इग्नू
जन-जन का
विश्वविद्यालय

इंदिरा गांधी राष्ट्रीय मुक्त विश्वविद्यालय
विज्ञान विद्यापीठ

BMTC-134

बीजगणित

किताब-I
समूह सिद्धांत

इकाई अनुसार पाठ्यक्रम रूपरेखा

किताब I समूह सिद्धांत

खंड 1 प्रारंभिक समूह सिद्धांत

इकाई 1: कुछ प्रारंभिक संकल्पनाएँ

इकाई 2: समूह

इकाई 3: उपसमूह

इकाई 4: चक्रीय समूह

खंड 2 प्रसामान्य उपसमूह और समूह समाकारिताएँ

इकाई 5: लग्रांज का प्रमेय

इकाई 6: प्रसामान्य उपसमूह

इकाई 7: विभाग समूह

इकाई 8: समूह समाकारिताएँ

इकाई 9: क्रमचय समूह

किताब II वलय सिद्धांत

खंड 3 वलयों से परिचय

इकाई 10: वलय

इकाई 11: उपवलय

इकाई 12: गुणजावलियाँ

इकाई13: वलय समाकारिताएँ

खंड 4 पूर्णांकीय प्राँत

इकाई 14: पूर्णांकीय प्राँत और क्षेत्र

इकाई 15: बहुपद वलय

इकाई16: बहुपदों के मूल और गुणनखंड

मार्च, 2021

ISBN-8]-

इंदिरा गाँधी राष्ट्रीय मुक्त विश्वविद्यालय के पाठ्यक्रमों के विषय में और अधिक जानकारी विश्वविद्यालय के कार्यालय मैदान गढ़ी, नई दिल्ली–110068 और इग्नू की वेबसाइट www.ignou.ac.in से प्राप्त की जा सकती है।

इंदिरा गांधी राष्ट्रीय मुक्त विश्वविद्यालय की ओर से प्रो. सुजाता वर्मा, निदेशक, विज्ञान विद्यापीठ द्वारा मुद्रित एवं प्रकाशित।

पाठ्यक्रम से परिचय

शब्द "बीजगणित" से आप पहले से परिचित हैं ही। आप यह भी जानते होंगे कि यह अरबी शब्द 'अल-जब्र' से आया है। पहले जमाने में बीजगणित का संबंध समीकरणों के हल प्राप्त करने से था। इसके बाद आया 'आधुनिक बीजगणित', जो ऐसा पारिभाषिक शब्द था जो चिरप्रतिष्ठित बीजगणित के अंतर्गत ही बारीक़ छानबीन से था। पाठ्यक्रम 'कलन' के खंड 1 में आप आधुनिक बीजगणित की कुछ संकल्पनाओं – जैसे समुच्चय और उन पर संक्रियाएँ, फलन, समुच्चय पर एक द्वि-आधारी संक्रिया, समतल ज्यामिति अध्ययन करने की बीजीय विधि, सम्मिश्र संख्याओं के गुण, $\mathbb{R}$ पर एक बहुपद क्या होता है, तथा कुछ बहुपद समीकरणों के हल – का अध्ययन कर चुके हैं। इस पाठ्यक्रम में आपने ये सब जो सीखा, उसे नींव मानते हुए आपको आगे ले जाएँगे।

इस पाठ्यक्रम में हम 'अमूर्त बीजगणित' पर ध्यान केन्द्रित करेंगे, जो कि आधुनिक बीजगणित का व्यापकीकरण है। **अमूर्त बीजगणित** में हम ऐसे बीजीय निकायों का अध्ययन करते हैं जो केवल अभिगृहीतों (axioms) द्वारा परिभाषित हैं। ये अभिगृहीत सामान्यतः वास्तविक स्थितियों से विकसित होते हैं। इस पाठ्यक्रम में, जिसमें **चार खंड शामिल हैं,** आप तीन मौलिक बीजीय निकायों, अर्थात्, समूहों, वलयों और क्षेत्रों का अध्ययन करेंगे।

खंड 1 में आप सीखेंगे कि एक समूह क्या होता है, तथा इस बीजीय निकाय के अनेक उदाहरणों और गुणों का अध्ययन करेंगे। आप अनेक प्रकार के समूहों का अध्ययन करेंगे, जिनमें अनेक अंतर तथा अनेक समानताएँ होंगी। यहाँ आप यह भी सीखेंगे कि एक उपसमूह क्या होता है। पूर्णांकों के समुच्चय से एक विशिष्ट प्रकार का समूह बनता है, जो चक्रीय समूह कहलाता है। ऐसे समूह के अनेक विशेष गुण होते हैं। इसी कारण से हम इस खंड में इस पर विशेष ध्यान देंगे।

खंड 2 में विभाग समूह कहलाने वाले एक विशिष्ट प्रकार के समूह पर हम ध्यान केन्द्रित करेंगे। जैसा कि आप देखेंगे, ऐसे समूह के लिए एक विशिष्ट प्रकार के उपसमूह की आवश्यकता होती है। आप ऐसे उपसमूहों का अध्ययन भी विस्तृत रूप से करेंगे। विभाग समूह का असली महत्व तब प्रदर्शित होता है जब एक समूह से एक अन्य समूह तक ऐसे फलन से सामना होता है जो प्राँत समूह की संक्रिया को 'बनाए रखने' के गुण को संतुष्ट करता है। ऐसे फलनों के महत्व तथा इनके विभाग समूहों के साथ संबंधों की चर्चा भी इस खंड में विस्तृत रूप से की जाएगी। अंत में, खंडों – 1 और 2 में आपके द्वारा समूहों के विभिन्न पहलुओं और गुणों के बारे में किए गए अध्ययन की एक विस्तृत स्थिति अध्ययन के रूप में, आप एक समुच्चय से स्वयं तक एकैकी आच्छादक फलनों का अध्ययन करेंगे।

खंड 3 में हम एक अन्य, परंतु संबंधित, बीजीय निकाय पर ध्यान केन्द्रित करने के लिए आगे बढ़ेंगे। यह वलय कहलाता है। इस खंड में आप वलय की परिभाषा के साथ उसके अनेक गुणों का अध्ययन करेंगे। यहाँ आप उपवलयों का, तथा विशिष्ट प्रकार के उपवलयों का, अध्ययन करेंगे। ये उपवलय ख़ास इसलिए हैं क्योंकि हमें इनकी मदद से ही विभाग वलयों को परिभाषित कर सकते हैं। अंत में, इस खंड में आप एक वलय से दूसरे वलय तक के एक विशेष प्रकार के फलनों के बारे में अध्ययन करेंगे। जैसे-जैसे आप इस खंड का अध्ययन करते जाएँगे, वैसे-वैसे आप देखेंगे कि किस प्रकार वलयों से संबंधित संकल्पनाएँ हैं। प्रथम दो खंडों में दी गई समूहों की संकल्पनाओं से मिलती-जुलती हैं।

खंड 4 में उन वलयों पर ध्यान केन्द्रित होगा जो कुछ विशेष गुणों को संतुष्ट करते हैं। विशिष्ट रूप से, आप एक अन्य महत्वपूर्ण बीजीय निकाय का अध्ययन करेंगे जो एक वलय तो है, पर वलय से कुछ अधिक भी है। यह है क्षेत्र की संकल्पना। आप देखेंगे कि वास्तविक संख्याओं के समुच्चय से, तथा सम्मिश्र संख्याओं के समुच्चय से क्षेत्र बनते हैं। इस खंड में आगे, हम $\mathbb{R}$ पर, $\mathbb{C}$ पर, तथा किसी भी क्षेत्र पर, बहुपदों के समुच्चयों के गुणों की चर्चा करेंगे।

आप शायद सोच रहे होंगे कि आपको इस पाठ्यक्रम का अध्ययन क्यों करना चाहिए। जैसे-जैसे आप इन खंडों का अध्ययन करते जाएँगे, आप अनुभव करेंगे कि आपके सोचने की विधि बदल रही है। आप देखेंगे कि किस प्रकार अमूर्त बीजगणित की विधियों से हम अनेक मिलते-जुलते बीजीय निकायों का अध्ययन केवल एक प्रतिनिधि निकाय का अध्ययन करके कर सकते हैं। इससे हमें निकायों के बारे में दीर्घ स्तर पर सोचने, परिशुद्ध और संक्षिप्त होने तथा अनेक समूहों या वलयों की संरचना को कम समय में समझने में सहायता मिलती है।

जो कुछ आप इस पाठ्यक्रम में अध्ययन करेंगे, उसके अनेक व्यावहारिक अनुप्रयोग हैं। आइए सबसे पहले हम समूह सिद्धांत के कुछ अनुप्रयोगों की बात करें। इस सिद्धांत का उपयोग भौतिकविदों और रसायनविदों द्वारा क्रिस्टल-विज्ञान, किरण-विश्लेषण, व्यापक आपेक्षिकता, ठोस अवस्था भौतिकी तथा मूलकण के आधुनिक सिद्धांत में किया जाता है। वस्तुतः, समूह सिद्धांत के प्रयोग से ही वैज्ञानिकों ने ओमेगा ऋण कण के अस्तित्व का पूर्वानुमान लगाया था। इन कणों की असली पहचान तो 1964 में जाकर ही हुई थी, पूर्वानुमान के काफ़ी सालों बाद।

आगे आइए वलयों और क्षेत्रों के कुछ अनुप्रयोगों को देखें। बहुपद वलयों और आव्यूह वलयों का उपयोग क्वाण्टम यांत्रिकी में किया जाता है। क्षेत्र सिद्धांत का प्रयोग आँकड़ों के संचारण क्षेत्र में त्रुटि का पता लगाने के लिए और त्रुटि-सुधार के लिए कार्यक्षम कोडों के निर्माण में किया जाता है। और, परिमित क्षेत्र सांख्यिकी में भी बहुत उपयोगी होते हैं।

अब, आप इस सामग्री का किस प्रकार अध्ययन करें, उसके बारे में भी हम कुछ शब्द कहना चाहेंगे। **हम यह मानकर इस पाठ्यक्रम को प्रस्तुत करेंगे कि आपने 'कलन' और 'वास्तविक विश्लेषण' के पाठ्यक्रमों का अध्ययन पहले ही कर लिया है।** इन खंडों में सामग्री को केवल पढ़ें ही नहीं। आपको इनमें प्रत्येक लिखित रेखा, विचार, उदाहरण और प्रश्न के साथ वास्तव में **जूझना** चाहिए। जैसा कि आप जानते हैं, जब भी हम आपका नई संकल्पनाओं से परिचय कराते हैं, तब हम कई ठोस उदाहरण भी देते हैं जिससे कि आप संकल्पना को अच्छी तरह से समझ सकें। हम संकल्पनाओं तथा प्रक्रियाओं की आपकी समझ बेहतर करने के लिए अधिक मात्रा में संबंधित प्रश्न भी देते हैं। इसका लाभ उठाने के लिए, आपको हर प्रश्न को तभी हल करने की कोशिश करनी चाहिए जब भी आप उस पर पहुँचें।

अब, कुछ शब्द खंड के ख़ाके के बारे में। प्रत्येक खंड में सर्वप्रथम आप एक खंड की प्रस्तावना को पाएँगे। उसके बाद उस खंड में इस्तेमाल होने वाली प्रतीकों की एक सूची होगी। इसके बाद उस खंड की इकाइयाँ आएँगी। प्रत्येक इकाई एक प्रस्तावना से शुरू होगी, जिसमें उस इकाई को सीखने के अपेक्षित उद्देश्यों की सूची होगी। प्रत्येक इकाई को भागों में बाँटा गया है। क्योंकि विभिन्न इकाइयों की सामग्री एक-दूसरे से काफ़ी जुड़ी हुई है, इसलिए हम बार-बार एक दूसरे के संदर्भ देते रहेंगे। इसके लिए, हमने **संकेत भाग x.y** का उपयोग किया है, जिसका अर्थ है **इकाई x का भाग y.** आपके द्वारा अध्ययन किए गए पिछले गणितीय पाठ्यक्रमों की तरह, यहाँ भी आप इकाई के उदाहरणों, प्रश्नों तथा महत्वपूर्ण समीकरणों को उस इकाई में क्रम में अंकित

पाएँगे। साथ ही, प्रत्येक इकाई में पाठ्यसामग्री के बीच-बीच में प्रश्न भी दिए गए हैं। ये इसलिए दिए गए हैं कि आप अपनी प्रगति की स्वयं जाँच कर सकें। इन प्रश्नों के हल, या हल की रूपरेखा या केवल उत्तर, इकाई के अंत में दिए गए हैं। **जब आप इकाई का अध्ययन समाप्त कर लें,** तब आप उस इकाई के उद्देश्यों पर वापस आ जाएँ (जो इकाई की प्रस्तावना में दिए गए हैं) तथा **जाँच कर लें कि आपने इन्हें किस हद तक प्राप्त कर लिया है।**

ट्यूटोरियल के एक हिस्से के रूप में, हमने प्रत्येक खंड के अंत में अनेक विविध उदाहरण और प्रश्न दिए हैं। ये प्रश्न उस खंड तक आपके द्वारा अध्ययन की गई सभी इकाइयों पर आधारित हैं। आपको इन प्रश्नों को भी स्वयं हल करना चाहिए। आगे, हम आपको एक सत्रीय कार्य भेजेंगे। यह भी शिक्षण का एक साधन है, और मूल्यांकन का साधन है। अध्ययन केन्द्र पर आपका परामर्शदाता (counsellor) इसका मूल्यांकन करेंगे तथा उपयुक्त विस्तृत टिप्पणियों के साथ **आपको वापस कर देंगे।**

आप इग्नू यूट्यूब आरकाइव्ज़ (archives) पर उपलब्ध हमारे **विडीयो प्रोग्राम** "सममितियों के समूह" को भी देख सकते हैं। इसमें हमने किसी वस्तु की सममिति की अवधारणा का मूर्तीकरण करने का प्रयास किया है। इस संकल्पना से आप इस पाठ्यक्रम के प्रथम दो खंडों में लगातार कार्य करते रहेंगे।

अब एक शब्द आवरण-पृष्ठ (cover) **के बारे में** इसमें दी गई पेंटिंग एक सुविख्यात कलाकार द्वारा की गई है। यह दर्शाता है कि आप तथा आपके सहपाठी एक सुंदर वन (जो बीजगणित है) में सुंदर बीजीय संकल्पनाओं और प्रक्रियाओं को ढूंढते हुए जा रहे हैं।

इस पाठ्यक्रम में दी गई सामग्री के अतिरिक्त यदि आप और अधिक पढ़ना चाहते हैं, तो **आप निम्नलिखित पुस्तकों को भी देख सकते** हैं:

i) A First Course in Abstract Algebra, by J. B. Fraleigh, Pearson.

ii) Contemporary Abstract Algebra, by J. A. Gallian, Narosa.

iii) Abstract Algebra, by Hodge, Schlicker and Sundstrom, CRC Press.

इस पाठ्यक्रम से जुड़े किसी भी पूछताछ के लिए आप हमसे directorsos@ignou.ac.in पर संपर्क कर सकते हैं।
आपका अध्ययन का यह अनुभव अच्छा रहे, यह हमारी उम्मीद है!

पाठ्यक्रम दल

इग्नू
जन-जन का
विश्वविद्यालय

इंदिरा गांधी राष्ट्रीय मुक्त विश्वविद्यालय
विज्ञान विद्यापीठ

BMTC-134
बीजगणित

खंड

1

प्रारंभिक समूह सिद्धांत

पाठ्यक्रम अभिकल्प समिति*

प्रो. रश्मी भारद्वाज
जी.जी.एस इंद्रप्रस्थ विश्वविद्यालय, दिल्ली

डॉ. सुनीता गुप्ता
दिल्ली विश्वविद्यालय

प्रो. अम्बर हबीब
शिव नाडार विश्वविद्यालय
गौतम बुद्ध नगर

प्रो. एस. ए. कात्रे
पुणे विश्वविद्यालय

प्रो. वी. कृष्ण कुमार
एन. आई. एस. ई. आर, भुवनेश्वर

डॉ. अमित कुलश्रेष्ठ
आई. आई. एस. ई. आर, मोहाली

प्रो. अपर्णा मेहरा
आई आई टी, दिल्ली

प्रो. राहुल राय
भारतीय सांख्यिकी संस्थान, दिल्ली

प्रो. मीना सहाय
लखनऊ विश्वविद्यालय

डॉ. शचि श्रीवास्तव
दिल्ली विश्वविद्यालय

प्रो. जुगल वर्मा
आई. आई. टी, मुंबई

संकाय सदस्य
विज्ञान विद्यापीठ, इग्नू

प्रो. एम. एस नाथावत (निदेशक)
डॉ. दीपिका
प्रो. परवीन सिंक्लेयर
श्री पवन कुमार
प्रो. पूर्णिमा मित्तल
प्रो. सुजाता वर्मा
डॉ. एस. वेंकटरामन

* इस समिति की अगस्त 2016 में बैठक हुई थी। यह पाठ्यक्रम अभिकल्प प्रोग्राम विशेषज्ञ समिति के सुझावों तथा यूजीसी–सीबीसीएस. के सांचे पर आधारित है।

खंड निर्माण दल

प्रो. परवीन सिंक्लेयर (*संपादक और लेखक*)
विज्ञान विद्यापीठ, इग्नू

पाठ्यक्रम समन्वयक: प्रो. परवीन सिंक्लेयर (email: sos@ignou.ac.in)

अनुवाद

श्री महेन्द्र शंकर (सेवानिवृत्त)
एन.सी.ई.आर.टी.

प्रो. परवीन सिंक्लेयर
विज्ञान विद्यापीठ, इं.गां.रा.मु.वि.

आभार:

i) **प्रो. मीना सहाय**, लखनऊ विश्वविद्यालय, और **डॉ. पूजा यादव**, कमला नेहरू कालेज, दिल्ली विश्वविद्यालय, के प्रति, उनकी विस्तृत टिप्पणियों के लिए।

ii) **श्री के. विश्वनाथन**, ग्राफ़िक यूनिट, ई. एम. पी. सी., इग्नू, के प्रति, कवर की कलाकृति और डिज़ाइन के लिए।

iii) श्री एस. एस. चौहान के प्रति इस खंड में रेखा आरेखों के लिए, और श्रीमति विनीता प्रजापति के प्रति इस खंड की सी. आर. सी. के लिए।

iv) इग्नू के पूर्व स्नातक पाठ्यक्रम, अमूर्त बीजगणित (एम. टी. ई-06), की कुछ सामग्री का इस खंड में उपयोग किया गया है।

खंड प्रस्तावना

समूह एक ऐसा बीजीय निकाय है जो एक समुच्चय, और उस पर परिभाषित एक द्वि-आधारी संक्रिया, से बनता है। समूहों का अध्ययन गणितज्ञों द्वारा दो सौ वर्षों से अधिक समय से किया जा रहा है। उन्नीसवीं शताब्दी के पूरे समय काल में समूह सिद्धांत का अध्ययन क्रमचयों और प्रतिस्थापनों (substitutions) का अध्ययन रहा। अपने वर्तमान अमूर्त रूप में यह धीरे-धीरे विकसित हुआ।

अपने वर्तमान रूप में, समूह सिद्धांत मौलिक गणितीय संरचनाओं के विश्लेषण करने में सहायता करता है। गणित की विभिन्न शाखाओं में कार्य करने वाले गणितज्ञ अपने स्वयं के गणितीय क्षेत्र में आगे बढ़ने के लिए समूह सिद्धांत की विधियाँ और साधनों का उपयोग करते हैं। गणितज्ञ ही नहीं, अपितु भौतिकविद् और रसायनविद् भी अणुओं और क्रिस्टलों की संरचनाओं का विश्लेषण करने के लिए, या बहुत जटिल इलेक्ट्रॉनिकों के ठोस परिपथों के अध्ययन करने में समूह सिद्धांत का उपयोग करते हैं। आइन्सटाइन (Einstein) ने विशिष्ट सापेक्षता के विश्लेषण करने के लिए हॉलेंड के एक भौतिकविद् लॉरेंत्ज़ (Lorentz) द्वारा निकाला गया बीजीय रूपांतरणों के समूह का उपयोग किया था। इसी रोचक और उपयोगी सिद्धांत की मूल धारणाओं से हम इस खंड में, तथा खंड 2 में, आपका परिचय कराना चाहते हैं।

इस खंड में हम बीजीय वस्तुओं की आपकी अब तक की समझ के आधार पर ही आगे बढ़ेंगे। याद कीजिए कि आपने अपने पहले सेमेस्टर के पाठ्यक्रम के खंड 1 में समुच्चयों, फलनों, सम्मिश्र संख्याओं तथा $\mathbb{R}$ पर बहुपदों का अध्ययन किया था। आगे, आपने अपने तीसरे सेमेस्टर के पाठ्यक्रम के खंड 1 में उपपत्ति के कई तरीक़ों का अध्ययन किया था। अब, आगे बढ़ने से पहले आपको उन सभी इकाइयों पर एक सरसरी नज़र डाल लेनी चाहिए।

इस खंड में चार इकाइयाँ हैं। इकाई 1 में हम पूर्णांकों की विभाज्यता के गुणों से संबंधित कुछ मौलिक धारणाओं का सारांश देंगे। इसके बाद हम विभाजनों से आपका परिचय कराएँगे तथा इनके तुल्यता संबंधों से जुड़े होने की चर्चा करेंगे। अंत में, हम आपका परिचय दो नई बीजीय वस्तुओं, आव्यूहों और क्रमचयों, से कराएँगे। हम इन वस्तुओं के कुछ मौलिक गुणों की भी चर्चा करेंगे।

इकाई 2 में आप समूह सिद्धांत के अध्ययन को शुरू करेंगे। इस इकाई में आप देखेंगे कि एक समूह क्या होता है तथा इस बीजीय निकाय के कुछ मौलिक गुणों का अध्ययन करेंगे। आप यह भी जानेंगे कि अनेक परिचित समुच्चय, जैसे पूर्णांकों और परिमेय संख्याओं के समुच्चय, योग के सापेक्ष समूह होते हैं। यहाँ हम आपका परिचय कुछ ऐसे समूहों से भी कराएँगे जो आपके सम्मुख इस पाठ्यक्रम में प्रायः आते रहेंगे, जैसे पूर्णांकों मॉड्यूलो n का समूह, क्रमचय समूह, द्वितल समूह, आव्यूह समूह, एक के nवें मूलों द्वारा बना समूह, तथा दो या अधिक समूहों को संयोजित करके एक रोचक तरीक़े से प्राप्त एक अन्य समूह।

इकाई 3 में आप समूहों के ऐसे उपसमुच्चयों का अध्ययन करेंगे जो स्वयं अपने समूह होते हैं। ये उपसमूह कहलाते हैं। यहाँ आप उपसमूहों के गुणों का अध्ययन करेंगे, जिनमें यह गुण भी सम्मिलित है कि उपसमूहों का कैसा व्यवहार रहता है जब उन पर समुच्चय संक्रियाएं लागू होती हैं।

इस खंड की अंतिम इकाई, इकाई 4 में हम एक विशिष्ट प्रकार के समूह पर ध्यान केन्द्रित करेंगे। यह चक्रीय समूह कहलाता है, जिसका कारण आपको इसका अध्ययन करते समय स्पष्ट हो जाएगा। जैसा कि आप देखेंगे, पूर्णांकों का समुच्चय एक प्रतिनिधिक चक्रीय समूह है। इन समूहों का अध्ययन करते समय, किसी भी समूह में अंतर्निहित समुच्चय के अवयव की कोटि की संकल्पना की भूमिका महत्वपूर्ण है। आप इस इकाई में इस संकल्पना का भी अध्ययन करेंगे। आगे, इस इकाई में आप चक्रीय उपसमूह की धारणा के एक व्यापकीकरण का भी अध्ययन करेंगे।

अगले खंड में आप समूह सिद्धांत कुछ गहराई में अध्ययन करेंगे। उसमें आपको उन सभी बातों की आवश्यकता होगी जिनका अध्ययन आपने इस खंड में किया है। इसलिए इस खंड का अध्ययन सावधानीपूर्वक कीजिए। जो भी प्रश्न आपके सम्मुख आए, उसे हल करने का प्रयास कीजिए, तथा आगे तभी बढ़िए जब आप उसे हल कर लें।

संकेत और प्रतीक (खंड 1 में प्रयोग होने वाले)

कृपया 'कलन' और 'वास्तविक विश्लेषण' पाठ्यक्रमों के खंड 1 में **दिए संकेतों और प्रतीकों को भी दोबारा देख लीजिए।**

$a \mid b \; (a \nmid b)$	b को a विभाजित करता है (b को a विभाजित नहीं करता है)
(a, b)	a और b का महत्तम समापवर्तक
$[a, b]$	a और b का लघुतम समापवर्त्य
$a \equiv b (\mathrm{mod}\ n)$	b, a के समशेष मॉड्यूल n है
$\mathbb{M}_{m\times n}(S) \, (\mathbb{M}_n(S))$	समुच्चय S पर सभी $m\times n$ आव्यूहों ($n\times n$ आव्यूहों) का समुच्चय
$\mathbf{0}(\mathbf{0}_{m\times n})$	उपयुक्त कोटि (कोटि $m\times n$) वाला शून्य आव्यूह
I_n	कोटि $n\times n$ वाला तत्समक आव्यूह
$(G, *)$	संक्रिया $*$ के सापेक्ष समूह G
$o(G)$	समूह G की कोटि
S_n	n प्रतीकों पर सममित समूह
D_{2n}	कोटि 2n वाला द्वितल समूह
S^1	एकक वृत्त
Q_8	चतुष्टयी समूह
K_4	क्लाइन 4-समूह
$\mathbb{Z}_n$	पूर्णांकों मॉड्यूलो n का समूह
U_n	एक के nवें मूलों का समूह
$(x_1 \, x_2 \ldots x_r)$	लंबाई r वाला चक्र
A^t	आव्यूह A का परिवर्त
$\det(A), \lvert A\rvert$	वर्ग आव्यूह का सारणिक
S^*	$S \setminus \{0\}$, जहाँ समुच्चय S, 0 को आविष्ट करता है
$GL_n(\mathbb{R})$	$\mathbb{R}$ पर कोटि n वाला व्यापक रैखिक समूह
$SL_n(\mathbb{R})$	$\mathbb{R}$ पर कोटि n वाला विशिष्ट रैखिक समूह
$\wp(S)$	समुच्चय S के उपसमुच्चयों का समुच्चय
$A \Delta B$	$(A \setminus B) \cup (B \setminus A)$
$G_1 \times G_2$	समूहों G_1 और G_2 का बाह्य अनुलोम गुणनफल
$\leq$	का उपसमूह है
$\lneq, <$	का उचित उपसमूह है
$\nleq$	का उपसमूह नहीं है
$Z(G)$	समूह G का केन्द्र
$< x >$	अवयव x द्वारा जनित चक्रीय समूह
$< S >$	समुच्चय S द्वारा जनित चक्रीय समूह
$o(x)$	अवयव x की कोटि
w.r.t.	के सापेक्ष
s.t.	जिससे कि / जिनसे कि
iff	यदि और केवल यदि

इकाई 1

कुछ प्रारंभिक संकल्पनाएँ

इकाई की रूपरेखा **पृष्ठ संख्या**

1.1 प्रस्तावना

इस इकाई में हमारा लक्ष्य है कि आपको कुछ ऐसे गणितीय संकल्पनाओं से परिचित होने में मदद करना जिनका आप इस पाठ्यक्रम में कई बार प्रयोग करेंगे। हम आपकी पूर्णांकों के कुछ ऐसे पहलुओं का स्मरण करने में सहायता करेंगे जिनका आप पहले अध्ययन कर चुके हैं। हम आपसे 'आव्यूह' और 'क्रमचय' की अवधारणाओं का भी परिचय कराएँगे।

इस इकाई में, तथा इस पाठ्यक्रम के शेष भाग में, हम आपके द्वारा प्रथम सेमेस्टर के पाठ्यक्रम 'कलन' के खंड 1 में फलनों और द्वि-आधारी संक्रियाओं के बारे में जो आपने पढ़ा है उसका संदर्भ प्रायः देंगे। हम प्रत्यक्ष और अप्रत्यक्ष रूप से तीसरे सेमेस्टर के पाठ्यक्रम 'वास्तविक विश्लेषण' की इकाइयों 1 और 2 का भी प्रायः संदर्भ लेंगे। अतः, इन इकाइयों को इस पाठ्यक्रम को पढ़ते समय कृपया अपनी सुविधा के लिए साथ रखिए।

यह इकाई वास्तव में भाग 1.2 से शुरू होती है। यहाँ हम पूर्णांकों की विभाज्यता से संबंधित विभिन्न संकल्पनाओं और ऐल्गोरिद्मों की चर्चा करेंगे। विशिष्ट रूप से, आप दो

शून्येतर पूर्णांकों का महत्तम समापवर्तक ज्ञात करने के लिए यूक्लिडीय ऐल्गोरिद्म का अध्ययन करेंगे।

कलन में आप सीख चुके हैं कि एक तुल्यता संबंध क्या होता है। भाग 1.3 में हम इस समझ को आगे बढ़ाएँगे तथा इसे एक समुच्चय के विभाजन की संकल्पना से संबंधित करेंगे।

भाग 1.4 में हम एक ऐसी संकल्पना की चर्चा करेंगे जिससे आप अपने स्कूली अध्ययन से शायद परिचित होंगे। यह है अरिक्त समुच्चय पर एक आव्यूह की संकल्पना। हम वास्तव में $\mathbb{C}$ (या $\mathbb{C}$ के उपसमुच्चयों) **पर आव्यूहों पर ज़्यादा** बात करेंगे। यहाँ आप $\mathbb{C}$ (या $\mathbb{C}$ के उपसमुच्चयों) पर आव्यूहों के समुच्चय पर कुछ संक्रियाओं का अध्ययन भी करेंगे।

अंत में, भाग 1.5 में, हम आपका परिचय किसी समुच्चय के अवयवों के क्रमचय की संकल्पना से कराएँगे। विशिष्ट रूप से, हम एक समभुजीय (regular) समतलीय आकृति की सममितियों की चर्चा करेंगे।

हमने नीचे वे अधिगम (learning) प्रत्याशाएँ दी हैं, जिनको ध्यान में रखकर इस इकाई को बनाया गया है। आप इस इकाई की पढ़ाई ध्यान से करें, तथा जैसे-जैसे आप दिए गए सवालों पर पहुँचे वैसे-वैसे आप इन्हें हल करने की पूरी कोशिश करें। तब आप इन प्रत्याशाओं को पूरा करने में समर्थ हो जाएँगे। इस तरह पढ़ाई करने में अपना समय लीजिए, परंतु इसे स्वयं ही कीजिए।

उद्देश्य

इस इकाई की पढ़ाई करने के बाद, आप निम्नलिखित कर पाएँगे :

- $\mathbb{Z}$ के लिए विभाजन कलन विधि का कथन देना, उसे सिद्ध करना तथा उसका अनुप्रयोग करना;
- $a, b \in \mathbb{Z}, a \neq 0$ का g.c.d किन्हीं $m, n \in \mathbb{Z}$ के लिए, $ma + nb$ के रूप का होता है– इसको सिद्ध करना, तथा इसका उपयोग करना;
- अंकगणित की मूलभूत प्रमेय को सिद्ध करना तथा उसका अनुप्रयोग करना;
- किन्हीं दो शून्येतर पूर्णांकों का g.c.d. ज्ञात करने के लिए यूक्लिडीय ऐल्गोरिद्म का अनुप्रयोग करना;
- किसी भी अरिक्त समुच्चय S का कोई भी विभाजन S पर एक तुल्यता संबंध परिभाषित करता है– इस कथन को, तथा इसके विलोम को, सिद्ध करना और उसका अनुप्रयोग करना;
- किसी समुच्चय पर आव्यूहों, तथा उन पर संक्रियाओं, को परिभाषित करना और उनके उदाहरण देना;
- किसी समुच्चय के क्रमचयों, तथा उनके संयोजन को, परिभाषित करना और उनके उदाहरण देना।

1.2 $\mathbb{Z}$ में विभाज्यता

आपने अपने स्कूल के समय तथा उसके बाद भी, पूर्णांकों का काफ़ी अध्ययन किया है और उनका इस्तेमाल किया है। इस भाग में हम इनसे जुड़ी एक ऐसी मूलभूत धारणा पर केन्द्रित होंगे जिससे आप परिचित होंगे, यानी, पूर्णांकों की विभाज्यता (divisibility). उदाहरणार्थ, 30 के भाजक (divisor) क्या हैं? हम क्यों कहते हैं कि $\mathbb{Z}$ में 30 को 5 विभाजित करता है तथा 7 विभाजित नहीं करता है? और फिर, क्या 0 किसी पूर्णांक को विभाजित करता है? इन प्रश्नों के उत्तरों के बारे में सोचिए, और निम्नलिखित परिभाषा पर विचार करें।

परिभाषा: मान लीजिए कि $a, b \in \mathbb{Z}, a \neq 0$. हम कहते हैं कि **b को a विभाजित करता** है, यदि एक ऐसा पूर्णांक c है जिससे कि $b = ac$. हम इसे $\mathbf{a \mid b}$ लिखते हैं, तथा इसे '**b का a एक भाजक** (divisor) (या **गुणनखंड** (factor)) है, या यह कि '**a से b विभाज्य** (divisible) है', या यह कि '**a का b एक गुणज** (multiple) **है**' पढ़ते हैं।

यदि b को a विभाजित नहीं करता है, तो हम इसे $\mathbf{a \nmid b}$ के रूप में लिखते हैं।

उदाहरणार्थ, $5 \mid 30$ है, क्योंकि 6 एक ऐसा पूर्णांक है जिससे कि $30 = 5 \times 6$. और, $7 \nmid 30$ क्योंकि ऐसा कोई पूर्णांक x नहीं है जिससे कि $30 = 7x$ हो।

यहाँ, आप भाजकों के बारे में निम्नलिखित महत्वपूर्ण टिप्पणी पर अवश्य विचार करें।

टिप्पणी 1: $a, b \in \mathbb{Z}, a \neq 0$ के लिए, यदि $a \mid b$, तो $\exists c \in \mathbb{Z}$ जिससे कि $ac = b$ है। यह c **अद्वितीय** है। इसका कारण यह है कि यदि $c, d \in \mathbb{Z}$ के लिए, $ac = b$ और $ad = b$ है, तो $ac = ad$. अब क्योंकि $a \neq 0$, इसलिए इससे $c = d$ प्राप्त हो जाता है। (वस्तुतः, इसके बारे में आप और अधिक खंड 3 में अध्ययन करेंगे।)

उपरोक्त हमें एक और टिप्पणी की ओर ले जाता है।

टिप्पणी 2: ध्यान दीजिए कि $0 \cdot z = 0 \ \forall \ z \in \mathbb{Z}$. अतः, ऐसा प्रतीत होता है कि $0 \mid 0$. परंतु, उदाहरण के तौर पर, $0 \cdot 1 = 0(-1)$ है और $1 \neq -1$. इसलिए टिप्पणी 1 की बात से हमें एक अंतर्विरोध प्राप्त होता है। इसलिए, 0 द्वारा विभाजन को अर्थहीन माना जाता है, तथा $\left(\frac{0}{0}\right)$ परिभाषित नहीं है, जैसा कि आप पहले से ही यह जानते होंगे।

हम निम्नलिखित प्रश्न में पूर्णांकों की विभाज्यता के कुछ गुण दे रहे हैं। आप इनमें से कुछ गुणों से पहले से ही परिचित होंगे। यहाँ, आपको इन्हें सिद्ध करने का एक अवसर है।

E1) मान लीजिए कि a, b, c शून्येतर पूर्णांक हैं। सिद्ध कीजिए कि

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

ii) $a \mid b \Rightarrow ac \mid bc.$

iii) $a|b$ और $b|c \Rightarrow a|c$.

iv) $a|b$ और $b|a \Leftrightarrow a = \pm b$.

v) $c|a$ और $c|b \Rightarrow c|(ax+by)\ \forall\ x, y \in \mathbb{Z}$.

आगे बढ़ने से पहले, हम आपको कुछ ऐसे तुल्य कथनों की याद दिलाएँगे जिनका आपने 'वास्तविक विश्लेषण' की इकाई 2 में कुछ विस्तार से अध्ययन किया है। इसके लिए हम आपको निम्नलिखित परिभाषा की भी याद दिलाते हैं।

परिभाषा: मान लीजिए कि $\mathbb{Z}$ का S एक अरिक्त उपसमुच्चय है। एक अवयव $a \in S$ समुच्चय S का एक **न्यूनतम अवयव** (या **लघुतम अवयव,** या **निम्नतम अवयव**) कहलाता है, यदि $a \le b\ \forall\ b \in S$ है।

उदाहरणार्थ, $\mathbb{N}$ का एक न्यूनतम अवयव है, और यह 1 है। परंतु $\mathbb{Z}$ का कोई न्यूनतम अवयव नहीं है। वास्तव में, $\mathbb{Z}$ के अनेक उपसमुच्चयों, जैसे $2\mathbb{Z}, \{-1, -2, -3, \ldots\}$, इत्यादि, के कोई न्यूनतम अवयव नहीं हैं।

अब हम पूर्णांकों के एक अभिगृहीत (axiom) का कथन देते हैं, जिसका हम स्पष्ट रूप से और अस्पष्ट रूप से प्रायः उपयोग करेंगे। यह है सुक्रमण सिद्धांत। यह हमें कुछ ऐसे समुच्चयों के बारे में बताता है, जिनका एक न्यूनतम अवयव होता है।

सुक्रमण सिद्धांत (Well-ordering Principle): $\mathbb{N}$ के प्रत्येक अरिक्त उपसमुच्चय का एक न्यूनतम अवयव होता है।

वास्तव में, यह सिद्धांत निम्न कथन के समतुल्य है:

$\mathbb{N} \cup \{0\}$ के प्रत्येक उपसमुच्चय का एक न्यूनतम अवयव होता है।

हम कभी-कभी 'गणितीय आगमन का सिद्धांत' के लिए संक्षिप्त में **PMI** लिखेंगे।

जैसा कि आपको 'वास्तविक विश्लेषण' से याद होगा, यह सिद्धांत वास्तव में **गणितीय आगमन के सिद्धांत (Principle of Mathematical Induction)** के समतुल्य है, जिसका आप विस्तार से उस कोर्स के खंड 1 में अध्ययन कर चुके हैं। आइए इस सिद्धांत का यहाँ कथन दें।

प्रमेय 1 (गणितीय आगमन का सिद्धांत): मान लीजिए कि $S \subseteq \mathbb{N}$ ऐसा है कि

i) $1 \in S$, तथा

ii) जब भी $k \in S$, तब $k+1 \in S$.

तब, $S = \mathbb{N}$. ■

यह प्रमेय आगे निम्नलिखित परिणाम के समतुल्य है।

प्रमेय 2 (आगमन का विस्तृत सिद्धांत): मान लीजिए कि $S \subseteq \mathbb{N}$ ऐसा है कि

i) $n_0 \in S$, तथा

ii) जब भी $k \in S$, तब $k+1 \in S$.

तब, $S = \{n \in \mathbb{N} \mid n \geq n_0\}$. ■

चौथा समतुल्य कथन, जिसका अध्ययन आप 'वास्तविक विश्लेषण' में कर चुके हैं, निम्नलिखित है :

प्रमेय 3 (आगमन के सिद्धांत का सशक्त रूप): मान लीजिए कि $S \subseteq \mathbb{N}$ ऐसा है कि

i) $n_0 \in S$, तथा

ii) जब भी $m \in S \ \forall \ n_0 \leq m < k$, तब $k \in S$.

तब, $S = \{n \in \mathbb{N} \mid n \geq n_0\}$. ■

हम इस पाठ्यक्रम में, प्रमेय 1, 2 और 3 का सुक्रमण सिद्धांत से समतुल्यता को सिद्ध नहीं करेंगे, क्योंकि इसकी उपपत्ति कुछ तकनीकी है। परंतु, हम प्रमेयों 2 और 3 को पुनः उन समतुल्य रूपों में लिखेंगे, जिनमें सामान्यतः हम इनका उपयोग करेंगे।

प्रमेय 2′ (गणितीय आगमन का विस्तृत सिद्धांत, PMI): मान लीजिए कि किसी धनात्मक पूर्णांक n के लिए $P(n)$ एक ऐसा विधेय है कि

i) किसी $n_0 \in \mathbb{N}$ के लिए, $P(n_0)$ एक सत्य कथन है, तथा

ii) जब भी किसी $k \in \mathbb{N}, k \geq n_0$ के लिए $P(k)$ सत्य है, तब $P(k+1)$ सत्य है।

तब, $P(n)$ उन सभी $n \in \mathbb{N}$ के लिए सत्य होगा, जिनके लिए $n \geq n_0$. ■

'वास्तविक विश्लेषण' के इकाई 2 से याद कीजिए कि 'विधेय' एक ऐसा वाक्य $P(n)$ है जो कुछ $n \in \mathbb{N}$ के लिए सत्य कथन हो सकते हैं, और कुछ n के लिए असत्य कथन हो सकते हैं।

प्रमेय 3′ (PMI का सशक्त रूप): मान लीजिए कि किसी धनात्मक पूर्णांक n के लिए $P(n)$ एक ऐसा विधेय है कि

i) किसी $n_0 \in \mathbb{N}$ के लिए, $P(n_0)$ एक सत्य कथन है, तथा

ii) जब भी सभी धनात्मक पूर्णांक m s.t. $n_0 \leq m < k$ के लिए, $P(m)$ सत्य है, तब $P(k)$ सत्य है।

तब, उन सभी $n \in \mathbb{N}$ के लिए, $P(n)$ सत्य होगा, जिनके लिए $n \geq n_0$. ■

ऊपर दिए गए समतुल्य कथन, 'विश्लेषण' में अनेक परिणामों को सिद्ध करने के लिए बहुत उपयोगी हैं जैसा कि आप देख चुके हैं। यही बात आप बीजगणित की स्थिति में भी देखेंगे। अब हम इसका उपयोग $\mathbb{Z}$ के लिए विभाजन कलन विधि (division algorithm) को सिद्ध करने में करेंगे। आप इस विधि का उपयोग अनगिनत बार कर चुके हैं। उदाहरणार्थ, यदि आपसे 365 दिनों में सप्ताहों की संख्या ज्ञात करने को कहा जाए, तो आप कहेंगे कि 52 हैं। क्यों? संभवतः इसलिए कि $365 = (7 \times 52) + 1$ है।

हो सकता है कि आपने देखा होगा कि $365 = (7 \times 50) + 65$ है। परंतु, चूँकि 7 से 65 बड़ा है। इसलिए शेष 65 दिनों में कुछ सप्ताह और हैं। उपरोक्त कलन विधि हमें बताती

है कि किस प्रकार एक अद्वितीय शेषफल पर पहुँचे, जिसमें कोई और 'सप्ताह शेष नहीं बचे' ।

खंड 4 में आप बहुपदों के लिए इस ऐल्गोरिद्म के एक रूप का अध्ययन करेंगे।

प्रमेय 4 (विभाजन कलन विधि): मान लीजिए कि $a, b \in \mathbb{Z}$ जहाँ $b > 0$. तब, ऐसे अद्वितीय पूर्णांकों q और r का अस्तित्व है जिनसे कि $a = qb + r$, जहाँ $0 \le r < b$.

उपपत्ति: पहले, हम सिद्ध करेंगे कि q और r का अस्तित्व है। इसके बाद, हम दर्शाएँगे कि ये अद्वितीय हैं। इनके अस्तित्व को सिद्ध करने के लिए, हम तीन विभिन्न स्थितियों पर विचार करेंगे :

$a = 0, a > 0, a < 0.$

स्थिति 1 ($\mathbf{a = 0}$): $q = 0, r = 0$ लीजिए। तब, $a = qb + r$ है।

स्थिति 2 ($\mathbf{a > 0}$): इस स्थिति में हम प्रमेय $2'$ का उपयोग करेंगे।

$n \in \mathbb{N}$ के लिए, मान लीजिए कि $P(n)$ यह विधेय है कि $n = qb + r$ किन्हीं $q, r \in \mathbb{Z}$, के लिए, जहाँ $0 \le r < b$. हम जानना चाहते हैं कि $\forall\ n \in \mathbb{N}, P(n)$ सत्य है या नहीं।

अतः, आइए देखें कि क्या $P(1)$ सत्य है।

यदि $b = 1$ है, तो $q = 1, r = 0$ ले सकते हैं, और इस प्रकार $1 = 1.1 + 0$ है।

यदि $b > 1$ है, तो $q = 0, r = 1$ लीजिए। इससे $1 = 0.b + 1$ है।

अतः, $b \ge 1$ की प्रत्येक स्थिति के लिए, $P(1)$ सत्य है।

अब, मान लीजिए कि किसी $k \in \mathbb{N}, k \ge 2$ के लिए $P(k-1)$ सत्य है, अर्थात्
$(k-1) = q_1 b + r_1$ किन्हीं $q_1, r_1 \in \mathbb{Z}$ के लिए, जहाँ $0 \le r_1 < b$.

$\Rightarrow k = q_1 b + (r_1 + 1)$, जहाँ $r_1 \le b - 1$, अर्थात् $r_1 + 1 \le b$ है।

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

यानी कि, $P(k)$ सत्य है।

इसलिए, प्रमेय $2'$ द्वारा, किसी भी $n \in \mathbb{N}$ के लिए, $P(n)$ सत्य है। अर्थात्, अगर $a > 0$ है, $a = qb + r$, तो किन्हीं $q, r \in \mathbb{Z}$ के लिए, जहाँ $0 \le r < b$.

स्थिति 3 ($\mathbf{a < 0}$): यहाँ $(-a) > 0$ है। इसलिए, स्थिति 2 द्वारा, हम लिख सकते हैं कि $(-a) = q'b + r'$, किन्हीं $q', r' \in \mathbb{Z}$ के लिए, जहाँ $0 \le r' < b$.

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

इस प्रकार, $a = qb + r$ किन्हीं $q, r \in \mathbb{Z}$ के लिए, जहाँ $0 \le r < b$.

अतः, आपने देखा कि $\forall\, a \in \mathbb{Z}, \exists\, q, r \in \mathbb{Z}$ जिनसे कि $a = qb + r$.

अब, आइए q और r की अद्वितीयता को सिद्ध करें। मान लीजिए कि $q', r' \in \mathbb{Z}$ इस प्रकार हैं कि $a = qb + r$ और $a = q'b + r'$, जहाँ $0 \le r < b$ और $0 \le r' < b$.

तब, $r - r' = b(q' - q)$. इस प्रकार, $b|(r - r')$. परंतु $|r - r'| < b$. अतः केवल एक ही संभावना है, यह कि $r - r' = 0$, अर्थात् $r = r'$, और तब $q = q'$.

अतः, हमने q और r की अद्वितीयता को सिद्ध कर लिया है। ■

जैसा कि हम पहले बता चुके हैं, आपने पूर्णांकों के साथ अपने पहले किए गए कार्यों में उपरोक्त ऐल्गोरिद्म का बहुत बार उपयोग किया होगा। उदाहरणार्थ, 62 को 6 से भाग देने के लिए आपने $62 = (6 \times 10) + 2$ लिखा होगा।

साथ ही, यदि आप (-25) को 3 से भाग दे रहे होंगे, तो आपने $(-25) = (-9)3 + 2$ प्राप्त किया होगा, जहाँ $q = -9$ और $r = 2$. यहाँ, इस ओर ध्यान दीजिए कि r को धनात्मक होना चाहिए। इसलिए, $(-25) = (-8)3 - 1$ लेना विभाजन कलन विधि का परिणाम नहीं होगा।

यह उदाहरण हमें यहाँ एक महत्वपूर्ण टिप्पणी की ओर ले जाता है।

टिप्पणी 3: विभाजन ऐल्गोरिद्म को केवल धनात्मक भाजक b के लिए सिद्ध किया गया है। अगर $b \le 0$, तो क्या होता है? जैसा कि टिप्पणी 2 में देखा था, $b \ne 0$.

यदि $b < 0$, तो a और $-b(>0)$ पर विचार कीजिए।

तब, $a = q(-b) + r$ जहाँ $0 \le r < -b$.

$\qquad = (-q)b + r,\ 0 \le r < |b|$, क्योंकि $|b| = -b$ है।

इस प्रकार, अपने अधिकतम व्यापक रूप में, **विभाजन कलन विधि कहता है** कि **$a, b \in \mathbb{Z}, b \ne 0$ दिया होने पर, ऐसे अद्वितीय $q, r \in \mathbb{Z}$ है जिनसे कि $a = qb + r$ जहाँ $0 \le r < |b|$.**

पारिभाषिक शब्दावली के संबंध में, निम्नलिखित टिप्पणी पर भी विचार कीजिए।

टिप्पणी 4: व्यंजक $a = qb + r$ में, जहाँ $0 \le r < b$, q को b से a को भाग देने पर प्राप्त **भागफल (quotient)** कहते हैं, तथा r को **शेषफल (remainder)** कहते हैं।

आगे चलकर कुछ समूहों का अध्ययन करते समय, आप प्रायः विभाजन कलन विधि के उपयोग को देखेंगे। इसके अनुप्रयोग में अभ्यास के लिए, कुछ संबंधित प्रश्नों को हल करने का प्रयास कीजिए।

E2) युग्मों $75, 30$ और $-75, -30$ पर विभाजन कलन विधि का अनुप्रयोग कीजिए।

E3) सिद्ध कीजिए कि यदि $a \in \mathbb{Z}$ ऐसा है कि $3 \nmid a$, तो a^2 को 3 से भाग देने पर शेषफल 1 आता है।

E4) मान लीजिए कि $a, b \in \mathbb{Z}$ ऐसे हैं कि $3|(a^2+b^2)$. दर्शाइए कि $3|a$ **और** $3|b$.

(**संकेत:** E3 का उपयोग कीजिए।)

आइए अब भाजक और गुणजों की चर्चा पर वापस आ जाएँ।

निम्नलिखित परिभाषाओं पर ग़ौर कीजिए।

याद कीजिए कि $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

परिभाषाएँ: मान लीजिए कि $a, b \in \mathbb{Z}^*$.

i) कोई पूर्णांक c पूर्णांकों a और b का एक **सार्व भाजक (common divisor)** कहलाता है, यदि $c|a$ और $c|b$.

ii) कोई पूर्णांक m पूर्णांकों a और b का एक **सार्व गुणज, या समापवर्तक (common multiple)** कहलाता है, यदि $a|m$ और $b|m$.

उदाहरण के लिए, 2 और 4 का 2 एक सार्व भाजक है तथा दोनों 4 और 8 2 और 4 के सार्व गुणज हैं। आगे, E1(i) से आप जानते हैं कि किन्हीं $a, b \in \mathbb{Z}$ के लिए, a और b के 1 और -1, सार्व भाजक हैं। इस तरह, पूर्णांकों के किसी भी युग्म के एक से अधिक सार्व भाजक और सार्व गुणज होते हैं। इससे हम निम्नलिखित परिभाषाओं पर पहुँचते हैं।

परिभाषा : कोई पूर्णांक d दो शून्येतर पूर्णांकों a और b का एक **महत्तम समापवर्तक (greatest common divisor)** (संक्षेप में, **g.c.d**) कहलाता है, यदि

i) $d|a$ और $d|b$, तथा

ii) जब भी $c \in \mathbb{Z}$ ऐसा है कि $c|a$ और $c|b$, तो $c|d$.

ध्यान दीजिए कि यदि a और b के दो g.c.d d और d' हैं, तो उपरोक्त परिभाषा का (ii) यह कहता है कि $d|d'$ और $d'|d$. इस प्रकार, $d = \pm d'$ (E1 को देखिए)।

परंतु तब इनमें से केवल एक धनात्मक है।

इस **अद्वितीय** धनात्मक **g.c.d.** को $(\mathbf{a}, \mathbf{b})$ **द्वारा व्यक्त किया जाता** है।

इसी प्रकार, निम्नलिखित परिभाषा पर विचार कीजिए :

परिभाषा: कोई पूर्णांक ℓ $a, b \in \mathbb{Z}^*$ का एक **लघुतम सार्व गुणज (least common multiple)** (संक्षिप्त में, l.c.m.) कहलाता है, यदि

i) $a|\ell$ और $b|\ell$, तथा

ii) जब भी $m \in \mathbb{Z}$ s.t. $a|m$ और $b|m$, तब $\ell|m$.

g.c.d की स्थिति की ही तरह, आप यह दर्शा सकते हैं कि a और b का **एक अद्वितीय धनात्मक l.c.m.** होता है, जिसे $[\mathbf{a}, \mathbf{b}]$ द्वारा व्यक्त किया जाता है।

उदाहरणार्थ, $(3, 5) = 1$ और $(-8, 20) = 4$ है। साथ ही, $[3, 5] = 15$ और $[-8, 20] = 40$ है।

यहाँ एक संबंधित टिप्पणी पर विचार कीजिए।

टिप्पणी 5: कुछ गणितज्ञ $a, b \in \mathbb{Z}$ के g.c.d को तब भी परिभाषित करते हैं, जबकि उनमें से केवल एक का शून्येतर होना आवश्यक है। यदि $b \neq 0$ है, तो $(0, b) = |b|$, क्योंकि $|b|$ ही 0 और b दोनों का सबसे बड़ा धनात्मक समापवर्तक है। परंतु, इस पाठ्यक्रम में हम दो शून्येतर पूर्णांकों के g.c.d की ही बात करेंगे। यदि आप चाहते हैं, तो आप इसका सत्यापन कर सकते हैं कि (a, b) के बारे में वे सभी परिणाम जिन्हें हम यहाँ सिद्ध करेंगे, तब भी वैध हैं जब पूर्णांकों a और b में से केवल एक ही पूर्णांक शून्येतर है।

क्या किन्हीं दो शून्येतर पूर्णांकों a और b के लिए (a, b) का अस्तित्व है? हाँ, ऐसा ही है, जो हमें निम्नलिखित प्रमेय बताता है।

प्रमेय 5: किन्हीं दो शून्येतर पूर्णांकों a और b का एक महत्तम समापवर्तक होता है। साथ ही, $(a,b) = ma + nb$, किन्हीं $m, n \in \mathbb{Z}$ के लिए।

उपपत्ति: मान लीजिए कि $S = \{xa + yb \,|\, x, y \in \mathbb{Z}, (xa + yb) > 0\}$.

क्योंकि $a^2 + b^2 > 0$, इसलिए $a^2 + b^2 \in S$, अर्थात् $S \neq \emptyset$. अतः, सुक्रमण सिद्धांत द्वारा, S का एक न्यूनतम अवयव है, मान लीजिए, $d = ma + nb$, किन्हीं $m, n \in \mathbb{Z}$ के लिए। आप देखेंगे कि $d = (a, b)$.

क्योंकि $d \in S$, इसलिए $d > 0$. अतः, विभाजन कलन विधि से, हम

$a = qd + r$, लिख सकते हैं, किन्हीं $q, r \in \mathbb{Z}$ के लिए, जहाँ $0 \le r < d$.

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

अब, यदि $r \neq 0$ है, तो (1) दर्शाता है कि $r \in S$, जो S में d की न्यूनतमता का अंतर्विरोध करता है।

अतः, $r = 0$, अर्थात् $a = qd$, अर्थात् $d \,|\, a$.

आप इसी प्रकार दर्शा सकते हैं कि $d \,|\, b$.

अतः, a और b का d एक सार्व भाजक है।

अब, मान लीजिए कि c एक ऐसा पूर्णांक है कि $c \,|\, a$ और $c \,|\, b$.

तब, किन्हीं $a_1, b_1 \in \mathbb{Z}$ के लिए, $a = a_1c$ और $b = b_1c$.

परंतु तब $d = ma + nb = ma_1c + nb_1c = (ma_1 + nb_1)c$.

इस प्रकार, $c \,|\, d$.

अतः, हमने दर्शा दिया है कि a और b का d एक g.c.d है। क्योंकि $d > 0$ है, इसलिए यह अद्वितीय धनात्मक g.c.d, (a, b) है। ■

प्रमेय 5 जो हमें बताता है, उसके एक उदाहरण के तौर पर, -7 और 9 पर विचार कीजिए। आप जानते हैं कि इनमें 1 और -1 के अतिरिक्त कोई सार्व गुणनखंड नहीं है। अतः, $(-7, 9) = 1$. साथ ही, भूल और प्रयास विधि द्वारा, आप देख सकते हैं कि $1 = (-4)(-7) + (-3)9$.

-7 और 9 जैसे पूर्णांकों के युग्मों, जिनके g.c.d = 1 हैं, के लिए एक विशेष नाम दिया जाता है।

परिभाषा: यदि दो शून्येतर पूर्णांक a और b इस प्रकार हैं कि $(a, b) = 1$, तो वे एक दूसरे के **सापेक्षतः अभाज्य (relatively prime)** या **असहभाज्य** (**coprime**) कहलाते हैं।

इस परिभाषा से, तथा प्रमेय 5 के उपयोग से, हम कह सकते हैं कि

a और b परस्पर असहभाज्य होते हैं यदि और केवल यदि ऐसे $m, n \in \mathbb{Z}$ का अस्तित्व है जिनसे कि $1 = ma + nb$.

असहभाज्य पूर्णांकों का एक बहुत उपयोगी गुण है, जिसकी बात हम अब करने जा रहे हैं।

प्रमेय 6: यदि $a, b \in \mathbb{Z}^*$ इस प्रकार हैं कि $(a, b) = 1$, तथा यदि $c \in \mathbb{Z}$ ऐसा है कि $b \mid ac$, तो $b \mid c$.

उपपत्ति: जैसा कि आप प्रमेय 5 से जानते हैं, $\exists\, m, n \in \mathbb{Z}$ जिनसे कि $1 = ma + nb$.

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

अब, $b \mid ac$ और $b \mid bc$. इसलिए, E1(v) से, $b \mid (mac + nbc)$.

इस प्रकार, $b \mid c$. ■

आगे बढ़ने से पहले, l.c.m के बारे में निम्नलिखित टिप्पणी पर विचार कीजिए।

टिप्पणी 6: $a, b \in \mathbb{Z}^*$ दिया रहने पर, $[a, b]$ का सदैव अस्तित्व होता है। वस्तुतः, $[a, b] = \dfrac{ab}{(a, b)}$ होता है, जिसे हम यहाँ सिद्ध नहीं करेंगे। इसके अतिरिक्त, हम आगे l.c.m की कोई चर्चा नहीं करेंगे।

जैसा कि आप शीघ्र देखेंगे, प्रमेय 6 अंकगणित के मूलभूत प्रमेय (Fundamental Theorem of Arithmetic) को सिद्ध करने का आधार है। अभी के लिए, आइए कुछ संबंधित परिभाषाओं को दोबारा याद करें।

परिभाषाएँ: कोई प्राकृतिक संख्या $p(\neq 1)$ एक **अभाज्य संख्या (prime number)** कहलाती है, यदि इसके भाजक केवल 1 और p हैं। यदि कोई प्राकृतिक संख्या $n(\neq 1)$ अभाज्य नहीं है, तो वह एक **भाज्य संख्या (composite number)** कहलाती है।

इस प्रकार, 5, 17 और 101 अभाज्य संख्याएँ हैं, तथा 4 और 100 भाज्य संख्याएँ हैं। निःसंदेह, जैसा कि आप जानते हैं, 1 न तो अभाज्य संख्या है और न ही भाज्य संख्या है।

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E5) ऐसे $m, n \in \mathbb{Z}$ ज्ञात कीजिए जिनसे कि $(a, b) = ma + nb$, जहाँ

i) $a = 7, b = 21$

ii) $a = -5, b = -271$

iii) $a = -c, b = c;\ c \in \mathbb{Z}^*$ के लिए।

E6) $a, b \in \mathbb{Z}^*$ के लिए, $(a, b), (-a, b)$ और $(-a, -b)$ के बीच कोई संबंध है तो उसे ज्ञात कीजिए।

E7) यदि p एक अभाज्य संख्या है तथा $p \mid ab$, तो दर्शाइए कि $p \mid a$ या $p \mid b$. (यह अभाज्य संख्या की एक **वैकल्पिक परिभाषा** है।)

E8) **यूक्लिड प्रमेयिका (Euclid's Lemma)** के शक्तिशाली रूप को सिद्ध कीजिए, जहाँ प्रमेयिका का कथन निम्न है : यदि p एक अभाज्य संख्या है तथा $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ ऐसे हैं कि $p \mid a_1a_2 \ldots a_n$, तो किसी $i = 1, \ldots, n$ के लिए $p \mid a_i$.

(**संकेत:** PMI का उपयोग कीजिए।)

E9) सिद्ध कीजिए कि, प्रमेय 4 में $(a, b) = (b, r)$.

अब संख्या 50 पर विचार कीजिए। जैसा कि आप जानते हैं, हम इसे अभाज्य संख्याओं के गुणनफल के रूप में, $50 = 2 \times 5 \times 5$ लिख सकते हैं। वस्तुतः, हम 1 के अतिरिक्त किसी भी प्राकृतिक संख्या को अभाज्य संख्याओं के गुणनफल के रूप में लिख सकते हैं। यही हमें **अद्वितीय अभाज्य गुणनखंडन प्रमेय (unique prime factorisation theorem)** बताता है। इस प्रमेय को अंकगणित का मूलभूत प्रमेय भी कहा जाता है। जैसा कि हम पहले कह चुके हैं, हम अब इसे प्रमेय 6 का उपयोग करते हुए सिद्ध करेंगे।

प्रमेय 7 (अंकगणित का मूलभूत प्रमेय): प्रत्येक पूर्णांक $n > 1$ को $n = p_1 p_2 \ldots p_m$ के रूप में लिखा जा सकता है, जहाँ $p_1, p_2, \ldots, p_m$ अभाज्य संख्याएँ हैं। इसके आगे, गुणनखंडन में अभाज्य गुणनखंडों के क्रम के अलावा, यह निरूपण अद्वितीय होता है।

उपपत्ति: इस प्रमेय के निरूपण में दो भाग हैं – अस्तित्व और अद्वितीयता। पहले, हम ऐसे गुणनखंडन के अस्तित्व को, गणितीय आगमन के सिद्धांत का उपयोग करते हुए, सिद्ध करेंगे।

मान लीजिए कि $n \in \mathbb{N}$ के लिए $P(n)$ यह विधेय है कि $n+1$ एक या अधिक अभाज्य संख्याओं का गुणनफल है।

$P(1)$ सत्य है, क्योंकि 2 स्वयं एक अभाज्य संख्या है।

अब, आइए परिकल्पना करें कि सभी धनात्मक पूर्णांकों $m < k$ के लिए, $P(m)$ सत्य है। हम यह दर्शाना चाहते हैं कि $P(k)$ सत्य है।

यदि $k+1$ एक अभाज्य संख्या है, तो $P(k)$ सत्य होगा।

यदि $k+1$ एक अभाज्य संख्या नहीं है, तो हम $k+1 = m_1 m_2$ लिख सकते हैं, जहाँ $1 < m_1 < k+1$ और $1 < m_2 < k+1$ हैं। तब $P(m_1 - 1)$ और $P(m_2 - 1)$ दोनों ही सत्य हैं। इस प्रकार, $m_1 = p_1 p_2 \dots p_r$ और $m_2 = q_1 q_2 \dots q_s$, जहाँ $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ अभाज्य संख्याएँ हैं, जिनका अलग-अलग होना आवश्यक नहीं है।

इस प्रकार, $k+1 = p_1 p_2 \dots p_r q_1 q_2 \dots q_s$, अर्थात्, $P(k)$ सत्य है।

अतः, प्रमेय 3′ द्वारा, प्रत्येक $n \in \mathbb{N}$ के लिए $P(n)$ सत्य है।

अब, आइए दर्शाएँ कि यह गुणनखंडन अद्वितीय है।

मान लीजिए कि $n = p_1 p_2 \dots p_t = q_1 q_2 \dots q_s$, जहाँ $p_1, p_2, \dots, p_t, q_1, q_2, \dots, q_s$ अभाज्य संख्याएँ हैं। हम t पर आगमन का उपयोग करेंगे।

यदि $t = 1$, तो $p_1 = q_1 q_2 \dots q_s$. परंतु p_1 अभाज्य है। इस प्रकार, इसके गुणनखंड केवल 1 और स्वयं वह संख्या है। अतः, $s = 1$ और $p_1 = q_1$.

अब मान लीजिए कि $t > 1$ है, तथा अद्वितीयता $t-1$ अभाज्य संख्याओं के गुणनफल के लिए लागू है।

अब, $p_1 | q_1 q_2 \dots q_s$, और इसी लिए, E8 द्वारा, किसी $i = 1, \dots, s$ के लिए, $p_1 | q_i$ है। यदि आवश्यक हो तो $q_1, q_2, \dots, q_s$ के क्रम को बदलने पर, हम मान सकते हैं कि $p_1 | q_1$ है।

परंतु p_1 और q_1 दोनों ही अभाज्य संख्याएँ हैं। अतः, $p_1 = q_1$.

परंतु तब $p_2 \dots p_t = q_2 \dots q_s$.

इसलिए, आगमन द्वारा, $t - 1 = s - 1$ तथा $p_2, p_3, \dots, p_t$ **किसी क्रम में** $q_2, q_3, \dots, q_s$ हैं।

इस तरह, हमने गुणनखंडन की अद्वितीयता को सिद्ध कर लिया है। ■

उपरोक्त प्रमेय मूलभूत है, क्योंकि यह हमें बताता है कि कोई भी धनात्मक पूर्णांक अभाज्य संख्याओं से निर्मित होता है। इस प्रकार, अभाज्य संख्याएँ वे अवयव हैं, जिन्हें 'मिलाकर' प्राकृतिक संख्याएँ बनती हैं और फिर सभी शून्येतर पूर्णांक बनते हैं।

किसी संख्या के गुणनखंडन में एक या ज़्यादा अभाज्य संख्याएँ दोहराई जा सकती हैं, जैसे कि गुणनखंडन $50 = 2 \times 5 \times 5$ में 5 दो बार आ रहा है। दोहराए जाने वाली अभाज्य संख्याओं को एक साथ रखके, हम प्रमेय 7 का निम्नलिखित उपप्रमेय प्राप्त करते हैं।

उपप्रमेय 1: किसी भी प्राकृतिक संख्या $n(>1)$ को अद्वितीय रूप से $n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$ के रूप में लिखा जा सकता है, जहाँ $i = 1, 2, \dots, r$ के लिए प्रत्येक $m_i \in \mathbb{N}$ तथा प्रत्येक p_i एक ऐसी अभाज्य संख्या है कि $1 < p_1 < p_2 < \dots < p_r$. ■

किसी प्रमेय का उपप्रमेय वह परिणाम है, जो उस प्रमेय से एक निष्कर्ष के रूप में प्राप्त होता है।

प्रमेय 7 के अनुप्रयोग के रूप में, हम निम्नलिखित महत्वपूर्ण प्रमेय दे रहे हैं, जिसका श्रेय प्राचीन यूनानी गणितज्ञ यूक्लिड (Euclid) को जाता है, जिनका ज़िक्र हम पहले कर चुके हैं।

प्रमेय 8: अनंततः अनेक अभाज्य संख्याएँ हैं।

उपपत्ति : हम इसे अंतर्विरोध द्वारा सिद्ध करेंगे। अतः, आइए परिकल्पना करें कि अभाज्य संख्याओं का समुच्चय P परिमित है, मान लीजिए $P = \{p_1, p_2, \dots, p_n\}$. प्राकृतिक संख्या $m = (p_1 p_2 \dots p_n) + 1$ पर विचार कीजिए।

अब, मान लीजिए कि कोई $p_i | m$. तब, $p_i | (m - p_1 p_2 \dots p_n)$. अर्थात्, $p_i | 1$, जो एक अंतर्विरोध है।

अतः, $p_i \nmid m \; \forall \; i = 1, \dots, n.$

परंतु, क्योंकि $m > 1$ है, इसलिए प्रमेय 7 से m का एक अभाज्य गुणनखंड अवश्य होना चाहिए। इस प्रकार, हम एक अंतर्विरोध पर पहुँच जाते हैं।

अतः, हमारी परिकल्पना कि 'अभाज्य संख्याओं का समुच्चय परिमित है' अवश्य ही ग़लत होगी।

इसलिए, अनंततः अनेक अभाज्य संख्याएँ अवश्य होनी चाहिएं। ■

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E10) सिद्ध कीजिए कि यदि p एक अभाज्य संख्या है तथा $a \in \mathbb{Z}$ ऐसे हैं कि

i) $p \nmid a$, तो $(p, a) = 1$;

ii) $p | a^2$, तो $p | a$.

