]$, $g \neq 0$ और $(fg)(x) = 0 \ \forall \ x \in [0,1]$. अतः fg शून्य फलन है। इस तरह $C[0,1]$ में f शून्य का भाजक है।

एक अन्य उदाहरण के लिए दो अतुच्छ वलयों A और B का कार्तीय गुणनफल लीजिए। A के प्रत्येक शून्येतर अवयव a के लिए, $A \times B$ में $(a, 0)$ एक शून्य का भाजक है। ऐसा इसलिए है, क्योंकि B के प्रत्येक शून्येतर अवयव b के लिए $(a, 0)(0, b) = (0, 0)$.

आइए अब हम वलय $\wp(X)$ पर विचार करें, जहां X कम से कम दो अवयवों वाला समुच्चय है। X का प्रत्येक अरिक्त उचित उपसमुच्चय A एक शून्य का भाजक है क्योंकि $A \cdot A^c = A \cap A^c = \phi$, जो $\wp(X)$ का शून्य अवयव है।

अब आप नीचे दिए गए प्रश्न हल कीजिए।

E2) Z में सभी शून्य के भाजक बताइए।

E3) । किन तत्समकी वलयों में शून्य का भाजक होगा ?

E4) मान लीजिए R एक वलय है और $a \in R$ एक शून्य का भाजक है। तब दिखाइए कि मुख्य गुणजावली Ra का प्रत्येक अवयव एक शून्य का भाजक होगा।

आइए अब हम एक ऐसे वलय पर विचार करें जिसमें कोई शून्य का भाजक नहीं है।

परिभाषा : हम शून्येतर वलय R को एक **पूर्णांकीय प्रांत** कहते हैं, यदि

(i) R तत्समकी हो, और

(ii) R में कोई शून्य के भाजक न हों।

अतः पूर्णांकीय प्रांत एक शून्येतर तत्समकी वलय होता है जिसमें दो शून्येतर अवयवों का गुणनफल एक शून्येतर अवयव होता है।

इस प्रकार के वलय का नाम पूर्णांकों के समुच्चय से आया है, जो कि ऐसे वलय का सबसे परिचित उदाहरण है। **Q, R** और **C** प्रांतों के अन्य उदाहरण हैं जो तुरंत दिमाग में आते हैं। क्या C[0,1] भी प्रांत है ? आप देख चुके हैं कि इसमें शून्य के भाजक होते हैं। इसलिए C[0, 1] प्रांत नहीं है।

कुछ लेखक कई बार पूर्णांकीय प्रांत को केवल प्रांत ही कहते हैं। हम भी ऐसा करेंगे।

अगले परिणाम से हमें पूर्णांकीय प्रांत के उदाहरणों का एक महत्वपूर्ण वर्ग प्राप्त होता है।

प्रमेय 1 : $\mathbf{Z}_p$ एक पूर्णांकीय प्रांत होता है यदि और केवल यदि p एक अभाज्य संख्या है।

हल : सबसे पहले आइए हम मान लें कि p एक अभाज्य संख्या है। तब आप जानते हैं कि $\mathbf{Z}_p$ एक शून्येतर तत्समकी वलय है। आइए देखें कि इसमें शून्य के भाजक हैं या नहीं।

इसके लिए, मान लीजिए $\bar{a}, \bar{b} \in \mathbf{Z}_p$, जहां $\bar{a}\ \bar{b} = \bar{0}$. तब $\overline{ab} = \bar{0}$, अर्थात् $p \mid ab$. चूंकि p अभाज्य संख्या है, इसलिए इकाई 1 के E25 को लागू करने पर हम पाते हैं कि $p \mid a$ या $p \mid b$. इस तरह $\bar{a} = \bar{0}$ या $\bar{b} = \bar{0}$. तो हमने दिखाया है कि यदि $\bar{a} \neq \bar{0}$ और $\bar{b} \neq \bar{0}$, तो $\overline{ab} \neq \bar{0}$. अतः $\mathbf{Z}_p$ में कोई शून्य के भाजक नहीं हैं। अतः यह एक प्रांत है।

वलय R में शून्य के भाजक नहीं होते हैं यदि a, b ∈ R के लिए $ab = 0 \Rightarrow a = 0$ या $b = 0$.

विलोमतः, हम दिखाएंगे कि यदि p अभाज्य नहीं है, तो $\mathbf{Z}_p$ प्रांत नहीं होगा। अब मान लीजिए p अभाज्य संख्या नहीं है। यदि p = 1, तो $\mathbf{Z}_p$ तुच्छ वलय है, जो कि प्रांत नहीं है।

यदि p भाज्य संख्या है और $m \mid p$, तो E1 से आप जानते हैं कि $\bar{m} \in \mathbf{Z}_p$ एक शून्य का भाजक है। इस तरह $\mathbf{Z}_p$ में शून्य के भाजक हैं। अतः यह एक प्रांत नहीं है।

अब आप एक प्रश्न को हल कीजिए।

E5) निम्नलिखित वलयों में से कौन-कौन से वलय प्रांत नहीं हैं ? क्यों ?

$\mathbf{Z}_4$, $\mathbf{Z}_5$, $2\mathbf{Z}$, $\mathbf{Z} + i\mathbf{Z}$, $\mathbf{R} \times \mathbf{R}$, {0}.

अब वलय R लीजिए। हम जानते हैं कि R में जोड़ का निरसन नियम (cancellation law) लागू होता है, अर्थात् R में जब भी $a + b = a + c$, तब $b = c$. परन्तु क्या $ab = ac$ से यह अर्थ निकलता है कि $b = c$? ज़रूरी नहीं। उदाहरण के लिए **Z** में $0.1 = 0.2$, परन्तु $1 \neq 2$. इसलिए यदि $a = 0$, तो ज़रूरी नहीं कि $ab = ac \Rightarrow b = c$. परन्तु, यदि $a \neq 0$ और $ab = ac$, तो क्या यह सत्य है कि $b = c$? यहां हम सिद्ध करेंगे कि यह पूर्णांकीय प्रांतों के लिए सत्य है।

प्रमेय 2 : वलय R में कोई शून्य का भाजक नहीं होता यदि और केवल यदि R में गुणन के लिए निरसन नियम लागू होता हो। अर्थात् यदि a, b, c ∈ R ऐसे हों कि $a \neq 0$ और $ab = ac$, तो $b = c$.

उपपत्ति : आइए पहले हम मान लें कि R में कोई शून्य का भाजक नहीं है। मान लीजिए कि a, b, c ∈ R ऐसे हैं कि $a \neq 0$ और $ab = ac$. तब $a(b - c) = ab - ac = 0$. और क्योंकि $a \neq 0$ और R में कोई शून्य के भाजक नहीं है, इसलिए हमें $b - c = 0$, अर्थात् $b = c$ प्राप्त होता है।

इस तरह, यदि $ab = ac$ और $a \neq 0$, तो $b = c$.

विलोमतः, मान लीजिए कि R में गुणन के लिए निरसन नियम लागू होता है। मान लीजिए a ∈ R ऐसा होता है कि $a \neq 0$ और किसी b ∈ R के लिए $ab = 0$. तब $ab = 0 = a.0$. गुणन के लिए निरसन नियम लागू करने पर हमें $b = 0$ प्राप्त होता है। इसलिए, a शून्य का भाजक नहीं है। अर्थात् R में कोई शून्य के भाजक नहीं हैं।

इस प्रमेय के अनुसार हम तुरंत कह सकते हैं कि पूर्णांकीय प्रांत में गुणन के लिए निरसन नियम लागू होता है। अब आप प्रांतों के इस गुण के प्रयोग से नीचे दिए गए प्रश्नों को हल कर सकते हैं।

E6) दिखाइए कि किसी प्रांत में समीकरण $x^2 = x$ के हल केवल $x = 0$ या $x = 1$ हैं।

E7) सिद्ध कीजिए कि किसी प्रांत में 0 ही एकमात्र शून्यंभावी अवयव (इकाई 10 का उदाहरण 9 देखिए) है।

आइए अब हम किसी पूर्णांकीय प्रांत से (वास्तव में, किसी वलय से) संबंधित एक संख्या का परिचय दें। इसके लिए आइए पहले हम $\mathbf{Z}_4$ पर विचार करें। हम जानते हैं कि $4x = \bar{0} \; \forall \; x \in \mathbf{Z}_4$ वास्तव में, किसी $x \in \mathbf{Z}_4$ के लिए $8x = \bar{0}$ और $12x = \bar{0}$ भी होता है। लेकिन 4 समुच्चय $\{n \in N \mid nx = \bar{0} \; \forall \; x \in \mathbf{Z}_4\}$ का न्यूनतम अवयव है। इससे पता चलता है कि 4, $\mathbf{Z}_4$ का अभिलक्षणिक है, जैसा कि आप अभी देखेंगे।

परिभाषा : मान लीजिए R एक वलय है। ऐसे न्यूनतम धन पूर्णांक n को, जिससे कि $nx = 0 \; \forall \; x \in R$, R का अभिलक्षणिक (characteristic) कहते हैं, यदि ऐसा कोई धन पूर्णांक n न हो जिससे कि $nx = 0 \; \forall \; x \in R$, तो हम कहते हैं कि R का अभिलक्षणिक शून्य है।

हम वलय R के अभिलक्षणिक को **char R** से प्रकट करते हैं। आप देख सकते हैं कि char $\mathbf{Z}_n = n$ और char $\mathbf{Z} = 0$.

नीचे दिए गए प्रश्नों को हल करने से आपको वलय का अभिलक्षणिक प्राप्त करने का अभ्यास हो जाएगा।

E8) दिखाइए कि char $\wp(X) = 2$, जहां X एक अरिक्त समुच्चय है।

E9) मान लीजिए R एक वलय है और char R = m. char $(R \times R)$ क्या होगा ?

आइए अब हम पूर्णांकीय प्रांतों के लिए एक सुंदर परिणाम पर विचार करें। इसकी सहायता से किसी प्रांत के अभिलक्षणिक को प्राप्त करने में हमें काफ़ी आसानी हो जाती है।

प्रमेय 3 : मान लीजिए m एक धन पूर्णांक है और R एक पूर्णांकीय प्रांत है। तब निम्नलिखित प्रतिबंध तुल्य हैं।

(क) $m \cdot 1 = 0$

(ख) सभी $a \in R$ के लिए $ma = 0$.

(ग) R के किसी $a \neq 0$ के लिए $ma = 0$.

उपपत्ति : हम सिद्ध करेंगे कि (क) $\Rightarrow$ (ख) $\Rightarrow$ (ग) $\Rightarrow$ (क)

(क) $\Rightarrow$ (ख) : हम जानते हैं कि $m \cdot 1 = 0$. अतः किसी $a \in R$ के लिए,

$ma = m(1a) = (m1)(a) = 0a = 0$, अर्थात् (ख) लागू होता है।

(ख) $\Rightarrow$ (ग) : यदि $ma = 0 \; \forall \; a \in R$, तो ज़रूर ही किसी $a \neq 0$ के लिए $ma = 0$.

(ग) $\Rightarrow$ (क) : मान लीजिए कि R के किसी $a \neq 0$ के लिए $ma = 0$.तब $0 = ma = m(1a) = (m1)a$. क्योंकि $a \neq 0$ और R में शून्य के भाजक नहीं हैं, इसलिए हमें $m1 = 0$ प्राप्त होता है।

प्रमेय 3 हमें बताता है कि **किसी प्रांत का अभिलक्षणिक प्राप्त करने के लिए हमें केवल समुच्चय $\{n \cdot 1 \mid n \in N\}$ पर ध्यान देने की आवश्यकता है।** आइए अब हम कुछ उदाहरण लें :

(i) char Q = 0, क्योंकि किसी भी $n \in N$ के लिए $n \cdot 1 \neq 0$.

(ii) इसी प्रकार char R = 0 और char C = 0.

(iii) आप देख चुके हैं कि char $Z_n = n$. इस तरह किसी भी धन पूर्णांक n के लिए अभिलक्षणिक n वाले वलय का अस्तित्व होता है।

आइए अब हम प्रांत के अभिलक्षणिक की एक विशेषता पर ध्यान दें।

प्रमेय 4 : किसी पूर्णांकीय प्रांत का अभिलक्षणिक या तो शून्य होता है या एक अभाज्य संख्या।

उपपत्ति : मान लीजिए R एक प्रांत है। हम सिद्ध करेंगे कि यदि R का अभिलक्षणिक 0 नहीं है, तो यह एक अभाज्य संख्या होगा। अतः मान लीजिए char R = m, जहां $m \neq 0$. तो m ऐसा न्यूनतम धन पूर्णांक है जिससे कि $m \cdot 1 = 0$. m को अभाज्य सिद्ध करने की हमारी विधि है कि हम मानकर चलेंगे कि m एक अभाज्य संख्या नहीं है, और तब सिद्ध करेंगे कि जो हम मानकर चले थे वह ग़लत है।

अब, मान लीजिए m=st, जहां $s,t \in \mathbf{N}$, $1 < s < m$ और $1 < t < m$. तब $m.1 = 0 \Rightarrow (st).1 = 0 \Rightarrow (s.1)\,(t.1) = 0$. क्योंकि R में कोई शून्य के भाजक नहीं हैं, इसलिए हमें $s.1 = 0$ या $t.1 = 0$ प्राप्त होता है। परंतु s और t, m से छोटे हैं। इसलिए m = char R का यह अंतर्विरोध है। अतः हमारा यह मानकर चलना कि m = st, जहां $1 < s < m$, $1 < t < m$ ग़लत है। इस तरह m के गुणनखंड केवल 1 और स्वयं m हैं। अर्थात् m एक अभाज्य संख्या है।

अब आप अभिलक्षणिकों की इतनी जानकारी से नीचे दिए गए प्रश्न हल कर सकते हैं।

E10) मान लीजिए R अभिलक्षणिक p वाला एक पूर्णांकीय प्रांत है। सिद्ध कीजिए कि

(क) सभी $a, b \in R$ के लिए

$(a + b)^p = a^p + b^p$ और

$(a - b)^p = a^p - b^p$.

(ख) उपसमुच्चय $\{a^p \mid a \in R\}$, R का उपवलय है।

(ग) फलन $\phi : R \to R : \phi(a) = a^p$ एक वलय एकैक समाकारिता (monomorphism) है।

(घ) यदि R परिमित पूर्णांकीय प्रांत हो, तो ϕ एक तुल्याकारिता है।

E11) मान लीजिए R तत्समक 1 वाला वलय है, और char R = m.

फलन $f : \mathbf{Z} \Rightarrow R : f(n) = n.1$

परिभाषित कीजिए। दिखाइए कि f एक समाकारिता है। Ker f क्या होगा ?

E 12) $\mathbf{Z}_3 \times \mathbf{Z}_4$ का अभिलक्षणिक ज्ञात कीजिए। एक उदाहरण के रूप में इस वलय का प्रयोग करके बताइए कि प्रमेय 3 और प्रमेय 4 केवल पूर्णांकीय प्रांतों के लिए क्यों सत्य हैं।

अब हम देखेंगे कि प्रांत के गुणन पर कुछ प्रतिबंध लगाने के बाद हमें कैसी बीजीय संरचना प्राप्त होती है। यदि आपने हमारे रैखिक बीजगणित के पाठ्यक्रम का अध्ययन किया हो तो आप उस बीजीय निकाय से अवश्य परिचित होंगे जिसकी चर्चा हम अब करने जा रहे हैं।

12.3 क्षेत्र (Field)

मान लीजिए (R, +,.) एक वलय है। हम जानते हैं कि (R, +) एक आवेली समूह है। हम यह भी जानते हैं कि संक्रिया · क्रमविनिमेय और साहचर्य है। परन्तु (R,.) आवेली समूह नहीं है। वास्तव में, यदि R तत्समकी भी हो, तो भी (R,.) समूह नहीं होगा, क्योंकि ऐसा कोई भी अवयव $a \in R$ नहीं है जिससे कि $a \cdot 0 = 1$. लेकिन, क्या $(R \setminus \{0\}, .)$ एक समूह हो सकता है ? हां, कुछ स्थितियों में। उदाहरण के लिए, इकाई 2 से आप जानते हैं कि गुणन के सापेक्ष $\mathbf{Q}^*$ और $\mathbf{R}^*$ समूह हैं। इस कारण से हम कह सकते हैं कि **Q** और **R** क्षेत्र हैं, एक शब्द जिसकी परिभाषा हम अब देंगे।

परिभाषा : हम वलय (R, +,.) को **क्षेत्र** कहते हैं यदि $(R \setminus \{0\}, .)$ एक आवेली समूह हो।

इस तरह, कोई निकाय (R, +, .) क्षेत्र तभी होगा जब यह R1 से R6 तक के वलय अभिगृहीतों को और निम्नलिखित अभिगृहीतों को संतुष्ट करेगा।

(i) · क्रमविनिमेय है,

(ii) R का तत्समक है (जिसे हम 1 से प्रकट करते हैं) और $1 \neq 0$, और

(iii) R के प्रत्येक शून्येतर अवयव x का एक गुणनात्मक व्युत्क्रम होता है, जिसे हम x^{-1} से प्रकट करते हैं।

केवल आपकी जानकारी के लिए हम आपको बताना चाहेंगे कि कोई वलय जो केवल (ii) और (iii) को संतुष्ट करता हो, **विभाजन-वलय** (division ring), **विषम क्षेत्र** (skew field) या **अक्रमविनिमेय क्षेत्र** कहलाता है। बीजगणित के अध्ययन में इन वलयों का काफ़ी महत्व है, लेकिन इस पाठ्यक्रम में हम इनकी चर्चा नहीं करेंगे।

आइए अब हम फिर क्षेत्रों पर ध्यान दें। 19वीं शताब्दी में जर्मन गणितज्ञों रिचर्ड डेडेकिण्ड और लियोपोल्ड क्रोनेकर ने बीजीय संख्या सिद्धांत पर शोध कार्य करने के दौरान क्षेत्र की संकल्पना का विकास किया। इस संकल्पना के लिए डेडेकिण्ड ने जर्मन शब्द Körper का प्रयोग किया था जिसका अर्थ है क्षेत्र। यही कारण है कि आप कई बार क्षेत्र को K से प्रकट होते देखेंगे।

जैसा कि आप जान गए होंगे, क्षेत्र के दो उदाहरण हैं **R** और **C**। ये ही वे क्षेत्र थे जिन पर डेडेकिण्ड ने विचार किया था। क्षेत्र का एक अन्य उदाहरण निम्नलिखित वलय है।

उदाहरण 1 : दिखाइए कि $\mathbf{Q} + \sqrt{2}\,\mathbf{Q} = \{a + \sqrt{2}\,b \mid a, b \in \mathbf{Q}\}$ एक क्षेत्र है।

हल : इकाई 9 में आपने देखा था कि $F = \mathbf{Q} + \sqrt{2}\,\mathbf{Q}$ तत्समक $1 + \sqrt{2}.0$ वाला एक क्रमविनिमेय वलय है।

अब, मान लीजिए $a + \sqrt{2}\,b$, F का एक शून्येतर अवयव है। तब या तो $a \neq 0$ या $b \neq 0$. अब परिमेयकरण प्रक्रिया (rationalisation process) लागू करने पर हम पाते हैं कि

$$(a+\sqrt{2}b)^{-1} = \frac{1}{a+\sqrt{2}b} = \frac{a-\sqrt{2}b}{(a+\sqrt{2}b)\ (a-\sqrt{2}b)} = \frac{a-\sqrt{2}b}{a^2-2b^2}$$

$$= \frac{a}{a^2-2b^2} + \sqrt{2}\ \frac{(-b)}{a^2-2b^2} \in F.$$

(ध्यान दीजिए कि $a^2 - 2b^2 \neq 0$, क्योंकि $\sqrt{2}$ परिमेय नहीं है और या तो $a \neq 0$ या $b \neq 0$.)

इस तरह, प्रत्येक शून्येतर अवयव का एक गुणनात्मक व्युत्क्रम होता है। अतः $\mathbf{Q} + \sqrt{2}\,\mathbf{Q}$ एक क्षेत्र है।

क्या आप ऐसे वलय का उदाहरण दे सकते हैं जो क्षेत्र नहीं है ? क्या प्रत्येक शून्येतर पूर्णांक का **Z** में गुणनात्मक व्युत्क्रम होता है ? नहीं। अतः **Z** क्षेत्र नहीं है। अब तक आप क्षेत्र के अनेक उदाहरण देख चुके हैं। क्या आपने इस बात पर ध्यान दिया है कि ये सभी क्षेत्र पूर्णांकीय प्रांत भी हैं ? यह संयोग की बात नहीं है। इससे संबंधित निम्नलिखित परिणाम देखिए।

प्रमेय 5 : प्रत्येक क्षेत्र एक पूर्णांकीय प्रांत होता है।

उपपत्ति : मान लीजिए F एक क्षेत्र है। तब $F \neq \{0\}$ और $1 \in F$. हमें देखना है कि F में शून्य के भाजक हैं कि नहीं। मान लीजिए F में a और b ऐसे अवयव हैं कि $ab = 0$ और $a \neq 0$. क्योंकि $a \neq 0$ और F एक क्षेत्र है, इसलिए a^{-1} का अस्तित्व है। अतः $b = 1.b = (a^{-1}a)\,b = a^{-1}\ (ab) = a^{-1}.0 = 0$.

इसलिए, यदि $a \neq 0$ और $ab = 0$, तो हमें $b = 0$ प्राप्त होता है, अर्थात् F में कोई शून्य के भाजक नहीं हैं। अतः F एक प्रांत है।

अब आप नीचे दिए गए प्रश्न हल कीजिए।

E13) निम्नलिखित वलयों में से कौन-कौन से वलय क्षेत्र नहीं है ?

$2\mathbf{Z}, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Q} \times \mathbf{Q}$

E14) क्या किसी क्षेत्र का उपवलय एक क्षेत्र होगा ? क्यों ?

प्रमेय 5 को पढ़ने के बाद शायद आप सोच रहे हों कि क्या प्रत्येक प्रांत एक क्षेत्र होता है। आप देख चुके हैं कि **Z** एक प्रांत है परंतु क्षेत्र नहीं है। यदि हम केवल परिमित प्रांतों की बात करें तो हम पाते हैं कि ये क्षेत्र हैं।

प्रमेय 6 : प्रत्येक परिमित पूर्णांकीय प्रांत एक क्षेत्र होता है।

उपपत्ति : मान लीजिए $R = \{a_0 = 0, a_1 = 1, a_2, \ldots, a_n\}$ एक परिमित प्रांत है। तब R क्रमविनिमेय भी होता है। यह दिखाने के लिए कि R एक क्षेत्र है, हमें दिखाना है कि R के प्रत्येक शून्येतर अवयव का एक गुणनात्मक व्युत्क्रम होता है।

मान लीजिए $a = a_i$, R का एक शून्येतर अवयव है (अर्थात् $i \neq 0$) । अवयव $aa_1, \ldots, aa_n$ लीजिए। प्रत्येक $j \neq 0$ के लिए $a_j \neq 0$; और क्योंकि $a \neq 0$, इसलिए $aa_j \neq 0$.

अतः समुच्चय $\{aa_1, \ldots, aa_n\} \subseteq \{a_1, \ldots, a_n\}$. साथ ही, $aa_1, aa_2, \ldots, aa_n$ सभी समुच्चय $\{a_1, \ldots, a_n\}$ के अलग-अलग अवयव हैं, क्योंकि गुणन के निरसन नियम से $aa_j = aa_k \Rightarrow a_j = a_k$.

इस तरह $\{aa_1, \ldots, aa_n\} = \{a_1, \ldots, a_n\}$. विशेष रूप में, किसी j के लिए $a_1 = aa_j$, अर्थात् $1 = aa_j$. इस तरह, R में a व्युत्क्रमणीय है। अतः R के प्रत्येक शून्येतर अवयव का गुणनात्मक व्युत्क्रम है । इसलिए R एक क्षेत्र है।

इस परिणाम को लागू करके अब हम एक प्रमेय सिद्ध कर सकते हैं जिससे परिमित क्षेत्रों के अनेक उदाहरण प्राप्त होते हैं।

वह क्षेत्र जिसका अधःस्थ समुच्चय परिमित है, परिमित क्षेत्र कहलाता है ।

प्रमेय 7 : Z_n एक क्षेत्र होता है यदि और केवल यदि n एक अभाज्य संख्या हो।

उपपत्ति : प्रमेय 1 से आप जानते हैं कि Z_n एक प्रांत होता है यदि और केवल यदि n एक अभाज्य संख्या हो। आप यह भी जानते हैं कि Z_n के केवल n अवयव होते हैं। अब हम परिणाम प्राप्त करने के लिए प्रमेय 6 लागू कर सकते हैं।

प्रमेय 7 से क्षेत्रों के अनेक उदाहरण प्राप्त होते हैं : Z_2, Z_3, Z_5, Z_7, आदि। इन उदाहरणों को और क्षेत्र के अन्य उदाहरणों को देखकर क्या आप क्षेत्र के अभिलक्षणिक के बारे में कुछ बता सकते हैं ? प्रमेय 4 और प्रमेय 5 की सहायता से हम कह सकते हैं कि

प्रमेय 8 : क्षेत्र का अभिलक्षणिक या तो शून्य होता है या एक अभाज्य संख्या।

अभी तक हमने परिमित क्षेत्रों के जितने उदाहरण देखे हैं उनमें p अवयव थे, जहां p एक अभाज्य संख्या है। नीचे के प्रश्न में हम परिमित क्षेत्र का एक ऐसा उदाहरण दे रहे हैं जिसके लिए यह बात लागू नहीं होती।

E 5) मान लीजिए $R = \{0, 1, a, 1 + a\}$· R में + और . को निम्नलिखित केली सारणियों के अनुसार परिभाषित कीजिए।

+	0	1	a	1+a
0	0	1	a	1+a
1	1	0	1+a	a
a	a	1+a	0	1
1+a	1+a	a	1	0

और

.	0	1	a	1+a
0	0	0	0	0
1	0	1	a	1+a
a	0	a	1+a	1
1+a	0	1+a	1	a

दिखाइए कि R एक क्षेत्र है। इस क्षेत्र का अभिलक्षणिक ज्ञात कीजिए।

आइए अब हम किसी वलय का क्षेत्र होने के लिए एक रोचक प्रतिबंध पर विचार करें।

प्रमेय 9 : मान लीजिए R एक तत्समकी वलय है। तब R एक क्षेत्र होता है यदि और केवल यदि R की गुणजावलियाँ केवल R और $\{0\}$ हों।

उपपत्ति : आइए पहले हम मान लें कि R एक क्षेत्र है। मान लीजिए I, R की एक गुणजावली है। यदि $I \neq \{0\}$, तो एक शून्येतर अवयव $x \in I$ का अस्तित्व होता है। क्योंकि $x \neq 0$ और R एक क्षेत्र है, इसलिए किसी $y \in R$ के लिए $xy = 1$. क्योंकि $x \in I$ और I एक गुणजावली है, इसलिए $xy \in I$, अर्थात् $1 \in I$.

अतः इकाई 10 के प्रमेय 4 के अनुसार, $I = R$. इसलिए R की गुणजावलियाँ केवल $\{0\}$ और R है।

विलोमतः, मान लीजिए R की गुणजावलियां केवल R और $\{0\}$ हैं। अब, मान लीजिए $a \in R$, $a \neq 0$. तब आप जानते है कि समुच्चय $Ra = \{ra \mid r \in R\}$, R की एक शून्येतर गुणजावली है। इसलिए $Ra = R$. अब $1 \in R = Ra$. इसलिए किसी $b \in R$ के लिए $1 = ba$, अर्थात् a^{-1} का अस्तित्व है। इस तरह, हम पाते हैं कि R के प्रत्येक शून्येतर अवयव का एक गुणनात्मक व्युत्क्रम होता है। अतः R एक क्षेत्र है।

यह परिणाम बहुत उपयोगी है। इस खंड की बाकी इकाइयों में आप इस परिणाम को बार-बार लागू करेंगे।

प्रमेय 9 की सहायता से हम क्षेत्र समाकारिताओं (अर्थात् एक क्षेत्र से दूसरे क्षेत्र तक की वलय समाकारिताओं) के बारे में कुछ रोचक तथ्य प्राप्त कर सकते हैं। हम इन तथ्यों को प्रश्न के रूप में आपको दे रहे हैं।

E16) मान लीजिए $f:F \to K$ एक क्षेत्र समाकारिता है। दिखाइए कि या तो f शून्य फलन है या f, 1–1 है।

E17) मान लीजिए R एक वलय है जो एक क्षेत्र F के तुल्याकारी है। दिखाइए कि तब R भी क्षेत्र होगा।

E17 से हमें फिर पता चलता है कि तुल्याकारी बीजीय संरचनाओं का बीजीयतः अभिन्न होना ज़रूरी है।

प्रांतों और क्षेत्रों की इस चर्चा के बाद, आइए अब हम वलय की कुछ गुणजावलियों पर विचार करें जिनके सापेक्ष विभाग वलय प्रांत अथवा क्षेत्र होते हैं।

12.4 अभाज्य गुणजावली और उच्चिष्ठ गुणजावली

Z के संबंध में हम जानते हैं कि यदि p एक अभाज्य संख्या हो और p दो पूर्णांकों a और b के गुणनफल को विभाजित करता हो तो या तो p, a को विभाजित करता है या p, b को विभाजित करता है। यानि कि यदि $ab \in p\mathbf{Z}$, तो या $a \in p\mathbf{Z}$ या $b \in p\mathbf{Z}$. इस गुण के आधार पर हम कहते हैं कि $p\mathbf{Z}$ एक अभाज्य गुणजावली है। लेकिन अभाज्य गुणजावली का मतलब क्या है ? आइए देखें।

परिभाषा : किसी वलय R की उचित गुणजावली P को R की अभाज्य गुणाजावली (prime ideal) कहते हैं यदि जब भी किन्हीं $a, b \in R$ के लिए $ab \in P$, तो या तो $a \in P$ या $b \in P$.

आप देख सकते हैं कि $\{0\}$, **Z** की एक अभाज्य गुणजावली है, क्योंकि $ab \in \{0\} \Rightarrow a \in \{0\}$ या $b \in \{0\}$ जहां $a,b \in \mathbf{Z}$. अभाज्य गुणजावली का एक अन्य उदाहरण है

उदाहरण 2 : मान लीजिए R एक पूर्णांकीय प्रांत है। दिखाइए कि $I = \{(0, x) \mid x \in R\}$, $R \times R$ की एक अभाज्य गुणजावली है।

हल : आप जानते हैं कि I, $R \times R$ की एक गुणजावली है। आप यह भी जानते हैं कि यह एक उचित गुणजावली है, क्योंकि $I \neq R \times R$. आइए अब हम जांच करें कि I एक अभाज्य गुणजावली है या नहीं। इसके लिए मान लीजिए $(a_1, b_1), (a_2, b_2) \in R \times R$, जहां $(a_1, b_1)(a_2, b_2) \in I$. तब, किसी $x \in R$ के लिए $(a_1 a_2, b_1 b_2) = (0, x)$. इसलिए $a_1 a_2 = 0$ अर्थात् $a_1 = 0$ या $a_2 = 0$, क्योंकि R एक प्रांत है।

इसलिए $(a_1 b_1) \in I$ या $(a_2, b_2) \in I$.

अतः I एक अभाज्य गुणजावली है।

अब आप नीचे दिए गए प्रश्नों को हल करने की कोशिश कीजिए। इससे आपको अभाज्य गुणजावलियों के आदी होने में मदद मिलेगी।

E18) दिखाइए कि समुच्चय $I = \{f \in C[0, 1] \mid f(0) = 0\}$, $C[0, 1]$ की अभाज्य गुणजावली है।

E19) दिखाइए कि तत्समकी वलय R एक पूर्णांकीय प्रांत होता है यदि और केवल यदि शून्य गुणजावली $\{0\}$, R की अभाज्य गुणजावली हो।

अब हम पूर्णांकीय प्रांत और अभाज्य गुणजावली के संबंध को सिद्ध करेंगे।

प्रमेय 10 : किसी तत्समकी वलय R की गुणजावली P, R की अभाज्य गुणजावली होती है यदि और केवल यदि विभाग वलय R/P एक पूर्णांकीय प्रांत हो।

उपपत्ति : आइए पहले हम मान लें कि P वलय R की अभाज्य गुणजावली है। क्योंकि R तत्समकी है, इसलिए R/P भी तत्समकी होगा। अब मान लीजिए R/P में a + P और b + P ऐसे हैं कि $(a + P)(b + P) = P$, जो कि R/P का शून्य अवयव है। तब $ab + P = P$, अर्थात् $ab \in P$, और चूंकि

P, R की अभाज्य गुणजावली है, इसलिए या तो $a \in P$ या $b \in P$. अतः या तो $a + P = P$ या $b + P = P$.

इस तरह R/P में कोई शून्य के भाजक नहीं हैं।

अतः R/P एक पूर्णांकीय प्रांत है।

विलोमतः, मान लीजिए कि R/P एक पूर्णांकीय प्रांत है। और मान लीजिए कि $a, b \in R$ ऐसे हैं कि $ab \in P$. तब R/P में $ab + P = P$, अर्थात् R/P में $(a+P)(b+P) = P$. चूंकि R/P एक पूर्णांकीय प्रांत है, इसलिए या तो $a+P$ या $b+P = P$. अर्थात् या तो $a \in P$ या $b \in P$. इससे पता चलता है कि P, R की एक अभाज्य गुणजावली है।

प्रमेय 10 और प्रमेय 1 की सहायता से हम कह सकते हैं कि $\mathbf{Z}$ की गुणजावली $m\mathbf{Z}$ अभाज्य होती है यदि और केवल यदि m एक अभाज्य संख्या हो। क्या हम $\mathbf{Z}$ की अभाज्य संख्याओं और अभाज्य गुणजावलियों के बीच के इस संबंध को किसी भी पूर्णांकीय प्रांत के लिए व्यापकीकृत कर सकते हैं ? इसका उत्तर प्राप्त करने के लिए आइए पहले हम विभाज्यता और अभाज्य अवयवों की संकल्पनाओं को उपयुक्त रूप से व्यापकीकृत करें।

परिभाषा : किसी वलय R में हम कहते हैं कि अवयव a अवयव b को **विभाजित करता है** (और $a|b$ से प्रकट करते हैं), यदि किसी $r \in R$ के लिए $b = ra$. इस स्थिति में हम यह भी कहते हैं कि a, b का एक **गुणनखंड** है या a, b का एक **भाजक** है।

इस तरह, $\mathbf{Z}_7$ में $\bar{3}$, $\bar{6}$ को विभाजित करता है, क्योंकि $\bar{3} \cdot \bar{2} = \bar{6}$.

आइए अब हम देखें कि अभाज्य अवयव क्या होता है।

परिभाषा : किसी पूर्णांकीय प्रांत R के शून्येतर अवयव p को **अभाज्य अवयव** कहते हैं, यदि

(i) p का कोई गुणनात्मक व्युत्क्रम न हो, और

(ii) जब भी $a, b \in R$ और $p \mid ab$, तो $p \mid a$, या $p \mid b$.