E11) सिद्ध कीजिए कि किसी भी अभाज्य संख्या p के लिए $\sqrt{p}$ एक अपरिमेय संख्या होती है।

(**संकेत:** मान लीजिए कि $\sqrt{p}$ परिमेय संख्या है। तब, $\sqrt{p} = \frac{a}{b}$. जहाँ $a, b \in \mathbb{Z}^*$ तथा हम मान सकते हैं कि $(a, b) = 1$. अब, अभाज्य संख्याओं के उन गुणों का उपयोग कीजिए जिनकी चर्चा हमने अभी-अभी की है।)

E12) सभी $n, m \in \mathbb{N}$ के लिए सिद्ध कीजिए कि यदि $n^{1/m} \notin \mathbb{Z}$ है, तो $n^{1/m} \notin \mathbb{Q}$.

E13) उपप्रमेय 1 को सिद्ध कीजिए।

E14) अंकगणित के मूलभूत प्रमेय के प्रयोग से सिद्ध कीजिए कि यदि $y \in \mathbb{N}$, तो ऐसी एक विषम प्राकृतिक संख्या x है कि किसी ऋणेतर पूर्णांक r के लिए $y = 2^r x$.

आप देख चुके हैं कि प्रत्येक पूर्णांक को अद्वितीय रूप से अभाज्य संख्याओं की घातों के गुणनफल के रूप में लिखा जा सकता है। अतः, जैसा कि आप अपने पिछले अध्ययनों से जानते हैं, आप इस निरूपण का उपयोग किन्हीं दो पूर्णांकों के g.c.d. को ज्ञात करने के लिए कर सकते हैं।

आकृति 1: यूक्लिड

उदाहरणार्थ, 175 और -2205 के g.c.d. को ज्ञात करने के लिए, हम इन दोनों को उपप्रमेय 1 में दिए रूप में लिखते हैं।

अतः, $175 = 5^2 \cdot 7$, और $-2205 = -(3^2 \cdot 5 \cdot 7)$.

इसके बाद, आप दोनों पूर्णांकों को विभाजित करने वाली प्रत्येक अभाज्य संख्या की अधिकतम घात के गुणनफल के रूप में इनका g.c.d. प्राप्त कर सकते हैं। इस स्थिति में, यह $5^1 \cdot 7^1 = 35$ है।

जैसा कि आप देख सकते हैं, यहाँ हमें दोनों पूर्णांकों की अभाज्य संख्याओं के गुणनफल के रूप में गुणनखंडन करने की आवश्यकता पड़ेगी। जब संख्याएँ ज़्यादा बड़ी हों, तब ऐसा करना सरल नहीं है। इसे कुछ सरल बनाने के लिए, प्राचीन यूनानियों ने एक ऐल्गोरिद्म विकसित की। ऐसा प्रतीत होता है कि इस ऐल्गोरिद्म को सर्वप्रथम प्राचीन यूनानी गणितज्ञ यूक्लिड ने अपने ग्रंथ 'एलीमेंट्स (Elements)' में दिया था। इस ग्रंथ में 13 पुस्तकें सम्मिलित हैं, तथा इसे लगभग 300 B.C. में लिखा गया था। इसलिए इस ऐल्गोरिद्म को यूक्लिड का नाम दिया गया है। यह विभाजन ऐल्गोरिद्म के निरंतर अनुप्रयोगों पर आधारित है।

यह देखने के लिए कि यूक्लिडीय ऐल्गोरिद्म किस प्रकार लागू होता है, एक उदाहरण पर विचार कीजिए।

उदाहरण 1: $(-246, 135)$ ज्ञात कीजिए। साथ ही, $m, n \in \mathbb{Z}$ ज्ञात कीजिए s.t. $m(-246) + n(135) = (-246, 135)$.

हल: E6 से आप जानते हैं कि $(-246, 135) = (246, 135)$.

246 और 135 के लिए, विभाजन ऐल्गोरिद्म द्वारा, हम प्राप्त करते हैं :

$$246 = 135 \cdot 1 + 111. \qquad \ldots(2)$$

अब विभाजन ऐल्गोरिद्म को 135 तथा (2) में प्राप्त शेषफल 111 पर लागू करके, हमें प्राप्त होता है :

$135 = 111 \cdot 1 + 24.$ …(3)

अब, 111 और 24 पर विभाजन ऐल्गोरिद्म का अनुप्रयोग करके प्राप्त होता है :

$111 = 24 \cdot 4 + 15.$ …(4)

आगे, $24 = 15 \cdot 1 + 9.$ …(5)

आगे, $15 = 9 \cdot 1 + 6$ …(6)

आगे, $9 = 6 \cdot 1 + 3.$ …(7)

आगे, $6 = 3 \cdot 2 + 0.$ …(8)

एक बार शेषफल शून्य आ जाए, तो हम रुक जाते हैं।

अब, E9 से आप जानते हैं कि
$(246,135) = (135,111) = (111, 24) = (24,15) = (15,9) = (9,6) = (6,3) = (3,0) = 3.$

इस प्रकार, $(-246, 135) = 3.$

ध्यान दीजिए कि यूक्लिडीय ऐल्गोरिद्म का प्रत्येक चरण दो पूर्णांकों के g.c.d. ज्ञात करने की समस्या को कम परिमाण वाले दो पूर्णांकों के g.c.d. को ज्ञात करने की समस्या में बदल देता है।

साथ ही, प्रमेय 5 के संदर्भ में, ध्यान दीजिए कि (7) से :

$3 = 9 - 6 = 9 - (15 - 9),$ (6) से।

$= 2 \cdot 9 - 15$

$= 2(24 - 15) - 15 = 2 \cdot 24 - 3 \cdot 15,$ (5) से।

$= 2 \cdot 24 - 3(111 - 4 \cdot 24) = 14 \cdot 24 - 3 \cdot 111,$ (4) से।

$= 14(135 - 111) - 3 \cdot 111 = 14 \cdot 135 - 17 \cdot 111,$ (3) से।

$= 14 \cdot 135 - 17(246 - 135) = (31 \cdot 135) - (17 \cdot 246),$ (2) से।

इस प्रकार, $3 = (-17) \cdot 246 + 31 \cdot 135$

$= 17 \cdot (-246) + 31 \cdot 135.$

इस प्रकार, प्रमेय 5 के संदर्भ में, $m = 17$ और $n = 31$.

***

उपरोक्त उदाहरण में आप देख सकते हैं कि $m, n \in \mathbb{Z}$ s.t. $ma + nb = (a, b)$ ज्ञात करने में किस प्रकार यह ऐल्गोरिद्म हमें सुविधा प्रदान करती है। अन्यथा, हमें इन पूर्णांकों को प्राप्त करने के लिए केवल भूल और प्रयास विधि का प्रयोग करना पड़ता, जैसा कि पहले के उदाहरणों में किया था।

आइए अब औपचारिक रूप से यूक्लिडीय ऐल्गोरिद्म को लिखें।

यूक्लिडीय ऐल्गोरिद्म: किन्हीं दो धनात्मक पूर्णांकों a और b के लिए, $\exists\, q_0, q_1, \ldots, q_{n+1}$ और $r_0, r_1, \ldots, r_n$ s.t.

$$a = bq_0 + r_0,\ 0 < r_0 < b.$$

$$b = r_0 q_1 + r_1,\ 0 < r_1 < r_0.$$

$$r_0 = r_1 q_2 + r_2,\ 0 < r_2 < r_1.$$

$$\vdots \qquad\qquad \vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n,\ 0 < r_n < r_{n-1}.$$

$$r_{n-1} = r_n q_{n+1} + 0.$$

तब, $(a, b) = r_n$ होता है।

उपपत्ति: जैसा कि आपने E9 में दर्शाया था,
$(a, b) = (b, r_0) = (r_0, r_1) = \cdots = (r_{n-1}, r_n) = r_n$. ■

उपरोक्त ऐल्गोरिद्म विभिन्न प्रकार की बीजीय समीकरणों को हल करने के लिए एक आधार है। इसका उपयोग इंटरनेट संचार (internet communication) को सुरक्षित रखने में तथा कोडिंग सिद्धांत (coding theory) में किया जाता है।

अब आप इस ऐल्गोरिद्म का अनुप्रयोग स्वयं ही क्यों नहीं करते?

E15) निम्नलिखित के लिए (a, b) ज्ञात करने के लिए, यूक्लिडीय ऐल्गोरिद्म को लागू कीजिए।

i) $a = 54321, b = 12345,$ तथा

ii) $a = -61880, b = -880.$

साथ ही, प्रत्येक स्थिति में ऐसे $m, n \in \mathbb{Z}$ ज्ञात कीजिए s.t. $(a, b) = ma + nb.$

अभी के लिए, हम $\mathbb{Z}$ में विभाज्यता पर अपनी चर्चा को यहीं ख़त्म करते हैं। परंतु, अब हम पूर्णांकों के युग्मों की विभाज्यता के आधार पर परस्पर असंयुक्त उपसमुच्चयों के रूप में $\mathbb{Z}$ के अवयवों को एकत्रित करने की एक विधि पर विचार करेंगे।

1.3 विभाजन और तुल्यता संबंध

कलन पाठ्यक्रम के खंड 1 में, आपने संबंधों तथा, विशिष्ट रूप में, तुल्यता संबंधों का अध्ययन किया था। आइए इनसे जुड़ी परिभाषाओं को फिर से देखें।

परिभाषाएँ: मान लीजिए कि S एक अरिक्त समुच्चय है।

i) S पर एक **संबंध** $S \times S$ का एक उपसमुच्चय R होता है। हम संबंध R को ~ द्वारा भी व्यक्त करते हैं, जिसे '$a \sim b$ iff $(a, b) \in R$' द्वारा परिभाषित किया जाता है।

यहाँ, हम कभी-कभी $\mathbf{a \sim b}$ को $\mathbf{aRb}$ के रूप में लिखते हैं।

ii) S पर संबंध R **स्वतुल्य (reflexive)** कहलाता है, यदि $(a, a) \in R \ \forall \ a \in S$, अर्थात्, $a \sim a \ \forall \ a \in S$.

iii) S पर संबंध R **सममित (symmetric)** कहलाता है, यदि $(a, b) \in R \Rightarrow (b, a) \in R$, अर्थात्, $a \sim b \Rightarrow b \sim a$, $a, b \in S$ के लिए।

iv) S पर संबंध R **संक्रामक (transitive)** कहलाता है, यदि

$(a, b) \in R$ और $(b, c) \in R \Rightarrow (a, c) \in R$, अर्थात्,

$a \sim b, b \sim c \Rightarrow a \sim c$; $a, b, c \in S$ के लिए।

v) S पर संबंध R एक **तुल्यता संबंध (equivalence relation)** कहलाता है, यदि वह स्वतुल्य, सममित और संक्रामक होता है।

आइए एक उदाहरण पर विचार करें।

उदाहरण 2: $\mathbb{C}$ पर '$a \sim b$ iff $|a| = |b|$' द्वारा दिए जाने वाले संबंध ~ पर विचार कीजिए। यहाँ, $R = \{(a, b) \in \mathbb{C} \times \mathbb{C} \mid |a| = |b|\}$. जाँच कीजिए कि R, $\mathbb{C}$ पर एक तुल्यता संबंध है या नहीं।

हल: क्योंकि $|a| = |a| \ \forall \ a \in \mathbb{C}$, इसलिए ~ स्वतुल्य है।

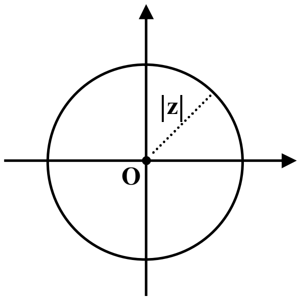
$a, b \in \mathbb{C}$ के लिए, यदि $|a| = |b|$, तो $|b| = |a|$. अतः, ~ सममित है।

$a, b, c \in \mathbb{C}$ के लिए, यदि $|a| = |b|$ और $|b| = |c|$, तब $|a| = |c|$. अतः, ~ संक्रामक है।

इस प्रकार, $\mathbb{C}$ पर ~ एक तुल्यता संबंध है, अर्थात्, $\mathbb{C}$ पर R एक तुल्यता संबंध है।

***

उदाहरण 2 में, एक निश्चित $z \in \mathbb{C}$ के लिए, $\mathbb{C}$ के उपसमुच्चय $[z] = \{\alpha \in \mathbb{C} \mid |\alpha| = |z|\}$ पर ग़ौर कीजिए। अतः, $[z]$ आकृति 2 में दर्शाए गए वृत्त पर स्थित सभी बिंदुओं का अपरिमित समुच्चय है। आकृति 2 से आप देख सकते हैं कि यदि $|z| \neq |z_1|$, तो $[z] \cap [z_1] = \emptyset$; तथा यदि $|z| = |z_1|$, तो $[z] = [z_1]$.



आकृति 2: केन्द्र O(0, 0) और त्रिज्या |z| वाला वृत्त जहाँ $z \in \mathbb{C}$.

साथ ही, $\mathbb{C} = \bigcup_{z \in \mathbb{C}} [z]$. इस सम्मिलन में, समान मापांक (modulus) वाले सभी अवयव एक उपसमुच्चय में हो जाते हैं। तथा हर ऐसा उपसमुच्चय अन्य उपसमुच्चयों से असंयुक्त है। समुच्चय [z] एक विशिष्ट स्थिति है उसकी, जिसे हम अब परिभाषित करेंगे।

परिभाषा: किसी समुच्चय S पर एक तुल्यता संबंध R दिया रहने पर, $[a] = \{b \in S \mid (a, b) \in R\}$, $a \in S$ का **तुल्यता वर्ग (equivalence class)** कहलाता है।

ध्यान दीजिए कि [a], S का एक उपसमुच्चय है। साथ ही, $b \in [a]$ iff $[a] = [b]$, क्योंकि R एक तुल्यता संबंध है।

इस प्रकार, $a, b \in S$ के लिए, $[a] = [b]$ या $[a] \cap [b] = \emptyset$.

साथ ही, किसी भी $z \in S$ के लिए $z \in [z]$.

इसलिए, हम S को असंयुक्त तुल्यता वर्गों के एक सम्मिलन के रूप में लिख सकते हैं।

आइए, तुल्यता संबंधों तथा संगत वर्गों के कुछ और उदाहरणों पर विचार करें।

उदाहरण 3: संबंध $R = \{(a, a+5m) \mid a, m \in \mathbb{Z}\}$ पर विचार कीजिए। दूसरे शब्दों में, $(a, b) \in R$ iff $\mathbb{Z}$ में $5 \mid (a-b)$ है। दर्शाइए कि R एक तुल्यता संबंध है, तथा 1 के तुल्यता वर्ग में दो अलग-अलग अवयव ज्ञात कीजिए।

हल: क्योंकि $5 \mid (a-a)$, इसलिए $(a, a) \in R \; \forall \; a \in \mathbb{Z}$. अतः, R स्वतुल्य है।

आगे, $(a, b) \in R \Rightarrow 5 \mid (a-b)$

$$\Rightarrow \exists\, c \in \mathbb{Z} \text{ s.t. } (a-b) = 5c$$

$$\Rightarrow (b-a) = 5(-c)$$

$$\Rightarrow 5 \mid (b-a)$$

$$\Rightarrow (b, a) \in R.$$

अतः, R सममित है।

अंत में, मान लीजिए कि R में (a, b) और (b, c) हैं।

तब, $\exists\, m, n \in \mathbb{Z}$ s.t. $(a-b) = 5m$ तथा $(b-c) = 5n$. इस प्रकार, $(a-c) = (a-b) + (b-c) = 5(m+n)$, अर्थात्, $5 \mid (a-c)$.

अतः, $(a, c) \in R$. इसलिए, R संक्रामक है।

इस प्रकार, R एक तुल्यता संबंध है।

$[1]=\{a\in\mathbb{Z} \mid (a,1)\in R\}=\{a\in\mathbb{Z} \mid (a-1)=5m,$ किसी $m\in\mathbb{Z}$ के लिए$\}$

$=\{5m+1 \mid m\in\mathbb{Z}\}.$

अतः, [1] में दो अलग अवयव ज्ञात करने के लिए, हम $m\in\mathbb{Z}$ के दो अलग मान लेते हैं, मान लीजिए ये $m=0$ और $m=1$ हैं। तब, हमें [1] में दो अलग अवयव 1 और 6 प्राप्त होते हैं।

***

आइए अब उदाहरण 3 को व्यापकीकृत करें।

उदाहरण 4: मान लीजिए कि $n\in\mathbb{N}$. 'aRb iff $n \mid (a-b)$' द्वारा दिए जाने वाला $\mathbb{Z}$ पर एक संबंध R परिभाषित कीजिए। दर्शाइए कि $\mathbb{Z}$ पर R एक तुल्यता संबंध है। R के कितने अलग-अलग तुल्यता वर्गों का $\mathbb{Z}$ एक सम्मिलन है, तथा क्यों?

हल: आप उदाहरण 3 में अपनाई गई प्रक्रिया के अनुसार यह दर्शा सकते हैं कि R एक तुल्यता संबंध है।

तुल्यता वर्गों को ज्ञात करने के लिए, आइए विभाजन ऐल्गोरिद्म का उपयोग करें। कोई भी $a\in\mathbb{Z}$ दिया होने पर, $\mathbb{Z}$ में ऐसे q और r हैं जिनसे कि

$$a=nq+r,\ 0\le r<n. \qquad \ldots(9)$$

अब, प्रत्येक $i=0,1,\ldots,n-1$ के लिए, $[i]=\{mn+i \mid m\in\mathbb{Z}\}$, जैसा कि आपने उदाहरण 3 में देखा था।

साथ ही, (9) से $[a]=[r]$ किसी r के लिए, जहाँ $0\le r<n$. अतः, $[0],[1],\ldots,[n-1]$ ही सभी तुल्यता वर्ग हैं।

आगे, यदि किसी j के लिए, जहाँ $0\le j<n$, $[i]=[j]$ है, तो किन्हीं $m,m'\in\mathbb{Z}$ के लिए, $mn+i=m'n+j \Rightarrow n(m-m')=j-i \Rightarrow n \mid (j-i)$.

परंतु $|i-j|<n$ है।

इसलिए, $n \mid (j-i)$ तभी संभव है, जबकि $j-i=0$ हो, अर्थात्, $i=j$ हो। और तब, $m=m'$.

अतः, $[0],[1],\ldots,[n-1]$, n अलग वर्ग हैं, तथा ये ही सभी वर्ग हैं।

अतः, $\mathbb{Z}=[0]\cup[1]\cup\ldots\cup[n-1]$, जो n असंयुक्त तुल्यता वर्गों का एक सम्मिलन है।

***

उदाहरण 4 में दिया तुल्यता संबंध '**समशेषता मॉड्यूलो (congruence modulo** n)' कहलाता है। हम $\mathbf{a\equiv b\,(mod\ n)}$ लिखते हैं (इसे '**a, b मोड्यूलो n के समशेष है**' पढ़ते हैं।), यदि उदाहरण 4 में $[a]=[b]$ है, यानी यदि $n \mid (a-b)$.

नोट कीजिए कि $\mathbb{Z}_n$ समुच्चयों का समुच्चय है, क्योंकि हर $i \in \mathbb{N}\cup\{0\}$ के लिए $[i]$ एक समुच्चय है।

यहाँ हम सभी तुल्यता वर्गों के समुच्चय को $\mathbb{Z}_n$ से दर्शाते हैं। अर्थात् $\mathbb{Z}_n = \{[0],[1],\ldots,[n-1]\}$.

उपरोक्त उदाहरण हमें निम्नलिखित परिभाषा की ओर ले जाते हैं।

परिभाषा: एक अरिक्त समुच्चय S का **विभाजन (partition)**, S के असंयुक्त अरिक्त उपसमुच्चयों S_i, $i \in I$, का एक संग्रह होता है जहाँ $S = \bigcup_{i \in I} S_i$ । यहाँ I सूचित करने वाला समुच्चय (indexing set) है।

उपसमुच्चय S_i इस विभाजन के खाने **(cells)** कहलाते हैं।

इस प्रकार, यदि S का खानों S_i में विभाजन होता है, तो S का प्रत्येक अवयव एक और केवल एक ही खाने में स्थित होता है।

एक विभाजन में अनंततः अनेक खाने हो सकते हैं, या परिमित संख्या में खाने हो सकते हैं। जैसे कि, उदाहरण 4 में $\mathbb{Z}$ का विभाजन n वर्गों में हुआ है। यहाँ खाने हैं $[0], [1], \ldots, [n-1]$. परंतु उदाहरण 2 में $\mathbb{C}$ अनंततः अनेक खानों में विभाजित हुआ है, तथा इनमें से हर खाना एक अपरिमित समुच्चय है।

आइए अब विभाजनों को तुल्यता संबंधों से जोड़ने वाले एक परिणाम को सिद्ध करें।

प्रमेय 9: एक अरिक्त समुच्चय S का विभाजन S पर एक तुल्यता संबंध परिभाषित करता है। विलोमतः, S पर एक तुल्यता संबंध S पर एक विभाजन परिभाषित करता है।

उपपत्ति: सर्वप्रथम, मान लीजिए कि $\{S_i \mid i \in I\}$ समुच्चय S पर एक विभाजन के खानों का समुच्चय है, जहाँ I एक सूचकांकी समुच्चय है।

$a, b \in S$ के लिए, 'aRb iff a और b विभाजन के एक ही खाने में स्थित हैं' द्वारा S पर एक संबंध R को परिभाषित कीजिए।

इस प्रकार, aRa है, क्योंकि a स्वयं के ही खाने में स्थित है। अतः, R स्वतुल्य है।

आगे, यदि aRb है, तो a और b के ही खाने में स्थित है। अतः, b और a एक ही खाने में स्थित हैं। इस प्रकार, bRa है। अर्थात्, R सममित है।

अंत में, यदि aRb और bRc हैं, तो a और b एक खाने, मान लीजिए S_i, में स्थित हैं तथा b और c एक खाने S_j में स्थित हैं। क्योंकि $S_i \cap S_j$ में b स्थित है, इसलिए $S_i \cap S_j \neq \emptyset$. इस प्रकार, $i = j$. इसलिए, S_i में दोनों a और c स्थित हैं। अतः, aRc है। अर्थात्, R संक्रामक है।

अतः, R एक तुल्यता संबंध है।

इसके विलोम को सिद्ध करने के लिए, S पर कोई तुल्यता संबंध R लीजिए। मान लीजिए कि किन्हीं $a, b \in S$ के लिए, $[a] \cap [b] \neq \emptyset$.

मान लीजिए कि $x \in [a] \cap [b]$. तब, xRa और xRb है, जिससे aRx और xRb हैं। अतः, aRb है। अर्थात्, $[a] = [b]$.

इस प्रकार, सभी तुल्यता वर्ग एक दूसरे के असंयुक्त हैं या बराबर हैं।

साथ ही, किसी भी $a \in S$ के लिए, $a \in [a]$.

अतः, सभी तुल्यता वर्ग मिलकर S का एक विभाजन बनाते हैं। ■

उदाहरण के लिए, उदाहरण 2 में तुल्यता संबंध $\mathbb{C}$ को अनंततः अनेक खानों में विभाजित करता है, और ये खाने $\mathbb{R}^2$ में सकेन्द्रीय वृत्त हैं, जिनके केन्द्र (0, 0) पर हैं, जैसा कि आप आकृति 2 में देख चुके हैं।

अब आप कुछ अन्य संबंधों को देखिए और मालूम कीजिए कि क्या ये संबद्ध समुच्चयों के विभाजन प्रदान करते हैं या नहीं।

E16) जाँच कीजिए कि निम्नलिखित संबंध $\mathbb{Z}^*$ पर तुल्यता संबंध हैं या नहीं :

i) nRm iff $nm > 0$,

ii) nRm iff n और m के आधार दस संकेतन में अंकों की संख्याएँ समान हैं।

जो R तुल्यता संबंध हैं, उनके लिए $\mathbb{Z}^*$ के संगत विभाजन प्राप्त कीजिए।

E17) दर्शाइए कि सभी सत्य गणितीय कथनों के समुच्चय पर, 'ARB iff $A \Rightarrow B$' एक स्वतुल्य और संक्रामक संबंध है, परंतु सममित नहीं है।

E18) 'समशेषता मॉड्यूलो 8' और 'समशेषता मॉड्यूलो 1' के संगत, $\mathbb{Z}$ के विभाजनों के सभी खाने ज्ञात कीजिए।

आइए अब एक अन्य बीजीय वस्तु पर दृष्टि डालें, जो बीजगणित में अति रोचक है। हम इन वस्तुओं का इस पाठ्यक्रम में उदाहरणों के रूप में उपयोग करेंगे।

1.4 आव्यूहों से परिचय

आपने गणित की अब तक की पढ़ाई में निम्नलिखित जैसे कई रैखिक समीकरणों के समान हलों को ज्ञात करने की विधियों का अध्ययन किया है :

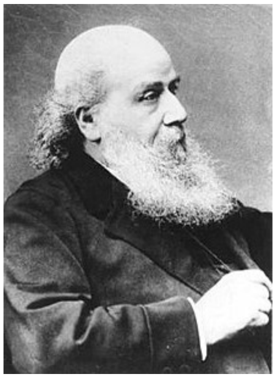
$$\left.\begin{array}{l} 2x + 3y = 5 \\ 3x + 2y = -5 \end{array}\right\} \qquad \ldots(I)$$

इन दोनों समीकरणों को एक साथ लेकर चरों x और y के गुणांकों तथा अचर पदों को पंक्तियों और स्तंभों में निम्नलिखित तरीक़े से भी व्यवस्थित करके निरूपित किया जा सकता है :

	x का गुणांक ↓	y का गुणांक ↓	अचर पद ↓
पहली समीकरण	2	3	5
दूसरी समीकरण	3	2	−5

इस तरह से हम एक आयताकार व्यवस्था प्राप्त करते हैं, जिसकी प्रविष्टियाँ संख्याएँ हैं, जैसे नीचे दिया गया है :

$$\begin{bmatrix} 2 & 3 & 5 \\ 3 & 2 & -5 \end{bmatrix}$$



आकृति 3: जे,जे, सिल्वेस्टर (1814-1897)

आप आगे चलकर देखेंगे कि इस तरह की व्यवस्था का उपयोग करते हुए, हम रैखिक निकाय (system) (I) को क्यों नीचे दर्शाए अनुसार लिख सकते हैं :

$$\begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 5 \\ -5 \end{bmatrix}$$

जैसा कि आप 5वें सेमेस्टर के पाठ्यक्रम में देखेंगे, ऐसी व्यवस्थाएँ कुछ रैखिक निकायों के हलों को ज्ञात करने में बहुत सहायक रहती हैं। ये वे निकाय हैं जिनमें चरों की संख्या बहुत बड़ी होती है, तथा संबद्ध गुणांकों का हस्तकौशल द्वारा परिकलित करना सरल नहीं होता है।

ऐसी आयताकार व्यवस्थाओं का बीजगणित में बहुत महत्व है। इसीलिए, हम आपका परिचय इनसे करा रहे हैं। इस भाग में, आप इनके कुछ मौलिक गुणों का अध्ययन करेंगे। आगे चलकर आप इनके बारे में और अध्ययन करेंगे।

ऐतिहासिक रूप से कहा जाए, तो इन ऐसी व्यवस्थाओं को इंग्लैंड में 19वीं शताब्दी में बीजीय महत्वता प्राप्त हुई। गणितज्ञों जेम्स सिल्वेस्टर (James Sylvester) और आर्थर केली (Arthur Cayley) ने सर्वप्रथम इनका अनुप्रयोग रैखिक समीकरणों के निकायों के अध्ययन के लिए किया था।

अतः, आइए इन वस्तुओं को परिभाषित करें।

परिभाषाएँ: मान लीजिए S एक अरिक्त समुच्चय है।

i) S के mn अवयवों को **गुरूकोष्ठकों (square brackets) में परिबद्ध** m लेटे पंक्तियों (rows) और n खड़े स्तंभों (columns) में व्यवस्थित करके जो आयताकार व्यवस्था प्राप्त होती है, वह **S पर एक $m \times n$ आव्यूह (matrix)** या **कोटि (order) $m \times n$ वाला आव्यूह** कहलाता है।

ii) S पर एक $n \times n$ आव्यूह **S पर कोटि n वाला एक वर्ग आव्यूह (square matrix)** कहलाता है।

iii) S पर एक $1 \times n$ आव्यूह S पर एक **पंक्ति सदिश (row vector)** कहलाता है तथा S पर एक $n \times 1$ आव्यूह S पर एक **स्तंभ सदिश (column vector)** कहलाता है।

किसी समुच्चय S पर सभी $m \times n$ आव्यूहों के समुच्चय को $\mathbb{M}_{m \times n}(S)$ द्वारा व्यक्त किया जाता है, तथा S पर सभी $n \times n$ आव्यूहों के समुच्चय को, $\mathbb{M}_n(S)$ द्वारा व्यक्त किया जाता है।

उदाहरणार्थ, $\begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix}$, $\mathbb{Z}$ पर कोटि 2 वाला एक वर्ग आव्यूह है।

$\begin{bmatrix} x \\ y \end{bmatrix}$ और $\begin{bmatrix} 5 \\ -5 \end{bmatrix}$, $\mathbb{M}_{2\times1}(\mathbb{R})$ में आव्यूह हैं, जहाँ $x, y \in \mathbb{R}$. ये $\mathbb{R}$ पर स्तंभ सदिशों के भी उदाहरण हैं।

$m \times n$ आव्यूह $\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$ को $\mathbf{[a_{ij}]_{m\times n}}$ द्वारा, या केवल $\mathbf{[a_{ij}]}$**,** द्वारा (यदि m और n पर ज़ोर देने की आवश्यकता नहीं है।) व्यक्त किया जाता है।

यहाँ, a_{ij} वह अवयव है जो iवीं पंक्ति और jवें स्तंभ में स्थित है, अर्थात् a_{ij} आव्यूह का (i, j)वाँ अवयव है।

यदि $A = [a_{ij}]$ कोटि n वाला एक वर्ग आव्यूह है, तो अवयव $a_{11}, a_{22}, \dots, a_{nn}$ आव्यूह A के **विकर्ण अवयव (diagonal elements)** कहलाते हैं, तथा **A का विकर्ण** क्रमित समुच्चय (ordered set) $\{a_{11}, a_{22}, \dots, a_{nn}\}$ है, अर्थात्, इसके अवयव दिये गए क्रम में ही हैं।

उदाहरणार्थ, $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ का विकर्ण $\{1, 4\}$ है, $\{4, 1\}$ नहीं है। यहाँ $a_{12} = 3$ और $a_{21} = 2$.

आप प्रायः $\mathbb{M}_{m\times n}(\mathbb{C})$ के साथ कार्य करेंगे, जो उन सभी $m \times n$ आव्यूहों का समुच्चय है जिनकी प्रविष्टियाँ सम्मिश्र संख्याएँ हैं।

ध्यान दीजिए कि $\mathbb{M}_{m\times n}(\mathbb{Z}) \subseteq \mathbb{M}_{m\times n}(\mathbb{Q}) \subseteq \mathbb{M}_{m\times n}(\mathbb{R}) \subseteq \mathbb{M}_{m\times n}(\mathbb{C})$, क्योंकि $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

आइए अब एक ऐसी रोज़मर्रा ज़िन्दगी की (सरलीकृत) स्थिति पर दृष्टि डालें जिसमें एक आव्यूह उत्पन्न हो सकता है।

उदाहरण 5: किसी कॉलेज के इतिहास प्रभाग में 5 पुरुष और 3 महिला सदस्य हैं, गणित प्रभाग में 4 महिला और 3 पुरुष सदस्य हैं तथा कम्प्यूटर विज्ञान प्रभाग में 7 महिला सदस्य हैं। इस सूचना को एक आव्यूह के रूप में प्रस्तुत कीजिए।

हल: इस सूचना को प्रस्तुत करने की एक विधि है निम्नलिखित 3×2 आव्यूह :

$$\begin{array}{l} \\ \text{इतिहास} \\ \text{गणित} \\ \text{कम्प्यूटर विज्ञान} \end{array} \begin{array}{c} \begin{array}{cc} \text{पुरुष} & \text{महिला} \end{array} \\ \begin{bmatrix} 5 & 3 \\ 3 & 4 \\ 0 & 7 \end{bmatrix} \end{array}$$

एक अन्य संभावना है निम्नलिखित 2×3 आव्यूह :

$$\begin{array}{c} \\ \text{महिला} \\ \text{पुरुष} \end{array} \begin{array}{c} \begin{array}{ccc} \text{इतिहास} & \text{गणित} & \text{कम्प्यूटर विज्ञान} \end{array} \\ \begin{bmatrix} 3 & 4 & 7 \\ 5 & 3 & 0 \end{bmatrix} \end{array}$$

इनमें से प्रत्येक निरूपण तुरंत हमें बताता है कि दिए हुए प्रभागों में कितने सदस्य हैं तथा इनमें से कितने महिला / पुरुष हैं।

***

अनेक दैनिक जीवन की समस्याएँ हैं जिनको आव्यूहों के उपयोग से गणित हल करने में सहायता करती है। इनमें से कुछ के बारे में आप 5वें सेमेस्टर पाठ्यक्रम में सीखेंगे। अभी के लिए, निम्नलिखित प्रश्नों को हल करके आव्यूहों के कुछ आदी हो जाएँ।

E19) मान लीजिए कि $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 0 \\ 0 & 0 & 7 \end{bmatrix}$ और $B = \begin{bmatrix} 2 & 5 & 3 & 2 \\ 5 & 4 & 1 & 5 \\ 0 & 3 & 2 & 0 \end{bmatrix}$. निम्नलिखित बताइएः

i) A और B के $(2, 3)$वें अवयव,

ii) A की तीसरी पंक्ति,

iii) A और B में से वर्ग आव्यूहों के विकर्ण,

iv) B का प्रथम स्तंभ,

v) B की चौथी पंक्ति।

E20) $\mathbb{M}_{4\times2}(\mathbb{Q}) \setminus \mathbb{M}_{4\times2}(\mathbb{Z})$ का एक अवयव लिखिए।

E21) $\mathbb{C}$ पर एक ऐसा वर्ग आव्यूह दीजिए जिसका विकर्ण $\{e, i, \pi, -1\}$ है, तथा जिसका $i > j$ के लिए (i, j)वाँ अवयव 1 है, और $i < j$ के लिए (i, j)वाँ अवयव 0 है, जहाँ $i, j = 1, 2, 3, 4$.

आइए अब देखें कि दो आव्यूह बराबर कब होते हैं। पहले तो आप $\mathbb{R}$ पर दो अलग 2×2 आव्यूह लिखें। क्या किन्हीं i और j के लिए, एक आव्यूह की (i, j)वीं प्रविष्टि में और दूसरे आव्यूह की (i, j)वीं प्रविष्टि में कोई अंतर है? यदि नहीं, तो ये आव्यूह अलग नहीं हैं। अपितु वे बराबर हैं। उदाहरणार्थ, दो 1×1 आव्यूह $[2]$ और $[2]$ बराबर हैं। परंतु, निम्नलिखित परिभाषा के अनुसार, $[2] \neq [-2]$.

परिभाषा: दो आव्यूह **बराबर (equal)** होते हैं, यदि

i) उनकी कोटि समान हैं, अर्थात्, दोनों की पंक्तियों की संख्या समान है और दोनों की स्तंभों की संख्या भी समान है; तथा

ii) सभी संगत स्थानों पर दोनों के अवयव समान हैं।

निम्नलिखित उदाहरण से आपको स्पष्ट हो जाएगा कि बराबर आव्यूहों से हमारा क्या मतलब है।

उदाहरण 6: यदि $\begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} x & y \\ z & 3 \end{bmatrix}$, तो x, y और z के मान क्या हैं?

हल: सर्वप्रथम, ध्यान दीजिए कि दोनों आव्यूह समान कोटि, अर्थात् 2×2 के हैं।

अब इन आव्यूहों को बराबर होने के लिए, सभी i, j के लिए इन दोनों के (i, j)वें अवयव बराबर होने चाहिए। अतः, $x = 1, y = 0$ और $z = 2.$

***

अब, कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E22) क्या $\mathbb{R}$ पर कोई आव्यूह $\mathbb{N}$ पर किसी आव्यूह के बराबर हो सकता है? क्यों, या क्यों नहीं?

E23) क्या [3 4] और $\begin{bmatrix} 3 \\ 4 \end{bmatrix}$ बराबर हैं? क्यों?

E24) क्या $\begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 1 \end{bmatrix}$? क्यों?

आइए अब $\mathbb{C}$ पर आव्यूहों की कुछ संक्रियाओं पर विचार करें।

परिवर्त

सर्वप्रथम, $\mathbb{M}_{2\times3}(\mathbb{R})$ में किसी आव्यूह, मान लीजिए $A = \begin{bmatrix} 2 & 5 & -1 \\ 0 & 0.5 & \sqrt{2} \end{bmatrix}$, पर विचार कीजिए।

अब $B = \begin{bmatrix} 2 & 0 \\ 5 & 0.5 \\ -1 & \sqrt{2} \end{bmatrix} \in \mathbb{M}_{3\times2}(\mathbb{R})$ को देखिए।

क्या आप A और B में कोई संबंध देख रहे हैं? A की प्रथम पंक्ति और B के प्रथम स्तंभ पर विचार कीजिए। क्या ये समान नहीं हैं? इसी प्रकार, A की दूसरी पंक्ति B का दूसरा स्तंभ है। वस्तुतः, B, A का परिवर्त है, जैसा कि आपको निम्नलिखित परिभाषा बताएगी।

परिभाषा: मान लीजिए कि S एक अरिक्त समुच्चय है। आव्यूह $A = [a_{ij}] \in \mathbb{M}_{m\times n}(S)$ का **परिवर्त (transpose)** ऐसा $n \times m$ आव्यूह है जिसकी पंक्तियाँ A के स्तंभ होते हैं, **उसी** क्रम में। इसे $\mathbf{A^t}$ द्वारा व्यक्त किया जाता है। इस प्रकार, $A^t = [a_{ji}] \in \mathbb{M}_{n\times m}(S).$

उदाहरणार्थ, यदि $A = \begin{bmatrix} 3 & 2 & 0 & 0 \\ \pi & 3+i & 0 & 0 \end{bmatrix}$, तो $A^t = \begin{bmatrix} 3 & \pi \\ 2 & 3+i \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$. ध्यान दीजिए कि यहाँ $A^t \neq \begin{bmatrix} \pi & 3 \\ 3+i & 2 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$ क्योंकि A^t के स्तंभों को लिखते समय, A की पंक्तियों के क्रम को वही रखना है।

साथ ही, ध्यान दीजिए कि $(A^t)^t = \begin{bmatrix} 3 & 2 & 0 & 0 \\ \pi & 3+i & 0 & 0 \end{bmatrix} = A.$

परिभाषा से, आप देख सकते हैं कि, उपरोक्त उदाहरण की ही तरह, **किसी भी आव्यूह A के लिए, $(A^t)^t = A$ होता** है।

अब 'परिवर्त' के बारे में निम्नलिखित टिप्पणी पर विचार कीजिए।

टिप्पणी 7: ध्यान दीजिए कि $f : \mathbb{M}_{m\times n}(\mathbb{C}) \to \mathbb{M}_{n\times m}(\mathbb{C}) : f(A) = A^t$ एक सुपरिभाषित फलन है। इसका कारण यह है कि यदि $A = B$, तो A की iवीं पंक्ति B की iवीं पंक्ति है $\forall\ i = 1,\ldots,m.$ इसलिए A^t का iवाँ स्तंभ B^t का iवाँ स्तंभ है $\forall\ i = 1,\ldots,m.$ अतः, $A^t = B^t$.

आइए अब $\mathbb{C}$ पर $m \times n$ आव्यूहों के समुच्चय पर एक द्वि-आधारी संक्रिया पर विचार करें।

आव्यूहों का योग

आइए $\mathbb{M}_{2\times 3}(\mathbb{C})$ में $\begin{bmatrix} 2 & 1 & -1 \\ \pi & i & 0.7 \end{bmatrix}$ और $\begin{bmatrix} 2 & 5 & 0.5 \\ 0 & -1 & \sqrt{2} \end{bmatrix}$ पर विचार करें। क्या इनको जोड़ने या घटाने की कोई स्वाभाविक विधि है? क्या दोनों के संगत स्थानों के अवयवों को जोड़ें? तब

$$\begin{bmatrix} 2 & 1 & -1 \\ \pi & i & 0.7 \end{bmatrix} + \begin{bmatrix} 2 & 5 & 0.5 \\ 0 & -1 & \sqrt{2} \end{bmatrix} = \begin{bmatrix} 2+2 & 1+5 & -1+0.5 \\ \pi+0 & i-1 & 0.7+\sqrt{2} \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 6 & -0.5 \\ \pi & i-1 & 0.7+\sqrt{2} \end{bmatrix}.$$

वास्तव में, यही वह विधि है जिससे आव्यूह के योग (जोड़ने) और व्यवकलन (घटाने) को व्यापक रूप में परिभाषित किया जाता है, जैसा कि अब आप देखेंगे।

यह परिभाषा किसी भी ऐसे समुच्चय S पर आव्यूहों के लिए सत्य है, जिस पर योग और व्यवकलन द्वि-आधारी संक्रियाएँ हैं।

परिभाषा: $\mathbb{M}_{m\times n}(\mathbb{C})$ में $A = [a_{ij}]$ और $B = [b_{ij}]$ के लिए, $\mathbf{A + B}$ को आव्यूह $[\mathbf{a_{ij} + b_{ij}}] \in \mathbb{M}_{m\times n}(\mathbb{C})$ के रूप में परिभाषित किया जाता है, तथा $\mathbf{A - B}$ को आव्यूह $[\mathbf{a_{ij} - b_{ij}}] \in \mathbb{M}_{m\times n}(\mathbb{C})$ के रूप में परिभाषित किया जाता है।

ध्यान दीजिए कि इन परिभाषाओं से दी गई जोड़ और घटाना, $\mathbb{M}_{m\times n}(\mathbb{C})$ पर द्वि-आधारी संक्रियाएँ हैं।

यहाँ एक महत्वपूर्ण टिप्पणी पर विचार कीजिए।

टिप्पणी 8: दी हुई परिभाषा में, ध्यान दीजिए कि **केवल एक ही कोटि (order) वाले दो आव्यूहों को जोड़ा या घटाया जा सकता** है। उदाहरणार्थ, $\begin{bmatrix}2\\1\end{bmatrix}+\begin{bmatrix}3 & 5\end{bmatrix}$ परिभाषित नहीं है, क्योंकि $\begin{bmatrix}2\\1\end{bmatrix}$ एक 2×1 आव्यूह है तथा $\begin{bmatrix}3 & 5\end{bmatrix}$ एक 1×2 आव्यूह है।

आइए उन संक्रियाओं के कुछ विस्तृत उदाहरणों को देखें, जिनका आपने अभी तक अध्ययन किया है।

उदाहरण 7: $A+B, B+A, A-B$ और $B-A$ ज्ञात कीजिए, जहाँ

$$A=\begin{bmatrix}-i & 1.5\\0.2 & i\\-1 & 0\end{bmatrix}, B=\begin{bmatrix}\sqrt{2} & \sqrt{3}\\-\sqrt{2} & -\sqrt{3}\\\pi & 4\end{bmatrix}\in\mathbb{M}_{3\times2}(\mathbb{C}).$$

साथ ही, यह भी निश्चित कीजिए कि $A+B=B+A$ और $A-B=B-A$ है या नहीं।

हल: परिभाषा से,

$$A+B=\begin{bmatrix}-i+\sqrt{2} & 1.5+\sqrt{3}\\0.2-\sqrt{2} & i-\sqrt{3}\\-1+\pi & 4\end{bmatrix}, B+A=\begin{bmatrix}\sqrt{2}-i & \sqrt{3}+1.5\\-\sqrt{2}+0.2 & -\sqrt{3}+i\\\pi-1 & 4\end{bmatrix},$$

$$A-B=\begin{bmatrix}-i-\sqrt{2} & 1.5-\sqrt{3}\\0.2+\sqrt{2} & i+\sqrt{3}\\-1-\pi & -4\end{bmatrix}, B-A=\begin{bmatrix}\sqrt{2}+i & \sqrt{3}-1.5\\-\sqrt{2}-0.2 & -\sqrt{3}-i\\\pi+1 & 4\end{bmatrix}.$$

ध्यान दीजिए कि $A+B$ और $B+A$ की सभी संगत प्रविष्टियाँ समान हैं। अतः, $A+B=B+A.$

क्योंकि $A-B$ और $B-A$ की $(1, 1)$वीं प्रविष्टियाँ समान नहीं हैं, इसलिए $A-B\neq B-A.$

***

उदाहरण 8: मान लीजिए कि $A=\begin{bmatrix}2 & 1 & 5\\-3 & i & 5i\end{bmatrix}$ और $B=\begin{bmatrix}-2 & 1 & 7\\0 & 9 & -8\end{bmatrix}\in\mathbb{M}_{2\times3}(\mathbb{C})$. $A^t, B^t, A+B$ और $(A+B)^t$ ज्ञात कीजिए। क्या $(A+B)^t=A^t+B^t$? क्यों?

हल: सर्वप्रथम, $A+B$ परिभाषित है, क्योंकि A और B की कोटियाँ समान हैं।

यहाँ, $A+B=\begin{bmatrix} 0 & 2 & 12 \\ -3 & 9+i & -8+5i \end{bmatrix}$.

अब, $A^t=\begin{bmatrix} 2 & -3 \\ 1 & i \\ 5 & 5i \end{bmatrix}, B^t=\begin{bmatrix} -2 & 0 \\ 1 & 9 \\ 7 & -8 \end{bmatrix}, (A+B)^t=\begin{bmatrix} 0 & -3 \\ 2 & 9+i \\ 12 & -8+5i \end{bmatrix}$.

साथ ही, $A^t+B^t=\begin{bmatrix} 0 & -3 \\ 2 & 9+i \\ 12 & -8+5i \end{bmatrix}$.

$(A+B)^t$ और A^t+B^t की संगत प्रविष्टियों को देख कर आप कह सकते हैं कि $(A+B)^t=A^t+B^t$.

***

उदाहरण 9: यदि $A\in\mathbb{M}_{2\times3}(\mathbb{R})$, तो क्या $A+A^t$ परिभाषित है? m और n पर कौनसे प्रतिबंधों के अधीन $\mathbb{R}$ पर किसी $m\times n$ आव्यूह A के लिए, $A-A^t$ परिभाषित होगा?

हल: क्योंकि A एक 2×3 आव्यूह है, इसलिए A^t एक 3×2 आव्यूह है। अतः, A और A^t की कोटियाँ अलग-अलग हैं। अतः, $A+A^t$ परिभाषित नहीं है।

आगे, क्योंकि A एक $m\times n$ आव्यूह है तथा A^t एक $n\times m$ आव्यूह है, इसलिए $A-A^t$ केवल तभी परिभाषित होगा, जब $m=n$ हो, अर्थात्, A एक वर्ग आव्यूह हो।

***

उपरोक्त उदाहरणों में जो आपने देखा है, वह किन्हीं भी दो आव्यूहों के लिए सत्य है। आइए इस परिणाम का औपचारिक रूप से कथन दें।

प्रमेय 10: मान लीजिए कि $A, B\in\mathbb{M}_{m\times n}(\mathbb{C})$. तब,

i) $A+B=B+A$,

ii) $(A+B)^t=A^t+B^t$.

उपपत्ति: यहाँ हम (ii) को सिद्ध करेंगे, तथा (i) को आपके लिए एक अभ्यास की तौर पर छोड़ रहे हैं (E27 देखिए)।

ii) मान लीजिए कि $A=[a_{ij}]$ और $B=[b_{ij}]$. तब, $A+B=[a_{ij}+b_{ij}]$.

अतः, $(A+B)^t=[c_{ij}]$, जहाँ

$c_{ij}=$ $(A+B)^t$ का (i, j)वाँ अवयव

$= A+B$ का (j, i)वाँ अवयव

$= a_{ji} + b_{ji}$

$=$ A के और B के (j, i)वें अवयवों का योग

$= A^t$ के और B^t के (i, j)वें अवयवों का योग

$= A^t + B^t$ का (i, j)वाँ अवयव।

इस प्रकार, $(A+B) = A^t + B^t$. ■

अब आप कुछ प्रश्नों को हल क्यों नहीं कर लेते?

E25) निम्नलिखित के योग ज्ञात कीजिए :

i) $\mathbb{M}_2(\mathbb{Z})$ में $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ और $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$,

ii) $\mathbb{M}_{m\times n}(\mathbb{C})$ में $[a_{ij}]_{m\times n} + [-a_{ij}]_{m\times n}$,

iii) $\mathbb{M}_{m\times n}(\mathbb{C})$ में $[a_{ij}]_{m\times n} + \mathbf{0}$, जहाँ $\mathbf{0}$ वह $m\times n$ आव्यूह है जिसकी प्रत्येक प्रविष्टि 0 है।

E26) उदाहरण 7 के A और B के लिए, प्रमेय 10(ii) का सत्यापन कीजिए।

E27) मान लीजिए कि $A, B, C \in \mathbb{M}_{m\times n}(S)$, जहाँ $S \subseteq \mathbb{C}, S \neq \emptyset$ तथा S पर '+' एक द्वि-आधारी संक्रिया है। जाँच कीजिए कि निम्नलिखित सत्य हैं या नहीं :

i) $A+B = B+A$,

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

E28) सिद्ध कीजिए कि

i) $(A^t)^t = A$, किसी भी $A \in \mathbb{M}_{m\times n}(\mathbb{C})$ के लिए।

ii) $(A+A^t)^t = A + A^t$ और $(A-A^t)^t = -(A-A^t)$, प्रत्येक $A \in \mathbb{M}_n(\mathbb{C})$ के लिए।

जैसा कि आप खंड 1, कलन, से जानते हैं, E27(i) कहता है कि S पर आव्यूहों का योग एक **क्रमविनिमेय** संक्रिया है तथा (ii) कहता है कि आव्यूहों का योग एक **साहचर्य** संक्रिया है। इकाई 2 में, आप इन गुणों का उपयोग करेंगे।

आइए अब **आव्यूहों पर दो अलग प्रकार के गुणन को** परिभाषित करें – अदिश गुणन और आव्यूह गुणन।

अदिश गुणन

आव्यूह $A = \begin{bmatrix} 2 & 5 & 2 \\ 3 & 5 & 7 \end{bmatrix}$ पर विचार कीजिए। अब $2A, A + A = \begin{bmatrix} 4 & 10 & 4 \\ 6 & 10 & 14 \end{bmatrix}$ के बराबर है। इसी तरह किसी $n \in \mathbb{N}$ के लिए, A को स्वयं के साथ n बार जोड़ने पर प्राप्त आव्यूह है। इसलिए, यह कहना सार्थक है कि

$$nA = \begin{bmatrix} 2n & 5n & 7n \\ 3n & 5n & 2n \end{bmatrix}, \text{ जहाँ } n \in \mathbb{N}.$$

इस प्रक्रिया को व्यापकीकृत करने पर, हम निम्नलिखित परिभाषा प्राप्त करते हैं।

यह परिभाषा तब भी लागू रहती है, जब $\mathbb{C}$ को $\mathbb{Z}$, $\mathbb{Q}$ या $\mathbb{R}$ से बदल दिया जाता है।

परिभाषा: किसी $\alpha \in \mathbb{C}$ और $A = [a_{ij}] \in \mathbb{M}_{m\times n}(\mathbb{C})$ के लिए, α और A के गुणनफल को **अदिश गुणनफल (scalar product)**, $\boldsymbol{\alpha A} = [\alpha a_{ij}]$ से परिभाषित किया जाता है।

ध्यान दीजिए कि यदि $A = [a_{ij}]$, तो $-\mathbf{A} = (-1)A = [(-1)a_{ij}]$

$$= [-a_{ij}].$$

अदिश गुणन के एक उदाहरण के तौर पर, निम्नलिखित पर विचार कीजिए।

$2+3i \in \mathbb{C}$ और $\begin{bmatrix} i & 5 \\ 0 & -i \end{bmatrix} \in \mathbb{M}_2(\mathbb{C})$ का गुणनफल है :

$$(2+3i)\begin{bmatrix} i & 5 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} (2+3i)i & (2+3i)5 \\ (2+3i)0 & (2+3i)(-i) \end{bmatrix}$$

$$= \begin{bmatrix} -3+2i & 10+15i \\ 0 & 3-2i \end{bmatrix}, \text{ क्योंकि } i^2 = -1.$$

इस तरह के गुणन के बारे में अब एक टिप्पणी पर ग़ौर कीजिए।

टिप्पणी 9: ऊपर परिभाषित किया गया गुणन 'अदिश' गुणन कहलाता है, क्योंकि उस समुच्चय के अवयव जिसमें आव्यूह की प्रविष्टियाँ हैं, इस स्थिति में $\mathbb{C}$, अदिश कहलाते हैं। यहाँ गुणन एक फलन $\bullet : \mathbb{C} \times \mathbb{M}_{m\times n}(\mathbb{C}) \to \mathbb{M}_{m\times n}(\mathbb{C})$ है। इस प्रकार, अदिश गुणन $\mathbb{M}_{m\times n}(\mathbb{C})$ पर एक द्वि-आधारी संक्रिया **नहीं** है।

आइए कुछ उदाहरणों पर विचार करें। इसके साथ-साथ आप कुछ ऐसे प्रारंभिक गुणों का अध्ययन करेंगे जो अब तक आपके द्वारा अध्ययन की गई आव्यूहों पर संक्रियाओं से संबंधित हैं।

उदाहरण 10: मान लीजिए कि $A = \begin{bmatrix} 2 & 1 \\ 7 & -1 \\ -0.5 & 0 \end{bmatrix}, B = \begin{bmatrix} 0.3 & -1/3 \\ 1 & 5 \\ -5 & 8 \end{bmatrix} \in \mathbb{M}_{3\times 2}(\mathbb{Q}).$

$5A, 5B, 5(A+B), 5(A-B)$ तथा $5A^t$ ज्ञात कीजिए।

क्या $5(A-B)=5A-5B$? क्या $(5A)^t = 5A^t$? अपने उत्तरों के लिए कारण दीजिए।

हल: $A^t = \begin{bmatrix} 2 & 7 & -0.5 \\ 1 & -1 & 0 \end{bmatrix}$.

$$5A = \begin{bmatrix} 5\times 2 & 5\times 1 \\ 5\times 7 & 5\times(-1) \\ 5\times(-0.5) & 5\times 0 \end{bmatrix} = \begin{bmatrix} 10 & 5 \\ 35 & -5 \\ -2.5 & 0 \end{bmatrix}.$$

इसी प्रकार, $5B = \begin{bmatrix} 1.5 & -5/3 \\ 5 & 25 \\ -25 & 40 \end{bmatrix}$.

साथ ही, $A+B = \begin{bmatrix} 2.3 & 2/3 \\ 8 & 4 \\ -5.5 & 8 \end{bmatrix}$, तथा $A-B = \begin{bmatrix} 1.7 & 4/3 \\ 6 & -6 \\ 4.5 & -8 \end{bmatrix}$.

अतः, $5(A+B) = \begin{bmatrix} 11.5 & 10/3 \\ 40 & 20 \\ -27.5 & 40 \end{bmatrix}$, $5(A-B) = \begin{bmatrix} 8.5 & 20/3 \\ 30 & -30 \\ 22.5 & -40 \end{bmatrix}$,

$$5A-5B = \begin{bmatrix} 8.5 & 20/3 \\ 30 & -30 \\ 22.5 & -40 \end{bmatrix}, (5A)^t = \begin{bmatrix} 10 & 35 & -2.5 \\ 5 & -5 & 0 \end{bmatrix},$$

$$5A^t = \begin{bmatrix} 5\times 2 & 5\times 7 & 5\times(-0.5) \\ 5\times 1 & 5\times(-1) & 5\times 0 \end{bmatrix} = \begin{bmatrix} 10 & 35 & -2.5 \\ 5 & -5 & 0 \end{bmatrix}.$$

आव्यूहों की संगत प्रविष्टियों को देखने पर, हम ज्ञात करते हैं कि

$5(A-B)=5A-5B$ और $(5A)^t = 5A^t$.

***

उपरोक्त उदाहरण में जो आपने देखा है, वह केवल इन A, B और $\alpha = 5$ के लिए ही सत्य नहीं है। यह सभी स्थितियों के लिए सत्य है, जो निम्नलिखित प्रमेय हमें बताता है।

प्रमेय 11: मान लीजिए कि $A, B \in \mathbb{M}_{m\times n}(\mathbb{C})$ तथा $\alpha, \beta \in \mathbb{C}$. तब,

i) $\alpha(A+B) = \alpha A + \alpha B$,

ii) $\alpha(A-B) = \alpha A - \alpha B$,

iii) $(\alpha A)^t = \alpha A^t$,

iv) $(\alpha\beta)A = \alpha(\beta A)$.

उपपत्ति: हम (i) को सिद्ध करेंगे, तथा आपको इस प्रमेय की उपपत्ति पूरी करने का अभ्यास दे रहे हैं (E29 देखिए)।

i) मान लीजिए कि $A = [a_{ij}]$ और $B = [b_{ij}]$. तब,

$$\alpha(A+B) = \alpha[a_{ij}+b_{ij}] = [\alpha(a_{ij}+b_{ij})] = [\alpha a_{ij} + \alpha b_{ij}]$$

$$= [\alpha a_{ij}] + [\alpha b_{ij}] = \alpha[a_{ij}] + \alpha[b_{ij}]$$

$$= \alpha A + \alpha B.$$

अतः, (i) सिद्ध हो गया। ■

अब निम्नलिखित प्रश्नों को हल कीजिए।

E29) प्रमेय 11(ii), (iii) और (iv) को सिद्ध कीजिए।

E30) यदि $(0.5)C = \sqrt{2}A - \sqrt{3}B$, जहाँ $A = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}$ तथा $B = \begin{bmatrix} \cos(\pi/3) & \sin(\pi/3) \\ -\sin(\pi/3) & \cos(\pi/3) \end{bmatrix}$, तो C ज्ञात कीजिए।

E31) मान लीजिए कि '$A \sim B$ iff $A - B = 5C$ किसी $C \in \mathbb{M}_{m\times n}(\mathbb{Z})$ के लिए' द्वारा $\mathbb{M}_{m\times n}(\mathbb{C})$ पर ~ परिभाषित है। जाँच कीजिए कि $\mathbb{M}_{m\times n}(\mathbb{C})$ पर ~ एक तुल्यता संबंध है या नहीं। यदि है, तो $[\mathbf{0}]$ ज्ञात कीजिए। अन्यथा, $\mathbb{M}_{m\times n}(\mathbb{R})$ पर एक तुल्यता संबंध परिभाषित कीजिए।

आइए अब देखें कि दो आव्यूहों को किस प्रकार गुणा किया जाता है।

आव्यूह गुणन

$\mathbb{M}_{2\times 3}(\mathbb{C})$ में $A = \begin{bmatrix} 2 & 5 & 7 \\ 3 & 5 & 2 \end{bmatrix}$ और $B = \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & -1 \end{bmatrix}$ पर विचार कीजिए। गुणा करने की एक स्वाभाविक विधि यह हो सकती है कि, योग की तरह, संगत अवयवों का गुणा कर लिया जाए। परंतु, आपको यह जान कर आश्चर्य होगा कि जिस विधि से आव्यूह गुणन को प्रायः परिभाषित किया जाता है, उसके अनुसार इन आव्यूहों का गुणा **नहीं किया जा सकता** है। आप ज़रूर सोच रहे होंगे कि ऐसा क्यों है।

जिस प्रकार से आव्यूह गुणन को परिभाषित किया जाता है वह इस तथ्य से जुड़ा है कि प्रत्येक आव्यूह एक फलन है, जैसे कि आप पाँचवें सेमेस्टर पाठ्यक्रम 'रैखिक बीजगणित' में अध्ययन करेंगे। ऐसा चलते, दो आव्यूहों का गुणा करना इन दोनों फलनों के संयोजन (composition) के संगत होता है। अतः, सामान्य आव्यूह गुणन को संगत अवयवों द्वारा परिभाषित नहीं किया जाता है, जैसा कि आप शीघ्र ही देखेंगे। ऐसा प्रतीत होता है कि आव्यूहों को गुणा करने की यह विधि फ़्रांसीसी गणितज्ञ जाक फ़िलीप मारी बीने (Jacques Philippe Marie Binet) (1786-1856) द्वारा 1812 में सूत्रित की गई थी।

अब आइए देखें कि दो आव्यूहों का गुणा किस प्रकार किया जाता है।

$A = [-1 \quad 3 \quad 5]$ और $B = \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix}$ पर विचार कीजिए।

तब, $AB = [-1 \quad 3 \quad 5]\begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix} = (-1)(0) + (3)(2) + (5)(1) = 11.$

अतः, हम इस विधि से एक पंक्ति सदिश को एक स्तंभ सदिश से गुणा तभी कर सकते हैं जबकि **इन दोनों में प्रविष्टियों की संख्या समान होती है।** हम इस गुणन का उपयोग दो ऐसे आव्यूहों का गुणनफल ज्ञात करने में करते हैं, जो एक प्रतिबंध को संतुष्ट करते हैं। इस प्रतिबंध को आप आगे देखेंगे।

$A = \begin{bmatrix} 2 & 5 & 7 \\ 3 & 5 & 2 \end{bmatrix}$ और $B = \begin{bmatrix} 1 & -\pi \\ 0 & i \\ 2 & 7 \end{bmatrix}$ पर विचार कीजिए। तो A एक $2 \times \mathbf{3}$ आव्यूह है तथा B एक $\mathbf{3} \times 2$ आव्यूह है। इनका आव्यूह गुणनफल AB एक 2×2 आव्यूह होगा। आइए देखें कि हम इसे किस प्रकार प्राप्त करते हैं।

AB का **(1, 1)वाँ** अवयव A की **प्रथम पंक्ति** और B के **प्रथम स्तंभ** का गुणनफल होता है; इसका **(1, 2)वाँ** अवयव A की **प्रथम पंक्ति** और B के **दूसरे स्तंभ** का गुणनफल होता है; इसका **(2, 1)वाँ** अवयव A की **दूसरी पंक्ति** और B के **प्रथम स्तंभ** का गुणनफल होता है; और इसका **(2, 2)वाँ** अवयव A की **दूसरी पंक्ति** और B के **दूसरे स्तंभ** का गुणनफल होता है। अतः,

$$A = \begin{bmatrix} [2 \quad 5 \quad 7]\begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} & [2 \quad 5 \quad 7]\begin{bmatrix} -\pi \\ i \\ 7 \end{bmatrix} \\ [3 \quad 5 \quad 2]\begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} & [3 \quad 5 \quad 2]\begin{bmatrix} -\pi \\ i \\ 7 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} 2(1)+5(0)+7(2) & 2(-\pi)+5(i)+7(7) \\ 3(1)+5(0)+2(2) & 3(-\pi)+5(i)+2(7) \end{bmatrix} = \begin{bmatrix} 16 & 49-2\pi+5i \\ 7 & 14-3\pi+5i \end{bmatrix}.$$

ध्यान दीजिए कि AB केवल तभी परिभाषित है, जब A की प्रत्येक पंक्ति में अवयवों की संख्या B के प्रत्येक स्तंभ में अवयवों की संख्या के बराबर हो। इसका अर्थ है कि **A के स्तंभों की संख्या B की पंक्तियों की संख्या के बराबर होनी चाहिए।**

तब, AB में पंक्तियों की संख्या = A में पंक्तियों की संख्या, तथा

AB में स्तंभों की संख्या = B में स्तंभों की संख्या।

व्यापक रूप में, निम्नलिखित परिभाषा पर विचार कीजिए।

परिभाषा: यदि $A=[a_{ij}]\in\mathbb{M}_{m\times n}(\mathbb{C})$ और $B=[b_{jk}]\in\mathbb{M}_{n\times s}(\mathbb{C})$, तो **आव्यूह गुणन** की संक्रिया को निम्न प्रकार से परिभाषित किया जाता है :

$\bullet:\mathbb{M}_{m\times n}(\mathbb{C})\times\mathbb{M}_{n\times s}(\mathbb{C})\to\mathbb{M}_{m\times s}(\mathbb{C}):\ \bullet(A,B)=AB=[c_{ik}]$, जहाँ

$$c_{ik}=[a_{i1}\ a_{i2}\ldots a_{in}]\cdot\begin{bmatrix}b_{1k}\\ b_{2k}\\ \vdots\\ b_{nk}\end{bmatrix}=\sum_{j=1}^{n}a_{ij}b_{jk}.$$

यहाँ कुछ महत्वपूर्ण प्रेक्षण हैं, जिनका आपको पुनः ध्यान रखना चाहिए।

टिप्पणी 10: i) दो आव्यूहों A और B का गुणा **तब तक नहीं किया जा सकता, जब तक** कि A के स्तंभों की संख्या B की पंक्तियों की संख्या के बराबर न हो।

ii) ध्यान दीजिए कि इस परिभाषा द्वारा दो $m\times n$ आव्यूहों $(m\neq n)$ का गुणा **नहीं किया जा सकता** है। अतः, $\mathbb{M}_{m\times n}(\mathbb{C})$ पर **आव्यूह गुणन एक द्वि-आधारी संक्रिया नहीं है**, **जब तक** $m=n$ न हो।

आइए कुछ उदाहरणों पर विस्तृत रूप से विचार करें।

उदाहरण 11: क्या $A=\begin{bmatrix}3 & 2\\ -1 & 1\\ -7/5 & 0\end{bmatrix}$ और $B=\begin{bmatrix}-1 & 3\\ 0 & 5\end{bmatrix}$ का गुणनफल परिभाषित है? यदि हाँ, तो ज्ञात कीजिए। साथ ही, BA ज्ञात कीजिए, यदि इसका अस्तित्व है तो।

हल: क्योंकि A एक 3×2 आव्यूह है तथा B एक 2×2 आव्यूह है, इसलिए AB परिभाषित है और यह एक 3×2 आव्यूह है। परंतु BA का अस्तित्व नहीं है, क्योंकि B में स्तंभों की संख्या $=2\neq 3$, जो A में पंक्तियों की संख्या है।

$$AB=\begin{bmatrix}[3\quad 2]\begin{bmatrix}-1\\ 0\end{bmatrix} & [3\quad 2]\begin{bmatrix}3\\ 5\end{bmatrix}\\ [-1\quad 1]\begin{bmatrix}-1\\ 0\end{bmatrix} & [-1\quad 1]\begin{bmatrix}3\\ 5\end{bmatrix}\\ [-7/5\quad 0]\begin{bmatrix}-1\\ 0\end{bmatrix} & [-7/5\quad 0]\begin{bmatrix}3\\ 5\end{bmatrix}\end{bmatrix}$$

$$=\begin{bmatrix}3(-1)+2(0) & 3(3)+2(5)\\ (-1)(-1)+1(0) & (-1)(3)+1(5)\\ \left(-\frac{7}{5}\right)(-1)+0(0) & \left(-\frac{7}{5}\right)(3)+0(5)\end{bmatrix}$$

$$= \begin{bmatrix} -3 & 19 \\ 1 & 2 \\ \frac{7}{5} & -\frac{21}{5} \end{bmatrix}.$$

***

उदाहरण 12: यदि $\mathbb{C}$ पर A और B क्रमशः $m \times n$ आव्यूह और $n \times s$ आव्यूह हैं, तो m, n और s पर कौनसे प्रतिबंधों के अधीन AB और BA दोनों परिभाषित होंगे? तथा तब, क्या $AB = BA$? क्यों, या क्यों नहीं?