क्या आप बता सकते हैं कि $\mathbf{Z}$ के अभाज्य अवयव क्या हैं ? ये अवयव अभाज्य संख्याएं और उनके ऋण हैं।

अब आप अभाज्य अवयव से परिचित हो चुके हैं। तो आइए देखें कि किसी पूर्णांकीय प्रांत में अभाज्य गुणजावलियों का अभाज्य अवयवों से क्या संबंध है।

प्रमेय 11 : मान लीजिए R एक पूर्णांकीय प्रांत है। शून्येतर अवयव $p \in R$ एक अभाज्य अवयव होता है यदि और केवल यदि Rp, R की एक अभाज्य गुणजावली हो।

उपपत्ति : आइए पहले हम मान लें कि p, R का एक अभाज्य अवयव है। क्योंकि p का कोई गुणनात्मक व्युत्क्रम नहीं है, इसलिए $1 \notin Rp$. इस तरह, हम पाते हैं कि Rp, R की एक उचित गुणजावली है।

अब, मान लीजिए $a, b \in R$ ऐसे हैं कि $ab \in Rp$. तब किसी $r \in R$ के लिए

$ab = rp$

$\Rightarrow$ $p \mid ab$

$\Rightarrow$ $p \mid a$ या $p \mid b$, क्योंकि p एक अभाज्य अवयव है।

$\Rightarrow$ $a = xp$ या $b = xp$ किसी $x \in R$ के लिए।

$\Rightarrow$ $a \in Rp$ या $b \in Rp$.

$x \in R$ का एक गुणनात्मक व्युत्क्रम होता है यदि और केवल यदि $Rx = R$.

इस तरह $ab \in Rp \Rightarrow a \in Rp$ या $b \in Rp$, अर्थात् Rp, R की एक अभाज्य गुणजावली है।

विलोमतः, मान लीजिए कि Rp एक अभाज्य गुणजावली है। तब $Rp \neq R$. इस तरह, $1 \notin Rp$. अतः p का कोई भी गुणनात्मक व्युत्क्रम नहीं है। अब, मान लीजिए $p \mid ab$, जहां $a, b \in R$. तब किसी $r \in R$ के लिए $ab = rp$, अर्थात् $ab \in Rp$.

क्योंकि Rp एक अभाज्य गुणजावली है, इसलिए $a \in Rp$ या $b \in Rp$. अतः या तो $p \mid a$ या $p \mid b$. इस तरह, हम पाते हैं कि p, R का एक अभाज्य अवयव है।

प्रमेय 11 बहुत उपयोगी है यह जांच करने के लिए कि कोई अवयव अभाज्य है कि नहीं या यह ज्ञात करने के लिए कि कोई मुख्य गुणजावली अभाज्य गुणजावली है कि नहीं। उदाहरण के लिए, अब हम E 19 के प्रयोग से कह सकते हैं कि 0, R का एक अभाज्य अवयव होता है यदि और केवल यदि R एक प्रांत हो।

अभाज्य गुणजावलियों के अनेक उपयोगी गुण हैं। नीचे दिए गए प्रश्नों में हमने आपसे इनमें से कुछ गुणों को सिद्ध करने को कहा है।

E20) मान लीजिए $f: R \to S$ अष्टि N वाली एक आच्छादक वलय समाकारिता है। दिखाइए कि

(क) यदि J, S की एक अभाज्य गुणजावली हो, तो $f^{-1}(J)$, R की एक अभाज्य गुणजावली होगी।

(ख) यदि I, R की एक अभाज्य गुणजावली हो, जो N को आविष्ट करती हो, तो f(I), S की एक अभाज्य गुणजावली होगी।

(ग) N को आविष्ट करने वाली R की अभाज्य गुणजावलियों के समुच्चय और S की सभी अभाज्य गुणजावलियों के समुच्चय के बीच के फलन ϕ को $\phi(I) = f(I)$ से हम परिभाषित करते हैं। दिखाइए कि ϕ एकैकी आच्छादक है।

E21) यदि I_1 और I_2 किसी वलय की ऐसी गुणजावलियां हों, कि न तो I_1, I_2 को और न ही I_2, I_1 को आविष्ट करती हो, तो दिखाइए कि गुणजावली $I_1 \cap I_2$ अभाज्य नहीं है।

अब **Z** की गुणजावली 2 **Z** लीजिए। मान लीजिए कि **Z** की गुणजावली n **Z** ऐसी है कि $2\mathbf{Z} \subseteq n\mathbf{Z} \subseteq \mathbf{Z}$ तब $n \mid 2$, $\therefore n = \pm 1$ या $n = \pm 2$. $\therefore n\mathbf{Z} = \mathbf{Z}$ या $n\mathbf{Z} = 2\mathbf{Z}$.

इससे पता चलता है कि कोई भी गुणजावली 2**Z** और **Z** के बीच नहीं हो सकती। अर्थात्, 2**Z** को आविष्ट करने वाली **Z** की उचित गुणजावलियों में से 2**Z** ही उच्चिष्ठ है। इसलिए हम कहते हैं कि यह एक उच्चिष्ठ गुणजावली है। आइए हम इस व्यंजक की परिभाषा दें।

परिभाषा : किसी वलय R की **उचित** गुणजावली M को **उच्चिष्ठ गुणजावली** (maximal ideal) कहते हैं यदि जब भी I, R की ऐसी गुणजावली हो कि $M \subseteq I \subseteq R$, तो I = M या I = R.

इस तरह, एक उचित गुणजावली M उच्चिष्ठ गुणजावली होती है, यदि R की ऐसी कोई उचित गुणजावली नहीं है जो इसे आविष्ट करती हो। इसका एक उदाहरण जो तुरंत दिमाग में आता है, वह है किसी क्षेत्र F की शून्य गुणजावली। यह उच्चिष्ठ है क्योंकि आप जानते हैं कि F की अन्य गुणजावली केवल F ही है।

उच्चिष्ठ गुणजावलियों के और उदाहरण प्राप्त करने के लिए हम इन गुणजावलियों के निम्नलिखित गुण का प्रयोग कर सकते हैं।

प्रमेय 12 : मान लीजिए R एक तत्समकी वलय है। R की गुणजावली M उच्चिष्ठ होती है यदि और केवल यदि R/M एक क्षेत्र हो।

उपपत्ति : आइए पहले हम मान लें कि M, R की एक उच्चिष्ठ गुणजावली है। हम सिद्ध करना चाहते हैं कि R/M एक क्षेत्र है। इसके लिए यह सिद्ध करना ही काफी होगा कि R/M की कोई शून्येतर उचित गुणजावली नहीं है (देखिए प्रमेय 9)। अतः मान लीजिए कि I, R/M की एक गुणजावली है। विहित समाकारिता $\eta : R \to R/M : \eta(r) = r + M$ लीजिए। तब इकाई 11 के प्रमेय 3 से आप जानते हैं कि $\eta^{-1}(I)$, η की अष्टि M को आविष्ट करने वाली R की एक गुणजावली है। क्योंकि M, R की उच्चिष्ठ गुणजावली है इसलिए $\eta^{-1}(I) = M$ या $\eta^{-1}(I) = R$. अतः $I = \eta(\eta^{-1}(I))$ या तो $\eta(M)$ है या $\eta(R)$. अर्थात् $I = \{\bar{0}\}$ या $I = R/M$, जहां $\bar{0} = 0 + M = M$. अतः R/M एक क्षेत्र है।

विलोमतः, मान लीजिए कि M, R की एक ऐसी गुणजावली है जिससे कि R/M एक क्षेत्र होता है। तब R/M की गुणजावलियाँ $\{\bar{0}\}$ और R/M ही होंगी। मान लीजिए I, M को आविष्ट करने वाली R की एक गुणजावली है। तब $\eta(I) = \{\bar{0}\}$ या $\eta(I) = R/M$. $\therefore I = \eta^{-1}(\eta(I))$ या M है या R, अतः M, R की एक उच्चिष्ठ गुणजावली है।

अब आप निम्नलिखित कथन पर ध्यान दीजिए; यह प्रमेय 12 (और कुछ अन्य प्रमेयों) का एक निष्कर्ष है।

उपप्रमेय : तत्समकी वलय की प्रत्येक उच्चिष्ठ गुणजावली एक अभाज्य गुणजावली होती है।

निम्नलिखित प्रश्न में हम आपसे इसे सिद्ध करने को कह रहे हैं।

E 22) ऊपर दिए गए उपप्रमेय को सिद्ध कीजिए।

अब, उपप्रमेय एक तरफ़ा कथन है। इसके विलोम के बारे में क्या कहा जा सकता है ? अर्थात् क्या प्रत्येक अभाज्य गुणजावली उच्चिष्ठ होती है ? $\mathbf{Z}$ की शून्य गुणजावली को देखकर क्या इसका जवाब मिल सकता है ? क्योंकि $\mathbf{Z}$ एक प्रांत है परन्तु क्षेत्र नहीं है और $\mathbf{Z} \simeq \mathbf{Z}/\{0\}$, इसलिए $\mathbf{Z}/\{0\}$ एक प्रांत है परन्तु क्षेत्र नहीं है। इस तरह, $\{0\}$, $\mathbf{Z}$ की अभाज्य गुणजावली है, परन्तु उच्चिष्ठ गुणजावली नहीं है।

आइए अब हम प्रमेय 12 की सहायता से उच्चिष्ठ गुणजावलियों के कुछ उदाहरण प्राप्त करें।

उदाहरण 3 : दिखाइए कि $\mathbf{Z}$ की गुणजावली $m\mathbf{Z}$ उच्चिष्ठ होती है यदि और केवल यदि m एक अभाज्य संख्या हो।

हल : प्रमेय 7 से आप जानते हैं कि $\mathbf{Z}_m$ एक क्षेत्र होता है यदि और केवल यदि m एक अभाज्य संख्या हो। आप यह भी जानते हैं कि $\mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}_m$. इस तरह, E17 के अनुसार $\mathbf{Z}/m\mathbf{Z}$ एक क्षेत्र होता है यदि और केवल यदि m अभाज्य हो। अतः प्रमेय 12 के अनुसार, $m\mathbf{Z}$, $\mathbf{Z}$ की उच्चिष्ठ गुणजावली होती है यदि और केवल यदि m एक अभाज्य संख्या हो।

उदाहरण 4 : दिखाइए कि $\overline{2}\,\mathbf{Z}_{12}$, $\mathbf{Z}_{12}$ की एक उच्चिष्ठ गुणजावली है, जबकि $\{\overline{0}, \overline{4}, \overline{8}\}$ नहीं है।

हल : आप जानते हैं कि $\mathbf{Z}_{12} \simeq \mathbf{Z}/12\mathbf{Z}$ और $\overline{2}\,\mathbf{Z}_{12} \simeq 2\mathbf{Z}/12\mathbf{Z}$. इस तरह, इकाई 11 के E23 के अनुसार हम पाते हैं कि

$$\mathbf{Z}_{12}/\overline{2}\,\mathbf{Z}_{12} \simeq (\mathbf{Z}/12\mathbf{Z})/(2\mathbf{Z}/12\mathbf{Z}) \simeq \mathbf{Z}/2\mathbf{Z} \simeq \mathbf{Z}_2,$$

जो एक क्षेत्र है। अतः $\overline{2}\,\mathbf{Z}_{12} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$, $\mathbf{Z}_{12}$ में उच्चिष्ठ है।

अब, $\{\overline{0}, \overline{4}, \overline{8}\} = \overline{4}\,\mathbf{Z}_{12} \subsetneq \overline{2}\,\mathbf{Z}_{12} \subsetneq \mathbf{Z}_{12}$.

इसलिए $\mathbf{Z}_{12}$ में $\{\overline{0}, \overline{4}, \overline{8}\}$ उच्चिष्ठ नहीं है।

अब आप नीचे दिए गए प्रश्न हल कीजिए।

E23) दिखाइए कि $\mathbf{Z}_{10}$ में $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$ उच्चिष्ठ है।

E24) इकाई 11 के उदाहरण 4 की सहायता से सिद्ध कीजिए कि $C[0, 1]$ में गुणजावली

$\{f \in C[0, 1] \mid f\left(\frac{1}{2}\right) = 0\}$ उच्चिष्ठ है।

आइए अब हम देखें कि इस भाग में हमने क्या-क्या किया है। पहले हमने आपको वलय की एक विशेष गुणजावली, अर्थात् अभाज्य गुणजावली से परिचित कराया। इसकी विशेषता इस बात में है कि इसका संगत विभाग वलय एक पूर्णांकीय प्रांत है।

इसके बाद हमने एक विशेष प्रकार की अभाज्य गुणजावली, अर्थात् उच्चिष्ठ गुणजावली पर चर्चा की। हम ऐसे गुणजावली को इतना विशेष क्यों मानते हैं ? क्योंकि इसका संगत विभाग वलय एक क्षेत्र होता है, और क्षेत्र एक ऐसी बीजीय संरचना है जिसको समझना कुछ हद तक आसान है।

अब, यदि हम अपना ध्यान केवल प्रांतों तक ही सीमित रखें, तो क्या आप किसी प्रांत से क्षेत्र प्राप्त करने की कोई और विधि बता सकते हैं ? अगले भाग में हम ऐसी विधि पर विचार करेंगे।

12.5 विभाग क्षेत्र

$\mathbf{Z}$ और $\mathbf{Q}$ लीजिए। आप जानते हैं कि $\mathbf{Q}$ का प्रत्येक अवयव $\frac{a}{b}$ के रूप का होता है, जहां $a \in \mathbf{Z}$ और $b \in \mathbf{Z}^*$. वास्तव में, हम $\frac{a}{b}$ को क्रमित युग्म $(a, b) \in \mathbf{Z} \times \mathbf{Z}^*$ से भी प्रकट कर सकते हैं। अब, हम जानते हैं कि $\mathbf{Q}$ में $\frac{a}{b} = \frac{c}{d}$ यदि और केवल यदि $ad = bc$. आइए हम $\mathbf{Z} \times \mathbf{Z}^*$ के अवयवों में भी इसी प्रकार का संबंध स्थापित करें।

अब, हम यह भी जानते हैं कि $\mathbf{Q}$ पर संक्रियाएं

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \text{ और } \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd} \ \forall \ \frac{a}{b}, \frac{c}{d}\in \mathbf{Q}.$$

से परिभाषित हैं।

इन परिभाषाओं को ध्यान में रखकर हम $\mathbf{Z}\times\mathbf{Z}^*$ पर संक्रियाओं को परिभाषित कर सकते हैं। फिर हम $\mathbf{Z}\times\mathbf{Z}^*$ पर इस प्रकार से एक तुल्यता संबंध परिभाषित कर सकते हैं जिससे कि हमें $\mathbf{Q}$ के तुल्यकारी एक क्षेत्र प्राप्त हो।

हम किसी भी पूर्णांकीय प्रांत से एक क्षेत्र प्राप्त करने के लिए इस प्रक्रिया को व्यापकीकृत कर सकते हैं। तो एक पूर्णांकीय प्रांत R लीजिए। मान लीजिए K क्रमित युग्मों का निम्न समुच्चय है :

$$K = \{(a,b) \mid a,b \in R \text{ और } b \neq 0\}.$$

हम K में संबंध ~ को

$$(a,b) \sim (c,d) \text{ यदि } ad = bc$$

से परिभाषित करते हैं।

हमारा दावा है कि ~ एक तुल्यता संबंध है। आइए देखें कि यह बात सही है या नहीं

(i) $(a,b) \sim (a,b) \ \forall \ (a,b) \in K$, क्योंकि R क्रमविनिमेय है। अतः ~ स्वतुल्य है।

(ii) मान लीजिए $(a,b), (c,d) \in K$ ऐसे हैं कि $(a,b) \sim (c,d)$. तब $ad = bc$, अर्थात्
$cb = da$. $\therefore (c,d) \sim (a,b)$.

इसलिए ~ सममित है।

(iii) अंत में, मान लीजिए $(a,b), (c,d), (u,v) \in K$ ऐसे हैं कि $(a,b) \sim (c,d)$ और $(c,d) \sim (u,v)$. तब $ad = bc$ और $cv = du$.

इसलिए $(ad)v = (bc)v = bdu$, अर्थात् $avd = bud$. इस तरह गुणन के निरसन नियम से, जो प्रांत पर लागू होता है, हमें $av = bu$, अर्थात् $(a,b) \sim (u,v)$ प्राप्त होता है।
इस तरह ~ संक्रामक है।

अतः ~ एक तुल्यता संबंध है।

आइए हम (a,b) को आविष्ट करने वाले तुल्यता वर्ग को $[a,b]$ से प्रकट करें। इस तरह, $[a, b] = \{(c, d) \mid c, d \in R, d \neq 0 \text{ और } ad = bc\}$.

मान लीजिए ~ के सापेक्ष K के सभी तुल्यता वर्गों का समुच्चय F है।

आइए हम F में + और · को परिभाषित करें। (परिमेय संख्याओं को जोड़ने और गुणा करने के नियमों को ध्यान में रखने से आप परिभाषाएं आसानी से समझ सकेंगे।)

$$[a,b] + [c,d] = [ad+bc, bd], \text{ और}$$

$$[a,b].[c,d] = [ac,bd].$$

क्या आप समझते हैं कि F पर + और · द्वि-आधारी संक्रियाएं हैं ?

ध्यान दीजिए कि पूर्णांकीय प्रांत R में $b \neq 0$ और $d \neq 0$ से अर्थ निकलता है कि $bd \neq 0$. अतः ऊपर दिए गए समीकरणों के दक्षिण पक्ष सुपरिभाषित तुल्यता वर्ग हैं। इस तरह, F के दो अवयवों का योगफल और गुणनफल भी F का अवयव है। हमें जांच कर लेनी चाहिए कि ये संक्रियाएं सुपरिभाषित हैं या नहीं। अतः, मान लीजिए कि $[a, b] = [a', b']$ और $[c, d] = [c', d']$. हमे दिखाना है कि

$[a, b] + [c, d] = [a', b'] + [c', d']$, अर्थात् $[ad+bc, bd] = [a'd'+b'c', b'd']$.

अब $(ad+bc)b'd' - (a'd' + b'c')bd$

$$= ab'dd' + cd'bb' - a'bdd' - c'dbb'$$

$$= (ab' - a'b)dd' + (cd' - c'd)bb'$$

$= \quad (0)\, dd' + (0) bb'$, क्योंकि $(a, b) \sim (a', b')$ और $(c, d) \sim (c', d')$.

$= \quad 0.$

अतः $[ad+bc, bd] = [a'd' + b'c', b'd']$, अर्थात् + सुपरिभाषित है।

आइए अब हम दिखाएं कि $[a, b] \cdot [c, d] = [a', b'] \cdot [c', d']$,

अर्थात् $[ac, bd] = [a'c', b'd']$.

अब $(ac)(b'd') - (bd)(a'c')$

$= ab'cd' - ba'dc' = ba'cd' - ba'cd'$, क्योंकि $ab' = ba'$ और $cd' = dc'$

$= 0$

इसलिए $[ac, bd] = [a'c', b'd']$. अतः $\cdot$ सुपरिभाषित है।

अब हम सिद्ध करेंगे कि F एक क्षेत्र है।

(i) + साहचर्य है : किन्हीं $[a, b], [c, d], [u, v] \in F$ के लिए,

$$\begin{aligned}([a, b] + [c, d]) + [u, v] &= [ad+bc, bd] + [u, v]\\ &= [(ad+bc)v + ubd, bdv]\\ &= [adv + b(cv+ud), bdv]\\ &= [a, b] + [cv+ud, dv]\\ &= [a, b] + ([c, d] + [u, v]).\end{aligned}$$

(ii) + क्रमविनिमेय है : $[a, b], [c, d] \in F$ के लिए,

$[a, b] + [c, d] = [ad+bc, bd] = [cb+da, db] = [c, d] + [a, b]$.

(iii) $[0, 1]$, F का योज्य तत्समक है :

$[a, b] \in F$ के लिए

$[0, 1] + [a, b] = [0 \cdot b + 1 \cdot a, 1 \cdot b] = [a, b]$.

(iv) $[a, b] \in F$ का योज्य प्रतिलोम $[-a, b]$ है :

$[a, b] + [-a, b] = [ab - ab, b^2] = [0, b^2] = [0, 1]$, क्योंकि $0 \cdot 1 = 0 \cdot b^2$.

हम चाहेंगे कि अब आप F के क्षेत्र होने के लिए शेष प्रतिबंधों को सिद्ध करें (नीचे दिया गया प्रश्न देखिए।

E25) दिखाइए कि F में $\cdot$ साहचर्य है, क्रमविनिमेय है, + पर बंटित है, और $[1, 1]$, F का गुणनात्मक तत्समक है।

तो हमने साथ मिलकर F को क्षेत्र सिद्ध कर लिया है।

अब हम $f: R \to F : f(a) = [a, 1]$ परिभाषित करते हैं।

हम दिखाना चाहते हैं कि f एक एकैक समाकारिता है।

सबसे पहले, $a, b \in R$ के लिए,

$$\begin{aligned}f(a+b) = [a+b, 1] &= [a, 1] + [b, 1]\\ &= f(a) + f(b), \text{ और}\end{aligned}$$

$f(ab) = [ab, 1] = [a, 1] \cdot [b, 1] = f(a) \cdot f(b)$.

इस तरह, f एक वलय समाकारिता है।

इसके बाद, मान लीजिए $a, b \in R$ ऐसे हैं कि $f(a) = f(b)$. तब $[a, 1] = [b, 1]$, अर्थात् $a = b$. इसलिए f, 1–1 है।

इस तरह, f एकैक समाकारिता है।

अतः $\text{Im} f = f(R)$, F का एक उपवलय है जो R के तुल्याकारी है।

जैसा कि आप जानते हैं, तुल्याकारी संरचनाएं बीजीयतः अभिन्न होती हैं। इसलिए हम f(R) और R को एक ही मान सकते हैं, और R को F का एक उपवलय मान सकते हैं। अब F का कोई भी अवयव निम्न रूप होता है :

$$[a, b] = [a, 1] [1, b] = [a, 1] [b, 1]^{-1} = f(a) f(b)^{-1}, \text{ जहां } b \neq 0.$$

अतः $f(x) \in f(R)$ और $x \in R$ को एक ही मानते हुए हम कह सकते हैं कि F का कोई भी अवयव ab^{-1} के रूप का होता है, जहां

$a, b \in R, b \neq 0.$

इस भाग में हमने जो भी चर्चा की है वह निम्नलिखित प्रमेय की उपपत्ति ही है।

प्रमेय 13 : मान लीजिए R एक पूर्णांकीय प्रांत है। तब एक ऐसे क्षेत्र F का अस्तित्व होता है जिसके लिए

(i) R से F तक एक एकैक समाकारिता परिभाषित है, और

(ii) F का प्रत्येक अवयव ab^{-1} के रूप का होता है, जहां $a, b \in R, b \neq 0$.

प्रमेय 13 में दिए गए क्षेत्र F को R का **विभाग क्षेत्र** (field of quotients) कहते हैं।

इस तरह, **Q**, **Z** का विभाग क्षेत्र है। **R** का विभाग क्षेत्र क्या है ? निम्नलिखित प्रमेय से इस प्रश्न का उत्तर प्राप्त होता है।

प्रमेय 14 : यदि $f : R \to K$ पूर्णांकीय प्रांत R से क्षेत्र K तक की एकैक समाकारिता हो, तो एक एकैक समाकारिता $g: F \to K: g([a,1]) = f(a)$ का अस्तित्व होता है, जहां F, R का विभाग क्षेत्र है।

हम यहां इस परिणाम को सिद्ध नहीं करेंगे, क्योंकि यह कुछ जटिल है। लेकिन, हम इसका प्रयोग करेंगे। आइए इस प्रमेय को ध्यान से देखें। इसके अनुसार **किसी पूर्णांकीय प्रांत का विभाग क्षेत्र उसे आविष्ट करने वाला सबसे छोटा क्षेत्र होता है**। इस तरह, किसी क्षेत्र का विभाग क्षेत्र स्वयं क्षेत्र ही होता है। अतः **R** का विभाग क्षेत्र **R** होगा और $\mathbf{Z}_p$ का विभाग क्षेत्र $\mathbf{Z}_p$ होगा, जहां p एक अभाज्य संख्या है।

अब आप नीचे दिए गए प्रश्न हल कीजिए।

E 26) क्या $\mathbf{Z} + \sqrt{2}\,\mathbf{Z}$ का विभाग क्षेत्र **R** है ? या **C** है ? या, $\mathbf{Q} + \sqrt{2}\,\mathbf{Q}$ है ? क्यों ?

E 27) प्रमेय 13 का क्षेत्र F प्राप्त करने के लिए किस चरण पर यह मान लेना आवश्यक है कि R एक प्रांत है ?

आइए अब हम इस इकाई में दिए गए पाठ्य सामग्री का संक्षिप्त विवरण देते हुए, इसे यहीं समाप्त करें।

12.6 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों पर चर्चा की है।

1. पूर्णांकीय प्रांत की परिभाषा और उसके उदाहरण।
2. क्षेत्र की परिभाषा और उसके उदाहरण।
3. प्रत्येक क्षेत्र एक प्रांत होता है।
4. परिमित प्रांत एक क्षेत्र होता है।
5. किसी प्रांत या क्षेत्र का अभिलक्षणिक या तो शून्य होता है या एक अभाज्य संख्या।

6. अभाज्य गुणजावली और उच्चिष्ठ गुणजावली की परिभाषा और उनके उदाहरण।
7. इस तथ्य की उपपत्ति और प्रयोग कि किसी तत्समकी वलय R की उचित गुणजावली P अभाज्य (या उच्चिष्ठ) होती है यदि और केवल यदि $R/_P$ एक पूर्णांकीय प्रांत (या क्षेत्र) हो।
8. प्रत्येक उच्चिष्ठ गुणजावली अभाज्य गुणजावली होती है।
9. पूर्णांकीय प्रांत R का अवयव p अभाज्य होता है यदि और केवल यदि मुख्य गुणजावली pR, R की एक अभाज्य गुणजावली हो।
10. $\mathbf{Z}_n$ एक क्षेत्र होता है यदि और केवल यदि n एक अभाज्य संख्या हो।
11. पूर्णांकीय प्रांत के विभाग क्षेत्र को बनाने की विधि।

12.7 हल/उत्तर

E1) मान लीजिए n=mr, जहां $r \in \mathbf{N}$.

तब $\overline{m}\,\overline{r} = \overline{n} = \overline{0}$, $\mathbf{Z}_n$ में।

क्योंकि $1 < m < n$, $\overline{m} \neq \overline{0}$. इसी प्रकार, $\overline{r} \neq \overline{0}$.

इस तरह, $\overline{m} \in \mathbf{Z}_n$ एक शून्य का भाजक है।

E2) **Z** में कोई शून्य के भाजक नहीं हैं।

E3) किसी के लिए भी नहीं, क्योंकि वलय के किसी $x \neq 0$ के लिए

$1 \cdot x = x \neq 0$

E4) मान लीजिए R में $b \neq 0$ ऐसा है कि $ab = 0$ तब किसी $r \in R$ के लिए $(ra)b = r(ab) = 0$. इस तरह, Ra का प्रत्येक अवयव एक शून्य का भाजक होता है।

E5) $\mathbf{Z}_4$, क्योंकि $\overline{2}$ एक शून्य का भाजक है।

2**Z**, क्योंकि $1 \notin 2\mathbf{Z}$.

$\mathbf{R} \times \mathbf{R}$, क्योंकि (1,0) एक शून्य का भाजक है।

{0}, क्योंकि प्रांत को शून्येतर होना चाहिए।

E6) $x^2 = x \Rightarrow x(x-1) = 0 \Rightarrow x = 0$ या $x-1 = 0$

$\Rightarrow x = 0$ या $x = 1$.

E7) मान लीजिए R एक प्रांत है और $x \in R$ शून्यंभावी है। तब किसी $n \in \mathbf{N}$ के लिए $x^n = 0$. क्योंकि R में कोई शून्य के भाजक नहीं हैं, इसलिए $x = 0$.

E8) हम दिखाना चाहते हैं कि $2A = \phi \ \forall A \subseteq x$, और 2 ऐसी न्यूनतम प्राकृतिक संख्या है। सबसे पहले, किसी $A \subseteq x$ के लिए

$2A = A \Delta A = (A \setminus A) \cup (A \setminus A) = \phi$

और क्योंकि $x \neq \phi$, $1 \cdot X \neq \phi$. अतः char $\wp(X) \neq 1$.

$\therefore$ char $\wp(X) = 2$.

E9) मान लीजिए char $(R \times R) = n$. हम जानते हैं कि $mr = 0 \ \forall r \in R$.

अब, मान लीजिए (r, s), $R \times R$ का कोई अवयव है।

तब $m(r, s) = (mr, ms) = (0, 0)$, क्योंकि $r, s \in R$.

इस तरह, $n \leq m$. ...(1)

दूसरी ओर, यदि $r \in R$, तो $(r, 0) \in R \times R$

$\therefore n(r, 0) = (0, 0)$.

अर्थात् $(nr, 0) = (0, 0)$.

अर्थात् $nr = 0$

यह किसी भी $r \in R$ के लिए सत्य है।

$\therefore m \le n$ ...(2)

इस तरह (1) और (2) से पता चलता है कि $m = n$, अर्थात् char R = char $(R \times R)$.

E10) (क) द्विपद – प्रसार (इकाई 9 का E11) के अनुसार

$(a+b)^p = a^p + {}^pC_1 a^{p-1} b + ... + {}^pC_{p-1} ab^{p-1} + b^p.$

क्योंकि $p \mid {}^pC_n \ \forall\ n = 1 ...., p-1$, ${}^pC_n x = 0 \ \forall\ x \in R$ और $\forall\ n = 1,...., p-1$

अतः ${}^pC_1 a^{p-1} b = 0 = ... = {}^pC_{p-1} ab^{p-1}$

$\therefore (a+b)^p = a^p + b^p.$

इसी प्रकार आप दिखा सकते हैं कि $(a-b)^p = a^p - b^p$.

(ख) मान लीजिए $S = \{a^p \mid a \in R\}$.

सबसे पहले, $S \neq \phi$.

इसके बाद, मान लीजिए $\alpha, \beta \in S$. तब किसी $a, b \in R$ के लिए $\alpha = a^p, \beta = b^p$.

तब $\alpha - \beta = (a-b)^p \in S$ और $\alpha\beta = (ab)^p \in S$. इस तरह, S, R का एक उपवलय है।

(ग) $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$,

$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\,\phi(b)$.

इस तरह, ϕ एक वलय समाकारिता है। ϕ, 1–1 है क्योंकि

$\phi(a) = \phi(b) \Rightarrow a^p = b^p \Rightarrow (a-b)^p = 0$, (क) से

$\Rightarrow a-b = 0$, क्योंकि R में कोई शून्य के भाजक नहीं है।

$\Rightarrow a = b$.

(घ) हमें दिखाना है कि यदि R परिमित हो तो ϕ आच्छादक होगा। मान लीजिए R के n अवयव हैं। क्योंकि ϕ, 1–1 है; इसलिए Im ϕ के भी n अवयव होंगे। और Im $\phi \subseteq R$. इस तरह Im$\phi = R$. अतः ϕ आच्छादक है।

E11) आप आसानी से दिखा सकते हैं कि f एक वलय समाकारिता है।

Ker $f = \{n \in \mathbf{Z} \mid n.1 = 0\}$

$= m\mathbf{Z}$, क्योंकि char R = m.

E12) char $(\mathbf{Z}_3 \times \mathbf{Z}_4)$ = char $\mathbf{Z}_3$ और char $\mathbf{Z}_4$ का l.c.m

= 12.

इस तरह, $\mathbf{Z}_3 \times \mathbf{Z}_4$ का अभिलक्षणिक न तो 0 है, और न ही एक अभाज्य।

ध्यान दीजिए कि $\mathbf{Z}_3 \times \mathbf{Z}_4$ एक प्रांत नहीं है, क्योंकि इसके अनेक शून्य के भाजक हैं। आइए अब हम देखें कि $\mathbf{Z}_3 \times \mathbf{Z}_4$ पर प्रमेय 3 लागू क्यों नहीं होता।

$(\bar{1}, \bar{0}) \in \mathbf{Z}_3 \times \mathbf{Z}_4$ लीजिए। तब $3(\bar{1}, \bar{0}) = (\bar{0}, \bar{0}) \in \mathbf{Z}_3 \times \mathbf{Z}_4$.

परंतु $3(\bar{1}, \bar{1}) \neq (\bar{0}, \bar{0})$. इस तरह, इस स्थिति में प्रमेय 3 (क) और प्रमेय 3 (ग) तुल्य नहीं हैं।

E13) $2\mathbf{Z}$, क्योंकि $2\mathbf{Z}$ में 2 व्युत्क्रमणीय नहीं है।

$\mathbf{Z}_6$, क्योंकि यह एक प्रांत नहीं है।

$\mathbf{Q} \times \mathbf{Q}$, क्योंकि यह एक प्रांत नहीं है।

E14) नहीं। उदाहरण के लिए, $\mathbf{Z}$, $\mathbf{Q}$ का एक उपवलय है, $\mathbf{Q}$ एक क्षेत्र है, परन्तु $\mathbf{Z}$ क्षेत्र नहीं है

E15) सारणियों से आप देख सकते है कि R तत्समकी है, क्रमविनिमेय है और प्रत्येक शून्येतर अवयव का एक व्युत्क्रम है। इस तरह, R एक क्षेत्र है। साथ ही, $2x = 0 \; \forall \; x \in R$ और $1.x \neq 0$ किसी $x \in R$ के लिए। इस तरह, char R = 2.

E16) Ker f, F की एक गुणजावली है। इस तरह, प्रमेय 9 के अनुसार

Ker f = {0} या Ker f = F.

यदि Ker f = {0}, तो f, 1–1 है।

यदि Ker f = F, तो f = 0.

E17) मान लीजिए $\phi : F \rightarrow R$ एक तुल्याकारिता है। तब $\phi(1)$, Im ϕ = R का तत्समक होगा। और, क्योंकि F क्रमविनिमेय है, इसलिए R भी क्रमविनिमेय होगा। अब, मान लीजिए $r \in R$, $r \neq 0$. क्योंकि ϕ आच्छादक है, $\exists \; a \in F$ जिससे कि $\phi(a) = r$. क्योंकि $r \neq 0$, $a \neq 0$. क्योंकि F एक क्षेत्र है, $\exists \;\; b \in F$ जिससे कि $ab = 1$.

तब $\phi(ab) = \phi(1)$, अर्थात् $r\,\phi(b) = \phi(1)$, अर्थात् r का एक गुणनात्मक व्युत्क्रम है।

इस तरह R एक क्षेत्र है।

E18) सबसे पहले, I, C[0,1] की एक गुणजावली है।

(क्योंकि $f, g \in I \Rightarrow f-g \in I$, और

$T \in C[0, 1], f \in I \Rightarrow Tf \in I$.)

इसके बाद, क्योंकि कोई भी शून्येतर अचर फलन $C[0,1] \setminus I$ में है, इसलिए I एक उचित गुणजावली है।

अंत में, मान लीजिए $fg \in I$. तो R में $f(0)\, g(0) = 0$. क्योंकि R एक प्रांत है, इसलिए $f(0) = 0$ या $g(0) = 0$ अर्थात् $f \in I$ या $g \in I$. इस तरह, I, C[0,1] की अभाज्य गुणजावली है।

E19) R तत्समकी वलय है। इस तरह, हमें दिखाना है कि R में कोई शून्य के भाजक नहीं हैं यदि और केवल यदि {0}, R की एक अभाज्य गुणजावली हो।

अब, {0}, R की एक अभाज्य गुणजावली होती है यदि और केवल यदि $a, b \in R$ के लिए $ab \in \{0\} \Rightarrow a \in \{0\}$ या $b \in \{0\}$, यदि और केवल यदि $ab = 0 \Rightarrow a = 0$ या $b = 0$, यदि और केवल यदि R में कोई शून्य के भाजक नहीं हैं। अतः जो हमें दिखाना था, हमने दिखा दिया।

E20) (क) इकाई 11 के प्रमेय 3 से आप जानते है कि $f^{-1}(J)$, R की एक गुणजावली है। क्योंकि f आच्छादक है और $J \neq S$, इसलिए $f^{-1}(J) \neq R$. अब मान लीजिए $a, b \in R$ ऐसे है कि $ab \in f^{-1}(J)$.

$\Rightarrow f(ab) \in J$.

$\Rightarrow f(a)\, f(b) \in J$.

$\Rightarrow f(a) \in J$ या $f(b) \in J$, क्योंकि J एक अभाज्य गुणजावली है।

$\Rightarrow a \in f^{-1}(J)$ या $b \in f^{-1}(J)$.

इस तरह, $f^{-1}(J)$, R की एक अभाज्य गुणजावली है।

(ख) पहले तो, क्योंकि f आच्छादक है, इसलिए आप जानते हैं कि f(I), S की एक गुणजावली है। और, क्योंकि $I \supseteq K$, और $f^{-1}(f(I)) = I$ (इकाई 11 के प्रमेय 4 से), इसलिए $f(1) \notin f(I)$. इस तरह, $f(I) \neq S$.

अंत में, मान लीजिए $x, y \in S$ ऐसे हैं कि $xy \in f(I)$. क्योंकि S = Im f, $\exists \; a, b \in R$ जिससे कि $x = f(a)$ और $y = f(b)$.
तब $f(ab) = xy \in f(I)$, अर्थात् $ab \in f^{-1}(f(I)) = I$.
$\therefore a \in I$ या $b \in I$, अर्थात $x \in f(I)$ या $y \in f(I)$.

इस तरह, $f(I)$, S की एक अभाज्य गुणजावली है।

(ग) ϕ, 1–1 है: $\phi(I) = \phi(J) \Rightarrow f(I) = f(J)$

$\Rightarrow f^{-1}(f(I)) = f^{-1}(f(J)) \Rightarrow I = J.$

ϕ आच्छादक है : मान लीजिए J, S की एक अभाज्य गुणजावली है। तब $f^{-1}(J)$, R की एक अभाज्य गुणजावली होगी और $\phi(f^{-1}(J)) = f(f^{-1}(J)) = J$ (इकाई 11 से)। इस तरह, $J \in \text{Im}\phi$.

E21) मान लीजिए $x \in I_1 \setminus I_2$ और $y \in I_2 \setminus I_1$. तब $xy \in I_1$, और $xy \in I_2$, क्योंकि I_1 और I_2 गुणजावलियां है।

$\therefore xy \in I_1 \cap I_2$. परन्तु $x \notin I_1 \cap I_2$ और $y \notin I_1 \cap I_2$.
इस तरह, $I_1 \cap I_2$ अभाज्य नहीं है।

E22) M, R की उच्चिष्ठ गुणजावली है

$\Rightarrow$ R/M एक क्षेत्र है, प्रमेय 12 के अनुसार

$\Rightarrow$ R/M एक प्रांत है, प्रमेय 5 के अनुसार

$\Rightarrow$ M,R की एक अभाज्य गुणजावली है, प्रमेय 10 के अनुसार

E23) $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} = \bar{2}\,\mathbf{Z}_{10}$ और $\mathbf{Z}_{10}/\,\bar{2}\,\mathbf{Z}_{10} \simeq \mathbf{Z}_2$, एक क्षेत्र। इस तरह, उदाहरण 4 की तरह $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$, $\mathbf{Z}_{10}$की उच्चिष्ठ गुणजावली है।

E24) इकाई 11 में हमने दिखाया है कि यह गुणजावली आच्छादक समाकारिता

$\phi : C[0,1] \to \mathbf{R} : \phi(f) = f\left(\frac{1}{2}\right)$की अष्टि है।

$\therefore C[0,1]/\text{Ker}\,\phi \simeq \mathbf{R}$, एक क्षेत्र है।

इस तरह, Ker ϕ, $C[0,1]$ में उच्चिष्ठ है।

E25) इन गुणों को R के संगत गुणों का प्रयोग करके आप सिद्ध कर सकते हैं।

E26) विभाग क्षेत्र F का कोई भी अवयव $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$ के रूप का होता है, जहां $c+d\sqrt{2} \neq 0$, a, b, c, d $\in$ **Z.**

अब, $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2} = \left(\frac{ac-2bd}{c^2-2d^2}\right) + \sqrt{2}\left(\frac{bc-ad}{c^2-2d^2}\right) \in \mathbf{Q} + \sqrt{2}\mathbf{Q}$

इस तरह, $F \subseteq \mathbf{Q} + \sqrt{2}\mathbf{Q}$.

और $\mathbf{Q}+\sqrt{2}\,\mathbf{Q}$ का कोई अवयव $\frac{a}{b} + \sqrt{2}\,\frac{c}{d}$ है, जहां a, b, c, d $\in$ **Z**, $b \neq 0$, $d \neq 0$.

अब $\frac{a}{b} + \sqrt{2}\,\frac{c}{d} = \frac{ad+bc\sqrt{2}}{bd} = \frac{ad+bc\sqrt{2}}{bd+0\sqrt{2}}$ जहां ad, bc, bd $\in$ **Z.**

इस तरह, $\frac{a}{b} + \sqrt{2}\,\frac{c}{d} \in F$.

अतः $\mathbf{Q} + \sqrt{2}\,\mathbf{Q} \subseteq F$.

इस तरह $F = \mathbf{Q} + \sqrt{2}\mathbf{Q}$.

E27) यदि R एक प्रांत नहीं है, तो संबंध ~ संक्रामक नहीं होगा, और फिर F परिभाषित नहीं होगा।

इकाई 13 बहुपद वलय

इकाई की रूपरेखा

13.1 प्रस्तावना

आपने पहले $x + 1$ और $x^2 + 2x + 1$ जैसे व्यंजक अवश्य देखे होंगे। ये सभी व्यंजक बहुपदों के उदाहरण हैं। आप रैखिक बीजगणित के पाठ्यक्रम में भी बहुपदों का प्रयोग कर चुके है। इस इकाई में हम ऐसे समुच्चयों पर चर्चा करेंगे जिनके अवयव $a_0 + a_1x + \ldots\ldots + a_nx^n$ के प्रकार के अवयव हैं, जहाँ $a_0, a_1, \ldots\ldots, a_n$ वलय R के अवयव हैं। आप देखेंगे कि यह समुच्चय, जिसे हम $R[x]$ से प्रकट करते हैं, भी एक वलय है।

शायद आप सोच रहे होंगे कि प्रांतों और क्षेत्रों के खंड में हम बहुपद वलयों के बारे में चर्चा क्यों कर रहे हैं ? इसका कारण यह है कि हम एक विशेष स्थिति पर ध्यान देना चाहते हैं, अर्थात् $R[x]$ पर, जहाँ R एक प्रांत है । आप देखेंगे कि यह अनेक उपयोगी गुणों वाला एक पूर्णांकीय प्रांत होगा। विशेष रूप से, किसी क्षेत्र पर बहुपदों का वलय एक विभाजन-कलन विधि को संतुष्ट करता है, जो कि **Z** द्वारा संतुष्ट कलन विधि के समान है (भाग 1.6.2 देखिए)। हम इस गुण को सिद्ध करेंगे और इसके प्रयोग से देखेंगे कि किसी क्षेत्र पर किसी बहुपद के कितने मूल हो सकते हैं।

अगली दो इकाइयों में हम बहुपदों और बहुपद वलयों पर अध्ययन करते रहेंगे। अतः इस इकाई को ध्यान से पढ़ें और इस बात से सुनिश्चित हो जाइए कि आपने निम्नलिखित उद्देश्य प्राप्त कर लिए हैं।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- किसी दिए हुए वलय पर बहुपदों को पहचान सकेंगे;
- इस तथ्य को सिद्ध कर सकेंगे कि वलय R पर बहुपदों का समुच्चय $R[x]$ एक वलय है, और इसका प्रयोग कर सकेंगे;
- $R[x]$ के कुछ गुणों को R के गुणों के साथ संबंधित कर सकेंगे;
- किसी क्षेत्र F के लिए, $F[x]$ के लिए विभाजन-कलन विधि को सिद्ध कर सकेंगे और इसका प्रयोग कर सकेंगे।

13.2 बहुपदों का वलय

जैसा कि हम ऊपर कह चुके हैं, शायद आप $1 + x$, $2 + 3x + 4x^2$ और $x^5 - 1$ जैसे व्यंजकों से परिचित होंगे। ये सभी वलय **Z** पर बहुपद के उदाहरण हैं। क्या इन उदाहरणों से आप बता सकते हैं कि वलय R पर बहुपद की परिभाषा क्या होगी ? आशा है कि आपकी परिभाषा नीचे दी गई परिभाषा से मेल खाती है।

परिभाषा : व्यंजक $a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n$ को किसी वलय R पर अनिर्धार्य (indeterminate) x में **बहुपद** (polynomial) कहते हैं, जहां n एक ऋणेतर पूर्णांक है और $a_0, a_1, \ldots\ldots a_n \in R$.

बहुपदों की चर्चा में हम निम्नलिखित परंपराओं का पालन करेंगे। हम

(i) x^0 के स्थान पर 1 लिखेंगे, जिससे कि हम a_0x^0 के स्थान पर a_0 लिखेंगे,

(ii) x^1 के स्थान पर x लिखेंगे,

(iii) $1.x^m$ के स्थान पर x^m लिखेंगे (अर्थात् जब $a_m = 1$),

(iv) $0.x^m$ के प्रकार के पदों को नहीं लिखेंगे।

इस तरह, बहुपद $2 + 3x^2 - 1.x^3$ और बहुपद $2x^0 + 0.x^1 + 3x^2 + (-1)x^3$ समान हैं।

आगे से जब भी हम शब्द बहुपद का प्रयोग करेंगे तो हमारा अर्थ होगा अनिधार्य x में बहुपद, और हम बहुपद $a_0 + a_1x + ... + a_nx^n$ के स्थान पर संक्षिप्त संकेतन $\sum\limits_{i=0}^{n} a_ix^i$ का प्रयोग करेंगे।

आइए, अब हम बहुपद से संबंधित कुछ आधारभूत परिभाषाओं पर विचार करें।

परिभाषा : मान लीजिए $a_0+a_1x+ ...... + a_nx^n$ वलय R पर एक बहुपद है। $a_0, a_1, ... a_n$ में से प्रत्येक इस बहुपद का एक **गुणांक** (coefficient) है। यदि $a_n \neq 0$, तो हम a_n को इस बहुपद का **अग्रग-गुणांक** (leading coefficient) कहते हैं।

यदि $a_1 = 0 = a_2 = ... = a_n$, तो हमें **अचर बहुपद** (constant polynomial) a_0 प्राप्त होता है। इस तरह, R का प्रत्येक अवयव एक अचर बहुपद है।

विशेष रूप में, अचर बहुपद 0 **शून्य बहुपद** (zero polynomial) कहलाता है। इसका कोई अग्रग-गुणांक नहीं होता।

अब, किसी शून्येतर बहुपद के साथ हम स्वाभाविक ढंग से एक ऋणेतर पूर्णांक को संबद्ध कर सकते हैं। देखिए कैसे।

परिभाषा : मान लीजिए $a_0+a_1x+ .... +a_nx^n$ वलय R पर एक बहुपद है, जहां $a_n \neq 0$. तब हम पूर्णांक n को इस बहुपद का **घात** (degree) कहते हैं, और हम लिखते हैं

$$\deg \left(\sum_{i=0}^{n} a_i x^i\right) = n, \text{ यदि } a_n \neq 0.$$

हम शून्य बहुपद का घात $-\infty$ मानते हैं। इस तरह,

$$\deg 0 = -\infty$$

आइए, अब हम कुछ उदाहरण लें।

(i) $3x^2 + 4x + 5$ घात 2 वाला एक बहुपद है, जिसके गुणांक पूर्णांकों के वलय **Z** के सदस्य हैं। इसका अग्रग-गुणांक 3 है।

(ii) $x^2 + 2x^4 + 6x + 8$ घात 4 वाला एक बहुपद है, जिसके गुणांक वलय **Z** के सदस्य हैं और जिसका अग्रग-गुणांक 2 है। (ध्यान दीजिए कि इस बहुपद को $8 + 6x + x^2 + 2x^4$ भी लिख सकते हैं।)

(iii) मान लीजिए R एक वलय है और $r \in R, r \neq 0$. तब r घात 0 वाला बहुपद है जिसका अग्रग-गुणांक r है।

और उदाहरण देने से पहले हम कुछ संकेतन देना चाहते हैं।

संकेतन : हम वलय R पर सभी बहुपदों के समुच्चय को R[x] से प्रकट करेंगे। (यहां वर्ग कोष्ठक [ ] के प्रयोग का ध्यान दीजिए। किसी अन्य प्रकार के कोष्ठक का प्रयोग मत कीजिए क्योंकि R[x] और R(x) अलग-अलग समुच्चयों को प्रकट करते हैं।

इस तरह, $R[x] = \left\{ \sum\limits_{i=0}^{n} a_i x^i \mid a_i \in R \ \forall \ i = 0, 1 ..... n, \text{ जहां } n \geq 0, n \in \mathbf{Z} \right\}$

हम बहुपद $a_0 + a_1 x + ... + a_n x^n$ को प्रायः f(x), p(x), q(x), आदि से भी प्रकट करेंगे।

इस तरह, $\mathbf{Z}_4[x]$ के अवयव का उदाहरण $f(x) = \bar{2}x^2 + \bar{3}x + \bar{1}$ है। यहाँ $\deg f(x) = 2$ और f(x) का अग्रग-गुणांक $\bar{2}$ है।

हमने अभी तक जो कुछ कहा है, उसे आप समझ गए हैं कि नहीं, यह देखने के लिए आप नीचे दिए गए प्रश्नों को हल कर सकते हैं।

E1) बताइए कि निम्नलिखित व्यंजकों में से कौन-कौन से व्यंजक बहुपद हैं। इनमें से कौन-कौन से बहुपद $Z[x]$ के अवयव हैं ?

(क) $x^6 + x^5 + x^4 + x^2 + x + 1$.

(ख) $\frac{2}{x^2} + \frac{1}{x} + x + x^2$.

(ग) $\sqrt{3}\,x^2 + \sqrt{2}\,x + \sqrt{5}$.

(घ) $1 + \frac{1}{2}x + \frac{1}{3}x^2 + \frac{1}{4}x^3$.

(ङ) $x^{1/2} + 2x^{3/2} + 3x^{5/2}$.

(च) -5.

E 2) $R[x]$ के निम्नलिखित बहुपदों के घात और अग्र-गुणांक ज्ञात कीजिए।

(क) $\sqrt{2}\,x + 7$.

(ख) $1 - 7x^3 + 3x$.

(ग) $1 + x^3 + x^4 + 0.x^5$.

(घ) $\frac{1}{3}x + \frac{1}{5}x^2 + \frac{1}{7}x^3$.

(ङ) 0.

अब, किसी भी वलय R के लिए हम जानना चाहेंगे कि क्या हम समुच्चय $R[x]$ पर ऐसी संक्रियाएं परिभाषित कर सकते हैं जिनके सापेक्ष यह एक वलय बन जाए। इसके लिए हम बहुपदों के योग और गुणन की संक्रियाएं परिभाषित करेंगे।

परिभाषा : मान लीजिए $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ और $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, $R[x]$ के दो बहुपद हैं। आइए हम $m \geq n$ मान लें। तब इनका योगफल होगा

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \ldots + b_m x^m,$$

$$= \sum_{i=0}^{m} (a_i + b_i)x^i, \text{ जहाँ } a_i = 0,\ i > n \text{ के लिए।}$$

उदाहरण के लिए, $Z[x]$ के दो बहुपद $p(x) = 1 + 2x + 3x^2$ और $q(x) = 4 + 5x + 7x^3$ लीजिए। तब

$$p(x) + q(x) = (1+4) + (2+5)x + (3+0)x^2 + 7x^3 = 5 + 7x + 3x^2 + 7x^3.$$

ध्यान दीजिए कि $p(x) + q(x) \in Z[x]$ और

$$\deg(p(x) + q(x)) = 3 = \max(\deg p(x), \deg q(x)).$$

ऊपर दी गई परिभाषा को देखने से लगता है कि $\deg(f(x) + g(x)) = \max(\deg f(x), \deg g(x))$. परंतु ऐसा हमेशा नहीं होता। उदाहरण के लिए, $Z[x]$ के $p(x) = 1 + x^2$ और $q(x) = 2 + 3x - x^2$ लीजिए।

तब $p(x) + q(x) = (1+2) + (0+3)x + (1-1)x^2 = 3 + 3x$.

यहाँ $\deg(p(x) + q(x)) = 1 < \max(\deg p(x), \deg q(x))$.

अतः हम कह सकते हैं कि सभी $f(x), g(x) \in R[x]$ के लिए

$$\mathbf{deg(f(x) + g(x)) \leq max\ (deg\ f(x), deg\ g(x)).}$$

आइए, अब हम बहुपदों के गुणनफल को परिभाषित करें।

परिभाषा : यदि $f(x) = a_0 + a_1 x + ... + a_n x^n$ और $g(x) = b_0 + b_1 x + ...+ b_m x^m$, $R[x]$ के दो बहुपद हों, तो हम उनके गुणनफल $f(x) \cdot g(x)$ को

$$f(x).\ g(x) = c_0 + c_1 x + ... + c_{m+n} x^{m+n}$$

से परिभाषित करते हैं, जहाँ

$$c_i = a_i b_0 + a_{i-1} b_1 + ...+ a_0 b_i \ \forall \ i = 0, 1, ..., m+n.$$

ध्यान दीजिए कि $i > n$ के लिए $a_i = 0$ और $i > m$ के लिए $b_i = 0$.

एक उदाहरण के रूप में आइए हम $\mathbf{Z}[x]$ के निम्नलिखित बहुपदों को गुणा करें :

$p(x) = 1 - x + 2x^3$, $q(x) = 2 + 5x + 7x^2$.

यहाँ $a_0 = 1$, $a_1 = -1$, $a_2 = 0$, $a_3 = 2$, $b_0 = 2$, $b_1 = 5$, $b_2 = 7$.

इस तरह, $p(x)\, q(x) = \sum_{i=0}^{5} c_i x^i$, जहां

$$c_0 = a_0 b_0 = 2,$$

$$c_1 = a_1 b_0 + a_0 b_1 = 3,$$

$$c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 = 2,$$

$$c_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 = -3 \text{ (क्योंकि } b_3 = 0).$$

$$c_4 = a_4 b_0 + a_3 b_1 + a_2 b_2 + a_1 b_3 + a_0 b_4 = 10 \text{ (क्योंकि } a_4 = 0 = b_4).$$

$$c_5 = a_5 b_0 + a_4 b_1 + a_3 b_2 + a_2 b_3 + a_1 b_4 + a_0 b_5 = 14 \text{ (क्योंकि } a_5 = 0 = b_5).$$

इसलिए $p(x) \,.\, q(x) = 2 + 3x + 2x^2 - 3x^3 + 10x^4 + 14x^5$.

ध्यान दीजिए कि $p(x) \,.\, q(x) \in \mathbf{Z}[x]$ और

$$\deg (p(x) \cdot q(x)) = 5 = \deg p(x) + \deg q(x)$$

एक और उदाहरण के लिए

$p(x) = \bar{1} + \bar{2}x$, $q(x) = \bar{2} + \bar{3}x^2 \in \mathbf{Z}_6[x]$ लीजिए।

तब $p(x).q(x) = \bar{2} + \bar{4}x + \bar{3}x^2 + \bar{6}x^3 = \bar{2} + \bar{4}x + \bar{3}x^2$.

यहां $\deg (p(x) \cdot q(x)) = 2 < \deg p(x) + \deg q(x)$

(क्योंकि $\deg p(x) = 1$, $\deg q(x) = 2$).

अगले भाग में हम आपको दिखाएंगे कि

$\deg(f(x)\, g(x)) \leq \deg f(x) + \deg g(x)$

अब आप नीचे दिया गया प्रश्न हल कीजिए। इससे आपको बहुपदों को जोड़ने और गुणा करने का कुछ अभ्यास हो जाएगा।

E3) निम्नलिखित बहुपद ज्ञात कीजिए :

(क) $\mathbf{Z}[x]$ में $(2 + 3x^2 + 4x^3) + (5x + x^3)$

(ख) $\mathbf{Z}_7[x]$ में $(\bar{6} + \bar{2}x^2) + (\bar{1} - \bar{2}x + \bar{5}x^3)$

(ग) $\mathbf{Z}[x]$ में $(1 + x)(1 + 2x + x^2)$

(घ) $Z_3[x]$ में $(\bar{1}+x)(\bar{1}+\bar{2}x+x^2)$

(ङ) $Z[x]$ में $(2+x+x^2)(5x+x^3)$

अब तक आप बहुपदों के जोड़ और गुणा से परिचित हो गए होंगे। हम अब सिद्ध करना चाहेंगे कि किसी भी वलय R के लिए इन संक्रियाओं के सापेक्ष R[x] एक वलय होता है। इसके लिए ध्यान दें कि परिभाषानुसार + और ., R[x] पर द्वि-आधारी संक्रियाएं हैं।

आइए अब हम निम्नलिखित प्रमेय सिद्ध करें। यह किसी भी वलय के लिए सत्य है, चाहे वह वलय क्रमविनिमेय हो या नहीं।

प्रमेय 1 : यदि R एक वलय है तो R[x] भी एक वलय होगा, जहां x एक अनिर्धार्य है।

उपपत्ति : हमें (R[x], +, .) के लिए इकाई 9 के R1 से R6 तक के अभिगृहीतों को स्थापित करना होगा।

(i) योग क्रमविनिमेय है : हमें देखना है कि

किन्हीं $p(x), q(x) \in R[x]$ के लिए

$$p(x)+q(x)=q(x)+p(x)$$

मान लीजिए

$$p(x)=a_0+a_1x+\ldots+a_nx^n, \text{ और}$$

$$q(x)=b_0+b_1x+\ldots+b_mx^m, R[x] \text{ में हैं।}$$

तब, $p(x)+q(x)=c_0+c_1x+\ldots+c_tx^t$,

जहाँ $c_i=a_i+b_i$ और $t=\max(m,n)$.

इसी प्रकार $q(x)+p(x)=d_0+d_1x+\ldots+d_sx^s$,

जहां $d_i=b_i+a_i$, $s=\max(n,m)=t$.

क्योंकि R में योग क्रमविनिमेय है, इसलिए $c_i=d_i \ \forall \ i \geq 0$.

अतः $p(x)+q(x)=q(x)+p(x)$.

(ii) योग साहचर्य है : R में योग की सहचारिता को लागू करके हम दिखा सकते हैं कि यदि $p(x), q(x), s(x) \in R[x]$, तब $\{p(x)+q(x)\}+s(x)=p(x)+\{q(x)+s(x)\}$.

(iii) योज्य तत्समक : R[x] में शून्य बहुपद योज्य तत्समक होता है, क्योंकि किसी $p(x)=a_0+a_1x+\ldots+a_nx^n \in R[x]$ के लिए,

$$0+p(x)=(0+a_0)+(0+a_1)x+\ldots+(0+a_n)x^n$$
$$=a_0+a_1x+\ldots+a_nx^n$$
$$=p(x)$$

दो बहुपद
$f(x)=a_0+a_1x+\ldots+a_nx^n$
और
$g(x)=b_0+b_1x+\ldots+b_mx^m$
बराबर होते हैं,
यदि $a_i=b_i \ \forall \ i \geq 0$.

(iv) योज्य प्रतिलोम : $p(x)=a_0+a_1x+\ldots+a_nx^n \in R[x]$ के लिए बहुपद $-p(x)=-a_0-a_1x-\ldots-a_nx^n$ को लीजिए, जहाँ $-a_i$, R में a_i का योज्य प्रतिलोम है। तब

$$p(x)+(-p(x))=(a_0-a_0)+(a_1-a_1)x+\ldots+(a_n-a_n)x^n$$
$$=0+0.x+0.x^2+\ldots+0.x^n$$
$$=0.$$

अतः $-p(x)$, $p(x)$ का योज्य प्रतिलोम है।

(v) गुणन साहचर्य है :

मान लीजिए

$$p(x)=a_0+a_1x+\ldots+a_nx^n,$$

$$q(x)=b_0+b_1x+\ldots+b_mx^m \text{ और}$$

$$t(x)=d_0+d_1x+\ldots+d_rx^r, R[x] \text{ में हैं।}$$

तब

$p(x).q(x) = c_0 + c_1x + ... + c_s x^s$, जहां $s = m+n$ और

$c_k = a_k b_0 + a_{k-1} b_1 + ... + a_0 b_k \ \forall \ k = 0, 1, ..., s.$

इसलिए

$\{p(x). q(x)\}. t(x) = e_0 + e_1 x + ... + e_t x^t,$

जहां $t = s+r = m+n+r$ और

$e_k = c_k d_0 + c_{k-1} d_1 + ... + c_0 d_k$

$\quad = (a_k b_0 + ... + a_0 b_k) d_0 + (a_{k-1} b_0 + ... + a_0 b_{k-1}) d_1 + ... + a_0 b_0 d_k .$

इसी प्रकार, हम दिखा सकते हैं कि किसी $k \geq 0$ के लिए $p(x) \ \{q(x).t(x)\}$ में x^k का गुणांक है :

$a_k b_0 d_0 + a_{k-1} (b_1 d_0 + b_0 d_1) + ... + a_0(b_k d_0 + b_{k-1} d_1 + ... + b_0 d_k) = e_k$, R में + और · के गुणों का प्रयोग करके।

अतः $\{p(x) \cdot q(x)\} \cdot t(x) = p(x) \cdot \{q(x) \cdot t(x)\}$

(vi) गुणन योग पर बंटित होता है :

मान लीजिए

$p(x) = a_0 + a_1 x + ... + a_n x^n$

$q(x) = b_0 + b_1 x + ... + b_m x^m$

और $t(x) = d_0 + d_1 x + ... + d_r x^r$, $R[x]$ में हैं।

$p(x) \cdot \{q(x)+t(x)\}$ में x^k का गुणांक है :

$c_k = a_k (b_0 + d_0) + a_{k-1} (b_1 + d_1) + ... + a_0 (b_k + d_k).$

और $p(x) . q(x) + p(x) . t(x)$ में x^k का गुणांक है :

$(a_k b_0 + a_{k-1} b_1 + ... + a_0 b_k) + (a_k d_0 + a_{k-1} d_1 + ... + a_0 d_k)$

$= a_k(b_0+d_0) + a_{k-1}(b_1+d_1) + ... + a_0 (b_k+d_k) = c_k .$

यह सभी $k \geq 0$ के लिए सत्य है।

अतः $p(x) . \{q(x)+t(x)\} = p(x) . q(x) + p(x) . t(x) .$

इसी प्रकार, हम सिद्ध कर सकते हैं कि

$\{q(x)+t(x)\} . p(x) = q(x) . p(x) + t(x) . p(x)$

अतः $R[x]$ एक वलय है।

ध्यान दीजिए कि इस भाग में दी गई परिभाषाएं और प्रमेय **किसी भी वलय** के लिए सत्य हैं। हमने अपने को क्रमविनिमेय वलयों तक सीमित नहीं रखा है। लेकिन हमें रुचि है उस स्थिति में जबकि R एक प्रांत हो। अगले भाग में हम इस स्थिति की ओर बढ़ेंगे।

13.3 R[x] के कुछ गुण

पिछले भाग में आपने वलय R की और वलय R[x] की संक्रियाओं के निकट संबंध को देखा है। निम्नलिखित प्रमेय इस तथ्य को और भी प्रदर्शित करता है।

प्रमेय 2 : मान लीजिए R एक वलय है।

(क) यदि R क्रमविनिमेय है, तो R[x] भी क्रमविनिमेय होगा।

(ख) यदि R तत्समकी है, तो R[x] भी तत्समकी होगा।

उपपत्ति : (क) मान लीजिए

$p(x) = a_0 + a_1 x + ... + a_n x^n$ और

$q(x) = b_0 + b_1 x + \ldots + b_m x^m$, $R[x]$ में हैं।

तब $p(x) \cdot q(x) = c_0 + c_1 x + \ldots + c_s x^s$, जहां $s = m + n$ और

$c_k = a_k b_0 + a_{k-1} b_1 + \ldots + a_0 b_k$

$= b_k a_0 + b_{k-1} a_1 + \ldots + b_1 a_{k-1} + b_0 a_k$, क्योंकि R में योग और गुणन दोनों ही क्रमविनिमेय हैं।

$= q(x)\, p(x)$ में x^k का गुणांक।

इस तरह, सभी $i \geq 0$ के लिए $p(x)q(x)$ और $q(x)p(x)$ में x^i के गुणांक बराबर हैं।

अतः $p(x)q(x) = q(x)p(x)$.

(ख) हम जानते हैं कि R का तत्समक 1 है। हम सिद्ध करेंगे कि अचर बहुपद 1, $R[x]$ का तत्समक है। इसके लिए कोई $p(x) = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ लीजिए।

तब $1 \cdot p(x) = c_0 + c_1 x + \ldots + c_n x^n$ (क्योंकि $\deg 1 = 0$).

जहां $c_k = a_k \cdot 1 + a_{k-1} \cdot 0 + a_{k-2} \cdot 0 + \ldots + a_0 \cdot 0$

$= a_k$

अतः $1.p(x) = p(x)$.

इसी प्रकार $p(x) . 1 = p(x)$.

इससे पता चलता है कि 1, $R[x]$ का तत्समक है।

नीचे दिए गए प्रश्न में हम आपसे यह जांच करने को कह रहे हैं कि प्रमेय 2 का विलोम सत्य है या नहीं।

E4) यदि R एक ऐसा वलय हो कि $R[x]$ क्रमविनिमेय और तत्समकी हो, तो

(क) क्या R क्रमविनिमेय होगा ?

(ख) क्या R तत्समकी होगा ?

आइए अब हम एक ऐसे परिणाम पर गौर करें जिसकी सहायता से हम दिखा सकेंगे कि R एक प्रांत होता है यदि और केवल यदि $R[x]$ एक प्रांत हो। यह परिणाम बहुपदों के गुणन की परिभाषा से सीधे प्राप्त हो जाता है।

प्रमेय 3 : मान लीजिए R एक वलय है और $f(x)$ तथा $g(x)$, $R[x]$ के दो शून्येतर अवयव है। तब,

$$\deg(f(x)\, g(x)) \leq \deg f(x) + \deg g(x).$$

यदि R पूर्णांकीय प्रांत हो; तो ये दोनों पक्ष बराबर होते हैं।

उपपत्ति : मान लीजिए $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_n \neq 0$, और $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, $b_m \neq 0$.

तब $\deg f(x) = n$, $\deg g(x) = m$. हम जानते हैं कि

$f(x) \cdot g(x) = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n}$,

जहां $c_k = a_k b_0 + a_{k-1} b_1 + \ldots + a_0 b_k$.

चूंकि $a_{n+1}, a_{n+2}, \ldots$ और $b_{m+1}, b_{m+2}, \ldots$ सभी शून्य हैं,

इसलिए $c_{m+n} = a_n b_m$.

अब, यदि R में कोई शून्य के भाजक नहीं हैं, तो $a_n b_m \neq 0$, क्योंकि $a_n \neq 0$ और $b_m \neq 0$. अतः इस स्थिति में $\deg(f(x)g(x)) = m+n = \deg f(x) + \deg g(x)$.

दूसरी ओर, यदि R में शून्य के भाजक हों, तो हो सकता है कि $a_n b_m = 0$. इस स्थिति मे

$\deg(f(x)g(x)) < m+n = \deg f(x) + \deg g(x)$

इस तरह, हमारा प्रमेय सिद्ध हो जाता है।

प्रमेय 3 से निम्नलिखित परिणाम तुरंत प्राप्त हो जाता है।

प्रमेय 4 : $R[x]$ एक पूर्णांकीय प्रांत है $\Leftrightarrow R$ एक पूर्णांकीय प्रांत है।

उपपत्ति : प्रमेय 2 और E4 से हम जानते हैं कि R एक तत्समकी क्रमविनिमेय वलय होता है यदि और केवल यदि $R[x]$ एक तत्समकी क्रमविनिमेय वलय हो। इस तरह, इस प्रमेय को सिद्ध करने के लिए हमें सिद्ध करना होगा कि R में कोई शून्य के भाजक नहीं है।

अतः आइए पहले हम यह मान लें कि R में कोई शून्य के भाजक नहीं है।

मान लीजिए $p(x) = a_0+a_1x+...+a_nx^n$ और
$q(x) = b_0+b_1x+...+b_mx^m$, $R[x]$ में हैं, जहां $a_n \neq 0$ और $b_m \neq 0$.

तब प्रमेय 3 में हमने देखा है कि

$$\deg(p(x)q(x)) = m + n$$

इस तरह, $p(x)q(x) \neq 0$.

अतः $R[x]$ में कोई शून्य के भाजक नहीं हैं।

विलोमतः, मान लीजिए $R[x]$ में कोई शून्य के भाजक नहीं है। मान लीजिए a और b, R के शून्येतर अवयव हैं। तब ये $R[x]$ के शून्येतर अवयव भी हैं। इसलिए $ab \neq 0$. इस तरह, R में कोई शून्य के भाजक नहीं हैं। इस तरह हमने प्रमेय सिद्ध कर दिया है।

अब देखिए कि आप नीचे दिए गए प्रश्नों को हल कर सकते हैं या नहीं।

E5) निम्नलिखित बहुपद वलयों में से कौन से वलयों में शून्य के भाजक नहीं हैं ?

(क) $R[x]$, जहां $R = \{a+b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$

(ख) $\mathbf{Z}_7[x]$

(ग) $\mathbf{Z}_6[x]$

(घ) $R[x]$, जहां $R = C[0, 1]$.

E6) मान लीजिए R एक प्रांत है। दिखाइए कि $\text{char } R = \text{char } R[x]$.

E7) मान लीजिए R और S क्रमविनिमेय वलय हैं और $f : R \to S$ एक वलय समाकारिता है।

दिखाइए कि फलन

$$\phi : R[x] \to S[x] : \phi(a_0+a_1 x + ... + a_n x^n) = f(a_0) + f(a_1)x + ... + f(a_n)x^n$$

एक समाकारिता है।

आपने देखा है कि वलय R के अनेक गुण $R[x]$ के भी गुण होते हैं। इस तरह, यदि F एक क्षेत्र है, तो हम आशा कर सकते हैं कि $F[x]$ भी एक क्षेत्र होगा। लेकिन ऐसा नहीं है। $F[x]$ कभी भी क्षेत्र नहीं हो सकता। इसका कारण है कि $F[x]$ में धन घात वाले किसी भी बहुपद का गुणनात्मक व्युत्क्रम नहीं होता है। आइए देखें ऐसा क्यों।

मान लीजिए $f(x) \in F[x]$ और $\deg f(x) = n > 0$.