हल: AB सदैव ही परिभाषित होगा, क्योंकि A के स्तंभों की संख्या B की पंक्तियों की संख्या के बराबर है। साथ ही, AB एक $m \times s$ आव्यूह होगा।

BA तभी परिभाषित होगा, जब $s = m$ हो। तथा तब AB और BA क्रमशः $m \times m$ और $n \times n$ आव्यूह होंगे।

अतः, $AB = BA$ के लिए सर्वप्रथम दोनों आव्यूहों को समान कोटियों का होना होगा, अर्थात् $m = n$ ज़रूरी है।

परंतु, $m = n$ होने पर भी हो सकता है कि ये दोनों बराबर न हों।

उदाहरणार्थ, यदि $A = \begin{bmatrix} 1 & -1 \\ 2 & 0 \end{bmatrix}$ और $B = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$, तो

$$AB = \begin{bmatrix} 1(1)+(-1)(1) & 1(0)+(-1)(0) \\ 2(1)+0(1) & 2(0)+0(0) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix} \text{ तथा}$$

$$BA = \begin{bmatrix} 1(1)+0(2) & 1(-1)+0(0) \\ 1(1)+0(2) & 1(-1)+0(0) \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}.$$

अतः, $AB \neq BA$.

इस प्रकार, व्यापक रूप से, $A, B \in \mathbb{M}_n(\mathbb{C})$ के लिए, $AB \neq BA$.

***

अब आइए उदाहरणों के माध्यम से आव्यूह गुणन के कुछ गुणों पर विचार करें।

उदाहरण 13: मान लीजिए कि $A = \begin{bmatrix} 2 & -1 & 0 \\ 3 & 1 & -2 \end{bmatrix}$ तथा $B = \begin{bmatrix} 1 & -4 & 0 \\ 0 & 2 & 0 \\ 0 & 4 & 1 \end{bmatrix}$. क्या AB और B^tA^t परिभाषित हैं? यदि ऐसा है, तो $(AB)^t$ और B^tA^t में एक संबंध ज्ञात कीजिए। अन्यथा, जाँच कीजिए कि क्या $AB = BA^t$ है या नहीं।

हल: आपको इसका सत्यापन करना चाहिए कि AB और B^tA^t दोनों परिभाषित हैं। साथ ही,

$$AB = \begin{bmatrix} 2(1)+(-1)(0)+0(0) & 2(-4)+(-1)(2)+0(4) & 2(0)+(-1)(0)+0(1) \\ 3(1)+1(0)+(-2)(0) & 3(-4)+1(2)+(-2)(4) & 3(0)+1(0)+(-2)(1) \end{bmatrix}$$

$$= \begin{bmatrix} 2 & -10 & 0 \\ 3 & -18 & -2 \end{bmatrix}.$$

अतः, $(AB)^t = \begin{bmatrix} 2 & 3 \\ -10 & -18 \\ 0 & -2 \end{bmatrix}.$

आगे, $B^t = \begin{bmatrix} 1 & 0 & 0 \\ -4 & 2 & 4 \\ 0 & 0 & 1 \end{bmatrix}$ और $A^t = \begin{bmatrix} 2 & 3 \\ -1 & 1 \\ 0 & -2 \end{bmatrix}.$

जाँच कीजिए कि $B^tA^t = \begin{bmatrix} 2 & 3 \\ -10 & -18 \\ 0 & -2 \end{bmatrix}.$

इस प्रकार, $(AB)^t = B^tA^t$.

***

उदाहरण 14: मान लीजिए कि $A = \begin{bmatrix} 4 \\ 2 \\ -2 \end{bmatrix}, B = \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix}$ और $C = \begin{bmatrix} -1 & 2 \end{bmatrix}$. क्या $AC + BC$ और $(A+B)C$ परिभाषित हैं? यदि हाँ, तो इन्हें ज्ञात कीजिए तथा इनमें संबंध भी ज्ञात कीजिए। यदि इनमें से कोई परिभाषित नहीं है, तो स्पष्ट कीजिए कि क्यों।

हल: यहाँ A, B और $A+B$, 3×1 आव्यूह हैं तथा C एक 1×2 आव्यूह है। इसलिए, AC, BC और $(A+B)C$ परिभाषित हैं, तथा ये सभी 3×2 आव्यूह हैं।

अब, $AC = \begin{bmatrix} 4(-1) & 4(2) \\ 2(-1) & 2(2) \\ (-2)(-1) & (-2)(2) \end{bmatrix} = \begin{bmatrix} -4 & 8 \\ -2 & 4 \\ 2 & -4 \end{bmatrix}, BC = \begin{bmatrix} -2 & 4 \\ -3 & 6 \\ -1 & 2 \end{bmatrix}.$

$A + B = \begin{bmatrix} 4+2 \\ 2+3 \\ (-2)+1 \end{bmatrix} = \begin{bmatrix} 6 \\ 5 \\ -1 \end{bmatrix}$, जिससे $(A+B)C = \begin{bmatrix} -6 & 12 \\ -5 & 10 \\ 1 & -2 \end{bmatrix}.$

साथ ही, $AC + BC = \begin{bmatrix} -4 & 8 \\ -2 & 4 \\ 2 & -4 \end{bmatrix} + \begin{bmatrix} -2 & 4 \\ -3 & 6 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} -6 & 12 \\ -5 & 10 \\ 1 & -2 \end{bmatrix}.$

इस प्रकार, $AC + BC = (A+B)C$.

***

उदाहरण 15: मान लीजिए कि $A = \begin{bmatrix} i & 7 & -1 \\ 0.25 & \pi & 0 \end{bmatrix}$, $B = \begin{bmatrix} -2 \\ i \\ 1+3i \end{bmatrix}$ और

$C = [-1 \quad 0 \quad 0 \quad 1]$. दर्शाइए कि (AB)C और A(BC) परिभाषित हैं, और बराबर हैं।

हल: यहाँ ध्यान दीजिए कि AB एक 2×1 आव्यूह है, $BC \in \mathbb{M}_{3\times4}(\mathbb{C})$, तथा इसी लिए $(AB)C \in \mathbb{M}_{2\times4}(\mathbb{C})$ और $A(BC) \in \mathbb{M}_{2\times4}(\mathbb{C})$. इस प्रकार, (AB)C और A(BC) दोनों परिभाषित हैं तथा समान कोटियों के हैं। अब,

$$AB = \begin{bmatrix} -2i+7i-(1+3i) \\ -0.5+\pi i \end{bmatrix} = \begin{bmatrix} -1+2i \\ -0.5+\pi i \end{bmatrix} \text{ तथा } BC = \begin{bmatrix} 2 & 0 & 0 & -2 \\ -i & 0 & 0 & i \\ -(1+3i) & 0 & 0 & 1+3i \end{bmatrix}.$$

अतः, $(AB)C = \begin{bmatrix} 1-2i & 0 & 0 & -1+2i \\ 0.5-\pi i & 0 & 0 & -0.5+\pi i \end{bmatrix}$ और

$$A(BC) = \begin{bmatrix} 1-2i & 0 & 0 & -1+2i \\ 0.5-\pi i & 0 & 0 & -0.5+\pi i \end{bmatrix}.$$

इस प्रकार, $(AB)C = A(BC)$.

***

उदाहरण 16: उदाहरण 13 के A और B के लिए, दर्शाइए कि $(\alpha A)B = \alpha(AB) = A(\alpha B) \ \forall \ \alpha \in \mathbb{C}$.

हल: यहाँ, $\alpha A = \begin{bmatrix} 2\alpha & -\alpha & 0 \\ 3\alpha & \alpha & -2\alpha \end{bmatrix}$, $\alpha B = \begin{bmatrix} \alpha & -4\alpha & 0 \\ 0 & 2\alpha & 0 \\ 0 & 4\alpha & \alpha \end{bmatrix}$ तथा

$$\alpha(AB) = \begin{bmatrix} 2\alpha & -10\alpha & 0 \\ 3\alpha & -18\alpha & -2\alpha \end{bmatrix}.$$

साथ ही, $(\alpha A)B = \begin{bmatrix} 2\alpha & -\alpha & 0 \\ 3\alpha & \alpha & -2\alpha \end{bmatrix} \begin{bmatrix} 1 & -4 & 0 \\ 0 & 2 & 0 \\ 0 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 2\alpha & -10\alpha & 0 \\ 3\alpha & -18\alpha & -2\alpha \end{bmatrix}$.

इसी प्रकार, $A(\alpha B) = \begin{bmatrix} 2 & -1 & 0 \\ 3 & 1 & -2 \end{bmatrix} \begin{bmatrix} \alpha & -4\alpha & 0 \\ 0 & 2\alpha & 0 \\ 0 & 4\alpha & \alpha \end{bmatrix} = \begin{bmatrix} 2\alpha & -10\alpha & 0 \\ 3\alpha & -18\alpha & -2\alpha \end{bmatrix}$.

इस तरह, $(\alpha A)B = \alpha(AB) = A(\alpha B)$.

***

उदाहरण 17: दर्शाइए कि यदि $A = \begin{bmatrix} 3 & i \\ 1+\sqrt{2} & 0 \end{bmatrix}$ है तथा $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, तो $AI = IA = A$.

हल: आप इसकी जाँच कर सकते हैं कि $AI = A$ और $IA = A$.

***

उदाहरण 13-17 वास्तव में उन गुणों की विशिष्ट स्थितियाँ हैं जो अधिक व्यापक रूप में सत्य हैं और जिनके अब हम कथन देने जा रहे हैं। परंतु हम इन्हें सिद्ध नहीं करेंगे, क्योंकि इनकी उपपत्तियाँ बहुत अव्यवस्थित हो सकती हैं। आप इन गुणों का उपयोग इस पाठ्यक्रम की अन्य इकाइयों में बारंबार करेंगे।

P1 **(साहचर्य नियम):** यदि $\mathbb{C}$ पर A, B और C क्रमशः $m \times n$, $n \times p$ और $p \times q$ आव्यूह हैं, तो $(AB)C = A(BC)$.

P2 **(बंटन नियम):** यदि $\mathbb{C}$ पर A एक $m \times n$ आव्यूह है तथा B और C दो $n \times p$ आव्यूह हैं, तो $A(B+C) = AB + AC$.

P3 **(गुणनात्मक तत्समक):** मान लीजिए कि I_n, $n \times n$ आव्यूह

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{bmatrix}$$ है, अर्थात् $I_n = [a_{ij}]$, जहाँ $a_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$.

तब, $AI_n = A$ और $I_m A = A$ होता है, $\mathbb{C}$ पर प्रत्येक $m \times n$ आव्यूह A के लिए।

P4 यदि $\alpha \in \mathbb{C}$ तथा $\mathbb{C}$ पर A और B क्रमशः $m \times n$ और $n \times p$ आव्यूह हैं, तो $\alpha(AB) = (\alpha A)B = A(\alpha B)$.

हालांकि गुण $P1 - P5$ $\mathbb{C}$ पर आव्यूहों के बारे में हैं। लेकिन ये गुण $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ या $\mathbb{Z}_n (n \in \mathbb{N})$ पर आव्यूहों पर भी लागू हैं।

P5 यदि $\mathbb{C}$ पर A और B क्रमशः $m \times n$ और $n \times p$ आव्यूह हैं, तो $(AB)^t = B^t A^t$.

अब निम्नलिखित प्रश्नों को हल करने के लिए, आप उपरोक्त गुणों का उपयोग क्यों

नहीं करते?

E32) यदि AB, AC और BC परिभाषित हैं तो इन्हें ज्ञात कीजिए, जहाँ

$$A = \begin{bmatrix} 9 & 5 & -4 \\ -3 & 0 & 2 \end{bmatrix}, B = A^t \text{ और } C = \begin{bmatrix} 3 & \sqrt{3} \\ 1 & i \\ i & 1 \end{bmatrix}.$$

E33) दर्शाइए कि किन्हीं दो $n \times n$ आव्यूहों A और B के लिए, $(A+B)^2 = A^2 + AB + BA + B^2$.

E34) किसी शहर में तीन पुस्तकों की दुकानों में से प्रत्येक पर दो पाठ्यपुस्तकों की माल-सूची (inventory) $A = \begin{bmatrix} 9 & 12 \\ 15 & 4 \\ 7 & 0 \end{bmatrix}$ द्वारा दी जाती है। यहाँ A की पंक्तियाँ विभिन्न दुकानों से संबद्ध हैं तथा A के स्तंभ उस दुकान में उपलब्ध प्रत्येक पाठ्यपुस्तक की संख्या को व्यक्त करते हैं। पुस्तकों की थोक लागत (₹ में) $C = [700 \quad 1200]^t$ द्वारा दी जाती है। AC ज्ञात कीजिए, तथा दिए हुए संदर्भ में बताइए यह क्या दर्शाता है।

E35) निम्नलिखित रैखिक समीकरण-निकाय पर विचार कीजिए।

$$7x + 3y + 4z - 5 = 0$$

$$2x + 3y = 6$$

$$z - 4y = 19$$

इसे $AX = B$ रूप में लिखिए, जहाँ A एक 3×3 आव्यूह है तथा X और B दो 3×1 आव्यूह हैं।

(**संकेत:** $X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ लीजिए।)

जैसा कि आपने $\mathbb{C}$ पर आव्यूहों को परिभाषित किया है, हम इन्हें किसी भी समुच्चय पर परिभाषित कर सकते हैं। उदाहरणार्थ, $\begin{bmatrix} \overline{2} & \overline{3} & \overline{0} \\ \overline{1} & \overline{0} & \overline{4} \end{bmatrix} \in \mathbb{M}_{2\times3}(\mathbb{Z}_6)$ है, जहाँ सभी प्रविष्टियाँ $\mathbb{Z}_6$ से हैं। इसी प्रकार, $\begin{bmatrix} -3 & 7 & 5 \\ 2 & 1 & -6 \end{bmatrix} \in \mathbb{M}_{2\times3}(\mathbb{Z})$. परंतु यदि हम $\mathbb{M}_{m\times n}(S)$ में आव्यूहों को जोड़ना चाहते हैं, जहाँ S एक समुच्चय है, तो परिभाषा के अनुसार, हम ऐसा केवल तभी कर सकते हैं, जब S पर '$+$' एक द्वि-आधारी संक्रिया हो। इसी प्रकार, यदि हम $\mathbb{M}_m(S)$ में आव्यूहों का गुणा करना चाहते हैं, तो '$+$' और '$\cdot$' को S पर द्वि-आधारी संक्रियाएँ होनी चाहिएं।

अतः, उदाहरणार्थ, यदि $A, B \in \mathbb{M}_2(\mathbb{Z}_n)$, तब $A+B$ तथा $A \cdot B$ परिभाषित हैं, जहाँ $\mathbb{Z}_n$ में अवयवों को जोड़ा तथा उनका गुणा किया जाता है।

इस प्रकार, **इस भाग में सभी परिभाषाएँ एक अरिक्त समुच्चय S पर आव्यूहों के लिए सत्य हैं, जहाँ S पर '$+$' और '$\cdot$' द्वि-आधारी संक्रियाएँ** हैं। सभी प्रमेय भी S पर आव्यूहों के लिए सत्य होंगे, अगर S कुछ ऐसे प्रतिबंधों को संतुष्ट करे, जिनका अध्ययन आप इकाई 2 में करेंगे।

आव्यूहों की इस परिचात्मक चर्चा को हम यहाँ समाप्त करेंगे। आइए अब एक अन्य प्रकार की बीजीय वस्तु पर विचार करें, जो समूहों के अध्ययन के लिए मौलिक है।

1.5 क्रमचयों से परिचय

आइए इस चर्चा को शब्द 'सममिति' पर दृष्टि डालते हुए प्रारंभ करें। आपने इस शब्द को प्रकृति या डिज़ाइन, की सुंदरता के संदर्भ में अनेक बार सुना होगा। यहाँ हम एक समतल में कुछ द्विविमीय (two-dimensional) वस्तुओं की सममितियों पर चर्चा करेंगे।

किसी त्रिभुज का केन्द्रक उसकी तीनों माध्यिकाओं (medians) का प्रतिच्छेद बिंदु होता है।

एक मेज़ पर रखे हुए किसी सपाट वस्तु, मान लीजिए कि प्लास्टिक के बने एक समबाहु त्रिभुज, पर विचार कीजिए, यदि आप इसे इसके केन्द्रक (centroid) के परित घुमाएँ, या इसे पलट दें, या इसे मेज़ पर धक्के से आगे कर दें, तो क्या इसके आकार या आमाप में कोई परिवर्तन होता है? नहीं, इन पर कोई प्रभाव नहीं पड़ता है। इसी कारण त्रिभुज पर ये क्रियाएँ दृढ़ पिंड गतियों के उदाहरण हैं, जिस पद को हम अब परिभाषित कर रहे हैं।

परिभाषा: किसी वस्तु X की एक **दृढ़ पिंड गति** (rigid body motion) X पर एक ऐसी क्रिया (action) है जो उसके आकार या आमाप में कोई परिवर्तन नहीं करती है।

इस प्रकार, किसी समतल में एक वस्तु की एक दृढ़ पिंड गति एक ऐसा एकैकी आच्छादक फलन $f:\mathbb{R}^2 \to \mathbb{R}^2$ है जिससे कि सभी $x, y \in \mathbb{R}^2$ के लिए, $f(x)$ और $f(y)$ के बीच दूरी वही है जो x और y के बीच की दूरी है।

आइए, अब मेज़ पर रखे समबाहु त्रिभुज पर वापस आ जाएँ। मेज़ पर इसकी बाहरी रेखा खींचिए। यदि आप इस त्रिभुज को मेज़ पर धक्का देकर 5cm सरकाएँ, तो इसकी स्थिति अपनी प्रारंभिक स्थिति से स्पष्ट रूप से बदल जाएगी। इसी प्रकार, इस त्रिभुज को मेज़ पर इसके केन्द्रक के प्रति 90° से घुमाने का प्रयास कीजिए। पुनः, आप देखेंगे कि इसकी स्थिति मेज़ पर खींची गई बाहरी रेखा को पूरा पूरा नहीं ढकेगी। यह बदल जाएगी। परंतु इसे अब 120° से इसके केंद्रक के प्रति घुमाने का प्रयास कीजिए। आप क्या देखते हैं? क्या इसकी स्थिति बदल गई है? नहीं, ऐसा नहीं हुआ है। तो यह क्रिया एक उदाहरण है उसका जिसे हम अब परिभाषित करने जा रहे हैं।

परिभाषा : समतल में किसी वस्तु की एक **सममिति (symmentry)** एक ऐसी दृढ़ पिंड गति है, जिससे उस समतल में उस वस्तु की स्थिति में कोई परिवर्तन नहीं होता है।

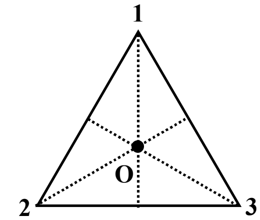
इस प्रकार, समतल में एक वस्तु X की एक सममिति $\mathbb{R}^2$ से $\mathbb{R}^2$ तक एक ऐसा एकैकी आच्छादक f है जिससे कि $f(X) = X$. अतः, सममिति कोइ ऐसी दृढ़ पिंड गति नहीं हो सकती है जो उस वस्तु की स्थिति को बदल दे, अर्थात्, उसे विस्थापित कर दे। उदाहरणार्थ, एक स्थानांतरण (translation) एक सममिति नहीं होगी।

समतलीय वस्तु की सममिति केवल निम्नलिखित में से एक हो सकती है :

i) **परावर्तन (Reflection):** एक सममिति-रेखा (line of symmetry) सापेक्ष (उदाहरणार्थ, समबाहु त्रिभुज का कोई भी कोण समद्विभाजक) वस्तु X के सभी बिंदुओं के दर्पण प्रतिबिंबों को लेना।

ii) **घूर्णन (Rotation):** किसी समतल में वस्तु X को उस समतल के किसी केन्द्र बिंदु के प्रति वामावर्त (anti-clockwise) दिशा में किसी कोण से ऐसे घुमाना कि

घूर्णन के बाद X की स्थिति में कोई बदलाव न हो (उदाहरणार्थ, समबाहु त्रिभुज को उसके केन्द्रक के प्रति 120° के कोण से घुमाना)।

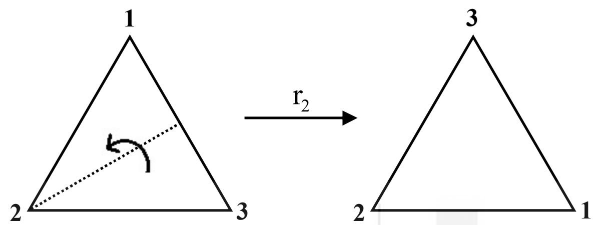


आकृति 4: एक समबाहु त्रिभुज।

आइए विस्तृत रूप से कुछ उदाहरणों पर दृष्टि डालें।

उदाहरण 18: एक समबाहु त्रिभुज की सममितियों के समुच्चय, D_6 को प्राप्त कीजिए।

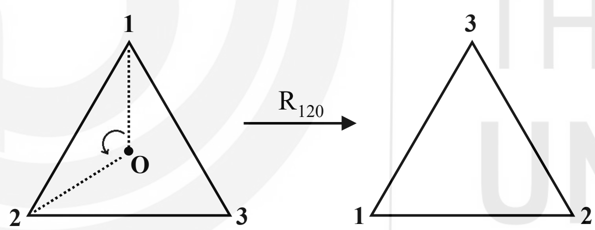
हल: शीर्षों 1, 2, 3 वाले समबाहु त्रिभुज पर विचार कीजिए (जैसा आकृति 4 में है)। मान लीजिए कि r_i शीर्ष i पर कोण के समद्विभाजक के प्रति परावर्तन को व्यक्त करता है। उदाहरण के तौर पर, आकृति 5 को देखिए।



आकृति 5: शीर्ष 2 के कोण समद्विभाजक में परावर्तन

इसलिए, हम कह सकते हैं कि r_2, {1, 2, 3} से {1, 2, 3} तक एक फलन है, जो 1 को 3 तक, 2 को 2 तक तथा 3 को 1 तक ले जाता है।

मान लीजिए कि R_{120} त्रिभुज का उसके केन्द्रक के प्रति वामावर्त दिशा में 120° का घूर्णन व्यक्त करता है (आकृति 6 देखिए)।



आकृति 6: त्रिभुज का, इसके केन्द्रक O के प्रति, वामावर्त दिशा में 120° से घूर्णन

इसलिए, {1, 2, 3} से {1, 2 3} तक R_{120} एक फलन है, जो 1 को 2 तक, 2 को 3 तक तथा 3 को 1 तक ले जाता है।

आइए {1, 2, 3} से {1, 2, 3} तक के इन एकैकी आच्छादक फलनों को निम्नलिखित दो-पंक्ति रूप में निरूपित करें :

इकाई 2 में, आप देखेंगे कि D_6 कोटि 6 वाला **द्वितल समूह** है।

$$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ r_2(1) & r_2(2) & r_2(3) \end{pmatrix}, \text{ अर्थात् } r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \text{ और } R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

तत्समक फलन (identity function) भी एक सममिति है, जो त्रिभुज को 'हिलाए बिना' छोड़ देती है। इसे $I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ द्वारा प्रदर्शित किया जाता है।

फिर आप इसका सत्यापन कीजिए कि समबाहु त्रिभुज की सभी संभव सममितियाँ

$I, r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \; r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$

$R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ और $R_{240} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ हैं।

इस प्रकार, $D_6 = \{I, r_1, r_2, r_3, R_{120}, R_{240}\}$.

अब, अगर हम त्रिभुज पर r_1 का दो बार प्रयोग करते हैं तो क्या होता है?

तब, $r_1^2(1) = r_1 \circ r_1(1) = r_1(1) = 1, r_1^2(2) = r_1(3) = 2$ तथा $r_1^2(3) = r_1(2) = 3.$

इस प्रकार, $r_1^2 = I.$

इसी प्रकार, आप इसकी जाँच कीजिए कि $r_2^2 = I, r_3^2 = I, R_{120}^2 = R_{240}, R_{120}^3 = I,$

$r_1 \circ R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = r_2,$ इत्यादि।

***

उदाहरण 19: एक ऐसी वस्तु का उदाहरण दीजिए, जिसमें निम्नलिखित हो :

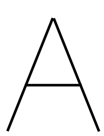
(i) कोई अतुच्छ घूर्णन सममिति नहीं,

(ii) ठीक दो परावर्तन सममितियाँ।

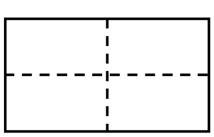
हल: i) अक्षर A पर विचार कीजिए (आकृति 7(i) देखिए)। यहाँ कोई ऐसा बिंदु नहीं है जिसके प्रति 0° और 360° के बीच के कोण से घूर्णन करने पर इस अक्षर की वही स्थिति प्राप्त हो जाए।

ii) असमान भुजाओं वाले एक आयत पर विचार कीजिए (जैसा आकृति 7(ii) में है)। आपको इसका सत्यापन करना चाहिए कि इसकी केवल दो परावर्तन सममितियाँ हैं, और ये इसकी सम्मुख भुजाओं के मध्य-बिंदुओं को मिलाने वाली रेखाओं के प्रति हैं।

***



(i)



(ii)

आकृति 7

अब, कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E36) दो-पंक्ति रूप में निम्नलिखित की सभी सममितियाँ लिखिए :

i) एक वर्ग, ii) एक समद्विबाहु त्रिभुज।

E37) अक्षरों N और B की सभी सममितियाँ ज्ञात कीजिए।

अभी-अभी आपने जो अध्ययन किया है, उसको व्यापकीकृत करने पर, हम कह सकते हैं कि n शीर्षों वाले **किसी भी सम बहुभुज की सममिति** $\{1, 2, \ldots, n\}$ से $\{1, 2, \ldots, n\}$

तक एक एकैकी आच्छादक फलन है। इन सभी सममितियों के समुच्चय को $\mathbf{D_{2n}}$ से व्यक्त किया जाता है। इनके बारे में आप और अधिक आने वाली इकाइयों में अध्ययन करेंगे।

अभी तक आपने एक विशेष प्रकार के एकैकी आच्छादक फलन का अध्ययन किया है। आइए एक व्यापकीकरण की ओर बढ़ें।

परिभाषाएँ: मान लीजिए कि X एक अरिक्त समुच्चय है।

i) X से X तक का एक एकैकी आच्छादक फलन $\mathbf{X}$ का एक **क्रमचय** (**permutation**) कहलाता है। हम X के सभी क्रमचयों के समुच्चय को $\mathbf{S(X)}$ द्वारा व्यक्त करते हैं।

ii) यदि $X = \{1, 2, \ldots, n\}$, तो $S(X)$ को $\mathbf{S_n}$ द्वारा व्यक्त किया जाता है, तथा S_n का प्रत्येक अवयव **n प्रतीकों पर एक क्रमचय** कहलाता है।

इस प्रकार, किसी वस्तु की सममिति एक क्रमचय होती है। परंतु कई और तरह के भी क्रमचय हैं। उदाहरणार्थ, S_4 में $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ है। अर्थात्, यह फलन $f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\} : f(1) = 2, f(2) = 4, f(3) = 3, f(4) = 1$ है। परंतु यह उस समुच्चय का अवयव नहीं है जिसे आपने E36(i) में ज्ञात किया था।

मान लीजिए कि हमें S_n में अवयव f बनाना है। हम आगे कैसे बढ़ें? हम $f(1)$ को चुनते हुए शुरू कर सकते हैं। अब, n प्रतीकों $1, 2, \ldots, n$ में से कोई भी एक $f(1)$ हो सकता है। $f(1)$ को चुनने के बाद, हम समुच्चय $\{1, 2, \ldots, n\} \setminus \{f(1)\}$ में से $f(2)$ को चुन सकते हैं, क्योंकि f एकैकी है। इस प्रकार, $f(2)$ को $(n-1)$ विधियों से चुना जा सकता है। आगमन के तरीक़े से, $f(i)$ को चुनने के बाद, हम $f(i+1)$ को $(n-i)$ विधियों से चुन सकते हैं। इस प्रकार, f को $(1 \times 2 \times \ldots \times n) = n!$ विधियों से चुना जा सकता है। अर्थात्, **$\mathbf{S_n}$ में n! अवयव होते हैं।**

जैसा कि हमने सममितियों के लिए किया था, हम $f \in S_n$ को दो-पंक्ति रूप में

$\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$ द्वारा निरूपित कर सकते हैं।

उदाहरणार्थ, S_4 में $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ को लीजिए। ऊपर की पंक्ति के अवयवों को किसी भी क्रम में रख सकते हैं, लेकिन ज़रूरी है कि नीचे वाली पंक्ति में संगत अवयवों को उसी क्रम में बदल दिया जाए।

इस प्रकार, $\begin{pmatrix} 2 & 1 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$ भी उपरोक्त फलन f को निरूपित करता है। परंतु फलन $\begin{pmatrix} 3 & 1 & 2 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ और f अलग हैं, क्योंकि, उदाहरणार्थ, यह फलन 3 को 2 तक ले जाता है, जबकि $f(3) = 3$.

अब, आइए उदाहरण 18 की सममिति r_3 पर दृष्टि डालें। आपने देखा था कि $r_3(3) = 3.$ अर्थात्, निम्नलिखित परिभाषा के अनुसार 3 को r_3 नियत करता है।

परिभाषा: किसी समुच्चय X का एक क्रमचय f, $x \in X$ को **नियत (fix) करता** है यदि $f(x) = x$, तथा f, x को **गतिमान** करता है यदि $f(x) \neq x.$

इस प्रकार, उदाहरण 18 में $r_1, 1$ को नियत करता है, $r_2, 2$ को नियत करता है तथा $r_3, 3$ को नियत करता है। ध्यान दीजिए कि R_{120} किसी भी अवयव को नियत नहीं करता है, तथा I प्रत्येक अवयव को नियत करता है।

अब, उदाहरण 18 में आपने देखा था कि $R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ सममितियों में से एक थी। अर्थात्, R_{120} अवयव 1 को 2 तक, 2 को 3 तक, 3 को 1 तक ले जाता है। इस प्रकार, R_{120} एक ऐसे क्रमचय का उदाहरण है, जिसे अब हम परिभाषित करेंगे।

परिभाषा: कोई क्रमचय $f \in S_n$ **लंबाई r वाला चक्र (cycle)** (या **r-चक्र**), जहाँ $r \in \mathbb{N}$ कहलाता है यदि $X = \{1, 2, \ldots, n\}$ में ऐसे $x_1, x_2, \ldots, x_r$ हैं कि $1 \leq i \leq r-1$ के लिए $f(x_i) = x_{i+1}$ तथा $f(x_r) = x_1$, और $t \neq x_1, x_2, \ldots, x_r$ के लिए t को f नियत करता है। इस f को $\mathbf{(x_1\ x_2 \ldots x_r)}$ से दर्शाते हैं।

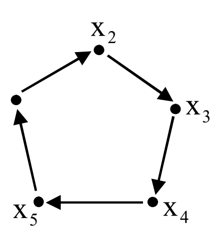
उदाहरणार्थ, $f = (2\ 4\ 5\ 10) \in S_{10}$ से हमारा तात्पर्य है कि $\{1, 2, \ldots, 10\}$ का f एक ऐसा क्रमचय है कि $f(2) = 4, f(4) = 5, f(5) = 10, f(10) = 2$ तथा $j \in \{1, 2, \ldots, 10\} \setminus \{2, 4, 5, 10\}$ के लिए $f(j) = j.$

इस प्रकार, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 3 & 5 & 10 & 6 & 7 & 8 & 9 & 2 \end{pmatrix}$ लंबाई 4 वाला एक चक्र है।

दो-पंक्ति रूप की तुलना में f को निरूपित करने के लिए $(2\ \ 4\ \ 5\ \ 10)$ एक अधिक सुंदर और संक्षिप्त विधि है कि नहीं?

एक अन्य उदाहरण के रूप में, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$ पर विचार कीजिए। यह S_5 में लंबाई 5 वाला चक्र $(1\ 2\ 5\ 3\ 4)$ है।

ध्यान दीजिए कि एक चक्र के संकेतन में, हम उन अवयवों को नहीं लिखते हैं जो क्रमचय द्वारा नियत हैं।



आकृति 8: चक्र $(x_1\ x_2 \ldots x_5)$ का एक चित्रीय निरूपण।

अब, लंबाई 1 वाला चक्र क्या है? $(2) \in S_7$ पर विचार कीजिए।

यह 2 को 2 तक ले जाता है, तथा 1, 3, 4, 5, 6 और 7 को नियत करता है। अतः, (2) द्वारा $\{1, 2, \ldots, 7\}$ के सभी प्रतीक नियत हैं। इस प्रकार, $(2) = I.$ इसी प्रकार, कोई भी 1-चक्र तत्समक फलन होता है।

इस संदर्भ में, निम्नलिखित प्रेक्षण पर विचार कीजिए।

टिप्पणी 11: एक चक्र को यह नाम इसलिए दिया गया है कि इसके अधीन प्रत्येक अवयव अगले अवयव को गतिमान होता है, तथा अंतिम अवयव चक्र के पहले अवयव

को गतिमान होता है। इसके एक चित्रीय निरूपण के लिए आकृति 8 को देखिए।

अब, कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E38) उदाहरण 18 की कौन-सी सममितियाँ चक्र हैं? क्या $D_6 = S_3$? अपने उत्तरों के लिए कारण दीजिए।

E39) S_7 में एक 3-चक्र, तथा उसका दो-पंक्ति निरूपण, दीजिए।

अब 'कलन' याद कीजिए कि हम दो क्रमचयों का संयोजन, अर्थात्, दो एकैकी आच्छादक फलनों का संयोजन किस प्रकार परिकलित करते हैं। S_5 में निम्नलिखित उदाहरण पर विचार कीजिए :

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

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

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

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (2\ 4), \text{ क्योंकि यहाँ } 1, 3 \text{ और } 5 \text{ को नियत किया गया है।}$$

अतः, $\alpha \circ \beta$ लंबाई 2 वाला चक्र है।

इस संदर्भ में, निम्नलिखित टिप्पणी पर विचार कीजिए।

टिप्पणी 12: ध्यान दीजिए कि यदि α और β, X के एकैकी आच्छादन हैं, तो $\alpha \circ \beta$ भी X का एक एकैकी आच्छादन होता है, जैसा कि आप 'कलन' से जानते हैं।

अब यह प्रश्न को हल कीजिए।

E40) S_4 में $\alpha = (1\ 3\ 2)$ और $\beta = (2\ 4\ 1)$ को दो-पंक्ति रूप में लिखिए। इसकी जाँच भी कीजिए कि क्या $\alpha \circ \beta$ एक चक्र है या नहीं। आगे, $\alpha^2 = \alpha \circ \alpha$ एक चक्र है? क्या β^2 एक चक्र है? क्या $\alpha \circ \beta = \beta \circ \alpha$? अपने उत्तरों के लिए कारण दीजिए।

इसके साथ, हम क्रमचयों के इस परिचय की समाप्ति करते हैं। आप इन फलनों का अध्ययन इकाई 2 में भी करेंगे, तथा विस्तृत रूप में इकाई 9 में भी करेंगे।

आइए अब देखें कि इस इकाई में हमने क्या चर्चा की है।

1.6 सारांश

इस इकाई में, आपने निम्नलिखित संकल्पनाओं और प्रक्रियाओं का अध्ययन किया है।

1. $a \in \mathbb{Z}, b \in \mathbb{Z}^*$ के लिए, $b \mid a$ iff $\exists\, c \in \mathbb{Z}$ s.t. $a = bc$.

2. i) **विभाजन कलन विधि (या ऐल्गोरिद्म)**: मान लीजिए कि $a, b \in \mathbb{Z}$ जहाँ $b > 0$. तब, ऐसे अद्वितीय पूर्णांकों q और r का अस्तित्व है जिनसे कि $a = qb + r$, जहाँ $0 \le r < b$.

   ii) इस कलन विधि की उपपत्ति और उसके अनुप्रयोग।

3. i) किन्हीं दो अवयवों $a, b \in \mathbb{Z}^*$ का g.c.d $(a, b) = ma + nb$, किन्हीं $m, n \in \mathbb{Z}$ के लिए। (वस्तुतः, $(a, 0)$, को $a \neq 0$ के लिए, भी परिभाषित है, तथा $(a, 0) = a$.)

   ii) किन्हीं दो अवयवों $a, b \in \mathbb{Z}^*$ का l.c.m. है $[a, b] = \dfrac{ab}{(a, b)}$.

4. $a, b \in \mathbb{Z}^*$ के लिए (a, b) ज्ञात करने की यूक्लिडीय ऐल्गोरिद्म।

5. i) **अंकगणित का मूलभूत प्रमेय** :
   प्रत्येक पूर्णांक $n > 1$ को $n = p_1 p_2 \ldots p_n$ के रूप में लिखा जा सकता है, जहाँ $p_1, p_2, \ldots, p_n$ अभाज्य संख्याएँ हैं। आगे, यह निरूपण अद्वितीय होता है केवल उस क्रम को छोड़ते हुए जिसमें वे अभाज्य गुणनखंड प्रकट हो रहे हैं।

   ii) इस प्रमेय की उपपत्ति और उसके अनुप्रयोग।

6. एक अरिक्त समुच्चय S का एक विभाजन S पर एक तुल्यता संबंध परिभाषित करता है। विलोमतः, S पर एक तुल्यता संबंध S पर एक विभाजन परिभाषित करता है।

7. आव्यूहों से संबंधित उदाहरण और मौलिक शब्दावली।

8. किसी आव्यूह का परिवर्त, $\mathbb{M}_{m\times n}(\mathbb{C})$ में दो आव्यूहों का योग और व्यवकलन, $\mathbb{M}_{m\times n}(\mathbb{C})$ में अदिश गुणन, एक $m \times n$ आव्यूह का एक $n \times r$ आव्यूह के साथ गुणन।

9. किसी समतल में एक वस्तु की सममिति की परिभाषा और उदाहरण।

10. किसी समुच्चय X के क्रमचय की परिभाषा और उदाहरण।

11. $|S_n| = n!$.

12. लंबाई $r, r \in \mathbb{N}$, वाले चक्र की परिभाषा और उदाहरण।

अब हम इस इकाई में दिए प्रश्नों के हल देने जा रहे हैं। जब आप **स्वयं** इन प्रश्नों को हल कर लें, तभी इन दिए गए हलों को देखें। ये हल इसलिए दिए गए हैं कि आप

अपने हलों की जाँच कर लें कि आपने प्रश्नों को किस हद तक सही हल किया है। विशेष रूप में, हमारे द्वारा दिए गए हल आपको **गणितीय सोच के हिसाब से सही तर्क प्रस्तुत करने में सहायता कर सकते** हैं। कुछ प्रश्नों के लिए हमने केवल उत्तर या बहुत ही संक्षिप्त में हल प्रस्तुत किए हैं।

1.7 हल / उत्तर

E1) i) क्योंकि $a \cdot 0 = 0$, इसलिए $a \mid 0$.

क्योंकि $1 \cdot a = a$ तथा $(-1)(-a) = a$, इसलिए $(\pm 1) \mid a$ और $(\pm a) \mid a$.

ii) $a \mid b \Rightarrow b = ad$, किसी $d \in \mathbb{Z}$ के लिए।

$\Rightarrow bc = (ad)c = (ac)d$

$\Rightarrow ac \mid bc.$

iii) $b = ad,\ c = be$, किन्हीं $d, e \in \mathbb{Z}$ के लिए।

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

iv) $a \mid b \Rightarrow b = ad$, किसी $d \in \mathbb{Z}$ के लिए।

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

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

$\therefore e = \pm 1.$

$\therefore a = \pm b.$

विलोमतः, यदि $a = \pm b$, तो (i) से $a \mid b$ और $b \mid a$.

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

$\therefore$ किन्हीं भी $x, y \in \mathbb{Z}$ के लिए, $ax + by = c(dx + ey)$ और $dx + ey \in \mathbb{Z}$.

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

E2) $75 = (2 \times 30) + 15,\ (-75) = [3 \times (-30)] + 15.$

E3) मान लीजिए कि $a = 3q + r,\ 0 < r < 3$. तब, $r = 1$ या 2.

यदि $r = 1$, तो $a^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1.$

यदि $r = 2$, तो $a^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3q' + 1$, जहाँ $q' = 3q^2 + 4q + 1.$

इस प्रकार, दोनों स्थितियों में, a^2 को 3 से भाग देने पर शेषफल 1 है।

E4) मान लीजिए कि $a^2 + b^2 = 3c$. किसी $c \in \mathbb{Z}$ के लिए। …(10)

अब, मान लीजिए कि $3|a$. तब $3|a^2$, मान लीजिए कि $a^2 = 3m$ किसी $m \in \mathbb{Z}$ के लिए।

अतः, (10) द्वारा, $b^2 = 3(c-m)$, अर्थात्, $3|b^2$.

इसलिए, E3 द्वारा, $3|b$.

इसी प्रकार, यदि $3|b$, तो $3|a$.

अब मान लीजिए कि $3 \nmid a$ और $3 \nmid b$. तब, E3 द्वारा,

$a^2 = 3q + 1$ और $b^2 = 3q' + 1$, किन्हीं $q, q' \in \mathbb{Z}$ के लिए।

अतः, $a^2 + b^2 = 3(q + q') + 2$, अर्थात्, $3 \nmid (a^2 + b^2)$, जो एक अंतर्विरोध है।

अतः, $3|a$ या $3|b$. परंतु यदि 3 इनमें से किसी एक को विभाजित करता है, तो आप पहले ही देख चुके हैं कि 3 दूसरे को विभाजित करता है।

अतः, $3|(a^2 + b^2) \Rightarrow 3|a$ और $3|b$.

E5) i) यहाँ $(a, b) = 7 = 1 \cdot 7 + 0 \cdot 21$. इस प्रकार, $m = 1$ और $n = 0$.

ii) क्योंकि 5 एक अभाज्य संख्या है और $5 \nmid 271$, इसलिए $(-5, -271) = 1$.

साथ ही, $(-271) = (-5)54 - 1$. इसलिए, $1 = 54(-5) + (-271)(-1)$.

इसलिए, यहाँ $m = 54$ और $n = -1$.

iii) यहाँ $(a, b) = (-c, c) = |c|$.

यदि $c > 0$, तो $(a, b) = c = 0(-c) + 1 \cdot c$.

यदि $c < 0$, तो $(a, b) = -c = 1(-c) + 0 \cdot c$.

E6) मान लीजिए कि $d = (a, b)$.

अब, मान लीजिए कि $h = (-a, b)$ और $k = (-a, -b)$.

क्योंकि $d|a$, इसलिए $d|(-a)$, अतः, $d|h$.

साथ ही, $h|(-a) \Rightarrow h|a$, अतः, $h|d$. इस प्रकार, $h = \pm d$.

परंतु $h > 0, d > 0$. अतः $h = d$.

इसी प्रकार, दर्शाइए कि $k = h$.

इस प्रकार, $d = h = k$.

E7) मान लीजिए कि $p \nmid a$. तब, $(p, a) = 1$. इसलिए, प्रमेय 6 द्वारा, $p \mid b$.

E8) मान लीजिए कि $P(n)$ निम्न विधेय है :

$p \mid a_1 a_2 \ldots a_n \Rightarrow$ किसी $i = 1, 2, \ldots, n$ के लिए, $p \mid a_i$.

सत्यापन कीजिए कि $P(1)$ सत्य है।

मान लीजिए कि किसी $m \geq 2$ के लिए, $P(m-1)$ सत्य है।

अब, मान लीजिए कि $p \mid a_1 a_2 \ldots a_m$. तब, $p \mid (a_1 \ldots a_{m-1}) a_m$.

E7 द्वारा, $p \mid (a_1 a_2 \ldots a_{m-1})$ या $p \mid a_m$.

यदि $p \mid a_1 a_2 \ldots a_{m-1}$, तो किसी $i = 1, \ldots, m-1$ के लिए, $p \mid a_i$ (क्योंकि $P(m-1)$ सत्य है)।

$\therefore$ किसी $i = 1, \ldots, m$ के लिए, $p \mid a_i$.

$\therefore P(m)$ सत्य है।

$\therefore P(n)$ सत्य है सभी $n \in \mathbb{N}$ के लिए।

E9) यहाँ $b > 0, q, r \in \mathbb{Z}$ s.t. $a = bq + r$.

अब मान लीजिए कि $(a, b) = d$. तब $d \mid a$ और $d \mid b$. इसलिए, $d \mid (a - bq)$, अर्थात्, $d \mid r$.

साथ ही, यदि $c \mid b$ और $c \mid r$, तो $c \mid (bq + r)$. अर्थात् $c \mid a$. इसलिए, $c \mid d$.

अतः, $d = (b, r)$.

E10) i) मान लीजिए कि $(p, a) = d$. तब, $d \mid p$. इसलिए $d = 1$ या $d = p$.

क्योंकि $d \mid a$ और $p \nmid a$, इसलिए $d \neq p$. अतः, $d = 1$.

ii) अब, यदि $a = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$, तो $a^2 = p_1^{2m_1} p_2^{2m_2} \ldots p_r^{2m_r}$.

इसलिए, $p \mid a^2 \Rightarrow$ किसी $i = 1, \ldots, r$ के लिए, $p = p_i$. अतः, $p \mid a$.

E11) मान लीजिए कि, इसके विपरीत, $\sqrt{p} \in \mathbb{Q}$.

तब, $\sqrt{p} = \dfrac{a}{b}$, जहाँ $a, b \neq 0$ तथा $(a, b) = 1$.

तब, $\frac{a^2}{b^2} = p \Leftrightarrow a^2 = pb^2 \Rightarrow p \mid a^2.$

अतः, E10(ii) द्वारा, $p \mid a$. अब मान लीजिए कि किसी $c \in \mathbb{Z}$ के लिए $pc = a$.

तब, $p^2c^2 = a^2 = pb^2.$

अतः, $pc^2 = b^2$. इसलिए, $p \mid b$.

अतः, $p \mid (a, b)$, अर्थात् $p \mid 1$, जो एक अंतर्विरोध है।

इसलिए, $\sqrt{p} \notin \mathbb{Q}$.

E12) हम दिए हुए कथन का प्रतिधनात्मक सिद्ध करेंगे (भाग 1.3, इकाई 1, वास्तविक विश्लेषण को देखिए)। अर्थात्, हम कथन यदि $n^{1/m} \in \mathbb{Q}$, तो $n^{1/m} \in \mathbb{Z}$, $n, m \in \mathbb{N}$ के लिए को सिद्ध करेंगे।

अतः, मान लीजिए कि $n^{1/m} = \frac{a}{b}$, जहाँ $(a, b) = 1$ तथा $b \neq 1$.

तब, $n = \frac{a^m}{b^m}$, अर्थात् $b^m n = a^m$.

मान लीजिए कि p एक ऐसी अभाज्य संख्या है कि $p \mid b^m$. तब, जैसा कि E10(ii) में, $p \mid b$.

साथ ही, $p \mid b^m \Rightarrow p \mid a^m \Rightarrow p \mid a$.

अतः, $p \mid (a, b) = 1$, जो अंतर्विरोध है।

इस प्रकार, $b = 1$.

अतः, $n^{1/m} \in \mathbb{Z}$.

E13) प्रमेय 7 द्वारा, $n = p_1, p_2 \ldots p_t$, $t \geq 1$, जहाँ हो सकता है कि सभी p_i अलग-अलग नहीं हों।

अब, यदि आवश्यक हो तो, $p_1, p_2, \ldots, p_t$ के क्रम में परिवर्तन करने पर, मान लीजिए कि सभी p_i में p_1 न्यूनतम है।

मान लीजिए कि $p_1 = p_{i_1+1} = p_{i_1+2} = \cdots = p_{i_1+m_1-1}$.

क्योंकि $p_i p_j = p_j p_i \ \forall \ i, j$, इसलिए हम इन $m_1 p_i$ को इकट्ठा करके, इन्हें $p_1^{m_1}$ के रूप में लिख सकते हैं।

अब, $\frac{n}{p_1^{m_1}} = m$ पर दृष्टि डालिए। पुनः, उन सभी p_i में से न्यूनतम p_i चुनिए,

जिसमें m गुणनखंडित हुआ है। इसे p_2 रखिए। ध्यान दीजिए कि $1 < p_1 < p_2$.
अब उन सभी p_i को इकट्ठा कीजिए जो p_2 के बराबर हैं, मान लीजिए m_2 ऐसे p_i हैं। तब $m = p_2^{m_2} p_j p_{j+1} \ldots p_s$.

अतः, $n = p_1^{m_1} p_2^{m_2} p_j p_{j+1} \ldots p_s$, जहाँ $t = m_1 + m_2 + (s - j + 1)$.

इसी प्रक्रिया को जारी रखते हुए, हम प्राप्त करते हैं :

$n = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}, 1 < p_1 < \ldots < p_r$ जहाँ $m_1 + m_2 + \cdots + m_r = t$.

E14) $y = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}, r \geq 1, m_i \in \mathbb{N}, 1 < p_1 < p_2 < \ldots < p_r$.

यदि y सम है, तो $2 | y$. तब, $p_1 = 2$ है। $m_1 = r$ कहिए।

तब, $y = 2^r x$, जहाँ $x = p_2^{m_2} \ldots p_r^{m_r}$ विषम है, क्योंकि $2 \nmid x$.

यदि y सम नहीं है, तो $y = 2^r y$ है, जहाँ $r = 0$.

अतः, परिणाम प्राप्त हो जाता है।

E15) i) $54321 = 4(12345) + 4941$ …(11)

$12345 = 2(4941) + 2463$ …(12)

$4941 = 2(2463) + 15$ …(13)

$2463 = 164(15) + 3$ …(14)

$15 = 5(3) + 0.$

$\therefore (54321, 12345) = 3.$

आगे, $3 = 2463 - 164(15)$, (14) से।

$= 2463 - 164[4941 - 2(2463)]$, (13) से।

$= 329(2463) - 164(4941)$

$= 329[12345 - 2(4941)] - 164(4941)$, (12) से।

$= (329 \cdot 12345) - (822 \cdot 4941)$

$= (329 \cdot 12345) + (-822)[54321 - 4(12345)]$

$= (3617 \cdot 12345) + [(-822) \cdot 54321].$

इस प्रकार, $m = -822$ और $n = 3617$.

ii) सर्वप्रथम, $(-61880, -880) = (61880, 880)$.

अब, $61880 = 70(880) + 280$ …(15)

$880 = 3(280) + 40$ …(16)

$280 = 7(40) + 0.$

$\therefore (61880, 880) = 40.$

आगे, $40 = 880 - 3(280)$, (16) से।

$= 880 - 3[61880 - 70(880)]$, (15) से।

$= [(-3) \cdot 61880] + (211 \cdot 880).$

अतः, $m = -3$ और $n = 211$.

E16) i) आपको इसका सत्यापन करना चाहिए कि R स्वतुल्य और सममित है।

R संक्रामक भी है, क्योंकि यदि nRm और mRp है, तो
$nm > 0,\ mp > 0 \Rightarrow (nm)(mp) > 0 \Rightarrow (np)m^2 > 0,$

$\Rightarrow np > 0$ क्योंकि $m^2 > 0.$

$\Rightarrow nRp$ है।

यहाँ, $[n] = \{m \in \mathbb{Z} \mid nm > 0\}$ है।

यदि $n < 0$, तो $[n]$ ऋणात्मक पूर्णांकों का समुच्चय है। अतः, $[n] = [-1]$.

साथ ही, कोई भी $n \in \mathbb{Z}^*$ या तो $[1]$ में है या $[-1]$ में है।

अतः, $\mathbb{Z}^* = [1] \cup [-1]$.

ii) आपको यह दर्शाना चाहिए कि R एक तुल्यता संबंध है।

साथ ही, यहाँ $\mathbb{Z}^* = [1] \cup [10] \cup [100] \cup \ldots$ एक अपरिमित सम्मिलन है।

इसका कारण यह है कि हर $m \in \mathbb{N}$ के लिए m अंकों वाले पूर्णांक हैं। तथा, ऐसा कोई भी पूर्णांक 10^{m-1} के तुल्य होता है।

E17) 'वास्तविक विश्लेषण' की इकाई 1 से आप जानते हैं कि '$p \Rightarrow q$' यह व्यक्त करता है कि 'यदि p सत्य है, तो q सत्य है'।

स्पष्टतः, यदि A सत्य है, तो A सत्य है। अतः, $A \Rightarrow A$.

इस प्रकार, '$\Rightarrow$' स्वतुल्य है।

आगे, यदि $A \Rightarrow B$ और $B \Rightarrow C$. तो B सत्य है, जब भी A सत्य है तथा C सत्य है, जब भी B सत्य है। अतः, C सत्य है, जब भी A सत्य है। अर्थात्, $A \Rightarrow C$.

इस प्रकार, '$\Rightarrow$' संक्रामक है।

अब निम्न A और B पर विचार कीजिए।

$A: a = b$, जहाँ $a, b \in \mathbb{C}$,

तथा $B: |a| = |b|$, जहाँ $a, b \in \mathbb{C}$.

तब, $A \Rightarrow B$, परंतु $B \not\Rightarrow A$ (जैसे कि $|\omega| = |1|$, जहाँ ω एक का एक संमिश्र घनमूल है, परंतु $\omega \neq 1$.)

इस प्रकार, '$\Rightarrow$' सममित नहीं है।

E18) उदाहरण 4 की ही तरह, आप $\equiv (\text{mod } 8)$ के संगत $[0], [1], \ldots, [7]$ प्राप्त कर सकते हैं।

अब, यदि $a \equiv b (\text{mod } 1)$, तो $1 | (a - b)$. अतः, किसी $n \in \mathbb{Z}$ के लिए $a = b + n$.

इस प्रकार, $[a] = \{a + n | n \in \mathbb{Z}\}$.

अतः, $\mathbb{Z} = [0]$, क्योंकि $[0] = \{n | n \in \mathbb{Z}\}$.

इस प्रकार, इस स्थिति में केवल एक वर्ग ही है।

E19) i) ये दूसरी पंक्ति तथा तीसरे स्तंभ के अवयव हैं।

इस प्रकार, ये क्रमशः 0 और 1 हैं।

ii) $[0 \quad 0 \quad 7]$.

iii) केवल A एक वर्ग आव्यूह है। इसका विकर्ण $\{1, 5, 7\}$ है।

iv) $\begin{bmatrix} 2 \\ 5 \\ 0 \end{bmatrix}$.

v) इसका अस्तित्व नहीं है, क्योंकि B में केवल 3 पंक्तियाँ हैं।

E20) ऐसे अनंततः अनेक अवयव हैं। ध्यान दीजिए कि यह एक 4×2 आव्यूह है, जिसकी प्रविष्टियाँ $\mathbb{Q}$ से हैं, और जिनमें से **कम से कम** एक प्रविष्टि $\mathbb{Z}$ में नहीं होनी चाहिए।

उदाहरणार्थ, $A = \begin{bmatrix} 1 & 2 \\ -3 & -4 \\ 0.25 & 0 \\ 0 & 0 \end{bmatrix}$. यह $\mathbb{M}_{4\times 2}(\mathbb{Z})$ में नहीं है, क्योंकि $0.25 \notin \mathbb{Z}$. परंतु A की सभी प्रविष्टियाँ $\mathbb{Q}$ में हैं।

E21) क्योंकि विकर्ण में 4 अवयव हैं, आव्यूह 4×4 कोटि का है। दिए हुए गुणों को देखते हुए आव्यूह निम्न होगा :

$$\begin{bmatrix} e & 0 & 0 & 0 \\ 1 & i & 0 & 0 \\ 1 & 1 & \pi & 0 \\ 1 & 1 & 1 & -1 \end{bmatrix}.$$

E22) क्योंकि $\mathbb{N} \subseteq \mathbb{R}$, इसलिए $\mathbb{N}$ पर प्रत्येक आव्यूह $\mathbb{R}$ पर एक आव्यूह है। अतः, यदि $A \in \mathbb{M}_n(\mathbb{R})$ ऐसा है कि $a_{ij} \in \mathbb{N}\ \forall\ i, j = 1, \ldots, n$ तो $A = [a_{ij}] \in \mathbb{M}_n(\mathbb{N})$.

E23) क्योंकि $[3 \quad 4]$ कोटि 1×2 का है तथा $\begin{bmatrix} 3 \\ 4 \end{bmatrix}$ कोटि 2×1 का है, इसलिए इनकी कोटियाँ अलग हैं। अतः, ये बराबर नहीं हैं।

E24) नहीं, क्योंकि इनकी कोटियाँ अलग हैं।

E25) i) $\begin{bmatrix} 1+(-1) & 0+0 \\ 0+0 & 1+(-1) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

ii) $[0]_{m\times n} = \mathbf{0}$, जो सभी प्रविष्टियों 0 वाला $m\times n$ आव्यूह है।

iii) $[a_{ij} + 0]_{m\times n} = [a_{ij}]_{m\times n}$.

E26) $A^t = \begin{bmatrix} -i & 0.2 & -1 \\ 1.5 & i & 0 \end{bmatrix}$, $B^t = \begin{bmatrix} \sqrt{2} & -\sqrt{2} & \pi \\ \sqrt{3} & -\sqrt{3} & 4 \end{bmatrix}$,

$$(A+B)^t = \begin{bmatrix} -i+\sqrt{2} & 0.2-\sqrt{2} & -1+\pi \\ 1.5+\sqrt{3} & i-\sqrt{3} & 4 \end{bmatrix}.$$

अब, $A^t + B^t = \begin{bmatrix} -i+\sqrt{2} & 0.2-\sqrt{2} & -1+\pi \\ 1.5+\sqrt{3} & i-\sqrt{3} & 4 \end{bmatrix} = (A+B)^t$, क्योंकि संगत स्थानों में प्रविष्टियाँ समान हैं।

E27) मान लीजिए कि $A = [a_{ij}]$, $B = [b_{ij}]$ और $C = [c_{ij}]$.

i) $A + B = [a_{ij} + b_{ij}] = [b_{ij} + a_{ij}]$, क्योंकि S में $+$ क्रमविनिमेय है।

$= B + A.$

ii) $A + (B + C) = [a_{ij} + (b_{ij} + c_{ij})] = [(a_{ij} + b_{ij}) + c_{ij}]$, क्योंकि S में + साहचर्य है।

$= (A + B) + C.$

E28) i) मान लीजिए कि $A = [a_{ij}]$ और $(A^t)^t = [c_{ij}]$.

सर्वप्रथम, ध्यान दीजिए कि यदि A की कोटि $m \times n$ है, तब A^t की कोटि $n \times m$ है। अतः, $(A^t)^t$ की कोटि $m \times n$ होगी।

आगे, $i = 1, \ldots, m;\ j = 1, \ldots, n$ के लिए,

$c_{ij} = (A^t)^t$ की (i, j) वीं प्रविष्टि

$= A^t$ की (j, i) वीं प्रविष्टि

$= A$ की (i, j) वीं प्रविष्टि।

$= a_{ij}.$

अतः, $(A^t)^t = A$.

ii) $(A + A^t)^t = A^t + (A^t)^t$, प्रमेय 10(ii) द्वारा।

$= A^t + A$, उपरोक्त (i) द्वारा।

$= A + A^t$, E27(i) द्वारा।

इसी प्रकार, आपको दर्शाना चाहिए कि $(A - A^t)^t = -(A - A^t)$.

E29) ii) मान लीजिए कि $A = [a_{ij}]$ और $B = [b_{ij}]$.

तब, $A - B = [a_{ij} - b_{ij}]$.

अतः, $\alpha(A - B) = \alpha[a_{ij} - b_{ij}] = [\alpha(a_{ij} - b_{ij})] = [\alpha a_{ij} - \alpha b_{ij}]$

$= [\alpha a_{ij}] - [\alpha b_{ij}]$

$= \alpha[a_{ij}] - \alpha[b_{ij}]$

$= \alpha A - \alpha B.$

iii) मान लीजिए कि $A = [a_{ij}]_{m \times n}$ है। तब $\alpha A = [\alpha a_{ij}]_{m \times n}$.

$(\alpha A)^t$ की (i, j) वीं प्रविष्टि

$= \alpha A$ की (j, i) वीं प्रविष्टि

$= \alpha a_{ji}$

$= \alpha$ (A^t की (i, j) वीं प्रविष्टि)।

यह प्रत्येक $i = 1, \ldots, m$ और $j = 1, \ldots, n$ के लिए सत्य है।

अतः, $(\alpha A)^t = \alpha A^t$.

iv) मान लीजिए कि $A = [a_{ij}]$. तब,

$$(\alpha\beta)A = (\alpha\beta)[a_{ij}] = [(\alpha\beta)a_{ij}] = [\alpha(\beta a_{ij})]$$

$$= \alpha[\beta a_{ij}] = \alpha(\beta A).$$

E30) $\sqrt{2}\,A = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ और $\sqrt{3}B = \sqrt{3}\begin{bmatrix} 1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{bmatrix} = \begin{bmatrix} \sqrt{3}/2 & 3/2 \\ -3/2 & \sqrt{3}/2 \end{bmatrix}$.

अतः, $\sqrt{2}A - \sqrt{3}B = \begin{bmatrix} \frac{2-\sqrt{3}}{2} & \frac{-1}{2} \\ \frac{1}{2} & \frac{2-\sqrt{3}}{2} \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2-\sqrt{3} & -1 \\ 1 & 2-\sqrt{3} \end{bmatrix}$.

इस प्रकार, $C = \begin{bmatrix} 2-\sqrt{3} & -1 \\ 1 & 2-\sqrt{3} \end{bmatrix}$.

E31) आपको यह दर्शाना चाहिए कि ~ स्वतुल्य, सममित और संक्रामक क्यों है। ध्यान दीजिए कि C की प्रविष्टियाँ $\mathbb{Z}$ से हैं।

तब, $[\mathbf{0}] = \{A \in \mathbb{M}_{m\times n}(\mathbb{C}) \mid A - \mathbf{0} = 5C$, किसी $C \in \mathbb{M}_{m\times n}(\mathbb{Z})$ के लिए $\}$

$= \{5C \mid C \in \mathbb{M}_{m\times n}(\mathbb{Z})\}$.

E32) क्योंकि A एक 2×3 आव्यूह है तथा B और C दो 3×2 आव्यूह हैं, इसलिए AB और AC परिभाषित हैं, परंतु BC परिभाषित नहीं है।

यहाँ, $AB = \begin{bmatrix} 9 & 5 & -4 \\ -3 & 0 & 2 \end{bmatrix}\begin{bmatrix} 9 & -3 \\ 5 & 0 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} 122 & -35 \\ -35 & 13 \end{bmatrix}$, तथा

$$AC = \begin{bmatrix} 9 & 5 & -4 \\ -3 & 0 & 2 \end{bmatrix}\begin{bmatrix} 3 & \sqrt{3} \\ 1 & i \\ i & 1 \end{bmatrix} = \begin{bmatrix} 32-4i & -4+9\sqrt{3}+5i \\ -9+2i & 2-3\sqrt{3} \end{bmatrix}.$$

E33) क्योंकि $A, B \in \mathbb{M}_n(\mathbb{C})$, इसलिए $A+B \in \mathbb{M}_n(\mathbb{C})$. अतः, $(A+B)^2$ परिभाषित है। अब,

$(A+B)^2 = (A+B)(A+B) = A(A+B)+B(A+B)$, P2 के उपयोग से।

$= A\cdot A + AB + BA + B\cdot B$, P2 के उपयोग से।

$= A^2 + AB + BA + B^2.$

E34) यहाँ $C = \begin{bmatrix} 700 \\ 1200 \end{bmatrix}$. अतः, $AC = [20{,}700 \;\; 15{,}300 \;\; 4{,}900]^t$, प्रत्येक दुकान द्वारा निवेशित धनराशियाँ यह निरूपित करता है दोनों पुस्तकों की उन कॉपियों के लिए जो बिकी नहीं हैं।

E35) आइए दी हुई समीकरणों को निम्न रूप में पुनः लिखें :

$7x + 3y + 4z = 5$

$2 + 3y + 0\cdot z = 6$

$0\cdot x - 4y + z = 19$

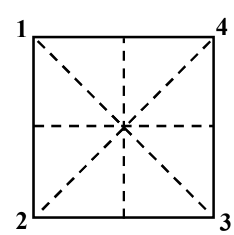
अब, आप यदि भाग 1.4 के प्रारंभ के रैखिक निकाय (I) पर दृष्टि डालें, तो आप देखेंगे कि इसे किस प्रकार वाँछित रूप में लिखा जाता है।

$A = \begin{bmatrix} 7 & 3 & 4 \\ 2 & 3 & 0 \\ 0 & -4 & 1 \end{bmatrix}, X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ और $B = \begin{bmatrix} 5 \\ 6 \\ 19 \end{bmatrix}$ लीजिए।

तब, जाँच कीजिए कि उपरोक्त समीकरणों को समतुल्य आव्यूह समीकरण $AX = B$ द्वारा प्रदर्शित किया जाता है।

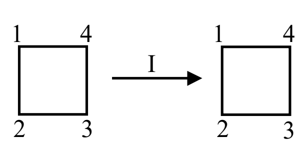
E36) i) जैसा हमने एक समबाहु त्रिभुज के साथ किया था वैसा ही एक वर्ग के साथ कीजिए। इसकी मेज़ पर एक बाहरी रूप रेखा खींचिए। इसके शीर्षों को वामावर्त दिशा में संख्याओं से अंकित कीजिए, जैसा आकृति 9 में है।

अब, देखिए कि इसकी कितनी सममिति-रेखाएँ हैं। उदाहरणार्थ, सम्मुख शीर्षों को मिलाने वाली रेखाएँ या इसकी सम्मुख भुजाओं के मध्य-बिंदुओं को मिलाने वाली रेखाएँ इसकी सममिति-रेखाएँ हैं। जाँच कीजिए कि क्या और भी कोई सममिति-रेखाएँ संभव हो सकती हैं।



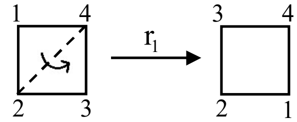
आकृति 9: एक वर्ग, और उसकी 4 परावर्तन सममिति की रेखाएँ।

पुनः, इस वर्ग को इसके केन्द्र (जो इसके विकर्ण का प्रतिच्छेद बिंदु है) के प्रति वामावर्त दिशा में 90° से घुमाइए। आपको एक सममिति प्राप्त होगी। अन्य घूर्णन सममितियाँ क्या हैं? निम्नलिखित चार्ट में, हम सभी सममितियाँ दे रहे हैं :

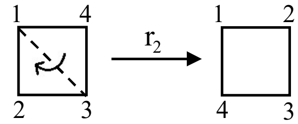


$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

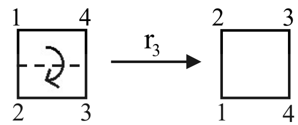
$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$



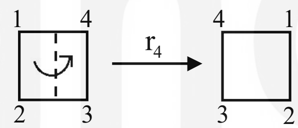
$$r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$



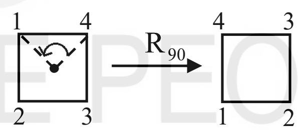
$$r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$



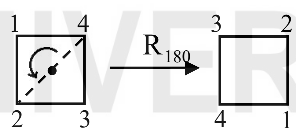
$$r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$



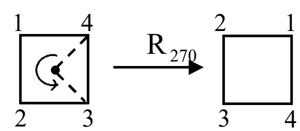
$$R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$



$$R_{180} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

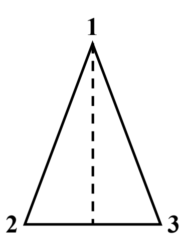


$$R_{270} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$



आप इनमें से किन्हीं के संयोजन ले सकते हैं। तब आप पाएँगे कि वह केवल इनमें से ही कोई होगा। उदाहरणार्थ,

$$r_1 \circ r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = R_{180}.$$

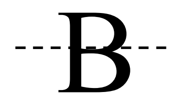


आकृति 10: समद्विबाहु त्रिभुज।

ii) किसी समद्विबाहु त्रिभुज की केवल एक ही सममिति रेखा है (आकृति 10 को देखिए), तथा इसकी कोई भी अतुच्छ घूर्णन सममिति नहीं है। इस प्रकार, इस समुच्चय में केवल दो अवयव, I और $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, हैं।

E37) सत्यापन कीजिए कि N की कोई परावर्तन सममिति नहीं है। इसकी दो घूर्णन सममितियाँ $R_0 = I$ और R_{180} हैं।

B की तुच्छ घूर्णन सममिति, I, है तथा इसकी क्षैतिज रेखा के प्रति एक परावर्तन सममिति है, जैसा आकृति 11 में दर्शाया गया है। इस प्रकार, B, N और एक समद्विबाहु त्रिभुज में सममितियों की संख्याएँ बराबर हैं।



आकृति 11

E38) I के अतिरिक्त, D_6 का प्रत्येक अवयव एक चक्र है।

$r_1 = (2\ \ 3),\ r_2 = (1\ \ 3),\ r_3 = (1\ \ 2)$ में से प्रत्येक 2-चक्र है।

दोनों $R_{120} = (1\ \ 2\ \ 3)$ और $R_{240} = (1\ \ 3\ \ 2)$ 3-चक्र हैं।

साथ ही, ध्यान दीजिए कि S_3 में $\{1, 2, 3\}$ के 6 क्रमचय हैं। ये सभी D_6 में सम्मिलित हैं। अतः, $S_3 = D_6$.