मान लीजिए $g(x) \in F[x]$ ऐसा है कि $f(x)g(x) = 1$.

तब $0 = \deg 1 = \deg (f(x)g(x)) = \deg f(x) + \deg g(x)$, क्योंकि F एक प्रांत है।
$= n+\deg g(x) \geq n > 0$

इस तरह हमें एक अंतर्विरोध प्राप्त होता है।

इसलिए F[x] क्षेत्र नहीं हो सकता।

परंतु F[x] के ऐसे अनेक रोचक गुण हैं, जो पूर्णांक समुच्चय Z के गुणों के समान हैं। अगले भाग में हम F[x] में विभाजन के गुणों पर चर्चा करेंगे। आप देखेंगे कि वे Z के उन गुणों के कितने समान हैं, जिन पर हम भाग 1.6.2 में चर्चा कर चुके हैं।

13.4 विभाजन-कलन विधि

उप-भाग 1.6.2 में हम Z में विभाज्यता के विभिन्न गुणों पर चर्चा कर चुके हैं। विशेष रूप में, हमने पूर्णांकों की विभाजन-कलन विधि को सिद्ध किया था। यही बात हम क्षेत्र F पर बहुपदों के लिए करेंगे।

प्रमेय 5 (विभाजन-कलन विधि) : मान लीजिए F एक क्षेत्र है। मान लीजिए $f(x)$ और $g(x)$, $F[x]$ में दो बहुपद हैं, जहां $g(x) \neq 0$, तब

(क) F[x] में ऐसे दो बहुपद $q(x)$ और $r(x)$ हैं जिनसे कि

$$f(x) = q(x)g(x)+r(x), \text{ जहाँ } \deg r(x) < \deg g(x)$$

(ख) बहुपद $q(x)$ और $r(x)$ अद्वितीय हैं।

उपपत्ति : (क) यदि $\deg f(x) < \deg g(x)$, तो हम $q(x) = 0$ ले सकते हैं।

तब $f(x) = 0 \cdot g(x) + f(x)$, जहाँ $\deg f(x) < \deg g(x)$.
आइए अब हम मान लें कि $\deg f(x) \geq \deg g(x)$.

मान लीजिए $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_n \neq 0$, और

$$g(x) = b_0 + b_1 x + \ldots + b_m x^m, \; b_m \neq 0, \text{ जहां } n \geq m.$$

हम $\deg f(x)$, अर्थात् n पर आगमन नियम (भाग 1.6.1 देखिए) लागू करेंगे।

यदि $n = 0$, तो $m = 0$, क्योंकि $g(x) \neq 0$.

अब $f(x) = a_0$, $g(x) = b_0$, अतः

$$f(x) = (a_0 b_0^{-1})\, b_0 + 0 = q(x)g(x) + r(x), \text{ जहाँ } q(x) = a_0 b_0^{-1}$$

और $r(x) = 0$.

इस तरह,

$$f(x) = q(x)g(x) + r(x), \text{ जहाँ } \deg r(x) < \deg g(x).$$

इसलिए $n = 0$ के लिए कलन विधि लागू होती है। आइए हम मान लें कि घात $\leq n-1$ वाले सभी बहुपदों पर कलन विधि लागू होती है और यह स्थापित करने की कोशिश करें कि यह $f(x)$ के लिए भी सही है। अब निम्नलिखित बहुपद लीजिए :

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$

$$= (a_0 + a_1 x + \ldots + a_n x^n) - (a_n b_m^{-1} b_0 x^{n-m} + a_n b_m^{-1} b_1 x^{n-m+1} + \ldots + a_n b_m^{-1} b_m x^n)$$

इस तरह, $f_1(x)$ में x^n का गुणांक शून्य है। अतः $\deg f_1(x) \leq n-1$.

आगमन-परिकल्पना के अनुसार $F[x]$ में ऐसे $q_1(x)$ और $r(x)$ हैं जिनसे कि

$$f_1(x) = q_1(x)g(x) + r(x), \text{ जहां } \deg r(x) < \deg g(x).$$

$f_1(x)$ का मान प्रतिस्थापित करने पर हमें निम्नलिखित प्राप्त होता है :

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = q_1(x)\, g(x) + r(x),$$

अर्थात् $f(x) = \{a_n b_m^{-1} x^{n-m} + q_1(x)\}\, g(x) + r(x)$

$= q(x)\,g(x) + r(x)$, जहां $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$

और $\deg r(x) < \deg g(x)$.

इसलिए, $f(x)$ के लिए कलन विधि सही है। अतः यह $F[x]$ के सभी बहुपदों के लिए सही है।

(ख) आइए अब हम दिखाएं कि $q(x)$ और $r(x)$ अद्वितीयतः निर्धारित होते हैं।

यदि संभव हो, तो मान लीजिए

$f(x) = q_1(x)g(x) + r_1(x)$, जहां $\deg r_1(x) < \deg g(x)$

और $f(x) = q_2(x)g(x) + r_2(x)$, जहां $\deg r_2(x) < \deg g(x)$.

तब, $q_1(x)g(x)+r_1(x) = q_2(x)\,g(x) + r_2(x)$, जिससे कि

$\{q_1(x) - q_2(x)\}\,g(x) = r_2(x) - r_1(x)$ ....(1)

अब, यदि $q_1(x) \neq q_2(x)$, तब

$\deg\{q_1(x) - q_2(x)\} \geq 0$, जिससे कि

$\deg[\{q_1(x) - q_2(x)\}\,g(x)] \geq \deg g(x)$.

दूसरी ओर, $\deg\{r_2(x) - r_1(x)\} < \deg g(x)$, क्योंकि

$\deg r_1(x) < \deg g(x)$ और $\deg r_2(x) < \deg g(x)$.

परंतु, यह समीकरण (1) का अंतर्विरोध करता है। अतः समीकरण (1) तभी सही होगा जबकि

$q_1(x) - q_2(x) = 0$, और तब $r_2(x) - r_1(x) = 0$.

अर्थात् $q_1(x) = q_2(x)$ और $r_1(x) = r_2(x)$.

इस तरह, हमने व्यंजक $f(x) = q(x)g(x)+r(x)$ में $q(x)$ और $r(x)$ की अद्वितीयता को सिद्ध कर दिया है।

यहां $q(x)$, $f(x)$ को $g(x)$ से भाग देने पर प्राप्त **भागफल** (quotient) है और $r(x)$ **शेषफल** (remainder) है।

अब, यदि हम प्रमेय 5 के $g(x)$ को रैखिक बहुपद मानें, तो क्या होता है ? हमें शेषफल प्रमेय प्राप्त होता है। इसे सिद्ध करने से पहले आइए हम कुछ संकेतन स्थापित करें।

संकेतन : मान लीजिए R एक वलय है और $f(x) \in R[x]$, मान लीजिए $f(x) = a_0 + a_1x + ... + a_nx^n$.

तब, किसी $r \in R$ के लिए $f(r) = a_0 + a_1r + ... + a_nr^n \in R$.

अर्थात् $f(r)$, **x के स्थान पर r प्रतिस्थापित करने पर प्राप्त $f(x)$ का मान** है। इस तरह, यदि $f(x) = 1+x+x^2 \in Z[x]$ तो $f(2) = 1+2+4 = 7$ और $f(0) = 1+0+0 = 1$.

आइए अब हम शेषफल प्रमेय (remainder theorem) सिद्ध करें जो विभाजन-कलन विधि का एक उपप्रमेय है।

प्रमेय 6 (शेषफल प्रमेय) : मान लीजिए F एक क्षेत्र है। यदि $f(x) \in F[x]$ और $b \in F$, तो एक ऐसा अद्वितीय बहुपद $q(x) \in F[x]$ है जिससे कि $f(x) = (x-b)q(x)+f(b)$.

उपपत्ति : मान लीजिए $g(x) = x - b$, तब $f(x)$ और $g(x)$ पर विभाजन-कलन विधि लागू करके हम $F[x]$ में ऐसे अद्वितीय $q(x)$ और $r(x)$ प्राप्त कर सकते हैं कि $f(x) = q(x)g(x)+r(x)$
$= q(x)(x-b)+r(x)$, जहां $\deg r(x) < \deg g(x) = 1$, क्योंकि $\deg r(x) < 1$, इसलिए $r(x)$, F का एक अवयव, मान लीजिए a, है।

अतः $f(x) = (x-b)q(x)+a$.

x के स्थान पर b प्रतिस्थापित करने पर हमें निम्नलिखित प्राप्त होता है :

$f(b) = (b - b)q(b)+a = 0\cdot q(b)+a.$

$= a.$

इस तरह, $a = f(b)$.

इसलिए $f(x) = (x-b)q(x)+f(b)$.

ध्यान दीजिए कि

$\deg f(x) = \deg(x-b)+\deg q(x) = 1+\deg q(x)$.

इसलिए $\deg q(x) = \deg f(x) - 1$.

आइए अब हम कुछ स्थितियों में विभाजन-कलन विधि लागू करें।

उदाहरण 1 : $x^4+x^3+5x^2-x$ को $Q[x]$ में $(x^2+x+1)q(x)+r(x)$ के रूप में व्यक्त कीजिए।

हल : हम बहुपदों के लिए भाग करने की लंबी विधि द्वारा इस प्रश्न को हल करेंगे।

$$\begin{array}{r|l} & x^2+4 \\ x^2+x+1 & x^4+x^3+5x^2-x \\ & \underline{x^4+x^3+x^2} \\ & \quad 4x^2-x \\ & \quad \underline{4x^2+4x+4} \\ & \qquad -5x-4 \end{array}$$

अब, क्योंकि शेषफल $(-5x-4)$ का घात $\deg(x^2+x+1)$ से कम है, इसलिए हम प्रक्रिया को रोक देते हैं। अतः हम पाते हैं कि $x^4+x^3+5x^2-x = (x^2+4)(x^2+x+1) - (5x+4)$.

यहां भागफल x^2+4 है और शेषफल $-(5x+4)$ है।

अब आप नीचे दिए गए प्रश्न हल कीजिए।

E8) निम्नलिखित स्थितियों में से प्रत्येक में f को $gq+r$ के रूप में व्यक्त कीजिए, जहां $\deg r < \deg g$.

(क) $Q[x]$ में $f = x^4+1$, $g = x^3$.

(ख) $Z_3[x]$ में $f = x^3+\bar{2}x^2-x+\bar{1}$, $g = x+\bar{1}$.

(ग) $R[x]$ में $f = x^3-1$, $g = x-1$.

E9) आप जानते हैं कि यदि $p, q \in Z$, $q \neq 0$, तो $\frac{p}{q}$ को हम एक पूर्णांक और एक भिन्न $\frac{m}{q}$ के योगफल के रूप में लिख सकते हैं, जहां $|m| < |q|$. $F[x]$ के अवयवों के लिए इसके अनुरूप गुण क्या है ?

आइए, अब हम देखें कि यदि व्यंजक $f = qg+r$ में शेषफल शून्य हो, तो क्या होता है।

13.5 बहुपदों के मूल

भाग 12.4 में आपने देखा है कि हम कब कह सकते हैं कि वलय का एक अवयव दूसरे अवयव को विभाजित करता है। आइए हम $F[x]$ के संदर्भ में परिभाषा याद करें, जहां F एक क्षेत्र है।

परिभाषा : मान लीजिए $f(x)$ और $g(x)$, $F[x]$ में हैं, जहां F एक क्षेत्र है और $g(x) \neq 0$. हम कहते हैं कि $g(x)$, $f(x)$ को **विभाजित** करता है (या $g(x)$, $f(x)$ का एक **गुणनखंड** है, या $f(x)$, $g(x)$ से **भाज्य** है) यदि ऐसा $q(x) \in F[x]$ है जिससे कि $f(x) = q(x)g(x)$. हम '$g(x)$, $f(x)$ को विभाजित करता है' को $g(x) \mid f(x)$ से और '$g(x)$, $f(x)$ को विभाजित नहीं करता' को $g(x) \nmid f(x)$ से दर्शाते हैं।

अब, यदि $f(x) \in F[x]$ और $g(x) \in F[x]$, जहां $g(x) \neq 0$, तो क्या हमें प्रमेय 5 से पता चलता है कि कब $g(x) \mid f(x)$? हाँ। प्रमेय 5 में यदि $r(x) = 0$ तो $g(x) \mid f(x)$.

नीचे दिए गए प्रश्न में हमने इसी प्रकार का एक महत्वपूर्ण कथन दिया है। प्रमेय 6 की सहायता से आप इसे सिद्ध कर सकते हैं।

E 10) मान लीजिए F एक क्षेत्र है और $f(x) \in F[x]$, जहाँ $\deg f(x) \geq 1$. मान लीजिए $a \in F$. दिखाइए कि $(x-a)$, $f(x)$ को विभाजित करता है यदि और केवल यदि $f(a) = 0$.

इस प्रश्न से संबंधित निम्नलिखित परिभाषा देखिए।

परिभाषा : मान लीजिए F एक क्षेत्र है और $f(x) \in F[x]$. हम कहते हैं कि अवयव $a \in F$, $f(x)$ का एक **मूल** (root) (या **शून्यक** (zero)) होता है, यदि $f(a) = 0$. उदाहरण के लिए, 1, $x^2-1 \in \mathbf{R}[x]$ का एक मूल है, क्योंकि $1^2-1 = 0$.

इसी प्रकार, (-1), $f(x) = x^3 + x^2 + \frac{1}{2}x + \frac{1}{2} \in \mathbf{Q}[x]$ का एक मूल है, क्योंकि

$f(-1) = -1 + 1 - \frac{1}{2} + \frac{1}{2} = 0.$

ध्यान दीजिए कि E10 में हमने किसी अवयव का बहुपद का एक मूल होने के लिए निम्नलिखित निकष सिद्ध किया है :

मान लीजिए F एक क्षेत्र है और $f(x) \in F[x]$. **तब** $a \in F$, $f(x)$ **का एक मूल होता है यदि और केवल यदि** $(x-a) \mid f(x)$.

हम F[x] में बहुपद के बहुकता (multiplicity) m वाले मूल को परिभाषित करने के लिए इस निकष का व्यापकीकरण कर सकते हैं।

परिभाषा : मान लीजिए F एक क्षेत्र है और $f(x) \in F[x]$. हम कहते हैं कि $a \in F$, $f(x)$ का बहुकता m वाला एक मूल होता है (जहाँ m एक धन पूर्णांक है) यदि $(x-a)^m \mid f(x)$, परंतु $(x-a)^{m+1} \nmid f(x)$.

उदाहरण के लिए, 3 बहुपद $(x-3)^2 (x+2) \in \mathbf{Q}[x]$ का बहुकता 2 वाला एक मूल है, और (-2) इस बहुपद का बहुकता 1 वाला मूल है।

अब, बताइए कि क्या किसी दिए हुए बहुपद के सभी मूल प्राप्त करना आसान है ? कोई भी रैखिक बहुपद $ax+b \in F[x]$ का केवल एक मूल, अर्थात् $-a^{-1}b$ होगा। ऐसा इसलिए है क्योंकि $ax+b = 0$ यदि और केवल यदि $x = -a^{-1}b$. यदि हमें कोई द्विघात बहुपद $ax^2+bx+c \in F[x]$ दिया हो तो, आप जानते हैं कि द्विघाती सूत्र (quadratic formula) $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ लागू करके हम इसके दोनों मूल प्राप्त कर सकते हैं। इससे बड़े घात वाले बहुपदों के कुछ मूल हम जांच और भूल विधि से प्राप्त कर सकते हैं। जैसे कि $f(x) = x^5-2x+1 \in \mathbf{R}[x]$ लीजिए। तब हम $x=1$ प्रतिस्थापित करके देखते हैं कि $f(1) = 0$. अतः हम पाते हैं कि 1, $f(x)$ का मूल है। लेकिन इस विधि से हमें $f(x)$ के सभी मूल प्राप्त नहीं होते।

अब आप नीचे दिए गए प्रश्न हल कीजिए।

E11) निम्नलिखित बहुपदों के मूल उनकी बहुकता के साथ ज्ञात कीजिए :

(क) $f(x) = \frac{1}{2}x^2 - \frac{5}{2}x + 3 \in \mathbf{Q}[x]$

(ख) $f(x) = x^2 + x + \overline{1} \in \mathbf{Z}_3[x]$

(ग) $f(x) = x^4 + \overline{2}x^3 - \overline{2}x - \overline{1} \in \mathbf{Z}_5[x]$

E12) मान लीजिए F एक क्षेत्र है और $a \in F$. फलन $\phi : F[x] \to F$: $\phi(f(x)) = f(a)$ परिभाषित कीजिए।

यह फलन a पर **मानांकन** (evaluation) है।

दिखाइए कि

(क) ϕ एक आच्छादक वलय समाकारिता है।

(ख) $\phi(b) = b \ \forall \ b \in F$.

(ग) $\text{Ker } \phi = \langle x - a \rangle$.

इस स्थिति में समाकारिता का मूल प्रमेय क्या कहता है ?

जैसा कि हमने अभी देखा है, किसी बहुपद के सभी मूल प्राप्त करना आसान नहीं है। लेकिन हम बहुपद के मूल की संख्या से संबंधित एक परिणाम दे सकते हैं।

प्रमेय 7 : मान लीजिए $f(x)$ क्षेत्र F पर घात n वाला एक शून्येतर बहुपद है। तब F में $f(x)$ के अधिक से अधिक n मूल होते हैं।

उपपत्ति : यदि $n = 0$, तो $f(x)$ एक शून्येतर अचर बहुपद होगा। इस तरह, इसका कोई भी मूल नहीं है। अतः F में इसके अधिक से अधिक $0 (= n)$ मूल होंगे।

तो, आइए हम मान लें कि $n \geq 1$. हम n पर आगमन नियम लागू करेंगे। यदि $\deg f(x) = 1$, तो $f(x) = a_0 + a_1x$, जहां $a_0, a_1 \in F$ और $a_1 \neq 0$. $f(x)$ का केवल एक मूल, अर्थात् $(-a_1^{-1}a_0)$ है।

अब मान लीजिए कि यह प्रमेय $F(x)$ में घात $< n$ वाले सभी बहुपदों के लिए सत्य है। हम दिखाएंगे कि $f(x)$ के मूलों की संख्या $\leq n$.

यदि $f(x)$ का F में कोई मूल नहीं है, तो F में $f(x)$ के मूलों की संख्या $0 \leq n$ है।

अब मान लीजिए कि $f(x)$ का एक मूल $a \in F$ है।

तब $f(x) = (x-a)g(x)$, जहां $\deg g(x) = n - 1$.

अतः आगमन-परिकल्पना से F में $g(x)$ के अधिक से अधिक $n - 1$ मूल होंगे। मान लीजिए ये $a_1, a_2, \ldots, a_{n-1}$ हैं।

अब a_i, $g(x)$ का मूल है $\Rightarrow g(a_i) = 0 \Rightarrow f(a_i) = (a_i - a)\, g(a_i) = 0$

$\Rightarrow a_i$, $f(x)$ का मूल है $\forall \ i = 1, \ldots, n-1$. इस तरह, $g(x)$ का प्रत्येक मूल $f(x)$ का एक मूल होता है। अब $b \in F$, $f(x)$ का एक मूल होता है यदि और केवल यदि $f(b) = 0$, अर्थात् यदि और केवल यदि $(b-a)g(b) = 0$, अर्थात् यदि और केवल यदि $b - a = 0$ या $g(b) = 0$, क्योंकि F एक पूर्णांकीय प्रांत है। अतः b, $f(x)$ का एक मूल होता है यदि और केवल यदि $b = a$ या b, $g(x)$ का एक मूल हो। इसलिए $f(x)$ के मूल केवल a और $a_1, \ldots, a_{n-1}$ हैं। इस तरह $f(x)$ के अधिक से अधिक n मूल होते हैं। इसलिए प्रमेय n के लिए सत्य है।

अतः प्रमेय सभी $n \geq 1$ के लिए सही है।

उदाहरण के लिए, इस परिणाम को लागू करने पर हम जान जाते हैं कि $x^3 - 1 \in Q[x]$ के Q में 3 से अधिक मूल नहीं हो सकते।

प्रमेय 7 में हमने मूलों के अलग-अलग होने के बारे में कुछ नहीं कहा है। लेकिन प्रमेय 7 से ज़ाहिर है कि

यदि $f(x) \in F[x]$ का घात n हो, तो F में $f(x)$ के अधिक से अधिक n अलग-अलग मूल होते हैं।

हम इस परिणाम का प्रयोग निम्नलिखित उपयोगी प्रमेय को सिद्ध करने के लिए करेंगे।

प्रमेय 8 : मान लीजिए $f(x)$ और $g(x)$ क्षेत्र F पर घात n वाले दो शून्येतर बहुपद हैं। यदि F में ऐसे $n+1$ अलग-अलग अवयव $a_1, \ldots, a_{n+1}$ हैं जिनके लिए $f(a_i) = g(a_i) \ \forall \ i = 1, \ldots, n+1$ तो $f(x) = g(x)$.

उपपत्ति : बहुपद $h(x) = f(x) - g(x)$ लीजिए। तब $\deg h(x) \leq n$, परंतु इसके $n+1$ अलग-अलग मूल $a_1, \ldots, a_{n+1}$ हैं। यह केवल तब संभव है जब $h(x) = 0$, अर्थात् $f(x) = g(x)$.

अब हम आपको एक उदाहरण देंगे यह दिखाने के लिए कि यदि प्रमेय 7 (और प्रमेय 8) में F को क्षेत्र न लेकर कोई भी वलय लें तो हो सकता है कि कथन सत्य न हो।

उदाहरण 2 : सिद्ध कीजिए कि $x^3 + \bar{5}x \in \mathbf{Z}_6[x]$ के मूलों की संख्या उसके घात से अधिक है। (ध्यान दीजिए कि $\mathbf{Z}_6$ एक क्षेत्र नहीं है।)

हल : क्योंकि वलय परिमित है इसलिए हम एक-एक करके सभी अवयव लेकर जांच कर सकते हैं कि इनमें से कौन से अवयव $f(x) = x^3 + \bar{5}x$ के मूल हैं।

प्रतिस्थापन करने पर हम पाते हैं कि

$$f(\bar{0}) = 0 = f(\bar{1}) = f(\bar{2}) = f(\bar{3}) = f(\bar{4}) = f(\bar{5}).$$

यानि कि $\mathbf{Z}_6$ का प्रत्येक अवयव $f(x)$ का शून्यक है। इस तरह, $f(x)$ के 6 शून्यक हैं जबकि $\deg f(x) = 3$.

अब आप नीचे दिए गए प्रश्नों को हल कीजिए।

E13) मान लीजिए p एक अभाज्य संख्या है। $x^{p-1} - \bar{1} \in \mathbf{Z}_p[x]$ लीजिए। आप जानते हैं कि $\mathbf{Z}_p$ कोटि p वाला एक समूह है। इस तथ्य के प्रयोग से दिखाइए कि $\mathbf{Z}_p$ का प्रत्येक शून्येतर अवयव $x^{p-1} - \bar{1}$ का एक मूल है और दिखाइए कि इसलिए

$$x^{p-1} - \bar{1} = (x - \bar{1})(x - \bar{2}) \text{ .... } (x - \overline{p-1}).$$

E14) बहुपद $x^4 + \bar{4}$ को $\mathbf{Z}_5[x]$ में रैखिक गुणनखंडों में गुणनखंडित किया जा सकता है।

इस गुणनखंडन को ज्ञात कीजिए।

अभी तक हम कहते आए हैं कि F पर घात n वाले बहुपद के F में अधिक से अधिक n मूल होते हैं। लेकिन यह भी हो सकता है कि बहुपद का F में कोई मूल न हो। उदाहरण के लिए, बहुपद $x^2 + 1 \in \mathbf{R}[x]$ लीजिए।

प्रमेय 7 से आप जानते हैं कि **R** में इसके अधिक से अधिक 2 मूल हो सकते हैं। परंतु, जैसा कि आप जानते हैं, **R** में इसका कोई भी मूल नहीं है (**C** में इसके दो मूल i और –i हैं)। हम $\mathbf{R}[x]$ में इस प्रकार के बहुपदों के अनेक उदाहरण प्राप्त कर सकते हैं। ऐसे बहुपदों को **R** पर **अखंडनीय बहुपद** (irreducible polynomial) कहते हैं। इन पर विस्तृत चर्चा हम अगली इकाइयों में करेंगे।

आइए, अब हम इस इकाई को इसमें दी गई पाठ्य सामग्री का संक्षिप्त विवरण देते हुए यहीं समाप्त करें।

13.6 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों पर ग़ौर किया है।

1) किसी वलय पर बहुपदों की परिभाषा और उनके उदाहरण।

2) $R[x]$ की वलय संरचना, जहां R एक वलय है।

3) R तत्समकी क्रमविनिमेय वलय होता है यदि और केवल यदि $R[x]$ तत्समकी क्रमविनिमेय वलय हो।

4) R एक पूर्णांकीय प्रांत होता है यदि और केवल यदि $R[x]$ एक पूर्णांकीय प्रांत हो।

5) $F[x]$ में विभाजन-कलन विधि, जहां F एक क्षेत्र है, जिसके अनुसार यदि $f(x), g(x) \in F[x], g(x) \neq 0$, तो ऐसे अद्वितीय $q(x), r(x) \in F[x]$, हैं जिनसे कि $f(x) = q(x)\,g(x) + r(x)$ और $\deg r(x) < \deg g(x)$.

6) $a \in F$, $f(x) \in F[x]$ का एक मूल होता है यदि और केवल यदि $(x-a) \mid f(x)$.

7) क्षेत्र F पर घात n वाले शून्येतर बहुपद के अधिक से अधिक n मूल हो सकते हैं।

13.7 हल/उत्तर

E1) बहुपद (क), (ग), (घ), (च) है। (ख) और (ङ) बहुपद नहीं है, क्योंकि इनमें x के ऋणात्मक और भिन्नात्मक घात हैं। (क) और (घ) $\mathbf{Z}[x]$ में हैं।

E 2) घात क्रमशः 1, 3, 4, 3, $-\infty$ हैं। पहले चार के अग्रग-गुणांक क्रमशः $\sqrt{2}, -7, 1, \frac{1}{7}$ हैं। 0 का कोई अग्रग-गुणांक नहीं हैं।

E3) (क) $2 + 5x + 3x^2 + (4+1)x^3 = 2 + 5x + 3x^2 + 5x^3$.

(ख) $(\overline{6}+\overline{1}) - \overline{2}x + \overline{2}x^2 + \overline{5}x^3 = -\overline{2}x + \overline{2}x^2 + \overline{5}x^3$, क्योंकि $\overline{7} = \overline{0}$.

(ग) $1 + 3x + 3x^2 + x^3$

(घ) $\overline{1} + x^3$, क्योंकि $\overline{3} = \overline{0}$.

(ङ) $10x + 5x^2 + 7x^3 + x^4 + x^5$.

E4) R का प्रत्येक अवयव R[x] का अवयव है। इसलिए, R में गुणन भी क्रमविनिमेय है। और R[x] का तत्समक R का अवयव है, और इसलिए R का तत्समक है।

E5) (क) और (ख)।

E6) हम जानते हैं कि R[x] एक प्रांत है। मान लीजिए char R = n. इकाई 12 के प्रमेय 3 से हम जानते हैं कि n न्यूनतम धन पूर्णांक है जिससे कि $n \cdot 1 = 0$. क्योंकि 1, R[x] का भी तत्समक है, इसलिए इकाई 12 के उसी प्रमेय के अनुसार char R[x] = n = char R.

E7) मान लीजिए

$p(x) = a_0 + a_1x + \ldots + a_n x^n$, $q(x) = b_0 + b_1x + \ldots + b_m x^m \in R[x]$

तब $\phi(p(x) + q(x)) = \phi\left(\sum_{i=0}^{t} (a_i+b_i) x^i\right)$, जहां $t = \max(m, n)$.

$$= \sum_{i=0}^{t} f(a_i + b_i) x^i$$

$$= \sum_{i=0}^{t} [f(a_i) + f(b_i)] x^i$$

$$= \sum_{i=0}^{t} f(a_i) x^i + \sum_{i=0}^{t} f(b_i) x^i$$

$= \phi(p(x)) + \phi(q(x))$, क्योंकि $f(a_i) = 0 = f(b_i)$ जब भी $a_i = 0,\ b_i = 0$.

और $\phi(p(x)\, q(x)) = \phi\left(\sum_{i=0}^{m+n} c_i x^i\right)$, जहां $c_i = a_i b_0 + a_{i-1} b_1 + \ldots + a_0 b_i$

$$= \sum_{i=0}^{m+n} f(c_i) x^i$$

$$= \sum_{i=0}^{m+n} [f(a_i) f(b_0) + f(a_{i-1}) f(b_1) + \ldots + f(a_0) f(b_i)] x^i,$$

क्योंकि f एक वलय समाकारिता है।

$$= \phi(p(x))\, \phi(q(x)).$$

अतः ϕ एक वलय समाकारिता है।

E8) (क) $f = x.g + 1,\ q = x,\ r = 1$.

(ख)
$$\begin{array}{r l} & x^2 + x - \bar{2} \\ x+\bar{1} & \overline{)\, x^3 + \bar{2}x^2 - x + \bar{1}} \\ & x^3 + x^2 \\ \hline & x^2 - x + \bar{1} \\ & x^2 + x \\ \hline & -\bar{2}x + \bar{1} \\ & -\bar{2}x - \bar{2} \\ \hline & \bar{3} \\ \hline \end{array}$$

इस तरह, $f = (x^2+x-\bar{2})\, g + \bar{0}$, क्योंकि $\bar{3} = \bar{0}$.

(ग) $f = (x^2+x+1)\, g + 0$.

E9) मान लीजिए $f(x), g(x) \in F[x]$, जहाँ $g(x) \neq 0$.

प्रमेय 5 के अनुसार, $f(x) = g(x)\, q(x) + r(x)$, जहाँ $\deg r(x) < \deg g(x)$. अब, यह समता तब भी सही होती है जब हम इसे $F[x]$ के विभाग क्षेत्र पर लें। तब हम पूरे को $g(x)$ से भाग देकर निम्नलिखित प्राप्त करते हैं :

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}, \text{ जहां } \deg r(x) < \deg g(x).$$

E10) प्रमेय 6 के अनुसार,

$f(x) = (x-a)\, q(x) + f(a)$.

इस तरह, $f(x) = (x-a)\, q(x)$ यदि और केवल यदि $f(a) = 0$, अर्थात् $(x-a) \mid f(x)$ यदि और केवल यदि $f(a) = 0$.

E11) (क) द्विघाती सूत्र से मूल 3 और 2 हैं, और प्रत्येक की बहुकता 1 है।

(ख) $x^2 + x + \bar{1} = (x-\bar{1})^2$, क्योंकि Z_3 में $-\bar{2} = \bar{1}$. इस तरह $\bar{1}$ ही इसका शून्यक है, और इसकी बहुकता 2 है।

(ग) जाँच से, एक मूल $\bar{1}$ है। अब भाग करने की लंबी विधि से हम देखते हैं कि

$$x^4 + \bar{2}x^3 - \bar{2}x - \bar{1} = (x-\bar{1})(x^3+\bar{3}x^2+\bar{3}x+\bar{1}).$$

फिर से जाँच और भूल विधि से हम जान लेते हैं कि $x + \bar{1}$, $x^3 + \bar{3}x^2 + \bar{3}x + \bar{1}$ का एक गुणनखंड है।

भाग की लंबी विधि से हम पाते हैं कि

$x^3 + \bar{3}x^2 + \bar{3}x + \bar{1} = (x+\bar{1})^3$

इस तरह, $x^4 + \bar{2}x^3 - \bar{2}x - \bar{1} = (x-\bar{1})(x+\bar{1})^3$.

इससे पता चलता है कि $\bar{1}$, बहुकता 1 वाला एक मूल है और $-\bar{1}\ (=\bar{4})$ बहुकता 3 वाला एक मूल है।

E12) (क) मान लीजिए

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ g(x) = \sum_{i=0}^{m} b_i x^i.$$

तब $\phi(f(x)+g(x)) = \phi\left(\sum_{i=0}^{t}(a_i+b_i)\,x^i\right)$, जहाँ $t = \max(m, n)$.

$$= \sum_{i=0}^{t}(a_i+b_i)a^i$$

$$= \sum_{i=0}^{t} a_i a^i + \sum_{i=0}^{t} b_i a^i$$

$$= f(a) + g(a)$$

$$= \phi(f(x)) + \phi(g(x)),\ \text{और}$$

$$\phi(f(x)\,g(x)) = \phi\left(\sum_{i=0}^{m+n}(a_i b_0 + a_{i-1} b_1 + \ldots + a_0 b_i)\,x^i\right)$$

$$= \sum_{i=0}^{m+n}(a_i b_0 + a_{i-1} b_1 + \ldots + a_0 b_i)a^i$$

$$= f(a)\,g(a)$$

$$= \phi(f(x))\,\phi(g(x)).$$

अतः ϕ एक समाकारिता है।

अब कोई अवयव $b \in F$ दिया हुआ हो, तो अचर बहुपद $f(x) = b \in F[x]$ ऐसा है कि $f(a) = b$, अर्थात् $\phi(f(x)) = b$.

अतः ϕ आच्छादक है।

(ख) पिछली दो पंक्तियों में यही दिखाया गया है।

(ग) $f(x) \in \text{Ker}\,\phi$ यदि और केवल यदि $\phi(f(x)) = 0$ यदि और केवल यदि $f(a) = 0$ यदि और केवल यदि $(x-a) \mid f(x)$ यदि और केवल यदि $f(x) \in \langle x-a \rangle$.

अतः $\text{Ker}\,\phi = \langle x-a \rangle$.

अतः समाकारिता के मूल प्रमेय के अनुसार

$F[x]/\langle x-a \rangle \simeq F$.

E13) $(\mathbf{Z}_p^*, .)$ एक समूह है और $o(\mathbf{Z}_p^*, .) = p-1$.

अतः इकाई 4 के E 8 के अनुसार $x^{p-1} = \bar{1}\ \forall\ x \in (\mathbf{Z}_p^*, .)$, अर्थात् $(\mathbf{Z}_p^*, .)$ के $p-1$ अवयवों में से प्रत्येक अवयव $x^{p-1} - \bar{1}$ का एक मूल है। इसलिए $(x-\bar{1}) \ldots\ldots (x-\overline{p-1}) \mid (x^{p-1} - \bar{1})$

क्योंकि $x^{p-1} - \bar{1}$ के Z_p में अधिक से अधिक $p-1$ मूल हो सकते हैं, इसलिए हम पाते हैं कि

$(\mathbf{Z}_p^*, .)$ के $(p-1)$ अवयव ही $x^{p-1} - \bar{1}$ के मूल हैं।

अतः $x^{p-1} - \bar{1} = (x-\bar{1})(x-\bar{2}) \ldots (x-\overline{p-1})$.