E39) आप किसी को भी चुन सकते हैं, उदाहरणार्थ, (1 3 5).

$$(1\ \ 3\ \ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 6 & 7 \end{pmatrix}.$$

E40) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix},\ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ \ 4\ \ 3),$$ एक 3-चक्र।

आपको इसकी जाँच करनी चाहिए कि $\alpha^2 = (1\ \ 2\ \ 3)$ और $\beta^2 = (1\ \ 4\ \ 2)$.

आगे, $\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} = (1\ \ 3\ \ 4).$

क्योंकि $\alpha \circ \beta(1) = 1$ और $\beta \circ \alpha(1) = 3$, इसलिए $\alpha \circ \beta \neq \beta \circ \alpha$.

इकाई 2

समूह

इकाई की रूपरेखा **पृष्ठ संख्या**

2.1 प्रस्तावना

अभी तक आपने जिन पाठ्यक्रमों का अध्ययन किया है, उनमें आपने अनेक समुच्चयों तथा कुछ समुच्चयों पर द्वि-आधारी संक्रियाओं के साथ कार्य किया है। इस इकाई में आप ऐसे समुच्चयों का अध्ययन करेंगे जिन पर नियमों का पालन करने वाले द्वि-आधारी संक्रियाएँ परिभाषित हैं। ये नियम संबंधित समुच्चयों पर एक बीजीय संरचना स्थापित कर देते हैं। हम ऐसी बीजीय निकाय को एक समूह कहते हैं।

समूह सिद्धांत अमूर्त बीजगणित की प्राचीनतम शाखाओं में से एक है। गणित में तथा अन्य विज्ञानों में इसके अनेक अनुप्रयोग हैं। समूह सिद्धांत ने भौतिकी, रसायन और कम्प्यूटर विज्ञान, तथा निःसंदेह गणित, के विकास में सहायता की है। इसकी जड़ें अठारहवीं शताब्दी के गणितज्ञों लंग्राज (Lagrange), रूफ़ीनी (Ruffini) और गैलोआ (Galois) के कार्यों में मिलती हैं। इस इकाई से, आप इस सिद्धांत का अध्ययन प्रारंभ करेंगे।

भाग 2.2 में आप एक समूह की परिभाषा का अध्ययन करेंगे, तथा समूहों पर कुछ उदाहरणों का भी अध्ययन करेंगे। यहाँ आप विविध प्रकार के समूहों, जैसे परिमित, अपरिमित, क्रमविनिमेय, अक्रमविनिमेय आदि को भी जानेंगे। इस भाग में आप परिमित समूहों से संबद्ध द्वि-आधारी संक्रियाओं की सारणियों का भी अध्ययन करेंगे।

भाग 2.3 में हम कुछ ऐसी मौलिक गुणों की विस्तृत रूप से चर्चा करेंगे, जिन्हें किसी भी समूह के अवयव संतुष्ट करते हैं।

अंत में, भाग 2.4 में आपका परिचय छः प्रकार के सुपरिचित समूहों से कराया जाएगा। इन समूहों का काफ़ी उपयोग किया जाता है।

आगे आने वाली इकाइयों में हम समूह सिद्धांत को आगे और बढ़ाएंगे। इस इकाई का अध्ययन अच्छी तरह से कीजिए ताकि शेष पाठ्यक्रम के लिए आपकी आधारशिला मजबूत हो जाए।

ऐसा करने से आपको इस इकाई को सीखने के उद्देश्यों को प्राप्त करने में सहायता मिलेगी। इनकी अब सूची हम दे रहे हैं।

उद्देश्य

इस इकाई की पढ़ाई के बाद, आप निम्नलिखित करने में समर्थ हो जाएँगे :

- समूहों को परिभाषित करना और उनके उदाहरण देना;
- आबेली और अन्आबेली समूहों को परिभाषित करना और उनके उदाहरण देना;
- परिमित और अपरिमित समूहों में अंतर स्पष्ट करना;
- सभी समूहों के कुछ मौलिक गुणों को सिद्ध करना और उनका उपयोग करना;
- पूर्णांकों मॉड्यूलो n का समूह, सममित समूह, द्वितल समूह, किसी समूह पर आव्यूहों का समूह, इकाई के **nवें** मूलों ($n \in \mathbb{N}$ के लिए) का समूह तथा किन्हीं दो समूहों के अनुलोम गुणनफल – इन समूहों के प्रारंभिक समूह गुणों की व्याख्या करना और उनका उपयोग करना।

2.2 समूह क्या है?

कलन में आपने समुच्चयों के बारे में तथा द्वि-आधारी संक्रियाओं के बारे में अध्ययन किया था। इस भाग में आप एक विशेष प्रकार के बीजीय निकाय का अध्ययन करेंगे, जो एक समुच्चय और उस पर एक द्वि-आधारी संक्रिया से बनता है। इस निकाय को समझने के लिए, $\mathbb{Z}$ को लीजिए, और उस पर द्वि-आधारी संक्रिया '+' को लीजिए। आपने कई दफ़ा पूर्णांकों के निम्नलिखित गुणों का उपयोग किया है :

i) $(a+b)+c = a+(b+c) \ \forall \ a, b, c \in \mathbb{Z}$,

ii) $a+0 = a = 0+a \ \forall \ a \in \mathbb{Z}$,

iii) $a \in \mathbb{Z}$ दिया रहने पर, हमें $(-a) \in \mathbb{Z}$ प्राप्त है जिससे कि $a+(-a) = 0$.

यही तीनों गुण हैं, जो $(\mathbb{Z}, +)$ को एक समूह बनाते हैं, जैसा कि अब आप देखेंगे।

परिभाषा: मान लीजिए कि G एक अरिक्त समुच्चय है तथा G पर $*$ एक द्वि-आधारी संक्रिया है। युग्म $(G, *)$ एक **समूह** (group) कहलाता है, यदि

G1) $*$ **साहचर्य** है, अर्थात्, $(a*b)*c = a*(b*c) \ \forall \ a, b, c \in G$.

G2) G में एक ऐसा अवयव e है जिससे कि $a*e = a = e*a \ \forall \ a \in G$. (यहाँ e, $*$ के लिए G का **तत्समक** अवयव (**identity element**) कहलाता है।);

G3) G के प्रत्येक अवयव a के लिए, G में एक अवयव b ऐसा होता है जिससे कि $a*b = e = b*a$. (यहाँ $*$ **के सापेक्ष** b, G में **a का प्रतिलोम (inverse)** कहलाता है।)

आप देख चुके हैं कि $(\mathbb{Z}, +)$ एक समूह है। आइए एक अन्य उदाहरण पर दृष्टि डालें।

उदाहरण 1: दर्शाइए कि $(\mathbb{R}, +)$ एक समूह है, परंतु $(\mathbb{R}, \cdot)$ समूह नहीं है।

हल: आप जानते हैं कि $\mathbb{R}$ पर + एक साहचर्य द्वि-आधारी संक्रिया है। + के सापेक्ष एक तत्समक अवयव 0 है, तथा + के सापेक्ष $r \in \mathbb{R}$ का एक प्रतिलोम $(-r)$ है। इस प्रकार, $(\mathbb{R}, +)$ गुणों G1, G2 और G3 को संतुष्ट करता है। अतः, यह एक समूह है।

अब, आप जानते हैं कि $\mathbb{R}$ में गुणन एक साहचर्य द्वि-आधारी संक्रिया है, तथा $1 \in \mathbb{R}$ एक गुणनात्मक तत्समक है। परंतु क्या $\mathbb{R}$ में प्रत्येक अवयव का गुणनात्मक प्रतिलोम होता है? जैसे कि, क्या 0 का $\cdot$ के सापेक्ष कोई प्रतिलोम है? नहीं, क्योंकि ऐसी कोई वास्तविक r नहीं है जिससे कि $r \cdot 0 = 1$ हो। अतः, $(\mathbb{R}, \cdot)$, G3 को संतुष्ट नहीं करता है।

इसलिए, $(\mathbb{R}, \cdot)$ एक समूह नहीं है।

***

निम्नलिखित संबंधित प्रेक्षण पर विचार कीजिए।

टिप्पणी 1: $(G, *)$ एक **सामिसमूह (semigroup)** कहलाता है, यदि वह गुण G1 को संतुष्ट करता है। इस प्रकार, **प्रत्येक समूह एक सामिसमूह होता है**। अतः, $(\mathbb{R}, \cdot)$ एक सामिसमूह है, क्योंकि यह G1 को संतुष्ट करता है। अतः, यह **उदाहरण है एक ऐसे सामिसमूह का जो एक समूह नहीं है।**

निम्नलिखित प्रश्नों को हल करने से आपको समूहों के कुछ और उदाहरण प्राप्त होंगे।

याद कीजिए कि $S^* = S \setminus \{0\}$, 0 को आविष्ट करने वाले किसी भी समुच्चय S के लिए।

E1) जाँच कीजिए कि $(\mathbb{Q}, +)$, $(\mathbb{R}^*, \cdot)$ और $(\mathbb{C}, -)$ समूह हैं या नहीं।

E2) क्या S_3 में 2-चक्रों का समुच्चय फलनों के संयोजन के सापेक्ष एक समूह है? क्यों, या क्यों नहीं?

आप देख चुके हैं कि यह दर्शाने के लिए कि $(G, *)$ एक समूह है, आपको यह दर्शाने की आवश्यकता है कि G1, G2 और G3 को G संतुष्ट करता है। G2 के लिए, आपको यह दर्शाना होता है कि एक ऐसा $e \in G$ है s.t. $a*e = a$ **और** $e*a = a$. इसी प्रकार, G3 के लिए आपको यह दर्शाना होता है कि $a \in G$ दिया रहने पर $\exists \ b \in G$ s.t. $a*b = e$ **और** $b*a = e$ है। परंतु, जैसा कि अब आप देखेंगे, यह दर्शाना काफ़ी है कि $*$ निम्नलिखित अभिगृहीतों को संतुष्ट करता है।

G1′) $*$ साहचर्य है (जो G1 ही है),

G2′) $\exists\, e \in G$ s.t. $a * e = a \;\forall\; a \in G$,

G3′) $a \in G$ दिया होने पर, $\exists\, b \in G$ s.t. $a * b = e$.

हम जो कह रहे हैं वह यह है कि अभिगृहीतों के दोनों समुच्चय G1, G2, G3 और G1′, G2′, G3′ समतुल्य हैं। अर्थात्, यह दर्शाने के लिए कि $(G, *)$ एक समूह है, हमें केवल यह सिद्ध करने की आवश्यकता है कि $a * e = a$ तथा किसी भी $a \in G$ के प्रतिलोम b को केवल $a * b = e$ संतुष्ट करने की आवश्यकता है। हमें **दोनों** $a * e = a$ **और** $e * a = a$, या $a * b = e$ **और** $b * a = e$, को दर्शाने की **आवश्यकता नहीं** है।

वस्तुतः, G1, G2 और G3 (एक साथ मिलकर) निम्नलिखित अभिगृहीतों के भी समतुल्य हैं :

G1″) $*$ साहचर्य है,

G2″) $\exists\, e \in G$ s.t. $e * a = a \forall a \in G$.

G3″) $a \in G$ दिया रहने पर, $\exists\, b \in G$ s.t. $b * a = e$.

निःसंदेह, जैसा कि आप देख सकते हैं, यदि $(G, *)$ गुणों G1, G2 और G3 को संतुष्ट करता है, तो यह निश्चित रूप से G1′, G2′ और G3′ को संतुष्ट करता है। नीचे दिया गया प्रमेय 1 हमें बताता है कि यदि $(G, *)$ अभिगृहीतों G1′, G2′ और G3′ को संतुष्ट करता है, तो यह G1, G2 और G3 को भी संतुष्ट करता है। एक बार प्रमेय 1 सिद्ध हो जाए, तो आपको G1, G2, G3 तथा G1′, G2′ और G3′ की समतुल्यता प्राप्त हो जाती है।

(इसी तरह, एक प्रमेय के अनुसार G1, G2 और G3 तथा G1″, G2″ और G3″ समतुल्य हैं।)

प्रमेय 1: मान लीजिए कि $(G, *)$ अभिगृहीतों G1′, G2′ और G3′ को संतुष्ट करता है। तब, $e * a = a \;\forall\; a \in G$.

साथ ही, $a \in G$ दिया रहने पर, यदि $\exists\, b \in G$ s.t. $a * b = e$, तो $b * a = e$ होता है। इस प्रकार, $(G, *)$ अभिगृहीतों G1, G2 और G3 को संतुष्ट करता है।

इस प्रमेय को सिद्ध करने के लिए, आइए सर्वप्रथम निम्नलिखित परिणाम को सिद्ध करें, जिसकी हमें आवश्यता होगी।

प्रमेयिका 1: मान लीजिए कि $(G, *)$, G1′, G2′ और G3′ को संतुष्ट करता है। यदि $\exists\, a \in G$ s.t. $a * a = a$, तो $a = e$.

प्रमेयिका (lemma) एक सिद्ध किया हुआ कथन होता है, जिसकी आवश्यकता एक प्रमेय को सिद्ध करने में पड़ती है।

उपपत्ति: G3′ द्वारा हम जानते हैं कि $\exists\, b \in G$ s.t. $a * b = e$.

अब, $(a * a) * b = a * b = e$.

साथ ही, $a * (a * b) = a * e = a$.

अतः, G1′ द्वारा, $a = e$. ■

अब, हम इस प्रमेयिका का उपयोग प्रमेय 1 को सिद्ध करने के लिए करेंगे।

प्रमेय 1 की उपपत्ति: G1 सत्य है, क्योंकि G1 और G1′ एक ही अभिगृहीत हैं।

आगे हम सिद्ध करेंगे कि G3 सत्य है। इसके लिए, मान लीजिए कि $a \in G$. $G3'$ द्वारा, $\exists\, b \in G$ s.t. $a * b = e$. अब,

$$(b * a) * (b * a) = (b * (a * b)) * a, \text{ G1 द्वारा।}$$

$$= (b * e) * a = b * a, \text{ G2}' \text{ द्वारा।}$$

अतः, प्रमेयिका 1 द्वारा, $b * a = e$. अतः, G3 सत्य है।

अब हम दर्शाएँगे कि G2 सत्य है। इसके लिए, मान लीजिए कि $a \in G$.

तब, $G2'$ द्वारा, $a * e = a$.

क्योंकि G3 सत्य है, इसलिए $\exists\, b \in G$ s.t. $a * b = b * a = e$.

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

अर्थात्, G2 सत्य है।

इस प्रकार, $(G, *)$ अभिगृहीतों G1, G2 और G3 को संतुष्ट करता है। ■

अतः, आपने देखा कि तीनों अभिगृहीतों के समुच्चय G1, G2, G3; $G1'$, $G2'$, $G3'$ तथा $G1''$, $G2''$, $G3''$ समतुल्य हैं। इस संदर्भ में, निम्नलिखित महत्वपूर्ण टिप्पणियों पर विचार कीजिए :

टिप्पणी 2: i) क्या आपने इस ओर ध्यान दिया है कि अभिगृहीत G1, G2 और G3 या $G1'$, $G2'$ और $G3'$ किस क्रम में दिए गए हैं? G2 और G3 का क्रम महत्वपूर्ण है, क्योंकि G3 का कोई अर्थ नहीं है, जब तक कि पहले G2 का कथन नहीं दिया गया हो। यही बात $G2'$ और $G3'$, तथा $G2''$ और $G3''$, के लिए भी सत्य है।

ii) ध्यान दीजिए कि यदि $(S, *)$ अभिगृहीतों $G1'$, $G2'$ और $G3''$, या $G1'$, $G2''$ और $G3'$, को संतुष्ट करता है, तो इसका **एक समूह होना आवश्यक नहीं** है। उदाहरणार्थ, $* : \{a, b\} \times \{a, b\} \to \{a, b\}$ पर विचार कीजिए, जो $x * y = x \;\forall\; x, y \in S = \{a, b\}$ द्वारा परिभाषित है।

तब, S पर '$*$' एक सुपरिभाषित द्वि-आधारी संक्रिया है। आप इसकी जाँच कर सकते हैं कि यह $G1'$ को संतुष्ट करता है।

साथ ही, $a * a = a$ और $b * a = b$ है। इसलिए, हम a को एक तत्समक e मान सकते हैं। इस प्रकार, $G2'$ भी संतुष्ट हो रहा है।

आगे, $a * a = a$ और $a * b = a$ है। अतः, $G3''$ संतुष्ट हो जाता है।

परंतु, समूह की परिभाषा के अनुसार $b * a = a$ भी होना चाहिए, जो सत्य नहीं है।

अतः, $(S, *)$ एक समूह नहीं है।

इसलिए, अभिगृहीतों की समतुल्यता के लिए ज़रूरी है कि **अभिगृहीतों के एक ही समुच्चय** के तीनों अभिगृहीत संतुष्ट होने चाहिए।

अब, आप जानते हैं कि G2 (या G2′) के कारण $(G, *)$ का एक तत्समक अवयव होता है। उदाहरणार्थ, $(\mathbb{Z}, +)$ का एक तत्समक अवयव 0 है। क्या $(\mathbb{Z}, +)$ का कोई अन्य तत्समक हो सकता है योग के सापेक्ष? हमारा अगला परिणाम इसी के बारे में है।

प्रमेय 2: मान लीजिए कि $(G, *)$ एक समूह है। तब, G का $*$ के सापेक्ष एक **अद्वितीय** तत्समक होता है, तथा G के प्रत्येक अवयव का $*$ के सापेक्ष एक **अद्वितीय** प्रतिलोम होता है।

उपपत्ति: मान लीजिए कि e और e', $*$ के सापेक्ष G के दो तत्समक हैं।

तब, क्योंकि e एक तत्समक है, इसलिए

$$e * e' = e'. \qquad \ldots(1)$$

क्योंकि e' एक तत्समक है, इसलिए

$$e * e' = e. \qquad \ldots(2)$$

(1) और (2) हमें बताते हैं कि $e = e'$.

इस प्रकार, G का $*$ के सापेक्ष एक अद्वितीय तत्समक e है।

अब मान लीजिए कि $a \in G$ तथा $*$ के सापेक्ष $b, c \in G$ इसके प्रतिलोम हैं। अतः,
$a * b = e = b * a$ और $a * c = e = c * a$.

तब, $b = b * e = b * (a * c)$

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

$= c.$

अतः, $*$ के सापेक्ष a का एक अद्वितीय प्रतिलोम है। ■

प्रमेय 2 के कारण, हम G का 'कोई एक तत्समक' के स्थान पर G का 'तत्समक' कह सकते हैं, तथा $a \in G$ के 'कोई एक प्रतिलोम' के स्थान पर a का 'प्रतिलोम' कह सकते हैं।

आइए अब प्रमेय 1 के प्रयोग के एक उदाहरण पर विचार करें।

उदाहरण 2: जाँच कीजिए कि $(\mathbb{M}_3(\mathbb{R}), +)$ एक समूह है या नहीं।

हल: सर्वप्रथम ध्यान दीजिए कि + के सापेक्ष $\mathbb{M}_3(\mathbb{R})$ **संवृत (closed)** है, अर्थात्, $\mathbb{M}_3(\mathbb{R})$ पर + एक द्वि-आधारी संक्रिया है, क्योंकि $A + B \in \mathbb{M}_3(\mathbb{R}) \ \forall\ A, B \in \mathbb{M}_3(\mathbb{R})$.

दूसरी ओर, भाग 1.4, इकाई 1 से, आप जानते हैं कि + साहचर्य है, यानी G1′ सत्य है।

तीसरे, किसी $A \in \mathbb{M}_3(\mathbb{R})$ के लिए, $A + \mathbf{0} = A$, जहाँ $\mathbf{0}$ वह 3×3 आव्यूह है जिसकी सभी प्रविष्टियाँ 0 हैं। इस प्रकार, G2′ सत्य है।

अंत में, $A = [a_{ij}] \in \mathbb{M}_3(\mathbb{R})$ दिया रहने पर, $\exists\ B = [-a_{ij}] \in \mathbb{M}_3(\mathbb{R})$ s.t. $A + B = \mathbf{0}.$
अतः, G3′ भी सत्य है।

इसलिए, प्रमेय 1 द्वारा, $(\mathbb{M}_3(\mathbb{R}), +)$ एक समूह है।

***

उदाहरण 2 में जैसा किया गया है, उसी तरह आप दर्शा सकते हैं कि **$(\mathbb{M}_n(\mathbb{R}), +)$ एक समूह है** $\forall$ **$n \in \mathbb{N}$**.

अब आप कुछ प्रश्नों को हल करने का प्रयास क्यों नहीं करते?

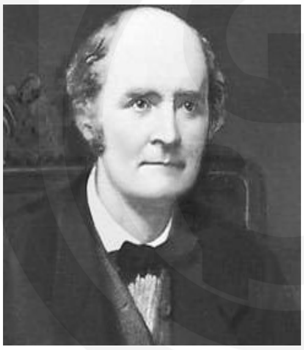
E3) जाँच कीजिए कि निम्नलिखित में से प्रत्येक एक समूह है या नहीं :

i) $(\mathbb{M}_{2\times 3}(\mathbb{C}), +)$, ii) $(\mathbb{M}_3(\mathbb{C}), \cdot)$, iii) $(\mathbb{Q}^*, \cdot)$, iv) $(\mathbb{Z}^*, \cdot)$.

E4) मान लीजिए कि $\mathbb{R}^+$ और $\mathbb{R}^-$ क्रमशः धनात्मक वास्तविक संख्याओं का समुच्चय और ऋणात्मक वास्तविक संख्याओं का समुच्चय व्यक्त करते हैं। जाँच कीजिए कि $(\mathbb{R}^+, \div)$ और $(\mathbb{R}^-, \cdot)$ समूह हैं या नहीं।

अभी तक आपने ऐसे समूहों G के उदाहरण देखें हैं जिनमें G अपरिमित है। तो क्या सभी समूहों में अंतर्निहित समुच्चय अपरिमित होते हैं? ऐसा नहीं है। हम अब समूहों के कुछ ऐसे उदाहरणों पर चर्चा करेंगे जिनमें अंतर्निहित समुच्चय परिमित होंगे। इसके लिए, आपको यह जानने की आवश्यकता होगी कि एक संक्रिया सारणी क्या होती है।

संक्रिया सारणी (Operation Table)



आकृति 1: आर्थर केली

मान लीजिए कि S एक परिमित समुच्चय है तथा S पर $*$ एक द्वि-आधारी संक्रिया है। हम इस द्वि-आधारी संक्रिया को एक वर्ग सारणी द्वारा निरूपित कर सकते हैं। इस सारणी को संक्रिया सारणी, या केली सारणी, कहते हैं। केली सारणी को प्रसिद्ध अंग्रेज़ गणितज्ञ आर्थर केली (1821-1895) का नाम दिया गया है। इन सारणियों को केली ने सर्वप्रथम 1854 में अपने एक शोध लेख में दिया था।

इस सारणी को लिखने के लिए, हम पहले S के अवयवों को **एक ही क्रम में** खड़े स्तंभ में तथा लेटी पंक्ति में लिखते हैं। फिर हम **शीर्षक a वाली पंक्ति** और **शीर्षक b वाले स्तंभ** के प्रतिच्छेदन पर सारणी में $a * b$ लिखते हैं। उदाहरणार्थ, यदि $S = \{-1, 0, 1\}$ है तथा द्वि-आधारी संक्रिया $\cdot$ द्वारा व्यक्त गुणन है, तो संक्रिया $\cdot$ को सारणी 1 द्वारा निरूपित किया जा सकता है।

सारणी 1

$\cdot$	-1	0	1
-1	$(-1)\cdot(-1)$ $=1$	$(-1)\cdot 0$ $=0$	$(-1)\cdot 1$ $=-1$
0	$0\cdot(-1)$ $=0$	$0\cdot 0$ $=0$	$0\cdot 1$ $=0$
1	$1\cdot(-1)$ $=-1$	$1\cdot 0$ $=0$	$1\cdot 1$ $=1$

विलोमतः, यदि हमें एक सारणी दी हुई है, तो हम S पर एक द्वि-आधारी संक्रिया को परिभाषित कर सकते हैं। उदाहरणार्थ, हम सारणी 2 द्वारा $S = \{1, 2, 3\}$ पर संक्रिया '$*$' को परिभाषित कर सकते हैं।

सारणी 2

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

सारणी 2 से, आप देख सकते हैं कि इसकी सभी प्रविष्टियाँ S से हैं। अतः, S पर $*$ एक द्वि-आधारी संक्रिया है।

आगे, यह सारणी हमें बताती है कि $1 * 2 = 2$ और $2 * 3 = 2$.

साथ ही, $2 * 1 = 3$ और $1 * 2 = 2$. इसलिए, $2 * 1 \neq 1 * 2$, अर्थात्, इस उदाहरण में $*$ क्रमविनिमेय नहीं है।

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

$\therefore (2 * 1) * 3 \neq 2 * (1 * 3)$. इसलिए, इस स्थिति में $*$ साहचर्य नहीं है। देखा आपने, एक सारणी हमें कितनी सूचना दे सकती है!

सारणी 2 में आपने देखा कि $*$ एक द्वि-आधारी संक्रिया है जो क्रमविनिमेय नहीं है। वास्तव में, एक संक्रिया सारणी को देखते ही आप निर्णय कर सकते हैं कि $*$ क्रमविनिमेय है या नहीं। आइए देखें कैसे $\{1, 2, 3\}$ पर एक द्वि-आधारी संक्रिया $*'$ के लिए, नीचे दी सारणी पर विचार कीजिए :

सारणी 3

$*'$	1	2	3
1	2	3	1
2	3	1	2
3	1	2	3

यदि आप सारणी 3 की प्रविष्टियों पर नज़र डालें तो आप देखेंगे कि ये प्रविष्टियाँ सारणी की ऊपरी बाईं प्रविष्टि से शुरू होती हुई सारणी की निचली दाईं प्रविष्टि तक के

विकर्ण, अर्थात् $\boxed{\begin{smallmatrix}2&&\\&1&\\&&3\end{smallmatrix}}$ के प्रति सममित हैं।

यह सममिति दर्शाती है कि $2 *' 1 = 1 *' 2$, $2 *' 3 = 3 *' 2$, इत्यादि।

अतः, यदि किसी संक्रिया सारणी में यह सममिति नहीं होगी, तो वह संक्रिया क्रमविनिमेय नहीं होगी। उदाहरणार्थ, यह सममिति सारणी 2 में नहीं दिखती।

अब, आप एक छोटे से प्रश्न को हल करने का प्रयास क्यों नहीं करते ?

E5) $S = \{0, 1, 2, 3\}$ पर संक्रिया $*$ के लिए निम्नलिखित सारणी को ऐसा पूरा कीजिए जिससे कि S पर $*$ संवृत हो तथा S पर $*$ क्रमविनिमेय हो :

$*$	0	1	2	3
0	0	1	2	3
1		2	3	
2			0	1
3		0		2

आइए अब कुछ परिमित समुच्चयों पर विचार करें तथा देखें कि क्या इन पर ऐसी संक्रियाएँ परिभाषित की जा सकती हैं जिनके सापेक्ष वे समूह बनें। निम्नलिखित उदाहरण पर दृष्टि डालिए।

उदाहरण 3 का समूह क्लाइन 4-समूह कहलाता है, जिसे गणितज्ञ फ़ीलिक्स क्लाइन (Felix Klein) के नाम पर रखा गया है।

उदाहरण 3: समुच्चय $G = \{a_1, a_2, a_3, a_4\}$ पर विचार कीजिए, जिस पर एक संक्रिया '·' नीचे दी गई केली सारणी द्वारा परिभाषित है :

सारणी 4

$\cdot$	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_1	a_4	a_3
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_3	a_2	a_1

जाँच कीजिए कि $(G, \cdot)$ एक समूह है या नहीं।

हल: सारणी 4 की प्रविष्टियों को देखने से हम निम्नलिखित सूचना प्राप्त करते हैं:

i) सभी प्रविष्टियाँ G में है। अतः, G पर $\cdot$ एक द्वि-आधारी संक्रिया है।

ii) $(a_1 \cdot a_2) \cdot a_3 = a_2 \cdot a_3 = a_4$, तथा

$a_1 \cdot (a_2 \cdot a_3) = a_1 \cdot a_4 = a_4$.

इस प्रकार, $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$.

इसी प्रकार, **आपको जाँच करनी चाहिए कि**

$(a_i \cdot a_j) \cdot a_k = a_i \cdot (a_j \cdot a_k) \; \forall \; i, j, k = 1, 2, 3, 4.$

इस प्रकार, $\cdot$ साहचर्य है।

iii) क्योंकि $a_1 \cdot a_i = a_i \; \forall \; i = 1, 2, 3, 4$, इसलिए $\cdot$ के सापेक्ष a_1 तत्समक अवयव है।

iv) क्योंकि $a_1 \cdot a_1 = a_1, a_2 \cdot a_2 = a_1, a_3 \cdot a_3 = a_1$ और $a_4 \cdot a_4 = a_1$, इसलिए G

के प्रत्येक अवयव का $\cdot$ के सापेक्ष एक प्रतिलोम है। वस्तुतः, यहाँ प्रत्येक अवयव, स्वयं अपना ही प्रतिलोम है।

अतः, $(G, \cdot)$ एक समूह है।

***

उदाहरण 3 की सारणी में, ध्यान दीजिए कि किसी भी पंक्ति या स्तंभ में कोई भी अवयव एक से ज़्यादा बार नहीं है। निम्नलिखित टिप्पणी इससे ही संबंधित है।

टिप्पणी 3: किसी भी समूह $(G, *)$ की संक्रिया की केली सारणी की किसी भी पंक्ति या स्तंभ में एक ही अवयव दोबारा नहीं हो सकता है। यह इस कारण है कि $a, b, c \in G$ के लिए, $a*b = a*c$ (a की संगत पंक्ति में) iff $b = c$, जैसा कि आप बाद में प्रमेय 3 में देखेंगे।

इसी प्रकार, $a*b = c*b$ (b के संगत स्तंभ में) iff $a = c$.

अब एक अन्य उदाहरण पर विचार कीजिए, जहाँ G परिमित है।

उदाहरण 4: मान लीजिए कि $G = \{\pm 1, \pm i\}$, $i = \sqrt{-1}$. जाँच कीजिए कि गुणन के सापेक्ष G एक समूह है या नहीं।

हल: G में गुणन के लिए केली सारणी निम्न है:

सारणी 5

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

यह सारणी दर्शाती है कि G पर $\cdot$ एक द्वि-आधारी संक्रिया है।

क्योंकि $\mathbb{C}$ में $\cdot$ साहचर्य है तथा $G \subseteq C$, इसलिए G में $\cdot$ साहचर्य है।

उपरोक्त सारणी हमें यह भी दिखाती है कि $a \cdot 1 = a \ \forall \ a \in G$. इसलिए, $\cdot$ के सापेक्ष 1 तत्समक अवयव है।

अंत में, क्योंकि 1 प्रत्येक पंक्ति में है, इसलिए यह सारणी दर्शाती है कि $G3'$ को $(G, \cdot)$ संतुष्ट करता है।

अतः, $(G, \cdot)$ एक समूह है।

***

उदाहरणों 3 और 4 से आप देख सकते हैं कि हम प्रमेय 1 के प्रयोग से किसी बीजीय निकाय को समूह सिद्ध करने के लिए की जाने वाली जाँच को कैसे कम कर सकते हैं।

अब इन दो उदाहरणों के बारे में एक टिप्पणी पर विचार कीजिए।

टिप्पणी 4: ध्यान दीजिए कि दोनों उदाहरण 3 और उदाहरण 4 के समूहों में 4 अवयव हैं। परंतु यदि आप उदाहरण 3 के a_1, a_2, a_3, a_4 को सारणी 4 में $1, -1, i, -i$ से किसी भी क्रम में प्रतिस्थापित करें; तो आप पाएँगे कि केली सारणियाँ समान नहीं होंगी। सारणी 4 से आप जानते हैं कि उदाहरण 3 में $a^2 = e \; \forall \; a \in G$. सारणी 5 यह दर्शाती है कि उदाहरण 4 में $i^2 \neq 1$. अतः, केली सारणियाँ अलग होंगी ही। इससे प्रदर्शित होता है कि दोनों समूहों के बीजीय बनावट अलग हैं।

अब, जैसा कि आप देख चुके हैं, किसी भी समूह का अंतर्निहित समुच्चय परिमित या अपरिमित हो सकता है। इस संदर्भ में, निम्नलिखित परिभाषाओं को देखिए।

परिभाषाएँ: मान लीजिए कि $(G, *)$ एक समूह है।

i) यदि G एक परिमित समुच्चय है, जिसमें n अवयव हैं, तो $(G, *)$ **कोटि n वाला परिमित समूह (finite group of order n)** कहलाता है। यहाँ हम $\mathbf{o(G) = n}$ लिखते हैं, जहाँ $o(G)$ 'समूह G की कोटि' को व्यक्त करता है।

ii) यदि G एक अपरिमित समुच्चय है, तो $(G, *)$ एक **अपरिमित समूह (infinite group)** कहलाता है।

iii) यदि G पर $*$ क्रमविनिमेय है, अर्थात् $a * b = b * a \; \forall \; a, b \in G$, तो $(G, *)$ को **क्रमविनिमेय समूह (commutative)**, या **आबेली समूह (abelian group)**, कहते हैं।

iv) यदि $(G, *)$ एक आबेली समूह नहीं है, तो वह एक **अन्आबेली (non-**abelian**) समूह** या एक **अक्रमविनिमेय (non-commutative) समूह** कहलाता है।

आकृति 2: आबेली समूह नॉर्वे के एक प्रतिभाशाली युवा गणितज्ञ नील्स हेनरीक आबल (1802-1829) के नाम पर रखा गया है।

इस प्रकार, उदाहरण 4 का समूह कोटि 4 वाला एक परिमित आबेली समूह है। उदाहरणों 1 और 2 के समूह अपरिमित आबेली समूह हैं।

अब, आइए अन्आबेली समूह के एक उदाहरण पर दृष्टि डालें।

यदि $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, तो $ad - bc$ को A का **सारणिक (determinant)** कहते हैं, और इसे **det A**, या $|\mathbf{A}|$, लिखते हैं।

उदाहरण 5: मान लीजिए कि G शून्येतर सारणिक वाले 2×2 आव्यूहों का समुच्चय है, अर्थात् $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \, a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$. दर्शाइए कि $(G, \cdot)$ एक अन्आबेली समूह है, जहाँ आव्यूह गुणन $\cdot$ है।

हल: पहले तो हम यह दर्शाएँगे कि $\cdot$ एक द्वि-आधारी संक्रिया है। भाग 1.4, इकाई 1, से आप जानते हैं कि यदि $A, B \in G$, तो $A \cdot B$ एक 2×2 आव्यूह होता है।

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

साथ ही, आप इसकी भी जाँच कर सकते हैं कि

$\det(A \cdot B) = (\det A) \cdot (\det B) \neq 0,$ क्योंकि $\det A \neq 0, \det B \neq 0.$

अतः, $A \cdot B \in G \;\; \forall A, B \in G.$

इकाई 1 से आप यह भी जानते हैं कि आव्यूह गुणन साहचर्य होता है तथा $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ गुणनात्मक तत्समक है। ध्यान दीजिए कि $\det(I) = 1$, और इसी लिए $I \in G$.

अब, G में $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ के लिए, आव्यूह $B = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$ ऐसा है कि

$\det B = \frac{1}{ad-bc} \neq 0$, तथा $AB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. इस प्रकार, $B = A^{-1}$.

इस प्रकार, $(G, \cdot)$ एक समूह है।

आगे, आइए देखें कि G अन्आबेली क्यों है। क्योंकि, उदाहरणार्थ,

$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$ तथा $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix}$, इसलिए हम देखते हैं कि

$(G, \cdot)$ क्रमविनिमेय नहीं है।

***

उदाहरण 5 में दिए अपरिमित अन्आबेली समूह को प्रायः $\mathbf{GL_2(\mathbb{R})}$ द्वारा व्यक्त किया जाता है, तथा इसे $\mathbb{R}$ पर **कोटि 2 वाला व्यापक रैखिक समूह (general linear group of degree 2)** कहा जाता है। हम उदाहरणों के लिए इस समूह का प्रयोग इस पाठ्यक्रम में अनेक बार करते रहेंगे।

अब, आइए फलनों से संबंधित एक उदाहरण पर विचार करें।

उदाहरण 6: $\mathbb{R}$ से $\mathbb{R}$ तक के सभी फलनों के समुच्चय $\mathcal{F}$ पर विचार कीजिए। जाँच कीजिए कि बिंदुशः योग (pointwise addition), अर्थात्
$f_1, f_2 \in \mathcal{F}$ के लिए, $(f_1 + f_2) : \mathbb{R} \to \mathbb{R} : (f_1 + f_2)(x) = f_1(x) + f_2(x) \ \forall \ x \in \mathbb{R}$, के सापेक्ष $\mathcal{F}$ एक समूह है या नहीं।

हल: सर्वप्रथम, $I \in \mathcal{F}$, जहाँ $I : \mathbb{R} \to \mathbb{R} : I(x) = x$. अतः, $\mathcal{F} \neq \emptyset$.

आगे, $f_1, f_2 \in \mathcal{F}$ के लिए, $f_1 + f_2$ भी $\mathbb{R}$ से $\mathbb{R}$ तक एक फलन है। इसलिए, $\mathcal{F}$ पर + एक द्वि-आधारी संक्रिया है।

तीसरे, $f_1, f_2, f_3 \in \mathcal{F}$ और $r \in \mathbb{R}$ के लिए,

$$[(f_1 + f_2) + f_3](r) = (f_1 + f_2)(r) + f_3(r)$$

$$= (f_1(r) + f_2(r)) + f_3(r) = f_1(r) + (f_2(r) + f_3(r))$$

$$= [f_1 + (f_2 + f_3)](r).$$

अतः, $\mathcal{F}$ में + साहचर्य है।

चौथी बात, $\mathcal{F}$ में $\mathbf{0}$ योज्य तत्समक है, जहाँ $\mathbf{0}:\mathbb{R}\to\mathbb{R}:\mathbf{0}(x)=0$.

अंत में, $f\in\mathcal{F}$ दिया रहने पर, $\exists -f\in\mathcal{F}$, जहाँ $(-f):\mathbb{R}\to\mathbb{R}:(-f)(x)=-f(x)$. तब, $f+(-f)=\mathbf{0}$.

अतः, $(\mathcal{F},+)$ एक समूह होने के लिए सभी अभिगृहीतों को संतुष्ट करता है।

ध्यान दीजिए कि $\mathcal{F}$ एक आबेली समूह है, क्योंकि $f_1+f_2=f_2+f_1\ \forall\ f_1, f_2\in\mathcal{F}$.

***

अब आबेली समूह के एक अन्य उदाहरण पर विचार कीजिए।

उदाहरण 7: $\mathbb{R}^2$ के सभी स्थानांतरणों के समुच्चय T, अर्थात्,
$T=\{f_{a,b}:\mathbb{R}^2\to\mathbb{R}^2 \mid f_{a,b}(x,\ y)=(x+a,\ y+b)$, किन्हीं $a,\ b\in\mathbb{R}$ के लिए$\}$ पर विचार कीजिए। ध्यान दीजिए कि T के प्रत्येक अवयव $f_{a,b}$ का $\mathbb{R}^2$ में निरूपण है बिंदु (a, b). दर्शाइए कि फलनों के संयोजन के सापेक्ष T एक आबेली समूह है।

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

$a,b,c,d\in\mathbb{R}$ और $(x,\ y)\in\mathbb{R}^2$ के लिए,

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

$$=(x+a+c,\ y+b+d),\text{ क्योंकि } \mathbb{R} \text{ में + क्रमविनिमेय है।}$$

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

$$\therefore\ f_{a,b}\circ f_{c,d}=f_{a+c,\ b+d}\in T. \qquad \ldots(3)$$

क्योंकि $a+c\in\mathbb{R}$ और $b+d\in\mathbb{R}$, इसलिए $f_{a,b}\circ f_{c,d}\in T$.

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

आगे, $f_{a,b}\circ f_{0,0}=f_{a,b}\in T$, (3) के उपयोग से।

अतः, $\circ$ के सापेक्ष $f_{0,0}$ तत्समक अवयव है।

साथ ही, $f_{a,b}\in T$ के लिए, $f_{a,b}\circ f_{-a,-b}=f_{0,0}$, (3) के उपयोग से।

अतः, $\circ$ के सापेक्ष $f_{-a,-b}$ का प्रतिलोम है $f_{a,b}\in T$.

इस प्रकार, $(T,\circ)$ अभिगृहीतों $G1'$, $G2'$ और $G3'$ को संतुष्ट करता है। इसी कारण से यह एक समूह है।

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

***

अब निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E6) निम्नलिखित में से कौन-से कथन सत्य हैं? अपने उत्तरों के लिए कारण दीजिए।

i) $(\mathbb{C}^*, \cdot)$ एक आबेली समूह है।

ii) $(\mathbb{R}^*, \cdot)$ एक परिमित समूह है।

iii) $(\mathbb{Z}_O, +)$ एक समूह है, जहाँ $\mathbb{Z}_O$ विषम पूर्णांकों का समुच्चय है।

iv) $(\mathbb{Q}, \cdot)$ एक सामिसमूह है।

v) $(\mathbb{Q}^+, *)$ एक समूह है, जहाँ $\mathbb{Q}^+$ धनात्मक परिमेय संख्याओं का समुच्चय है, तथा $*$, $\mathbb{Q}^+ \times \mathbb{Q}^+$ पर $a * b = 2ab$ द्वारा परिभाषित है।

E7) दर्शाइए कि $(G, *)$ एक अन्आबेली समूह है, जहाँ $G = \{(a, b) | a, b \in \mathbb{R}, a \neq 0\}$ तथा $*$, $G \times G$ पर $(a, b) * (c, d) = (ac, bc + d)$ द्वारा परिभाषित है।

E8) किसी परिमित समुच्चय G पर एक द्वि-आधारी संक्रिया $*$ की सारणी का एक उदाहरण दीजिए, जो यह दर्शाती है कि $(G, *)$ एक समूह नहीं हो सकता। अपने उदाहरण की पुष्टि कीजिए।

अब हम कुछ ऐसे मौलिक गुणों पर दृष्टि डालेंगे जो किसी भी समूह के अवयव संतुष्ट करते हैं।

2.3 समूहों के प्रारंभिक गुण

इस भाग में हम एक समूह के अवयवों के कुछ प्रारंभिक गुणों की चर्चा करेंगे। परंतु पहले हम संकेतन की प्रथा का उल्लेख करेंगे।

टिप्पणी 5: आगे से, अपनी सुविधा के लिए, **हम समूह** $(G, *)$ को **केवल** G से **व्यक्त करेंगे,** यदि संबंधित संक्रिया के बारे में कोई भ्रम नहीं हो तो। और हम $a, b \in G$ के लिए, **$a * b$ को ab से व्यक्त करेंगे,** तथा कहेंगे कि हम **a और b का गुणा कर रहे हैं।**

और अंत में, हम **समूह के तत्समक को e द्वारा**, और **$a \in G$ के प्रतिलोम को a^{-1} से, व्यक्त करेंगे।**

अब, आइए समूह के कुछ सरल गुणों पर विचार करें। आप जानते हैं कि $\mathbb{R}^*$ के a, b, c के लिए, जब भी $ba = ca$ या $ab = ac$, तो हम निष्कर्ष निकाल सकते हैं कि $b = c$, अर्थात् हम a का **निरसन** (cancel) **कर** सकते हैं। यह बात किसी भी समूह के लिए सत्य होती है आप अब देखेंगे।

प्रमेय 3: किसी समूह G में a, b, c के लिए,

i) $ab = ac \Rightarrow b = c$. (इसे **वाम निरसन नियम (left cancellation law)** कहा जाता है।)

ii) $ba = ca \Rightarrow b = c$. (इसे **दक्षिण निरसन नियम (right cancellation law)** कहा जाता है।)

उपपत्ति: यहाँ हम केवल (i) को सिद्ध करेंगे, तथा (ii) की उपपत्ति आप पर छोड़ देंगे (E9 देखिए)।

i) मान लीजिए कि $ab = ac$. ...(4)

अब, G3 द्वारा $\exists\, d \in G$ s.t. $da = e$. (4) के दोनों पक्षों को बाईं ओर d से गुणा करने पर, $d(ab) = d(ac)$ प्राप्त करते हैं।

$\Rightarrow \quad (da)b = (da)c$, G1 के उपयोग से।

$\Rightarrow \quad eb = ec$

$\Rightarrow \quad b = c$.

याद रखिए कि गुणा करने से हमारा मतलब है कि हम संक्रिया $*$ लागू कर रहे हैं, जिसके सापेक्ष G एक समूह है। ■

आगे बढ़ने से पहले, एक क्षण के लिए टिप्पणी 3 पर वापस जाइए। आपको देखना चाहिए कि वहाँ जो नोट किया गया है, उसे यहाँ प्रमेय 3 किस तरह दर्शा रहा है।

आइए अब आगे बढ़ें। $\mathbb{Z}$ के किसी अवयव n पर विचार कीजिए। आप जानते हैं कि $-(-n) = n$. आप यह भी जानते हैं कि $m, n \in \mathbb{Z}$ के लिए, $-(m+n) = (-m) + (-n)$.

इसी प्रकार, $2 \in \mathbb{Q}$ के लिए आप जानते हैं कि $(2^{-1})^{-1} = 2$.

अधिक व्यापक रूप में, किसी भी समूह के अवयव के प्रतिलोम के निम्नलिखित गुणों पर विचार कीजिए।

प्रमेय 4: मान लीजिए कि G एक समूह है। तब,

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

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

उपपत्ति: i) $a \in G$ के लिए, $a^{-1} \in G$. मान लीजिए कि $(a^{-1})^{-1} = b$. तब, प्रतिलोम की परिभाषा के अनुसार,

$$b(a^{-1}) = e = (a^{-1})b. \quad \ldots(5)$$

परंतु, परिभाषा द्वारा,

$$a\,a^{-1} = a^{-1}a = e. \quad \ldots(6)$$

क्योंकि अवयव का प्रतिलोम अद्वितीय होता है (प्रमेय 2), इसलिए हम (5) और (6) से देखते हैं कि $b = a$, अर्थात्, $(a^{-1})^{-1} = a$.

ii) $a, b \in G$ के लिए, $ab \in G$. अतः, $(ab)^{-1} \in G$ ऐसा है कि

$$(ab)(ab)^{-1} = e. \qquad \ldots(7)$$

परंतु, $(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1}$, G1 द्वारा।

$= (a(bb^{-1})a^{-1})$, G1 द्वारा।

$= (ae)a^{-1}$, क्योंकि $bb^{-1} = e$.

$= aa^{-1}$, क्योंकि $ae = a$.

$= e$, क्योंकि $aa^{-1} = e$.

इस प्रकार, $(ab)(b^{-1}a^{-1}) = e. \qquad \ldots(8)$

इसलिए, (7) और (8) से, तथा प्रतिलोम की अद्वितीयता को देखते हुए हम $(ab)^{-1} = b^{-1}a^{-1}$ प्राप्त करते हैं। ■

ध्यान दीजिए कि किसी समूह G के लिए, $(ab)^{-1} = a^{-1}b^{-1} \ \forall \ a, b \in G$ **केवल तभी होता** है जब G आबेली हो। जैसे कि निम्नलिखित उदाहरण में ऐसा नहीं है।

उदाहरण 8: दर्शाइए कि किसी $A, B \in GL_2(\mathbb{R})$ के लिए, $A^{-1}B^{-1} \neq (AB)^{-1}$ (देखिए उदाहरण 5)।

हल: $A = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$ और $B = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ पर विचार कीजिए।

तब, $AB = \begin{bmatrix} 1 & 2 \\ -1 & 0 \end{bmatrix}$.

साथ ही, $A^{-1} = \begin{bmatrix} 1/2 & -1/2 \\ 0 & 1 \end{bmatrix}$ और $B^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$. इसलिए, $A^{-1}B^{-1} = \begin{bmatrix} -1/2 & -1 \\ 1 & 1 \end{bmatrix}$.

इस प्रकार, $(AB)(A^{-1}B^{-1}) = \begin{bmatrix} 3/2 & 1 \\ 1/2 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

अतः, $A^{-1}B^{-1} \neq (AB)^{-1}$.

***

अब कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E9) प्रमेय 3 के भाग (ii) को सिद्ध कीजिए।

E10) मान लीजिए कि $*$ के सापेक्ष $G = \{a_1, a_2, a_3\}$ एक क्रमविनिमेय समूह है। नीचे दी हुई केली सारणी को पूरा कीजिए।

$*$	a_1	a_2	a_3
a_1			
a_2		a_3	a_1
a_3			

E11) यदि किसी समूह G में एक ऐसा अवयव g है कि सभी $x \in G$ के लिए $gx = g$, तो दर्शाइए कि $G = \{e\}$.

E12) किसी समूह G में a, b, c के लिए, $ab = bc \Rightarrow a = c$. क्या यह सत्य है या असत्य है? अपने उत्तर के कारण दीजिए।

E13) मान लीजिए कि $a_1, a_2, \ldots, a_n$ एक समूह G के अवयव हैं। $(a_1 a_2 \ldots a_n)^{-1}$ ज्ञात कीजिए।

E14) मान लीजिए कि किसी समूह G में प्रत्येक x के लिए, $x^2 = x$. दर्शाइए कि G आबेली है। क्या इसका विलोम सत्य है? क्यों, या क्यों नहीं?

E15) मान लीजिए कि किसी समूह G में प्रत्येक x के लिए, $x^2 = e$ है। दर्शाइए कि G आबेली है। क्या इसका विलोम सत्य है?

आइए अब समूहों के एक और गुण को सिद्ध करें।

प्रमेय 5: समूह G में अवयवों a, b के लिए, समीकरणों $ax = b$ और $ya = b$ के G में अद्वितीय हल होते हैं।

उपपत्ति: पहले आप यह देखेंगे कि G में $ax = b$ का एक हल क्यों है, तथा फिर आप देखेंगे कि यह हल अद्वितीय क्यों है।

$a, b \in G$ के लिए, $a^{-1}b \in G$ पर विचार कीजिए।

तब, $a(a^{-1}b) = (aa^{-1})b = eb = b.$

इस प्रकार, $a^{-1}b$ समीकरण $ax = b$ को संतुष्ट करता है, अर्थात् $ax = b$ का G में एक हल है।

आगे, अद्वितीयता को देखने के लिए, मान लीजिए कि G में $ax = b$ के दो हल x_1, x_2 हैं। तब, $ax_1 = b = ax_2$. वाम निरसन नियम द्वारा, हम $x_1 = x_2$ प्राप्त करते हैं।

इस प्रकार, $a^{-1}b$ ही G में अद्वितीय हल है।

इसी प्रकार, दक्षिण निरसन नियम का उपयोग करते हुए, आपको सिद्ध करना चाहिए कि G में $ya = b$ का अद्वितीय हल ba^{-1} है। ■

आइए देखें कि प्रमेय 5 हमें कुछ विशिष्ट स्थितियों में क्या बताता है।

उदाहरण 9: $GL_2(\mathbb{R})$ में $A=\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix}$ और $B=\begin{bmatrix}1 & 5\\0 & 4\end{bmatrix}$ पर विचार कीजिए। ऐसे X और Y ज्ञात कीजिए जिनसे कि $AX = B$ और $YA = B$.

हल: प्रमेय 5 से आप जानते हैं कि $X = A^{-1}B$. अब,

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

$$\therefore A^{-1}B=\begin{bmatrix}2 & -3\\-1 & 2\end{bmatrix}\begin{bmatrix}1 & 5\\0 & 4\end{bmatrix}=\begin{bmatrix}2 & -2\\-1 & 3\end{bmatrix}=X.$$

सत्यापन कीजिए कि इस X के लिए $AX = B$ है।

इसी प्रकार, आपको $Y = BA^{-1}$ ज्ञात करना चाहिए।

***

अगले उदाहरण में हम एक असाधारण समूह पर विचार करेंगे।

उदाहरण 10: मान लीजिए कि S एक अरिक्त समुच्चय है। $\wp(S)$ पर विचार कीजिए, जो S के सभी उपसमुच्चयों का समुच्चय है। इस पर $A \Delta B = (A \setminus B) \cup (B \setminus A)\ \forall\ A, B \in \wp(S)$ द्वारा परिभाषित **सममित अंतर Δ** एक द्वि-आधारी संक्रिया है।

आप कलन की इकाई 2 से, $\wp(S)$ से परिचित होंगे।

जाँच कीजिए कि क्या $(\wp(S), \Delta)$ और $(\wp(S), \cap)$ समूह हैं या नहीं। यदि हैं, तो क्या वे आबेली समूह हैं?

आगे, क्या समीकरणों $Y \Delta A = B$ और $Y \cap A = B\ \forall\ A, B \in \wp(S)$ के अद्वितीय हल हैं? क्यों, या क्यों नहीं?

हल: आइए पहले $(\wp(S), \Delta)$ पर विचार करें। $\wp(S)$ पर Δ एक साहचर्य द्वि-आधारी संक्रिया है। आप इसकी जाँच कलन के खंड 1 में आपके द्वारा अध्ययन की गई समुच्चय संक्रियाओं के गुणों का उपयोग करते हुए कर सकते हैं। ये गुण हैं :

$$A \setminus B = A \cap B^c,\ (A \cap B)^c = A^c \cup B^c,\ (A \cup B)^c = A^c \cap B^c\ \forall\ A, B \in \wp(S),$$

तथा $\cup$ और $\cap$ क्रमविनिमेय और साहचर्य हैं।

Δ क्रमविनिमेय भी है, क्योंकि

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B)$$

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

यहाँ Δ के सापेक्ष $\emptyset$ तत्समक अवयव है, क्योंकि $A \Delta \emptyset = A\ \forall\ A \in \wp(S)$.

आगे, कोई भी अवयव स्वयं अपना प्रतिलोम है क्योंकि $A \Delta A = \emptyset\ \forall\ A \in \wp(S)$.

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

अब, आइए $(\wp(S), \cap)$ पर विचार करें। जैसा कि आप जानते हैं, $\wp(S)$ पर $\cap$ एक साहचर्य द्वि-आधारी संक्रिया है। साथ ही, $A \cap S = A\ \forall\ A \in \wp(S)$, जिससे कि $\cap$ के सापेक्ष S तत्समक अवयव है। परंतु, S का एक उचित उपसमुच्चय दिया रहने पर, ऐसा कोई $B \in \wp(S)$ नहीं है जिससे कि $A \cap B = S$ हो।

इस प्रकार, $(\wp(S), \cap)$ एक समूह नहीं है।

ध्यान दीजिए कि किसी भी $A \in \wp(S), A \neq S$ के लिए, $Y \cap A = S$ का कोई हल नहीं है।

$(\wp(S), \Delta)$ में A, B के लिए, हम $Y \Delta A = B$ को हल करना चाहते हैं। परंतु, हम जानते हैं कि A स्वयं अपना प्रतिलोम है। अतः, प्रमेय 5 द्वारा, $Y = B \Delta A^{-1} = B \Delta A$ अद्वितीय हल है।

हमने यहाँ यह भी सिद्ध कर दिया है कि $\wp(S)$ में किन्हीं A, B के लिए, $(B \Delta A) \Delta A = B$.

***

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E16) क्या $(\mathbb{Z}, -)$ एक समूह है? क्या आप $a - x = b,\ \forall\ a, b \in \mathbb{Z}$ के लिए एक अद्वितीय हल प्राप्त कर सकते हैं? इससे आप प्रमेय 5 के विलोम के बारे में क्या निष्कर्ष निकाल सकते हैं?

E17) यदि G एक सामिसमूह है, परंतु एक समूह नहीं है, तो क्या सभी $a, b \in G$ के लिए, $ax = b$ का एक हल होगा? क्यों, या क्यों नहीं?

और अब आइए चर्चा करें समूह के किसी अवयव की स्वयं पर संक्रिया लागू करने की। उदाहरणार्थ, $n \in (\mathbb{Z}, +)$ पर विचार कीजिए। तब, $n + n = 2n, (n + n) + n = 3n$, इत्यादि।

इसी प्रकार, n के प्रतिलोम, अर्थात् $-n$ पर बार-बार जोड़ की संक्रिया लागू करने से $(-n) + (-n) = 2(-n), [(-n) + (-n)] + (-n) = 3(-n)$, इत्यादि। इस संदर्भ में, निम्नलिखित परिभाषा पर विचार कीजिए :

परिभाषा: मान लीजिए G एक समूह है। $a \in G$ और $\mathbf{n} \in \mathbb{Z}$ के लिए, हम $\mathbf{a^n}$ को निम्न तरीक़े से परिभाषित करते हैं :

i) $a^0 = e$.

ii) $a^n = a^{n-1} \cdot a$, यदि $n > 0$.

iii) $a^n = (a^{-1})^{(-n)}$, यदि $n < 0$.

यहाँ a की **पूर्णांकीय घात (integral power)** a^n है, और n इसका **घातांक (exponent,** or **index)** कहलाता है।

इस प्रकार, परिभाषा से, $a^1 = a, a^2 = a \cdot a, a^3 = a^2 \cdot a$, इत्यादि, तथा

$a^{-2} = (a^{-1})^2, a^{-3} = (a^{-1})^3,$ इत्यादि।

टिप्पणी 6: जब द्वि-आधारी संक्रिया योग है, तब a^n, na हो जाता है। उदाहरणार्थ, किसी $a \in \mathbb{Z}$ के लिए, उपरोक्त परिभाषा कहती है कि

i) $na = 0$, यदि $n = 0$;

ii) $na = a + a + \cdots + a$(n बार), यदि $n > 0$;

iii) $na = (-a) + (-a) + \cdots + (-a)$ ($-n$ बार), यदि $n < 0$.

आइए अब हम समूह के अवयवों के लिए, कुछ घातांक नियमों को सिद्ध करें।

प्रमेय 6: मान लीजिए कि G एक समूह है। $a \in G$ तथा $m, n \in \mathbb{Z}$ के लिए,

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

ii) $a^m \cdot a^n = a^{m+n}$,

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

उपपत्ति: हम (i) और (ii) को सिद्ध करेंगे, तथा (iii) की उपपत्ति आपके लिए छोड़ेंगे (E18 को देखिए)।

i) यदि $n = 0$, तो $(a^n)^{-1} = (a^0)^{-1} = e^{-1} = e$; $a^{-n} = a^0 = e$; तथा $(a^{-1})^n = (a^{-1})^0 = e$.

अतः, इस स्थिति में, (i) सत्य है।

अब, मान लीजिए कि $n > 0$ है। क्योंकि $aa^{-1} = e$, इसलिए हम देखते हैं कि

$$e = e^n = (aa^{-1})^n$$

$$= (aa^{-1})(aa^{-1})\ldots(aa^{-1}) \text{ (n बार)}$$

$$= a^n(a^{-1})^n, \text{ क्योंकि } a \text{ और } a^{-1} \text{ क्रमविनिमेय करते हैं।}$$

$$\therefore (a^n)^{-1} = (a^{-1})^n.$$

साथ ही, $(a^{-1})^n = a^{-n}$, परिभाषा के (iii) द्वारा क्योंकि $(-n) < 0$.

$$\therefore (a^n)^{-1} = (a^{-1})^n = a^{-n}, \text{ जब } n > 0.$$

यदि $n < 0$, तो $(-n) > 0$ तथा

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

$$= [(a^{-n})^{-1}]^{-1}, n > 0 \text{ की स्थिति से।}$$

$= a^{-n}$, क्योंकि $(x^{-1})^{-1} = x \;\forall\; x \in G.$

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

$= [(a^{-1})^{-1}]^{-n}$, $n > 0$ की स्थिति से।

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

अतः, इस स्थिति में भी

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

ii) पहले मान लीजिए कि $m = 0$. तब, $m + n = n$. अतः,

$a^{m+n} = a^{n} = a^{0} \cdot a^{n}$, क्योंकि $a^{0} = e.$

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

इसी प्रकार, यदि $n = 0$, तो $a^{m+n} = a^{m} \cdot a^{n}.$

अब, मान लीजिए कि $m \neq 0$ और $n \neq 0$. तब 4 स्थितियां हो सकती हैं।

स्थिति 1 ($m > 0$ और $n > 0$) : आइए इस स्थिति में परिणाम को n पर आगमन द्वारा सिद्ध करें।

मान लीजिए $P(n)$ यह विधेय है कि $a^{m} \cdot a^{n} = a^{m+n}$, जहाँ m दिया हुआ है।

यदि $n = 1$, तो $a^{m} \cdot a = a^{m+1}$, परिभाषा द्वारा।

इस प्रकार, $P(1)$ एक सत्य कथन है।

अब, परिकल्पना कीजिए कि $P(k)$ सत्य है, अर्थात् किसी $k \geq 1$ के लिए, $a^{m} \cdot a^{k} = a^{m+k}$.

तब, $a^{m} \cdot a^{k+1} = a^{m}(a^{k} \cdot a) = (a^{m} \cdot a^{k})a = a^{m+k} \cdot a$, क्योंकि $P(k)$ सत्य है।

$= a^{m+(k+1)}.$

इस प्रकार, $P(k+1)$ सत्य है।

अतः, आगमन नियम द्वारा, सभी $m > 0$ और $n > 0$ के लिए, (i) सत्य है।

स्थिति 2 ($m < 0$ और $n < 0$) : यहाँ $(-m) > 0$ और $(-n) > 0$ है। इस प्रकार, स्थिति 1 द्वारा, $a^{-n} \cdot a^{-m} = a^{-(n+m)} = a^{-(m+n)}$.

दोनों पक्षों के प्रतिलोमों को लेकर, तथा (i) का उपयोग करते हुए, हम प्राप्त करते हैं कि

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

स्थिति 3 ($m > 0, n < 0$ ताकि $m + n \geq 0$) : यहाँ $(-n) > 0$ है। अतः, स्थिति 1 द्वारा, $a^{m+n} \cdot a^{-n} = a^m$.

इसके दोनों पक्षों को दाईं तरफ़ $a^n = (a^{-n})^{-1}$ से गुणा करने पर, तथा (i) द्वारा, हम प्राप्त करते हैं कि

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

स्थिति 4 ($m > 0, n < 0$ ताकि $m + n < 0$): स्थिति 2 से, $a^{-m} \cdot a^{m+n} = a^n$. दोनों पक्षों को बाईं तरफ़ $a^m = (a^{-m})^{-1}$ से गुणा करने पर, हम प्राप्त करते हैं कि $a^{m+n} = a^m \cdot a^n$.

जैसा कि स्थितियों 3 और 4 में किया गया है, उसी प्रकार आप उन स्थितियों के लिए परिणाम को सिद्ध कीजिए, जब $m < 0$ और $n > 0$.

अतः, सभी $a \in G$ और $m, n \in \mathbb{Z}$ के लिए, $a^{m+n} = a^m \cdot a^n$.

आप E18 को हल कर लेंगे, तब प्रमेय 6 की उपपत्ति पूरी हो जाएगी। ■

आप प्रमेय 6 का अनुप्रयोग इस पाठ्यक्रम के अध्ययन में बहुत बार करते रहेंगे। आइए देखें कि एक विशिष्ट स्थिति में यह क्या बताता है।

उदाहरण 11: मान लीजिए कि $A \in \wp(S)$, जहाँ $S \neq \emptyset$. $n \in \mathbb{Z}$ A^n $\forall$ मालूम कीजिए।

हल: यहाँ संक्रिया Δ है। साथ ही, आप जानते हैं कि $A^2 = A \Delta A = \emptyset$.

इसलिए, $A^{-1} = A$.

अब, यदि $n = 2m$, जहाँ $m \in \mathbb{Z}$, तो $A^n = (A^2)^m = \emptyset^m = \emptyset$.

यदि $n = 2m + 1$, जहाँ $m \in \mathbb{Z}$, तो $A^n = A^{2m} \Delta A = \emptyset \Delta A = A$.

इस प्रकार, $A^n = \emptyset$ या A, जो इस बात पर निर्भर है कि n सम है या विषम।

***

अब निम्नलिखित प्रश्नों को हल कीजिए।

E18) प्रमेय 6 (iii) को सिद्ध कीजिए।

(**संकेत:** स्थिति $n > 0$ के लिए, n पर आगमन द्वारा सिद्ध कीजिए। इसके बाद $n < 0$ के लिए सिद्ध कीजिए।)

E19) मान लीजिए कि G एक आबेली समूह है। सिद्ध कीजिए कि

i) $ab^m = b^m a \ \forall \ m \in \mathbb{Z}$ तथा $\forall \ a, b \in G$;

ii) $(ab)^m = a^m b^m \ \forall \ m \in \mathbb{Z}$.

अब हम कुछ समूहों की चर्चा विस्तृत रूप से करेंगे। आप इन समूहों के साथ इस पाठ्यक्रम में कार्य करते रहेंगे।

2.4 कुछ महत्वपूर्ण समूह

इस भाग में, हम आपका परिचय एक-एक करके छः प्रकार के समूहों से कराएँगे। इनका अध्ययन सावधानीपूर्वक कीजिए, क्योंकि हम इस पाठ्यक्रम में इनका उपयोग अनेक बार उदाहरणों (और प्रतिउदाहरणों!) के रूप में करते रहेंगे। इन समूहों के प्रकार हैं : पूर्णांक मोड्यूलो n का समूह, सममित समूह, द्वितल समूह, आव्यूह समूह, एक के nवें मूलों का समूह $(n \in \mathbb{Z})$ तथा समूहों का अनुलोम गुणनफल।

2.4.1 पूर्णांक मोड्यूलो n

पूर्णांकों के समुच्चय $\mathbb{Z}$ तथा $n \in \mathbb{N}$ को लीजिए। इकाई 1 में आपने पढ़ा था कि 'समशेषता मॉड्यूलो n' का संबंध (अर्थात्, 'aRb iff n, $a-b$ को विभाजित करता है') द्वारा दिए जाने वाला संबंध R एक तुल्यता संबंध है। इस प्रकार, इकाई 1 से आप जानते हैं कि यह $\mathbb{Z}$ का असंयुक्त तुल्यता वर्गों में विभाजन करता है। ये वर्ग **समशेषता वर्ग मॉड्यूलो n** कहलाते हैं। हम r को अंतर्विष्ट करने वाले तुल्यता वर्ग को $\bar{r}$ या $[r]$ से व्यक्त करते हैं।

इस प्रकार, $\mathbf{\bar{r} = \{m \in \mathbb{Z} \mid m \equiv r \,(mod\, n)\}}$.

अतः, पूर्णांक m $\bar{r}$ में सम्मिलित होता है किसी r के लिए, जहाँ $0 \le r < n$, iff $m \equiv r (\text{mod}\, n)$, अर्थात् iff $n \mid (m-r)$, अर्थात् iff किसी $k \in \mathbb{Z}$ के लिए $m - r = kn$.

$\therefore\ \mathbf{\bar{r} = \{r + kn \mid k \in \mathbb{Z}\}}$.