E14) $Z_5[x]$ में बहुपद $x^4 + \bar{4}$ और $x^4 - \bar{1}$ समान हैं क्योंकि $\bar{4} = -\bar{1}$. अतः E13 के परिणाम से हम देखते हैं कि $x^4 + \bar{4} = (x-\bar{1})(x-\bar{2})(x-\bar{3})(x-\bar{4})$.

इकाई 14 विशेष पूर्णांकीय प्रांत

इकाई की रूपरेखा

14.1 प्रस्तावना

इस इकाई में हम तीन विशेष प्रकार के पूर्णांकीय प्रांतों पर चर्चा करेंगे। इन प्रांतों का अध्ययन मुख्यतः संख्या सिद्धांत के विकास को नज़र में रखकर किया गया था। आइए, हम इन प्रांतों के बारे में कुछ प्रारंभिक शब्द कहें।

इकाई 13 में आपने देखा कि विभाजन-कलन विधि $F[x]$ पर लागू होती है, जहां F एक क्षेत्र है। इकाई 1 में आपने देखा कि यह विधि Z पर लागू होती है। वास्तव में, ऐसे अनेक प्रांत हैं जिन पर यह कलन विधि लागू होती है। इन पूर्णांकीय प्रांतों को यूक्लिडीय प्रांत कहते हैं। हम भाग 14.2 में इनके गुणों पर चर्चा करेंगे।

अगले भाग में हम ऐसे कुछ प्रांतों पर विचार करेंगे जो बीजीय तौर पर Z से काफ़ी मिलते-जुलते हैं। इन्हें मुख्य गुणजावली प्रांत कहते हैं क्योंकि इनकी प्रत्येक गुणजावली मुख्य होती है।

अंत में, हम उन प्रांतों पर चर्चा करेंगे, जिनके प्रत्येक शून्येतर अव्युत्क्रमणीय अवयव को एक विशेष विधि से अद्वितीयतः गुणनखंडित किया जा सकता है। इन प्रांतों को एक उचित नाम दिया गया है, वह है अद्वितीय गुणनखंडन प्रांत। इन पर चर्चा के दौरान हम आपका परिचय प्रांत के अखंडनीय अवयवों से भी कराएंगे।

इस इकाई को पढ़ने के दौरान आप यूक्लिडीय प्रांत, मुख्य गुणजावली प्रांत और अद्वितीय गुणनखंडन प्रांत के परस्पर संबंध को भी जान जाएंगे।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- जांच कर सकेंगे कि कोई फलन यूक्लिडीय मानांकन है कि नहीं;
- मुख्य गुणजावली प्रांतों को पहचान सकेंगे;
- अद्वितीय गुणनखंडन प्रांतों को पहचान सकेंगे;
- किसी अद्वितीय गुणनखंडन प्रांत के किन्हीं दो अवयवों का gcd प्राप्त कर सकेंगे;
- यूक्लिडीय प्रांत, मुख्य गुणजावली प्रांत और अद्वितीय गुणनखंडन प्रांत के बीच के संबंध को सिद्ध कर सकेंगे और उनका प्रयोग कर सकेंगे।

14.2 यूक्लिडीय प्रांत (Euclidean Domain)

इस पाठ्यक्रम में आपने देखा है कि Z और $F[x]$ एक विभाजन-कलन विधि को संतुष्ट करते हैं। इनके अलावा अनेक प्रांत हैं जिनमें यह गुण है। इस भाग में हम आपको इनसे परिचित कराएंगे और इनके कुछ गुणों पर चर्चा करेंगे। आइए एक परिभाषा से शुरू करें।

परिभाषा : मान लीजिए R एक पूर्णांकीय प्रांत है। हम कहते हैं कि फलन $d : R\setminus\{0\} \to N \cup \{0\}$, R पर **यूक्लिडीय मानांकन** (Euclidean Valuation) है।

यदि निम्नलिखित प्रतिबंध संतुष्ट होते हों :

i) $d(a) \le d(ab) \ \forall\ a, b \in R\setminus\{0\}$, और

ii) किन्हीं $a, b \in R, b \neq 0$ के लिए $\exists\, q, r \in R$

जिनसे कि $a = bq + r$, जहां $r = 0$ या $d(r) < d(b)$.

और तब R **यूक्लिडीय प्रांत** कहलाता है।

इस तरह, यूक्लिडीय प्रांत एक ऐसा प्रांत है जिस पर हम एक यूक्लिडीय मानांकन परिभाषित कर सकते हैं।

आइए, हम एक उदाहरण लें।

उदाहरण 1 : दिखाइए कि **Z** एक यूक्लिडीय प्रांत है।

हल : $d : \mathbf{Z} \to \mathbf{N} \cup \{0\} : d(n) = |n|$

परिभाषित कीजिए।

तब किन्हीं $a, b \in \mathbf{Z} \setminus \{0\}$ के लिए

$d(ab) = |ab| = |a|\,|b| \geq |a| = d(a)$, (क्योंकि $b \neq 0$ के लिए $|b| \geq 1$)

अर्थात् $d(a) \leq d(ab)$.

और, **Z** पर लागू विभाजन-कलन विधि (भाग 1.6.2 देखिए) के अनुसार

यदि $a, b \in \mathbf{Z}, b \neq 0$, तो $\exists\, q, r \in \mathbf{Z}$ जिनसे कि

$a = bq + r$, जहां $r = 0$ या $0 < |r| < |b|$,

अर्थात् $a = bq + r$, जहां $r = 0$ या $d(r) < d(b)$.

अतः d एक यूक्लिडीय मानांकन है और **Z** एक यूक्लिडीय प्रांत है।

अन्य उदाहरणों के लिए नीचे दिए गए प्रश्न हल कीजिए।

E1) मान लीजिए F एक क्षेत्र है। दिखाइए कि $d(a) = 1 \;\forall\, a \in F \setminus \{0\}$ द्वारा परिभाषित यूक्लिडीय मानांकन सहित F एक यूक्लिडीय प्रांत है।

E2) मान लीजिए F एक क्षेत्र है। फलन

$d : F[x] \setminus \{0\} \to \mathbf{N} \cup \{0\} : d(f(x)) = \deg f(x)$

परिभाषित कीजिए। दिखाइए कि d, F[x] पर एक यूक्लिडीय मानांकन है, और इसलिए F[x] एक यूक्लिडीय प्रांत है।

आइए अब हम यूक्लिडीय प्रांतों के कुछ गुणों पर चर्चा करें। पहले गुण का मात्रक (unit) की संकल्पना से संबंध है। अतः आइए हम इस संकल्पना को परिभाषित करें। (ध्यान रखिए कि यह परिभाषा किसी भी पूर्णांकीय प्रांत के लिए सही है।)

परिभाषा : मान लीजिए R एक पूर्णांकीय प्रांत है। अवयव $a \in R$ को R में **मात्रक (या व्युत्क्रमणीय अवयव)** कहते हैं, यदि हम एक ऐसा अवयव $b \in R$ ज्ञात कर सकें जिससे कि $ab = 1$, अर्थात् यदि a का एक गुणनात्मक व्युत्क्रम हो।

उदाहरण के लिए, 1 और –1 दोनों ही **Z** में मात्रक हैं क्योंकि $1 \cdot 1 = 1$ और $(-1)\cdot(-1) = 1$.

ध्यान दीजिए कि प्रांत का तत्समक हमेशा एक मात्रक होता है। परंतु प्रांत के अन्य मात्रक भी हो सकते हैं जैसा कि आपने **Z** के संबंध में ऊपर देखा है।

अब, बताइए कि क्या हम किसी प्रांत के सभी मात्रकों को प्राप्त कर सकते हैं ? आप जानते हैं कि किसी क्षेत्र F का प्रत्येक शून्येतर अवयव व्युत्क्रमणीय होता है। अतः F के मात्रकों का समुच्चय $F \setminus \{0\}$ है। आइए अब हम कुछ अन्य स्थितियों पर भी विचार करें।

उदाहरण 2 : F[x] के सभी मात्रक प्राप्त कीजिए, जहां F एक क्षेत्र है।

हल : मान लीजिए $f(x) \in F[x]$ एक मात्रक है। तब $\exists\, g(x) \in F[x]$ जिससे कि $f(x)\,g(x) = 1$. इसलिए

$\deg(f(x)\,g(x)) = \deg(1) = 0$, अर्थात्

$\deg f(x) + \deg g(x) = 0$.

क्योंकि $\deg f(x)$ और $\deg g(x)$ ऋणेतर पूर्णांक हैं, इसलिए यह समीकरण सिर्फ़ तब सही होगा जब $\deg f(x) = 0 = \deg g(x)$.

अतः f(x) एक शून्येतर अचर, अर्थात् $F \setminus \{0\}$ का अवयव होगा। इस तरह, F[x] के मात्रक F के शून्येतर अवयव हैं। अर्थात् F के मात्रक और F[x] के मात्रक समान हैं।

उदाहरण 3 : $R = \left\{ a + b\sqrt{-5} \mid a, b \in \mathbf{Z} \right\}$ के सभी मात्रक ज्ञात कीजिए।

हल : मान लीजिए $a + b\sqrt{-5}$, R का एक मात्रक है। तब ऐसा $c + d\sqrt{-5} \in R$ है जिससे कि

$(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1.$

$\Rightarrow \quad (ac - 5bd) + (bc + ad)\sqrt{-5} = 1$

$\Rightarrow \quad ac - 5bd = 1$ और $bc + ad = 0$

$\Rightarrow \quad abc - 5b^2 d = b$ और $bc + ad = 0$

$\Rightarrow \quad a(-ad) - 5b^2 d = b$, $bc = -ad$ प्रतिस्थापित करने पर।

$\Rightarrow \quad (a^2 + 5b^2)\, d = -b.$

इसलिए, यदि $b \neq 0$, तो $(a^2 + 5b^2) \mid b$, जो संभव नहीं है।

$\therefore \quad b = 0$

अतः R के मात्रक **Z** के व्युत्क्रमणीय अवयव ही हैं।

हमने नीचे दिए गए E3 में इन अवयवों और अन्य मात्रकों को प्राप्त करने के लिए कहा है।

E3) निम्नलिखित के सभी मात्रक ज्ञात कीजिए :

क) **Z**, ख) $\mathbf{Z}_6$, ग) **Z**/5**Z**.

घ) **Z** + i**Z**.

E4) मान लीजिए R एक पूर्णांकीय प्रांत है। सिद्ध कीजिए कि $u \in R$ एक मात्रक होता है यदि और केवल यदि $Ru = R$.

अब हम युक्लिडीय प्रांत के कुछ सरल गुणों पर चर्चा करने की स्थिति में हैं।

प्रमेय 1 : मान लीजिए कि R युक्लिडीय मानांकन d सहित एक युक्लिडीय प्रांत है। तब, किसी $a \in R \setminus \{0\}$ के लिए $d(a) = d(1)$ यदि और केवल यदि a, R का एक मात्रक हो।

उपपत्ति : आइए पहले हम मान लें कि $a \in R \setminus \{0\}$, जहां $d(a) = d(1)$. R पर विभाजन-कलन विधि के अनुसार, $\exists\, q, r \in R$ जिनसे कि $1 = aq + r$, जहां $r = 0$ या $d(r) < d(a) = d(1)$.

अब, यदि $r \neq 0$, तो $d(r) = d(r \cdot 1) \geq d(1)$.

अतः $d(r) < d(1)$ नहीं हो सकता।

अतः r के लिए संभावना $r = 0$ ही रह जाती है।

इसलिए, $1 = aq$, यानि कि a एक मात्रक है।

विलोमतः, मान लीजिए a, R का एक मात्रक है और $b \in R$ जिससे कि $ab = 1$. तब $d(a) \leq d(ab) = d(1)$. परंतु हम जानते हैं कि $d(a) = d(a \cdot 1) \geq d(1)$. अतः $d(a) = d(1)$.

इस प्रमेय की सहायता से हम उदाहरण 2 को तुरंत हल कर सकते हैं, क्योंकि f(x), F[x] का मात्रक होता है यदि और केवल यदि $\deg f(x) = \deg(1) = 0$.

इसी प्रकार, प्रमेय 1 के अनुसार $n \in \mathbf{Z}$, $\mathbf{Z}$ का मात्रक होता है यदि और केवल यदि $|n| = |1| = 1$.

अतः $\mathbf{Z}$ के मात्रक केवल 1 और (-1) हैं।

आइए अब हम यूक्लिडीय प्रांत की गुणजावलियों पर विचार करें।

प्रमेय 2 : मान लीजिए R यूक्लिडीय मानांकन d सहित एक यूक्लिडीय प्रांत है। तब R की प्रत्येक गुणजावली I, Ra के रूप की होती है, किसी $a \in R$ के लिए।

उपपत्ति : यदि $I = \{0\}$, तो $I = Ra$, जहां $a = 0$. तो आइए हम मान लें कि $I \neq \{0\}$. तब $I \setminus \{0\}$ अरिक्त होगा। समुच्चय $\{d(a) \mid a \in I \setminus \{0\}\}$ लीजिए। सुक्रमण सिद्धांत (भाग 1.6.1 देखिए) के अनुसार इस समुच्चय का एक अल्पिष्ठ अवयव है। मान लीजिए यह $d(b)$ है, जहां $b \in I \setminus \{0\}$. हम दिखाएंगे कि $I = Rb$.

क्योंकि $b \in I$ और I, R की एक गुणजावली है, इसलिए

$Rb \subseteq I$ ....(1)

अब कोई $a \in I$ लीजिए। क्योंकि $I \subseteq R$ और R एक पूर्णांकीय प्रांत है, इसलिए हम ऐसे $q, r \in R$ प्राप्त कर सकते हैं कि

$a = bq + r$, जहां $r = 0$ या $d(r) < d(b)$.

अब $b \in I \to bq \in I$, और $a \in I$. इसलिए $r = a - bq \in I$.

परंतु $r = 0$ या $d(r) < d(b)$. जिस तरह हमने $d(b)$ को चुना है उससे $d(r) < d(b)$ संभव नहीं है। इसलिए $r = 0$. अतः $a = bq \in Rb$. इस तरह,

$I \subseteq Rb$ ....(2)

(1) और (2) से हमें

$$I = Rb$$

प्राप्त होता है।

अतः यूक्लिडीय मानांकन d सहित यूक्लिडीय प्रांत R की प्रत्येक गुणजावली I मुख्य होती है और $a \in I$ से जनित होती है, जहां $d(a)$ समुच्चय $\{d(x) \mid x \in I \setminus \{0\}\}$ का एक अल्पिष्ठ अवयव है।

अतः उदाहरण के लिए, $\mathbf{Z}$ की प्रत्येक गुणजावली मुख्य होती है। इस तथ्य को आप इकाई 10 में सिद्ध कर चुके हैं।

मुख्य गुणजावली Ra को $\langle a \rangle$ से भी प्रकट करते हैं।

अब आप यूक्लिडीय प्रांत की गुणजावलियों से संबंधित निम्नलिखित प्रश्न हल कीजिए।

E5) दिखाइए कि $F[x]$ की प्रत्येक गुणजावली मुख्य होती है, जहां F एक क्षेत्र है।

E6) $\mathbf{Z}$ का उदाहरण लेकर दिखाइए कि समुच्चय

$S = \{a \in R \setminus \{0\} \mid d(a) > d(1)\} \cup \{0\}$

यूक्लिडीय मानांकन d सहित यूक्लिडीय प्रांत R की गुणजावली नहीं है।

अब हम प्रमेय 2 से संबंधित संकल्पना पर चर्चा करेंगे।

14.3 मुख्य गुणजावली प्रांत (Principal Ideal Domain)

पिछले भाग में आपने सिद्ध किया है कि $F[x]$ की प्रत्येक गुणजावली मुख्य होती है, जहां F एक क्षेत्र है। यूक्लिडीय प्रांतों के अतिरिक्त ऐसे अनेक पूर्णांकीय प्रांत होते हैं जिनमें यह गुण होता है। इस प्रकार के वलय को हम एक उपयुक्त नाम देते हैं।

परिभाषा : पूर्णांकीय प्रांत R को हम **मुख्य गुणजावली प्रांत** कहते हैं यदि R की प्रत्येक गुणजावली एक मुख्य गुणजावली हो। ऐसे प्रांत को हम संक्षेप में **PID** कहते हैं, जो कि इसके अंग्रेज़ी नाम principal ideal domain के पहले अक्षर हैं।

अतः Z एक PID है। क्या आप PID के अन्य उदाहरण दे सकते हैं ? वास्तव में प्रमेय 2 के अनुसार सभी यूक्लिडीय प्रांत मुख्य गुणजावली प्रांत होते हैं। लेकिन, इसका विलोम सही नहीं है। अर्थात् प्रत्येक मुख्य गुणजावली प्रांत यूक्लिडीय प्रांत नहीं होता है। उदाहरण के लिए,

$$a + \frac{b}{2}\,(1 + i\sqrt{19}), \text{ जहां } a, b \in \mathbf{Z},$$

के रूप की सभी सम्मिश्र संख्याओं का वलय मुख्य गुणजावली प्रांत होता है, परंतु यह यूक्लिडीय प्रांत नहीं है। इस पाठ्यक्रम के लिए इस तथ्य की उपपत्ति कुछ जटिल है। इसलिए इसकी उपपत्ति हम नहीं दे रहे हैं।

आइए अब हम पूर्णांकीय प्रांत का एक ऐसा उदाहरण लें जो मुख्य गुणजावली प्रांत नहीं है।

उदाहरण 4 : दिखाइए कि $\mathbf{Z}[x]$ एक PID नहीं है।

हल : आप जानते हैं कि $\mathbf{Z}[x]$ एक प्रांत है, क्योंकि $\mathbf{Z}$ एक प्रांत है। हम दिखाएंगे कि इसकी सभी गुणजावलियां मुख्य नहीं हैं। 2 और x से जनित $\mathbf{Z}[x]$ की गुणजावली, अर्थात् $< 2, x >$ लीजिए। हम दिखाना चाहते हैं कि किसी भी $f(x) \in \mathbf{Z}[x]$ के लिए $< 2, x > \neq < f(x) >$.

इसके विपरीत, मान लीजिए $\exists\, f(x) \in \mathbf{Z}[x]$ जिससे कि $< 2, x > = < f(x) >$. स्पष्ट है कि $f(x) \neq 0$. साथ ही $\exists\, g(h), h(x) \in \mathbf{Z}[x]$ जिससे कि $2 = f(x)\, g(x)$ और $x = f(x)\, h(x)$.

इस तरह,

$$\deg f(x) + \deg g(x) = \deg 2 = 0 \qquad \ldots\ldots\ldots(1)$$

और

$$\deg f(x) + \deg h(x) = \deg x = 1 \qquad \ldots\ldots\ldots(2)$$

(1) से पता चलता है कि $\deg f(x) = 0$, अर्थात् $f(x) \in \mathbf{Z}$, मान लीजिए $f(x) = n$. तब (2) से पता चलता है कि $\deg h(x) = 1$. मान लीजिए $h(x) = ax + b$, जहां $a, b \in \mathbf{Z}$.

तब $x = f(x)\, h(x) = n(ax+b)$.

इस समीकरण के दोनो पक्षों के गुणांकों की तुलना करने पर हम पाते हैं कि $na = 1$ और $nb = 0$. अतः n, $\mathbf{Z}$ का एक मात्रक है,

अर्थात् $\quad n = \pm 1$.

इसलिए $\quad 1 \in < f(x) > = < x, 2 >$.

अतः $\quad 1 = x\,(a_0 + a_1 x + \ldots\ldots + a_r x^r) + 2\,(b_0 + b_1 x + \ldots\ldots + b_s x^s)$,

जहां $\quad a_i, b_j \in \mathbf{Z}\ \forall\ i = 0, 1, \ldots\ldots, r$ और $j = 0, 1, \ldots\ldots, s$.

दोनों पक्षों के अचर पदों की तुलना करने पर हम पाते हैं कि $1 = 2b_0$, परंतु यह सत्य नहीं हो सकता, क्योंकि Z में 2 व्युत्क्रमणीय नहीं है।

इसलिए $< x, 2 >$ मुख्य गुणजावली नहीं है।

अतः $\mathbf{Z}[x]$ मुख्य गुणजावली प्रांत नहीं है।

अब आप नीचे दिए गए प्रश्न हल कीजिए।

E7) दिखाइए कि यह आवश्यक नहीं है कि किसी PID का उपवलय भी PID हो।

E8) क्या किसी PID का विभाग वलय PID होगा ? क्यों ? ध्यान रखिए कि PID एक पूर्णांकीय प्रांत होता है।

अब हम मुख्य गुणजावली प्रांतों में विभाज्यता के कुछ गुणों पर चर्चा करेंगे। आपको इकाई 12 से याद होगा कि यदि R एक वलय हो और $a, b \in R$, जहां $a \neq 0$ तो a, b को **विभाजित** करता है यदि एक ऐसा $c \in R$ है जिससे कि $b = ac$.

अब हम Z के संदर्भ में इकाई 1 में दिए गए कुछ शब्दों की परिभाषा को व्यापक रूप देना चाहेंगे।

परिभाषा : यदि वलय R के दो अवयव a और b दिए हुए हों, तो हम $c \in R$ को a और b का **सार्व भाजक** (common divisor) कहते हैं यदि $c \mid a$ और $c \mid b$.

अवयव $d \in R$ को $a, b \in R$ का **महत्तम सार्व भाजक** (greatest common divisor संक्षेप में gcd) कहते हैं यदि

i) $d \mid a$ और $d \mid b$, और

ii) a और b के किसी सार्व भाजक c के लिए $c \mid d$. उदाहरण के लिए, Z में 5 और 15 का gcd 5 है और 5 और 7 का gcd 1 है।

हम आपको दिखाएंगे कि यदि दो अवयवों का gcd हो तो यह मात्रकों तक अद्वितीय होता है, अर्थात् यदि d और d′, a और b के दो gcd हों, तो किसी मात्रक u के लिए $d = ud'$. इसको सिद्ध करने के लिए हमें एक परिणाम की आवश्यकता है जिसे आप नीचे दिए गए प्रश्न में हल कर सकते हैं।

प्रांत के दो अवयव **सहचारी** कहलाते हैं यदि R के किसी मात्रक u के लिए $a = bu$.

E9) मान लीजिए R एक पूर्णांकीय प्रांत है। दिखाइए कि

(क) R में u एक मात्रक होता है यदि और केवल यदि $u \mid 1$.

(ख) किन्हीं $a, b \in R$ के लिए $a \mid b$ और $b \mid a$ यदि और केवल यदि R में a और b सहचारी हों।

आइए अब हम निम्नलिखित परिणाम को सिद्ध करें।

प्रमेय 3 : मान लीजिए R एक पूर्णांकीय प्रांत है और $a, b \in R$. यदि a और b के gcd का अस्तित्व हो तो यह मात्रकों तक अद्वितीय होता है।

उपपत्ति : मान लीजिए a और b के दो gcd, d और d′ हैं। क्योंकि d एक सार्व भाजक है और d′ एक gcd है, इसलिए $d \mid d'$. इसी प्रकार हमें $d' \mid d$ प्राप्त होता है। अतः E9 से हम पाते हैं कि R में d और d′ सहचारी हैं। इसलिए a और b का gcd मात्रकों तक अद्वितीय है।

हम a और b के gcd को (a, b) से प्रकट करते हैं। (यूं तो इस संकेतन का प्रयोग $R \times R$ के अवयवों के लिए भी किया जाता है। परंतु भ्रम में पड़ने का कोई कारण नहीं है, क्योंकि संदर्भ से ही स्पष्ट हो जाएगा कि इस संकेतन का प्रयोग किसके लिए किया जा रहा है।)

अब बताइए कि हम दो अवयवों का gcd कैसे प्राप्त कर सकते हैं ? हमने इसे Z में कैसे प्राप्त किया था ? हमने दोनों अवयवों के सार्व गुणनखंड प्राप्त किए थे और उनका गुणनफल ही उनका gcd था। हम इसी विधि को नीचे दिए उदाहरण में लागू करेंगे।

उदाहरण 5 : Q[x] में $p(x) = x^2 + 3x - 10$ और $q(x) = 6x^2 - 10x - 4$ का gcd ज्ञात कीजिए।

हल : द्विघाती सूत्र से हम जानते हैं कि p(x) के मूल 2 और −5 हैं और q(x) के मूल 2 और −1/3 हैं। इसलिए $p(x) = (x - 2)(x + 5)$ और $q(x) = 2(x - 2)(3x + 1)$.

p(x) और q(x) का gcd, p(x) और q(x) के सार्व गुणनखंडों का गुणनफल होता है, अर्थात् $(x - 2)$.

अब आप इस प्रश्न को हल कीजिए।

E10) निम्नलिखित के gcd ज्ञात कीजिए

क) $Z/\langle 8 \rangle$ में $\bar{2}$ और $\bar{6}$.

ख) Z[x] में $x^2 + 8x + 15$ और $x^2 + 12x + 35$.

ग) Q[x] में $x^3 - 2x^2 + 6x - 5$ और $x^2 - 2x + 1$.

आइए अब हम किसी मुख्य गुणजावली प्रांत के अवयवों के gcd पर विचार करें।

प्रमेय 4 : मान लीजिए R एक मुख्य गुणजावली प्रांत है और $a, b \in R$. तब (a, b) का अस्तित्व होता है और किन्हीं $x, y \in R$ के लिए यह $ax + by$ के रूप का होता है।

उपपत्ति : गुणजावली $< a, b >$, लीजिए। क्योंकि R एक PID है, इसलिए यह गुणजावली भी मुख्य होगी। मान लीजिए $d \in R$ ऐसा है कि $< a, b > = < d >$. हम दिखाएंगे कि a और b का gcd, d है।

क्योंकि $a \in < d >$, इसलिए $d \mid a$. इसी प्रकार, $d \mid b$. अब मान लीजिए $c \in R$ ऐसा है कि $c \mid a$ और $c \mid b$. क्योंकि $d \in < a, b >$, इसलिए $\exists\ x, y \in R$ जिससे कि $d = ax + by$. क्योंकि $c \mid a$, और $c \mid b$, इसलिए $c \mid (ax + by)$, अर्थात् $c \mid d$.

इस तरह हमने दिखाया है कि $d = (a, b)$ और किन्हीं $x, y \in R$ के लिए $d = ax + by$.

इस तथ्य से कि F[x] एक PID है, हमें प्रमेय 4 का निम्नलिखित उपप्रमेय प्राप्त होता है।

उपप्रमेय : मान लीजिए F एक क्षेत्र है। तब F[x] के किन्हीं दो बहुपदों $f(x)$ और $g(x)$ का एक gcd होता है जो कि किन्हीं $a(x), b(x) \in F[x]$ के लिए $a(x) f(x) + b(x) g(x)$ के रूप का होता है।

उदाहरण के लिए, E10 (c) में

$$x - 1 = \frac{1}{5}(x^3 - 2x^2 + 6x - 5) + \left(\frac{-x}{5}\right)(x^2 - 2x + 1).$$

अब आप प्रमेय 4 की सहायता से किसी PID के **सापेक्षतः अभाज्य** (relatively prime) अवयवों, अर्थात् ऐसे अवयव-युग्म जिनका gcd, 1 है, से संबंधित निम्नलिखित प्रश्न को सिद्ध कर सकते हैं।

E11) मान लीजिए R एक PID है और $a, b, c \in R$ ऐसे हैं कि $a \mid bc$. दिखाइए कि यदि $(a, b) = 1$, तो $a \mid c$.

(संकेत : प्रमेय 4 के अनुसार $\exists\ x, y \in R$ जिससे कि $ax + by = 1$)

आइए अब हम प्रांत के अभाज्य अवयवों (भाग 12.4 देखिए) से संबंधित एक संकल्पना पर चर्चा करें।

परिभाषा : मान लीजिए R एक पूर्णांकीय प्रांत है। हम अवयव $x \in R$ को अखंडनीय (irreducible) कहते हैं यदि

i) x एक मात्रक नहीं हो, और

ii) यदि $x = ab$, जहां $a, b \in R$, तो या a मात्रक होगा या b मात्रक होगा।

इस तरह, कोई अवयव अखंडनीय होता है यदि इसे अतुच्छ तरीके से गुणनखंडित नहीं किया जा सकता हो, अर्थात् इसके गुणनखंड केवल इसके सहचारी और वलय के मात्रक हों।

अतः उदाहरण के लिए, **Z** के अखंडनीय अवयव अभाज्य संख्याएं और उनके सहचारी होते हैं। इससे यह अर्थ निकलता है कि **Z** का कोई अवयव अभाज्य होता है यदि और केवल यदि वह अखंडनीय हो।

किसी क्षेत्र F के लिए, F[x] एक प्रांत है जिसमें हमें अनेक उदाहरण प्राप्त हो सकते हैं। आइए हम **R** [x] और **C** [x] के अखंडनीय अवयवों, अर्थात् **R** और **C** पर अखंडनीय बहुपदों पर गौर करें। **C** [x] के बहुपदों के बारे में इस महत्वपूर्ण प्रमेय पर विचार कीजिए। हम इस प्रमेय का ज़िक्र रैखिक बीजगणित के पाठ्यक्रम में कर चुके हैं।

प्रमेय 5 (बीजगणित का मूल प्रमेय) : **C**[x] के किसी बहुपद का, जो अचर न हो, **C** में एक मूल होता है। (वास्तव में, इसके सभी मूल **C** में होते हैं।)

क्या इससे हमें **C** पर अखंडनीय बहुपदों के बारे में कुछ पता चलता है ? हाँ। बल्कि हम इस परिणाम को निम्न प्रकार से भी व्यक्त कर सकते हैं।

प्रमेय 5′ : कोई बहुपद **C**[x] में अखंडनीय होता है यदि और केवल यदि वह रैखिक हो।

इस परिणाम का एक उपप्रमेय है :

प्रमेय 6 : $\mathbf{R}[x]$ के किसी भी अखंडनीय बहुपद का घात 1 या 2 होता है।

यहां हम इन परिणामों को सिद्ध नहीं करेंगे, परंतु **R** या **C** पर बहुपदों की चर्चा करने के दौरान हम इनका प्रयोग कई बार करेंगे। आप इनकी सहायता से निम्नलिखित प्रश्न हल कर सकते हैं।

E12) निम्नलिखित बहुपदों में से कौन से बहुपद अखंडनीय हैं ? अपने उत्तर का कारण बताइए।

(क) $x^2 - 2x + 1 \in \mathbf{R}[x]$

(ख) $x^2 + x + 1 \in \mathbf{C}[x]$,

(ग) $x - i \in \mathbf{C}[x]$

(घ) $x^3 - 3x^2 + 2x + 5 \in \mathbf{R}[x]$.

आइए अब हम PID में अभाज्य अवयवों और अखंडनीय अवयवों के बीच के संबंध पर चर्चा करें।

प्रमेय 7 : किसी मुख्य गुणजावली प्रांत में एक अवयव अभाज्य होता है यदि और केवल यदि वह अखंडनीय हो।

उपपत्ति : मान लीजिए R एक PID है और $x \in R$ अखंडनीय है। मान लीजिए $x \mid ab$, जहां $a, b \in R$ और $x \nmid a$. तब $(x, a) = 1$, क्योंकि मात्रकों तक x का गुणनखंड सिर्फ़ x ही होगा। इस तरह, E11 के अनुसार, $x \mid b$. अतः x अभाज्य है।

इसका विलोम सिद्ध करने के लिए निम्नलिखित प्रश्न हल कीजिए।

E13) मान लीजिए R एक प्रांत है और $p \in R$ एक अभाज्य अवयव है। दिखाइए कि p अखंडनीय है।

(**संकेत:** मान लीजिए $p = ab$. तब, $p \mid ab$. यदि $p \mid a$, तो दिखाइए कि b एक मात्रक होगा।)

अब बताइए कि हम क्यों कहते हैं कि प्रमेय 7 केवल PID के लिए सत्य है ? E13 से आप देख सकते हैं कि एक तरफ़ा कथन किसी भी प्रांत के लिए सत्य है। क्या किसी भी प्रांत के लिए विलोम सत्य है ? अर्थात् क्या किसी प्रांत का प्रत्येक अखंडनीय अवयव अभाज्य होता है ? इस प्रश्न का उत्तर आपको उदाहरण 6 में मिलेगा। अभी हम प्रमेय 7 के कुछ उपयोगों पर विचार करेंगे।

प्रमेय 7 की सहायता से हम F[x] के अभाज्य अवयवों के अनेक उदाहरण दे सकते हैं। उदाहरण के लिए, F पर कोई भी रैखिक अवयव अखंडनीय होता है, अतः यह अभाज्य होता है। अगली इकाई में हम Q[x] पर अखंडनीयता (और अभाज्यता) पर विशेष रूप से विचार करेंगे।

अब हम PID के अभाज्य अवयवों के लिए इकाई 1 के प्रमेय 10 के अनुरूप एक परिणाम को सिद्ध करेंगे। इसके लिए पहले हम किसी PID की गुणजावलियों के एक अति रोचक गुण को सिद्ध करेंगे। इस गुण को **आरोही शृंखला प्रतिबंध** (ascending chain condition) कहते हैं। इसके अनुसार, मुख्य गुणजावली प्रांत में गुणजावलियों की कोई भी वर्धमान शृंखला कुछ चरणों के बाद अवश्य रुक जाएगी।

प्रमेय 8 : मान लीजिए R एक मुख्य गुणजावली प्रांत है और $I_1, I_2, \ldots\ldots$ R की गुणजावलियों का एक अनंत अनुक्रम है जो

$I_1 \subseteq I_2 \subseteq \ldots..$

को संतुष्ट करता है।

तब किसी $m \in N$ के लिए $I_m = I_{m+1} = I_{m+2} = \ldots\ldots$

उपपत्ति : समुच्चय $I = I_1 \cup I_2 \cup \ldots.. = \bigcup_{n=1}^{\infty} I_n$ लीजिए। हम सिद्ध करेंगे कि I, R की एक गुणजावली है। सबसे पहले, $I \neq \phi$, क्योंकि $I_1 \neq \phi$ और $I_1 \subseteq I$. इसके बाद, यदि $a, b \in I$, तो किन्हीं $r, s \in N$ के

लिए $a \in I_r$ और $b \in I_s$. मान लीजिए $r \geq s$. तब $I_s \subseteq I_r$. इसलिए $a, b \in I_r$. क्योंकि I_r, R की एक गुणजावली है, इसलिए $a - b \in I_r \subseteq I$. इस तरह, $a - b \in I \; \forall \; a, b \in I$.

अंत में, मान लीजिए $x \in R$ और $a \in I$. तब किसी $r \in \mathbf{N}$ के लिए $a \in I_r$.

$\therefore$ $xa \in I_r \subseteq I$. अतः जब भी $x \in R$ और $a \in I$, तब $xa \in I$.

इसलिए I, R की एक गुणजावली है। क्योंकि R मुख्य गुणजावली प्रांत है, इसलिए किसी $a \in R$ के लिए $I = <a>$ क्योंकि $a \in I$, इसलिए किसी $m \in \mathbf{N}$ के लिए $a \in I_m$.

तब, $I \subseteq I_m$. परंतु $I_m \subseteq I$. अतः $I = I_m$. अब, क्योंकि $I_m \subseteq I_{m+1} \subseteq I = I_m$, इसलिए $I_m = I_{m+1}$.

इसी प्रकार, $I_m = I_{m+2}$ आदि-आदि।

इस तरह, $I_m = I_{m+1} = I_{m+2} = \ldots\ldots\ldots\ldots\ldots$

अब एक क्षण के लिए आइए हम भाग 12.4 पर लौट चलें, जहां हमने अभाज्य गुणजावलियों के बारे में चर्चा की है। वहां हमने बताया है कि अवयव $p \in R$ अभाज्य होता है यदि और केवल यदि $< p >$, R की एक अभाज्य गुणजावली हो। यदि R मुख्य गुणजावली प्रांत है तो प्रमेय 7 की सहायता से हम एक और प्रबल कथन दे सकते हैं।

प्रमेय 9 : मान लीजिए R मुख्य गुणजावली प्रांत है। गुणजावली $< a >$, R की उच्चिष्ठ गुणजावली होती है यदि और केवल यदि a, R का एक अभाज्य अवयव है।

उपपत्ति : यदि $< a >$, R की एक उच्चिष्ठ गुणजावली है, तो यह R की अभाज्य गुणजावली होगी। इसलिए a, R का एक अभाज्य अवयव होगा।

विलोमतः, मान लीजिए a अभाज्य है और I, R की एक गुणजावली है जिससे कि $< a > \subsetneq I$. क्योंकि R, PID है, इसलिए किसी $b \in R$ के लिए $I = < b >$. अब हम दिखाएंगे कि b, R में एक मात्रक है; और तब E4 के अनुसार, $< b > = R$, अर्थात् $I = R$.

अब, $< a > \subsetneq < b > \Rightarrow a = bc$, किसी $c \in R$ के लिए। क्योंकि a अखंडनीय है, इसलिए b, a का सहचारी होगा या b, R में एक मात्रक होगा। परंतु यदि b, a का सहचारी हो, तो $< b > = < a >$, जो एक अंतर्विरोध है। अतः b, R में एक मात्रक होगा। इसलिए $I = R$.

अतः $< a >$, R की एक उच्चिष्ठ गुणजावली है।

प्रमेय 9 के अनुसार **मुख्य गुणजावली प्रांत की अभाज्य गुणजावलियां और उच्चिष्ठ गुणजावलियां संपाती होती हैं।**

अब आप नीचे दिया गया प्रश्न हल कीजिए।

E14) निम्नलिखित गुणजावलियों में से कौन सी उच्चिष्ठ हैं ? अपने उत्तर का कारण बताइए।

(क) Z में $< 5 >$

(ख) $Q[x]$ में $< x^2-1 >$

(ग) $R[x]$ में $< x^2+x+1 >$

(घ) $Z[x]$ में $< x >$.

अब एक पूर्णांक n लीजिए। तब $n = 0$ या $n = \pm 1$ या n का एक अभाज्य गुणनखंड होगा। पूर्णांकों का यह गुण किसी भी मुख्य गुणजावली प्रांत के अवयवों के लिए सही है, जैसा कि आप अभी देखेंगे।

प्रमेय 10 : मान लीजिए R एक मुख्य गुणजावली प्रांत है और a, R का एक शून्येतर अव्युत्क्रमणीय अवयव है। तब R में एक ऐसा अभाज्य अवयव p होता है जिससे कि $p \mid a$.

उपपत्ति : यदि a अभाज्य है, तो $p = a$ लीजिए। वरना हम $a = a_1 b_1$ लिख सकते हैं जहां न तो a_1 और न ही b_1, a के सहचारी हैं। तब $< a > \subsetneq < a_1 >$. यदि a_1 अभाज्य है तो $p = a_1$ लीजिए। वरना हम $a_1 = a_2 b_2$ लिख सकते हैं, जहां न तो a_2 और न ही b_2, a_1 के सहचारी हैं। तब $< a_1 > \subsetneq < a_2 >$.

इस प्रक्रिया को जारी रखने पर हमें एक वर्धमान शृंखला $<a> \subsetneq <a_1> \subsetneq <a_2> \subsetneq \ldots\ldots\ldots$ प्राप्त होती है।

प्रमेय 8 के अनुसार, यह शृंखला किसी $<a_n>$ पर रुक जाती है। तब a_n अभाज्य होगा, क्योंकि इसके कोई भी अतुच्छ गुणनखंड नहीं होंगे। $p = a_n$ लेने पर प्रमेय सिद्ध हो जाता है।

और अब हम सिद्ध कर सकते हैं कि मुख्य गुणजावली प्रांत के किसी शून्येतर अव्युत्क्रमणीय अवयव को अभाज्य अवयवों (अर्थात् अखंडनीय अवयवों) के परिमित गुणनफल के रूप में अद्वितीयतः लिखा जा सकता है।

प्रमेय 11 : मान लीजिए R एक मुख्य गुणजावली प्रांत है। मान लीजिए $a \in R$ ऐसा है कि $a \neq 0$ और a एक मात्रक नहीं है। तब $a = p_1 p_2 \ldots\ldots p_r$, जहां $p_1, p_2, \ldots, p_r$, R के अभाज्य अवयव हैं।

उपपत्ति : यदि a अभाज्य अवयव है, तो सिद्ध करने के लिए कुछ नहीं रह जाता है। यदि यह अभाज्य अवयव नहीं है तो प्रमेय 10 के अनुसार R के किसी अभाज्य p_1 के लिए $p_1 | a$. मान लीजिए $a = p_1 \ a_1$. यदि a_1 अभाज्य है, तो कुछ करना शेष नहीं रहता। वरना R के किसी अभाज्य p_2 के लिए $p_2 | a_1$. मान लीजिए $a_1 = p_2 a_2$. तब $a = p_1 p_2 a_2$. यदि a_2 अभाज्य है, तो कुछ करना शेष नहीं रहता। वरना हम प्रक्रिया को जारी रखते हैं। ध्यान दीजिए कि क्योंकि a_1, a का एक अतुच्छ गुणनखंड है, इसलिए $<a> \subsetneq <a_1>$. इसी प्रकार, $<a_1> \subsetneq <a_2>$. अतः प्रक्रिया को जारी रखने पर हमें मुख्य गुणजावली प्रांत R में गुणजावलियों की एक वर्धमान शृंखला $<a> \subsetneq <a_1> \subsetneq <a_2> \subsetneq \ldots\ldots$ प्राप्त होती है। प्रमेय 10 की उपपत्ति की तरह यह शृंखला किसी $m \in \mathbf{N}$ के लिए $<a_m>$ पर समाप्त होती है और a_m अखंडनीय होता है। अतः m चरणों के बाद प्रक्रिया समाप्त हो जाती है, अर्थात् हम $a = p_1 p_2 \ldots\ldots p_m$ लिख सकते हैं, जहां p_i, R का अभाज्य अवयव है $\forall \ i=1,\ldots, m$.

इस तरह, मुख्य गुणजावली प्रांत के किसी भी शून्येतर अव्युत्क्रमणीय अवयव को अभाज्य अवयवों के गुणनफल में गुणनखंडित किया जा सकता है। इस गुणनखंडन की विशेषता निम्नलिखित परिणाम में दी गई है, जिसे आप इकाई 1 में **Z** के लिए सिद्ध कर चुके हैं।

प्रमेय 12 : मान लीजिए R एक मुख्य गुणजावली प्रांत है और $a \neq 0$, R में अव्युत्क्रमणीय है। मान लीजिए $a = p_1 \ p_2 \ldots\ldots p_n = q_1 \ q_2 \ldots\ldots q_m$, जहां p_i और q_j, R के अभाज्य अवयव हैं। तब $n=m$ और $1 \leq i \leq n$, $1 \leq j \leq m$ के लिए प्रत्येक p_i किसी न किसी q_j का सहचारी होता है।

इस परिणाम की उपपत्ति देने से पहले हम आपको अभाज्य अवयवों का एक गुण सिद्ध करने के लिए दे रहे हैं। इसकी आवश्यकता उपपत्ति में पड़ेगी।

E15) n पर आगमन नियम लागू करके सिद्ध कीजिए कि यदि पूर्णांकीय प्रांत R में p एक अभाज्य अवयव हो और यदि $p \mid a_1 \ a_2 \ldots\ldots a_n$ (जहां $a_1, a_2, \ldots, a_n \in R$), तो किसी $i = 1, 2, \ldots, n$ के लिए $p \mid a_i$.

आइए, अब हम प्रमेय 12 को सिद्ध करें।

उपपत्ति : क्योंकि $p_1 \ p_2 \ldots\ldots p_n = q_1 \ q_2 \ldots\ldots q_m$, इसलिए $p_1 \mid q_1 q_2 \ldots\ldots q_m$. अतः E15 के अनुसार, किसी $j=1, 2, \ldots, m$ के लिए $p_1 \mid q_j$. यदि आवश्यक हो, तो q_j के क्रम में परिवर्तन करके हम मान सकते हैं कि $j=1$, अर्थात् $p_1 \mid q_1$. मान लीजिए $q_1 = p_1 \ u_1$. क्योंकि q_1 अखंडनीय है, इसलिए u_1, R में एक मात्रक अवश्य होगा। अतः p_1 और q_1 सहचारी हैं। अब,

$p_1 \ p_2 \ldots\ldots p_n = (p_1 \ u_1)q_2 \ldots\ldots q_m$.

दोनों ओर p_1 का निरसन करने पर हमें

$p_2 \ p_3 \ldots\ldots p_n = u_1 \ q_2 q_3 \ldots\ldots q_m$

प्राप्त होता है।

अब, यदि $m > n$, तो हम p_2, p_3, आदि पर इसी प्रक्रिया को लागू कर सकते हैं। तब, n चरणों के बाद हमें $1 = u_1 u_2 \ldots u_n q_{n+1} \ldots q_m$ प्राप्त होगा। इससे पता चलता है कि q_{n+1} एक मात्रक है। परंतु यह इस बात का अंतर्विरोध करता है कि q_{n+1} अखंडनीय है।

इस तरह, $m \le n$.

p और q की भूमिकाओं में अदला-बदली करने और ऊपर की तरह तर्क देने पर हमें $n \le m$ प्राप्त होता है।

अतः $n=m$.

उपपत्ति में हमने यह भी दिखाया है कि प्रत्येक p_i किसी q_j का और प्रत्येक q_j किसी p_i का सहचारी होता है ।

प्रमेय 12 के अनुसार, **मुख्य गुणजावली प्रांत में किसी अवयव के कोई दो अभाज्य गुणनखंडन अभिन्न होते हैं, गुणनखंड के लिखने के क्रम के अलावा और गुणनखंडों के स्थान पर उनके सहचारियों को प्रतिस्थापित करने के अलावा।**

अतः प्रमेय 11 और प्रमेय 12 के अनुसार, मुख्य गुणजावली प्रांत के प्रत्येक शून्येतर अवयव को, जो एक मात्रक नहीं है, परिमित संख्या में लिए गए अभाज्य अवयवों के गुणनफल के रूप में (सहचारियों तक) अद्वितीयतः व्यक्त किया जा सकता है।

उदाहरण के लिए, $x^2-1 \in \mathbf{R}[x]$ को $\mathbf{R}[x]$ में $(x-1)(x+1)$ या $(x+1)(x-1)$ या $[\frac{1}{2}(x+1)]\ [2(x-1)]$ लिख सकते हैं।

अब आप नीचे दिए गए प्रश्न को हल कीजिए।

E16) $\mathbf{Q}[x]$ और $\mathbf{Z}_2[x]$ में $2x^2 - 3x + 1$ का अभाज्य गुणनखंडन बताइए।

जिस गुण को हमने प्रमेय 11 और प्रमेय 12 में PID के लिए सिद्ध किया है, वह अन्य अनेक प्रांतों के लिए भी सत्य होता है। आइए अब हम इन वलयों पर चर्चा करें।

14.4 अद्वितीय गुणनखंडन प्रांत (Unique Factorisation Domain)

इस भाग में हम प्रांतों के एक ऐसे वर्ग पर कुछ विस्तार से चर्चा करेंगे जिसमें मुख्य गुणजावली प्रांत भी शामिल है।

परिभाषा : हम पूर्णांकीय प्रांत R को **अद्वितीय गुणनखंडन प्रांत** कहते हैं यदि R के प्रत्येक शून्येतर अवयव को, जो R में मात्रक नहीं है, परिमित संख्या में लिए गए R के अखंडनीय अवयवों के गुणनफल के रूप में अद्वितीयतः व्यक्त किया जा सकता है। ऐसे प्रांत को हम संक्षेप में UFD कहते हैं, जो कि इसके अंग्रेज़ी नाम unique factorisation domain के पहले अक्षर हैं।

इस तरह, यदि R एक अद्वितीय गुणनखंडन प्रांत हो और $a \in R$, जहां $a \neq 0$ और a अव्युत्क्रमणीय हो, तो

i) a को परिमित संख्या में लिए गए अखंडनीय अवयवों के गुणनफल के रूप में लिखा जा सकता है, और

ii) यदि $a = p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m$ अखंडनीय अवयवों में a के दो गुणनखंडन हों, तो $n=m$ और प्रत्येक p_i किसी q_j का सहचारी होता है, जहां $1 \le i \le n$, $1 \le j \le m$.

क्या आप UFD का एक उदाहरण दे सकते हैं ? प्रमेय 11 और प्रमेय 12 से आपको कोई सहायता मिलती है ? निश्चय ही। इन प्रमेयों में हमने सिद्ध किया है कि **प्रत्येक मुख्य गुणजावली प्रांत एक अद्वितीय गुणनखंडन प्रांत होता है।**

प्रत्येक यूक्लिडीय प्रांत एक अद्वितीय गुणनखंडन प्रांत होता है।

अतः किसी क्षेत्र F के लिए F[x] एक अद्वितीय गुणनखंडन प्रांत होता है। और क्योंकि कोई भी यूक्लिडीय प्रांत एक PID होता है, इसलिए यह UFD भी होता है। इकाई 1 में आपने सीधा ही सिद्ध किया था कि $\mathbf{Z}$ एक UFD है। क्यों न आप वहां दी गई उपपत्ति को फिर से पढ़ लें और नीचे दिए गए प्रश्नों को हल करें।

E17) सीधा सिद्ध कीजिए कि किसी क्षेत्र F के लिए F[x] एक अद्वितीय गुणनखंडन प्रांत है।

(**संकेत :** मान लीजिए आप f(x) का गुणनखंडन करना चाहते हैं। तब आप deg f(x) पर आगमन नियम लागू कीजिए।)

E18) **Z** में 10 के दो अलग-अलग अभाज्य गुणनखंडन दीजिए।

तो आपने UFD के अनेक उदाहरण देख लिए हैं। अब हम एक ऐसे प्रांत का उदाहरण देंगे जो अद्वितीय गुणनखंडन प्रांत नहीं है (और इस तरह, न तो वह PID है और न ही यूक्लिडीय प्रांत)।

उदाहरण 6 : दिखाइए कि $\mathbf{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$ एक अद्वितीय गुणनखंडन प्रांत नहीं है।

हल : आइए हम फलन

$f : \mathbf{Z}[\sqrt{-5}] \to \mathbf{N} \cup \{0\}$

को $f(a+b\sqrt{-5}) = a^2 + 5b^2$

से परिभाषित करें। यह फलन **मानक फलन** (norm function) है और इसे प्रायः N से प्रकट किया जाता है।

आप सत्यापित कर सकते हैं कि

$f(\alpha\beta) = f(\alpha) f(\beta) \ \forall \ \alpha, \beta \in \mathbf{Z}[\sqrt{-5}]$

अब, $\mathbf{Z}[\sqrt{-5}]$ में 9 के दो गुणनखंडन हैं, अर्थात् $9 = 3.3 = (2+\sqrt{-5})(2-\sqrt{-5})$

उदाहरण 3 में आप दिखा चुके हैं कि $\mathbf{Z}[\sqrt{-5}]$ के मात्रक केवल 1 और –1 हैं। अतः 3, $2+\sqrt{-5}$ और $2-\sqrt{-5}$ में से कोई भी दो एक-दूसरे के सहचारी नहीं हैं।

और इनमें से प्रत्येक अखंडनीय है। क्योंकि, यदि इनमें से एक, मान लीजिए $2+\sqrt{-5}$, खंडनीय (reducible) है, तब किसी अव्युत्क्रमणीय $\alpha, \beta \in \mathbf{Z}[\sqrt{-5}]$ के लिए $2+\sqrt{-5} = \alpha\beta$. फलन f को लागू करने पर हम पाते हैं कि

$f(2+\sqrt{-5}) = f(\alpha) f(\beta)$,

अर्थात् $9 = f(\alpha) f(\beta)$.

क्योंकि $f(\alpha), f(\beta) \in \mathbf{N}$ और α, β मात्रक नहीं हैं, इसलिए केवल यही संभावना रह जाती है कि $f(\alpha) = 3 = f(\beta)$.

इसलिए यदि $\alpha = a + b\sqrt{-5}$, तो $a^2 + 5b^2 = 3$. लेकिन, यदि $b \neq 0$, तो $a^2 + 5b^2 \geq 5$; और यदि $b = 0$, तो **Z** में $a^2=3$, जो संभव नहीं है। इस तरह हमें एक अंतर्विरोध प्राप्त होता है। अतः हमारा यह मानकर चलना कि $2+\sqrt{-5}$ खंडनीय है, गलत है। अर्थात् $2+\sqrt{-5}$ अखंडनीय है।

इसी प्रकार, हम दिखा सकते हैं कि 3 और $2-\sqrt{-5}$ अखंडनीय हैं। अतः अखंडनीय अवयवों के गुणनफल के रूप में 9 का गुणनखंडन अद्वितीय नहीं है। इसलिए, $\mathbf{Z}[\sqrt{-5}]$ एक अद्वितीय गुणनखंडन प्रांत नहीं है।

इस उदाहरण से आप यह भी देख सकते हैं कि अखंडनीय अवयव का अभाज्य अवयव होना आवश्यक नहीं है। उदाहरण के लिए, $2+\sqrt{-5}$ अखंडनीय है और $2+\sqrt{-5} \mid 3.3$, परंतु $2+\sqrt{-5} \nmid 3$. अतः $2+\sqrt{-5}$ एक अभाज्य अवयव नहीं है।

अब एक प्रश्न।

E19) $\mathbf{Z}[\sqrt{-5}]$ में अखंडनीय अवयवों के गुणनफल के रूप में 6 के अलग-अलग गुणनखंडन दीजिए।

आइए अब हम UFD के कुछ गुणों पर चर्चा करें। पहला गुण है कि किसी UFD के किन्हीं दो अवयवों का एक gcd होता है; और उनका gcd उनके सभी सार्व गुणनखंडों का गुणनफल होता है। यहां हम इस तथ्य का प्रयोग करेंगे कि अद्वितीय गुणनखंडन प्रांत R के किसी भी अवयव a को

$$a = p_1^{r_1}\ p_2^{r_2}\ \ldots\ p_n^{r_n}$$

के रूप में लिखा जा सकता है, जहां p_i, R के अलग-अलग अखंडनीय अवयव हैं। उदाहरण के लिए, Z[x] में

$x^3 - x^2 - x + 1 = (x-1)(x+1)(x-1) = (x-1)^2 (x+1)$.

तो आइए हम निम्नलिखित परिणाम को सिद्ध करें।

प्रमेय 13 : अद्वितीय गुणनखंडन प्रांत के किन्हीं भी दो अवयवों का एक gcd होता है।

उपपत्ति : मान लीजिए R एक अद्वितीय गुणनखंडन प्रांत है और $a, b \in R$. मान लीजिए

$a = p_1^{r_1}\ p_2^{r_2}\ \ldots\ p_n^{r_n}$ और $b = p_1^{s_1}\ p_2^{s_2}\ \ldots\ p_n^{s_n}$, जहां $p_1, p_2, \ldots, p_n$, R के अलग-अलग

अखंडनीय अवयव हैं और $\forall\ i = 1, 2, \ldots, n$ के लिए r_i और s_i ऋणेतर पूर्णांक हैं। (यदि कोई p_i, a के गुणनखंडन में नहीं आता हो, तो उनका संगत $r_i = 0$. इसी प्रकार यदि कोई p_i, b का गुणनखंडन हो, तो संगत $s_i = 0$. उदाहरण के लिए, **Z** में 20 और 15 लीजिए। तब $20 = 2^2 \times 3^0 \times 5^1$, और $15 = 2^0 \times 3^1 \times 5^1$.)

अब मान लीजिए $t_i = \min(r_i, s_i)\ \forall i = 1, 2, \ldots, n$. तब

$d = p_1^{t_1}\ p_2^{t_2}\ \ldots\ p_n^{t_n}$, a को और b को विभाजित करता है, क्योंकि $t_i \le r_i$ और $t_i \le s_i\ \forall\ i = 1,$

$2, \ldots, n$. अब, मान लीजिए $c \mid a$ और $c \mid b$. तब अद्वितीय गुणनखंडन गुण के कारण c का प्रत्येक अखंडनीय गुणनखंड a का और b का एक अखंडनीय गुणनखंड होगा। इस तरह,

$c = p_1^{m_1}\ p_2^{m_2}\ \ldots\ p_n^{m_n}$, जहां $m_i \le r_i$ और $m_i \le s_i\ \forall i = 1, 2, \ldots, n$.

इस तरह, $m_i \le t_i\ \ \forall\ i = 1, 2, \ldots, n$. इसलिए $c \mid d$.

अतः $d = (a, b)$.

इस प्रमेय से पता चलता है कि उदाहरण 5 और E10 में gcd प्राप्त करने के लिए हमने जो विधि लागू की थी, वह सही थी।

आइए, कुछ क्षणों के लिए उदाहरण 6 पर फिर विचार करें। वहां हमें एक प्रांत प्राप्त हुआ था, जो अद्वितीय गुणनखंडन प्रांत नहीं था और जिसमें यह आवश्यक नहीं था कि अखंडनीय अवयव अभाज्य अवयव भी हो। निम्नलिखित परिणाम के अनुसार अखंडनीय अवयव और अभाज्य अवयव में भेद केवल उस प्रांत में हो सकता है जो अद्वितीय गुणनखंडन प्रांत नहीं है।

प्रमेय 14 : मान लीजिए R एक अद्वितीय गुणनखंडन प्रांत है। R का कोई अवयव अभाज्य होता है यदि और केवल यदि वह अखंडनीय हो।

उपपत्ति : E13 से हम जानते हैं कि R में प्रत्येक अभाज्य अवयव अखंडनीय होता है। तो आइए हम इसका विलोम सिद्ध करें।

मान लीजिए $a \in R$ अखंडनीय है और $a \mid bc$, जहां $b, c \in R$. (a, b) लीजिए। क्योंकि a अखंडनीय है, इसलिए $(a, b) = 1$ या $(a, b) = a$.

यदि $(a, b) = a$, तो $a \mid b$.

यदि $(a, b) = 1$, तब $a \nmid b$. मान लीजिए $bc = ad$, जहां $d \in R$. मान लीजिए

$b = p_1^{r_1}\ p_2^{r_2}\ \ldots\ p_m^{r_m}$ और $c = q_1^{s_1}\ q_2^{s_2}\ \ldots\ q_n^{s_n}$, b और c के अखंडनीय गुणनखंडन हैं। क्योंकि

$bc = ad$ और a अखंडनीय है, इसलिए a कोई p_i या q_j अवश्य होगा। क्योंकि $a \nmid b$, इसलिए $a \ne p_i$ किसी i के लिए। इसलिए किसी j के लिए $a = q_j$, अर्थात् $a \mid c$.

अतः, यदि $(a, b) = 1$, तो $a \mid c$. इस तरह, हमने दिखाया है कि $a \mid bc \Rightarrow a \mid b$ या $a \mid c$. अतः a अभाज्य है।

अब हम आपको अद्वितीय गुणनखंडन प्रांतों का अंतिम गुण बताने जा रहे हैं। एक क्षण के लिए आइए हम उदाहरण 4 को फिर से देखें। वहां हमने मुख्य गुणजावली प्रांत R का एक उदाहरण दिया था, जिसके लिए R[x] एक मुख्य गुणजावली प्रांत नहीं था। अब आप पूछ सकते हैं कि यदि R एक UFD हो, तो क्या R[x] भी UFD होगा ? इस संबंध में यह परिणाम देखिए।

प्रमेय 15 : मान लीजिए R एक अद्वितीय गुणनखंडन प्रांत है। तब R[x] एक अद्वितीय गुणनखंडन प्रांत होगा।

हालांकि यह प्रमेय गणितज्ञों के लिए काफ़ी उपयोगी है, फिर भी हम इसे यहां सिद्ध नहीं करेंगे। परंतु इसे लागू अवश्य करेंगे। इसकी सहायता से आप नीचे दिए गए प्रश्नों को हल कीजिए।

E20) एक ऐसे UFD का उदाहरण दीजिए जो PID नहीं है।

E21) यदि p अद्वितीय गुणनखंडन प्रांत R का एक अखंडनीय अवयव है, तो क्या यह R के प्रत्येक विभाग वलय में अखंडनीय होता है ?

E22) क्या UFD का प्रत्येक विभाग वलय UFD होगा ? क्यों ?

E23) क्या UFD का प्रत्येक उपवलय UFD होगा ? क्यों ?

इस इकाई में हमने जो कुछ कहा है, उसका संक्षिप्त विवरण देते हुए इस इकाई को हम यहीं समाप्त कर रहे हैं।

14.5 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों पर चर्चा की है।

1. यूक्लिडीय प्रांत की परिभाषा और उसके उदाहरण।
2. Z, कोई क्षेत्र और किसी क्षेत्र पर बहुपद वलय यूक्लिडीय प्रांत होते हैं।
3. पूर्णांकीय प्रांत में मात्रक, सहचारी, गुणनखंड, दो अवयवों का महत्तम सार्व भाजक (gcd), अभाज्य अवयव और अखंडनीय अवयव।
4. मुख्य गुणजावली प्रांत (PID) की परिभाषा और उसके उदाहरण।
5. प्रत्येक यूक्लिडीय प्रांत एक PID होता है, परंतु इसका विलोम सही नहीं है।

   इस तरह, Z, F और F[x] मुख्य गुणजावली प्रांत हैं, जहां F एक क्षेत्र है।
6. मुख्य गुणजावली प्रांत R में किन्हीं दो अवयवों a और b के gcd का अस्तित्व होता है और किन्ही $x, y \in R$ के लिए यह $ax+by$ के रूप का होता है।
7. बीजगणित का मूल प्रमेय : C पर किसी अनाचर बहुपद के सभी मूल C में होते हैं।
8. PID में प्रत्येक अभाज्य गुणजावली उच्चिष्ठ गुणजावली होती है।
9. अद्वितीय गुणनखंडन प्रांत (UFD) की परिभाषा और उसके उदाहरण।
10. प्रत्येक PID एक UFD होता है। परंतु इसका विलोम सही नहीं है। इस तरह, Z और किसी क्षेत्र F के लिए, F और F[x], UFD हैं।
11. UFD में (और इस तरह PID में) कोई अवयव अभाज्य होता है यदि और केवल यदि वह अखंडनीय हो।
12. UFD में किन्हीं दो अवयवों का एक gcd होता है।
13. यदि R एक UFD है, तो R[x] भी UFD होगा।

14.6 हल/उत्तर

E1) $d : F \setminus \{0\} \to N \cup \{0\} : d(x) = 1.$

किन्हीं $a, b \in F \setminus \{0\}$ के लिए,

$d(ab) = 1 = d(a)$.

$\therefore\ d(a) = d(ab)\ \forall\ a, b \in F \setminus \{0\}$,

और किन्हीं $a, b \in F, b \neq 0$ के लिए

$a = (ab^{-1})\, b + 0$

इसलिए किसी प्रांत का यूक्लिडीय होने के लिए दूसरे प्रतिबंध को F संतुष्ट करता है।

अतः F एक यूक्लिडीय प्रांत है।

E2) इकाई 13 में आपने देखा है कि

$\deg\,(f(x)\,g(x)) = \deg f(x) + \deg g(x)\ \forall\ f(x), g(x) \in F[x] \setminus \{0\}$.

अब इकाई 13 के प्रमेय 5 को लागू करके आप परिणाम सिद्ध कर सकते हैं।

E3) (क) $m \in \mathbf{Z}$ एक मात्रक है यदि और केवल यदि $\exists\ n \in \mathbf{Z}$ जिससे कि $mn = 1$, अर्थात् यदि और केवल यदि $m = \pm 1$.

(ख) मान लीजिए $\bar{m} \in \mathbf{Z}_6$ एक मात्रक है। तब $\exists\ \bar{n} \in \mathbf{Z}_6$ जिससे कि $\bar{m}\ \bar{n} = \bar{1}$. इस तरह भाग 1.6.2 से हम पाते हैं कि $\bar{m}$ एक मात्रक है, यदि m और 6 का gcd, 1 हो।

$\therefore\ \bar{m} = \bar{1}$ या $\bar{5}$

(ग) $\mathbf{Z}/5\,\mathbf{Z}$ एक क्षेत्र है। अतः इसके मात्रक इसके सभी शून्येतर अवयव हैं।

(घ) मान लीजिए $a + ib$ एक मात्रक है। तब

$\exists\ c + id \in \mathbf{Z} + i\,\mathbf{Z}$ जिससे कि

$(a+ib)\,(c + id) = 1$.

$\Rightarrow (ac-bd) + (ad + bc)i = 1$

$\Rightarrow ac-bd = 1$ और $ad + bc = 0$.

$\Rightarrow b = 0$, उदाहरण 3 की तरह।

अतः $a + ib = 1$ या -1, ऊपर के (क) से।

E4) मान लीजिए $u \in R$ एक मात्रक है। तब $\exists\ v \in R$ जिससे कि $v\,u = 1$. इस तरह, किसी $r \in R$ के लिए $r = r\,.\,1 = r\,(vu) = (rv)\,u \in Ru$.

इस तरह, $R \subseteq Ru$. $\therefore\ R = Ru$

विलोमतः, मान लीजिए $Ru = R$. क्योंकि $1 \in R = Ru$,
इसलिए $\exists\ v \in R$ जिससे कि $1 = vu$.

अतः R में u एक मात्रक है।

E5) यूक्लिडीय प्रांत $F[x]$ पर प्रमेय 2 लागू कीजिए।

E6) मान लीजिए $R = \mathbf{Z}$, तब $S = \{n \in \mathbf{Z}^* \mid |n| > 1\} \cup \{0\}$. तब $2 \in S, 3 \in S$, परंतु $2-3 \notin S$ क्योंकि $|2-3| = 1$. अतः S, R का एक उपवलय भी नहीं है।

E7) उदाहरण के लिए, $\mathbf{Z}[x]$, $\mathbf{Q}[x]$ का एक उपवलय है। $\mathbf{Q}[x]$ एक PID है। परंतु $\mathbf{Z}[x]$, PID नहीं है।

E8) Z एक मुख्य गुणजावली प्रांत है। परंतु $\mathbf{Z}/6\,\mathbf{Z}$ एक प्रांत भी नहीं है। अतः यह मुख्य गुणजावली प्रांत नहीं है।

E9) (क) u एक मात्रक होता है यदि और केवल यदि किसी $v \in R$ के लिए $u\,v = 1$ यदि और केवल यदि $u \mid 1$.

(ख) $a \mid b$ और $b \mid a$.

$\Rightarrow$ किन्हीं $c, d \in R$ के लिए $b = ac$ और $a = bd$.

$\Rightarrow b = bdc$

$\Rightarrow b = 0$ या $dc = 1$.

यदि $b = 0$, तो $a = 0$, और तब a और b सहचारी होते हैं।

यदि $b \neq 0$, तो $dc = 1$, अतः c एक मात्रक है और $b = ac$.

इसलिए a और b सहचारी हैं।

विलोमतः, मान लीजिए R में a और b सहचारी हैं, और $a = bu$, जहां R में u एक मात्रक है। तब $b \mid a$. और मान लीजिए $v \in R$ जिससे कि $uv = 1$. तब $av = buv = b$. इस तरह, $a \mid b$.

E10) (क) $\overline{2}$

(ख) $x^2 + 8x + 15 = (x+3)(x+5)$, $x^2 + 12x + 35 = (x+5)(x+7)$.

अतः इनका gcd, $x+5$ है।

(ग) $x^3 - 2x^2 + 6x - 5 = (x-1)(x^2 - x + 5)$, $x^2 - 2x + 1 = (x-1)^2$.

अतः इनका gcd, $x-1$ है।

E11) $\exists\, x, y \in R$ जिससे कि $ax + by = 1$

तब $c = 1 \cdot c = (ax+by)\,c = acx + bcy$.

क्योंकि $a \mid ac$ और $a \mid bc$, इसलिए $a \mid (acx+bcy) = c$.

E12) (ग) है, प्रमेय 5′ से।

(क) नहीं है, क्योंकि यह $(x-1)^2$ है।

प्रमेय 5′ के अनुसार (ख) नहीं है।

प्रमेय 6 के अनुसार (घ) नहीं है।

E13) मान लीजिए $p = ab$. तब $p \mid ab \Rightarrow p \mid a$ या $p \mid b$. मान लीजिए $p \mid a$ और $a = pc$. तब $p = ab = pcb \Rightarrow p(1 - cb) = 0 \Rightarrow 1 - cb = 0$, क्योंकि R एक प्रांत है और $p \neq 0$. इस तरह, $bc = 1$, अर्थात् b एक मात्रक है।

इसी प्रकार आप दिखा सकते हैं कि यदि $p \mid b$, तो a एक मात्रक है।

इसलिए $p = ab \Rightarrow$ a एक मात्रक है या b एक मात्रक है, अर्थात् p अखंडनीय है।

E14) (क), (ग), क्योंकि 5 और $x^2 + x + 1$ क्रमशः **Z** और **R**[x] में अखंडनीय है। प्रमेय 9 के अनुसार (ख) नहीं है।

(घ) नहीं है, क्योंकि $\mathbf{Z}[x]/\langle x \rangle \simeq \mathbf{Z}$, जो एक क्षेत्र नहीं है।

E15) $n = 1$ के लिए परिणाम सही है। मान लीजिए कि यह सभी $m < n$ के लिए लागू होता है, अर्थात् जब भी $m < n$ और $p \mid a_1 a_2 \ldots a_m$, तब $p \mid a_i$ किसी $i = 1, 2, \ldots, m$ के लिए। अब मान लीजिए $p \mid a_1 a_2 \ldots a_n$. तब $p \mid (a_1 a_2 \ldots a_{n-1}) a_n$, क्योंकि p अभाज्य है, हम पाते हैं कि $p \mid a_1 a_2 \ldots a_{n-1}$ या $p \mid a_n$.

यदि $p \mid a_1 a_2 \ldots a_{n-1}$, तो $p \mid a_i$ किसी $i = 1, 2, \ldots, n-1$ के लिए हमारी परिकल्पना से। यदि $p \nmid a_1 a_2 \ldots a_{n-1}$ तो $p \mid a_n$.

अतः, दोनों स्थितियों में किसी $i = 1, \ldots, n$ के लिए $p \mid a_i$.