आपने इकाई 1 में, यह भी देखा था कि $\mathbb{Z}$ के सभी समशेषता वर्ग मॉड्यूलो n क्रमशः $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ हैं।

ध्यान दीजिए कि $\forall\ i \in \mathbb{Z}$, $\bar{i}$ समुच्चय $\mathbb{Z}$ का एक उपसमुच्चय है, $\mathbb{Z}$ का एक अवयव नहीं।

आगे, $\mathbb{Z} = \bigcup_{i=0}^{n-1} \bar{i}$ (एक असंयुक्त सम्मिलन)

मान लीजिए कि $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$. हम

$\bar{a} + \bar{b} = \overline{a+b}$

द्वारा $\mathbb{Z}_n$ पर संक्रिया '+' को परिभाषित करते हैं।

क्या यह संक्रिया सुपरिभाषित है? इस प्रश्न का उत्तर देने के लिए, हमें देखना होगा कि क्या $\mathbb{Z}_n$ में $\bar{a} = \bar{b}$ और $\bar{c} = \bar{d}$ से $\overline{a+c} = \overline{b+d}$ मिलता है या नहीं।

अब, $a \equiv b (\text{mod}\, n)$ तथा $c \equiv d (\text{mod}\, n)$. इसलिए ऐसे पूर्णांक k_1 और k_2 हैं जिनसे कि कि $a - b = k_1 n$ और $c - d = k_2 n$. परंतु, तब

$(a + c) - (b + d) = (a - b) + (c - d) = (k_1 + k_2)n.$

$\therefore\ \overline{a+c} = \overline{b+d}.$

इस प्रकार, $\mathbb{Z}_n$ में '+' एक सुपरिभाषित द्वि-आधारी संक्रिया है।

ध्यान दीजिए कि किन्हीं $r = 0,\ldots,n-1$ के लिए, $\overline{a+c} = \bar{r}$, क्योंकि $a + c \in \mathbb{Z} = \bigcup_{i=0}^{n-1} \bar{i}.$

उदाहरणार्थ, $\mathbb{Z}_4$ में $\bar{2}+\bar{3}=\bar{5}=\bar{1}$, क्योंकि $2+3=5$ और $5 \equiv 1 (\text{mod}\, 4)$.

साथ ही, $\mathbb{Z}_{11}$ में $\bar{7}-\overline{10}=\overline{-3}=\bar{8}$, क्योंकि $\bar{8}+\bar{3}=\overline{11}=\bar{0}$.

$\mathbb{Z}_n$ में योग की अपनी समझ को बेहतर करने के लिए, निम्नलिखित प्रश्न को हल कीजिए।

E20) $\mathbb{Z}_5$ पर + के लिए निम्नलिखित संक्रिया सारणी में रिक्त स्थानों को भरिए :

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$					
$\bar{1}$					
$\bar{2}$					
$\bar{3}$					
$\bar{4}$					

अब आइए दर्शाएँ कि $(\mathbb{Z}_n, +)$, $n \in \mathbb{N}$ के लिए, एक क्रमविनिमेय समूह है।

i) $\bar{a}+(\bar{b}+\bar{c}) = \bar{a}+(\overline{b+c}) = \overline{a+(b+c)} = \overline{(a+b)+c} = (\overline{a+b})+\bar{c}$

$= (\bar{a}+\bar{b})+\bar{c}\ \forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, अर्थात् $\mathbb{Z}_n$ में योग साहचर्य है।

ii) $\bar{a}+\bar{0}=\bar{a}\ \forall\ \bar{a} \in \mathbb{Z}_n$, अर्थात् $\bar{0}$ योग के लिए तत्समक अवयव है।

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

इस प्रकार, $\mathbb{Z}_n$ में प्रत्येक अवयव $\bar{a}$ का योग के सापेक्ष एक प्रतिलोम है।

iv) $\bar{a}+\bar{b}=\overline{a+b}=\overline{b+a}=\bar{b}+\bar{a}\ \forall\ \bar{a}, \bar{b} \in \mathbb{Z}_n$, अर्थात् $\mathbb{Z}_n$ में योग क्रमविनिमेय है।

उपरोक्त गुण (i) से (iv) यह दर्शाते हैं कि **$(\mathbb{Z}_n, +)$ कोटि n वाला एक आबेली समूह** है।

क्या हम $\mathbb{Z}_n$ पर इसी प्रकार से गुणन को परिभाषित कर सकते हैं? आइए देखें।

आइए $\bar{a} \cdot \bar{b} = \overline{ab}$ द्वारा $\mathbb{Z}_n$ **पर गुणन को परिभाषित** करें।

आपको यह सिद्ध करना चाहिए कि $\mathbb{Z}_n$ पर यह एक सुपरिभाषित द्वि-आधारी संक्रिया है।

साथ ही, $(\bar{a}\ \bar{b})\bar{c} = \bar{a}(\bar{b}\ \bar{c})\ \forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$, तथा $\bar{a}\ \bar{b} = \bar{b}\ \bar{a}\ \ \forall\ \bar{a}, \bar{b} \in \mathbb{Z}_n$.

इस प्रकार, $\mathbb{Z}_n$ में गुणन साहचर्य और क्रमविनिमेय द्वि-आधारी संक्रिया है।

आपको इसका सत्यापन करना चाहिए कि $\mathbb{Z}_n$ का गुणनात्मक तत्समक $\bar{1}$ है।

परंतु, $(\mathbb{Z}_n, \cdot)$ एक समूह नहीं है। क्यों? इसका कारण वही है जो $(\mathbb{Z}, \cdot)$ के समूह न होने का है। $\mathbb{Z}_n$ के प्रत्येक अवयव का गुणनात्मक प्रतिलोम नहीं है। उदाहरणार्थ, $\bar{0}$ का कोई गुणनात्मक प्रतिलोम नहीं है क्योंकि $\bar{0} \cdot \bar{r} = \bar{0}\ \forall\ \bar{r} \in \mathbb{Z}_n$.

परंतु, मान लीजिए कि हम $\mathbb{Z}_n$ के शून्येतर अवयवों को लेते हैं, यानी $(\mathbb{Z}_n^*, \cdot)$. क्या यह एक समूह है? देखिए, $\mathbb{Z}_4^* = \{\bar{1}, \bar{2}, \bar{3}\}$ एक समूह नहीं है क्योंकि $\mathbb{Z}_4^*$ पर $\cdot$ एक द्वि-आधारी संक्रिया भी नहीं है चूँकि $\bar{2} \cdot \bar{2} = \bar{0} \notin \mathbb{Z}_4^*$. परंतु, किसी भी अभाज्य संख्या p के लिए, $(\mathbb{Z}_p^*, \cdot)$ एक आबेली समूह होता है, जैसा कि आप अब $p = 5$ के लिए दिखाएँगे।

E21) दर्शाइए कि $(\mathbb{Z}_5^*, \cdot)$ एक आबेली समूह है।

(**संकेत:** केली सारणी बनाइए।)

E22) i) $\mathbb{Z}_{11}^*$ के प्रत्येक अवयव का गुणनात्मक प्रतिलोम क्या है?

ii) $\mathbb{Z}_p^*$ के किसी भी अवयव का गुणनात्मक प्रतिलोम क्या है, जहाँ p एक अभाज्य संख्या है?

(**संकेत:** ध्यान दीजिए कि $\bar{r} \in \mathbb{Z}_p^*$ के लिए, g.c.d. $(r, p) = 1$.)

iii) दर्शाइए कि $(\mathbb{Z}_p^*, \cdot)$ एक आबेली समूह है, जहाँ p एक अभाज्य संख्या है।

आइए अब सममित समूह की चर्चा करें।

2.4.2 सममित समूह

अब हम एक ऐसे समूह पर दृष्टि डालेंगे जिसके अवयव किसी समुच्चय के क्रमचय हैं। इस संकल्पना से आपका परिचय भाग 1.5, इकाई 1, में हुआ था। इकाई 9 में आप इस समूह के बारे में अधिक विस्तार से पढ़ेंगे।

आइए एक उदाहरण से शुरू करें।

उदाहरण 12: मान लीजिए कि B, $\mathbb{R}$ से $\mathbb{R}$ तक के सभी एकैकी आच्छादक फलनों का समुच्चय है। दर्शाइए कि B फलनों के संयोजन के सापेक्ष एक समूह है।

हल: $B \neq \emptyset$, क्योंकि $I : \mathbb{R} \to \mathbb{R} : I(x) = x$, B में है।

आगे, कलन से आप जानते हैं कि यदि B में f और g हैं, तो B में $f \circ g$ भी होता है। इस प्रकार, B में $\circ$ संवृत है।

आप यह भी जानते हैं कि $(f \circ g) \circ h = f \circ (g \circ h) \ \forall \ f, g, h \in B$. इस प्रकार, B पर $\circ$ साहचर्य है।

क्योंकि $f \circ I = f \ \forall \ f \in B$, इसलिए $\circ$ के सापेक्ष I तत्समक है।

साथ ही, यदि $f \in B$, तो f, $\mathbb{R}$ से $\mathbb{R}$ तक एक एकैकी आच्छादक फलन है। अतः, जैसा कि आप जानते हैं, $\exists g \in B$ s.t. $f \circ g = I$.

अतः, $(B, \circ)$ एक समूह है।

***

उपरोक्त उदाहरण में $B, \mathbb{R}$ के क्रमचयों का समुच्चय है। अधिक व्यापक रूप में, यदि X एक अरिक्त समुच्चय है, तो X के सभी क्रमचयों का समुच्चय $S(X)$ होता है।

कलन से आप जानते हैं कि α और β, X से X तक एकैकी आच्छादक फलन हैं, तो $\alpha \circ \beta$ भी एकैकी आच्छादक फलन होता है।

इस प्रकार, फलनों का संयोजन समुच्चय $S(X)$ पर एक द्वि-आधारी संक्रिया है। जैसा कि आप कलन से जानते हैं, व्यापक रूप से यह द्वि-आधारी संक्रिया साहचर्य है। अतः, $S(X)$ मे $\circ$ साहचर्य है।

तत्समक फलन I_X समुच्चय $S(X)$ के लिए तत्समक है, क्योंकि $f \circ I_X = I_X \circ f = f \ \forall \ f \in S(X)$.

आप यह भी जानते हैं कि यदि $f: X \to X$ एकैकी आच्छादक है, तो $\exists \ g: X \to X$ s.t. $f \circ g = g \circ f = I_X$. है। अतः g भी एकैकी आच्छादक है, तथा हम g को f^{-1} द्वारा व्यक्त करते हैं।

इसलिए, यदि $f \in S(X)$ है, तो $f^{-1} \in S(X)$.

आइए अभी जो हमने $(S(X), \circ)$ के बारे में देखा है उसे एक साथ रखें :

i) $S(X)$ पर $\circ$ एक द्वि-आधारी संक्रिया है।

ii) $\circ$ साहचर्य है,

iii) I_X तत्समक अवयव है,

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

इस प्रकार, $(S(X), \circ)$ एक समूह है। इसे **X पर क्रमचय समूह (permutation group)** कहते हैं।

अब, इकाई 1 से आप यह भी जानते हैं कि यदि X परिमित है, मान लीजिए $X = \{1, 2, 3, \ldots, n\}$, तो हम $S(X)$ को $\mathbf{S_n}$ द्वारा व्यक्त करते हैं।

परिभाषा: $n \in \mathbb{N}$ के लिए $(S_n, \circ)$ को **n** प्रतीकों पर, **सममित समूह (symmetric group on n symbols)** कहते हैं।

इकाई 1 से, आप जानते हैं कि $\mathbf{o(S_n) = n!}$.

अब, $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \in S_4$ लीजिए। f^{-1} का दो-पंक्ति रूप क्या होगा?

क्योंकि $f \circ f^{-1} = f^{-1} \circ f = I$, इसलिए हम जानते हैं कि $f^{-1}f(i) = i \;\forall\; i = 1, \ldots, 4.$

अतः, $1 = f^{-1}f(1) = f^{-1}(3),\ 2 = f^{-1}(1),\ 3 = f^{-1}(4)$ तथा $4 = f^{-1}(2).$ इस प्रकार, $f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, अर्थात् f^{-1} प्राप्त करने के लिए f की ऊपरी और निचली पंक्तियों को परस्पर बदलना है। यह व्यापक रूप में सत्य है **– S_n में f^{-1} का 2-पंक्ति निरूपण $f \in S_n$ के 2-पंक्ति निरूपण की पंक्तियों को परस्पर बदलने से प्राप्त हो जाता** है। इसका कारण है कि प्रत्येक $f \in S_n$ एक एकैकी आच्छादक फलन है।

अतः, उदाहरणार्थ, यदि $f = (1\ 2\ 3)$, तो f^{-1} क्या है?

याद कीजिए कि 3-चक्र $(1\ 2\ 3)$ वह फलन है जो $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ द्वारा दिया जाता है।

अतः, $f^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = (2\ \ 1\ \ 3)$, जो फिर एक 3-चक्र है!

निम्नलिखित प्रश्नों को हल करने से आपको S_n के अवयवों के गुणनफल और प्रतिलोम निकालने का कुछ अभ्यास हो जाएगा।

E23) यदि S_5 में f चक्र $(1\ \ 3)$ है, तो f^{-1} को 2-पंक्ति रूप में लिखिए। साथ ही, जाँच कीजिए कि f^{-1} एक चक्र है या नहीं।

E24) भाग 1.5, इकाई 1, में आपने S_3 के सभी, अर्थात् 6, अवयव प्राप्त किए थे। $(S_3, \circ)$ के लिए, केली सारणी लिखिए। इस तरह S_3 के प्रत्येक अवयव का प्रतिलोम प्राप्त कीजिए।

E25) S_5 में $(1\ \ 2)$ और $(2\ \ 4\ \ 5)$ के प्रतिलोम लिखिए। यह भी दर्शाइए कि $[(1\ 2) \circ (2\ 4\ 5)]^{-1} \neq (1\ 2)^{-1} \circ (2\ 4\ 5)^{-1}$. (यह फिर दर्शाता है कि प्रमेय 4 में हम $(ab)^{-1} = a^{-1}b^{-1}$ नहीं लिख सकते हैं।)

जैसा कि हमने इस उपभाग के शुरू में कहा था, हम $(S_n, \circ)$ के बारे में विस्तृत रूप से चर्चा इकाई 9 में करेंगे। अभी के लिए, आइए इन समूहों से संबंधित कुछ समूहों की चर्चा करें।

2.4.3 द्वितल समूह

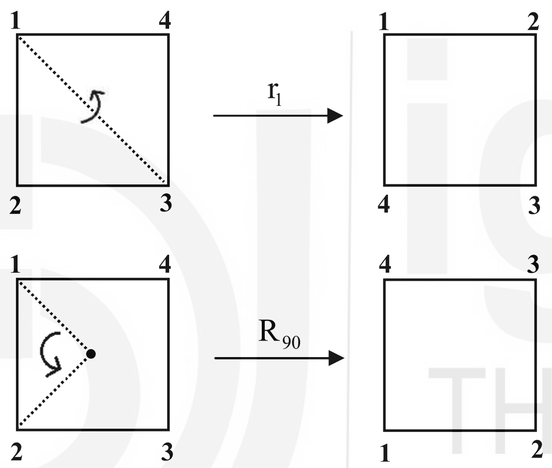
भाग 1.5, इकाई 1, में आपने कुछ समबहुभुजों की सममितियों के समुच्चयों का अध्ययन

किया था। जैसा कि आप जानते हैं, n भुजाओं वाले समबहुभुज की प्रत्येक सममिति n प्रतीकों पर एक क्रमचय होती है। आपने इकाई 1 के E38 में भी देखा था कि $(S_3, \circ)$ एक सम 3-भुज, अर्थात् एक समबाहु त्रिभुज की सममितियों का समूह होता है। परंतु S_4 वर्ग की सममितियों का समुच्चय, D_8, नहीं है। ऐसा इसलिए है क्योंकि D_8 में 8 अवयव हैं, जबकि S_4 में $4!(=24)$ अवयव हैं।

वस्तुतः, $n \neq 3$ के लिए, S_n एक सम n-भुज की सममितियों का समुच्चय नहीं है। परंतु एक सम n-भुज की सममितियों का समुच्चय S_n का एक उपसमुच्चय है तथा यह $\circ$ के सापेक्ष एक समूह है। इसको देखने के लिए आइए फिर से इकाई 1 के E36 में दिए समुच्चय को विस्तृत रूप से देखें।

उदाहरण 13: दर्शाइए कि एक वर्ग की सममितियों का समुच्चय S, $\circ$ के सापेक्ष एक समूह बनाता है।

हल: आकृति 3 पर विचार कीजिए।



आकृति 3: r_1 शीर्षों 1 और 3 से होकर जाने वाले विकर्ण के प्रति परावर्तन है; R_{90} वर्ग के केन्द्र के प्रति 90° से वामावर्त दिशा में घूर्णन है।

आकृति 3 में शीर्षों के नामांकन को लेते हुए, आइए इसकी सभी सममितियों को 2-पंक्ति रूप में लिखें। ये हैं:

$$I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix},\ r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},\ r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},\ r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},\ R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

$$R_{180} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},\ R_{270} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

अब, संक्रिया सारणी बनाने के लिए, मान लीजिए, $r_2 \circ r_3$ को देखें।

$$r_2 \circ r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ r_2r_3(1) & r_2r_3(2) & r_2r_3(3) & r_2r_3(4) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ r_2(2) & r_2(1) & r_2(4) & r_2(3) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = R_{90}.$$

इसी प्रकार, आपको अन्य संयोजनों को मालूम करना चाहिए, तथा जाँच करनी चाहिए कि वाँछित सारणी है :

$\circ$	I	r_1	r_2	r_3	r_4	R_{90}	R_{180}	R_{270}
I	I	r_1	r_2	r_3	r_4	R_{90}	R_{180}	R_{270}
r_1	r_1	I	R_{180}	R_{270}	R_{90}	r_4	r_2	r_3
r_2	r_2	R_{180}	I	R_{90}	R_{270}	r_3	r_1	r_4
r_3	r_3	R_{90}	R_{270}	I	R_{180}	r_1	r_4	r_2
r_4	r_4	R_{270}	R_{90}	R_{180}	I	r_2	r_3	r_1
R_{90}	R_{90}	r_3	R_4	r_2	r_1	R_{180}	R_{270}	I
R_{180}	R_{180}	r_2	r_1	r_4	r_3	R_{270}	I	R_{90}
R_{270}	R_{270}	r_4	r_3	r_1	r_2	I	R_{90}	R_{180}

अब, सारणी से आप देख सकते हैं कि

i) S पर $\circ$ एक द्वि-आधारी संक्रिया है।

ii) $\exists\, I \in S$ s.t. $x \circ I = x \ \forall\ x \in S$.

iii) प्रत्येक $x \in S$ के लिए, $\exists\, y \in S$ s.t. $x \circ y = I$.

साथ ही, क्योंकि व्यापक रूप में फलनों का संयोजन साहचर्य होता है, इसलिए यहाँ भी यह साहचर्य है।

अतः, $(S, \circ)$ एक समूह है।

साथ ही, ध्यान दीजिए कि $R_{180} = R_{90}^2$ और $R_{270} = R_{90}^3$. आगे, यदि r_1 को r लिखें, तो $r_2 = rR_{90}^2$, $r_3 = rR_{90}^3$, $r_4 = rR_{90}$ और $rR_{90} = R_{90}^3 r$, जहाँ टिप्पणी 5 के अनुसार हम फलनों के संयोजन को गुणन का नाम दे रहे हैं।

इसी प्रकार के समीकरण लागू रहेंगे अगर हम r_1 के बदले $r = r_2$, या $r = r_3$, या $r = r_4$ लेते हैं। अतः, हम $S = \{I, R_{90}, R_{90}^2, R_{90}^3, r, rR_{90}, rR_{90}^2, rR_{90}^3\}$ लिख सकते हैं; जहाँ $r^2 = I = R_{90}^4$ और $rR_{90} = R_{90}^3 r$.

***

उपरोक्त उदाहरण में दिया गया समूह ऐसे समूह की एक विशिष्ट स्थिति है जिसे अब हम परिभाषित करेंगे।

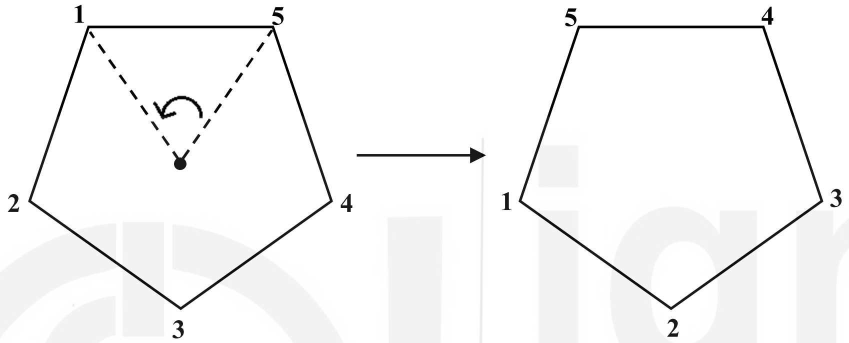
शब्द 'dihedral' यूनानी शब्दों 'di', जिसका अर्थ 'दो' होता है, तथा 'hedron', जिसका अर्थ पृष्ठ होता है, से आया है।

परिभाषा: किसी सम n-भुज की सममितियों का समूह **कोटि 2n वाला द्वितल (dihedral) समूह** कहलाता है, जहाँ $n \geq 3$. इसे $\mathbf{D_{2n}}$ द्वारा व्यक्त किया जाता है। (कुछ लेखक इसे D_n से भी व्यक्त करते हैं।)

उपरोक्त उदाहरण 13, तथा इकाई 1 के उदाहरण 18 से, आप समझ गए होंगे कि $o(D_{2n}) = 2n$ क्यों है। इसका कारण देखें, पहले $n = 5$ को लेते हुए।

आइए सम पंचभुज के शीर्षों को $1, 2, \ldots, 5$ से नामांकित करें, जहाँ 1 के बगल में 2 है, 2 के बगल में 3 है, ..., 4 के बगल में 5 है, और 5 के बगल में 1 है, पंचभुज की भुजाओं के अनुदिश वामावर्त दिशा में चलते हुए।

प्रत्येक सममिति एक शीर्ष को एक शीर्ष में ले जाएगी। इसलिए 1 को 5 शीर्षों में से किसी भी एक शीर्ष तक ले जाया जा सकता है। उदाहरणार्थ, आकृति 4 में हम पंचभुज को उसके केन्द्र के प्रति $\left(\frac{360}{5}\right)^{\circ}$ से वामावर्त दिशा में घूर्णन करने के बाद प्राप्त सममिति को दर्शा रहे हैं। यहाँ हम 1 को 2 पर भेज रहे हैं।



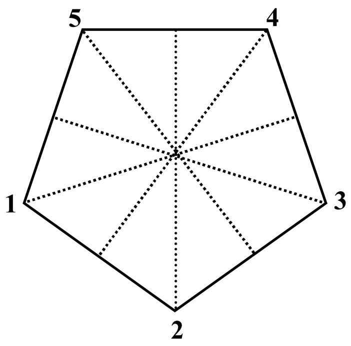
आकृति 4: एक सम पंचभुज की $\left(\frac{360}{5}\right)^{\circ} = 72^{\circ}$ से घूर्णन सममिति

एक बार 1 का प्रतिबिंब नियत हो जाए, तो 2 को बगल वाले शीर्ष पर जाना पड़ेगा। अतः, 2 के लिए केवल 2 विकल्प हैं। एक बार 2 का प्रतिबिंब भी नियत हो जाए, तो शीर्षों 3, 4 और 5 के प्रतिबिंब निर्धारित हो जाते हैं। इस प्रकार, सम पंचभुज की $5 \times 2 = 10$ सममितियाँ हो सकती हैं।

इसी प्रकार, **किसी भी सम n-भुज की अधिकतम 2n सममितियाँ होती** हैं।

साथ ही, आपने जो उदाहरण 13 में देखा था, उसका व्यापकीकरण करने पर, यदि कोई सम n-भुज अपने केन्द्र के प्रति वमावर्त दिशा में $\left(\frac{360}{n}\right)^{\circ}$ से घूर्णन करता है, तो हमें एक सममिति प्राप्त होती है। वस्तुतः, हमें n अलग घूर्णन सममितियाँ प्राप्त होती हैं – 0° से (जो इसके समान है कि हिला ही नहीं है), $\left(\frac{360}{n}\right)^{\circ}$ से, $2\left(\frac{360}{n}\right)^{\circ}$ से, $3\left(\frac{360}{n}\right)^{\circ}$ से, ..., $(n-1)\left(\frac{360}{n}\right)^{\circ}$ से।

भूलिए नहीं! ऐसे बहुभुज की n अलग परावर्तन सममितियाँ भी होती हैं। यह जानने के लिए कि n कैसे हैं, सम n के लिए उदाहरण 13 पर विचार कीजिए। यहाँ $\frac{n}{2}$ सममितियाँ सम्मुख भुजाओं के मध्य-बिंदुओं को मिलाने वाली रेखाओं के प्रति हैं, तथा $\frac{n}{2}$ सममितियाँ सम्मुख शीर्षों को मिलाने वाली रेखाओं के प्रति हैं।



आकृति 5: एक सम पंचभुज की 5 परावर्तन सममितियों के संगत 5 सममित रेखाएँ।

यह समझने के लिए कि n के विषम होने पर n परावर्तन सममितियाँ क्यों होती हैं, आकृति 5 में दिए पंचभुज पर विचार कीजिए। ये n परावर्तन सममितियाँ प्रत्येक शीर्ष को उसकी सम्मुख भुजा के मध्य-बिंदु से मिलाने वाली रेखा के प्रति हैं।

इस प्रकार, एक सम n-भुज की n घूर्णन सममितियाँ और n परावर्तन सममितियाँ होती हैं, सभी $n \geq 3$ के लिए अतः, $o(D_{2n}) = 2n$.

यदि हम एक सम n-भुज की $\left(\frac{360}{n}\right)^\circ$ से घूर्णन सममिति को R द्वारा व्यक्त करें, तो $2\left(\frac{360}{n}\right)^\circ$ का घूर्णन R का दो बार अनुप्रयोग करने पर प्राप्त होता है। अतः, इसे R^2 से व्यक्त करते हैं। इसी प्रकार, अन्य घूर्णन सममितियाँ $R^3, R^4, \ldots, R^{n-1}$ हैं, तथा इनके साथ हमें I भी प्राप्त है, जो 0° से घूर्णन से प्राप्त सममिति है, जब n-भुज हिला नहीं है।

आगे, इस n-भुज की किसी भी परावर्तन सममिति, मान लीजिए, शीर्ष 1 से होकर जाने वाली रेखा के प्रति, सममिति लीजिए। इसे r से व्यक्त कीजिए। तब, इस रेखा के प्रति n-भुज के दर्पण प्रतिबिंब का दर्पण प्रतिबिंब लेने पर, आपको n-भुज की शुरूआती स्थिति प्राप्त हो जाएगी। इस प्रकार, $r^2 = I$. यह किसी भी परावर्तन सममिति के लिए सत्य है।

अंत में, उदाहरण 13 की ही तरह, हम प्राप्त करते हैं
$D_{2n} = \{I, R, R^2, \ldots, R^{n-1}, r, rR, rR^2, \ldots, rR^{n-1}\}$, जहाँ $r^2 = I, R^n = I$ और $rR = R^{n-1}r$.

अब कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E26) S_4 का ऐसा अवयव बताइए जो D_8 का अवयव नहीं है।

E27) $(D_{10}, \circ)$ के लिए केली सारणी बनाइए ।

E28) क्या D_{2n} एक आबेली समूह है, $\forall\, n \geq 3$? अपने उत्तरों के लिए कारण दीजिए।

अब हम समूहों के एक अन्य महत्वपूर्ण प्रकार की चर्चा करेंगे। आपको इसका परिचय इकाई 1 में तथा इस इकाई के कुछ पूर्व उदाहरणों में करवाया जा चुका है।

2.4.4 आव्यूह समूह

भाग 1.4, इकाई 1, में आपने आव्यूहों तथा उन पर संक्रियाओं के बारे में सीखा। उदाहरण 2 और उदाहरण 5 में आप देख चुके हैं कि किस प्रकार आव्यूहों के कुछ समुच्चय आव्यूह योग या गुणन के सापेक्ष एक समूह बनाते हैं। अब आगे बढने से पहले, उन हिस्सों का दोबारा अध्ययन कर लें। वहाँ किए गए आपके अध्ययन के आधार पर हम इस उपभाग में अपनी चर्चा को आगे बढाएँगे।

आइए एक उदाहरण से शुरू करें।

उदाहरण 14: दर्शाइए कि $(\mathbb{M}_{m\times n}(\mathbb{C}), +)$ एक आबेली समूह है।

हल: इकाई 1 में आप देख चुके हैं कि $\mathbb{M}_{m\times n}(\mathbb{C})$ पर $+$,
$[a_{ij}]_{m\times n}+[b_{ij}]_{m\times n}=[a_{ij}+b_{ij}]_{m\times n}$, जहाँ $i=1,\ldots,m,\ j=1,\ldots,n$ के लिए, $a_{ij}, b_{ij}\in\mathbb{C}$

द्वारा परिभाषित एक द्वि-आधारी संक्रिया है।

आप यह भी देख चुके हैं कि + साहचर्य और क्रमविनिमेय है।

आगे, किसी भी $A\in\mathbb{M}_{m\times n}(\mathbb{C})$ के लिए, $A+\mathbf{0}=A$, जहाँ $\mathbf{0}$ वह $m\times n$ आव्यूह है जिसकी सभी प्रविष्टियाँ 0 हैं।

अंत में, $A=[a_{ij}]\in\mathbb{M}_{m\times n}(\mathbb{C})$ दिया रहने पर, $(-A)=[-a_{ij}]\in\mathbb{M}_{m\times n}(\mathbb{C})$ इस प्रकार है कि $A+(-A)=\mathbf{0}.$

अतः, $(\mathbb{M}_{m\times n}(\mathbb{C}), +)$ एक आबेली समूह है।

***

उदाहरण 15: दर्शाइए कि $(\mathbb{M}_n(\mathbb{C}), \cdot)$ एक सामिसमूह है, परंतु एक समूह नहीं है, जहाँ $n\geq 2$. क्या $(\mathbb{M}_n(\mathbb{C})^*, \cdot)$ एक समूह है?

हल: इकाई 1 से आप जानते हैं कि $\mathbb{M}_n(\mathbb{C})$ पर $\cdot$ एक सुपरिभाषित साहचर्य द्वि-आधारी संक्रिया है। इस प्रकार, $(\mathbb{M}_n(\mathbb{C}), \cdot)$ एक सामिसमूह है।

E3 में आप देख चुके हैं कि $(\mathbb{M}_3(\mathbb{C}), \cdot)$ एक समूह क्यों नहीं है। इसी प्रकार, आप देख सकते हैं कि $(\mathbb{M}_n(\mathbb{C}), \cdot)$, किसी भी $n\in\mathbb{N}$ के लिए, एक समूह नहीं है।

वस्तुतः, प्रत्येक $n\geq 2$ के लिए, $\mathbb{M}_n(\mathbb{C})$ में अनंततः अनेक ऐसे आव्यूह हैं जिनके कोई गुणनात्मक प्रतिलोम नहीं हैं। उदाहरणार्थ, $n=2$ के लिए, $A=\begin{bmatrix} a & 0\\ 0 & 0\end{bmatrix}\neq\mathbf{0}$ और

$B=\begin{bmatrix} b_{11} & b_{12}\\ b_{13} & b_{14}\end{bmatrix}\in\mathbb{M}_2(\mathbb{C})^*$ पर विचार कीजिए।

तब, $AB=\begin{bmatrix} a & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix} b_{11} & b_{12}\\ b_{13} & b_{14}\end{bmatrix}=\begin{bmatrix} ab_{11} & ab_{12}\\ 0 & 0\end{bmatrix}\neq\begin{bmatrix} 1 & 0\\ 0 & 1\end{bmatrix}=I_2$, क्योंकि AB की $(2, 2)$वाँ प्रविष्टि 0 है और I_2 की यह प्रविष्टि 1 है।

इस प्रकार, $(\mathbb{M}_2(\mathbb{C})^*, \cdot)$ एक समूह नहीं है।

इसी प्रकार आप दर्शा सकते हैं कि $(\mathbb{M}_n(\mathbb{C})^*, \cdot)$ किसी भी $n\geq 2$ के लिए एक समूह नहीं है।

***

उदाहरण 16: दर्शाइए कि $\mathbb{M}_{3\times 2}(\mathbb{Z}_8)$ आव्यूह योग के सापेक्ष एक परिमित आबेली समूह है। इस समूह की कोटि क्या है?

हल: $\mathbb{M}_{3\times 2}(\mathbb{Z}_8)=\left\{\left.\begin{bmatrix}\bar{a} & \bar{b}\\ \bar{c} & \bar{d}\\ \bar{e} & \bar{f}\end{bmatrix}\right| \bar{a}, \bar{b},\ldots,\bar{f}\in\mathbb{Z}_8\right\}.$

उदाहरण 14 की ही तरह, आपको इसकी जाँच करनी चाहिए कि योग एक सुपरिभाषित साहचर्य द्वि-आधारी संक्रिया है। इसके लिए आपने उपभाग 2.4.1 में जो सीखा उसका उपयोग करें।

यहाँ, $\mathbf{0}=\begin{bmatrix}\bar{0} & \bar{0}\\ \bar{0} & \bar{0}\\ \bar{0} & \bar{0}\end{bmatrix}$ तथा $\begin{bmatrix}\bar{a} & \bar{b}\\ \bar{c} & \bar{d}\\ \bar{e} & \bar{f}\end{bmatrix}$ का प्रतिलोम $\begin{bmatrix}\overline{8-a} & \overline{8-b}\\ \overline{8-c} & \overline{8-d}\\ \overline{8-e} & \overline{8-f}\end{bmatrix}$ है।

अतः, $(\mathbb{M}_{3\times 2}(\mathbb{Z}_8),+)$ एक समूह है।

परंतु यह परिमित क्यों है? यहाँ प्रत्येक आव्यूह में 6 प्रविष्टियाँ हैं। प्रत्येक प्रविष्टि $\mathbb{Z}_8$ के अवयवों, अर्थात् $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}$ में से कोई एक है। अतः, प्रत्येक प्रविष्टि के लिए 8 संभावनाएँ हैं। ध्यान दीजिए कि आव्यूह की दो अलग प्रविष्टियाँ $\mathbb{Z}_8$ का एक ही अवयव हो सकती हैं। इस प्रकार, $\mathbb{M}_{3\times 2}(\mathbb{Z}_8)$ में अवयवों की कुल संख्या 8^6 है।

अतः, यह समूह कोटि 8^6 का एक परिमित समूह है।

अंत में, आपको यह दर्शाना चाहिए कि यह समूह आबेली है, इस बात का उपयोग करते हुए कि $(\mathbb{Z}_8,+)$ आबेली है।

***

अब, आप कुछ प्रश्नों को हल क्यों नहीं करते?

E29) मान लीजिए कि $\mathbb{M}_2(\mathbb{C})$ में, $A=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$ और $B=\begin{bmatrix}0 & i\\ i & 0\end{bmatrix}$, जहाँ $i=\sqrt{-1}.$

दर्शाइए कि $A^4=I, B^4=I$ और $AB=-BA$. साथ ही, $Q_8=\{I, A, A^2, A^3, B, AB, A^2B, A^3B\}$ में गुणन के लिए केली सारणी बनाइए। इससे दर्शाइए कि $(Q_8,\cdot)$ एक समूह है। क्या यह आबेली है? $o(Q_8)$ क्या है?

(इस समूह को **चतुष्टयी समूह (group of quaternions)** कहते हैं।)

E30) यदि $\mathbb{M}_{m\times n}(\mathbb{C})^*$ में गुणन $[a_{ij}]\cdot[b_{ij}]=[a_{ij}\cdot b_{ij}]$ द्वारा परिभाषित होता है, तो जाँच कीजिए कि $(\mathbb{M}_{m\times n}(\mathbb{C})^*,\cdot)$ एक समूह है या नहीं।

इस उपभाग में, आपने आव्यूहों के ऐसे अनेक समुच्चयों का अध्ययन किया है जो समूह बनाते हैं। ये **आव्यूह समूहों (matrix groups)** के उदाहरण हैं। आप इनके बारे में और अधिक पाठ्यक्रम 'रैखिक बीजगणित' में सीखेंगे। अभी के लिए, हम आव्यूहों के समूहों के बारे में अपनी चर्चा को यहीं समाप्त करेंगे, तथा आपको एक अन्य प्रकार के समूह से परिचित कराएँगे। इस समूह का अंतर्निहित समुच्चय $\mathbb{C}^*$ का एक उपसमुच्चय होता है।

2.4.5 एक के मूल

'कलन' के खंड 1 में आपने यह देखा था कि किसी सम्मिश्र संख्या के तीसरे, चौथे पाँचवें, ... मूल कैसे मालूम ज्ञात किए जाते हैं। विशेष रूप में, आप जानते हैं कि किसी भी $n \in \mathbb{N}$ के लिए $\mathbb{C}$ में 1 के n अलग-अलग nवें मूल होते हैं। आप यह भी जानते हैं कि ये सभी मूल एक समतल में उस वृत्त की परिधि पर स्थित हैं जिसका केन्द्र मूलबिंदु पर है तथा त्रिज्या 1 इकाई है।

आइए अब एक ऐसा उदाहरण देखें, जो दर्शाता है कि 1 के nवें मूल किस प्रकार एक समूह बनाते हैं।

उदाहरण 17: दर्शाइए कि 1 के सभी चौथे मूलों का समुच्चय, U_4 गुणन के सापेक्ष एक समूह बनाता है।

हल: 'कलन' के खंड 1 से आप जानते हैं कि 1 का ध्रुवीय रूप है
$(\cos 0 + i\sin 0) = \cos(0+2k\pi) + i\sin(0+2k\pi) \ \forall \ k \in \mathbb{Z}.$

अतः, 1 के चौथे मूलों का ध्रुवीय रूप है
$[\cos(0+2k\pi) + i\sin(0+2k\pi)]^{1/4} = \cos\frac{k\pi}{2} + i\sin\frac{k\pi}{2}, k = 0, 1, 2, 3$ के लिए।

इस प्रकार, $U_4 = \{1, i, -1, -i\}$.

अतः, $(U_4, \cdot)$ उदाहरण 4 में चर्चित समूह है।

***

उपरोक्त उदाहरण में, क्या आपने इस ओर ध्यान दिया है कि $U_4 = \{i, i^2, i^3, i^4\}$, क्योंकि $i = \sqrt{-1}$? हम इसका संदर्भ दोबारा इकाई 4 में देंगे।

आइए उसे अब व्यापकीकृत करें जो आप उदाहरण 17 में देख चुके हैं। इसके लिए, आइए पहले संक्षिप्त में देखें कि 1 के nवें मूल क्या हैं। 'कलन' के खंड 1 से आप जानते हैं कि एक शून्येतर सम्मिश्र संख्या $z \in \mathbb{C}$ का ध्रुवीय रूप $z = r(\cos\theta + i\sin\theta)$ है, जहाँ $r = |z|$ तथा θ सम्मिश्र संख्या z का एक कोणांक (argument) है।

साथ ही, यदि z_1 का कोणांक θ_1 है तथा z_2 का कोणांक θ_2 है, तो z_1z_2 का एक कोणांक $\theta_1 + \theta_2$ होता है। इन तथ्यों का उपयोग करते हुए, आइए 1 के nवें मूल ज्ञात करें, जहाँ $n \in \mathbb{N}$.

यदि $z = r(\cos\theta + i\sin\theta)$, 1 का nवाँ मूल है, तो $z^n = 1$.

इस प्रकार, द मुआव्र प्रमेय द्वारा,

$1 = z^n = r^n(\cos n\theta + i\sin n\theta)$, अर्थात्

$\cos(0+2k\pi) + i\sin(0+2k\pi) = r^n(\cos n\theta + i\sin n\theta)$, $k \in \mathbb{Z}$ के लिए। ...(9)

(9) के दोनों पक्षों के मापांकों को बराबर करने पर, हम प्राप्त करते हैं $r^n = 1$, अर्थात् $r = 1$, क्योंकि मापांक एक वास्तविक संख्या है।

(9) के दोनों पक्षों के कोणांकों की तुलना करने पर, हम देखते हैं कि $0+2\pi k$ $(k \in \mathbb{Z})$ और $n\theta$ एक ही सम्मिश्र संख्या के कोणांक हैं। इस प्रकार, $n\theta$ मानों $2\pi k, k \in \mathbb{Z}$ में से कोई भी एक मान ले सकता है। क्या इसका अर्थ यह है कि जब $k, \mathbb{Z}$ में सभी मान लेता है, तथा θ $\frac{2\pi k}{n}$ पर के सब मान लेता है, तब हमें 1 के अलग-अलग nवें मूल प्राप्त होते हैं? आइए इसका पता लगाएँ।

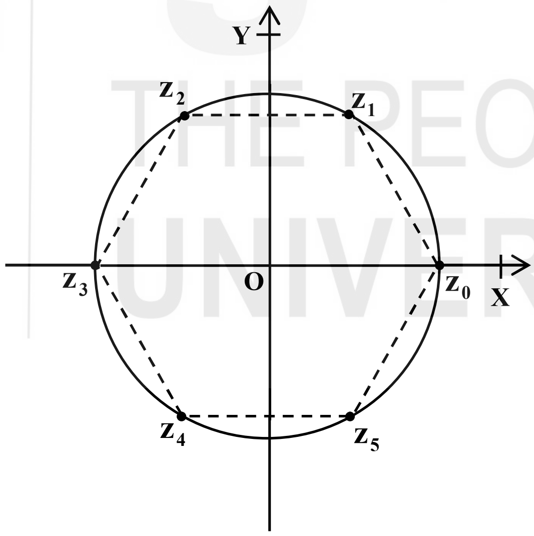
अब, $\cos\frac{2\pi k}{n}+i\sin\frac{2\pi k}{n}=\cos\frac{2\pi m}{n}+i\sin\frac{2\pi m}{n}$ यदि और केवल यदि

$\frac{2\pi k}{n}-\frac{2\pi m}{n}=2\pi t$, किसी $t \in \mathbb{Z}$ के लिए।

ऐसा होगा iff $k = m + nt$, अर्थात् जब $k \equiv m \pmod n$. इस प्रकार,

$\mathbb{Z}_n$ में प्रत्येक $\bar{r}$ के संगत, $0 \le r < n$ हम 1 का एक nवाँ मूल $z=\cos\frac{2\pi r}{n}+i\sin\frac{2\pi r}{n}$ प्राप्त करते हैं; तथा ये ही 1 के सभी nवें मूल हैं।

उदाहरणार्थ, यदि $n = 6$, तो हम 1 के छहों 6वें मूल z_0, z_1, z_2, z_3, z_4 और z_5 प्राप्त करते हैं, जहाँ $z_j=\cos\frac{2\pi j}{6}+i\sin\frac{2\pi j}{6}$, जहाँ $j = 0, 1, 2, 3, 4, 5$. आकृति 6 में आप देख सकते हैं कि ये सभी मूल एकक वृत्त (unit circle) (अर्थात्, त्रिज्या एक और केन्द्र (0, 0) वाले वृत्त) पर स्थित हैं। ये मूल एक समषट्भुज (regular hexagon) के शीर्ष हैं।



आकृति 6: इकाई के 6वें मूल, $z_0, \ldots, z_5$

ζ यूनानी अक्षर ज़ीटा 'zeta' है।

अब, मान लीजिए कि $\zeta=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$. तब 1 के सभी nवें मूल $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ हैं, क्योंकि $\zeta^j=\cos\frac{2\pi j}{n}+i\sin\frac{2\pi j}{n}, 0 \le j \le n-1$ के लिए (द मुआव्र प्रमेय के उपयोग से)। हम 1 के nवें मूलों के समुच्चय को $\mathbf{U_n}$ द्वारा व्यक्त करते हैं।

इस प्रकार, $\mathbf{U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}}$. ध्यान दीजिए कि $U_n \subseteq \mathbb{C}$.

निम्नलिखित प्रश्नों को हल करने पर आप 1 के सभी nवें मूलों से संबंधित एक रोचक गुण को सिद्ध कर लेंगे। यह गुण 1 के nवें मूलों के साथ कार्य करते समय प्रायः उपयोग किया जाता है।

E31) यदि $n > 1$ तथा $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, तो दर्शाइए कि

$$1 + \zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^{n-1} = 0.$$

E32) दर्शाइए कि $U_3 = \{1, \omega, -(1+\omega)\}$ है, जहाँ $\omega = \frac{-1 + i\sqrt{3}}{2}$.

अब हम उदाहरण 17 को व्यापकीकृत करने की स्थिति में हैं।

उदाहरण 18: दर्शाइए कि U_n गुणन के सापेक्ष एक परिमित आबेली समूह है।

हल: जैसा कि आपने ऊपर देखा है, 1 के nवें मूल $z_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ हैं, जहाँ $k = 0, 1, \ldots, (n-1)$.

अतः, U_n में n अवयव हैं।

अब, $z_r z_m = \left(\cos\frac{2r\pi}{n} + i\sin\frac{2r\pi}{n}\right)\left(\cos\frac{2m\pi}{n} + i\sin\frac{2m\pi}{n}\right)$

$$= \cos\frac{2(r+m)\pi}{n} + i\sin\frac{2(r+m)\pi}{n}$$

$= \cos\frac{2j\pi}{n} + i\sin\frac{2j\pi}{n}$, है, जहाँ $(r+m) \equiv j (\bmod n)$, किसी j के लिए जहाँ $0 \le j \le n-1$, विभाजन कलन विधि के उपयोग से।

अतः, U_n पर गुणन एक द्वि-आधारी संक्रिया है।

क्योंकि $\mathbb{C}$ पर गुणन साहचर्य है तथा $U_n \subseteq \mathbb{C}$, इसलिए U_n पर गुणन साहचर्य है।

गुणनात्मक तत्समक $1 = \cos 0 + i\sin 0$ है।

z_r का गुणनात्मक प्रतिलोम z_{n-r} है, क्योंकि $z_r z_{n-r} = \cos\frac{2n\pi}{n} + i\sin\frac{2n\pi}{n} = 1$.

अंत में, क्योंकि $\mathbb{C}$ में गुणन क्रमविनिमेय है, इसलिए यही U_n के लिए भी सत्य है।

इस प्रकार, $(U_n, \cdot)$ एक परिमित आबेली समूह है। ध्यान दीजिए कि $\mathbf{o(U_n) = n.}$

***

अब एक संबंधित प्रश्न को हल करने का प्रयास कीजिए।

E33) समुच्चय U_6 में गुणन के लिए केली सारणी बनाइए। इससे निर्णय कीजिए कि क्या $(U_6, \cdot)$ और $(D_6, \circ)$ समान समूह हैं।

अभी तक आपने विभिन्न प्रकार के अनेक समूहों के बारे में सीखा है। अब हम एक ऐसे समूह पर विचार करेंगे, जो दो या अधिक समूहों से बनता है।

2.4.6 अनुलोम गुणनफल

इस उपभाग में हम दिए हुए समूहों से नए समूह बनाने की एक अति महत्वपूर्ण विधि पर चर्चा करेंगे। उदाहरणार्थ, अपने पिछले पाठ्यक्रमों से आप समुच्चय $\mathbb{R}\times\mathbb{R}$, अर्थात् $\mathbb{R}^2$ से परिचित हैं। यह $\mathbb{R}$ का स्वयं के साथ कार्तीय गुणनफल है, जैसा कि आप जानते हैं।

आप यह भी जानते हैं कि $(x, y), (a, b) \in \mathbb{R}\times\mathbb{R}$ के लिए,

$(x, y)\cdot(a, b) = (xa, yb)$ तथा $(x, y) + (a, b) = (x + a, y + b).$

वास्तव में, $(\mathbb{R}\times\mathbb{R}, +)$ एक समूह है जिसका तत्समक $(0, 0)$ है तथा (a, b) का प्रतिलोम $(-a, -b)$ है। ऐसी ही प्रक्रिया को अपनाते हुए, किन्हीं दो समूहों से हम उन पर परिभाषित द्वि-आधारी संक्रियाओं का उपयोग करते हुए एक समूह बना सकते हैं। आइए देखें कैसे।

मान लीजिए कि $(G_1, *_1)$ और $(G_2, *_2)$ दो समूह हैं। G_1 और G_2 का कार्तीय गुणनफल G लीजिए (जिसका अध्ययन आपने 'कलन' के खंड 1 में किया था।) अतः, $G = G_1 \times G_2 = \{(x, y) \mid x \in G_1, y \in G_2\}.$

क्या हम G_1 और G_2 पर संक्रियाओं का उपयोग करते हुए, G पर एक द्वि-आधारी संक्रिया को परिभाषित कर सकते हैं? आइए स्पष्ट विधि, अर्थात् घटकों के अनुसार, लागू करके देखें। अर्थात्, हम

$(a, b) * (c, d) = (a *_1 c, b *_2 d)\ \forall\ a, c \in G_1, b, d \in G_2$ द्वारा G पर संक्रिया $*$ परिभाषित करते हैं।

$*$ **सुपरिभाषित है:** मान लीजिए कि G में $(a, b) = (a', b'), (c, d) = (c', d')$. तब, $a = a', b = b', c = c', d = d'$. इसलिए

$$(a, b) * (c, d) = (a *_1 c, b *_2 d) = (a' *_1 c', b' *_2 d') = (a', b') * (c', d').$$

इस प्रकार, $*$ सुपरिभाषित है।

G पर $*$ संवृत है: $(a,b),(c,d) \in G$ के लिए $(a,b)*(c,d) \in G$ क्योंकि $a *_1 c \in G_1$ तथा $b *_2 d \in G_2$.

अतः, G पर $*$ एक द्वि-आधारी संक्रिया है।

यह सिद्ध करने के लिए कि $(G, *)$ एक समूह है, आपको निम्नलिखित प्रश्न को हल करने की आवश्यकता है।

E34) दर्शाइए कि $G = G_1 \times G_2$ पर द्वि-आधारी संक्रिया $*$ साहचर्य है। $*$ के सापेक्ष तत्समक अवयव, तथा G के किसी अवयव (x, y) का प्रतिलोम, ज्ञात कीजिए।

अतः, आपने दर्शा 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। (अगले खंड में, आप 'आंतरिक अनुलोम गुणनफल' के बारे में अध्ययन करेंगे।)

उदाहरणार्थ, $(\mathbb{R}, +)$ का स्वयं के साथ बाह्य अनुलोम गुणनफल $(\mathbb{R}^2, +)$ है।

एक अन्य उदाहरण है, अनुलोम गुणनफल $(\mathbb{Z}, +) \times (\mathbb{R}^*, \cdot)$, जिस पर संक्रिया $(m, x) * (n, y) = (m + n, xy)$ द्वारा दी जाती है।

इसी प्रकार हम 3, 4, या अधिक, समूहों के बाह्य अनुलोम गुणनफल को परिभाषित कर सकते हैं, जैसा नीचे दर्शाया गया है।

परिभाषा: मान लीजिए कि n समूहों $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$ दिए हैं। इनका **बाह्य अनुलोम गुणनफल** समूह $(G, *)$ है, जहाँ $G = G_1 \times G_2 \times \ldots \times G_n$ तथा
$(x_1, x_2, \ldots, x_n) * (y_1, y_2, \ldots, y_n) = (x_1 *_1 y_1, x_2 *_2 y_2, \ldots, x_n *_n y_n) \;\forall\; x_i, y_i \in G_i$,
$i = 1, \ldots, n.$

इस प्रकार, $n \in \mathbb{N}$ के लिए, $\mathbb{R}^n$, $\mathbb{R}$ की स्वयं से n बार का बाह्य अनुलोम गुणनफल है; तथा $\mathbb{C}^n$, $\mathbb{C}$ की स्वयं से n बार का बाह्य अनुलोम गुणनफल है।

अब हम संकेतन और शब्दावली के बारे में एक टिप्पणी देना चाहेंगे।

टिप्पणी 7: आइंदा, हम टिप्पणी 5 में की गई बात की ही तरह सभी संक्रियाएँ $*, *_1, \ldots, *_n$ को गुणन मानेंगे, जब तक अन्यथा न कहा जाए। इस प्रकार, $G = G_1 \times G_2 \times \ldots \times G_n$ पर संक्रिया
$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n) \;\forall\; a_i, b_i \in G_i$

द्वारा दी जाएगी।

साथ ही, हम G को 'बाह्य अनुलोम गुणनफल' कहने के बजाय **केवल 'अनुलोम गुणनफल' कहेंगे।**

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E35) दर्शाइए कि $G_1 \times G_2$ आबेली है यदि और केवल यदि दोनों समूह G_1 और G_2 आबेली हैं।

E36) यदि $G_1 \times G_2$ अपरिमित है, तो क्या G_1 और G_2 अपरिमित होंगे? यदि $G_1 \times G_2$ परिमित है, तो क्या G_1 और G_2 परिमित होंगे? अपने उत्तरों के कारण दीजिए।

E37) $(U_3 \times S_3, *)$ के लिए केली सारणी बनाइए। $o(U_3 \times S_3)$ क्या है?

इसके साथ ही, हम समूहों के इस परिचय को ख़त्म करते हैं। निःसंदेह, समूहों के विभिन्न पहलुओं पर चर्चा इस पाठ्यक्रम में निरंतर जारी रहेगी। अभी के लिए, आइए संक्षिप्त में देखें कि इस इकाई में आपने क्या अध्ययन किया है।

2.5 सारांश

इस इकाई में आपने निम्नलिखित बातों की पढ़ाई की है।

1. वे अभिगृहीत जो एक समूह को परिभाषित करते हैं, तथा इस बीजीय वस्तु के कुछ उदाहरण।

2. किसी समूह $(G, *)$ में, $*$ के सापेक्ष तत्समक, तथा $*$ के सापेक्ष प्रत्येक अवयव का प्रतिलोम, अद्वितीय होता है।

3. एक समूह के लिए दक्षिण और वाम निरसन नियम सत्य होते हैं।

4. परिमित और अपरिमित समूह, आबेली और अन्आबेली समूह, और परिमित समूह की कोटि, इन सब की परिभाषा तथा कई उदाहरण।

5. एक समूह G में a, b के लिए, $(ab)^{-1} = b^{-1}a^{-1}$ होता है।

6. समूह के अवयवों के लिए घातांक नियम।

7. पूर्णांक मोड्यूलो $n(n \in \mathbb{N})$ के समूहों, सममित समूहों, द्वितल समूहों, $n \in \mathbb{N}$ के लिए 1 के nवें मूलों के समूहों, तथा समूहों के अनुलोम गुणनफलों से परिचय।

2.6 हल / उत्तर

E1) पहले इसकी जाँच कीजिए कि $\mathbb{Q}$ पर $+$ एक द्वि-आधारी संक्रिया है। फिर, उदाहरण 1 की तरह, दर्शाइए कि G1, G2, G3 को $(\mathbb{Q}, +)$ संतुष्ट करता है।

उदाहरण 1 में, आप देख चुके हैं कि G1 और G2 को $(\mathbb{R}, \cdot)$ संतुष्ट करता है। अतः, G1 और G2 को $(\mathbb{R}^*, \cdot)$ भी संतुष्ट करता है।

अब, $r \in \mathbb{R}^*$ के लिए, $\frac{1}{r} \in \mathbb{R}^*$ s.t. $r \cdot \left(\frac{1}{r}\right) = 1 = \left(\frac{1}{r}\right) \cdot r.$

अतः, G3 को भी $(\mathbb{R}^*, \cdot)$ संतुष्ट करता है।

इस प्रकार, $(\mathbb{R}^*, \cdot)$ एक समूह है।

इसी प्रकार, जाँच कीजिए कि $\mathbb{C}$ पर घटाने की संक्रिया एक द्वि-आधारी संक्रिया है। फिर जाँच कीजिए कि क्या यह साहचर्य है या नहीं। उदाहरणार्थ, क्या $(2-3)-4 = 2-(3-4)$

क्योंकि G1 संतुष्ट नहीं हो रहा है, इसलिए $(\mathbb{C}, -)$ एक समूह नहीं है।

E2) इकाई 1 से आप जानते हैं कि S_3 में 2-चक्रों का समुच्चय $S = \{(1\ 2), (1\ 3), (2\ 3)\}$ है। ध्यान दीजिए कि $(1\ 2) = (2\ 1)$, इत्यादि। अतः, सवाल यह है कि क्या $(S, \circ)$ एक समूह है।

अब, $(1\ 2) \circ (1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3\ 2) \notin S.$

इसलिए, S पर $\circ$ एक द्वि-आधारी संक्रिया नहीं है।

अतः, $(S, \circ)$ एक समूह नहीं है।

E3) i) भाग 1.4, इकाई 1, से आप जानते हैं कि +, $\mathbb{M}_{2\times3}(\mathbb{C})$ पर संवृत है। आप यह भी जानते हैं कि $\mathbb{M}_{2\times3}(\mathbb{C})$ पर + साहचर्य है।

अब, आपको इसकी जाँच करनी चाहिए कि $\mathbf{0} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$, + के सापेक्ष तत्समक है।

साथ ही, $A = [a_{ij}] \in \mathbb{M}_{2\times3}(\mathbb{C})$ के लिए, $-A = [-a_{ij}] \in \mathbb{M}_{2\times3}(\mathbb{C})$ ऐसा है कि $A + (-A) = \mathbf{0}.$

इस प्रकार, $(\mathbb{M}_{2\times3}(\mathbb{C}), +)$ एक समूह है।

ii) भाग 1.4, इकाई 1, से आप जानते हैं कि $\mathbb{M}_3(\mathbb{C})$ पर '$\cdot$' एक साहचर्य द्वि-आधारी संक्रिया है।

साथ ही, $I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ संक्रिया '$\cdot$' के लिए तत्समक है।

परंतु, इसके प्रत्येक अवयव का प्रतिलोम नहीं है।

उदाहरणार्थ, $\mathbf{0} \in \mathbb{M}_3(\mathbb{C})$ के लिए ऐसा कोई $A \in \mathbb{M}_3(\mathbb{C})$ नहीं है जिससे कि $\mathbf{0} \cdot A = I$, क्योंकि $\mathbf{0} \cdot A = \mathbf{0} \ \forall \ A \in \mathbb{M}_3(\mathbb{C})$.

अतः, $(\mathbb{M}_3(\mathbb{C}), \cdot)$ एक समूह नहीं है।

iii) जैसे E1 में $(\mathbb{R}^*, \cdot)$ के लिए आपने किया था, वैसे आप ही दिखाइए कि $(\mathbb{Q}^*, \cdot)$ एक समूह है।

iv) क्या $\mathbb{Z}^*$ में '$\cdot$' के सापेक्ष 2 का प्रतिलोम है? नहीं।

अतः, $(\mathbb{Z}^*, \cdot)$ एक समूह नहीं है।

E4) $a, b \in \mathbb{R}^+$ के लिए, $\frac{a}{b} \in \mathbb{R}^+$. अतः, $\mathbb{R}^+$ पर '$\div$' एक द्वि-आधारी संक्रिया है। परंतु, दर्शाइए कि यह G1 को संतुष्ट नहीं करता है। अतः, $(\mathbb{R}^+, \div)$ एक समूह नहीं है।

दर्शाइए कि $\mathbb{R}^-$ पर $\cdot$ एक द्वि-आधारी संक्रिया नहीं है। अतः, $(\mathbb{R}^-, \cdot)$ एक समूह नहीं है।

E5) 'S पर $*$ संवृत है' बताता है कि सारणी की सभी प्रविष्टियाँ S से होनी चाहिए।

'S पर $*$ क्रमविनिमेय है' बताता है कि सारणी की प्रविष्टियाँ विकर्ण के प्रति सममित होनी चाहिए।

इस प्रकार, क्योंकि पहली पंक्ति (0 1 2 3) है, इसलिए पहला स्तंभ वही,

अर्थात् $\begin{pmatrix}0\\1\\2\\3\end{pmatrix}$ होना चाहिए, इत्यादि। अतः, सारणी नीचे दिए अनुसार है।

∗	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

E6) i) जैसा E3(iii) में किया था वैसे ही दर्शाइए कि $(\mathbb{C}^*, \cdot)$ एक समूह है। फिर स्पष्ट कीजिए कि यह आबेली क्यों है।

ii) क्योंकि $\mathbb{R}^*$ परिमित नहीं है, इसलिए यह असत्य है।

iii) यह असत्य है, क्योंकि $\mathbb{Z}_O$ पर + एक द्वि-आधारी संक्रिया नहीं है।

iv) उदाहरण 1 की ही तरह स्पष्ट कीजिए कि यह क्यों सत्य है।

v) जाँच कीजिए कि $\mathbb{Q}^+$ पर ∗ संवृत है, यह साहचर्य है, इसका तत्समक $\frac{1}{2} \in \mathbb{Q}^+$ है तथा a का प्रतिलोम $\frac{1}{4a} \in \mathbb{Q}^+$ है।

E7) पहले जाँच कीजिए कि G पर ∗ एक द्वि-आधारी संक्रिया है।

आगे, $(a, b), (c, d), (e, f) \in G$ के लिए,

$$((a,b)*(c,d))*(e,f) = (ac, bc+d)*(e,f) = (ace, (bc+d)e+f)$$
$$= (ace, bce+(de+f))$$
$$= (a, b)*((c, d)*(e, f)).$$

इस प्रकार, $G1'$ को ∗ संतुष्ट करता है।

$(a, b)*(1, 0) = (a, b) \ \forall \ (a, b) \in G.$

इस प्रकार, $G2'$ सत्य है।

$(a, b) \in G$ के लिए, $(a, b)*(a^{-1}, -a^{-1}b) = (1, 0).$

अतः, $G3'$ सत्य है।

अतः, $(G, *)$ एक समूह है।

E8) नीचे दी गई सारणी पर विचार कीजिए।

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

यहाँ, $G = \{1, 2, 3\}$. $*$ की संक्रिया सारणी से आप देख सकते हैं कि सारणी की सभी प्रविष्टियाँ G से हैं। अतः, G पर $*$ एक द्वि-आधारी संक्रिया है।

परंतु G में ऐसा कोई अवयव नहीं है जो $*$ के सापेक्ष तत्समक हो। इस प्रकार, $G2'$ को $(G, *)$ संतुष्ट नहीं करता है। अतः, $(G, *)$ एक समूह नहीं है।

E9) (i) की उपपत्ति की ही तरह, $ad = e$.

तब, $ba = ca \Rightarrow bad = cad \Rightarrow b = c$.

E10) क्योंकि G एक समूह है, इसलिए इसमें $*$ के सापेक्ष एक तत्समक e है। दी हुई प्रविष्टियों से आप जानते हैं कि $a_2 * a_2 \neq a_2$ तथा $a_2 * a_3 \neq a_2$. अतः, $a_2 \neq e$, $a_3 \neq e$. इसलिए $a_1 = e$.

आगे, टिप्पणी 3 द्वारा, सारणी की प्रत्येक पंक्ति और प्रत्येक स्तंभ में प्रत्येक अवयव एक और केवल एक बार प्रकट हो रहा है।

अंत में, क्योंकि $(G, *)$ क्रमविनिमेय है, इसलिए यह सारणी $a_1 * a_1$ से $a_3 * a_3$ तक के विकर्ण के सापेक्ष सममित है।

उपरोक्त बिंदुओं का उपयोग करके आप देख सकते हैं कि सारणी निम्न है :

$*$	a_1	a_2	a_3
a_1	a_1	a_2	a_3
a_2	a_2	a_3	a_1
a_3	a_3	a_1	a_2

E11) G का कोई भी अवयव लीजिए मान लीजिए कि a. तब, दिए हुए प्रतिबंध द्वारा, $ga = g = ge$. वाम निरसन नियम द्वारा, इससे $a = e$ मिलता है। क्योंकि a, G का कोई भी अवयव था, इसलिए यह प्रदर्शित होता है कि $G = \{e\}$.

E12) $GL_2(\mathbb{R})$ में $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ और $B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ लीजिए। अब, $AB = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$.

साथ ही, $C = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix}$ ऐसा है कि $BC = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$.

इसलिए, $AB = BC$, परंतु $A \neq C$ क्योंकि, उदाहरण के लिए, इनके $(1, 1)$ वें अवयव अलग-अलग हैं।

E13) $(a_1 a_2 \ldots a_n)(a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1})$

$= a_1a_2 \ldots a_{n-1}(a_na_n^{-1})a_{n-1}^{-1} \ldots a_1^{-1}$

$= a_1a_2 \ldots a_{n-1}(e)a_{n-1}^{-1} \ldots a_1^{-1}$

$= a_1a_2 \ldots (a_{n-1}a_{n-1}^{-1}) \ldots a_1^{-1}$

$\vdots$

$= e.$

अतः, $(a_1a_2 \ldots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \ldots a_2^{-1}a_1^{-1}$.

E14) मान लीजिए कि $x, y \in G$.

तब, $xy = (xy)^2 = xyxy$.

इस प्रकार, $x^2y^2 = xyxy$, क्योंकि $x^2 = x$ और $y^2 = y$.

$\Rightarrow xy = yx$, बाईं ओर से x का तथा दाईं ओर से y का निरसन करने पर।

अतः, G आबेली है।

यह देखने के लिए कि विलोम सत्य है या नहीं, $(\mathbb{Z}, +)$ पर विचार कीजिए। यह आबेली है, परंतु किसी भी शून्येतर $x \in \mathbb{Z}$ के लिए, $x + x \neq x$. अतः, विलोम सत्य नहीं है।

E15) $x \in G$ के लिए, $x^2 = e \Rightarrow x = x^{-1}$, दोनों पक्षों को x^{-1} से गुणा करने पर।

अब, $x \in G, y \in G$ के लिए, $xy \in G$.

अतः, $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

इस प्रकार, G आबेली है।

यह दर्शाने के लिए कि विलोम क्यों असत्य है, आप $(\mathbb{Z}, +)$ का उपयोग कर सकते हैं।

E16) क्योंकि व्यवकलन साहचर्य नहीं है, इसलिए $(\mathbb{Z}, -)$ एक समूह नहीं है। परंतु $\mathbb{Z}$ में $a - x = b$ का एक अद्वितीय हल $a - b$ है। अतः, प्रमेय 5 का विलोम सत्य नहीं है।

E17) नहीं, उदाहरणार्थ, $(\mathbb{Z}^*, \cdot)$ को लीजिए। यह एक सामिसमूह है, परंतु समूह नहीं है। साथ ही, $\mathbb{Z}^*$ में $2x = 3$ का कोई हल नहीं है।

E18) जब $n = 0$, तब $(a^m)^0 = e = a^{m \cdot 0}$. अतः, यह कथन सत्य है।

अब मान लीजिए कि $n > 0$ है। हम n पर आगमन का प्रयोग करेंगे।

$n = 1$ के लिए, यह कथन सत्य है, क्योंकि $(a^m)^1 = a^{m \cdot 1} = a^m$.

अब, मान लीजिए कीजिए कि यह $k-1$ के लिए सत्य है, अर्थात्, किसी $k \ge 2$ के लिए, $(a^m)^{(k-1)} = a^{m(k-1)}$.

तब, $(a^m)^k = (a^m)^{(k-1+1)} = (a^m)^{(k-1)} \cdot a^m$ प्रमेय 6 (ii) से।

$= a^{m(k-1)} \cdot a^m$, क्योंकि यह $(k-1)$ के लिए सत्य है।

$= a^{m(k-1+1)}$, प्रमेय 6 (ii) से।

$= a^{mk}$.

अतः, (iii), k के लिए सत्य है। इसलिए, यह सभी $n > 0$ और सभी $m \in \mathbb{Z}$ के लिए सत्य है।

अब मान लीजिए कि $n < 0$ है। तब, $(-n) > 0$ है।

$\therefore (a^m)^n = [(a^m)^{-n}]^{-1}$, प्रमेय 6 के (i) द्वारा।

$= [a^{m(-n)}]^{-1}$, $n > 0$ की स्थिति द्वारा।

$= [a^{-mn}]^{-1}$

$= a^{mn}$, प्रमेय 6 के (i) द्वारा।

इस प्रकार, $\forall\ m, n \in \mathbb{Z}$, (iii) सत्य है।

E19) i) क्योंकि $b \in G$, इसलिए $b^m \in G$. अतः, $ab^m = b^m a$, क्योंकि G आबेली है।

ii) यदि $m = 0$, तो $(ab)^m = e$, $a^m = e$ और $b^m = e$. अतः, $(ab)^m = a^m b^m$.

यदि $m > 0$, तो इसे सिद्ध करने के लिए m पर आगमन का उपयोग कीजिए।

यदि $m < 0$, तो $(ab)^{-m} = a^{-m} \cdot b^{-m}$, क्योंकि $(-m) > 0$ है।

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

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

$\Rightarrow b^m a^m = (ab)^m$

$\Rightarrow a^m b^m = (ab)^m$, क्योंकि G आबेली है।

E20) ध्यान दीजिए कि $\mathbb{Z}_5$ पर + एक द्वि-आधारी संक्रिया है।

इसलिए सारणी में प्रविष्टियाँ केवल $\mathbb{Z}_5$ से होनी चाहिए। इस प्रकार, यह सारणी निम्न है :

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

क्या आपने इस ओर ध्यान दिया कि सभी प्रविष्टियाँ $\overline{0}+\overline{0}$ से $\overline{4}+\overline{4}$ तक के विकर्ण के प्रति सममित हैं? यह आपको संक्रिया के बारे में क्या बताता है?

E21) इन प्रश्नों से पहले हुई चर्चा से आप जानते हैं कि $\mathbb{Z}_5^*$ पर $\cdot$ एक आबेली साहचर्य द्वि-आधारी संक्रिया है, जिसका तत्समक $\overline{1}$ है। इस प्रकार, सारणी निम्न है :

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

उपरोक्त केली सारणी दर्शाती है कि प्रत्येक $\overline{r}\in\mathbb{Z}_5^*$ के लिए, $\exists\ \overline{s}\in\mathbb{Z}_5^*$ s.t. $\overline{r}\cdot\overline{s}=\overline{1}$. अतः, $(\mathbb{Z}_5^*,\cdot)$ एक आबेली समूह है।

E22) i) आप $\mathbb{Z}_{11}^*$ पर गुणन की केली सारणी बना सकते हैं, तथा निम्न प्रतिलोमों को प्राप्त कर सकते हैं:

$$\overline{1}^{-1}=\overline{1},\ \overline{2}^{-1}=\overline{6},\ \overline{6}^{-1}=\overline{2},\ \overline{3}^{-1}=\overline{4},\ \overline{4}^{-1}=\overline{3},\ \overline{5}^{-1}=\overline{9},\ \overline{9}^{-1}=\overline{5},\ \overline{7}^{-1}=\overline{8},$$
$$\overline{8}^{-1}=\overline{7},\ \overline{10}^{-1}=\overline{10}.$$

ii) $\overline{r}\in\mathbb{Z}_p^*$ के लिए, $(r,p)=1\Rightarrow rs+pt=1$, किसी $s,t\in\mathbb{Z}$ के लिए।

$\Rightarrow \overline{r}\ \overline{s}\equiv\overline{1}\pmod p\Rightarrow\overline{r}^{-1}=\overline{s}.$

क्योंकि $s\in\mathbb{Z}=\bigcup\limits_{i=0}^{p-1}\overline{i}$, $\exists\ \overline{m}\in\mathbb{Z}_p$ s.t. $\overline{s}=\overline{m},\ 0\le m\le(p-1)$.

परंतु, क्योंकि $\overline{r}\,\overline{s}=\overline{1}$, इसलिए $\mathbb{Z}_p$ में $\overline{s}\ne\overline{0}$. अतः, $\overline{m}\ne\overline{0}$, अर्थात्, $0<m\le(p-1)$.

उदाहरणार्थ, $\overline{1}^{-1}=\overline{1}$, क्योंकि $1\cdot1+p\cdot0=1$. (यहाँ $t=0$.)

पुनः, $(\overline{p-1})^{-1}=\overline{p-1}$, क्योंकि $(p-1)^2\equiv1\pmod p$. (ध्यान दीजिए कि $(p-1)(p-1)+p(2-p)=1$.) ।

iii) **$\mathbb{Z}_p^*$ पर गुणन संवृत है:** $\overline{r},\overline{s}\in\mathbb{Z}_p^*$ के लिए, $p\nmid r$ और $p\nmid s$.

क्योंकि p एक अभाज्य संख्या है, इसलिए $p \nmid rs$. इस प्रकार,
$\overline{rs} = \bar{r}\,\bar{s} \in \mathbb{Z}_p^*$.

$\mathbb{Z}_p^*$ पर गुणन साहचर्य और क्रमविनिमेय है, क्योंकि गुणन $\mathbb{Z}_p$ पर भी ऐसा ही है। **$\bar{1}$ गुणनात्मक तत्समक है,** जैसा कि पहले चर्चा की जा चुकी है।

गुणन के सापेक्ष प्रत्येक अवयव का एक प्रतिलोम है, जैसा ऊपर (ii) में दर्शाया जा चुका है।

इस प्रकार, $(\mathbb{Z}_p^*, \cdot)$ एक आबेली समूह है।

E23) $f = (1\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$.

अतः, $f^{-1} = \begin{pmatrix} 3 & 2 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = f$.

इस प्रकार, f^{-1} भी एक चक्र है।

E24) $S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

केली सारणी निम्न है :

$\circ$	I	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
I	I	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	I	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	I	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	I	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	I
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	I	(1 2 3)

इस सारणी से हम देखते हैं कि $I^{-1} = I$, $(1\ 2)^{-1} = (1\ 2)$, $(1\ 3)^{-1} = (1\ 3)$,

$(2\ 3)^{-1} = (2\ 3)$, $(1\ 2\ 3)^{-1} = (1\ 3\ 2)$ और $(1\ 3\ 2)^{-1} = (1\ 2\ 3)$.

E25) जाँच कीजिए कि $(1\ 2)^{-1} = (1\ 2)$ तथा $(2\ 4\ 5)^{-1} = (2\ 5\ 4)$.

अब, $(1\ 2) \circ (2\ 4\ 5) = (2\ 4\ 5\ 1)$.

आपको इसकी जाँच करनी चाहिए कि $[(1\ 2) \circ (2\ 4\ 5)]^{-1} = (1\ 5\ 4\ 2)$.

साथ ही, $(1\ 2)^{-1} \circ (2\ 4\ 5)^{-1} = (1\ 2) \circ (2\ 5\ 4) = (2\ 5\ 4\ 1) \neq (1\ 5\ 4\ 2)$, क्योंकि, उदाहरणार्थ, $(2\ 5\ 4\ 1)$, 2 को 5 में ले जाता है तथा $(1\ 5\ 4\ 2)$, 2 को 1 में ले जाता है।

E26) $(1\ 2\ 3) \in S_4$ पर विचार कीजिए। यह D_8 में स्थित नहीं है क्योंकि यदि आप वर्ग के शीर्षों 1, 2 और 3 को हिलाते हैं, तो शीर्ष 4 को भी हिलाना होगा। परंतु $(1\ 2\ 3)$, 4 को नियत रखता है, तथा अन्य 3 अवयवों को हिलाता है।

E27) $D_{10} = \{I, r, R, R^2, R^3, R^4, rR, rR^2, rR^3, rR^4\}$, है जहाँ $r^2 = I$, $R^5 = I$ तथा $rR = R^4 r$.

$\circ$	I	r	R	R^2	R^3	R^4	rR	rR^2	rR^3	rR^4
I	I	r	R	R^2	R^3	R^4	rR	rR^2	rR^3	rR^4
r	r	I	rR	rR^2	rR^3	rR^4	R	R^2	R^3	R^4
R	R	rR^4	R^2	R^3	R^4	I	r	rR	rR^2	rR^3
R^2	R^2	rR^3	R^3	R^4	I	R	rR^4	r	rR	rR^2
R^3	R^3	rR^2	R^4	I	R	R^2	rR^3	rR^4	r	rR
R^4	R^4	rR	I	R	R^2	R^3	rR^2	rR^3	rR^4	r
rR	rR	R^4	rR^2	rR^3	rR^4	r	I	R	R^2	R^3
rR^2	rR^2	R^3	rR^3	rR^4	r	rR	R^4	I	R	R^2
rR^3	rR^3	R^2	rR^4	r	rR	rR^2	R^3	R^4	I	R
rR^4	rR^4	R	r	rR	rR^2	rR^3	R^2	R^3	R^4	I

E28) नहीं। जैसे कि उदाहरण 13 की संक्रिया सारणी से आप देख सकते हैं कि D_8 में $r_1 \circ R_{90} \neq R_{90} \circ r_1$, क्योंकि $r_4 \neq r_3$.

व्यापक रूप में, $rR = R^{n-1} r \neq Rr$, सिवाय $n = 2$ के लिए।

E29) क्योंकि $A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, इसलिए $A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$.

इसी प्रकार, जाँच कीजिए कि $B^2 = A^2, B^4 = I$ और $BA = -AB = A^3 B$, क्योंकि $-A = (-I)A = A^2 \cdot A = A^3$.

इस प्रकार, $(Q_8, \cdot)$ के लिए सारणी नीचे दिए अनुसार है :

$\bullet$	I	A	A^2	A^3	B	AB	A^2B	A^3B
I	I	A	A^2	A^3	B	AB	A^2B	A^3B
A	A	A^2	A^3	I	AB	A^2B	A^3B	B
A^2	A^2	A^3	I	A	A^2B	A^3B	B	AB
A^3	A^3	I	A	A^2	A^3B	B	AB	A^2B
B	B	A^3B	A^2B	AB	A^2	A	I	A^3
AB	AB	B	A^3B	A^2B	A^3	A^2	A	I
A^2B	A^2B	AB	B	A^3B	I	A^3	A^2	A
A^3B	A^3B	A^2B	AB	B	A	I	A^3	A^2

क्योंकि $BA \neq AB$, इसलिए Q_8 आबेली नहीं है।

साथ ही, Q_8 में 8 अवयव हैं। अतः, $o(Q_8) = 8$.

E30) $\mathbb{M}_{m\times n}(\mathbb{C})^*$ पर संगत अवयवों का गुणन एक सुपरिभाषित संक्रिया है। परंतु, यह $\mathbb{M}_{m\times n}(\mathbb{C})^*$ पर संवृत नहीं है, क्योंकि उदाहरणार्थ,

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in \mathbb{M}_2(\mathbb{C})^*, \text{ परंतु}$$

$$A \cdot B = \begin{bmatrix} 1.0 & 0.1 \\ 0.0 & 0.0 \end{bmatrix} = \mathbf{0} \notin \mathbb{M}_2(\mathbb{C})^*.$$

अतः, $(\mathbb{M}_{m\times n}(\mathbb{C})^*, \cdot)$ एक समूह नहीं है।

E31) ध्यान दीजिए कि $\mathbb{C}$ में $0 = 1 - \zeta^n = (1-\zeta)(1+\zeta+\zeta^2+\cdots+\zeta^{n-1})$.

साथ ही, $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \neq 1$, क्योंकि $n > 1$ है।

अतः, $1+\zeta+\zeta^2+\cdots+\zeta^{n-1} = 0$.

E32) 1 के घनमूल $1, \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}, \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$, अर्थात् $1, \omega, \omega^2$ हैं,

जहाँ $\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{-1}{2} + i\frac{\sqrt{3}}{2} = \frac{-1+i\sqrt{3}}{2}$.

E31 द्वारा, $1+\omega+\omega^2 = 0$. इसलिए, $\omega^2 = -(1+\omega) = \frac{-1-i\sqrt{3}}{2}$.

E33) $U_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$, जहाँ $\zeta = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}$.

इसलिए $(U_6, \cdot)$ के लिए सारणी है :

•	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5
1	1	ζ	ζ^2	ζ^3	ζ^4	ζ^5
ζ	ζ	ζ^2	ζ^3	ζ^4	ζ^5	1
ζ^2	ζ^2	ζ^3	ζ^4	ζ^5	1	ζ
ζ^3	ζ^3	ζ^4	ζ^5	1	ζ	ζ^2
ζ^4	ζ^4	ζ^5	1	ζ	ζ^2	ζ^3
ζ^5	ζ^5	1	ζ	ζ^2	ζ^3	ζ^4

अब, आप जानते हैं कि $D_6 = S_3$. E24 में आपने इस समूह की केली सारणी दी थी। यदि आप इन सारणियों की तुलना करें, तो आप देख सकते हैं कि ऊपर वाली सारणी क्रमविनिमेय संक्रिया के लिए है, जबकि E24 की सारणी ऐसी नहीं है। अतः, $(U_6, \cdot)$ और $(D_6, \circ)$ की संरचनाएं अलग हैं।

E34) $*$ **साहचर्य है:** मान लीजिए $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$ हैं। यह सिद्ध करने के लिए कि
$((a_1, b_1)*(a_2, b_2))*(a_3, b_3) = (a_1, b_1)*((a_2, b_2)*(a_3, b_3))$, अर्थात्
$*$ साहचर्य है, इस तथ्य का उपयोग कीजिए कि $*_1$ और $*_2$ साहचर्य हैं।

$*$ **के सापेक्ष तत्समक अवयव :** $*$ के सापेक्ष तत्समक (e_1, e_2) है, जहाँ e_1 और e_2 क्रमशः G_1 और G_2 के तत्समक हैं। इसका कारण है कि
$(a, b)*(e_1, e_2) = (a *_1 e_1, b *_2 e_2) = (a, b) \ \forall \ (a, b) \in G.$

$*$ **के सापेक्ष प्रतिलोम:** आपको इसकी जाँच करनी चाहिए कि $(x, y) \in G$ का प्रतिलोम (x^{-1}, y^{-1}) है, जहाँ $x *_1 x^{-1} = e_1$, $y *_2 y^{-1} = e_2$.

E35) पहले आइए मान कर चलें कि $G_1 \times G_2$ आबेली है।

अब, किन्हीं $a, c \in G_1$, $b, d \in G_2$ के लिए,

$(a, b)(c, d) = (c, d)(a, b)$, अर्थात् $(ac, bd) = (ca, db)$.

इस प्रकार, $ac = ca$ और $bd = db$.

अतः, G_1 और G_2 आबेली हैं।

आपको इसके विलोम को सिद्ध करना चाहिए। इसके लिए आप ऊपर दिए तर्क के अनुसार विपरीत दिशा में चल सकते हैं।

E36) $(\{0\}, +)$ और $(\mathbb{Z}, +)$ पर विचार कीजिए। तब, $\{0\} \times \mathbb{Z} = \{(0, m) | m \in \mathbb{Z}\}$ अपरिमित है, परंतु $\{0\}$ परिमित है। अतः, $G_1 \times G_2$ अपरिमित होने पर यह आवश्यक नहीं है कि G_1 या G_2 दोनों ही अपरिमित हों।

यदि G_1 या G_2 में से कोई एक अपरिमित है, तो $G_1 \times G_2$ अपरिमित होता है। अतः, $G_1 \times G_2$ के परिमित होने के लिए, दोनों का परिमित होना आवश्यक है।

E37) $U_3 \times S_3 = \{(x, y) | x \in U_3, \ y \in S_3\}$.

अब, $U_3 = \{1, \omega, \omega^2\}$ (E32 को देखिए)।

साथ ही, S_3, E24 में है।

अतः, $|U_3 \times S_3| = 3 \times 6 = 18$, अर्थात्, $o(U_3 \times S_3) = 18$.

हम आपके लिए सारणी को प्रारंभ करेंगे। आप इसे पूरी कीजिए।

$\cdot$	$(1, I)$	$(\omega, (1\ 2))$	$\ldots$
$(1, I)$	$(1, I)$	$(\omega, (1\ 2))$	$\ldots$
$(\omega, (1\ 2))$	$(\omega, (1\ 2))$	(ω^2, I)	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\ldots$

इकाई 3

उपसमूह

इकाई की रूपरेखा **पृष्ठ संख्या**

3.1 प्रस्तावना

अब तक आपने पूर्णांकों की, परिमेय संख्याओं की, वास्तविक संख्याओं की तथा, अंत में, सम्मिश्र संख्याओं की बीजीय संरचनाओं के बारे में कुछ सीखा है। आपने इस ओर ध्यान दिया होगा कि न केवल $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, अपितु इन समुच्चयों में योग की संक्रियाएँ समान हैं। इसी तरह, गुणन की संक्रिया इनमें समान हैं। साथ ही, ये सभी उपसमुच्चय एक ही योग के सापेक्ष समूह हैं। इस इकाई में समूहों के ऐसे ही उपसमुच्चयों पर ही हमारी बात होगी।

भाग 3.2 में आप देखेंगे कि किसी समूह $(G, *)$ के उपसमुच्चयों को जो स्वयं $*$ के सापेक्ष समूह हैं, G के उपसमूह कहलाते हैं। इस भाग में, आप विभिन्न प्रकारों के उपसमूहों के अनेक उदाहरणों का भी अध्ययन करेंगे।

भाग 3.3 में आप समूह के एक उपसमुच्चय पर ऐसे प्रतिबंधों का अध्ययन करेंगे जो यह सुनिश्चित करेंगे कि वह उस समूह का एक उपसमूह है। आपको इन प्रतिबंधों को लागू करने के भी अनेक अवसर प्राप्त होंगे।

अंत में, भाग 3.4 में आप कई ऐसे प्रश्नों के उत्तरों को खोज रहे होंगे, जैसे क्या दो उपसमूहों का सम्मिलन एक उपसमूह होता है? क्या दो उपसमूहों का प्रतिच्छेदन एक उपसमूह होता है? इस भाग में हम समूह के दो उपसमूहों के गुणनफल को भी परिभाषित करेंगे तथा इसकी चर्चा करेंगे कि क्या यह भी एक उपसमूह है या नहीं।

इस इकाई को ध्यान से पढ़िए क्योंकि इसमें मौलिक संकल्पनाओं की बात हो रही है, जिनका इस पाठ्यक्रम के शेष हिस्से में बार-बार उपयोग किया जाएगा। स्वयं अपना मूल्यांकन ज़रूर करें यह सुनिश्चित करने के लिए कि आपने इस इकाई के नीचे दिए अपेक्षित सीखने के उद्देश्यों को प्राप्त कर लिया है। ऐसे करने की एक विधि, जैसा कि हमने अन्य सेमेस्टरों के पाठ्यक्रमों में भी कहा है, यह है कि प्रत्येक प्रश्न को तब ही स्वयं हल करें जब आप उस पर पहुँचते हैं।

उद्देश्य

इस इकाई की पढ़ाई के बाद, आप निम्नलिखित कर सकेंगे:

- समूह के उपसमूह को परिभाषित करना, और उसके उदाहरण देना;
- इसकी जाँच करना कि एक दिए हुए समूह का एक उपसमुच्चय उपसमूह होने के प्रतिबंध को संतुष्ट कर रहा है या नहीं;
- उपसमूहों के प्रतिच्छेदन, सम्मिलन तथा गुणनफल से संबंधित परिणामों को सिद्ध करना और उनको लागू करना।

3.2 उपसमूह क्या होता है?

जैसा कि आप जानते हैं, $\mathbb{Z} \subseteq \mathbb{R}$. साथ ही, $(\mathbb{Z}, +)$ और $(\mathbb{R}, +)$ एक ही तरह से परिभाषित संक्रिया $+$ के सापेक्ष समूह हैं। जैसा कि आप देखेंगे, यह हमें बताता है कि $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ का एक उपसमूह है।

परिभाषा: मान लीजिए कि $(G, *)$ एक समूह है। G का एक अरिक्त उपसमुच्चय H समूह G का एक **उपसमूह (subgoup)** कहलाता है, यदि

i) $a * b \in H \ \forall\ a, b \in H$ अर्थात्, H पर $*$ एक द्वि-आधारी संक्रिया है, तथा

ii) $(H, *)$ एक समूह है।

यदि $(H, *)$, $(G, *)$ का उपसमूह है, तो हम इस तथ्य को, प्रतीकों में, $\mathbf{(H, *) \le (G, *)}$ द्वारा व्यक्त करते हैं।

उदाहरणार्थ, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ और $(\mathbb{C}, +)$, तीनों समूहों का $(\mathbb{Z}, +)$ एक उपसमूह है।

अब इस संकल्पना के बारे में, कुछ टिप्पणियों पर विचार कीजिए।

टिप्पणी 1: उपरोक्त परिभाषा के (ii) के संदर्भ में, $*$ की साहचर्यता पहले से ही तय है, क्योंकि यह G के लिए सत्य है और $H \subseteq G$. अतः, वास्तव में (ii) को पूरा करने के लिए H को इकाई 2 के $G2'$ और $G3'$ (या $G2$ और $G3$) को ही संतुष्ट करने की ज़रूरत है।

टिप्पणी 2: उपसमूह की परिभाषा में ध्यान दीजिए कि H और G दोनों को **एक ही संक्रिया** के सापेक्ष समूह होना चाहिए। उदाहरणार्थ, $\mathbb{Q}^* \subseteq \mathbb{Q}$ तथा $(\mathbb{Q}^*, \cdot)$ एक समूह है। तो क्या $\mathbb{Q}^* \le \mathbb{Q}$? नहीं, क्योंकि $\mathbb{Q}$ योग के सापेक्ष एक समूह है तथा $\mathbb{Q}^*$ योग के सापेक्ष समूह नहीं है। (क्यों?)

अब, आप परिभाषा से इसका सत्यापन कर सकते हैं कि $(\mathbb{Z}, +) \le (\mathbb{Z}, +)$. इसी प्रकार, आप देख सकते हैं कि **किसी भी समूह G के लिए, $(G, *) \le (G, *)$.** इस बात से निम्नलिखित परिभाषा जुड़ी है।

परिभाषा: मान लीजिए कि $(G, *)$ एक समूह है तथा $(H, *) \leq (G, *)$ जहाँ $H \subsetneq G$. तब, H, G का एक **उचित उपसमूह (proper subgroup)** कहलाता है। हम इसे $\mathbf{H < G}$, या $\mathbf{H \lneq G}$, द्वारा व्यक्त करते हैं।

संकेतन के बारे में, हम यहाँ एक महत्वपूर्ण टिप्पणी देना चाहेंगे।

टिप्पणी 3: यदि $(G, *)$ का $(H, *)$ एक उपसमूह है, **तो हम केवल कहेंगे कि G का H एक उपसमूह** है (अगर संबंधित द्वि-आधारी संक्रियाओं के बारे में कोई भ्रम नहीं हो)। हम इस बात को $\mathbf{H \leq G}$ द्वारा भी व्यक्त करेंगे।

यदि G का H एक उपसमूह नहीं है, तो हम इसे $\mathbf{H \nless G}$ द्वारा व्यक्त करेंगे।

आइए कुछ उदाहरणों को विस्तार से देखें।

उदाहरण 1: जाँच कीजिए कि $\mathbb{Z}_O$ और $\mathbb{Z}_E$, $(\mathbb{Z}, +)$ के उपसमूह हैं या नहीं, जहाँ $\mathbb{Z}_O = \{2n+1 | n \in \mathbb{Z}\}$ तथा $\mathbb{Z}_E = \{2n | n \in \mathbb{Z}\}$, अर्थात् $\mathbb{Z}_O$ और $\mathbb{Z}_E$ क्रमशः विषम पूर्णांकों और सम पूर्णांकों के समुच्चय हैं।

हल: पहले तो, ध्यान दीजिए कि $\mathbb{Z}_O$ और $\mathbb{Z}_E$, $\mathbb{Z}$ के अरिक्त उचित उपसमुच्चय हैं। अब, $\mathbb{Z}_O$ पर + को लीजिए। इकाई 2 के E6 में आप देख चुके हैं कि $\mathbb{Z}_O$ पर + एक द्वि-आधारी संक्रिया नहीं है। अतः, $\mathbb{Z}_O \nless \mathbb{Z}$.

अब, $\mathbb{Z}_E$ के संदर्भ में, किन्हीं $n, m \in \mathbb{Z}$ के लिए, $2n + 2m = 2(n+m)$.

अतः, $\mathbb{Z}_E$ पर + एक द्वि-आधारी संक्रिया है।

क्योंकि $\mathbb{Z}$ पर + साहचर्य है, इसलिए यह $\mathbb{Z}_E$ पर भी साहचर्य है।

आगे, + के सापेक्ष $0 \in \mathbb{Z}_E$ तत्समक अवयव है।

साथ ही, $a \in \mathbb{Z}_E$ के लिए, किसी $n \in \mathbb{Z}$ के लिए। $a = 2n$, अतः, $-a = 2(-n) \in \mathbb{Z}_E$.

इस प्रकार, परिभाषा द्वारा, $\mathbb{Z}_E$ उसी संक्रिया के सापेक्ष एक समूह है, जिसके सापेक्ष $\mathbb{Z}$ एक समूह है। अतः, $\mathbb{Z}_E \leq \mathbb{Z}$.

***

उदाहरण 2: दर्शाइए कि $\mathbb{M}_3(\mathbb{Q})$, $\mathbb{M}_3(\mathbb{C})$ का एक उचित उपसमूह है (देखिए उपभाग 2.4.4, इकाई 2)।

हल: पहले तो $\mathbb{M}_3(\mathbb{Q}) \neq \emptyset$ तथा $\mathbb{M}_3(\mathbb{Q}) \subsetneq \mathbb{M}_3(\mathbb{C})$. (क्यों?)

आगे, इकाई 2 से आप जानते हैं कि $\mathbb{M}_3(\mathbb{Q})$ उसी संक्रिया + के सापेक्ष एक समूह है जिसके सापेक्ष $\mathbb{M}_3(\mathbb{C})$ एक समूह है।

अतः, यह $\mathbb{M}_3(\mathbb{C})$ का एक उचित उपसमूह है।

***

उदाहरण 3: दर्शाइए कि $n\mathbb{Z} \leq \mathbb{Z} \ \forall \ n \in \mathbb{Z}$.

हल: ध्यान दीजिए कि $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\} \subseteq \mathbb{Z}$.

अब, किन्हीं $x, y \in n\mathbb{Z}$ $x = nm$ और $y = nr$, किन्हीं $m, r \in \mathbb{Z}$ के लिए।

अतः, $x+y = nm + nr = n(m+r) \in n\mathbb{Z}$, क्योंकि $m+r \in \mathbb{Z}$.

इस प्रकार, $n\mathbb{Z}$ पर + संवृत है।

आगे, $n\mathbb{Z}$ पर + साहचर्य है, क्योंकि यह $\mathbb{Z}$ पर साहचर्य है।

साथ ही, $0 \in n\mathbb{Z}$ योज्य तत्समक है, क्योंकि यह $\mathbb{Z}$ के लिए तत्समक है।

अंत में, $nm \in n\mathbb{Z}$ का योज्य प्रतिलोम $-nm = n(-m) \in n\mathbb{Z}$ है।

इस प्रकार, $(n\mathbb{Z}, +)$ एक समूह है।

अतः, $n\mathbb{Z} \leq \mathbb{Z}$.

***

अब, कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E1) निम्नलिखित में से प्रत्येक के लिए यह जाँच कीजिए कि $H \leq G$ है या नहीं, जहाँ संक्रिया + है :

i) $H = \mathbb{R}, G = \mathbb{C}$;

ii) $H = \{I_3, -I_3, \mathbf{0}\}$, जहाँ $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, तथा $G = \mathbb{M}_3(\mathbb{Z})$;

iii) $H = \{5n \mid n \in \mathbb{Z}\}, G = \mathbb{Z}$;

iv) $H = \mathbb{Z}_n, G = \mathbb{Z}$ (देखिए उपभाग 2.4.1, इकाई 2);

v) $H = \mathbb{M}_{m\times n}(\mathbb{R}), G = \mathbb{M}_{m\times n}(\mathbb{C})$ (देखिए उपभाग 2.4.4, इकाई 2)।

E2) $\bar{2}\mathbb{Z}_8$ और $\mathbb{Z}_8$ के लिए केली सारणियाँ बनाइए। इससे निर्णय लीजिए कि $\bar{2}\mathbb{Z}_8 \leq \mathbb{Z}_8$ है या नहीं। दोनों केली सारणियों में क्या संबंध है?

E3) सिद्ध कीजिए कि आबेली समूह का उपसमूह आबेली होता है।

यहाँ परिमित उपसमूहों तथा संगत केली सारणियों के बारे में एक महत्वपूर्ण टिप्पणी है।

टिप्पणी 4: E2 हल करते समय आपने देखा होगा कि यदि G परिमित है, तथा $H \leq G$, तो $(H, *)$ की केली सारणी $(G, *)$ की केली सारणी की एक उप-सारणी है।

इसी के साथ आइए उपसमूहों पर अपनी यह शुरूआती चर्चा को समाप्त करें। अब हम समूह के किसी उपसमुच्चय पर उन प्रतिबंधों को देखेंगे जिससे पता चलता है कि यह एक उपसमूह है या नहीं। ये प्रतिबंध हमें उपसमूहों के उदाहरण देने में सहायता करेंगे।

3.3 उपसमूह के परीक्षण

E1 को हल करते समय, आपने प्रत्येक स्थिति में चार प्रतिबंधों की जाँच की होगी, जो हैं $-H$ पर $*$ द्वि-आधारी है या नहीं, तथा इकाई 2 के $G1', G2'$ और $G3'$. क्या कोई उपसमुच्चय एक उपसमूह है या नहीं जानने के लिए इससे कोई संक्षिप्त विधि है? हाँ है। नीचे दिया गया एक परिणाम है, जो हमारे कार्य को कुछ कम करने में मदद करेगा।

प्रमेय 1: किसी समूह $(G, *)$ का एक अरिक्त उपसमुच्चय H समूह G का उपसमूह है यदि और केवल यदि

i) H पर $*$ एक द्वि-आधारी संक्रिया है;

ii) $e \in H$, जहाँ G में $*$ के सापेक्ष e तत्समक है;

iii) $\forall\, h \in H$, H में h का प्रतिलोम वही है जो G में h का प्रतिलोम है।

उपपत्ति: पहले, आइए सिद्ध करें कि यदि $H \leq G$, तो ये तीनों प्रतिबंध लागू होते हैं।

अब, यदि $H \leq G$, तो एक उपसमूह की परिभाषा से, प्रतिबंध (i) सत्य है।

(ii) के बारे में, यदि $(G, *)$ का $(H, *)$ एक उपसमूह है, तो क्या $(H, *)$ का तत्समक अवयव $(G, *)$ के तत्समक अवयव से अलग हो सकता है? अभी तक आपने जितने भी उदाहरणों को पढ़ा है, उन सभी में ये समान हैं। परंतु क्या यह केवल एक संयोग है? आइए देखें।

यदि $(H, *)$ का तत्समक h है, तो किसी भी $a \in H$ के लिए, $h * a = a$.

परंतु, $a \in H \subseteq G$. इस प्रकार, $e * a = a$, जहाँ $*$ के सापेक्ष G का तत्समक e है।

अतः, G में, $h * a = e * a$.

$(G, *)$ में दाएँ निरसन से, हम $h = e$ प्राप्त करते हैं।

इस प्रकार, जब भी $(G, *)$ का $(H, *)$ एक उपसमूह है, तब $e \in H$.

(iii) के बारे में, मान लीजिए $h \in H$. क्या $(H, *)$ में इसका प्रतिलोम $(G, *)$ में इसके प्रतिलोम से अलग है? आइए देखें।

मान लीजिए कि $h \in H$ का H में प्रतिलोम x है तथा G में प्रतिलोम y है।

क्योंकि G में $y = h^{-1}$, इसलिए G में $hy = e$.

साथ ही, $hx = e$, (ii) द्वारा।

अतः, $hx = hy$, अर्थात् $x = y = h^{-1}$. अतः, $h^{-1} \in H$, यानी (iii) सत्य है।

अब, आइए विलोम को सिद्ध करें, अर्थात् सिद्ध करें कि यदि (i), (ii) और (iii) सत्य हैं, तो $H \leq G$.

पहले, (i) द्वारा, H पर $*$ एक द्वि-आधारी संक्रिया है।

दूसरे, क्योंकि G पर $*$ साहचर्य है, तथा यही संक्रिया H पर है, इसलिए यह H पर साहचर्य ही रहती है। इस प्रकार, भाग 2.2, इकाई 2 के $G1'$ को H संतुष्ट करता है।

(ii) और (iii) बताते हैं कि $(H, *)$ भाग 2.2, इकाई 2 के $G2'$ और $G3'$ को संतुष्ट करता है।

इस प्रकार, $(H, *)$ एक समूह है।

क्योंकि $H \subseteq G$, इसलिए $(H, *) \le (G, *)$. ■

उपरोक्त परीक्षण में तीनों प्रतिबंधों को वास्तव में एक ही प्रतिबंध के रूप में और संक्षिप्त किया जा सकता है। निम्नलिखित परिणाम में दिए निकष पर विचार कीजिए।

ध्यान दीजिए कि योग की स्थिति में, प्रमेय 2(ii) का प्रतिबंध $a - b \in H \ \forall \ a, b \in H$ बन जाता है।

प्रमेय 2 (उपसमूह परीक्षण): मान लीजिए कि किसी समूह G का H एक **अरिक्त** उपसमुच्चय है। तब, निम्नलिखित कथन समतुल्य हैं:

i) G का H एक उपसमूह है।

ii) जब भी $a, b \in H$, तब $ab^{-1} \in H$.

उपपत्ति: यह सिद्ध करने के लिए कि कथन (i) और (ii) समतुल्य हैं, हमें यह सिद्ध करने की आवश्यकता है कि $(i) \Rightarrow (ii)$ और $(ii) \Rightarrow (i)$.

$\mathbf{(i) \Rightarrow (ii)}$**:** आइए मान लें कि $H \le G$. तब, किन्हीं $a, b \in H$ के लिए, $a, b^{-1} \in H$ है, प्रमेय1(iii) द्वारा।

अतः, $ab^{-1} \in H$, प्रमेय 1(i) द्वारा।

$\mathbf{(ii) \Rightarrow (i)}$**:** क्योंकि $H \ne \emptyset$, इसलिए $\exists \ a \in H$. परंतु तब $aa^{-1} = e \in H$, (ii) द्वारा।

फिर, किसी भी $a \in H$ के लिए, क्योंकि $e \in H$, इसलिए $ea^{-1} = a^{-1} \in H$, (ii) द्वारा।

अंत में, यदि $a, b \in H$, तो $a, b^{-1} \in H$. इस प्रकार, $a(b^{-1})^{-1} = ab \in H$, अर्थात्, H संवृत है G की द्वि-आधारी संक्रिया के सापेक्ष।

अतः, प्रमेय 1 द्वारा, H, G का एक उपसमूह है। ■

प्रमेय 2 में **आवश्यक और पर्याप्त निकष** से हमें अब उपसमूहों के उदाहरणों के देने में सरलता हो जाती है। आइए देखें कैसे, उदाहरण 1 की स्थिति को दोबारा जाँच करें।

उदाहरण 4: इसकी जाँच कीजिए कि सम पूर्णांकों का समुच्चय $\mathbb{Z}_E$, $\mathbb{Z}$ का एक उपसमूह है या नहीं।

ध्यान दीजिए कि $\mathbb{Z}_E = 2\mathbb{Z}$.

हल: सर्वप्रथम, $\mathbb{Z}_E \ne \emptyset$.

आगे, $a, b \in \mathbb{Z}_E$ के लिए, $a = 2n$ और $b = 2m$, है। किन्हीं $n, m \in \mathbb{Z}$ के लिए।

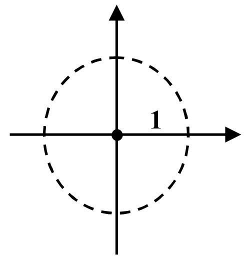
इस प्रकार, $a + (-b) = 2n - 2m = 2(n - m) \in \mathbb{Z}_E$.

अतः, प्रमेय 2 द्वारा, $\mathbb{Z}_E \le \mathbb{Z}$.

***

उदाहरणों 1 और 4 से आप देख सकते हैं कि उपसमूह परीक्षण हमारे जीवन को कितना सरल बना देता है! आइए कुछ और उदाहरण देखें।

उदाहरण 5: समूह $(\mathbb{C}^*, \cdot)$ लीजिए। दर्शाइए कि $S = \{z \in \mathbb{C} \,|\, |z| = 1\}$, $\mathbb{C}^*$ का एक उपसमूह है। (S समतल में **एकक वृत्त (unit circle)** कहलाता है तथा इसे प्रायः $\mathbf{S^1}$ द्वारा दर्शाया जाता है।)



आकृति 1: बिंदुकित वृत्त एकक वृत्त S^1 है।

हल: सर्वप्रथम, $S \neq \emptyset$, क्योंकि $1 \in S$.

साथ ही, किन्हीं $z_1, z_2 \in S$ 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 2 द्वारा, $S \leq \mathbb{C}^*$.

***

उदाहरण 6: दर्शाइए कि $\mathbb{R}$ से $\mathbb{R}$ तक के संतत फलनों का समुच्चय C बिंदशः योग के सापेक्ष $\mathbb{R}$ से $\mathbb{R}$ तक के सभी फलनों के समूह $\mathcal{F}$ का एक उपसमूह है (उदाहरण 6, इकाई 2 देखिए)।

हल: 'कलन' से आप जानते हैं कि $I : \mathbb{R} \to \mathbb{R} : I(x) = x$ एक संतत फलन है। अतः, $I \in C$. इस प्रकार, $C \neq \emptyset$.

आगे, यदि $\mathbb{R}$ पर f संतत है, तो आप 'कलन' से यह जानते हैं कि $\mathbb{R}$ पर $(-f)$ भी संतत है।

अंत में, यदि $f, g \in C$, तो $\mathbb{R}$ पर $f - g$ भी संतत है। अतः, $f - g \in C$.

इस प्रकार, प्रमेय 2 द्वारा, $C \leq \mathcal{F}$.

***

उदाहरण 7: मान लीजिए $G = \mathbb{M}_{2\times 3}(\mathbb{C})$, $\mathbb{C}$ पर सभी 2×3 आव्यूहों का समूह। दर्शाइए कि $S = \left\{ \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} \,\middle|\, a, b, c \in \mathbb{C} \right\}$, $(G, +)$ का एक उपसमूह है।

हल: क्योंकि $\mathbf{0} \in S$, इसलिए $S \neq \emptyset$.

साथ ही, $\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix}, \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} \in S$ के लिए,

$$\begin{bmatrix} 0 & a & b \\ 0 & 0 & c \end{bmatrix} - \begin{bmatrix} 0 & d & e \\ 0 & 0 & f \end{bmatrix} = \begin{bmatrix} 0 & a-d & b-e \\ 0 & 0 & c-f \end{bmatrix} \in S, \text{ क्योंकि } a-d, b-e, c-f \in \mathbb{C}.$$

अतः, प्रमेय 2 द्वारा, $S \leq G$.

***

उदाहरण 8: इकाई 2 के उदाहरण 5 में दिए, $GL_2(\mathbb{R}) = \{A \in \mathbb{M}_2(\mathbb{R}) | \det(A) \neq 0\}$ पर विचार कीजिए।

$SL_2(\mathbb{R})$ को $\mathbb{R}$ पर **कोटि 2 वाला विशिष्ट रैखिक समूह (special linear group)** कहते हैं।

i) दर्शाइए कि $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) | \det(A) = 1\}$, $(GL_2(\mathbb{R}), \cdot)$ का एक उपसमूह है।

ii) अब $H = \{A \in GL_2(\mathbb{R}) | \det(A) = 2\}$ लीजिए। क्या $H \leq GL_2(\mathbb{R})$? क्यों?

हल: i) 2×2 तत्समक आव्यूह $SL_2(\mathbb{R})$ में है क्योंकि $\det\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = 1.$

अतः, $SL_2(\mathbb{R}) \neq \emptyset.$

अब, $A, B \in SL_2(\mathbb{R})$ के लिए,

$\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\dfrac{1}{\det(B)} = 1$, क्योंकि $\det(A) = 1$ है तथा $\det(B) = 1.$

$\therefore \quad AB^{-1} \in SL_2(\mathbb{R}).$

$\therefore \quad SL_2(\mathbb{R}) \leq GL_2(\mathbb{R}).$

ii) क्योंकि $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ का सारणिक 2 है, इसलिए $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \in H.$

$\therefore H \neq \emptyset.$

परंतु, किसी भी $A \in H$ के लिए, $A^{-1} \notin H$, क्योंकि $\det(A^{-1}) = \dfrac{1}{\det(A)} = \dfrac{1}{2}.$

अतः, $H \not\leq GL_2(\mathbb{R}).$

***

अब, E3 में आपने दर्शाया है कि आबेली समूह का प्रत्येक उपसमूह आबेली होता है। अब सवाल है : क्या एक अन्आबेली समूह का प्रत्येक उपसमूह अन्आबेली होता है? ऐसा नहीं है। निम्नलिखित उदाहरण पर विचार कीजिए।

उदाहरण 9: मान लीजिए कि $D = \left\{A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in \mathbb{R}^*\right\}$. दर्शाइए कि $D \leq GL_2(\mathbb{R})$ तथा D आबेली है। इकाई 2 से याद कीजिए कि $GL_2(\mathbb{R})$ अन्आबेली है।

हल: क्योंकि $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in D$, इसलिए $D \neq \emptyset.$

साथ ही, $AI = A \;\forall\; A \in D.$ अतः, I गुणन के सापेक्ष तत्समक है।

आगे, D में $A=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, B=\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$ के लिए,

$AB=\begin{bmatrix} a\alpha & 0 \\ 0 & b\beta \end{bmatrix} \in D$, क्योंकि $a, b, \alpha, \beta \in \mathbb{R}^*$.

साथ ही, यदि $A=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, तो $A^{-1}=\begin{bmatrix} a^{-1} & 0 \\ 0 & b^{-1} \end{bmatrix}$, क्योंकि

$AA^{-1}=\begin{bmatrix} aa^{-1} & 0 \\ 0 & bb^{-1} \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, जो तत्समक है। इस प्रकार, $A^{-1} \in D$.

इसलिए, प्रमेय 1 द्वारा, $D \le GL_2(\mathbb{R})$.

आगे, D में किन्हीं $A=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, B=\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}$ के लिए,

$AB=\begin{bmatrix} a\alpha & 0 \\ 0 & b\beta \end{bmatrix}=\begin{bmatrix} \alpha a & 0 \\ 0 & \beta b \end{bmatrix}=BA.$

इस प्रकार, D एक आबेली समूह है।

***

अब, दो समूहों के अनुलोम गुणनफल पर विचार कीजिए, (उपभाग 2.4.6, इकाई 2) क्या आप सोच सकते हैं कि इसके उपसमूह क्या हो सकते हैं? एक तो ज़ाहिर है, जिसे हम अब दे रहे हैं।

उदाहरण 10: समूहों G_1 और G_2 का अनुलोम गुणनफल $G_1 \times G_2$ लीजिए। दर्शाइए कि $G_1 \times \{e_2\} \le G_1 \times G_2$, जहाँ e_2 है G_2 का तत्समक।

हल: पहले तो $G_1 \times \{e_2\} = \{(a, e_2) | a \in G_1\}$. क्योंकि $G_1 \neq \emptyset$, इसलिए $G_1 \times \{e_2\} \neq \emptyset$.

आगे, मान लीजिए कि $(a, e_2), (b, e_2) \in G_1 \times \{e_2\}$. तब,
$(b, e_2)^{-1} = (b^{-1}, e_2) \in G_1 \times \{e_2\}$, क्योंकि $(b, e_2)(b^{-1}, e_2) = (bb^{-1}, e_2) = (e_1, e_2)$,
जहाँ e_1 है G_1 का तत्समक।

इसलिए, $(a, e_2)(b, e_2)^{-1} = (a, e_2)(b^{-1}, e_2) = (ab^{-1}, e_2) \in G_1 \times \{e_2\}$, क्योंकि $ab^{-1} \in G_1$.

अतः, प्रमेय 2 द्वारा, $G_1 \times \{e_2\} \le G_1 \times G_2$.

***

अब, एक कुछ अलग से उदाहरणों पर विचार कीजिए।

उदाहरण 11: मान लीजिए कि X एक समुच्चय है, तथा X का Y एक अरिक्त उपसमुच्चय है। इकाई 2 के उदाहरण 10 में आपने पढ़ा था कि $(\wp(X), \Delta)$ एक समूह है। दर्शाइए कि $\wp(Y) \le \wp(X)$.

हल: क्योंकि $Y \ne \emptyset$, इसलिए $\wp(Y) \ne \emptyset$.

अब, किसी भी $A \in \wp(Y)$ के लिए, $A \subseteq Y \subseteq X$. अतः, $A \in \wp(X)$. इस प्रकार, $\wp(Y) \subseteq \wp(X)$.

साथ ही, किसी भी $A \in \wp(X)$ के लिए, $A^{-1} = A$, क्योंकि $A \Delta A = \emptyset$.

अतः, $A, B \in \wp(Y)$ के लिए, $AB^{-1} = A \Delta B \subseteq Y$. इस प्रकार, $AB^{-1} \in \wp(Y)$.

अतः, प्रमेय 2 द्वारा, $\wp(Y) \le \wp(X)$.

***

उदाहरण 12: जाँच कीजिए कि $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$, $\mathbb{R}$ का उपसमूह है या नहीं।

हल: पहले तो आप दिखाइए कि $\mathbb{Z}[\sqrt{3}] \ne \emptyset$ और $\mathbb{Z}[\sqrt{3}] \subseteq \mathbb{R}$.

आगे, $\mathbb{Z}[\sqrt{3}]$ में $\alpha = a + b\sqrt{3}$ और $\beta = c + d\sqrt{3}$ के लिए, $\alpha - \beta = (a - c) + (b - d)\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$.

अतः, $\mathbb{Z}[\sqrt{3}] \le \mathbb{R}$.

***

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E4) दर्शाइए कि किसी भी समूह G के दो उपसमूह हैं $\{e\}$ और G. (G का $\{e\}$ **तुच्छ (trivial) उपसमूह** कहलाता है।)

E5) यदि G एक परिमित समूह है तथा $H \le G$, तो $o(H)$ के अधिकतम और न्यूनतम मान क्या हो सकते हैं?

E6) मान लीजिए कि G_1 और G_2 दो समूह हैं। मान लीजिए कि $H \le G_1$ और $K \le G_2$. दर्शाइए कि $H \times K \le G_1 \times G_2$.

E7) दर्शाइए कि $(U_n, \cdot) \le (\mathbb{C}^*, \cdot)$, जहाँ U_n एक के nवें मूलों का समूह है।

E8) दर्शाइए कि अपरिमित समूह $\mathbb{C}^*$ का कोटि n वाला एक परिमित उपसमूह है, प्रत्येक $n \in \mathbb{N}$ के लिए।

E9) पुष्टि करते हुए, निम्नलिखित का एक उदाहरण दीजिए :

i) $\mathbb{M}_{3\times2}(\mathbb{Z})$ का एक उचित अतुच्छ उपसमूह,

ii) $\mathbb{M}_{3\times2}(\mathbb{C})$ का एक उचित उपसमुच्चय, जो एक उपसमूह नहीं है,

iii) $\mathbb{R}$ का एक उचित उपसमूह जो $\mathbb{Q}$ एक उपसमूह नहीं है।

E10) i) मान लीजिए कि G एक समूह है, G का H एक उपसमूह है तथा H का K एक उपसमूह है। क्या K, G का उपसमूह होगा? अपने उत्तर के लिए कारण दीजिए।

E10(i) कहता है कि 'का एक उपसमूह है' संक्रामक है।

ii) मान लीजिए कि G एक समूह है तथा $H \le G$. यदि $K \le G$ s.t. $H \subseteq K$, है, तो क्या $H \le K$? क्यों, या क्यों नहीं?

E11) दर्शाइए कि $\mathcal{F}$ (उदाहरण 6 का) का वह उपसमुच्चय जिसमें $\mathbb{R}$ पर सभी अवकलनीय फलन हैं, $\mathcal{F}$ का एक उपसमूह है।

E12) जाँच कीजिए कि $\mathbb{Z}[\sqrt{6}] \le \mathbb{R}$ या नहीं।

आइए अब किसी भी समूह के एक महत्वपूर्ण उपसमूह की चर्चा करें। आप इस उपसमूह का उपयोग इस पूरे पाठ्यक्रम में बारंबार करेंगे। अतः, आइए इस उपसमूह में अंतर्निहित समुच्चय को परिभाषित करें।

परिभाषा: किसी **समूह** G **का केन्द्र**, जिसे $\mathbf{Z(G)}$ द्वारा व्यक्त किया जाता है, G के उन अवयवों का समुच्चय है जो G के प्रत्येक अवयव से क्रमविनिमय करते हैं। इस प्रकार, $\mathbf{Z(G) = \{g \in G \mid xg = gx\ \forall\ x \in G\}}$.

अक्षर Z, जो केन्द्र को व्यक्त करता है, केन्द्र के लिए जर्मन शब्द 'ज़ेन्ट्रम' 'zentrum' से आया है।

उदाहरणार्थ, यदि G आबेली है, तो $Z(G) = G$, क्योंकि प्रत्येक $g \in G$ प्रत्येक $x \in G$ से क्रमविनिमय करता है।

अब, हम इस देखेंगे कि क्यों प्रत्येक समूह G के लिए $Z(G) \le G$.

प्रमेय 3: किसी भी समूह G का केन्द्र, G का एक उपसमूह होता है।

उपपत्ति: क्योंकि $e \cdot g = g = g \cdot e\ \forall\ g \in G$, इसलिए $e \in Z(G)$. अतः, $Z(G) \ne \emptyset$.

आगे, $a \in Z(G)$.

$\Rightarrow ax = xa\ \forall\ x \in G$

$\Rightarrow a^{-1}ax = a^{-1}xa\ \forall\ x \in G$

$\Rightarrow x = a^{-1}xa\ \forall\ x \in G$, क्योंकि $a^{-1}ax = ex = x$.

$\Rightarrow xa^{-1} = a^{-1}x\ \forall\ x \in G$, समीकरण के दोनों पक्षों को a^{-1} से गुणा करने पर।

$\Rightarrow a^{-1} \in Z(G)$.

साथ ही, किन्हीं $a, b \in Z(G)$ तथा किसी भी $x \in G$ के लिए,

$(ab)x = a(bx) = a(xb)$, क्योंकि $b \in Z(G)$.

$= (ax)b = (xa)b$, क्योंकि $a \in Z(G)$.

$= x(ab)$

$\therefore \quad ab \in Z(G)$.

इस प्रकार, प्रमेय 1 द्वारा, $Z(G)$, G का एक उपसमूह है। ■

ध्यान दीजिए कि प्रमेय 3 को सिद्ध करने के लिए, हमें प्रमेय 1 के प्रत्येक प्रतिबंध को सिद्ध करने की आवश्यकता पड़ी। इस स्थिति में प्रक्रिया को छोटा करने में प्रमेय 2 हमारी सहायता नहीं करती।

आइए समूह के केन्द्र के कुछ उदाहरणों पर विचार करें।

उदाहरण 13: जाँच कीजिए कि $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in Z(G)$ या नहीं, जहाँ $G = GL_2(\mathbb{R})$.

हल: किसी भी $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ के लिए, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} a & 2b \\ c & 2d \end{bmatrix}$, तथा

$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ 2c & 2d \end{bmatrix}$.

अतः, A से $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ केवल तभी क्रमविनिमय करता है, यदि $b = 0 = c$, अर्थात् यदि A एक विकर्ण आव्यूह है। अतः, G के प्रत्येक A के साथ $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ क्रमविनिमय नहीं करता है।

इस प्रकार, $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \notin Z(G)$.

***

उदाहरण 14: $Z(Q_8)$ ज्ञात कीजिए (देखिए E29, इकाई 2)।

हल: उस केली सारणी पर विचार कीजिए, जो आपने E29, इकाई 2 हल करते वक़्त बनाई थी। यदि Q_8 का कोई भी अवयव x, $Z(Q_8)$ में है, तो इसे Q_8 के प्रत्येक अवयव के साथ क्रमविनिमय करना चाहिए। अतः, केली सारणी में शीर्षक x वाले स्तंभ में अवयव ठीक उसी क्रम में होने चाहिए जो शीर्षक x वाली पंक्ति में अवयवों का क्रम है। यह केवल स्थिति $x = I$ और $x = A^2 (= -I)$ में होता है।

अतः, $Z(Q_8) = \{I, -I\}$.

***

समूह के केन्द्रों को प्राप्त करने में कुछ अभ्यास के लिए निम्नलिखित प्रश्नों को हल कीजिए।

E13) i) $Z(S_3)$ और $Z(D_8)$ ज्ञात कीजिए।

(**संकेत:** S_3 और D_8 की संक्रिया सारणियाँ बनाइए।)

ii) किसी परिमित समूह $(G, *)$ की केली सारणी को देखकर ही आप कैसे तय कर सकते हैं कि $Z(G)$ में G का कौनसा अवयव है?

E14) क्या $Z(G)$ एक आबेली समूह है? क्यों, या क्यों नहीं?

E15) सिद्ध कीजिए कि $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$, जहाँ G_1 और G_2 समूह हैं।

अभी तक आपने इसकी जाँच करने के लिए कि कोई उपसमुच्चय एक उपसमूह है या नहीं कुछ परीक्षणों का अनुप्रयोग किया है। जब G एक परिमित समूह है, तब हमें प्रमेय 2 के निकष से एक सरल निकष प्राप्त है यह तय करने के लिए कि G का कोई भी उपसमुच्चय एक उपसमूह है या नहीं। वास्तव में, यह कहता है कि यदि G परिमित है, तो प्रमेय 1 का केवल (i) ही यह निर्णय लेने के लिए काफ़ी है कि G का एक उपसमुच्चय एक उपसमूह है या नहीं।

प्रमेय 4 (परिमित समूहों के लिए उपसमूह परीक्षण): मान लीजिए कि $(G, *)$ एक परिमित समूह है। G का एक अरिक्त उपसमुच्चय H, G का एक उपसमूह होता है यदि और केवल यदि $*$ के सापेक्ष H संवृत हो।

उपपत्ति: यदि $H \le G$, तो परिभाषा द्वारा, $*$ के सापेक्ष H संवृत है।

आइए अब विलोम को सिद्ध करें।

क्योंकि $H \neq \emptyset$. $\exists a \in H$. तब $A = \{a, a^2, \ldots, a^n, \ldots\} \subseteq H$.

क्योंकि G परिमित है, इसलिए H भी परिमित है। अतः, A को परिमित होना चाहिए।

इसलिए, $a^m = a^n$ किन्हीं $m, n \in \mathbb{N}$ के लिए, जहाँ $m \neq n$. …(1)

मान लीजिए कि $m > n$. तब, $a^{m-n} = a^m \cdot a^{-n} = a^n \cdot a^{-n} = e$.

इस प्रकार, $e \in H$.

और, (1) बताता है कि $a^{m-n-1} = a^{m-n} \cdot a^{-1} = e \cdot a^{-1} = a^{-1}$.

इस प्रकार, $a^{-1} \in H$.

अतः, प्रमेय 1 द्वारा, $H \le G$.

ठीक इसी प्रकार आप दर्शा सकते हैं कि $H \le G$, यदि (1) में $n > m$. ■

आइए प्रमेय 4 के एक अनुप्रयोग पर विचार करें, तथा देखें कि यह किस प्रकार हमारे जीवन को सरल बनाती है!

उदाहरण 15: जाँच कीजिए कि $S=\{\overline{0}, \overline{5}, \overline{10}, \overline{15}\}$ और $T=\{\overline{0}, \overline{6}, \overline{12}\}$, $\mathbb{Z}_{20}$ के उपसमूह हैं या नहीं।

हल: आप इसकी जाँच कर सकते हैं कि S के किन्हीं दो अवयवों का योग S में है। अतः, प्रमेय 4 द्वारा, $S \le \mathbb{Z}_{20}$.

आगे, $\overline{6}+\overline{12}=\overline{18} \notin T$. अतः, $T \not\le \mathbb{Z}_{20}$.

***

अब आप कुछ स्थितियों में प्रमेय 4 का अनुप्रयोग कीजिए।

E16) इकाई 2 के उदाहरण 13 में D_8 की केली सारणी पर विचार कीजिए। इससे निर्णय लीजिए कि $\{I, R_{90}, R_{90}^2, R_{90}^3\}$, D_8 का एक उपसमूह है या नहीं।

E17) जाँच कीजिए कि $H=\{I, (1\ 2)\}$ और $K=\{I, (1\ 2\ 3), (1\ 3\ 2)\}$, S_3 के उपसमूह हैं या नहीं (देखिए उपभाग 2.4.2, इकाई 2)।

E18) यह दर्शाने के लिए एक उदाहरण दीजिए कि प्रमेय 4 में दिया निकष अपरिमित समूहों के लिए कार्य नहीं करता है।

E19) मान लीजिए कि ζ एक का एक दसवाँ मूल है। जाँच कीजिए कि $\{1, \zeta^2, \zeta^4, \zeta^8\}$, U_{10} का उपसमूह है या नहीं।

आइए अब उपसमूहों पर कुछ संक्रियाओं की चर्चा करें।

3.4 उपसमूहों पर समुच्चय-संक्रियाएँ

अब हम उपसमूहों के समुच्चय-संक्रियाओं-प्रतिच्छेदन, सम्मिलन और गुणनफल, के अधीन उपसमूहों के व्यवहार की चर्चा करेंगे। आइए, पहले, समूह के किन्हीं दो उपसमूहों के प्रतिच्छेदन पर विचार करें।

कोई भी $m, n \in \mathbb{Z}$ लीजिए। तब, $m\mathbb{Z} \le \mathbb{Z}$ और $n\mathbb{Z} \le \mathbb{Z}$. जैसा कि अब आप देखेंगे, $m\mathbb{Z} \cap n\mathbb{Z}$ भी $\mathbb{Z}$ का उपसमूह है।

प्रमेय 5: यदि H और K समूह G के दो उपसमूह हैं, तो $H \cap K$ भी G का एक उपसमूह होता है।

उपपत्ति : आप जानते हैं कि $e \in H$ और $e \in K$, जहाँ e, G का तत्समक है। इसलिए $e \in H \cap K$. इस प्रकार, $H \cap K \neq \emptyset$.

अब, मान लीजिए कि $a, b \in H \cap K$.

क्योंकि $a, b \in H$ और $H \le G$, इसलिए $ab^{-1} \in H$.

इसी प्रकार, क्योंकि $a, b \in K$ और $K \le G$, इसलिए $ab^{-1} \in K$.

अतः, $ab^{-1} \in H \cap K$.

अतः, प्रमेय 2 द्वारा, $H \cap K$, G का एक उपसमूह है। ■

प्रमेय 5 का पूरा तर्क तब भी मान्य रहता है, जब हम केवल दो उपसमूहों के बदले अनगिनत उपसमूह ले लेते हैं। अतः, हम निम्नलिखित परिणाम प्राप्त करते हैं।

प्रमेय 6: यदि $\{H_i\}_{i \in I}$ किसी समूह G के उपसमूहों का एक समुच्चय हो, जहाँ I एक सूचकांक समुच्चय है, तो $\bigcap_{i \in I} H_i$ भी G का एक उपसमूह होता है। ■

अब, क्या आप सोचते हैं कि दो (या अधिक) उपसमूहों का सम्मिलन पुनः एक उपसमूह होता है? $\mathbb{Z}$ के दो उपसमूहों $2\mathbb{Z}$ और $3\mathbb{Z}$ पर विचार कीजिए। मान लीजिए कि $S = 2\mathbb{Z} \cup 3\mathbb{Z}$. अब, $3 \in 3\mathbb{Z} \subseteq S$ और $2 \in 2\mathbb{Z} \subseteq S$. परंतु $1 = 3 - 2$ न तो $2\mathbb{Z}$ में है और न ही $3\mathbb{Z}$ में। (क्यों?)

अतः, $1 \notin S$. इस प्रकार, S, $(\mathbb{Z}, +)$ का उपसमूह नहीं है।

इस तरह, यदि A और B किसी समूह G के उपसमूह हैं, तो यह **आवश्यक नहीं है** कि **$A \cup B$ भी G का एक उपसमूह हो**। परंतु, यदि $A \subseteq B$ (या $B \subseteq A$), तो $A \cup B = B$ (या $A \cup B = A$ क्रमशः)। तो ऐसी स्थिति में $A \cup B$, G का एक उपसमूह है। E21 बताता है कि केवल इसी स्थिति में $A \cup B$, G का एक उपसमूह होता है। आपको इसे सिद्ध करने, और साथ ही अन्य नीचे दिए प्रश्नों को हल करने, की आवश्यकता है।

E20) $G = \mathbb{M}_{2\times 3}(\mathbb{C})$ लीजिए, तथा मान लीजिए कि S उदाहरण 7 में दिया उपसमूह है। मान लीजिए कि $T = \left\{ \begin{bmatrix} a & b & c \\ 0 & 0 & 0 \end{bmatrix} \middle| a, b, c \in \mathbb{C} \right\}$. दर्शाइए कि $T \le G$, तथा $S \cap T$ ज्ञात कीजिए।

साथ ही, G के इस उपसमूह के दो अलग अतुच्छ अवयव दीजिए, पुष्टि सहित।

E21) मान लीजिए कि A और B एक समूह G के दो उपसमूह हैं। सिद्ध कीजिए कि $A \cup B$, G का एक उपसमूह है iff $A \subseteq B$ या $B \subseteq A$.

(**संकेत:** मान लीजिए कि $A \not\subseteq B$ और $B \not\subseteq A$. $a \in A \setminus B$ तथा $b \in B \setminus A$ लीजिए। तब, दर्शाइए कि $ab \notin A \cup B$. अतः, $A \cup B \not\le G$. ध्यान दीजिए कि इसे सिद्ध करना $\mathbf{A \cup B \le G \Rightarrow A \subseteq B}$ या $\mathbf{B \subseteq A}$ सिद्ध करने के समान है।)

E22) आप जानते हैं कि यदि G एक समूह है तथा $A \le G$ और $B \le G$, तो $A \cap B \le G$. क्या $A^c = G \setminus A$ भी G का एक उपसमूह है? क्या किसी भी समूह G के लिए, $A \Delta B = (A \setminus B) \cup (B \setminus A)$, G का एक उपसमूह है? अपने उत्तरों के लिए कारण दीजिए।

आइए अब देखें कि किसी समूह G के दो उपसमुच्चयों के गुणनफल से हमारा क्या मतलब है।

परिभाषा: मान लीजिए कि G एक समूह है तथा A और B, G के अरिक्त उपसमुच्चय हैं। **A और B का गुणनफल** समुच्चय $\mathbf{AB = \{ab \mid a \in A, b \in B\}}$ होता है।

ध्यान दीजिए कि AB में अवयवों का क्रम महत्वपूर्ण है। AB के अवयव xy के रूप के हैं, जहाँ $x \in A$ और $y \in B$ है। निःसंदेह, यदि G आबेली है, तो $xy = yx$ है। परंतु यदि G आबेली नहीं है, तो हो सकता है कि AB में yx स्थित नहीं हो।

अब, यदि $H \le G$ और $K \le G$ है, तो क्या $HK \le G$ है? आइए कुछ उदाहरणों पर विचार करें, जो हमें इस प्रश्न का उत्तर देने में सहायता कर सकते हैं।

उदाहरण 16: दर्शाइए कि $(2\mathbb{Z})(3\mathbb{Z}) = 6\mathbb{Z} \le \mathbb{Z}$, परंतु $HK \not\le S_3$, जहाँ $H = \{I, (1\ 2)\}$ और $K = \{I, (1\ 3)\}$.

हल: $(2\mathbb{Z})(3\mathbb{Z}) = \{(2m)(3n) \mid m, n \in \mathbb{Z}\}$

$$= \{6mn \mid m, n \in \mathbb{Z}\} \subseteq 6\mathbb{Z}. \qquad \ldots(2)$$

साथ ही, यदि $r \in 6\mathbb{Z}$, तो $r = 6s$, किसी $s \in \mathbb{Z}$ के लिए।

इस प्रकार, $r = (2 \cdot 1)(3s) \in (2\mathbb{Z})(3\mathbb{Z})$.

इस प्रकार, $6\mathbb{Z} \subseteq (2\mathbb{Z})(3\mathbb{Z})$. $\qquad \ldots(3)$

(2) और (3) से, हम प्राप्त करते हैं कि $(2\mathbb{Z})(3\mathbb{Z}) = 6\mathbb{Z}$.

इस प्रकार, इस स्थिति में $\mathbb{Z}$ के दो उपसमूहों $2\mathbb{Z}$ और $3\mathbb{Z}$ का गुणनफल $6\mathbb{Z}$ भी $\mathbb{Z}$ का एक उपसमूह है।

अब, $S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, तथा उसके उपसमूहों $H = \{I, (1\ 2)\}$ और $K = \{I, (1\ 3)\}$, पर विचार कीजिए।

$HK = \{I \circ I, I \circ (1\ 3), (1\ 2) \circ I, (1\ 2) \circ (1\ 3)\}$

$= \{I, (1\ 3), (1\ 2), (1\ 3\ 2)\}$.

अब, $(1\ 3), (1\ 2) \in HK$, परंतु $(1\ 3) \circ (1\ 2) = (1\ 2\ 3) \notin HK$.

अतः, HK, S_3 का एक उपसमूह नहीं है।

***

इस प्रकार, दो उपसमूहों के गुणनफल का एक उपसमूह होना आवश्यक नहीं है। अब प्रश्न उठता है – दो उपसमूहों का गुणनफल कब एक उपसमूह होगा है? निम्नलिखित प्रमेय इस प्रश्न का उत्तर देता है।

प्रमेय 7: मान लीजिए कि H और K समूह G के दो 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 दर्शाएँगे कि $HK = KH$.

मान लीजिए $hk \in HK$. तब, $(hk)^{-1} \in HK$, क्योंकि $HK \leq G$.

अर्थात्, $k^{-1}h^{-1} \in HK$.

इसलिए किसी $h_1 \in H, k_1 \in K$ के लिए, $k^{-1}h^{-1} = h_1k_1$. परंतु तब,
$hk = (k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$.

इस प्रकार, $HK \subseteq KH$. …(4)

अब, मान लीजिए $kh \in KH$. तब, $(kh)^{-1} = h^{-1}k^{-1} \in HK$. परंतु $HK \leq G$.

इसलिए, $((kh)^{-1})^{-1} \in HK$, अर्थात्, $kh \in HK$.

इस प्रकार, $KH \subseteq HK$. …(5)

(4) और (5) को साथ लेने पर, हम पाते हैं $HK = KH$.

विलोमतः, मान लीजिए कि $HK = KH$. हम सिद्ध करेंगे कि $HK \leq G$.

क्योंकि $e = e^2 \in HK$, इसलिए $HK \neq \emptyset$.

अब, मान लीजिए $a, b \in HK$. तब, $a = hk$ और $b = h_1k_1$ किन्हीं $h, h_1 \in H$ और $k, k_1 \in K$ के लिए।

तब, $ab^{-1} = (hk)(k_1^{-1}h_1^{-1}) = h[(kk_1^{-1})h_1^{-1}]$. …(6)

अब, $(kk_1^{-1})h_1^{-1} \in KH = HK$. अतः, $\exists\ h_2k_2 \in HK$ जिससे कि

$(kk_1^{-1})h_1^{-1} = h_2k_2$. …(7)

तब, (6) और (7) से, $ab^{-1} = h(h_2k_2) = (hh_2)k_2 \in HK$, क्योंकि $hh_2 \in H$.

इस प्रकार, प्रमेय 2 द्वारा, $HK \leq G$. ■

चेतावनी: प्रमेय 7 में ध्यान दीजिए कि $HK = KH$ का **अर्थ यह नहीं कि** $hk = kh \ \ \forall\ h \in H$ और $k \in K$.