अतः हमारा परिणाम n के लिए सही है। अतः यह सभी $n \in \mathbf{N}$ के लिए सही है।

E16) $2x^2 - 3x + 1 = (2x-1)(x-1)$, **Q** [x] में। $\mathbf{Z}_2[x]$ में दिया हुआ बहुपद $x + \overline{1}$ है, क्योंकि $\overline{2} = \overline{0}$ और $-\overline{3} = \overline{1}$. यह बहुपद रैखिक है, और इसलिए $\mathbf{Z}_2$ पर अखंडनीय है। अतः इसका अभाज्य गुणनखंडन केवल $x + \overline{1}$ है।

E17) मान लीजिए $f(x)$, $F[x]$ में एक शून्येतर अव्युत्क्रमणीय बहुपद है और $\deg f(x) = n$. तब $n > 0$. n पर आगमन नियम लागू करके हम सिद्ध करेंगे कि $f(x)$ को अखंडनीय अवयवों के गुणनफल के रूप में लिखा जा सकता है।

यदि $n = 1$, तो $f(x)$ रैखिक है, और इसलिए अखंडनीय है। अब मान लीजिए घात $< n$ वाले बहुपदों के लिए परिणाम सही है। अब $f(x)$ को लीजिए। यदि $f(x)$ अखंडनीय है, तो कुछ करना बाकी नहीं है।

वरना ऐसा अभाज्य $f_1(x)$ है जिससे कि $f_1(x) | f(x)$. मान लीजिए $f(x) = f_1(x)\ g_1(x)$. ध्यान दें कि $\deg f_1(x) > 0$.

अतः $\deg g_1(x) < \deg f(x)$. यदि $g_1(x)$ अभाज्य है, तो कुछ करना बाकी नहीं है।

वरना ऐसा अभाज्य $f_2(x)$ है जिससे कि $g_1(x) = f_2(x)\ g_2(x)$. तब $\deg g_2(x) < \deg g_1(x)$. यह प्रक्रिया कुछ चरणों के बाद रुकेगी क्योंकि हर बार हमें कम घात के बहुपद प्राप्त होते हैं। अतः अंत में हमें $f(x) = f_1(x)\ f_2(x) \ldots\ldots f_m(x)$, प्राप्त होगा, जहां प्रत्येक $f_i(x)$, $F[x]$ में अभाज्य है।

अब आप प्रमेय 12 की उपपत्ति की तरह ही सिद्ध कर सकते हैं कि गुणनखंडन अद्वितीय है।

E18) $10 = 2 \times 5 = 5 \times 2$.

E19) $6 = 2.3 = (1 + \sqrt{-5})\ (1 - \sqrt{-5})$

मानक फलन के प्रयोग से आप सत्यापित कर सकते हैं कि $\mathbf{Z}[\sqrt{-5}]$ में $2, 3, 1 + \sqrt{-5}$ और $1 - \sqrt{-5}$ में से प्रत्येक अखंडनीय है।

E20) $\mathbf{Z}[x]$

E21) नहीं। उदाहरण के लिए, $\mathbf{Z}[x]$ में x अखंडनीय है, पर $\mathbf{Z}[x]/< x > \simeq \mathbf{Z}$ में $\bar{x}$ शून्य है।

E22) यह आवश्यक नहीं है कि किसी प्रांत का विभाग वलय भी एक प्रांत हो। उदाहरण के लिए, $\mathbf{Z}$ एक अद्वितीय गुणनखंडन प्रांत है, परंतु $\mathbf{Z}/< 4 >$ नहीं है।

और, यदि विभाग वलय एक प्रांत हो भी, तो ज़रूरी नहीं कि यह अद्वितीय गुणनखंडन प्रांत हो।

उदाहरण के लिए, $\mathbf{Z}[\sqrt{-5}] \simeq \mathbf{Z}[x]/< x^2 + 5 >$ एक अद्वितीय गुणनखंडन प्रांत नहीं है, जबकि $\mathbf{Z}[x]$ है।

E23) नहीं। उदाहरण के लिए, $\mathbf{Z}[\sqrt{-5}]$, UFD $\mathbf{C}$ का एक उपवलय है। लेकिन यह अद्वितीय गुणनखंडन प्रांत नहीं है।

इकाई 15 अखंडनीयता और क्षेत्र विस्तार

इकाई की रूपरेखा

15.1 प्रस्तावना

पिछली इकाई में हमने अद्वितीय गुणनखंडन प्रांतों और अन्य विभिन्न प्रकार के पूर्णांकीय प्रांतों पर चर्चा की थी। वहाँ आपने देखा कि Z [x] और Q [x] अद्वितीय गुणनखंडन प्रांत हैं। इस तरह, इन वलयों के अभाज्य और अखंडनीय अवयव समान हैं। इस इकाई में हम आपको Z [x] और Q [x] के अभाज्य (या अखंडनीय) अवयव प्राप्त करने की एक विधि की जानकारी देंगे। इस विधि को आइसनस्टाइन निकष कहते हैं, जिसका प्रयोग किसी अद्वितीय गुणनखंडन प्रांत पर बहुपद वलय के अखंडनीय अवयवों को प्राप्त करने के लिए भी किया जा सकता है।

इसके बाद हम आपको क्षेत्र विस्तार और उपक्षेत्र से परिचित कराएंगे। हम F [x] से क्षेत्र F के क्षेत्र विस्तार प्राप्त करने के लिए अखंडनीय बहुपदों का प्रयोग करेंगे। आप यह भी देखेंगे कि प्रत्येक क्षेत्र, Q या Z_p (किसी अभाज्य p के लिए) का एक क्षेत्र विस्तार होता है। यही कारण है कि हम Q और Z_p को अभाज्य क्षेत्र कहते हैं। इन क्षेत्रों के बारे में हम संक्षिप्त चर्चा करेंगे।

चित्र 1 : एवारीस्त गाल्वा
(1811-1832)

अंत में हम परिमित क्षेत्र पर विचार करेंगे। इन क्षेत्रों को संख्या सिद्धांत पर शोध कार्य करने के दौरान युवा फ्रांसिसी गणितज्ञ एवारीस्त गाल्वा (चित्र 1) ने प्रस्तुत किया था। हम परिमित क्षेत्रों के कुछ गुणों पर चर्चा करेंगे जिनसे परिमित क्षेत्रों को वर्गीकृत करने के बारे में हमें जानकारी प्राप्त होगी।

हमारा सुझाव है कि इस इकाई को पढ़ने से पहले आप इकाई 14 में दी गई अखंडनीयता की परिभाषा पढ़ लें। हमारा यह भी सुझाव है कि यदि आप इस इकाई के प्रमेय 7 की उपपत्ति को ठीक से समझना चाहते हैं तो आप रैखिक बीजगणित के पाठ्यक्रम की इकाई 3 और इकाई 4 को पढ़ लें। उपपत्ति को पढ़ें अथवा नहीं, यह आपकी इच्छा है। परंतु एक बार आप सदिश समष्टि और उसके आधार की परिभाषा जान लें, तो आपके लिए उपपत्ति सरल हो जाएगी।

उद्देश्य

इस इकाई को पढ़ने के बाद आप

- Z [x] और Q [x] में अखंडनीयता के लिए आइसनस्टाइन निकष को सिद्ध कर सकेंगे और उसका प्रयोग कर सकेंगे ;
- F [x] से क्षेत्र F के क्षेत्र विस्तार प्राप्त कर सकेंगे;
- किसी क्षेत्र का अभाज्य क्षेत्र प्राप्त कर सकेंगे;
- इस तथ्य का प्रयोग कर सकेंगे कि किसी भी परिमित क्षेत्र F के p^n अवयव होते हैं, जहाँ char F = p और $\dim_{Z_p} F = n$.

15.2 Q[x] में अखंडनीयता

इकाई 14 में हमने आपको F[x] में अखंडनीय बहुपदों से परिचित कराया था, जहाँ F एक क्षेत्र है। हमने बीजगणित के मूल प्रमेय का कथन भी दिया था, जिसके अनुसार C पर बहुपद अखंडनीय होता है यदि और

केवल यदि यह रैखिक हो। आपने यह भी देखा था कि यदि **R** पर कोई बहुपद अखंडनीय हो तो उसका घात 1 या 2 होगा। इस तरह, **R** पर 2 से अधिक घात वाला बहुपद खंडनीय होता है। और द्विघाती सूत्र लागू करके हम जान सकते हैं कि **R** पर कौन से द्विघात बहुपद अखंडनीय हैं।

आइए अब हम **Q** पर बहुपदों के बारे में चर्चा करें। जैसा कि किसी क्षेत्र F के लिए है, **Q** पर भी रैखिक बहुपद अखंडनीय होता है। और, द्विघाती सूत्र लागू करके हम **Q** पर किसी द्विघात बहुपद के मूल प्राप्त कर सकते हैं, और इस तरह हम पता लगा सकते हैं कि बहुपद अखंडनीय है कि नहीं। परंतु क्या आप बता सकते हैं कि **Q** पर $2x^7 + 3x^5 - 6x^4 + 3x^3 + 12$ अखंडनीय है कि नहीं ? हम तुरंत बता सकते हैं कि यह बहुपद अखंडनीय है, आइसनस्टाइन निकष (Eisenstein criterion) लागू करके। इस निकष को उन्नीसवीं शताब्दी में गणितज्ञ फर्डिनंड आइसनस्टाइन ने प्रस्तुत किया था। इस भाग में हम इस उपयोगी निकष को सिद्ध करने के लिए सिद्धांतिक जानकारी देंगे।

आइए, हम एक परिभाषा से शुरू करें।

परिभाषा : मान लीजिए $f(x) = a_0 + a_1x + ... + a_n x^n \in \mathbf{Z}[x]$. हम f(x) के **आधेय** (content) को पूर्णांकों $a_0, a_1, ..., a_n$ के gcd से परिभाषित करते हैं।

हम f(x) को **पूर्वग** (primitive) कहते हैं यदि f(x) का आधेय 1 हो।

उदाहरण के लिए, $3x^2 + 6x + 12$ का आधेय 3, 6 और 12 का gcd, अर्थात् 3 है। इस तरह, यह बहुपद पूर्वग नहीं है। परंतु बहुपद $x^5 + 3x^2 + 4x - 5$ पूर्वग है, क्योंकि 1, 0, 0, 3, 4, –5 का gcd, 1 है।

अब शायद आप नीचे दिए गए प्रश्न हल करना चाहेंगे।

E1) **Z** पर निम्नलिखित बहुपदों के आधेय क्या हैं ?

(क) $1 + x + x^2 + x^3 + x^4$

(ख) $7x^4 - 7$

(ग) $5(2x^2 - 1)(x + 2)$

E2) सिद्ध कीजिए कि किसी भी बहुपद $f(x) \in \mathbf{Z}[x]$ को $dg(x)$ के रूप में लिखा जा सकता है, जहाँ d, f(x) का आधेय है और g(x) एक पूर्वग बहुपद है।

अब हम सिद्ध करेंगे कि पूर्वग बहुपदों का गुणनफल एक पूर्वग बहुपद होता है। यह परिणाम गाउस प्रमेयिका (Gauss' lemma) के नाम से प्रसिद्ध है।

प्रमेय 1 : मान लीजिए f(x) और g(x) पूर्वग बहुपद हैं। तब f(x) g(x) भी पूर्वग बहुपद होता है।

उपपत्ति : मान लीजिए

$f(x) = a_0 + a_1x + ... + a_n x^n \in \mathbf{Z}[x]$ और

$g(x) = b_0 + b_1x + ...+ b_m x^m \in \mathbf{Z}[x]$, जहाँ

$a_0, a_1, ..., a_n$ का gcd, 1 है और $b_0, b_1, ..., b_m$ का gcd, 1 है। अब

$f(x)\, g(x) = c_0 + c_1x + ... + c_{m+n} x^{m+n}$,

जहाँ $c_k = a_0b_k + a_1 b_{k-1} + ... + a_k b_0$.

इस परिणाम को सिद्ध करने के लिए हम यह मानकर चलेंगे कि यह गलत है और तब एक अंतर्विरोध प्राप्त करेंगे। अतः मान लीजिए कि f(x) g(x) पूर्वग नहीं है। तब $c_0, c_1, ..., c_{m+n}$ का gcd, 1 से अधिक होगा और कोई अभाज्य p इसे अवश्य विभाजित करेगा। इस तरह, $p \mid c_i \ \forall\ i = 0, 1, ..., m+n$. क्योंकि f(x) पूर्वग है, इसलिए p कम से कम एक a_i को विभाजित नहीं करेगा। मान लीजिए r एक ऐसा न्यूनतम पूर्णांक है कि $p \nmid a_r$. इसी प्रकार मान लीजिए कि s एक ऐसा न्यूनतम पूर्णांक है कि $p \nmid b_s$. अब, c_{r+s} को लीजिए।

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + ... + a_r b_s + ... + a_{r+s} b_0.$$

$$= a_r b_s + (a_0 b_{r+s} + a_1 b_{r+s-1} + ... + a_{r-1} b_{s+1} + a_{r+1} b_{s-1} + ...+ a_{r+s} b_0)$$

जिस तरह हमने r और s को चुना है,

$p \mid a_0, p \mid a_1, \ldots, p \mid a_{r-1}$, और

$p \mid b_0, p \mid b_1, \ldots, p \mid b_{s-1}$. साथ ही $p \mid c_{r+s}$.

इसलिए $p \mid c_{r+s} - (a_0 b_{r+s} + \ldots + a_{r-1} b_{s+1} + a_{r+1} b_{s-1} + \ldots + a_{r+s} b_0)$

अर्थात्, $p \mid a_r b_s$.

$\Rightarrow p \mid a_r$ या $p \mid b_s$, क्योंकि p अभाज्य है। परंतु $p \nmid a_r$ और $p \nmid b_s$. इस तरह हमें एक अंतर्विरोध प्राप्त होता है। अतः हम जो मानकर चले थे वह सही नहीं था। अर्थात् हमारा प्रमेय सही है।

आइए, अब हम अपना ध्यान Q पर बहुपदों की ओर ले चलें। Q पर कोई बहुपद f(x) लीजिए, मान लीजिए

$$f(x) = \frac{3}{2}x^3 + \frac{1}{5}x^2 + 3x + \frac{1}{3}.$$

यदि हम सभी हरों के, अर्थात् 2, 5, 1 और 3 का लघुतम सार्व गुणज (lcm) लें, जो 30 है, और इससे f(x) को गुणा करें तो हमें $30\,f(x) = 45x^3 + 6x^2 + 90x + 10 \in \mathbf{Z}[x]$ प्राप्त होता है।

इसी प्रक्रिया को लागू करके हम किसी भी $f(x) \in \mathbf{Q}[x]$ को एक ऐसे पूर्णांक d से गुणा कर सकते हैं जिससे कि $f(x) \in \mathbf{Z}[x]$. हम इस तथ्य का प्रयोग $\mathbf{Z}[x]$ में अखंडनीयता और $\mathbf{Q}[x]$ में अखंडनीयता के संबंध को स्थापित करने के लिए करेंगे।

प्रमेय 2 : यदि $f(x) \in \mathbf{Z}[x]$, $\mathbf{Z}[x]$ में अखंडनीय हो, तो यह $\mathbf{Q}[x]$ में भी अखंडनीय होगा।

उपपत्ति : आइए, हम मान लें कि $\mathbf{Q}[x]$ पर f(x) अखंडनीय नहीं है। फिर हमें एक अंतर्विरोध प्राप्त होना चाहिए। तो मान लीजिए कि $\mathbf{Q}[x]$ में $f(x) = g(x)\,h(x)$, जहाँ न तो g(x) और न ही h(x) मात्रक हैं, अर्थात् $\deg g(x) > 0$, $\deg h(x) > 0$. क्योंकि $g(x) \in \mathbf{Q}[x]$, $\exists\, m \in \mathbf{Z}$, जिससे कि $mg(x) \in \mathbf{Z}[x]$. इसी प्रकार, $\exists\, n \in \mathbf{Z}$ जिससे कि $nh(x) \in \mathbf{Z}[x]$. तब,

$$mn\,f(x) = mg(x)\,nh(x) \qquad \ldots\ldots\ldots (1)$$

अब आइए, हम E2 का प्रयोग करें। E2 के अनुसार,
$f(x) = rf_1(x)$, $mg(x) = sg_1(x)$, $nh(x) = th_1(x)$, जहां r, s और t क्रमशः f(x), mg(x) और nh(x) के आधेय हैं और $f_1(x)$, $g_1(x)$, $h_1(x)$ धन घात वाले पूर्वग बहुपद हैं। इस तरह, (1) से

$$mn\,r\,f_1(x) = st\,g_1(x)\,h_1(x) \qquad \ldots\ldots\ldots (2)$$

प्राप्त होता है।

क्योंकि $g_1(x)$ और $h_1(x)$ पूर्वग हैं, इसलिए प्रमेय 1 के अनुसार $g_1(x)\,h_1(x)$ पूर्वग है। इस तरह, समीकरण (2) के दाएँ पक्ष के बहुपद का आधेय 2 है। लेकिन समीकरण (2) के वाम पक्ष के बहुपद का आधेय mnr है।

इस तरह, (2) के अनुसार, $mnr = st$.

अतः (2) में निरसन नियम के प्रयोग से हमें

$f_1(x) = g_1(x)\,h_1(x)$ प्राप्त होता है।

इसलिए $\mathbf{Z}[x]$ में $f(x) = rf_1(x) = (rg_1(x))\,h_1(x)$, जहाँ न तो $rg_1(x)$ और न ही $h_1(x)$ मात्रक हैं। यह इस तथ्य का अंतर्विरोध करता है कि $\mathbf{Z}[x]$ में f(x) अखंडनीय है।

इस तरह, हम जो मानकर चले थे वह सही नहीं है। अतः $\mathbf{Q}[x]$ में f(x) अखंडनीय होगा।

इस परिभाषा से यह अर्थ निकलता है कि $\mathbf{Q}[x]$ में किसी बहुपद की अखंडनीयता को जांच करने के लिए $\mathbf{Z}[x]$ में इसकी अखंडनीयता की जांच कर लेना ही काफ़ी है। और, $\mathbf{Z}[x]$ में इसकी अखंडनीयता की जांच के लिए हम प्रबल आइसनस्टाइन निकष का प्रयोग कर सकते हैं।

प्रमेय 3 (आइसनस्टाइन निकष) : मान लीजिए

$f(x) = a_0 + a_1 x + \ldots\ldots\ldots + a_n x^n \in \mathbf{Z}[x]$, और किसी अभाज्य संख्या p के लिए,

(i) $p \nmid a_n$

(ii) $p | a_0, p | a_1, \ldots\ldots, p | a_{n-1}$, और

(iii) $p^2 \nmid a_0$.

तब $\mathbf{Z}$ [x] में (और इसलिए $\mathbf{Q}$ [x] में) f(x) अखंडनीय होता है।

उपपत्ति : क्या आप बता सकते हैं कि हम इसे कैसे सिद्ध करेंगे ? यहां भी हम अंतर्विरोध वाली विधि को लागू करेंगे। तो मान लीजिए कि $\mathbf{Z}$ [x] में f(x) अखंडनीय है, और मान लीजिए $f(x) = g(x)\, h(x)$,

जहां $g(x) = b_0 + b_1 x + \ldots + b_m x^m$, $m > 0$, और

$h(x) = c_0 + c_1 x + \ldots + c_r x^r$, $r > 0$.

तब $n = \deg f = \deg g + \deg h = m + r$, और

$a_k = b_0 c_k + b_1 c_{k-1} + \ldots + b_k c_0 \; \forall \; k = 0, 1, \ldots, n$.

अब, $a_0 = b_0 c_0$. हम जानते हैं कि $p | a_0$. अतः $p \mid b_0 c_0$ इसलिए $p \mid b_0$ या $p \mid c_0$. क्योंकि $p^2 \nmid a_0$, इसलिए p, b_0 और c_0 दोनों को विभाजित नहीं कर सकता। आइए, हम मान लें कि $p | b_0$ और $p \nmid c_0$. आइए अब हम $a_n = b_m c_r$ को लें। क्योंकि $p \nmid a_n$, इसलिए $p \nmid b_m$ और $p \nmid c_r$. इस तरह, हम पाते हैं कि किसी i के लिए $p \nmid b_i$. मान लीजिए k ऐसा न्यूनतम पूर्णांक है कि $p \nmid b_k$. ध्यान दीजिए कि $0 < k \le m < n$.

इसलिए $p | a_k$.

अब $a_k = (b_0 c_k + \ldots + b_{k-1} c_1) + b_k c_0$.

क्योंकि $p | a_k$ और $p | b_0, p | b_1, \ldots, p | b_{k-1}$,

इसलिए $p | a_k - (b_0 c_k + \ldots + b_{k-1} c_1)$, अर्थात् $p \mid b_k c_0$. परंतु $p \nmid b_k$ और $p \nmid c_0$. अतः हमें एक अंतर्विरोध प्राप्त होता है।

इस तरह, $\mathbf{Z}$ [x] में f(x) अखंडनीय होगा।

आइए, इस निकष के प्रयोग को समझने के लिए एक उदाहरण लें।

उदाहरण 1 : क्या $\mathbf{Q}$ [x] में $2x^7 + 3x^5 - 6x^4 + 3x^3 + 12$ अखंडनीय है ?

हल : इस बहुपद के गुणांकों को देखने पर हम पाते हैं कि अभाज्य संख्या 3 आइसनस्टाइन निकष में दिए गए प्रतिबंधों को संतुष्ट करती है। इसलिए दिया हुआ बहुपद $\mathbf{Q}$ [x] में अखंडनीय है।

उदाहरण 2 : मान लीजिए p एक अभाज्य संख्या है। क्या $\mathbf{Q}[x] \;/ < x^3 - p >$ एक क्षेत्र है ?

हल : इकाई 14 से आप जानते हैं कि किसी क्षेत्र F के लिए यदि F[x] में f(x) अखंडनीय है, तो $< f(x) >$, F[x] की उच्चिष्ठ गुणजावली है।

अब $x^3 - p$ के लिए प्रमेय 3 में दिए गए प्रतिबंधों को p संतुष्ट करता है। इसलिए आइसनस्टाइन निकष के अनुसार $x^3 - p$ अखंडनीय है। अतः, $< x^3 - p >$, $\mathbf{Q}$ [x] की एक उच्चिष्ठ गुणजावली है।

इकाई 12 से आप जानते हैं कि यदि R एक वलय हो, और M, R की उच्चिष्ठ गुणजावली हो तो R/M एक क्षेत्र होता है।

अतः $\mathbf{Q}[x] / < x^3 - p >$ एक क्षेत्र है।

इस उदाहरण में हमने एक महत्वपूर्ण तथ्य को देखा है। निम्नलिखित प्रश्न में हम आपसे इस तथ्य को सिद्ध करने को कह रहे हैं।

E3) किसी $n \in \mathbf{N}$ और अभाज्य संख्या p के लिए दिखाइए कि $\mathbf{Q}$ [x] पर $x^n - p$ अखंडनीय है। ध्यान दें कि इससे हमें पता चलता है कि $\mathbf{Q}$ [x] पर हम किसी भी घात का अखंडनीय बहुपद प्राप्त कर सकते हैं।

आइए, अब हम अखंडनीय बहुपद का एक और उदाहरण लें। इस उदाहरण को हल करने के दौरान आप देखेंगे कि हम कैसे अप्रत्यक्ष रूप से प्रमेय 3 का प्रयोग कर सकते हैं।

उदाहरण 3 : मान लीजिए p एक अभाज्य संख्या है। दिखाइए कि $\mathbf{Z}[x]$ में

$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ अखंडनीय है।

$f(x)$ को p वां **वृत्तभाजनिक बहुपद** कहते हैं।

हल : सबसे पहले आप इस बात की ओर ध्यान दीजिए कि $\mathbf{Z}[x]$ में $f(x) = g(x)\,h(x)$ होता है यदि और केवल यदि $\mathbf{Z}[x]$ में $f(x+1) = g(x+1)\,h(x+1)$ हो। इस तरह, $\mathbf{Z}[x]$ में $f(x)$ अखंडनीय होता है यदि और केवल यदि $\mathbf{Z}[x]$ में $f(x+1)$ अखंडनीय हो।

अब, $f(x) = \dfrac{x^p - 1}{x - 1}$.

$$\therefore\ f(x+1) = \frac{(x+1)^p - 1}{x}$$

$$= \frac{1}{x}\left(x^p + {}^pC_1\,x^{p-1} + \ldots + {}^pC_{p-1}\,x + 1 - 1\right),\ (\text{द्विपद प्रमेय से})$$

$$= x^{p-1} + px^{p-2} + {}^pC_2\,x^{p-3} + \ldots + {}^pC_{p-2}\,x + p.$$

अब p को अभाज्य लेकर आइसनस्टाइन निकष लागू करें। हम पाते हैं कि $f(x+1)$ अखंडनीय है। अतः $f(x)$ अखंडनीय है।

अब आप नीचे दिए गए प्रश्न हल कर सकते हैं।

E4) यदि $\mathbf{Q}[x]$ में $a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Z}[x]$ अखंडनीय हो, तो क्या आप सदा ही एक ऐसा अभाज्य p प्राप्त कर सकते हैं जो प्रमेय 3 के प्रतिबंधों (i), (ii) और (iii) को संतुष्ट करता हो ?

E5) $\mathbf{Z}[x]$ के निम्नलिखित अवयवों में से कौन से $\mathbf{Q}$ पर अखंडनीय हैं ?

(क) $x^2 - 12$

(ख) $8x^3 + 6x^2 - 9x + 24$

(ग) $5x + 1$

E6) मान लीजिए p एक अभाज्य पूर्णांक है। मान लीजिए a एक शून्येतर अव्युत्क्रमणीय पूर्णांक है, और किसी भी $b \in \mathbf{Z}$ के लिए $b^2 \nmid a$. दिखाइए कि $\mathbf{Z}[x] / < x^p + a >$ एक पूर्णांकीय प्रांत है।

E7) दिखाइए कि किसी भी $\bar{a} \in \mathbf{Z}_p$ के लिए $x^p + \bar{a} \in \mathbf{Z}_p[x]$ अखंडनीय नहीं है।

(संकेत : क्या आपको इकाई 13 के E13 से मदद मिलती है ?)

अभी तक हमने इस तथ्य का प्रयोग किया है कि यदि $f(x) \in \mathbf{Z}[x]$, $\mathbf{Z}$ पर अखंडनीय हो, तो यह $\mathbf{Q}$ पर भी अखंडनीय होता है। क्या आप समझते हैं कि इसी प्रकार का संबंध $\mathbf{Q}$ पर अखंडनीयता और $\mathbf{R}$ पर अखंडनीयता के बीच भी हो सकता है ? इस प्रश्न का उत्तर प्राप्त करने के लिए $f(x) = x^2 - 2$ लीजिए। यह $\mathbf{Q}[x]$ में अखंडनीय है, परंतु $\mathbf{R}[x]$ में $f(x) = (x - \sqrt{2})(x + \sqrt{2})$. इस तरह, हम पाते हैं कि हम $\mathbf{Q}$ पर अखंडनीयता को $\mathbf{R}$ पर विस्तृत नहीं कर सकते।

परंतु हम प्रमेय 2 का व्यापकीकरण कर सकते हैं। यह न केवल $\mathbf{Z}$ और $\mathbf{Q}$ के लिए सत्य है, बल्कि किसी भी UFD, R और उसके विभाग क्षेत्र F (भाग 12.5 देखिए) के लिए सत्य होता है। आइए हम इस संबंध को स्पष्ट करें।

प्रमेय 4 : मान लीजिए R एक अद्वितीय गुणनखंडन प्रांत है, जिसका विभाग क्षेत्र F है।

i) यदि $f(x) \in R[x]$ एक अखंडनीय पूर्वग बहुपद है, तो यह $F[x]$ में भी अखंडनीय होगा।

ii) **(आइसनस्टाइन निकष)** : मान लीजिए

$f(x) = a_0 + a_1 x + ... + a_n x^n \in R[x]$ और $p \in R$ एक ऐसा अभाज्य है कि $p \nmid a_n$, $p^2 \nmid a_0$ और $0 \le i < n$ के लिए $p \mid a_i$. तब $F[x]$ में $f(x)$ अखंडनीय होता है।

इस परिभाषा की उपपत्ति ठीक प्रमेय 2 और प्रमेय 3 की उपपत्तियों की तरह है। हम इसे यहां नहीं दे रहे हैं। परंतु यदि आप चाहें तो इस परिणाम को सिद्ध करने का प्रयास कर सकते हैं।

हम आपको बता चुके हैं कि यदि F एक क्षेत्र हो और F पर $f(x)$ अखंडनीय हो, तो $F[x] / < f(x) >$ एक क्षेत्र होता है। यह क्षेत्र और F कैसे संबंधित हैं ? अगले भाग में होने वाली चर्चा का यह एक हिस्सा है।

15.3 क्षेत्र विस्तार (Field Extension)

इस भाग में हम उपक्षेत्रों और क्षेत्र विस्तारों पर चर्चा करेंगे। आइए पहले हम इन शब्दों की परिभाषा दें। अब तक शायद आप इस परिभाषा का अनुमान लगा सकते हैं।

परिभाषा : किसी क्षेत्र F के अरिक्त उपसमुच्चय S को F का **उपक्षेत्र** (subfield) कहते हैं यदि यह F की संक्रियाओं के सापेक्ष एक क्षेत्र हो। यदि $S \neq F$, तो S को F का **उचित उपक्षेत्र** (proper subfield) कहते हैं।

क्षेत्र K को F का **क्षेत्र विस्तार** कहते हैं यदि F, K का उपक्षेत्र हो। इस तरह, **Q**, **R** का एक उपक्षेत्र है और और **R**, **Q** का एक क्षेत्र विस्तार है। इसी प्रकार, **C**, **Q** और **R** दोनों का क्षेत्र विस्तार है।

ध्यान दीजिए कि क्षेत्र F का अरिक्त उपसमुच्चय S क्षेत्र F का उपक्षेत्र होता है यदि और केवल यदि

i) S, (F, +) का एक उपसमूह है, और

ii) S के सभी शून्येतर अवयवों का समुच्चय गुणन के सापेक्ष F के शून्येतर अवयवों के समूह का एक उपसमूह है।

इस तरह, इकाई 3 के प्रमेय 1 से हमें निम्नलिखित प्रमेय प्राप्त होता है।

प्रमेय 5 : क्षेत्र F का अरिक्त उपसमुच्चय S, F का एक उपक्षेत्र होता है यदि और केवल यदि

i) $a \in S, b \in S \Rightarrow a - b \in S$, और

ii) $a \in S, b \in S, b \neq 0 \Rightarrow ab^{-1} \in S$.

अब प्रमेय 5 की सहायता से निम्नलिखित प्रश्न हल कीजिए।

E8) दिखाइए कि

क) $\mathbf{Q} + i\mathbf{Q}$, **C** का उपक्षेत्र है।

ख) $\mathbf{Z} + \sqrt{2}\,\mathbf{Z}$, **R** का उपक्षेत्र नहीं है।

आइए अब हम क्षेत्र F के एक विशेष क्षेत्र विस्तार पर विचार करें। क्योंकि $F[x]$ एक पूर्णांकीय प्रांत है, इसलिए हम इसका विभाग क्षेत्र प्राप्त कर सकते हैं (इकाई 12 देखिए)। हम इस क्षेत्र को $\mathbf{F(x)}$ से प्रकट करते हैं। तब F, $F(x)$ का एक उपक्षेत्र है। अतः $F(x)$, F का एक क्षेत्र विस्तार है। इसके अवयव $\frac{f(x)}{g(x)}$ के रूप के व्यंजक होते हैं, जहां $f(x), g(x) \in F[x]$ और $g(x) \neq 0$.

हम एक अन्य विधि से भी $F[x]$ से क्षेत्र F का क्षेत्र विस्तार प्राप्त कर सकते हैं। उच्चिष्ठ गुणजावलियों के सापेक्ष $F[x]$ के विभाग वलयों पर विचार कीजिए। आप जानते हैं कि $F[x]$ में गुणजावली उच्चिष्ठ होती है यदि और केवल यदि यह F पर किसी अखंडनीय बहुपद से जनित होती हो। अतः $F[x] / < f(x) >$ एक क्षेत्र होता है यदि और केवल यदि $f(x)$, F पर अखंडनीय हो।

अब, यदि $f(x) \in F[x]$ ऐसा हो कि $\deg f(x) > 0$, तो हम दिखाएंगे कि F से $F[x] / < f(x) >$ तक एक क्षेत्र एकैक समाकारिता होता है। इसका मतलब होगा कि $F[x] / < f(x) >$ में F की एक तुल्याकारी प्रति है;

अतः हम कह सकते हैं कि यह वलय F को आविष्ट करता है।

तो आइए, हम फलन

$\phi : F \to F[x] / < f(x) > : \phi(a) = a + < f(x) >$

से परिभाषित करें।

तब, $\phi(a+b) = \phi(a) + \phi(b)$, और

$\phi(ab) = \phi(a)\phi(b)$.

अतः ϕ एक वलय समाकारिता है।

Ker ϕ क्या होगा ?

$$\text{Ker}\,\phi = \{ a \in F \mid a + < f(x) > = < f(x) > \}$$

$$= \{ a \in F \mid a \in < f(x) > \}$$

$$= \{ a \in F \mid f(x) \mid a \}$$

$$= \{0\}, \text{ क्योंकि } \deg f(x) > 0 \text{ और } \deg a \le 0.$$

इस तरह, ϕ, 1–1 है। अतः यह एक आविष्टि (inclusion) है। अतः $F[x] / < f(x) >$, F को आविष्ट करता है। अतः यदि f(x), F[x] में अखंडनीय हो, तो $F[x] / < f(x) >$, F का क्षेत्र विस्तार होगा।

अब एक संबंधित प्रश्न।

E9) निम्नलिखित वलयों से कौन से वलय **Q** के क्षेत्र विस्तार हैं ?

क) $\mathbf{Q}[x] / < x^3 + 10 >$,

ख) $\mathbf{R}[x] / < x^2 + 2 >$,

ग) **Q**,

घ) $\mathbf{Q}[x] / < x^2 - 5x + 6 >$.

तो, अब तक हमने किसी क्षेत्र F के क्षेत्र विस्तारों पर काफ़ी चर्चा कर ली है। आइए, अब हम ऐसे क्षेत्रों पर विचार करें, जिनमें से किसी एक का विस्तार F है।

15.3.1 अभाज्य क्षेत्र

आइए, हम कोई क्षेत्र F लें। क्या हम इसके उपक्षेत्रों के बारे में कुछ कह सकते हैं ? हाँ, एक उपक्षेत्र को पहचान सकते हैं। आइए, हम इस चौंकाने वाले और उपयोगी तथ्य को सिद्ध करें। इसे सिद्ध करने से पहले हमारा सुझाव है कि आप इकाई 12 के प्रमेय 3, 4 और 8 को जल्दी से दोहरा लें।

तो आइए, परिणाम देखें।

प्रमेय 6 : प्रत्येक क्षेत्र का एक उपक्षेत्र या **Q** के तुल्याकारी होता है या $\mathbf{Z}_p$ के, किसी अभाज्य संख्या p के लिए ।

उपपत्ति : मान लीजिए F एक क्षेत्र है। फलन

$f : \mathbf{Z} \to F : f(n) = n \cdot 1 = 1 + 1 + \ldots\ldots + 1$ (n बार)
को परिभाषित कीजिए।

इकाई 12 के E11 में आपने दिखाया है कि f एक वलय समाकारिता है और Ker f = p **Z**, जहाँ p, क्षेत्र F का अभिलक्षणिक है।

अब, इकाई 12 के प्रमेय 8 से आप जानते हैं कि char F = 0 या char F = p, जो एक अभाज्य है। तो आइए हम इन दोनों स्थितियों पर अलग-अलग विचार करें ।

स्थिति 1 (char $F = 0$) : इस स्थिति में f, 1–1 है। $\therefore \mathbf{Z} \simeq f(\mathbf{Z})$. अतः $f(\mathbf{Z})$ क्षेत्र F में आविष्ट एक पूर्णांकीय प्रांत है। और क्योंकि F एक क्षेत्र है, इसलिए यह $f(\mathbf{Z})$ के विभाग क्षेत्र को भी आविष्ट करेगा; और यह क्षेत्र $\mathbf{Z}$ के विभाग क्षेत्र, अर्थात् $\mathbf{Q}$ के तुल्याकारी होगा। इस तरह, F का एक उपक्षेत्र $\mathbf{Q}$ के तुल्याकारी होगा।

स्थिति 2 (किसी अभाज्य p के लिए, char $F = p$) : क्योंकि p एक अभाज्य संख्या है, इसलिए $\mathbf{Z}/p\mathbf{Z}$ एक क्षेत्र है। और, समाकारिता के मूल प्रमेय को f पर लागू करने पर हमें $\mathbf{Z}/p\,\mathbf{Z} \simeq f(\mathbf{Z})$ प्राप्त होता है। इस तरह, $f(\mathbf{Z})$, $\mathbf{Z}_p$ के तुल्याकारी है और F में आविष्ट है। अतः F का एक उपक्षेत्र $\mathbf{Z}_p$ के तुल्याकारी है।

आइए, हम इसी प्रमेय 6 को दूसरे शब्दों में कहें। इस प्रमेय के अनुसार :

मान लीजिए F एक क्षेत्र है।

i) **यदि char $F = 0$, तो F का एक उपक्षेत्र $\mathbf{Q}$ के तुल्याकारी होता है।**

ii) **यदि char $F = p$, तो F का एक उपक्षेत्र $\mathbf{Z}_p$ के तुल्याकारी होता है।**

$\mathbf{Q}$ और $\mathbf{Z}_p$ (जहाँ p एक अभाज्य संख्या है) के इस गुण के कारण इन क्षेत्रों को हम अभाज्य क्षेत्र (prime field) कहते हैं। इस तरह, अभाज्य क्षेत्र $\mathbf{Q}, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_5$, आदि हैं।

प्रमेय 6 में प्राप्त अभाज्य क्षेत्र के तुल्याकारी उपक्षेत्र को हम दिए हुए क्षेत्र का **अभाज्य उपक्षेत्र** (prime subfield) कहते हैं।

आइए, हम प्रमेय 6 को दूसरे शब्दों में फिर से लिखें, इस दफ़ा क्षेत्र विस्तार का प्रयोग करके। इस प्रमेय के अनुसार **प्रत्येक क्षेत्र किसी अभाज्य क्षेत्र का क्षेत्र विस्तार होता है।**

अब, मान लीजिए क्षेत्र F क्षेत्र K का एक विस्तार है। क्या K और F के अभाज्य उपक्षेत्र तुल्याकारी हैं ? इस प्रश्न का उत्तर पाने के लिए आइए हम char K और char F पर विचार करें। हम जानना चाहते हैं कि char K = char F या नहीं। क्योंकि F, K का एक क्षेत्र विस्तार है, इसलिए F और K के तत्समक बराबर होंगे, अर्थात् 1, अतः ऐसा न्यूनतम धन पूर्णांक n जिससे कि $n \,.\, 1 = 0$, F और K दोनों के लिए बराबर होगा। इस तरह, char K = char F. अतः K और F के अभाज्य उपक्षेत्र तुल्याकारी हैं।

क्या आप अब नीचे दिए गए प्रश्न हल कर सकते हैं ?

E10) दिखाइए कि किसी क्षेत्र का लघुतम उपक्षेत्र उस क्षेत्र का अभाज्य उपक्षेत्र है।

E11) मान लीजिए F एक क्षेत्र है, जिसके कोई उचित उपक्षेत्र नहीं हैं। दिखाइए कि F किसी अभाज्य क्षेत्र के तुल्याकारी है।

E12) $\mathbf{R}$, $\mathbf{Z}$ और इकाई 12 के E15 में दिए गए क्षेत्र के अभाज्य उपक्षेत्र प्राप्त कीजिए।

E13) दिखाइए कि यदि किसी दिए हुए क्षेत्र का अभिलक्षणिक ज्ञात हो, तो उसका अभाज्य उपक्षेत्र प्राप्त किया जा सकता है; और इसका विलोम भी सही होता है।

E10 और E11 से एक अति महत्वपूर्ण तथ्य प्राप्त होता है, अर्थात्

एक क्षेत्र अभाज्य क्षेत्र होता है यदि और केवल यदि इसका कोई उचित उपक्षेत्र न हो।

आइए, अब हम क्षेत्र $\mathbf{Z}_p$ के कुछ क्षेत्र विस्तारों पर विचार करें।

15.3.2 परिमित क्षेत्र

आप परिमित क्षेत्रों $\mathbf{Z}_p$ से काफ़ी परिचित हो चुके हैं। अब हम इन क्षेत्रों के क्षेत्र विस्तारों पर चर्चा करेंगे। आप जानते हैं कि किसी भी परिमित क्षेत्र F का अभिलक्षणिक p होता है, जहाँ p एक अभाज्य संख्या है। और, तब F, $\mathbf{Z}_p$ का एक विस्तार होता है। मान लीजिए F में q अवयव हैं। तब q, p का एक घात होगा। इसी तथ्य को अब हम सिद्ध करेंगे।

प्रमेय 7 : मान लीजिए F, q अवयवों और अभिलक्षणिक p वाला एक परिमित क्षेत्र है। तब किसी धन पूर्णांक n के लिए $q = p^n$.

इस परिणाम की उपपत्ति में सदिश समष्टि (vector space) और उसके आधार (basis) की संकल्पनाओं का प्रयोग किया जाता है। इन पर चर्चा रैखिक बीजगणित के पाठ्यक्रम के खंड 1 में की जा चुकी है। यदि आप

उपपत्ति को समझना चाहते हैं तो हमारा सुझाव है कि आप रैखिक बीजगणित के पाठ्यक्रम की इकाइयाँ 3 और 4 को जल्दी से दोहरा लें। और यदि उपपत्ति में आपको रुचि नहीं है, तो आप इसे छोड़ सकते हैं।

प्रमेय 7 की उपपत्ति : क्योंकि char $F = p$, इसलिए F का $\mathbf{Z}_p$ के तुल्याकारी एक अभाज्य उपक्षेत्र होता है। अतः यदि हम मान लें कि F का उपक्षेत्र $\mathbf{Z}_p$ है, तो इससे कुछ नहीं बिगड़ता। पहले हम दिखाएंगे कि $\mathbf{Z}_p$ पर F एक परिमित-विम सदिश समष्टि है।

याद करें कि क्षेत्र K पर समुच्चय V एक सदिश समष्टि होता है यदि

i) हम V पर एक द्वि-आधारी संक्रिया + परिभाषित कर सकते हैं जिससे कि $(V, +)$ एक आबेली समूह हो,

ii) हम एक "अदिश गुणन" (scalar multiplication) : $K \times V \to V$ परिभाषित कर सकते हैं जिससे कि $\forall\ a, b \in K$ और $v, w \in V$

$a.(v + w) = a.v + a.w$

$(a + b).v = a.v + b.v$

$(ab).v = a.(b.v)$

$1.v = v.$

अब, हम जानते हैं कि $(F, +)$ एक आबेली समूह है। हम यह भी जानते हैं कि F में गुणन उन सभी प्रतिबंधों को संतुष्ट करता है जिन्हें अदिश गुणन को संतुष्ट करना चाहिए। इस तरह, $\mathbf{Z}_p$ पर F एक सदिश समष्टि है। क्योंकि F एक परिमित क्षेत्र है, इसलिए $\mathbf{Z}_p$ पर इसकी विमा परिमित होगी। मान लीजिए कि $\dim_{\mathbf{Z}_p} F = n$. तब हम $a_1, \ldots, a_n \in F$ प्राप्त कर सकते हैं जिनसे कि

$$F = \mathbf{Z}_p a_1 + \mathbf{Z}_p a_2 + \ldots\ldots + \mathbf{Z}_p a_n.$$

हम दिखाएंगे कि F के p^n अवयव हैं। अब F के किसी भी अवयव का रूप होगा —

$$b_1 a_1 + b_2 a_2 + \ldots\ldots + b_n a_n, \text{ जहां } b_1, \ldots\ldots, b_n \in \mathbf{Z}_p.$$

अब, क्योंकि $o(\mathbf{Z}_p) = p$, इसलिए b_1 इसके p अवयवों में से कोई भी एक अवयव हो सकता है। इसी प्रकार, $b_2, b_3, \ldots, b_n$ में से प्रत्येक को p तरह से चुन सकते हैं। और इनमें से प्रत्येक विकल्प के संगत F का एक अलग अवयव होता है। इस तरह, F में अवयवों की संख्या $p \times p \times \ldots \times p$ (n बार) $= p^n$ है।

इस परिणाम की उपयोगिता लगभग वही है जो कि लग्रांज प्रमेय की है। उदाहरण के लिए, इस परिणाम के प्रयोग से हम जान जाते हैं कि कोटि 26 वाला कोई क्षेत्र नहीं होता है। परंतु, क्या कोई कोटि 25 वाले क्षेत्र हैं ? क्या प्रमेय 7 से इस प्रश्न का उत्तर मिलता है ? यह प्रमेय केवल इतना बताता है कि कोई कोटि 25 वाला क्षेत्र **हो सकता है**। लेकिन इससे यह नहीं पता चलता कि कोई कोटि 25 वाला क्षेत्र **है**। निम्नलिखित परिणाम से हमें इच्छित उत्तर मिलता है। हम इसकी उपपत्ति इस पाठ्यक्रम में नहीं देंगे, लेकिन इसका प्रयोग करेंगे। इस परिणाम को 1893 में अमरीकी गणितज्ञ ई. एच. मुअर ने प्रस्तुत किया था।

किसी परिमित क्षेत्र की कोटि उसमें आविष्ट होने वाले अवयवों की संख्या है।

प्रमेय 8 : किसी भी अभाज्य संख्या p और $n \in \mathbf{N}$ के लिए p^n अवयव वाला एक क्षेत्र है। और, समान कोटि वाले परिमित क्षेत्र तुल्याकारी होते हैं।

अब आप परिमित क्षेत्रों से संबद्ध अपनी जानकारी की सहायता से निम्नलिखित प्रश्नों को हल कर सकते हैं। पहला प्रश्न इकाई 13 के E 13 का व्यापकीकरण है।

E14) मान लीजिए F, p^n अवयवों वाला एक परिमित क्षेत्र है। दिखाइए कि $a^{p^n} = a\ \forall\ a \in F$, और इस तरह दिखाइए कि $x^{p^n} - x = \prod_{a_i \in F} (x - a_i)$.

(संकेतः ध्यान दीजिए कि $(F \setminus \{0\}, .)$ कोटि $p^n - 1$ वाला एक समूह है।)

E15) मान लीजिए F, p^n अवयवों वाला एक परिमित क्षेत्र है। $f : F \to F$: $f(a) = a^p$ परिभाषित कीजिए। दिखाइए कि f, F की एक स्वाकारिता (automorphism) है जिसकी कोटि n है, अर्थात् f एक ऐसी तुल्याकारिता है जिसके लिए $f^n = I$, और $r < n$ के लिए, $f^r \neq I$.

गणितज्ञ जॉर्ज फ्रोबिनियस (1848-1917) के नाम से f को F की **फ्रोबिनियस स्वाकारिता** कहते हैं।

E16) मान लीजिए F एक ऐसा क्षेत्र है जिसके लिए $a \in F$ यदि और केवल यदि a, $x^{27} - x \in F[x]$ का मूल हो। तब

(क) char F क्या है ?

(ख) क्या $\mathbf{Z}_2 \subseteq F$?

(ग) क्या $\mathbf{Q} \subseteq F$?

(घ) क्या $F \subseteq \mathbf{Q}$? क्यों ?

E17) कोई भी दो अनंत क्षेत्र तुल्याकारी होते हैं। सत्य या असत्य ? क्यों ? याद रखें कि तुल्याकारी संरचनाओं के समान बीजीय गुण होने चाहिए।

अब हम क्षेत्र विस्तार पर अपनी चर्चा समाप्त कर रहे हैं। आइए देखें कि हमने इस इकाई में क्या किया है।

15.4 सारांश

इस इकाई में हमने निम्नलिखित तथ्यों पर चर्चा की है।

1) गाउस प्रमेयिका, अर्थात् पूर्वग बहुपदों का गुणनफल पूर्वग होता है।

2) $\mathbf{Z}$ और $\mathbf{Q}$ पर बहुपदों के लिए आइसनस्टाइन का अखंडनीयता निकष। इसके अनुसार, यदि

   $f(x) = a_0 + a_1 x + \ldots\ldots + a_n x^n \in \mathbf{Z}[x]$ और एक अभाज्य $p \in \mathbf{Z}$ ऐसा हो कि

   i) $p \mid a_i \ \forall\ i = 0, 1, \ldots, n-1,$

   ii) $p \nmid a_n$, और

   iii) $p^2 \nmid a_0$,

   तो $\mathbf{Z}$ पर (और इस तरह $\mathbf{Q}$ पर) $f(x)$ अखंडनीय होता है।

3) किसी $n \in \mathbf{N}$ के लिए हम $\mathbf{Q}$ पर घात n वाला एक अखंडनीय बहुपद प्राप्त कर सकते हैं।

4) उपक्षेत्रों और क्षेत्र विस्तारों की परिभाषाएं और उनके उदाहरण।

5) $F[x]$ से क्षेत्र F के क्षेत्र विस्तार प्राप्त करने की विभिन्न विधियाँ।

6) प्रत्येक क्षेत्र का एक उपक्षेत्र होता है जो किसी अभाज्य क्षेत्र के तुल्याकारी होता है। अभाज्य क्षेत्र $\mathbf{Q}$ या किसी अभाज्य p के लिए $\mathbf{Z}_p$ होते हैं।

7) किसी परिमित क्षेत्र F में अवयवों की संख्या p^n है, जहां char F = p और $\dim_{\mathbf{Z}_p} F = n$.

8) यदि एक अभाज्य संख्या p और $n \in \mathbf{N}$ दिया हुआ हो तो p^n अवयव आविष्ट करने वाले एक क्षेत्र का अस्तित्व होता है। समान कोटि वाले परिमित क्षेत्र तुल्याकारी होते हैं।

9) यदि F, p^n अवयवों वाला एक परिमित क्षेत्र हो, तो $x^{p^n} - x$, F पर p^n रैखिक बहुपदों का गुणनफल होता है।

अब हम इस इकाई और इस पाठ्यक्रम के अंत पर पहुंच गए हैं। हम उम्मीद करते हैं कि आपको समूह, वलय और क्षेत्र सिद्धांत की मौलिक जानकारी मिल गई होगी। हम यह भी आशा करते हैं कि आपको यह पाठ्यक्रम रुचिकर लगा होगा।

15.5 हल/उत्तर

E1) क) 1 ख) 7 ग) 5

E2) मान लीजिए $f(x) = a_0 + a_1 x + \ldots\ldots + a_n x^n$ और $f(x)$ का आधेय d है। मान लीजिए $a_i = db_i \ \forall i = 0, 1, \ldots, n$. तब $b_0, b_1, \ldots\ldots b_n$ का gcd, 1 होगा। इस तरह,

$g(x) = b_0 + b_1x + ... + b_n x^n$ पूर्णांग है और,

$f(x) = db_0 + db_1 x + ... + db_n x^n$

$= d(b_0 + b_1x + ... + b_n x^n)$

$= d\, g(x).$

E3) $f(x) = x^n - p = a_0 + a_1x + ... + a_n x^n$,

जहां $a_0 = -p,\ a_1 = 0 = \ .....\ = a_{n-1},\ a_n = 1.$

इस तरह, $p | a_i\ \forall\ i=0, 1, ..., n-1,\ p^2 \nmid a_0,\ p \nmid a_n$. इसलिए, आइसनस्टाइन निकष के अनुसार , $\mathbf{Q}$ पर $f(x)$ अखंडनीय है।

E4) आवश्यक नहीं है।

उदाहरण के लिए, ऐसा कोई p नहीं है जो उदाहरण 3 के $f(x)$ के लिए उन प्रतिबंधों को संतुष्ट करता हो ।

E5) सभी। (क) और (ख), आइसनस्टाइन निकष से; और (ग) क्योंकि कोई भी रैखिक बहुपद अखंडनीय होता है।

E6) क्योंकि $a \neq 0, \pm 1$, इसलिए एक ऐसा अभाज्य q है जिससे कि $q \mid a$. और $q^2 \nmid a$, हमारी परिकल्पना से। तब आइसनस्टाइन निकष में q को अभाज्य लेकर हम देख सकते हैं कि $\mathbf{Z}[x]$ में $x^2 + a$ अखंडनीय है, और इसलिए अभाज्य है। अतः, $< x^p + a >$, $\mathbf{Z}[x]$ की एक अभाज्य गुणजावली है। अब परिणाम ज़ाहिर है।

E7) इकाई 13 के E13 से हम जानते हैं कि

$\bar{a}^p = \bar{a}\ \forall\ \bar{a} \in \mathbf{Z}_p.$

अब $x^p + \bar{a} \in \mathbf{Z}_p[x]$ लीजिए।

$\overline{p-a}$ इस बहुपद का एक शून्यक है, क्योंकि $\mathbf{Z}_p$ में

$(\overline{p-a})^p + \bar{a} = \overline{p-a} + \bar{a} + \bar{p} = \bar{0}.$

इस तरह, $\mathbf{Z}_p$ पर $x^p + \bar{a}$ खंडनीय है।

E8) (क) $\mathbf{Q} + i\,\mathbf{Q}$, $\mathbf{C}$ का एक अरिक्त उपसमुच्चय है। अब, मान लीजिए $a + ib$ और $c + id$, $\mathbf{Q} + i\mathbf{Q}$ में हैं। तब $(a+ib) - (c+id) = (a-c) + i(b-d) \in \mathbf{Q} + i\mathbf{Q}$. और आगे, मान लीजिए कि $c + id \neq 0$, जिससे कि $c^2 + d^2 \neq 0$.

तब $(c + id)^{-1} = \dfrac{c - id}{c^2 + d^2}$.

इस तरह, $(a + ib)\,(c + id)^{-1} = (a + ib)\ \dfrac{(c - id)}{c^2 + d^2}$

$$= \frac{ac + bd}{c^2 + d^2} + i\frac{(bc - ad)}{c^2 + d^2} \in \mathbf{Q} + i\mathbf{Q}.$$

इस तरह, $\mathbf{Q} + i\mathbf{Q}$, $\mathbf{C}$ का एक उपक्षेत्र है।

ख) $2 \in \mathbf{Z} + \sqrt{2}\,\mathbf{Z}$, परंतु $2^{-1} \notin \mathbf{Z} + \sqrt{2}\,\mathbf{Z}$.

अतः $\mathbf{Z} + \sqrt{2}\,\mathbf{Z}$ एक क्षेत्र नहीं है और इस तरह, यह $\mathbf{R}$ का उपक्षेत्र नहीं है।

E9) (क), (ख) और (ग)।

E10) मान लीजिए F एक क्षेत्र है और K, F का एक उपक्षेत्र है। तब, हमने अभी देखा है कि K और F दोनों के तुल्याकारी अभाज्य उपक्षेत्र हैं।

अतः, K, F के अभाज्य उपक्षेत्र को आविष्ट करता है। इस तरह, हमने दिखाया है कि F का प्रत्येक उपक्षेत्र उसके अभाज्य उपक्षेत्र को आविष्ट करता है। अतः अभाज्य उपक्षेत्र F का लघुतम उपक्षेत्र है।

E11) F अभाज्य उपक्षेत्र को अवश्य आविष्ट करेगा। परंतु यह कोई उचित उपक्षेत्र आविष्ट नहीं करता। अतः यह स्वयं अपना अभाज्य उपक्षेत्र होगा। अर्थात् F अभाज्य क्षेत्र के तुल्याकारी होगा।

E12) Q, Z_5, Z_2 क्योंकि इनके अभिलक्षणिक क्रमशः 0, 5 और 2 हैं।

E13) मान लीजिए F एक क्षेत्र है। सबसे पहले मान लीजिए कि char F = p ज्ञात है। तब प्रमेय 6 से हम F के अभाज्य उपक्षेत्र को प्राप्त कर सकते हैं।

विलोमतः, मान लीजिए K, F का अभाज्य उपक्षेत्र है। तब हमें char K ज्ञात हो जाता है, और जैसा कि E10 से पहले दिखाया गया है, char F = char K. इस तरह हमें char F प्राप्त हो जाता है।

E14) क्योंकि $(F\setminus\{0\}, .)$ कोटि p^n-1 वाला एक समूह है, इसलिए $a^{p^n-1} = 1 \; \forall \; a \in F\setminus\{0\}$.

$\therefore a^{p^n} = a \; \forall \; a \in F\setminus\{0\}$. और $0^{p^n} = 0$. इस तरह, $a^{p^n} = a \; \forall \; a \in F$.

अब, इकाई 13 के प्रमेय 7 के अनुसार, F में $x^{p^n} - x \in F[x]$ के अधिक से अधिक p^n मूल हो सकते हैं। और, F के p^n अवयवों में से प्रत्येक अवयव, एक मूल है। इस तरह, ये ही $x^{p^n} - x$ के सभी मूल हैं।

$\therefore x^{p^n} - x = \prod_{a_i \in F} (x-a_i)$.

E15) $f(a+b) = (a+b)^p = a^p + b^p$ (इकाई 12 के E10 से)

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

$f(ab) = (ab)^p = a^p b^p = f(a) f(b)$.

इकाई 12 के E10 (ग) के अनुसार f, 1–1 है। अतः Imf के अवयवों की संख्या उतनी ही है जितनी कि f के प्रांत, अर्थात् F के अवयवों की संख्या और $\text{Im} f \subseteq F$.

$\therefore \text{Im} f = F$. अर्थात् f आच्छादक है। अतः f एक स्वाकारिता है।

अब, $f^n(a) = [f(a)]^n = (a^p)^n = a^{p^n} = a \; \forall \; a \in F$.

$f^n = I$.

और $r < n$ के लिए, $f^r(a) = a^{p^r}$.

अब, $a^{p^r} = a \; \forall \; a \in F$ नहीं हो सकता, क्योंकि इसका अर्थ होगा कि बहुपद $x^{p^r} - x \in F[x]$ के p^r से अधिक मूल हैं। यह इकाई 13 के प्रमेय 7 का अंतर्विरोध है। अतः किसी $a \in F$ के लिए $f^r(a) \neq a$.

$\therefore f^r \neq I$. यदि $r < n$.

अतः $o(f) = n$.

E16) $a \in F$ यदि और केवल यदि $a^{27} = a$, अर्थात् $a^{3^3} = a$.

(क) char F = 3.

(ख) नहीं, क्योंकि char $Z_2 \neq$ char F.

(ग) नहीं।

(घ) नहीं, क्योंकि $F \subseteq Q \Rightarrow$ char F = char Q = 0.

E17) असत्य।

उदाहरण के लिए, **Q** और **R** अनंत हैं, परंतु **Q** का कोई उचित उपक्षेत्र नहीं है, जबकि **R** का है। इस तरह, **Q** और **R** तुल्याकारी नहीं हैं।

शब्दावली

अखंडनीय बहुपद	irreducible polynomial
अग्रग-गुणांक	leading coefficient
अद्वितीय गुणनखंडन प्रांत	unique factorisation domain, UFD
अनिर्धार्य	indeterminate
अभाज्य उपक्षेत्र	prime subfield
अभाज्य गुणजावली	prime ideal
अभिलक्षणिक	characteristic
अल्पिष्ठ अवयव	minimal element
आइसनस्टाइन नियम	Eisenstein's criterion
आधार	basis
आधेय	content
आरोही शृंखला प्रतिबंध	ascending chain condition
आविष्टि फलन	inclusion map
उच्चिष्ठ गुणजावली	maximal ideal
उपक्षेत्र	subfield
एकैक समाकारिता	monomorphism
क्रमित युग्म	ordered pair
क्षेत्र विस्तार	field extension
गुणांक	coefficient
निरसन नियम	law of cancellation
परिमित क्षेत्र	finite field
पूर्णांकीय प्रांत	integral domain
पूर्वग बहुपद	primitive polynomial
बहुकता	multiplicity
बहुपद वलय	polynomial ring
बीजगणित का मूल प्रमेय	fundamental theorem of algebra
भागफल	quotient
महत्तम सार्व भाजक	greatest common divisor, gcd
मात्रक	unit
मानक फलन	norm function
मुख्य गुणजावली प्रांत	principal ideal domain, PID
मूल	root
यूक्लिडीय प्रांत	Euclidean domain
यूक्लिडीय मानांकन	Euclidean valuation
विभाग क्षेत्र	field of quotients
विभाग वलय	quotient ring

विभाजन-कलन विधि	division algorithm
विभाजन वलय	division ring
विषम क्षेत्र	skew field
वृत्तविभाजनिक बहुपद	cyclotomic polynomial
शून्यक	zero or root
शून्य का भाजक	zero-divisor
शून्येतर	non-zero
शेषफल	remainder
सदिश समष्टि	vector space
सहचारी	associate
सार्व भाजक	common divisor
स्वाकारिता	automorphism

शुद्धि पत्र
MTE–06 (खंड 1)

<table>
<tr><th>पृष्ठ सं.</th><th>पंक्ति सं.</th><th>होना चाहिए</th></tr>
<tr><td>6</td><td>1 (ऊपर से)</td><td>$\{ x \vert x$, P को संतुष्ट करता है $\}$ ...</td></tr>
<tr><td>9</td><td>हाशिए में दी गई टिप्पणी</td><td>यूनानी अक्षर "$\in$" "का सदस्य है" को ....</td></tr>
<tr><td>12</td><td>10 (ऊपर से)</td><td>...... $A = \{1, 2\}$ ....</td></tr>
<tr><td>12</td><td>18 (ऊपर से)</td><td>ख) $A \subsetneq B \Rightarrow A \cap B = A$</td></tr>
<tr><td>24</td><td>16 (नीचे से)</td><td>.... लीजिए, अर्थात् $1 = 0.b + 1$.</td></tr>
<tr><td>33</td><td>12 (ऊपर से)</td><td>$f \circ g \in \mathcal{F}(X)\ \forall$....</td></tr>
<tr><td>34</td><td>3 (नीचे से)</td><td>.... द्वि-आधारी संक्रिया $\oplus : \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ ....</td></tr>
<tr><td>35</td><td>सारणी की पहली पंक्ति</td><td>$\begin{array}{|c|ccc|}\hline \cdot & -1 & 0 & 1 \\ \hline\end{array}$</td></tr>
<tr><td>36</td><td>9 (ऊपर से)</td><td>.... $\neq 1 * 2$. अर्थात् $*$ क्रमविनिमेय नहीं है।</td></tr>
<tr><td>46</td><td>12 (नीचे से)</td><td>$\begin{pmatrix} 1 & 2 \ldots\ldots & n \\ f(1) & f(2) \ldots\ldots & f(n) \end{pmatrix}$</td></tr>
<tr><td>48</td><td>7 (नीचे से)</td><td>.... $= y \oplus x\ \forall\ x, y \in \mathbf{R}$.</td></tr>
<tr><td>49</td><td>18 (नीचे से)</td><td>$= (ace, (bc + d)\, c + f)$</td></tr>
<tr><td>50</td><td>E13) की सारणी की पहली पंक्ति</td><td>$\begin{array}{|c|cccc|}\hline \cdot & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \hline\end{array}$</td></tr>
<tr><td>56</td><td>13 (ऊपर से)</td><td>..... अर्थात् $s\mathbf{Z} \subseteq H$.</td></tr>
<tr><td>59</td><td>हाशिए में दी गई टिप्पणी</td><td>"$\not\leq$" "का उपसमूह नहीं है" ....</td></tr>
<tr><td>59</td><td>3 (नीचे से)</td><td>.... अतः $A \cup B \not\leq G$. ध्यान ....</td></tr>
<tr><td>61</td><td>15 (नीचे से)</td><td>$\langle S \rangle = \{ a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k} \vert a_i \in S$, ...</td></tr>
<tr><td>62</td><td>हाशिए में दी गई टिप्पणी</td><td>........., यदि $H \subsetneq G$.</td></tr>
<tr><td>66</td><td>1 (नीचे से)</td><td>.... $x + H = \{x + h \vert h \in H\}$ है।</td></tr>
<tr><td>67</td><td>9 (नीचे से)</td><td>.... $Hx \subseteq H$.</td></tr>
<tr><td>69</td><td>19 (ऊपर से)</td><td>.... $x \sim y$ और $y \sim z$, तो $xy^{-1} \in H$ ....</td></tr>
<tr><td>70</td><td>17 (नीचे से)</td><td>.... $o(S_n) = n!$.</td></tr>
<tr><td>71</td><td>(ऊपर से) 16 के साथ हाशिए में टिप्पणी</td><td>किसी भी परिमित समुच्चय A के लिए $\vert A \vert$, A के अवयवों की संख्या को प्रकट करता है।</td></tr>
<tr><td>71</td><td>2 (नीचे से)</td><td>.... न्यूनतम धन पूर्णांक n है .....</td></tr>
<tr><td>72</td><td>6 (नीचे से)</td><td>.... मान लीजिए कि $(g^m)^t = (g^m)^w$ ....</td></tr>
<tr><td>76</td><td>2 (ऊपर से)</td><td>.... $h, h' \in H$ के लिए $hx = h'x \Rightarrow$ ....</td></tr>
<tr><td>76</td><td>6 (नीचे से)</td><td>.... Z_{23} में $(\overline{3})^{\phi(23)} = \overline{1}$</td></tr>
<tr><td>76</td><td>1 (नीचे से)</td><td>.... और $\phi(p) = p - 1$ का प्रयोग ....</td></tr>
</table>

शुद्धि पत्र

MTE-06 (खंड 2)

पृष्ठ सं.	पंक्ति सं.	होना चाहिए
4	4 (नीचे से)	$(i_1\, i_2 \ldots i_r)$ एक r-चक्र
12	4 (ऊपर से)	.... तब $x^{-1}y^{-1}xy$ को x और y का
17	21 (ऊपर से)	$f(x) *_2 f(x^{-1}) = f(x *_1 x^{-1}) = \ldots$
17	2 (नीचे से)	$= \{x \in G \mid x \in H\}, \ldots$
18	14 (नीचे से)	.... अर्थात् $\sigma(k) = k \; \forall \; k = m+1, \ldots, n$.
22	17 (ऊपर से)	$f\|_K : K \to f(K)$ ..... संकुचन $f\|_K$
26	4 (नीचे से)	$hkK = hK$, क्योंकि $k \in K$.
29	9 (ऊपर से)	... $\exists\, f_{g^{-1}} \in \operatorname{Inn} G$,
29	11 (ऊपर से)	इसी प्रकार, $f_{g^{-1}} \circ f_g = I_G$.
29	12 (ऊपर से)	इस तरह, $f_{g^{-1}} = [f_g]^{-1}, \ldots$
42	5 (ऊपर से)	... समूह A_n को डिग्री n का एकांतर समूह .....
42	16 (ऊपर से)	$(i_1\, i_2 \ldots i_r) = (i_1\, i_r)(i_1\, i_{r-1}) \ldots (i_1\, i_2)$,
48	13 (नीचे से)	$G = G_1 \times G_2 \times \ldots \times G_n$ और
49	2 (ऊपर से)	$\ldots = \pi_1(ac, bd)$
49	3 (ऊपर से)	$= ac$
50	7 (नीचे से)	.... $\therefore h_1^{-1}h = k_1k^{-1}$. अब....
54	1 (नीचे से)	$\Rightarrow x^{r^2-1} = e$.

शुद्धि पत्र
MTE–06 (खंड 3)

पृष्ठ सं.	पंक्ति सं.	होना चाहिए
5	15 (नीचे से)	.... उद्देश्यों को पा लें।
10	चित्र 2 का शीर्षक	[0, 1] पर f और (–f) के आलेख
11	18 (ऊपर से)	.... Map (X, R) में + और . परिभाषित ......
11	4 (नीचे से)	(G, *) के लिए ......
14	17 (नीचे से)	E13) उदाहरण 1, 2, 3, 4, 6, 7 में .....
15	1 (ऊपर से)	.... यदि और केवल यदि A और B .....
18	5 (ऊपर से)	E11) चूंकि $(a+b)^t = a^t + b^t$, ...
18	17 (ऊपर से)	$= c'$, क्योंकि....
22	7 (नीचे से)	$R/I = \{a + I \mid a \in R\}$.
24	4 (ऊपर से)	..... A – B भी X का परिमित उपसमुच्चय .....
24	19 (ऊपर से)	.... $x \in [0, 1]$ के लिए $0(x) = 0$ से.....
26	16 (ऊपर से)	ग) $IJ = \{x \in R \mid \ldots b_i \in J\}$
26	17 (ऊपर से)	R की गुणजावलियां हैं।
28	7 (ऊपर से)	तब $ab = (a'+x)(b'+y) = a'b' + (xb' + a'y + xy)$,
28	11 (नीचे से)	..... वजह से शब्द 'R मॉड I' का ....
28	1 (नीचे से)	$= o(R/I) = \dfrac{o(R)}{o(I)} = \ldots$
29	सारणियाँ	(नीचे देखें)

+	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{0}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{1}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$	$\bar{0}+I$
$\bar{2}+I$	$\bar{2}+I$	$\bar{3}+I$	$\bar{0}+I$	$\bar{1}+I$
$\bar{3}+I$	$\bar{3}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$

•	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{0}+I$	$\bar{0}+I$	$\bar{0}+I$	$\bar{0}+I$	$\bar{0}+I$
$\bar{1}+I$	$\bar{0}+I$	$\bar{1}+I$	$\bar{2}+I$	$\bar{3}+I$
$\bar{2}+I$	$\bar{0}+I$	$\bar{2}+I$	$\bar{0}+I$	$\bar{2}+I$
$\bar{3}+I$	$\bar{0}+I$	$\bar{3}+I$	$\bar{2}+I$	$\bar{1}+I$

पृष्ठ सं.	पंक्ति सं.	होना चाहिए
33	22 (ऊपर से)	मान लीजिए $s \in N$......
33	8 (नीचे से)	$= Z_s$
34	9 (नीचे से)	$\begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$ एक समाकारिता है।
34	1 (नीचे से)	$Y^c \in$ Ker f?.....
35	17 (ऊपर से)	इस तरह $B \in \mathrm{Im}\, f$.....
40	15 (ऊपर से)	.... f संयोजन $\psi \circ \eta$ है,...
43	26 (ऊपर से)	लिए $n \mid 12$, अर्थात्....
45	2 (नीचे से)	साहचर्य associative.

NOTES

NOTES

NOTES