निम्नलिखित परिणाम प्रमेय 7 का एक अच्छा उपप्रमेय है।

उपप्रमेय 1: यदि H और K एक आबेली समूह G के उपसमूह हैं, तो HK समूह G का एक उपसमूह होता है। ■

निम्नलिखित प्रश्नों को हल करते समय, हम आपको इस उपप्रमेय को सिद्ध करने का अवसर दे रहे हैं E23।

E23) उपप्रमेय 1 को सिद्ध कीजिए।

E24) यदि $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in \mathbb{C} \right\}$ तथा $T = \left\{ \begin{bmatrix} a_1 & a_2 \\ 0 & a_3 \end{bmatrix} \middle| a_1, a_2, a_3 \in \mathbb{C} \right\}$, तो दर्शाइए कि S और T, $\mathbb{M}_2(\mathbb{C})$ के उपसमूह हैं। साथ ही, जाँच कीजिए कि $S \cap T, S \cup T$ और ST भी $\mathbb{M}_2(\mathbb{C})$ के उपसमूह हैं या नहीं।

E25) सिद्ध कीजिए कि एक समूह $(G, *)$ का एक उपसमुच्चय H एक उपसमूह है iff $HH^{-1} = H.$

आपने अभी-अभी देखा कि यदि H और K किसी समूह G के उपसमूह हैं, तो $HK \le G$ केवल तभी जबकि कुछ प्रतिबंध संतुष्ट हों।

अब मान लीजिए कि G परिमित है, तथा $HK \le G$. क्या $o(HK) = o(H)o(K)$?

उदाहरणार्थ, $G = \mathbb{Z}_{30}, H = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24})$ और $K = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \ldots, \overline{28}\}$ लीजिए।

तब, $o(H) = 5, o(K) = 15.$ अतः, $o(H)o(K) = 75 > o(G).$

क्या यह संभव है, क्योंकि $HK \subseteq G$? नहीं। अतः, $o(HK)$ का $o(H)o(K)$ होना ज़रूरी नहीं है। अतः, क्या हम $o(H)$ और $o(K)$ के पदों में $o(HK)$ को लिख सकते हैं? इसका उत्तर निम्नलिखित प्रमेय में दिया है।

प्रमेय 8: मान लीजिए कि G एक परिमित समूह है, तथा $H \le G, K \le G$ ऐसे हैं कि $HK \le G.$ तब, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)}.$

उपपत्ति: पहले, तो $o(HK) \le o(H)o(K),$ क्योंकि $HK = \{hk | h \in H, k \in K\}.$

परंतु, $o(HK)$ को प्राप्त करने के लिए हमें यह जानने की आवश्यकता है कि क्या $hk \in HK$ फिर दोहराया जाता है HK में; और यदि ऐसा है, तो कितनी बार। अतः, हम यह जानना चाहते हैं कि किन प्रतिबंधों के अधीन $hk = h'k',$ जहाँ $h, h' \in H$ और $k, k' \in K, h \ne h', k \ne k'.$

अब, $hk = h'k' \Rightarrow h'^{-1}h = k'k^{-1} = x,$ मान लीजिए।

क्योंकि $x = h'^{-1}h \in H$ और $x = k'k^{-1} \in K,$ इसलिए $x \in H \cap K.$

साथ ही, $h' = hx^{-1}, k' = xk.$

अतः, $hk = (hx^{-1})(xk),$ जहाँ $x \in H \cap K.$

साथ ही, किसी $y \in H \cap K$ के लिए, $hk = (hy^{-1})(yk),$ जहाँ $hy^{-1} \in H, yk \in K.$

अतः, प्रत्येक $hk \in HK,$ $o(H \cap K)$ बार ही HK में दोहराया जाता है।

इसलिए $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)}.$ ■

इस प्रमेय के पहले के उदाहरण पर यदि हम लौटें, अर्थात् $G = \mathbb{Z}_{30}$ पर, तो $H = \bar{6}\mathbb{Z}_{30}$, $K = \bar{2}\mathbb{Z}_{30}$ तथा $H \cap K = H$, क्योंकि $H \subseteq K$. अतः प्रमेय 8 द्वारा,

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)} = \frac{o(H)o(K)}{o(H)} = o(K) = 15.$$

आइए एक और उदाहरण को देखें जो S_n से संबंधित है।

उदाहरण 17: मान लीजिए $H = \{I, (1\ 2\ 3), (1\ 3\ 2)\}$ और $K = \{I, (1\ 2)\}$. जाँच कीजिए कि $HK \leq S_3$ या नहीं। यदि है, तो $o(HK)$ ज्ञात कीजिए। यदि $HK \not\leq S_3$, तो $o(H \cap K)$ ज्ञात कीजिए।

हल: आपको सत्यापित करना चाहिए कि $HK = KH$. अतः, $HK \leq S_3$.

अब, $o(H) = 3$ और $o(K) = 2$. साथ ही, $o(H \cap K) = 1$, क्योंकि केवल I ही दोनों में है।

इस प्रकार $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)} = 6 = o(S_3)$.

ध्यान दीजिए कि $HK \leq S_3$ तथा दोनों की एक ही कोटि है।

अतः, इस स्थिति में $HK = S_3$.

***

अब कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E26) D_{10} लीजिए। जाँच कीजिए कि $HK \leq D_{10}$ या नहीं, जहाँ $H = Z(D_{10})$ तथा $K = \{1, x, x^2, x^3, x^4 \mid x = R_{72}\}$.

यदि यह एक उपसमूह है, तो $o(HK)$ ज्ञात कीजिए।

यदि $HK \not\leq D_{10}$, तो $o(H \cap K)$ ज्ञात कीजिए।

E27) जाँच कीजिए कि $AB \leq S_4$ या नहीं, जहाँ $A = \{I, (1\ 4)\}$ और $B = \{I, (1\ 2)\}$. यदि यह है, तो $o(AB)$ ज्ञात कीजिए। यदि $AB \not\leq S_4$, तो ऐसा $C \leq S_4$ ज्ञात कीजिए जिससे कि $AC \leq S_4$.

इसके साथ, हम उपसमूहों पर संक्रियाओं की अपनी चर्चा को समाप्त करते हैं, तथा हम इस इकाई को भी समाप्त कर रहे हैं। हाँ, यह ज़रूर है कि आप इस खंड में, तथा अगले खंड की अन्य इकाइयों में, और उपसमूहों के बारे में अध्ययन करेंगे। अब आइए देखें कि आपने इस इकाई में किन बातों की पढ़ाई की है।

3.5 सारांश

इस इकाई में, आपने निम्नलिखित बिंदुओं पर अध्ययन किया है।

1. समूह के उपसमूह की परिभाषा, तथा उसके उदाहरण।

2. एक समूह $(G, *)$ का एक अरिक्त समुच्चय H समूह G का एक उपसमूह होता है यदि और केवल यदि

   i) H पर $*$ एक द्वि-आधारी संक्रिया है;

   ii) $e \in H$, जहाँ e, G में $*$ के सापेक्ष तत्समक है;

   iii) $\forall\ h \in H$, H में h का प्रतिलोम वही है जो G में h का प्रतिलोम है।

3. $(G, *)$ का एक अरिक्त समुच्चय H समूह $(G, *)$ का एक उपसमूह होता है iff $a * b^{-1} \in H\ \forall\ a, b \in H.$

4. समूह G के केन्द्र $Z(G)$ की परिभाषा, और उदाहरण। आगे, $Z(G)$ समूह G का एक आबेली उपसमूह है।

5. मान लीजिए कि $(G, *)$ एक परिमित समूह है। G का एक अरिक्त समुच्चय H, G का एक उपसमूह है iff $*$ के सापेक्ष H संवृत है।

6. यदि H और K किसी समूह G के उपसमूह हैं, तो

   i) $H \cap K \leq G;$

   ii) $H \cup K \leq G$ iff $H \subseteq K$ या $K \subseteq H;$

   iii) $HK = \{hk \mid h \in H, k \in K\} \leq G$ iff $HK = KH.$

7. यदि G एक परिमित समूह है, H और K समूह G के ऐसे उपसमूह हैं कि $HK \leq G$, तो $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)}.$

3.6 हल / उत्तर

E1) i) जैसा कि आप जानते हैं, $(\mathbb{R}, +)$ एक समूह है तथा $\mathbb{R} \subseteq \mathbb{C}$. अतः, $(\mathbb{R}, +) \leq (\mathbb{C}, +).$

ii) $G = (\mathbb{M}_3(\mathbb{Z}), +).$ क्योंकि $I_3 \in H$, इसलिए $I_3 + I_3 = 2I_3$ को H में होना चाहिए यदि $H \leq G.$ परंतु $2I_3 \notin H.$ अतः, H पर $+$ एक द्वि-आधारी संक्रिया नहीं है। अतः, $H \not\leq G.$

iii) यहाँ, $H = 5\mathbb{Z}.$ दर्शाइए कि $H \leq G$, जैसा उदाहरण 3 में किया था।

iv) क्योंकि H के अवयव $\mathbb{Z}$ के उपसमुच्चय हैं न कि $\mathbb{Z}$ के अवयव, इसलिए $H \not\subset G.$ अतः, H का G का उपसमूह होने का कोई सवाल ही नहीं है।

v) उपरोक्त (i) की तरह तर्क दीजिए।

E2) $\bar{2}\mathbb{Z}_8 = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$.

$\bar{2}\mathbb{Z}_8$ के लिए सारणी

+	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

$\mathbb{Z}_8$ के लिए सारणी

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$

यह देखने के लिए कि $\bar{2}\mathbb{Z}_8$ क्यों एक समूह है, $\bar{2}\mathbb{Z}_8$ की सारणी देखिए।

ध्यान दीजिए कि $\bar{2}\mathbb{Z}_8$ की सारणी $\mathbb{Z}_8$ की सारणी की वह उपसारणी है जो अवयवों $\bar{0}, \bar{2}, \bar{4}, \bar{6}$ के संगत है। आप इस तथ्य को बड़ी सारणी में केवल $\bar{0}, \bar{2}, \bar{4}, \bar{6}$ शीर्षक वाली पंक्तियों तथा $\bar{0}, \bar{2}, \bar{4}, \bar{6}$ शीर्षक वाले स्तंभों के अवयवों को लेकर, देख सकते हैं।

अतः, $\bar{2}\mathbb{Z}_8 \le \mathbb{Z}_8$.

E3) मान लीजिए कि $H \le G$ है, जहाँ G आबेली है। मान लीजिए कि $a, b \in H$ हैं।

तब, $a, b \in G$ हैं। इसलिए, $ab = ba$ हैं। अतः, H आबेली है।

E4) क्योंकि $G \subseteq G$ तथा G उसी संक्रिया के सापेक्ष एक समूह है जिसके सापेक्ष G समूह है, इसलिए $G \le G$.

क्योंकि $\{e\} \subseteq G$ तथा $\{e\}$ में केवल अवयव e है, इसलिए $e \cdot e^{-1} = e \in \{e\}$.

अतः, $\{e\} \le G$.

E5) मान लीजिए $o(G) = n$. क्योंकि $G \le G$, इसलिए $o(H)$ का अधिकतम मान तब होगा, जब $H = G$. अर्थात् यह अधिकतम मान n है। अतः, $o(H) \in \mathbb{N}$ s.t. $o(H) \le n$.

साथ ही, $\{e\} \le G$ तथा $o(\{e\}) = 1$. अतः, $o(H)$ द्वारा लिए जा सकने वाला न्यूनतम मान 1 है।

E6) क्योंकि H और K समूह G के उपसमूह हैं, इसलिए ये अरिक्त हैं।

अतः, $H \times K \ne \emptyset$.

साथ ही, $(h, k) \in H \times K$ के लिए, $(h, k)^{-1} = (h^{-1}, k^{-1})$.

इसलिए, $(a, b), (c, d) \in H \times K$ के लिए,

$(a, b)(c, d)^{-1} = (a, b)(c^{-1}, d^{-1}) = (ac^{-1}, bd^{-1}) \in H \times K$, क्योंकि $a, c \in H \Rightarrow ac^{-1} \in H$ तथा $b, d \in K \Rightarrow bd^{-1} \in K$.

इस प्रकार, $H \times K \le G_1 \times G_2$.

E7) उपभाग 2.4.5 में आप देख चुके हैं कि $U_n \subseteq \mathbb{C}^*$ तथा $(U_n, \cdot)$ एक समूह है। अतः, $(U_n, \cdot) \le (C^*, \cdot)$.

E8) E7 से, $U_n \le \mathbb{C}^* \ \forall\, n \in \mathbb{N}$. साथ ही, $o(U_n) = n$. इससे परिणाम प्राप्त हो जाता है।

E9) i) $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \\ 0 & 0 \end{bmatrix} \middle|\, a, b \in \mathbb{Z} \right\}$ लीजिए। फिर जाँच कीजिए कि $S \ne \emptyset$. तथा $S \le (\mathbb{M}_{3\times 2}(\mathbb{Z}), +)$.

क्योंकि $\begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \in \mathbb{M}_{3\times 2}(\mathbb{Z}) \setminus S$, इसलिए S एक उचित उपसमूह है। साथ ही, क्योंकि $S \ne \{\mathbf{0}\}$, इसलिए S एक अतुच्छ उपसमूह है।

यह ऐसा एक उदाहरण है। अन्य उदाहरणों को भी खोजिए।

ii) $S = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix} \right\}$ पर विचार कीजिए। तब, $S \subsetneq \mathbb{M}_{3\times 2}(\mathbb{C})$.

क्योंकि $\mathbf{0} \notin S$, इसलिए $S \not\le \mathbb{M}_{3\times 2}(\mathbb{C})$.

ऐसे अनेक उदाहरण हो सकते हैं।

E10) i) क्योंकि $K \le H$, इसलिए $K \ne \emptyset$ तथा $ab^{-1} \in K \ \forall\, a, b \in K$. अतः, प्रमेय 2 द्वारा, $K \le G$.

ii) क्योंकि H और K उसी संक्रिया के सापेक्ष समूह हैं जिसके सापेक्ष G एक समूह है, तथा $H \subseteq K$, इसलिए $H \le K$.

E11) 'कलन' से आप जानते हैं कि $\mathbb{R}$ पर I अवकलनीय है। उदाहरण 6 की तरह तर्क देकर, सिद्ध कीजिए कि यह उपसमुच्चय G का एक उपसमूह है।

E12) $\emptyset \ne \mathbb{Z}[\sqrt{6}] \subseteq \mathbb{R}$, जैसे कि उदाहरण 12 में।

मान लीजिए $\alpha = a + b\sqrt{6}$ और $\beta = c + d\sqrt{6}$, $\mathbb{Z}[\sqrt{6}]$ में हैं।

तब $\alpha - \beta = (a-c) + (b-d)\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$.

$\therefore \mathbb{Z}[\sqrt{6}] \le \mathbb{R}$.

E13) i) E24, इकाई 2, के अपने हल की केली सारणी को देखिए। आप पाएँगे कि S_3 में वह अवयव जिसके शीर्षक वाली पंक्ति में **एक ही क्रम** में वही प्रविष्टियाँ हैं जो उसी अवयव के शीर्षक वाले स्तंभ में प्रविष्टियाँ हैं, केवल I है। अतः, $Z(S_3) = \{I\}$.

उदाहरण 13, इकाई 2, में दी सारणी को देखिए। किन अवयवों के शीर्षक वाली पंक्ति और स्तंभ में प्रविष्टियाँ ठीक एक ही क्रम में हैं? I के लिए ऐसा है, परंतु r_1 के लिए ऐसा नहीं है, क्योंकि, उदाहरणार्थ, $r_1 \circ r_3 \ne r_3 \circ r_1$.

इसी प्रकार, r_2, r_3, r_4 और R_{90} के लिए ऐसा नहीं है।

परंतु R_{180} के लिए है, अर्थात् $R_{180} \circ \sigma = \sigma \circ R_{180}\ \forall\ \sigma \in D_8$.

पुनः R_{270} शीर्षक वाली पंक्ति और स्तंभ में एक ही (समान) प्रविष्टियाँ नहीं हैं, क्योंकि उदाहरणार्थ, R_{270} सममिति r_1 के साथ क्रमविनिमेय नहीं करता है।

अतः, $Z(D_8) = \{I, R_{180}\}$.

ii) उदाहरण 13 और उपरोक्त (i) से आपको कुछ अनुमान लग गया होगा।

अब, $x \in Z(G)$ iff $xg = gx\ \forall\ g \in G$, अर्थात् iff x के संगत पंक्ति की प्रविष्टियाँ ठीक उसी क्रम में हैं जिस क्रम में x के संगत स्तंभ की प्रविष्टियाँ हैं।

E14) मान लीजिए कि $x, y \in Z(G)$.

$xy = yx$, क्योंकि $x \in Z(G)$ और $y \in G$. इस प्रकार, $Z(G)$ आबेली है।

E15) पहले तो ध्यान दीजिए कि $G_1 \times G_2$ के दोनों $Z(G_1 \times G_2)$ और $Z(G_1) \times Z(G_2)$ उपसमूह हैं ($Z(G)$ की परिभाषा और E6 के उपयोग से)।

आगे, $(x, y) \in Z(G_1 \times G_2)$

$\Leftrightarrow (x, y)(a, b) = (a, b)(x, y)\ \forall\ (a, b) \in G_1 \times G_2$

$\Leftrightarrow (xa, yb) = (ax, by)\ \forall\ a \in G_1, b \in G_2$

$\Leftrightarrow xa = ax\ \forall\ a \in G_1$ और $yb = by\ \forall\ b \in G_2$

$\Leftrightarrow x \in Z(G_1)$ और $y \in Z(G_2)$

$\Leftrightarrow (x, y) \in Z(G_1) \times Z(G_2)$

$\therefore Z(G_1 \times G_2) = Z(G_1) \times Z(G_2).$

ध्यान दीजिए कि उपपत्ति के प्रत्येक चरण पर **हमने दो तरफ़ा निहितार्थ (two-way implication) $\Leftrightarrow$ का उपयोग किया है।** इसी कारण से इस तर्क द्वारा हम दोनों समूहों की समानता का निष्कर्ष निकाल सके।

E16) इस सारणी में केवल I, $R_{90}, R_{180}(= R_{90}^2), R_{270}(= R_{90}^3)$ की संगत पंक्तियों और स्तंभों के अवयवों को लेकर एक उपसारणी बनाइए। इन संबंधों के उपयोग से, आपको निम्नलिखित सारणी प्राप्त होगी:

$\circ$	I	R_{90}	R_{90}^2	R_{90}^3
I	I	R_{90}	R_{90}^2	R_{90}^3
R_{90}	R_{90}	R_{90}^2	R_{90}^3	I
R_{90}^2	R_{90}^2	R_{90}^3	I	R_{90}
R_{90}^3	R_{90}^3	I	R_{90}	R_{90}^2

यह सारणी दर्शाती है कि दिया हुआ समुच्चय $\circ$ के सापेक्ष संवृत है।

अतः, प्रमेय 4 द्वारा, $\{I, R_{90}, R_{90}^2, R_{90}^3\} \le D_8$.

E17) E16 की ही तरह, S_3 की उस केली सारणी पर विचार कीजिए, जिसका आपने E13(i) में उपयोग किया था। संबंधित उपसारणियाँ लीजिए। तब, स्पष्ट कीजिए कि $H \le S_3, K \le S_3$ क्यों हैं।

E18) $\mathbb{N} \subseteq (\mathbb{Z}, +)$ पर विचार कीजिए।

$+$ के सापेक्ष $\mathbb{N}$ संवृत है। परंतु, $(\mathbb{N}, +) \not\le (\mathbb{Z}, +)$, क्योंकि $0 \notin \mathbb{N}$.

($\mathbb{N} \not\le \mathbb{Z}$ दर्शाने के लिए आप अन्य कारण भी दे सकते हैं। आप उनको भी क्यों नहीं लिख लेते?)

E19) क्योंकि $\zeta^2 \cdot \zeta^4 = \zeta^6 \notin \{1, \zeta^2, \zeta^4, \zeta^8\}$, इसलिए यह गुणन के सापेक्ष संवृत नहीं है। अतः, यह U_{10} का उपसमूह नहीं है।

E20) आपको इसका सत्यापन करना चाहिए कि $T \ne \emptyset$ तथा $T \le (G, +)$.

स्पष्ट कीजिए कि क्यों $S \cap T = \left\{ \begin{bmatrix} 0 & \alpha & \beta \\ 0 & 0 & 0 \end{bmatrix} \middle| \alpha, \beta \in \mathbb{C} \right\}.$

तब, उदाहरणार्थ, $\alpha = 1, \beta = 0$ तथा $\alpha = 0, \beta = 1$ रख कर, आपको $S \cap T$ के दो शून्येतर अवयव प्राप्त होंगे। स्पष्ट कीजिए कि वे अलग-अलग कैसे हैं।

E21) आप जानते हैं कि यदि $A \subseteq B$ और $B \subseteq A$, तो $A \cup B$ या तो A है या B है, तथा इसी लिए यह G का एक उपसमूह है।

विलोमतः, हम यह मान कर चलेंगे कि $A \not\subset B$ और $B \not\subset A$, तथा निष्कर्ष निकालेंगे कि $A \cup B \not\leq G$.

क्योंकि $A \not\subset B$, $\exists\, a \in A$ s.t. $a \notin B$.

क्योंकि $B \not\subset A$, $\exists\, b \in B$ s.t. $b \notin A$.

अब, यदि $ab \in A$, तो किसी $c \in A$ के लिए $ab = c$.

तब, $b = a^{-1}c \in A$, जो एक अंतर्विरोध है। $\therefore ab \notin A$.

इसी प्रकार, $ab \notin B$.

$\therefore ab \notin A \cup B$.

परंतु, $a \in A \cup B$ और $b \in A \cup B$. अतः, $A \cup B \not\leq G$.

E22) जैसे कि, उदाहरण 15 में दिए $S \leq \mathbb{Z}_{20}$ पर विचार कीजिए। तब, $\overline{3}$ और $\overline{2}$, S^c में हैं, परंतु $\overline{3} + \overline{2} = \overline{5} \notin S^c$. अतः, $S^c \not\leq \mathbb{Z}_{20}$.

क्योंकि, परिभाषा द्वारा, $A \setminus B \not\subset B \setminus A$ तथा $B \setminus A \not\subset A \setminus B$ इसलिए E21 द्वारा, $A \Delta B \not\leq G$.

E23) किसी भी $hk \in HK$ के लिए, $hk = kh \in KH$. अतः, $HK \subseteq KH$. इसी प्रकार, $KH \subseteq HK$. अतः, $HK = KH$. अतः, $HK \leq G$.

E24) उदाहरण 9 की ही तरह, दर्शाइए कि $S \leq \mathbb{M}_2(\mathbb{C})$. इसी प्रकार, यह दर्शाने के लिए कि $T \leq \mathbb{M}_2(\mathbb{C})$ प्रमेय 2 का अनुप्रयोग कीजिए। ध्यान दीजिए कि संक्रिया + है।

प्रमेय 5 द्वारा, $S \cap T \leq G$.

ध्यान दीजिए कि $S \subseteq T$. अतः, $S \cup T = T \leq G$.

अब, $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in S$ और $\begin{bmatrix} a_1 & a_2 \\ 0 & a_3 \end{bmatrix} \in T$ के लिए,

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} a_1 & a_2 \\ 0 & a_3 \end{bmatrix} = \begin{bmatrix} aa_1 & aa_2 \\ 0 & ba_3 \end{bmatrix}.$$

अतः, $ST = \left\{ \begin{bmatrix} aa_1 & aa_2 \\ 0 & \alpha \end{bmatrix} \middle| a, a_1, a_2, \alpha \in \mathbb{C} \right\}$.

साथ ही, जाँच कीजिए कि $TS = \left\{ \begin{bmatrix} \beta & bb_1 \\ 0 & bb_2 \end{bmatrix} \middle| \beta, b, b_1, b_2 \in \mathbb{C} \right\}$.

अब, ST का कोई भी अवयव TS में स्थित है क्योंकि

$$\begin{bmatrix} aa_1 & aa_2 \\ 0 & \alpha \end{bmatrix} = \begin{bmatrix} \beta & aa_2 \\ 0 & a(a^{-1}\alpha) \end{bmatrix},$$ यदि $a \neq 0.$

यदि $a = 0$, तो $\begin{bmatrix} aa_1 & aa_2 \\ 0 & \alpha \end{bmatrix}$, TS में है ही स्थित।

इस प्रकार, $ST \subseteq TS$. इसी प्रकार, दर्शाइए कि $TS \subseteq ST$.

अतः, $ST = TS$, तथा $ST \leq \mathbb{M}_2(\mathbb{C})$.

E25) ध्यान दीजिए कि $HH^{-1} = \{ab^{-1} \mid a, b \in H\}$.

यदि $H \leq G$, तो $ab^{-1} \in H \; \forall \; a, b \in H$. अतः, $HH^{-1} \subseteq H$.

साथ ही,

किसी भी $h \in H$ के लिए, $h = he^{-1} \in HH^{-1}$. अतः, $H \subseteq HH^{-1}$.

इस प्रकार, $HH^{-1} = H$.

विलोमतः, यदि $HH^{-1} = H$, तो $ab^{-1} \in H \; \forall \; a, b \in H$. अतः, $H \leq G$.

E26) क्योंकि $zy = yz \; \forall \; z \in Z(D_{10})$ और $y \in D_{10}$, इसलिए $zx = xz$. अतः, $zx^i = x^i z \; \forall \; i = 2, 3, 4.$

अतः, $HK = KH$.

इस प्रकार, $HK \leq D_{10}$.

अब, $H = \{I\}$. (इसकी जाँच D_{10} के लिए केली सारणी बना कर कीजिए।)

अतः, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)} = \dfrac{1 \times 5}{1} = 5.$

E27) $AB = \{I, (1\ 4), (1\ 2), (1\ 2\ 4)\}$.

परंतु, $(1\ 2) \circ (1\ 4) = (1\ 4\ 2) \notin AB$. इसलिए, $AB \not\leq S_4$.

अब $C = A$ लीजिए।

तब, $AC = A^2 = \{I, (1\ 4)\} \leq S_4$.

इकाई 4

चक्रीय समूह

इकाई की रूपरेखा

पृष्ठ संख्या

4.1 प्रस्तावना

अभी तक आपने समूहों और उपसमूहों के अनेक उदाहरणों का अध्ययन किया है। इस इकाई की पढ़ाई करते समय आप जानेंगे कि इनमें से कुछ ऐसे समूह के उदाहरण हैं, जिसके बारे में यह इकाई हैं, अर्थात् चक्रीय समूह। उदाहरणार्थ, आप जानेंगे कि $\mathbb{Z}_n$ और $\mathbb{Z}$ चक्रीय समूह हैं। वस्तुतः, जैसा कि आप इकाई 8 में सीखेंगे, मौलिक रूप से केवल ये ही चक्रीय समूह हैं। ये समूह कई कारणों के लिए महत्वपूर्ण हैं, जिनमें से एक कारण है कि सभी आबेली समूह इन्हीं चक्रीय समूहों से निर्मित किए जाते हैं।

इकाई 2 में आपने परिमित समूह की कोटि के बारे में सीखा था। भाग 4.2 में, हम इस संकल्पना का उपयोग समूह के अवयव की कोटि की धारणा का परिचय कराने में करेंगे। इसके बाद आप अवयव की कोटि के अनेक उदाहरणों तथा महत्वपूर्ण गुणों का अध्ययन करेंगे। इस भाग में हम एक चक्रीय समूह को भी परिभाषित करेंगे, तथा आप ऐसे समूह के अनेक उदाहरणों को भी जानेंगे।

भाग 4.3 में आप परिमित और अपरिमित चक्रीय समूहों के अनेक महत्वपूर्ण गुणों का अध्ययन करेंगे। आप यह भी देखेंगे कि प्रत्येक चक्रीय समूह आबेली क्यों होता है। साथ ही, इस भाग में आप देखेंगे कि $\mathbb{Z}$ का कोई भी उपसमूह, किसी $m \in \mathbb{Z}$ के लिए, $m\mathbb{Z}$ के रूप का क्यों

होता है। साथ ही, आप यह भी देखेंगे कि $n \in \mathbb{N}$ के लिए, $\mathbb{Z}_n$ या U_n जैसे किसी समूह के सभी उपसमूह किस प्रकार प्राप्त किए जाते हैं।

अंत में, भाग 4.4 में हम चक्रीय समूह के एक जनक का विस्तार एक जनक समुच्चय की धारणा तक करेंगे। आप देखेंगे कि विभिन्न गणनांक वाले अनेक अलग-अलग समुच्चय एक ही समूह जनित कर सकते हैं।

अब आइए उन विशिष्ट सीखने के उद्देश्यों की सूची दें, जिनको केंद्र में रखकर यह इकाई बनाई गई है।

उद्देश्य

इस इकाई की पढ़ाई के बाद, आप निम्नलिखित करने में समर्थ हो जाएँगे:

- समूह के अवयव की कोटि को परिभाषित करना, तथा उसके उदाहरण देना;
- समूह के एक अवयव की कोटि तथा उस अवयव की पूर्णांकीय घातों की कोटि के बीच संबंधों को सिद्ध करना, और उनका उपयोग करना;
- स्पष्ट करना कि चक्रीय समूह क्या है, तथा ऐसे समूह के उदाहरण देना;
- चक्रीय समूह का प्रत्येक उपसमूह चक्रीय होता है – इस कथन को सिद्ध करना तथा उसका अनुप्रयोग करना;
- परिमित चक्रीय समूह के सभी उपसमूह प्राप्त करना;
- समूह के एक जनक समुच्चय को परिभाषित करना, तथा उसके उदाहरण देना।

4.2 अवयव की कोटि

इकाई 2 में आपने परिमित और अपरिमित समूहों के बारे में सीखा है। आप यह भी जानते हैं कि एक परिमित समूह की कोटि क्या होती है। उदाहरणार्थ, $n \in \mathbb{N}$ के लिए, $o(D_{2n}) = 2n$, तथा $o(S_n) = n!$. यहाँ, हम इस पर चर्चा करेंगे कि किसी समूह के अवयव की कोटि क्या होती है। जैसा कि आप देखेंगे, यह उस समूह की कोटि होती है, जो इस अवयव द्वारा 'निर्मित' होता है।

इकाई 3 से याद कीजिए कि $m \in \mathbb{Z}$ के लिए, $m\mathbb{Z} = \{0, \pm m, \pm 2m, \ldots\}$ समूह $\mathbb{Z}$ का एक उपसमूह है। अब, यदि $H \le \mathbb{Z}$ s.t. $m \in H$, तो आपके हिसाब से $m\mathbb{Z}$ और H किस तरह संबद्ध होंगे? क्या आप यह जान कर हैरान हैं कि $m\mathbb{Z} \subseteq H$?

आप जानते हैं कि यदि $m \in H$, तो $-m \in H$. इसलिए, $2m, 3m, \ldots$ तथा $-2m, -3m, \ldots$ भी H में हैं। इस प्रकार, $m\mathbb{Z} \subseteq H$.

अतः, $m\mathbb{Z}$ समूह $\mathbb{Z}$ के ऐसे प्रत्येक उपसमूह में आविष्ट है, जिसमें m आविष्ट है। इस तरह, $m\mathbb{Z}$, m को आविष्ट करने वाला $\mathbb{Z}$ का सबसे छोटा (यानी न्यूनतम) उपसमूह है।

जो आपने ऊपर देखा है, वह केवल $\mathbb{Z}$ के लिए ही सत्य नहीं है। यह किसी भी समूह के लिए सत्य है, जैसा कि अब हम सिद्ध करेंगे।

प्रमेय 1: मान लीजिए कि G एक समूह है तथा $a \in G$. तब,

$A = \{a^0, a^1, a^{-1}, a^2, a^{-2}, \ldots\} = \{a^n \mid n \in \mathbb{Z}\}$, a को आविष्ट करने वाला G का सबसे छोटा उपसमूह है।

उपपत्ति: आइए पहले दर्शाएँ कि $A \leq G$.

क्योंकि G पर संक्रिया G में साहचर्य है, इसलिए यह A में साहचर्य है।

क्योंकि $a^0 = e$, इसलिए $e \in A$.

प्रत्येक $a^n \in A$ के लिए, $\exists\, a^{-n} \in A$ s.t. $a^n a^{-n} = e$.

अतः, इकाई 3 के उपसमूह निकष द्वारा, $A \leq G$.

आगे, मान लीजिए कि H अवयव a को आविष्ट करने वाला G का कोई उपसमूह है।

क्योंकि $a \in H$ और H एक समूह है, इसलिए $a^n \in H \ \forall\ n \in \mathbb{N}$.

इसी प्रकार, क्योंकि $a^n \in H$ और H एक समूह है, इसलिए $a^{-n} \in H \ \forall\ n \in \mathbb{N}$.

साथ ही, $e \in H$, क्योंकि $H \leq G$. अर्थात्, $a^0 \in H$.

अतः, $A \subseteq H$.

इस प्रकार, A समूह G के ऐसे प्रत्येक उपसमूह में आविष्ट है, जिसमें a आविष्ट है।

अतः, A, G का ऐसा न्यूनतम उपसमूह है, जिसमें a आविष्ट है। ■

प्रमेय 1 हमें निम्नलिखित परिभाषाओं की ओर ले जाता है।

परिभाषाएँ: मान लीजिए कि G एक समूह है तथा $a \in G$.

i) a को आविष्ट करने वाला G का सबसे छोटा उपसमूह **a द्वारा जनित G का चक्रीय उपसमूह** कहलाता है, तथा इसे $<\mathbf{a}>$ द्वारा व्यक्त किया जाता है।

ii) यदि किसी $a \in G$ के लिए, $G = <a>$, तो G एक **चक्रीय समूह (cyclic group)** कहलाता है।

iii) a समूह $<\mathbf{a}>$ का **एक जनक (generator)** कहलाता है।

iv) यदि $<a>$ परिमित है, तो **अवयव a की कोटि** समूह $<\mathbf{a}>$ की कोटि है। यदि $<a>$ अपरिमित है, तो **a की कोटि अपरिमित होती है।**

इन दोनों स्थितियों में a की कोटि को **o(a)** से दर्शाते हैं।

उदाहरणार्थ, $0 \in \mathbb{Z}$ द्वारा जनित $\mathbb{Z}$ का चक्रीय उपसमूह $\{0\}$ है, क्योंकि $n \cdot 0 = 0 \ \forall\ n \in \mathbb{Z}$.

इस प्रकार, $o(0) = o(\{0\}) = 1$.

इसी तरह, किसी भी समूह G के लिए, $\mathbf{o(e) = o(\{e\}) = 1.}$

साथ ही, ध्यान दीजिए कि $\mathbb{Z}$ में, $<1> = \{n \cdot 1 | n \in \mathbb{Z}\} = \{n | n \in \mathbb{Z}\} = \mathbb{Z}.$

इस प्रकार, $\mathbb{Z} = <1>$, अर्थात् **$\mathbb{Z}$ एक चक्रीय समूह है।** इससे यह भी मालूम होता है कि **$1 \in \mathbb{Z}$ की कोटि अपरिमित है।**

इसी प्रकार, $2 \in \mathbb{Z}$ के लिए, $<2> = \{2n | n \in \mathbb{Z}\}$, जिससे कि 2 की कोटि अपरिमित है। वस्तुतः, **किसी भी शून्येतर पूर्णांक की कोटि अपरिमित होती है।**

आइए अब समूह के अवयवों की कोटियों को मालूम करने के कुछ और उदाहरणों को देखें।

उदाहरण 1: निम्नलिखित की कोटि ज्ञात कीजिएः

i) $\mathbb{Z}_5$ में $\overline{3}$, तथा

ii) $\mathbb{Z}_9$ में $\overline{3}$.

हल: प्रत्येक स्थिति में, $<\overline{3}> = \{0, \pm\overline{3}, \pm 2\cdot\overline{3}, \pm 3\cdot\overline{3}, \ldots\}$ है।

i) यहाँ $\mathbb{Z}_5$ में $2\cdot\overline{3} = \overline{6} = \overline{1}$ तथा $\mathbb{Z}_5$ में $-\overline{3} = \overline{5-3} = \overline{2}$, जैसा कि आप भाग 2.4, इकाई 2 से जानते हैं।

इसी प्रकार, $(-2)\overline{3} = -\overline{6} = \overline{4}$, इत्यादि।

आप इसकी जाँच कर सकते हैं कि $<\overline{3}> = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \mathbb{Z}_5$.

इस प्रकार, **$\mathbb{Z}_5$ को $\overline{3}$ जनित करता है।** इसलिए, $\overline{3}$ की कोटि है $o(\overline{3}) = o(\mathbb{Z}_5) = 5.$

साथ ही, इस ओर भी ध्यान दीजिए कि $\mathbb{Z}_5$ एक चक्रीय समूह है।

ii) यहाँ, $-\overline{3} = \overline{6}, 2\cdot\overline{3} = \overline{6}, (-2)\overline{3} = -\overline{6} = \overline{3}, 3\cdot\overline{3} = \overline{0}, -3\cdot\overline{3} = \overline{0}, 4\cdot\overline{3} = \overline{3}, -4\cdot\overline{3} = -\overline{3} = \overline{6}$, इत्यादि।

जैसे जैसे आप $<\overline{3}>$ के सभी अवयवों को ज्ञात करेंगे वैसे वैसे आप देखेंगे कि अवयव $\pm n\cdot\overline{3}$ वापस $\{\overline{0}, \overline{3}, \overline{6}\}$ में से कोई एक आता रहता है।

अतः, यहाँ $<\overline{3}> = \{\overline{0}, \overline{3}, \overline{6}\}$.

इसलिए, $o(\overline{3}) = 3.$

***

अब, उदाहरण 1 के (i) में $\overline{3}$ पर विचार कीजिए। यदि आप $\overline{3}, 2\cdot\overline{3}, \ldots,$ अभिकलित करेंगे, तो आप देखेंगे कि $o(\overline{3}) = 5$ ऐसा न्यूनतम धनात्मक पूर्णांक n है जिसके लिए $n\cdot\overline{3} = \overline{0}$. यह बात व्यापक रूप में सत्य है, जैसा कि अब आप देखेंगे।

प्रमेय 2: मान लीजिए कि G एक समूह है तथा $g \in G$.

i) यदि $o(g)$ परिमित है, तो $o(g)$ ही वह न्यूनतम धनात्मक पूर्णांक n है जिससे कि $g^n = e$. (ध्यान दीजिए कि यदि $g \in (G, +)$, तो $o(g)$ वह न्यूनतम धनात्मक पूर्णांक n है जिससे कि $ng = e$.)

$o(g) = 1$ यदि और केवल यदि $g = e$.

ii) यदि $o(g)$ परिमित है तथा $s \in \mathbb{Z}$ s.t. $g^s = e$, तो $o(g) \mid s$.

iii) यदि $o(g)$ अपरिमित है, तो $g^m \neq g^n$, यदि $m \neq n$, जहाँ $m, n \in \mathbb{Z}$.

उपपत्ति: ध्यान दीजिए कि $o(g) = o(< g >)$, जहाँ $< g > = \{e, g^{\pm 1}, g^{\pm 2}, \ldots\}$.

i) यहाँ $g \in G$ की कोटि परिमित है। इसलिए, समुच्चय $\{e, g, g^2, \ldots\}$ परिमित है। अतः, g की सभी घातें अलग-अलग नहीं हो सकती हैं। अतः, किसी $r > s$ के लिए, $g^r = g^s$. तब, $g^{r-s} = e$, तथा $r - s \in \mathbb{N}$.

इस प्रकार, समुच्चय $T = \{t \in \mathbb{N} \mid g^t = e\}$ अरिक्त है। इसलिए, सुक्रमण सिद्धांत द्वारा (देखिए भाग 1.2, इकाई 1), T का एक न्यूनतम अवयव, मान लीजिए n, है।

तब, $g^n = e$. …(1)

मान लीजिए कि $A = \{e, g, g^2, \ldots, g^{n-1}\}$.

तब, $A \subseteq < g >$. …(2)

साथ ही, किसी भी $m \in \mathbb{Z}^*$ के लिए, विभाजन ऐल्गोरिद्म द्वारा $m = qn + r$ किन्हीं $q, r \in \mathbb{Z}$, के लिए, $0 \le r < n$.

तब, $g^m = (g^n)^q \cdot g^r = g^r$, किसी r के लिए $0 \le r < n$, (1) द्वारा।

अतः, $g^m \in A$.

इसलिए, $< g > \subseteq A$. …(3)

(2) और (3) द्वारा, $< g > = \{e, g, \ldots, g^{n-1}\}$.

अतः, $o(g) = o(< g >) = n$, जो ऐसा **न्यूनतम** धनात्मक पूर्णांक है जिससे कि $g^n = e$.

ii) मान लीजिए कि $o(g) = n$ और $g^s = e$, किसी $s \in \mathbb{Z}$ के लिए। विभाजन ऐल्गोरिद्म द्वारा, $\exists\, q, r \in \mathbb{Z}$ s.t. $s = qn + r$, $0 \le r < n$.

तब, $g^s = e \Rightarrow g^{qn} \cdot g^r = e \Rightarrow g^r = e$.

परंतु, n वह न्यूनतम धनात्मक पूर्णांक है s.t. $g^n = e$.

अतः r के लिए केवल एक ही संभावना है, $r = 0$.

तब, $s = qn$, अर्थात् $n \mid s$.

iii) मान लीजिए कि $g \in G$ अपरिमित कोटि का है। मान लीजिए कि $m, n \in \mathbb{Z}$ s.t. $m \neq n$.

अब, अगर संभव है, तो मान लीजिए कि $g^m = g^n$. तब, $g^{m-n} = e$. तब, जैसे कि ऊपर (i) में था, यह दिखाता है कि $< g >$ एक परिमित समूह है, जो इस परिकल्पना का अंतर्विरोध है कि g की कोटि अपरिमित है।

अतः, यदि $m \neq n$, तो $g^m \neq g^n$.

तो आइए अब देखें कि प्रमेय 2 हमारे लिए क्या कुछ सरल बनाता है!

उदाहरण 2: $\mathbb{Z}_9$ में $\overline{3}$ की कोटि ज्ञात कीजिए।

हल: उदाहरण 1(ii) में एक पैटर्न मालूम करने से पहले, आपको $n \in \mathbb{Z}$ के अनेक मानों के लिए, $n \cdot \overline{3}$ को परिकलित करना पड़ा था। परंतु, अब आप देख सकते हैं कि $1 \cdot \overline{3} = \overline{3},\ 2 \cdot \overline{3} = \overline{6},\ 3 \cdot \overline{3} = \overline{9} = \overline{0}.$

अतः, प्रमेय 2 के उपयोग से, $\mathbb{Z}_9$ में $o(\overline{3}) = 3.$

***

उदाहरण 3: S_5 में $(1\ 2)$ और $(1\ 2\ 3)$ की कोटियाँ ज्ञात कीजिए।

हल: याद कीजिए कि $(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq I.$ है।

आगे, $(1\ 2)^2 = (1\ 2) \circ (1\ 2) = I.$

$\therefore\ o((1\ 2)) = 2.$

इसी प्रकार, आपको दिखाना चाहिए कि $o((1\ 2\ 3)) = 3.$

***

उपरोक्त उदाहरण से जुड़ा निम्नलिखित प्रेक्षण पर विचार कीजिए।

टिप्पणी 1: इकाई 9 में आप देखेंगे कि लंबाई n के किसी भी चक्र की कोटि n होती है, जहाँ $n \in \mathbb{N}$.

अब कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E1) निम्नलिखित की कोटियाँ ज्ञात कीजिए :

i) D_8 में R_{90} और R_{180}, ii) Q_8 में $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$,

iii) $\mathbb{Z}_{10}$ में $\overline{1}$, iv) $\mathbb{Z}_n$ में $\overline{1}$ किसी $n \in \mathbb{N}$ के लिए,

v) $(-5) \in \mathbb{Z}$, vi) $\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix} \in \mathbb{M}_2(\mathbb{Z})$.

E2) दर्शाइए कि यदि $H \leq G, H \neq \{e\}$, तो $H \neq <e>$.

E3) दर्शाइए कि एक समूह G में किसी भी a के लिए, $<a> = <a^{-1}>$.

E3 हमें बताता है कि चक्रीय उपसमूह का एक अद्वितीय जनक नहीं होता है।

E4) दर्शाइए कि यदि G एक समूह है और $a \in G$, तो $<a> = \cap\{H \mid H \leq G$ और $a \in H\}$.

E5) सिद्ध कीजिए कि $\mathbb{Z}_n = <\overline{1}> \;\forall\; n \in \mathbb{N}$.

E6) $A \in \mathbb{M}_{2\times 3}(\mathbb{R}), A \neq \mathbf{0}$ के लिए, $o(A)$ ज्ञात कीजिए।

E7) $o(A)$ ज्ञात कीजिए, जहाँ $A = \begin{bmatrix} 0 & r \\ 1 & 0 \end{bmatrix} \in GL_2(\mathbb{R})$.

E8) मान लीजिए कि S एक अरिक्त समुच्चय है। $A \in \wp(S)$ की कोटि ज्ञात कीजिए (देखिए उदाहरण 10, इकाई 2)।

आइए अब अवयव की कोटि के कुछ गुणों पर दृष्टि डालें। पहले गुण के एक उदाहरण के रूप में, कोई $\overline{x} \in \mathbb{Z}_5$ पर विचार कीजिए। अब, $n \cdot \overline{x} = n(\overline{m} + \overline{x} - \overline{m})$, किसी भी $\overline{m} \in \mathbb{Z}_5$ के लिए। अतः, यदि $r = o(\overline{x})$, तो $r = o(\overline{m} + \overline{x} - \overline{m})$ भी। वस्तुतः, यह केवल $\mathbb{Z}_5$ के लिए ही सत्य नहीं है, अपितु किसी भी समूह के लिए सत्य है, जैसे कि आप अब देखेंगे।

प्रमेय 3: मान लीजिए कि G एक समूह है। $a \in G$ की कोटि और gag^{-1} की कोटि, किसी भी $g \in G$ के लिए, समान हैं।

gag^{-1}, **g** द्वारा **a** का **संयुग्मी (conjugate)** कहलाता है।

उपपत्ति: पहले तो ध्यान दीजिए कि $ga^ng^{-1} = (gag^{-1})^n \;\forall\; g \in G$ और $n \in \mathbb{Z}$. (क्यों?)। अब दो स्थितियाँ हैं – $o(a)$ परिमित है, या $o(a)$ अपरिमित है।

स्थिति 1: मान लीजिए कि $o(a)$ परिमित, अर्थात् m है। तब, m न्यूनतम धनात्मक पूर्णांक है s.t. $a^m = e$.

अतः, $ga^mg^{-1} = gg^{-1} = e$. इसलिए, $(gag^{-1})^m = e$.

अतः, $o(gag^{-1})$ भी परिमित है। मान लीजिए कि $o(gag^{-1}) = r$.

तब, प्रमेय 2(ii) द्वारा,

$r \mid m$. …(4)

इसी प्रकार, क्योंकि $(gag^{-1})^r = e$, इसलिए $ga^rg^{-1} = e$, अर्थात् $a^r = e$.

अतः, $m \mid r$. …(5)

(4) और (5) द्वारा, $r = \pm m$. परंतु r और m दोनों धनात्मक हैं।

अतः, $r = m$.

इस प्रकार, $o(gag^{-1}) = o(a)$, किसी भी $g \in G$ के लिए।

स्थिति 2: मान लीजिए कि $o(a)$ अपरिमित है। तब, किसी भी $n \in \mathbb{N}$ के लिए, $a^n \neq e$. अतः, $(gag^{-1})^n \neq e$, किसी भी $n \in \mathbb{N}$ के लिए।

इस प्रकार, $o(gag^{-1})$ भी अपरिमित है, जैसा कि $o(a)$ है। ■

आइए प्रमेय 3 का एक तत्काल अनुप्रयोग देखें। आप जानते हैं कि $(1\ \ 2\ldots n) \in S_n$.

टिप्पणी 1 द्वारा, $n = o((1\ \ 2\ldots n))$. अतः, प्रमेय 3 द्वारा,

$o(\sigma(1\,2\ldots n)\sigma^{-1}) = n$ किसी भी $\sigma \in S_m$ के लिए, जहाँ $m \geq n$. आप इस परिणाम का इकाई 9 में अनेक बार उपयोग करेंगे।

अब, आइए एक अन्य गुण पर दृष्टि डालें। आप पहले देख चुके हैं कि $\mathbb{Z} = \langle 1 \rangle$, जिससे कि $o(1)$ अपरिमित है। वस्तुतः, $o(n)$ अपरिमित है $\forall\ n \in \mathbb{Z}^*$.

इससे शायद आप सोचें कि किसी भी समूह G और $g \in G$ के लिए, $o(g) = o(g^r)$, $r \in \mathbb{Z}$ के लिए।

परंतु, अगर $\mathbb{Z}_{12}$ लें, तो $o(\bar{1}) = 12$. परंतु, $o(\bar{4}) \neq 12$. वस्तुतः, $o(\bar{4}) = 3$, जैसा कि आप सत्यापन कर सकते हैं।

अतः, सवाल उठता है – जब $o(g)$ परिमित है, तब क्या $o(g^r)$ और $o(g)$ संबद्ध हैं? आइए देखें।

प्रमेय 4: मान लीजिए कि G एक समूह है तथा $g \in G$.

i) यदि g अपरिमित कोटि का है, तो प्रत्येक $m \in \mathbb{Z}^*$ के लिए, g^m भी अपरिमित कोटि का होता है।

ii) यदि $o(g) = n$, तो $o(g^m) = \dfrac{n}{(n,\ m)}\ \forall\ m = 1, \ldots, n-1$ है। (याद कीजिए कि $(n,\ m)$, n और m का g.c.d है।)

उपपत्ति: i) कोई अवयव अपरिमित कोटि का है यदि और केवल यदि उसकी सभी घातें अलग-अलग होती हैं। हम जानते हैं कि g की सभी घातें भिन्न-भिन्न हैं। हमें यह दर्शाना है कि g^m की सभी घातें भिन्न-भिन्न हैं, जहाँ $m \in \mathbb{Z}^*$.

यदि संभव है तो, मान लीजिए कि किन्हीं $t, w \in \mathbb{Z}$ के लिए, $(g^m)^t = (g^m)^w$.

तब, $g^{mt} = g^{mw}$.

परंतु, तब प्रमेय 2 द्वारा, $mt = mw$, क्योंकि g अपरिमित कोटि का है। अतः, $t = w$.

यह बताता है कि g^m की सभी घातें भिन्न-भिन्न हैं, और इसी कारण g^m अपरिमित कोटि का है।

ii) क्योंकि $o(g) = n$, इसलिए $< g > = \{e, g, \ldots, g^{n-1}\}$. अब, $< g^m >$ समूह $< g >$ का एक उपसमूह है, और इसी लिए इसे परिमित कोटि का होना चाहिए।

इस प्रकार, g^m परिमित कोटि का है।

मान लीजिए कि $o(g^m) = t$. हम दर्शाएँगे कि $t = \dfrac{n}{(n, m)}$.

अब, $g^{mt} = (g^m)^t = e$.

अतः, प्रमेय 2(ii) द्वारा, $n \mid mt$. …(6)

मान लीजिए कि $d = (n, m)$. तब, हम $n = n_1 d$ और $m = m_1 d$ लिख सकते हैं, जहाँ $(m_1, n_1) = 1$.

तब, $n_1 = \dfrac{n}{d} = \dfrac{n}{(n, m)}$.

(6) द्वारा, $n \mid tm_1 d \Rightarrow n_1 d \mid tm_1 d \Rightarrow n_1 \mid tm_1$.

परंतु $(n_1, m_1) = 1$.

अतः, $n_1 \mid t$, जैसा कि आपने इकाई 1 में सीखा है। …(7)

साथ ही, $(g^m)^{n_1} = g^{m_1 d n_1} = g^{m_1 n} = (g^n)^{m_1} = e^{m_1} = e$.

इस प्रकार, $o(g^m)$ की परिभाषा तथा प्रमेय 2 द्वारा, हम प्राप्त करते हैं कि

$t \mid n_1$. …(8)

(7) और (8) दर्शाते हैं कि $t = n_1 = \dfrac{n}{(n, m)}$.

अर्थात्, $o(g^m) = \dfrac{n}{(n, m)}$. ■

प्रमेय 4 के उपयोग से, हम जानते हैं कि उदाहरणार्थ, $\mathbb{Z}_{72}$ में $o(\bar{4}) = \dfrac{72}{(72, 4)} = \dfrac{72}{4} = 18$, क्योंकि $\mathbb{Z}_{72}$ में $o(\bar{1}) = 72$. आइए एक अन्य उदाहरण पर विचार करें।

उदाहरण 4: $D_{20} = \{1, R, \ldots, R^9, r, rR, \ldots, rR^9\}$ पर विचार कीजिए, जहाँ $o(r) = 2, o(R) = 10$ तथा $rR = R^{-1}r$. $o(R^2)$ और $o(R^3)$ को ज्ञात कीजिए।

हल: क्योंकि $o(R)=10$, इसलिए $o(R^2)=\frac{10}{(10,\,2)}=\frac{10}{2}=5$, तथा

$o(R^3)=\frac{10}{(10,\,3)}=\frac{10}{1}=10$.

***

अब, प्रमेय 4 के एक उपप्रमेय पर विचार कीजिए।

उपप्रमेय 1: यदि $G=<g>$ परिमित है, और कोटि n का है, तो

i) $o(g^m)=o(g^{(n,\,m)}),\quad m\in\mathbb{N}$ के लिए।

ii) $G=<g^m>$ iff $(m,\,n)=1$. ■

हम उपप्रमेय 1 की उपपत्ति आपके लिए छोड़ रहे हैं (देखिए E9)।

उपप्रमेय 1(ii) के संदर्भ में, निम्नलिखित टिप्पणी पर विचार कीजिए। इस टिप्पणी में हम शिक्षार्थियों द्वारा की जाने वाली एक आम त्रुटि के कारण इस बिंदु पर बल दे रहे हैं।

टिप्पणी 2: उपप्रमेय 1 के संदर्भ में, किसी $m\in\mathbb{Z}$ के लिए, $<g>=<g^m>$ हो सकता है, परंतु $g\neq g^m$. उदाहरणार्थ, $\mathbb{Z}_{30}$ में $o(\overline{1})=30$. साथ ही प्रमेय 4(ii) द्वारा,
$o(\overline{7})=\frac{30}{(30,\,7)}=30.$

अतः, $<\overline{1}>=<\overline{7}>$, परंतु $\overline{1}\neq\overline{7}$.

इसी प्रकार, $o(\overline{2})=\frac{30}{(30,\,2)}=15$ तथा $o(\overline{4})=15$, परंतु $\overline{2}\neq\overline{4}$.

अगले कुछ प्रश्न आपको प्रमेय 4 को लागू करने का कुछ अभ्यास कराएँगे।

E9) उपप्रमेय 1 को सिद्ध कीजिए।

E10) $\overline{2},\overline{4}$ और $\overline{5}\in\mathbb{Z}_{18}$ की कोटियाँ ज्ञात कीजिए।

E11) यदि G एक परिमित चक्रीय समूह है, तो दर्शाइए कि $o(G)$ को $o(x)$ विभाजित करता है $\forall\ x\in G$. विशेष रूप में, दर्शाइए कि $x^{o(G)}=e\ \forall\ x\in G$.

E12) मान लीजिए कि $U_{10}=<\zeta>$. $o<\zeta^3>$ ज्ञात कीजिए।

E13) मान लीजिए कि G एक समूह है तथा $x\in G$ कोटि 15 का है। x^2, x^6 और x^{10} की कोटियाँ ज्ञात कीजिए।

E14) मान लीजिए कि G एक समूह है तथा $x\in G$ की कोटि n है। सिद्ध कीजिए कि $<x^m>=<x^{n-m}>$, जहाँ $0<m\leq n$. इससे सिद्ध कीजिए कि $(n,\,m)=(n,\,n-m)$.

E15) $\mathbb{Z}_{30}$ में $<\overline{25}>$ के अवयव, तथा U_{10} में $<\zeta^7>$ के अवयव, ज्ञात कीजिए, जहाँ ζ एक जनक है U_{10} का।

इस भाग में आपने जिन गुणों को सीखा है, वे हमें स्वाभाविक रूप से चक्रीय समूहों के गुणों पर विचार करने की ओर ले जाते हैं। इन्हीं की चर्चा हम अगले भाग में करने जा रहे हैं।

4.3 चक्रीय समूह के गुण

भाग 4.2 में आपने चक्रीय समूह की परिभाषा का अध्ययन किया था। यहाँ पर हम ऐसे समूहों के कुछ उदाहरणों तथा उनके कुछ गुणों पर दृष्टि डालेंगे। पिछले भाग में, आप देख चुके हैं कि $\mathbb{Z} = <1>, \mathbb{Z}_5 = <\overline{3}>$ तथा $\mathbb{Z}_{18} = <\overline{5}>$. इस प्रकार, चक्रीय समूहों के उदाहरण हैं, जैसा कि आप जानते हैं। आइए कुछ और उदाहरणों पर विचार करें।

उदाहरण 5: दर्शाइए कि $\forall\ n \in \mathbb{N}, U_n$ एक चक्रीय समूह है।

हल: उपभाग 2.4.5, इकाई 2 में आप देख चुके हैं कि यदि $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, तो

$U_n = \{\zeta, \zeta^2, \ldots, \zeta^n(=1)\}$.

इस प्रकार, $U_n = <\zeta>$, जहाँ $o(\zeta) = n$.

***

ध्यान दीजिए कि अभी तक जो आपने चक्रीय समूहों के उदाहरणों को देखा है, वे सभी आबेली हैं। क्या हम अन्आबेली चक्रीय समूह ज्ञात कर सकते हैं? इस प्रश्न का उत्तर निम्नलिखित प्रमेय में है।

प्रमेय 5: चक्रीय समूह आबेली होता है।

उपपत्ति: मान लीजिए कि $G = <a>$ एक चक्रीय समूह है, तथा $x, y \in G$. तब, किन्हीं $m, n \in \mathbb{Z}$ के लिए, $x = a^n$ और $y = a^m$. अतः,

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

$= yx$, प्रमेय 6, इकाई 2 के उपयोग से।

अतः, G एक क्रमविनिमेय समूह है। ■

प्रमेय 5 के कारण, अब आप जानते हैं कि **किसी भी समूह का प्रत्येक चक्रीय उपसमूह आबेली होता है,** चाहे वह समूह आबेली हो या नहीं। उदाहरणार्थ, आप जानते हैं कि S_3 आबेली नहीं है। परंतु, $<(1\ 2)>$ और $<(1\ 3\ 2)>$ समूह S_3 के आबेली उपसमूह हैं।

अब, प्रश्न उठता है– क्या सभी आबेली समूह चक्रीय होते हैं? इसका उत्तर निम्नलिखित उदाहरणों में है।

ऐसे भी आबेली समूह हैं जो चक्रीय नहीं हैं।

उदाहरण 6: समुच्चय $K_4 = \{e, a, b, ab\}$ तथा नीचे दी सारणी द्वारा K_4 पर द्वि-आधारी संक्रिया पर विचार कीजिए :

आकृति 1: फ़ीलिक्स क्लाइन (Felix klein) (1849-1925) ने 1884 में एक शोध पत्र में क्लाइन 4-समूह को परिभाषित किया था।

$\cdot$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

दर्शाइए कि K_4 आबेली है, परंतु चक्रीय नहीं है। (यह समूह **क्लाइन 4-समूह** है, जिसे आपने पहले उदाहरण 3, इकाई 2 में देखा है।)

हल: सारणी से आप देख सकते हैं कि इसमें प्रविष्टियाँ उस विकर्ण के प्रति सममित हैं जिसकी सभी प्रविष्टियाँ e हैं। अतः, K_4 आबेली है।

यदि K_4 चक्रीय होता, तो वह e, a, b या ab में से किसी एक से जनित होता। अब, $< e > = \{e\} \neq K_4$.

साथ ही, आप सारणी से देख सकते हैं कि $< a > = \{e, a\} \neq K_4$.

इसी प्रकार, $< b > = \{e, b\} \neq K_4$ तथा $< ab > = \{e, ab\} \neq K_4$.

इसलिए, K_4 को e, a, b या ab से जनित नहीं किया जा सकता है।

इस प्रकार, K_4 चक्रीय नहीं है।

***

उदाहरण 7: दर्शाइए कि $\mathbb{Q}$ एक चक्रीय समूह नहीं है।

हल: हम इसे अंतर्विरोध द्वारा सिद्ध करेंगे। अतः, आइए मान लें कि $\frac{p}{q}$, $\mathbb{Q}$ को जनित करता है, $(p, q) = 1, q \neq 0$.

अब, $\frac{p}{q} + 1 \in \mathbb{Q}$. अतः, $\exists\, n \in \mathbb{Z}$ s.t. $\frac{p}{q} + 1 = n\left(\frac{p}{q}\right)$, अर्थात् $(n-1)p = q$.

क्योंकि $(p, q) = 1$, इसलिए इकाई 1 के प्रमेय 6 से आप जानते हैं कि $q \mid (n-1)$. मान लीजिए कि $qr = n-1$, जहाँ $r \in \mathbb{Z}$.

तब, $(n-1)p = q$ से $pr = 1$ प्राप्त होता है।

यह केवल तभी संभव है जब $p = 1, r = 1$ हो, या $p = -1, r = -1$ हो। प्रत्येक स्थिति में, $\frac{p}{q} = \frac{1}{n-1}$.

अब, $\frac{1}{3(n-1)} \in \mathbb{Q}$ पर विचार कीजिए।

क्योंकि $\mathbb{Q} = < \frac{1}{n-1} >$, इसलिए $\exists\, m \in \mathbb{Z}$ s.t. $m\left(\frac{1}{n-1}\right) = \frac{1}{3(n-1)}$.

इससे $m = \frac{1}{3}$ प्राप्त होता है, जो संभव नहीं है।

अतः, हमारा यह मानना कि $\mathbb{Q}$ चक्रीय है, ग़लत होगा।

इस प्रकार, $\mathbb{Q}$ चक्रीय नहीं है।

***

तो, आप परिमित तथा अपरिमित, आबेली समूहों अचक्रीय के उदाहरणों को देख चुके हैं। अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E16) या D_8 चक्रीय है? क्यों, या क्यों नहीं?

E17) सिद्ध कीजिए कि अन्आबेली समूह का एक उचित अतुच्छ उपसमूह अवश्य होना चाहिए।

अब, आइए चक्रीय समूहों के एक अन्य विशिष्ट गुण को देखें। इस गुण को समझने के लिए, $\mathbb{Z}$ पर विचार कीजिए। आप जानते हैं कि $n\mathbb{Z} \le \mathbb{Z}\ \forall\ n \in \mathbb{Z}$. अब प्रश्न है : $\mathbb{Z}$ के अन्य उपसमूह क्या हैं? इस प्रश्न का उत्तर निम्नलिखित प्रमेय देता है।

प्रमेय 6: चक्रीय समूह का कोई भी उपसमूह चक्रीय होता है।

आगे, यदि $G = < x >$ और $H \le G$, तो $H = \{e\}$ या $H = < x^n >$, जहाँ n ऐसा न्यूनतम धनात्मक पूर्णांक है जिसके लिए $x^n \in H$.

उपपत्ति: मान लीजिए कि $G = < x >$ एक चक्रीय समूह है तथा H, G का एक उपसमूह है। यदि $H = \{e\}$, तो $H = < e >$. इसी लिए H चक्रीय है।

मान लीजिए कि $H \ne \{e\}$. तब, $\exists\ n \in \mathbb{Z}$ s.t. $x^n \in H,\ n \ne 0$.

क्योंकि H एक उपसमूह है, इसलिए $(x^n)^{-1} = x^{-n} \in H$. अतः, कम से कम एक धनात्मक पूर्णांक m है (अर्थात्, n या $-n$) जिसके लिए $x^m \in H$.

इस प्रकार, समुच्चय $S = \{t \in \mathbb{N} \mid x^t \in H\}$ अरिक्त है। अतः, सुक्रमण सिद्धांत द्वारा, S का एक न्यूनतम अवयव, मान लीजिए k है।

हम दर्शाएँगे कि $H = < x^k >$.

अब, $< x^k > \subseteq H$, क्योंकि $x^k \in H$. …(9)

विलोमतः, मान लीजिए कि H में x^n कोई भी एक अवयव है। विभाजन ऐल्गोरिद्म द्वारा, $n = mk + r$, किन्हीं $m, r \in \mathbb{Z}$ के लिए जहाँ $0 \le r \le k-1$.

अतः, $x^r = x^{n-mk} = x^n.(x^k)^{-m} \in H$, क्योंकि $x^n, x^k \in H$.

परंतु, k सबसे छोटा धनात्मक पूर्णांक है ताकि $x^k \in H$.

अतः, H में x^r केवल तभी होगा, जब $r = 0$.

और तब, $n = mk$ और $x^n = (x^k)^m \in < x^k >$.

इस प्रकार, $H \subseteq < x^k >$. …(10)

(9) और (10) से हम निष्कर्ष निकालते हैं कि $H = < x^k >$, अर्थात् H चक्रीय है। ■

आइए प्रमेय 6 के प्रयोग का एक उदाहरण देखें।

उदाहरण 8: $\mathbb{Z}$ का प्रत्येक अतुच्छ उपसमूह $m\mathbb{Z}$ के रूप का होता है, किसी $m \in \mathbb{Z}$ के लिए। अतः, $\mathbb{Z}$ के सभी उपसमूह ज्ञात हैं।

हल: मान लीजिए कि $H \le \mathbb{Z}$, $H \ne \{0\}$.

क्योंकि $\mathbb{Z} = < 1 >$, इसलिए $H = < m > = m\mathbb{Z}$, जहाँ H में m सबसे छोटा धनात्मक पूर्णांक है, प्रमेय 6 द्वारा।

***

अब, प्रमेय 6 कहता है कि एक चक्रीय समूह का प्रत्येक उपसमूह चक्रीय होता है। क्या आप सोच रहे हैं कि इसका विलोम सत्य है? ऐसा है कि कुछ समूह हैं जिनके सभी उचित उपसमूह चक्रीय होते हैं, लेकिन वे समूह स्वयं चक्रीय नहीं होते। आपको ऐसे उदाहरण इकाई 5, खंड 2 में देखने को मिलेंगे। अतः, प्रमेय 6 का विलोम सत्य नहीं है।

अब, उदाहरण 8 में आपने देखा कि $\mathbb{Z}$ के सभी उपसमूह ज्ञात हैं। अन्य चक्रीय समूहों के बारे में आप क्या कह सकते हैं? ऐसा है कि हम एक परिमित चक्रीय समूह के ठीक कितने उपसमूह होते हैं मालूम कर सकते हैं, तथा हम इन सभी की एक सूची बना सकते हैं! निम्नलिखित प्रमेय से हम यह सब कर सकते हैं।

प्रमेय 7: मान लीजिए कि G कोटि n वाला एक परिमित चक्रीय समूह है। n के प्रत्येक धनात्मक भाजक m के लिए, G का कोटि m वाला एक **अद्वितीय** उपसमूह है। आगे, केवल ये ही G के उपसमूह हैं।

उपपत्ति: मान लीजिए कि $G = < g >$, जहाँ $o(g) = n$. वास्तव में, यहाँ तीन कथनों को सिद्ध किया जाना है :

i) यदि $m | n$, $\exists\, H \le G$ s.t. $o(H) = m$;

ii) यदि $H \le G, K \le G$ s.t. $o(H) = o(K)$, तो $H = K$; तथा

iii) यदि $H \le G$, तो $o(H) | n$.

पहले हम (i) को सिद्ध करेंगे। अतः, मान लीजिए कि $n = mr$ तथा यह भी मान लीजिए कि $o(g^r) = s$. तब, s सबसे छोटा धनात्मक पूर्णांक है जिससे कि $(g^r)^s = e$, अर्थात्, $g^{rs} = e$.

क्योंकि $o(g) = n$, इसलिए प्रमेय 2 से, $n | rs$.

अतः, $n \leq rs$, अर्थात् $mr \leq rs$, अर्थात्,

$$m \leq s. \qquad \ldots(11)$$

अब, $(g^r)^m = g^n = e$. अतः, फिर प्रमेय 2 (ii) द्वारा, $s \mid m$, अर्थात्,

$$s \leq m. \qquad \ldots(12)$$

(11) और (12) द्वारा, हमें $s = m$ प्राप्त होता है।

इस प्रकार, $H = < g^r > \; = < g^{\frac{n}{m}} >$, G का कोटि m वाला उपसमूह है।

अब, आइए (ii) को सिद्ध करें। अर्थात्, प्रमेय में दिए अद्वितीयता को सिद्ध करें।

माना $H = < g^r >$ और $K = < g^t >$ दोनों ही G के कोटि m वाले उपसमूह हैं, जहाँ $n = mr$.

अब, $m = o(g^t) = \dfrac{n}{(n, t)} = \dfrac{mr}{(mr, t)}$. अतः, $r = (mr, t)$.

इस प्रकार, $r \mid t$. मान लीजिए कि $t = vr$, जहाँ $v \in \mathbb{N}$.

इसलिए, $g^t = (g^r)^v \in H$.

इस प्रकार, $K \subseteq H$.

परंतु इन दोनों समुच्चयों में अवयवों की संख्या समान है, यानी m.

अतः, $K = H$.

अब, (iii) को सिद्ध करने के लिए, मान लीजिए कि $H \leq G$. तब, प्रमेय 6 द्वारा, आप जानते हैं कि $H = < g^s >$, जहाँ s न्यूनतम धनात्मक पूर्णांक है जिससे कि $g^s \in H$. विभाजन ऐल्गोरिद्म द्वारा, $\exists\, q, r \in \mathbb{Z}$ s.t. $n = qs + r,\ 0 \leq r < s$.

अतः, $g^{n-qs} = g^r$.

क्योंकि $g^n = e$ और $g^s \in H$, इसलिए $g^{-qs} \in H$.

इस प्रकार, $g^r \in H$. क्योंकि $r < s$, इसलिए यह तभी संभव है, जब $r = 0$. तब, $n = qs$.

अब, ऊपर (i) की उपपत्ति की तरह, आप दर्शा सकते हैं कि $o(H) = q$, तथा $q \mid n$. इस प्रकार, H, n के भाजक q के संगत है। ■

अब, मान लीजिए कि $G = < g >$ एक चक्रीय समूह है तथा $H = < g^m >$ और $K = < g^n >$ समूह G के उपसमूह हैं। $H \leq K$ कब होता है? यह होगा यदि और केवल यदि $H \subseteq K$. तो, m और n के बीच में यदि कोई संबंध है, तो वह क्या है? वास्तव में, आप इसका उत्तर प्रमेय 8 की उपपत्ति में पाएंगे। परंतु, पहले निम्नलिखित उदाहरण पर विचार कीजिए।

उदाहरण 9: उदाहरण 8 में आप देख चुके हैं कि $\mathbb{Z}$ का कोई भी उपसमूह $m\mathbb{Z}$ के रूप का होता है, किसी $m \in \mathbb{N}$ के लिए। मान लीजिए कि $m\mathbb{Z}$ और $k\mathbb{Z}$, $\mathbb{Z}$ के दो उपसमूह हैं। दर्शाइए कि $m\mathbb{Z}$, $k\mathbb{Z}$ का एक उपसमूह है यदि और केवल यदि $k \mid m$.

हल: हमें यह दर्शाने की आवश्यकता है कि $m\mathbb{Z} \subseteq k\mathbb{Z} \Leftrightarrow k \mid m.$

अब, $m\mathbb{Z} \subseteq k\mathbb{Z} \Rightarrow m \in k\mathbb{Z} \Rightarrow m = kr,$ किसी $r \in \mathbb{Z}$ के लिए

$$\Rightarrow k \mid m.$$

विलोमतः, मान लीजिए कि $k \mid m.$ तब किसी $r \in \mathbb{Z}$ के लिए, $m = kr.$

अब, कोई $n \in m\mathbb{Z}$ लीजिए, तथा मान लीजिए कि $t \in \mathbb{Z}$ ऐसा है कि $n = mt.$

अतः, $n = mt = (kr)t = k(rt) \in k\mathbb{Z}.$

क्योंकि $m\mathbb{Z}$ का n कोई भी एक अवयव था, इसलिए इससे प्रदर्शित होता है कि $m\mathbb{Z} \subseteq k\mathbb{Z}.$

इस प्रकार, हमने दर्शा दिया है कि $m\mathbb{Z} \le k\mathbb{Z}$ iff $k \mid m$.

***

उदाहरण 9 का व्यापकीकरण करते हुए, निम्नलिखित प्रमेय पर विचार कीजिए जिसमें वास्तव में तीन कथन हैं!

प्रमेय 8: मान लीजिए कि $G = \langle g \rangle$, $H = \langle g^m \rangle$ और $K = \langle g^n \rangle$.

i) $H \le K$ iff $n \mid m$;

ii) $H \cap K = \langle g^s \rangle$, जहाँ s है, m और n का l.c.m;

iii) $HK \le G$ और $HK = \langle g^d \rangle$, जहाँ $d = (m, n)$.

[ध्यान दीजिए कि यदि + संक्रिया है, तो (iii) कहता है कि $H + K = \langle d \rangle$, जहाँ $d = (m, n)$.]

उपपत्ति: हम (i) की उपपत्ति आपके लिए छोड़ रहे हैं (देखिए E19)।

ii) क्योंकि $H \cap K \le G$, इसलिए किसी $s \in \mathbb{N}$ के लिए, $H \cap K = \langle g^s \rangle$.

क्योंकि $H \cap K$, दोनों H और K का एक उपसमूह है, इसलिए उपरोक्त (i) द्वारा, $m \mid s$ तथा $n \mid s$. इस प्रकार, m और n का s एक सार्वगुणज है।

अब, मान लीजिए कि t, m और n का कोई सार्वगुणज है। तब, (i) द्वारा $\langle g^t \rangle \le H$ और $\langle g^t \rangle \le K$. अतः, $\langle g^t \rangle \le H \cap K = \langle g^s \rangle$.

$\therefore s \mid t.$

अतः, इकाई 1 में दी l.c.m की परिभाषा से, s है m और n का l.c.m.

iii) प्रमेय 5 द्वारा, G आबेली है। अतः, $HK \le G$.

अब, $HK = \{hk \mid h \in H, k \in K\}$.

कोई भी $h \in H, k \in K$ के लिए $h = (g^m)^{m_1}$ और $k = (g^n)^{n_1}$ किन्हीं $m_1, n_1 \in \mathbb{Z}$ के लिए।

इसलिए $hk = g^{mm_1+nn_1} = g^{dd_1}$, किसी $d_1 \in \mathbb{Z}$ के लिए, जहाँ $d = (m, n)$.

इस प्रकार, $HK \subseteq \langle g^d \rangle$. …(13)

साथ ही, इकाई 1 से आप जानते हैं कि किन्हीं $r, s \in \mathbb{Z}$ के लिए, $d = mr + ns$.

अतः, $g^d = g^{mr+ns} = (g^m)^r \cdot (g^n)^s \in HK$.

इसलिए, $\langle g^d \rangle \subseteq HK$. …(14)

अतः, (13) और (14) द्वारा, $HK = \langle g^d \rangle$. ■

यहाँ हम एक ऐसी समुच्चय संक्रिया पर टिप्पणी देंगे जिसके बारे में प्रमेय 8 में कुछ नहीं बताया गया है।

टिप्पणी 3: प्रमेय 8 सम्मिलन $H \cup K$ के बारे में चुप है। इकाई 3 में आप देख चुके हैं कि $H \cup K \le G$ iff $H \subseteq K$ या $K \subseteq H$. इस प्रकार, प्रमेय 8 के संदर्भ में, $H \cup K \le G$ iff $n \mid m$ या $m \mid n$, प्रमेय 8(i) द्वारा। अतः, उदाहरणार्थ, $\langle \bar{3} \rangle \cup \langle \bar{5} \rangle \not\le \mathbb{Z}_{15}$. आपको इसका सत्यापन करना चाहिए।

प्रमेय 7 और 8 हमें एक परिमित चक्रीय समूह के उपसमूहों का एक संपूर्ण चित्रण देते हैं।

प्रमेय 7 हमें यह भी बताता है कि कोटि m वाला उपसमूह, जहाँ $m \mid n$, $\langle g^{\frac{n}{m}} \rangle$ है। आइए इस समझ का कुछ स्थितियों में अनुप्रयोग करें।

उदाहरण 10: एक के 12वें मूलों के समूह, U_{12} के सभी उपसमूहों को ज्ञात कीजिए।

हल: 12 के धनात्मक भाजक 1, 2, 3, 4, 6 और 12 हैं।

मान लीजिए कि $U_{12} = \langle \zeta \rangle$, जहाँ ζ की कोटि 12 है, अर्थात्, ζ एक का पूर्वग 12वाँ मूल है।

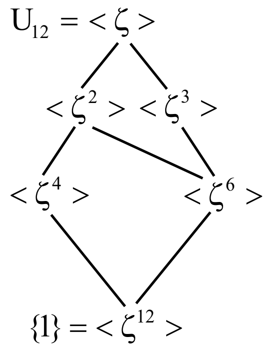
U_n का कोई भी जनक **एक का पूर्वग nवाँ मूल (primitive)** कहलाता है।

तब, $A_1 = \{1\} = \langle \zeta^{12} \rangle$ की कोटि 1 है।

आगे, $A_2 = \langle \zeta^{\frac{12}{2}} \rangle = \langle \zeta^6 \rangle$ की कोटि 2 है। इसी प्रकार,
$A_3 = \langle \zeta^4 \rangle, A_4 = \langle \zeta^3 \rangle, A_5 = \langle \zeta^2 \rangle, A_6 = \langle \zeta \rangle = U_{12}$ क्रमशः U_{12} के कोटियों 3, 4, 6 और 12 वाले उपसमूह है।

प्रमेय 8 द्वारा, $A_1 \leq A_2 \leq A_4 \leq A_6$, तथा $A_1 \leq A_3 \leq A_5 \leq A_6$.

हम इस संबंध को **एक उपसमूह आरेख** के रूप में आकृति 2 में दर्शा रहे हैं।



आकृति 2: U_{12} के लिए एक उपसमूह आरेख। इसमें हर रेखा जो नीचे वाले उपसमूह H को ऊपर वाले उपसमूह K से जोड़ती है यह दर्शाती है कि $H \leq K$.

***

उदाहरण 11: $\mathbb{Z}_{30}$ के सभी उपसमूहों को ज्ञात कीजिए, तथा $\mathbb{Z}_{30}$ के लिए एक उपसमूह आरेख बनाइए।

हल: याद कीजिए कि $\mathbb{Z}_{30} = <\overline{1}>$.

अब 30 के धनात्मक भाजक 1, 2, 3, 5, 6, 10, 15 और 30 हैं।

इस प्रकार, उपरोक्त कोटियों वाले $\mathbb{Z}_{30}$ के उपसमूह हैं क्रमशः

$<\overline{30}> = \{\overline{0}\}$,

$<\overline{15}> = \{\overline{0}, \overline{15}\}$,

$<\overline{10}> = \{\overline{0}, \overline{10}, \overline{20}\}$,

$<\overline{6}> = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}\}$,

$<\overline{5}> = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}\}$,

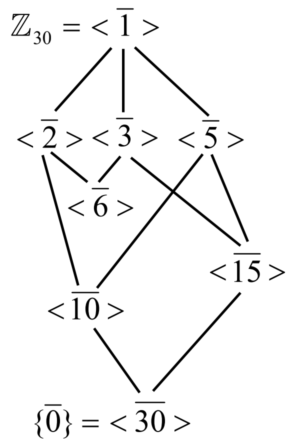
$<\overline{3}> = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}\}$,

$<\overline{2}> = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}, \overline{20}, \overline{22}, \overline{24}, \overline{26}, \overline{28}\}$,

$<\overline{1}> = \mathbb{Z}_{30}$.

आकृति 3 में दिए $\mathbb{Z}_{30}$ की उपसमूह संरचना के आरेखित निरूपण पर विचार कीजिए।

यह कई बातें दर्शाता है, जैसे कि $<\overline{6}> \leq <\overline{3}>$ तथा $<\overline{6}> \leq <\overline{2}>$. इसी प्रकार, $<\overline{30}> \leq <\overline{15}>$, जो $<\overline{3}>$ और $<\overline{5}>$ दोनों का एक उपसमूह है।



आकृति 3: $\mathbb{Z}_{30}$ का उपसमूह आरेख

***

उदाहरण 12: $\mathbb{Z}$ में $<15>+<18>$ तथा $<15>\cap<18>$ ज्ञात कीजिए।

हल: प्रमेय 8(iii) से, $<15>+<18> = <d>$, जहाँ $d = (15, 18) = 3$.

अतः, $<15>+<18> = <3>$.

इसी प्रकार, प्रमेय 8(ii) द्वारा, $<15>\cap<18> = <s>$, जहाँ $s = 15, 18 = 90$.

अतः, $<15>\cap<18> = <90>$.

***

अब, आप निम्नलिखित प्रश्नों को क्यों नहीं करने का प्रयास करते?

E18) $\mathbb{Z}$ के किन उपसमूहों का $9\mathbb{Z}$ एक उपसमूह है? अपने उत्तर के लिए कारण दीजिए।

E19) i) यदि $G = <g>$ परिमित है, $H = <g^m>$ और $K = <g^r>$, जहाँ $m, r \in \mathbb{Z}$, तो m और r पर किन प्रतिबंधों के अधीन $H \le K$ होगा? अपने उत्तर के लिए कारण दीजिए।

ii) यदि $G = <g>$ अपरिमित है तथा $H = <g^m>$ और $K = <g^n>$ किन्हीं $m, n \in \mathbb{Z}$ के लिए, तो सिद्ध कीजिए कि $H \le K$ iff $n \mid m$.

E20) $\mathbb{Z}_{12}$ का उपसमूह आरेख दीजिए। इसकी संरचना की आकृति 2 में दी U_{12} की संरचना से तुलना कीजिए। इससे आप किन निष्कर्षों पर पहुँचते हैं।

E21) $\mathbb{Z}_{25}$ के सभी उपसमूहों को ज्ञात कीजिए, तथा संगत उपसमूह आरेख दीजिए।

E22) दर्शाइए कि $\mathbb{Z}_p$ का कोई उचित अतुच्छ उपसमूह नहीं है, जहाँ p एक अभाज्य संख्या है।

E23) $\mathbb{Z}_n$, $n \ge 2$, के सभी उपसमूहों को ज्ञात कीजिए।

E24) $\mathbb{Z}_{30}$ में $<\overline{4}>+<\overline{6}>$ तथा $<\overline{4}>\cap<\overline{6}>$ के जनकों को ज्ञात कीजिए।

E25) HK और $H \cap K$ का एक एक जनक ज्ञात कीजिए, जहाँ U_{12} में $H = <\zeta^8>$ और $K = <\zeta^{10}>$.

E26) मान लीजिए कि G एक चक्रीय समूह है। क्या G अपने उचित उपसमूहों का सम्मिलन हो सकता है? अपने उत्तरों के लिए कारण दीजिए।

आइए अब उपप्रमेय 1(ii) में बताए गए बिंदु पर वापस लौटें। आप देख सकते हैं कि अगर $o(g) = n$, तो $<g>$ के विभिन्न जनकों की संख्या $<g>$ में कोटि n वाले अलग-अलग अवयवों की संख्या के बराबर है। उपप्रमेय 1 द्वारा, यह संख्या है उन धनात्मक पूर्णांकों की जो n से छोटे हैं तथा n के सापेक्षतः अभाज्य हैं। यह संख्या ऑयलर फ़ाइ-फलन (phi-function) द्वारा दिया जाता है, जो प्रसिद्ध स्विस गणितज्ञ लियोनार्ड ऑयलर (Leonhard Euler) के नाम पर है। (आप इनसे पिछली इकाइयों में मिल चुके हैं!)

आकृति 4: लियोनार्ड ऑयलर (1707-1783)

परिभाषा: ऑयलर फ़ाइ-फलन $\phi : \mathbb{N} \to \mathbb{N}$ को निम्न तरह से परिभाषित किया जाता है:

$\phi(1) = 1$, तथा

$\phi(n) =$ उन प्राकृत संख्याओं की संख्या जो n से कम हैं तथा n के सापेक्षतः अभाज्य हैं, $n \geq 2$ के लिए।

उदाहरणार्थ, $\phi(2) = 1$ और $\phi(6) = 2$ (क्योंकि 6 से छोटी तथा 6 के सापेक्षतः अभाज्य धनात्मक पूर्णांक केवल 1 और 5 हैं)।

अतः, **परिमित समूह $<g>$ के भिन्न-भिन्न जनकों की संख्या $\phi(n)$ है,** जहाँ $n = o(g)$.

अब, इससे एक अन्य प्रश्न उठता है : $n = o(g)$ के प्रत्येक धनात्मक भाजक d के लिए, $<g>$ में कोटि d वाले कितने अवयव हैं?

आप जानते हैं कि कोटि 1 वाला अवयव केवल e है, तथा आप जानते हैं कि G में कोटि n वाले अवयवों की संख्या $\phi(n)$ है। n के अन्य भाजकों के बारे में क्या कह सकते हैं?

निम्नलिखित परिणाम पर विचार कीजिए।

प्रमेय 9: मान लीजिए कि $G = <g>$ कोटि n का है, तथा d, n का एक धनात्मक भाजक है। तब, G के कोटि d वाले अवयवों की संख्या $\phi(d)$ है।

उपपत्ति: प्रमेय 7 में आप देख चुके हैं कि क्यों $g^{\frac{n}{d}}$ कोटि d का है। मान लीजिए कि $\frac{n}{d} = m$, तथा $g^m = a$. G के कोटि d वाले अद्वितीय उपसमूह $H = <a>$ को देखिए। प्रमेय 7 तथा उपरोक्त चर्चा से, आप जानते हैं कि H के भिन्न-भिन्न जनकों की संख्या $\phi(d)$ है।

अतः, G के कोटि d वाले भिन्न-भिन्न अवयवों की संख्या $\phi(d)$ है। ■

आइए जो प्रमेय 9 हमें बताता है, उसे एक उदाहरण के द्वारा और समझें।

उदाहरण 13: $\mathbb{Z}_{50}$, U_{17} और U_{25} के कितने कोटि 2 वाले और कोटि 5 वाले अवयव हैं? क्या आप इन अवयवों को ज्ञात कर सकते हैं, यदि उनका अस्तित्व है तो?

हल: ध्यान दीजिए कि $o(\mathbb{Z}_{50}) = 50$, $o(U_{17}) = 17$ और $o(U_{25}) = 25$.

क्योंकि $2|50$ और $5|50$, इसलिए $\mathbb{Z}_{50}$ का $\phi(2) = 1$ कोटि 2 वाला अवयव है, और $\phi(5) = 4$ कोटि 5 वाले अवयव हैं। ध्यान दीजिए कि $\phi(5) = 4$, क्योंकि 5 एक अभाज्य संख्या है, जिस कारण से वह 1, 2, 3, 4 के सापेक्षतः अभाज्य है।

$\mathbb{Z}_{50}$ में कोटि 2 वाला अवयव $\overline{25}$ है।

$\mathbb{Z}_{50}$ में कोटि 5 वाले अवयव $m \cdot \overline{10}$ हैं, जहाँ $(m, 5) = 1$.

ये हैं $\overline{10}, \overline{20}, \overline{30}$ और $\overline{40}$, जो क्रमशः $m = 1, 2, 3$ और 4 के संगत हैं।

आगे, क्योंकि U_{17} कोटि 17 का है, तथा $2 \nmid 17$ और $5 \nmid 17$, इसलिए U_{17} में कोटि 2 वाले या कोटि 5 वाले कोई अवयव नहीं हैं।

अंत में, क्योंकि $2 \nmid 25$, इसलिए U_{25} में कोटि 2 वाला कोई अवयव नहीं है।

क्योंकि $5|25$, इसलिए U_{25} में कोटि 5 वाले $\phi(5) = 4$ अवयव हैं।

ये हैं ζ^{5m} जहाँ $(m, 5) = 1$. अर्थात् ये $\zeta^5, \zeta^{10}, \zeta^{15}$ और ζ^{20} हैं, जहाँ ζ एक का कोई पूर्वग 25 वाँ मूल है।

***

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E27) दर्शाइए कि

i) किसी भी अभाज्य संख्या p के लिए, $\phi(p) = p - 1$,

ii) $n = \sum_{d|n} \phi(d)$, (**संकेत:** प्रमेय 7 का उपयोग कीजिए।)

iii) व्यापक रूप में, $\phi(mn) \neq \phi(m)\phi(n)$. (इकाई 8 में आप देखेंगे कि $\phi(mn) = \phi(m)\phi(n)$ यदि $(m, n) = 1$ जहाँ $m, n \in \mathbb{N}$.)

E28) $\mathbb{Z}_{30}$ में $< \overline{25} >$ के, तथा U_{10} में $< \zeta^3 >$ के, सभी जनक ज्ञात कीजिए।

अभी तक आपने परिमित चक्रीय समूहों के उपसमूहों के अध्ययन पर काफ़ी समय लगाया है। अपरिमित चक्रीय समूहों के उपसमूहों के बारे में हम क्या जानते हैं इसके अलावा कि वे भी चक्रीय होते हैं? आइए देखें।

प्रमेय 10: मान लीजिए कि $G = < g >$ एक अपरिमित चक्रीय समूह है तथा $x \in G, x \neq e$. तब, $< x >$ भी एक अपरिमित चक्रीय समूह है।

उपपत्ति: पहले तो प्रमेय 6 से आप जानते हैं कि $x = g^n$, किसी $n \in \mathbb{N}$ के लिए। अतः, प्रमेय 4(i) द्वारा, $o(x)$ अपरिमित है। इस प्रकार, $< x > = < g^n >$ अपरिमित है। ■

आइए $\mathbb{Z}$ पर विचार करें। आप जानते हैं कि यह 1 या (−1) द्वारा जनित एक अपरिमित चक्रीय समूह है। क्या $\mathbb{Z}$ किसी अन्य अवयव द्वारा जनित हो सकता है? निम्नलिखित उदाहरण का अध्ययन करते हुए इसके बारे में सोचिए।

उदाहरण 14: दर्शाइए कि यदि $<g>$ अपरिमित है तथा $<g^n> = <g>$, किसी $n \in \mathbb{Z}$ के लिए, तो $n = 1$ या -1.

हल: E3 से आप जानते हैं कि किसी भी चक्रीय समूह $<g>$ के लिए, $<g> = <g^{-1}>$.

अब, मान लीजिए कि $<g^n> = <g>$, जहाँ g अपरिमित कोटि का है। तब, $g \in <g^n>$. अतः, $\exists\, m \in \mathbb{Z}$ s.t. $g^{nm} = g$. तब, प्रमेय 2 द्वारा, $nm = 1$.

क्योंकि $n, m \in \mathbb{Z}$, इसलिए यह केवल तभी संभव है, जब $n = 1$ या -1.

***

उदाहरण 14 से, आप देख सकते हैं कि $\mathbb{Z} = <1>$ या $\mathbb{Z} = <-1>$. साथ ही, सिर्फ़ ये ही $\mathbb{Z}$ के संभावित जनक हैं।

अब, कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E29) क्या शून्येतर सम्मिश्र संख्याओं के समूह $\mathbb{C}^*$ का चक्रीय उपसमूह $<1>$ अपरिमित है? क्यों?

E30) निम्नलिखित में से कौन-से कथन सत्य हैं? अपने उत्तरों के लिए कारण दीजिए।

i) यदि H एक अपरिमित चक्रीय समूह है, तथा H समूह G में आविष्ट है, तब G चक्रीय होगा।

ii) एक अपरिमित चक्रीय समूह का केवल एक ही परिमित उपसमूह होता है।

iii) एक ऐसा अपरिमित चक्रीय समूह है जिसके 4 भिन्न-भिन्न जनक हैं।

अब, आइए एक क्षण के लिए, उदाहरण 6 पर वापस जाएँ। आपने देखा था कि K_4 एक चक्रीय समूह नहीं है। परंतु, जैसा कि आप अब देखेंगे, इसे जनित करने वाला एक समुच्चय है।

4.4 जनक समुच्चय

पिछले भाग में आपने देखा था कि यदि g समूह G का एक अवयव है, तो $<g>$ न्यूनतम उपसमूह है G का जो g को आविष्ट करता है। आइए देखें कि क्या इस धारणा को G के दो अवयवों के समुच्चय के लिए विस्तृत किया जा सकता है।

मान लीजिए कि $S = \{a, b\}$ समूह G का एक उपसमुच्चय है। मान लीजिए कि $H \le G$ s.t. $S \subseteq H$. तब, $\{a^m | m \in \mathbb{Z}\}$ और $\{b^n | n \in \mathbb{Z}\}$, H के उपसमुच्चय होंगे। साथ ही, $a^2b^3a^{-3}b^7$ जैसे अवयव H में होंगे। (ध्यान दीजिए कि हम $a^2b^3a^{-3}b^7$ को $a^{-1}b^{10}$ नहीं लिख सकते हैं, क्योंकि हो सकता है कि H आबेली नहीं हो।)

अब, मान लीजिए कि $K \leq G$ s.t. $S \subseteq K$. तब, ऊपर की ही तरह, $\{a^m \mid m \in \mathbb{Z}\} \subseteq K$ और $\{b^n \mid n \in \mathbb{Z}\} \subseteq K$, तथा $baba^2$ जैसे गुणनफल भी K में हैं।

इसलिए, ये सभी समुच्चय और अवयव $H \cap K$ में स्थित हैं। वस्तुतः, ये S को अंतर्विष्ट करने वाले G के सभी उपसमूहों के प्रतिच्छेदन में स्थित हैं, जो S! को अंतर्विष्ट वाले G का भी एक उपसमूह है। इससे हम निम्नलिखित परिभाषा पर पहुँचते हैं।

परिभाषा: मान लीजिए G एक समूह है। **$S = \{a, b\}$ द्वारा जनित G का उपसमूह** S को आविष्ट करने वाला G का न्यूनतम उपसमूह होता है। इस उपसमूह को $< a, b >$ या $< \mathbf{S} >$, द्वारा व्यक्त किया जाता है। वस्तुतः, $< S >$, S को आविष्ट करने वाले G के सभी उपसमूहों का प्रतिच्छेदन है।

उदाहरणार्थ, D_6 को $\{r, R_{120}\}$ जनित करता है, जहाँ $r^2 = I, R_{120}^3 = I$ तथा $r \circ R_{120} = R_{120}^{-1} \circ r$.

एक अन्य उदाहरण के रूप में देखिए उदाहरण 6 में K_4 को। इसे $\{a, b\}$ जनित करता है।

आइए आपने जो अभी $S = \{a, b\}$ के लिए देखा है, उसे किसी भी अरिक्त समुच्चय S के लिए व्यापकीकृत करें।

मान लीजिए कि G एक समूह है तथा S, G का एक अरिक्त उपसमुच्चय है।

S को आविष्ट करने वाले G के सभी उपसमूहों के समुच्चय $\mathcal{F}$ पर विचार कीजिए।

अर्थात् $\mathcal{F} = \{H \mid H \leq G$ और $S \subseteq H\}$.

हम दावा करते हैं कि $\mathcal{F} \neq \emptyset$. क्यों? क्या $G \in \mathcal{F}$ सत्य नहीं है?

आगे, इकाई 3 के प्रमेय 6 द्वारा, G का $\bigcap_{H \in \mathcal{F}} H$ 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 वाला G का न्यूनतम उपसमूह है। (क्योंकि यदि K, S को आविष्ट करने वाला G का एक उपसमूह है, तो $K \in \mathcal{F}$. अतः, $\bigcap_{H \in \mathcal{F}} H \subseteq K$.)

ये प्रेक्षण हमें निम्नलिखित परिभाषाओं पर पहुँचाते हैं।

परिभाषाएँ: मान लीजिए कि S किसी समूह G का एक अरिक्त उपसमुच्चय है।

i) S को आविष्ट करने वाला G का न्यूनतम उपसमूह **समुच्चय S द्वारा जनित उपसमूह** कहलाता है, तथा इसे $< \mathbf{S} >$ द्वारा व्यक्त किया जाता है।

इस प्रकार, $< S > = \cap\{H \mid H \leq G, S \subseteq H\}$.

ii) यदि $<S> = G$, तो हम कहते हैं कि **G समुच्चय S द्वारा जनित है**, तथा S, G का **जनक समुच्चय** कहलाता है।

iii) यदि समुच्चय S परिमित है, तो हम कहते हैं कि $<S>$ **परिमिततः जनित (finitely generated)** है।

उदाहरणार्थ, एक चक्रीय समूह $<g>$ परिमिततः जनित समूह है, जैसा कि $<a, b>$ भी है।

ध्यान दीजिए कि $<a, b>$ को $\{a, b\}$ जनित करता है, और $\{a, b, ab\}$ भी, क्योंकि $ab \in <a, b>$. अतः, **किसी उपसमूह का जनक समुच्चय अद्वितीय नहीं होता है।**

अन्य उदाहरणों को देने से पहले, हम $<S>$ की व्याख्या करने की एक दूसरी विधि देंगे। इस प्रमेय से $<S>$ को प्राप्त करना ज़्यादा सरल बन जाता है, परिभाषा की तुलना में।

ध्यान दीजिए कि प्रमेय 11 में a_i का भिन्न-भिन्न होना आवश्यक नहीं है, क्योंकि हो सकता है कि G आबेली नहीं हो।

प्रमेय 11: यदि S किसी समूह G का एक अरिक्त उपसमुच्चय है, तो

$$<S> = \{a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \,|\, a_i \in S \text{ और } n_i \in \mathbb{Z},\ 1 \le i \le k,\ k \in \mathbb{N} \text{ के लिए}\}.$$

उपपत्ति: मान लीजिए $A = \{a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} \,|\, a_i \in S \text{ और } n_i \in \mathbb{Z}, 1 \le i \le k \text{ के लिए}\}$.

क्योंकि $a_1, \dots, a_k \in S \subseteq <S>$ तथा $<S>$ समूह 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, $A \subseteq <S>$. …(15)

अब, आइए देखें कि $<S> \subseteq A$ क्यों है। हम दर्शाएँगे कि A एक उपसमूह है जिसमें S आविष्ट है। तब, $<S>$ की परिभाषा से, यह निष्कर्ष निकलेगा कि $<S> \subseteq A$.

क्योंकि किसी भी $a \in S$ को $a = a^1$ के रूप में लिखा जा सकता है, इसलिए $S \subseteq A$.

क्योंकि $S \ne \emptyset$, इसलिए $A \ne \emptyset$.

अब मान लीजिए कि $x, y \in A$. तब, $x = a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}$, $y = b_1^{m_1} b_2^{m_2} \dots b_r^{m_r}$, जहाँ $a_i, b_j \in S$ और $n_i, m_j \in \mathbb{Z}$, $1 \le i \le k, 1 \le j \le r$ के लिए।

तब, $xy^{-1} = (a_1^{n_1} a_2^{n_2} \dots a_k^{n_k})\,(b_1^{m_1} b_2^{m_2} \dots b_r^{m_r})^{-1}$

$$= (a_1^{n_1} a_2^{n_2} \dots a_k^{n_k})\,(b_r^{-m_r} \dots b_1^{-m_1}) \in A, \text{ परिभाषा द्वारा।}$$

अतः, प्रमेय 2, इकाई 3 द्वारा, G का A एक उपसमूह है।

इस प्रकार, A, S को आविष्ट करने वाला G का एक उपसमूह है।

अतः, $<S> \subseteq A$. …(16)

(15) और (16) से, $<S> = A$. ■

ध्यान दीजिए कि यदि $(G, +)$, S द्वारा जनित एक समूह है, तो G का कोई भी अवयव $n_1a_1 + n_2a_2 + \cdots + n_ra_r$ के रूप का होता है, जहाँ $a_1, a_2, \ldots, a_r \in S$ और $n_1, n_2, \ldots, n_r \in \mathbb{Z}$. यहाँ अवयवों a_i को भिन्न-भिन्न माना जा सकता है, क्योंकि G आबेली है।

आइए एक उदाहरण पर विचार करें।

उदाहरण 15: आप जानते हैं कि $\mathbb{Z}$ को $\{1\}$ या $\{-1\}$ जनित करता है। दर्शाइए कि $\mathbb{Z}$ विषम पूर्णांकों के समुच्चय $S = \{\pm 1, \pm 3, \pm 5, \ldots\}$ द्वारा भी जनित होता है।

हल: मान लीजिए कि $m \in \mathbb{Z}$. तब, $m = 2^r s$, जहाँ $r \geq 0$ और $s \in S$.

इस प्रकार, $m \in < S >$.

अतः, $\mathbb{Z} \subseteq < S >$.

निःसंदेह, $< S > \subseteq \mathbb{Z}$, क्योंकि $S \subseteq \mathbb{Z}$.

इस प्रकार, $< S > = \mathbb{Z}$.

***

उदाहरण 15 से आप देख सकते हैं कि एक चक्रीय समूह $< g >$ को एक ज़्यादा बड़े समुच्चय द्वारा भी जनित किया जा सकता है। जैसे कि $< g > = < g, g^2, g^3 >$, क्योंकि $g^2, g^3 \in < g >$.

यहाँ, संकेतन के बारे में एक टिप्पणी है।

टिप्पणी 4: यदि $G = < S >$ तथा $S = \{a_1, a_2, \ldots, a_n\}$ परिमित है, तो प्रायः हम धनुःकोष्ठकों (curly brackets) को न दिखाते हुए, $G = < a_1, a_2, \ldots, a_n >$ लिखते हैं।

अब निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E31) दर्शाइए कि $\mathbb{N}$ का एक उपसमुच्चय S समूह $\mathbb{Z}$ को जनित करता है यदि और केवल यदि S में ऐसे अवयव $s_1, \ldots, s_k$ हैं तथा $\mathbb{Z}$ में $n_1, \ldots, n_k$ हैं जिनसे कि $n_1s_1 + \cdots + n_ks_k = 1$.

E32) दर्शाइए कि यदि S एक समूह G को जनित करता है तथा $S \subseteq T \subseteq G$, तो T भी G को जनित करता है।

E33) दर्शाइए कि $D_{2n} = < r, R >$, जहाँ r एक परावर्तन है तथा $R = R_\theta$, जहाँ $\theta = \frac{360}{n}$, जैसे कि उपभाग 2.4.3, इकाई 2 में चर्चा की जा चुकी है।

E34) यदि $G_1 = < g_1 >$ और $G_2 = < g_2 >$, तो दर्शाइए कि $G_1 \times G_2$ को चक्रीय होना ज़रूरी नहीं है। आगे, $G_1 \times G_2$ के लिए एक जनक समुच्चय ज्ञात कीजिए।

(यह सवाल E27(iii) से जुड़ा हुआ है।)

इकाई 8 में आप देखेंगे कि $\mathbb{Z}_m \times \mathbb{Z}_n$ चक्रीय होता है यदि $(m, n) = 1$.

इकाई 9 में आप देखेंगे कि S_n भी परिमिततः जनित है $\forall\ n \in \mathbb{N}$.

इसके साथ हम जनकों की अपनी चर्चा ख़त्म करते हैं। हम इस इकाई को भी यहाँ ख़त्म कर रहे हैं। आइए अब इस इकाई में आपने जो पढ़ाई की है, उसका सारांश दें।

4.5 सारांश

इस इकाई में, हमने निम्नलिखित बातों पर चर्चा की है।

1. किसी समूह G के एक अवयव x की कोटि, $o(x)$, उस समूह G के चक्रीय उपसमूह $< x >$ की कोटि है।

2. यदि $o(x)$ परिमित है, तो $o(x)$ वह न्यूनतम धनात्मक पूर्णांक है जिससे कि $x^n = e$.

3. यदि $o(x) = n$ तथा $x^s = e$, किसी $s \in \mathbb{Z}$ के लिए, तो $n \mid s$.

4. यदि $o(x)$ अपरिमित है, तो $x^m \neq x^n$, यदि $m \neq n$, $\forall\ m, n \in \mathbb{Z}$.

5. $o(g) = o(xgx^{-1})\ \forall\ x, g \in G$, जहाँ G एक समूह है।

6. मान लीजिए कि G एक समूह है तथा $g \in G$.

   i) यदि g अपरिमित कोटि का है, तो प्रत्येक $m \in \mathbb{Z}^*$ के लिए g^m भी अपरिमित कोटि का है।

   ii) यदि $o(g) = n$, तो $o(g^m) = \dfrac{n}{(n, m)}\ \forall\ m = 1, \ldots, n-1$.

7. परिमित और अपरिमित चक्रीय समूहों के उदाहरण।

8. प्रत्येक चक्रीय समूह आबेली होता है।

9. चक्रीय समूह का प्रत्येक उपसमूह चक्रीय होता है।

10. मान लीजिए कि G कोटि n वाला एक परिमित चक्रीय समूह है। n के प्रत्येक धनात्मक भाजक m के लिए, G का कोटि m वाला एक अद्वितीय उपसमूह है। आगे, केवल ये ही G के उपसमूह हैं।

11. मान लीजिए कि $G = < g >$, $H = < g^m >$ और $K = < g^n >$.

    i) $H \leq K$ iff $n \mid m$.

    ii) $H \cap K = < g^s >$, जहाँ s, m और n का l.c.m है।

    iii) $HK \leq G$ और $HK = < g^d >$, जहाँ $d = (m, n)$.

    [ध्यान दीजिए कि यदि संक्रिया + है, तो (iii) कहता है कि $H + K = < d >$, जहाँ $d = (m, n)$.]

12. मान लीजिए कि $G = <g>$ कोटि n का है और d, n का एक धनात्मक भाजक है। तब, G के कोटि d वाले अवयवों की संख्या $\phi(d)$ होती है, जहाँ ϕ ऑयलर फ़ाइ-फलन है।

13. $S \subseteq G, S \neq \emptyset,$ द्वारा समूह G के जनित उपसमूह की परिभाषा और उदाहरण। इसे $<S>$ द्वारा व्यक्त किया जाता है।

14. यदि $G = <S>$, तो किसी भी $T \supseteq S$ के लिए $G = <T>$. विशिष्ट रूप से, $G = <G>$.

15. चक्रीय समूहों के अनुलोम गुणनफल का चक्रीय होना आवश्यक नहीं है।

4.6 हल / उत्तर

E1) i) $R_{90} \neq I, R_{90}^2 = R_{180} \neq I, R_{90}^3 = R_{270} \neq I, R_{90}^4 = R_{360} = I.$

$R_{180} \neq I, R_{180}^2 = R_{360} = I.$

इस प्रकार, $o(R_{90}) = 4, o(R_{180}) = 2.$

ii) यहाँ $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \neq I, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \neq I,$

$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \neq I, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$

इस प्रकार, $o(A) = 4.$

iii) सत्यापन कीजिए कि $n \cdot \overline{1} \neq \overline{0}, n \in \{1, 2, \ldots, 9\}$ के लिए तथा $10 \cdot \overline{1} = \overline{10} = \overline{0}.$ इस प्रकार, $o(\overline{1}) = 10.$

ध्यान दीजिए कि $\mathbb{Z}_{10} = <\overline{1}>.$

iv) किसी भी m के लिए, जहाँ $0 < m < n-1,$ $\overline{m} \in \mathbb{Z}_n$ तथा $\overline{m} = m \cdot \overline{1} \neq \overline{0},$, क्योंकि $n \nmid m.$

आगे, $\overline{n} = n \cdot \overline{1} = \overline{0}.$ इस प्रकार, $o(\overline{1}) = n.$

v) क्योंकि $n(-5) \neq 0 \quad \forall\ n \in \mathbb{N},$ इसलिए $o(-5)$ अपरिमित है।

vi) मान लीजिए कि $A = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}.$ तब, $nA = \begin{bmatrix} 2n & 3n \\ 4n & 5n \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \forall\ n \in \mathbb{N}.$

अतः, $o(A)$ अपरिमित है।

E2) क्योंकि $H \neq \{e\}$, इसलिए H में ऐसा अवयव a है, जहाँ $a \neq e$. क्योंकि $a \neq e$, इसलिए किसी भी $r \in \mathbb{Z}$ के लिए $a \neq e^r$. इसलिए $a \notin <e>$.
$\therefore H \neq <e>$.

E3) हम दर्शाएँगे कि $<a> \subseteq <a^{-1}>$ और $<a^{-1}> \subseteq <a>$.

अब, $<a>$ का कोई भी अवयव है $a^n = (a^{-1})^{-n}$, $n \in \mathbb{Z}$ के लिए।

$\therefore a^n \in <a^{-1}>$. $\therefore <a> \subseteq <a^{-1}>$.

इसी प्रकार, आपको यह दर्शाना चाहिए कि $<a^{-1}> \subseteq <a>$.

$\therefore <a> = <a^{-1}>$.

E4) मान लीजिए कि $H \le G$ s.t. $a \in H$. तब, प्रमेय 1 द्वारा, $<a> \subseteq H$.

इस प्रकार, $<a> \subseteq \cap\{H \mid H \le G$ और $a \in H\}$.

साथ ही, $<a> \le G$ s.t. $a \in <a>$.

अतः, $\cap\{H \mid H \le G$ और $a \in H\} \subseteq <a>$.

इसलिए $<a> = \cap\{H \mid H \le G$ और $a \in H\}$.

E5) E1(iv) से आप जानते हैं कि $o(\bar{1}) = n$.

अतः, $<\bar{1}> \le \mathbb{Z}_n$ तथा दोनों की कोटि एक ही है। इसलिए, $\mathbb{Z}_n = <\bar{1}>$.

E6) क्योंकि $A \neq \mathbf{0}$, इसलिए किसीं $i = 1, 2$ और $j = 1, 2, 3$ के लिए $a_{ij} \neq 0$.

तब, $na_{ij} \neq 0 \ \forall \ n \in \mathbb{N}$.

अतः, $nA \neq \mathbf{0} \ \forall \ n \in \mathbb{N}$.

इस प्रकार, $o(A)$ अपरिमित है।

E7) $A \neq I$, $A^2 = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix} = I$, यदि $r = 1$. अतः, $o(A) = 2$ यदि $r = 1$.

अब मान लीजिए कि $r \neq 1$.

व्यापक रूप से आपको सत्यापन करना चाहिए कि $A^{2n+1} \neq I \ \forall \ n \in \mathbb{N}$, तथा

$$A^{2n} = \begin{bmatrix} r^n & 0 \\ 0 & r^n \end{bmatrix}.$$

इस प्रकार, यदि r एक का एक वास्तविक nवाँ मूल है, तो $o(A) = 2n$. अन्यथा $o(A)$ अपरिमित होता है।

E8) यहाँ $\emptyset$ तत्समक अवयव है।

यदि $A = \emptyset$, तो $o(A) = 1$.

यदि $A \neq \emptyset$, तो $A \Delta A = \emptyset$, अतः, $o(A) = 2$.

E9) i) मान लीजिए कि $d = (n, m)$. तब, $d \mid n$ और $d \mid m$.

प्रमेय 4 द्वारा, $o(g^m) = \frac{n}{d}$.

साथ ही, $o(g^{(n,m)}) = o(g^d) = \frac{n}{(n,d)} = \frac{n}{d}$, क्योंकि $d \mid n$.

अतः, $o(g^m) = o(g^{(n,m)})$.

ii) $G = < g^m >$ iff $o(g^m) = n$ iff $(m, n) = 1$, प्रमेय 4(ii) द्वारा।

E10) $\mathbb{Z}_{18}$ में $o(\bar{1}) = 18$. इसलिए,

$o(\bar{2}) = o(2 \cdot \bar{1}) = \frac{18}{(18, 2)} = 9$.

$o(\bar{4}) = \frac{18}{(18, 4)} = \frac{18}{2} = 9$. (ध्यान दीजिए कि $\bar{4} = 2.\bar{2}$, है, परंतु $o(\bar{4}) = o(\bar{2})$.)

साथ ही, $o(\bar{5}) = \frac{18}{(18, 5)} = \frac{18}{1} = 18$.

(इस प्रकार, $\mathbb{Z}_{18} = < \bar{5} >$ भी।)

E11) मान लीजिए कि $G = < g >$, जहाँ $o(g) = n$. मान लीजिए कि $x \in G$. तब, $x = g^m$, किसी m के लिए, जहाँ $0 \leq m < n$.

यदि $x = e$, तो $1 \mid n$. $o(x) = 1$ और यदि

$x \neq e$, तब $o(x) = o(g^m) = \frac{n}{(n, m)}$. अतः, $o(x) \mid n$. मान लीजिए कि $o(x) = r$.

क्योंकि $r \mid n$, मान लीजिए कि $n = rs$.

तब, $x^{o(G)} = x^n = x^{rs} = (x^r)^s = e$.

E12) क्योंकि $o(\zeta) = 10$, इसलिए $o(\zeta^3) = \frac{10}{(10, 3)} = 10$.

E13) $o(x^2) = \frac{15}{(15, 2)} = 15$, $o(x^6) = \frac{15}{(15, 6)} = \frac{15}{3} = 5$, $o(x^{10}) = \frac{15}{(15, 10)} = 3$.

E14) $o(x) = n$. इसलिए $x^m \cdot x^{n-m} = x^n = e$.

इस प्रकार, $(x^m)^{-1} = x^{n-m}$.

अतः, E3 द्वारा, $< x^m > = < x^{n-m} >$.

इसलिए, $o(x^m) = o(x^{n-m})$, अर्थात् $\frac{n}{(n, m)} = \frac{n}{(n, n-m)}$.

अतः, $(n, m) = (n, n-m)$.

E15) क्योंकि E14 से $(30, 25) = (30, 5)$, इसलिए $< \overline{25} > = < \overline{5} >$. अतः,

$< \overline{25} > = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}\}$.

$< \zeta^7 > = < \zeta > = U_{10}$, क्योंकि $(7, 10) = 1$.

E16) क्योंकि D_8 आबेली नहीं है, इसलिए यह चक्रीय नहीं हो सकता है।

E17) मान लीजिए कि G एक अन्आबेली समूह है। तब, $G \neq \{e\}$.

मान लीजिए कि $g \in G, g \neq e$. तब, $< g > \leq G, < g > \neq \{e\}$. साथ ही, $G \neq < g >$, क्योंकि G अन्आबेली है।

अतः, $< g >$ समूह G का एक उचित अतुच्छ उपसमूह है।

E18) उदाहरण 9 से, $9\mathbb{Z} \leq m\mathbb{Z}$ iff $m \mid 9$, अर्थात् $m = 1, 3, 9$.

इस प्रकार, $9\mathbb{Z}$ केवल $\mathbb{Z}, 3\mathbb{Z}$ और $9\mathbb{Z}$ का उपसमूह है।

E19) i) हम सिद्ध करेंगे कि $H \leq K$ iff $r \mid m$.

पहले तो यदि $H \leq K$, तो $g^m \in < g^r > = K$.

विभाजन कलन-विधि से, $m = qr + r'$ किन्हीं $q, r' \in \mathbb{Z}$ के लिए, जहाँ $0 \leq r' < r$. तो $g^m \cdot (g^r)^{-q} \in K$, यानी, $g^{r'} \in K$.

परंतु, प्रमेय 6 द्वारा, r न्यूनतम धनात्मक पूर्णांक है s.t. $g^r \in K$.

अतः, $r' = 0$, अर्थात् $m = qr$, अर्थात् $r \mid m$.

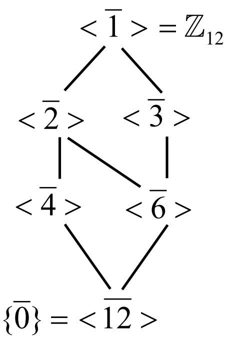
विलोमतः, यदि $r \mid m$, तो किसी $s \in \mathbb{Z}$ के लिए $m = rs$.

इसलिए, $g^m = (g^r)^s \in K$. अतः, $H \subseteq K$, अर्थात् $H \leq K$, E10, इकाई 3 द्वारा।

ii) उदाहरण 9 की ही तरह, दर्शाइए कि यदि $H \leq K$, तो $n \mid m$.

फिर, दर्शाइए कि यदि $n \mid m$, तो $H \le K$.

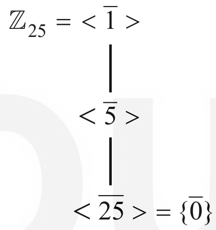
E20) $\mathbb{Z}_{12}$ के उपसमूह $\{\bar{0}\} = <\overline{12}>, <\bar{6}>, <\bar{4}>, <\bar{3}>, <\bar{2}>$ और $<\bar{1}> = \mathbb{Z}_{12}$ है। इसका आरेख आकृति 5 में दिया गया है। यह संरचनात्मक रूप से आकृति 2 के आरेख के समान ही है, जहाँ $<\zeta^i>$ को $<\bar{i}>$ से प्रतिस्थापित किया गया है।



आकृति 5: $\mathbb{Z}_{12}$ के लिए एक उपसमूह आरेख

E21) 25 के धनात्मक भाजक 1, 5 और 25 हैं। अतः, $\mathbb{Z}_{25}$ के उपसमूह $<\bar{1}>, <\bar{5}>$ और $<\overline{25}>$ हैं।

संगत आरेख आकृति 6 में दिया है।



आकृति 6: $\mathbb{Z}_{25}$ के लिए एक उपसमूह आरेख

E22) $\mathbb{Z}_p = <\bar{1}>$, जहाँ $\bar{1}$, $1 (\bmod p)$ वाला समशेषता वर्ग है।

इसलिए,

$o(\mathbb{Z}_p) = p$. क्योंकि p के भाजक केवल 1 और p हैं, इसलिए प्रमेय 7 से $\mathbb{Z}_p$ के उपसमूह केवल $<\bar{1}>$ और $<\bar{p}> = <\bar{0}>$ हैं।

अतः, $\mathbb{Z}_p$ का कोई अतुच्छ उचित उपसमूह नहीं है।

E23) प्रमेय 6 द्वारा, कोई भी उपसमूह H, $<\bar{m}>$ के रूप का होता है, जहाँ m ऐसा न्यूनतम धनात्मक पूर्णांक है कि $\bar{m} \in H$.

आगे, प्रमेय 7 द्वारा, यदि n के धनात्मक भाजक $m_1, m_2, \ldots, m_r$ हैं, तो उपसमूह $H_1, H_2, \ldots, H_r$ हैं, जहाँ $H_i = <\overline{\left(\frac{n}{m_i}\right)}>$.

E24) $\mathbb{Z}_{30} = <\bar{1}>$, जहाँ $o(\bar{1}) = 30$.

$\mathbb{Z}_{30}$ में $\bar{4}$ और $\bar{6}$ का l.c.m $= \overline{12}$ तथा $(\bar{4}, \bar{6}) = \bar{2}$.

अतः, $<\bar{4}> \cap <\bar{6}> = <\overline{12}>$ तथा $<\bar{4}> + <\bar{6}> = <\bar{2}>$.

E25) $HK = <\zeta^8><\zeta^{10}> = <\zeta^d>$, जहाँ $d = (8, 10) = 2$.

$H \cap K = <\zeta^\ell>$, जहाँ ℓ, 8 और 10 का l.c.m है यानी $\ell = 40$

अब, $\zeta^{40} = \zeta^4$, U_{12} में। अतः, $H \cap K = <\zeta^4>$.

E26) इकाई 3 से, आप जानते हैं कि यदि A और B, G के उपसमूह हैं, तो $A \cup B \leq G$ iff $A \subseteq B$ या $B \subseteq A$.

इस प्रकार, जब भी उचित उपसमूहों का सम्मिलन एक उपसमूह होता है, तो वह केवल एक उचित उपसमूह ही हो सकता है। अतः, यह G कभी नहीं हो सकता है।

E27) i) किसी भी अभाज्य संख्या p के लिए, $(m, p) = 1 \ \forall \ m$ s.t. $1 \leq m < p$, अंकगणित के मूलभूत प्रमेय द्वारा।

अतः, $\phi(p) = p - 1$.

ii) प्रमेय 7 द्वारा, प्रत्येक $d \mid n$ के लिए, $< g^{n/d} >$ समूह $< g >$ का कोटि d वाला एक अद्वितीय उपसमूह है, जहाँ $o(g) = n$.

साथ ही, $< g^{n/d} >$ के जनकों की संख्या $\phi(d)$ है।

आगे, प्रत्येक i के लिए s.t. $1 \leq i \leq n$, $o(g^i) = d$, किसी $d \mid n$ के लिए।

अतः, $n = \sum_{d \mid n} \phi(d)$.

iii) $\phi(4) = 2$, क्योंकि 1 और 3 दोनों 4 के सापेक्षतः अभाज्य हैं। साथ ही, $\phi(2) = 1$.

अतः, $\phi(4) = \phi(2 \times 2) \neq \phi(2)\phi(2)$.

E28) क्योंकि $<\overline{25}> = <\overline{5}>$, इसलिए $o(\overline{25}) = 6$.

$\mathbb{Z}_{30}$ में कोटि 6 वाले अवयवों की संख्या $\phi(6) = 2$ है।

ये हैं $1 \cdot \overline{25}$ और $5 \cdot \overline{25}$, अर्थात् $\overline{25}$ और $\overline{5}$.

$o(\zeta^3) = 10$, क्योंकि $(3, 10) = 1$.

$\phi(10) = 4$. ये संख्याएँ 1, 3, 7 और 9 हैं।

इस प्रकार, $<\zeta^3>$ के सभी जनक ζ, ζ^3, ζ^7 और ζ^9 हैं।

E29) $<1> = \{1\}$, क्योंकि $1^n = 1 \ \forall \ n \in \mathbb{Z}$.

अतः, $<1>$ परिमित है।

E30) i) असत्य है। उदाहरणार्थ, $\mathbb{Z} \leq \mathbb{Q}$, परंतु $\mathbb{Q}$ चक्रीय नहीं है, जैसा आप उदाहरण 7 में देख चुके हैं।

ii) सत्य है। प्रमेय 10 द्वारा, केवल $\{e\}$ परिमित उपसमूह है।

iii) असत्य है। उदाहरण 14 को देखिए।

E31) पहले, मान लीजिए कि $\mathbb{Z} = < S >$.

क्योंकि $1 \in \mathbb{Z}$, इसलिए $\exists\ n_1, \ldots, n_k \in \mathbb{Z}$ और $s_1, \ldots, s_k \in S$ s.t. $1 = \sum_{i=1}^{k} n_i s_i$.

विलोमतः, मान लीजिए कि $1 = n_1 s_1 + \cdots + n_k s_k$, $n_i \in \mathbb{Z}$, $s_i \in S$.

तब, किसी भी $m \in \mathbb{Z}$ के लिए, $m = m \cdot 1 = m(n_1 s_1 + \cdots + n_k s_k) \in < S >$.

अतः, $\mathbb{Z} \subseteq < S >$.

क्योंकि $S \subseteq \mathbb{Z}$, इसलिए $< S > \subseteq \mathbb{Z}$.

इस प्रकार, $\mathbb{Z} = < S >$.

E32) $G = < S >$ और $S \subseteq T$. इसलिए $G = < S > \subseteq < T > \leq G$.

अतः, $G = < T >$.

E33) इकाई 2 से आप जानते हैं कि D_{2n} का कोई भी अवयव R^i या rR^i, $i = 0, 1, \ldots, n-1$, के रूप का होता है। अतः, $D_{2n} \subseteq < r, R > \subseteq D_{2n}$. इस प्रकार, $D_{2n} = < r, R >$.

E34) $\mathbb{Z} \times \mathbb{Z}$ पर विचार कीजिए। यदि यह चक्रीय होता और जनक (x, y) होता, तो $(1, 0) = (mx, my)$ और $(0, 1) = (nx, ny)$, किन्हीं $m, n \in \mathbb{Z}$ के लिए। अतः, $mx = 1, my = 0, nx = 0$ और $ny = 1$.

$my = 0 \Rightarrow m = 0$ या $y = 0$. परंतु, तब $mx = 1$ और $ny = 1$ संभव नहीं है।

हम एक अंतर्विरोध पर पहुँचते हैं।

अतः, $\mathbb{Z} \times \mathbb{Z}$ चक्रीय नहीं है।

$G_1 \times G_2$ का कोई भी अवयव का रूप है $(g_1^{n1}, g_2^{n2}) = (g_1^{n1}, e_2)(e_1, g_2^{n2}) = (g_1, e_2)^{n1}(e_1, g_2)^{n2}$, $n_1, n_2 \in \mathbb{Z}$, जहाँ e_1 और e_2 क्रमशः G_1 और G_2 के तत्समक हैं।

अतः, $G_1 \times G_2 = < (g_1, e_2), (e_1, g_2) >$.

विविध उदाहरण और प्रश्न

नीचे दिए हुए कुछ उदाहरण और प्रश्न, इस खंड में आपके द्वारा अध्ययन की गई संकल्पनाओं और प्रक्रियाओं पर आधारित हैं। इन उदाहरणों का अध्ययन करने से, तथा प्रश्नों को हल करने से, आपको संबंधित संकल्पनाओं की बेहतर समझ प्राप्त होगी। यह आपको ऐसे सवालों को हल करने में और अधिक अभ्यास भी देगा।

उदाहरण 1: निम्नलिखित में से कौन-से कथन सत्य हैं? अपने उत्तरों के लिए कारण दीजिए।

i) किसी समुच्चय S पर एक द्वि-आधारी संक्रिया का प्राँत S होता है।

ii) यदि $(G,\cdot)$ एक आबेली समूह है, तो $x^2 = e \;\forall\; x \in G.$

iii) यदि $n, m \in \mathbb{N},$ तो $[n, m](n, m) = nm.$

हल: i) असत्य। प्राँत $S \times S$ है।

ii) असत्य। उदाहरणार्थ, $\mathbb{Z}$ आबेली है, परंतु $2n \neq 0 \;\forall\; n \neq 0.$

iii) सत्य। यहाँ हम अद्वितीय गुणनखंडन प्रमेय का उपयोग करते हैं।

मान लीजिए कि $n = p_1^{n_1} \ldots p_r^{n_r}$ तथा $m = p_1^{m_1} \ldots p_r^{m_r}$, जहाँ $n_i \geq 0,\ m_i \geq 0,$ $i = 1, \ldots, r$ के लिए।

मान लीजिए $s_i = \min(n_i, m_i)$ और $t_i = \max(n_i, m_i)\ \forall i = 1,\ldots, r.$ तब $(n,m) = p_1^{s_1} p_2^{s_2} \ldots p_r^{s_r}$ और $[n,m] = p_1^{t_1} p_2^{t_2} \ldots p_r^{t_r}.$

(उदाहरणार्थ, 15 और 100 पर विचार कीजिए। अब, $15 = 2^0 \cdot 3^1 \cdot 5^1$ तथा $100 = 2^2 \cdot 3^0 \cdot 5^2.$ अतः, $(15, 100) = 2^0 \cdot 3^0 \cdot 5^1$ तथा $[15, 100] = 2^2 \cdot 3^1 \cdot 5.$)

साथ ही, $s_i + t_i = n_i + m_i \;\forall\; i = 1, \ldots r.$

तब,
$$(n, m)[n, m] = p_1^{s_1+t_1} \cdot p_2^{s_2+t_2} \ldots p_r^{s_r+t_r}$$
$$= p_1^{n_1+m_1} \ldots p_r^{n_r+m_r}$$
$$= (p_1^{n_1} \ldots p_r^{n_r})(p_1^{m_1} \ldots p_r^{m_r})$$
$$= nm.$$

***

उदाहरण 2: मान लीजिए कि $G = GL_2(\mathbb{Q}).$ मान लीजिए कि $X \in G.$ सिद्ध कीजिए कि $A * B = X^{-1}ABX$ द्वारा $G \times G$ पर परिभाषित संक्रिया $*$, G पर एक द्वि-आधारी संक्रिया है। आगे, क्या $(G, *)$ एक समूह है? क्यों, या क्यों नहीं?

हल: पहले तो, $A, B \in G$ के लिए, $\det(A) \neq 0, \det B \neq 0.$

$\therefore \det(X^{-1}ABX) = [\det(X)]^{-1}\det(A)\det(B)\det(X) \neq 0.$

साथ ही, $X^{-1}ABX$ की सभी प्रविष्टियाँ $\mathbb{Q}$ से हैं।

इस प्रकार, $X^{-1}ABX \in G.$

अतः, G पर $*$ संवृत है।

आगे, ऐसा कोई $Y \in G$ नहीं है s.t. $A * Y = A \ \forall\ A \in G.$

इसका कारण है कि $A * Y = A$ iff $Y = A^{-1}XAX^{-1}$.

अतः, उदाहरणार्थ, यदि X के साथ A क्रमविनिमेय नहीं होता है, तो

$$I * Y = X^{-1}YX = X^{-1}A^{-1}XAX^{-1}X$$

$$= X^{-1}A^{-1}XA \neq I.$$

अतः, $(G, *)$ एक समूह नहीं है।

***

उदाहरण 3: सिद्ध कीजिए कि यदि $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$ एक धनात्मक पूर्णांक है, तो $a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod 9$.

इससे सिद्ध कीजिए कि a, 9 का गुणज है iff $9 | (a_0 + a_1 + \cdots + a_n)$.

हल: $m \in \mathbb{N}$ के लिए, $10^m = (10^m - 1) + 1 = (10-1)(10^{m-1} + 10^{m-2} + \cdots + 10 + 1) + 1$

$$= 9(10^{m-1} + \cdots + 1) + 1.$$

अतः, $a = 9[a_n(10^{n-1} + \cdots + 1) + a_{n-1}(10^{n-2} + \cdots + 1) + \cdots + a_2(10+1) + a_1]$

$$+ (a_n + a_{n-1} + \cdots + a_1 + a_0).$$

$\therefore a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod 9.$

अब, $9 | a \Leftrightarrow a \equiv 0 \pmod 9 \Leftrightarrow a_n + a_{n-1} + \cdots + a_0 \equiv 0 \pmod 9$

$$\Leftrightarrow 9 | (a_n + \cdots + a_0).$$

***

उदाहरण 4: दर्शाइए कि $(\mathbb{Z}, *)$ एक समूह है, जहाँ एक स्थिर $a \in \mathbb{Z}$ के लिए, $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : *(m, n) = m + n + a$ है।

हल: सर्वप्रथम दिखाइए कि $\mathbb{Z}$ पर $*$ एक सुपरिभाषित द्वि-आधारी संक्रिया है।

आगे, $\mathbb{Z}$ में + साहचर्य और क्रमविनिमेय होता है, इन गुणों का उपयोग करते हुए दिखाइए कि $(m*n)*p = m*(n*p)\ \forall\ m, n, p \in \mathbb{Z}$.

तीसरी बात, जाँच कीजिए कि $m*(-a) = m = (-a)*m\ \forall\ m \in \mathbb{Z}$.

अंत में, जाँच कीजिए कि $m*(-2a-m) = (-2a-m)*m = (-a)\ \forall\ m \in \mathbb{Z}$.

अतः, $(\mathbb{Z}, *)$ एक समूह है।

***

उदाहरण 5: $\mathbb{R}$ पर एक संबंध ~ '$x \sim y$ iff $x - y \in \mathbb{Z}$ है' द्वारा परिभाषित कीजिए। जाँच कीजिए कि $\mathbb{R}$ पर ~ एक तुल्यता संबंध है या नहीं। यदि है, तो $[\pi]$ ज्ञात कीजिए। यदि ~, $\mathbb{R}$ पर एक तुल्यता संबंध नहीं है, तो $\mathbb{R}$ का एक ऐसा उपसमुच्चय ज्ञात कीजिए, जिस पर यह तुल्यता संबंध है।

हल: क्योंकि $x - x = 0 \in \mathbb{Z}\ \forall\ x \in \mathbb{R}$, इसलिए ~ स्वतुल्य है।

यह भी दर्शाइए कि ~ क्यों सममित और संक्रामक है।

अतः, $\mathbb{R}$ पर ~ एक तुल्यता संबंध है।

आगे, $[\pi] = \{x \in \mathbb{R} \mid x \sim \pi\} = \{x \in \mathbb{R} \mid x - \pi \in \mathbb{Z}\}$

$= \{\pi + n \mid n \in \mathbb{Z}\}$.

***

विविध प्रश्नावली

E1) जाँच कीजिए कि $A = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| a, b \in \mathbb{R} \right\}$ और $B = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \middle| a \in \mathbb{R} \right\}$,

$(\mathbb{M}_2(\mathbb{R}), +)$ के उपसमूह हैं या नहीं।

क्या $A \cap GL_2(\mathbb{R}) \le (GL_2(\mathbb{R}), \cdot)$? क्यों, या क्यों नहीं?

E2) $(\wp(X), \Delta)$ के एक उचित अतुच्छ चक्रीय उपसमूह का उदाहरण दीजिए, जहाँ $X = \{x_1, x_2\}$.

E3) यदि G एक समूह है s.t. $(xy)^2 = x^2y^2\ \forall\ x, y \in G$, तो G आबेली है। क्या यह कथन सत्य है? अपने उत्तर के लिए कारण दीजिए।

E4) दर्शाइए कि $(\mathbb{Z}[\sqrt{n}], +)$ एक समूह है, जहाँ n एक वर्ग-मुक्त पूर्णांक है।

E5) A को $\mathbb{M}_2(\mathbb{Z}_7)$ का, तथा $GL_2(\mathbb{Z}_7)$ का, अवयव मानते हुए $o(A)$ ज्ञात कीजिए, जहाँ $A = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix}$.

E6) क्या D_8 का D_6 एक उपसमूह है? क्यों, या क्यों नहीं?

E7) i) मान लीजिए कि G एक आबेली समूह है तथा $T = \{g \in G \mid o(g) < \infty\}$. दर्शाइए कि $T \leq G$. (T को G का **विमोटन उपसमूह** कहते हैं।)

ii) $\mathbb{Z} \times K_4$ का विमोटन उपसमूह मालूम कीजिए।

E8) निम्नलिखित में से कौनसे कथन सत्य हैं? अपने उत्तरों की पुष्टि कीजिए।

i) यदि G एक समूह है और $n \in \mathbb{N}$, तो G का $\{g^n \mid g \in G\}$ एक उपसमूह है।

ii) यदि G एक अन्आबेली समूह है और $n \in \mathbb{N}$, तो G का $\{g \in G \mid o(g) = n\}$ एक उपसमूह है।

iii) $\mathbb{Z}_{45}$ के 6 और केवल 6 अलग-अलग उपसमूह हैं।

iv) यदि G एक समूह है जिसके क्रमशः कोटियों n और m वाले दो अवयव x और y हैं, तो $o(xy) = [n, m]$, n और m का l.c.m.

v) यदि G एक अपरिमित समूह है और $x \in G$ ऐसा है कि $o(x)$ अपरिमित है, तो $G = < x >$.

E9) सिद्ध कीजिए कि यदि X एक अपरिमित समुच्चय है, तो सममितियों का समुच्चय $S(X)$ अपरिमित है।

E10) i) यदि $\sigma = (1\,2\,3\,4\,5\,6) \in S_{10}$, तो किन $n \in \mathbb{N}$ के लिए σ^n भी एक 6-चक्र होगा?

ii) सिद्ध कीजिए कि यदि $\sigma = (1\,2 \ldots m)$, तो σ^n लंबाई m वाला एक चक्र है iff $(n, m) = 1$. यहाँ $m, n \in N$.

E11) दर्शाइए कि यदि G कोटि n वाला एक अचक्रीय समूह है, तो G में कोटि n वाला कोई अवयव नहीं है।

E12) क्रमचय $(3\,5\,7)(1\,3\,5)(5\,7)$ को असंयुक्त चक्रों के एक गुणनफल के रूप में लिखिए। क्या यह क्रमचय सम है? अपने उत्तर के लिए कारण दीजिए।

E13) समूह $(\mathbb{Z}_{36}, +)$ में निम्नलिखित अवयवों की कोटियाँ ज्ञात कीजिए:

$\overline{1}, -\overline{1}, \overline{5}, \overline{6}, \overline{13}, -\overline{13}$

E14) $\mathbb{Z}$ के एक दिए हुए अवयव c के लिए, c पर किन प्रतिबंधों के अधीन $(\mathbb{Z}, *)$ एक समूह होगा, जहाँ $*$, $a * b = ab + a + b + c$ द्वारा परिभाषित है?

E15) जाँच कीजिए कि आव्यूह गुणन के सापेक्ष $GL_2(\mathbb{Z}_4)$ और $GL_2(\mathbb{Z}_5)$ समूह हैं या नहीं।

हल / उत्तर

E1) उपसमूह परीक्षण के अनुप्रयोग से तय कीजिए कि A और B, $(\mathbb{M}_2(\mathbb{R}), +)$, के उपसमूह हैं।

$A \cap GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| a^2 \neq b^2, \ a, \ b \in \mathbb{R} \right\}$. उपसमूह परीक्षण द्वारा, यह $(GL_2(\mathbb{R}), \cdot)$ का एक उपसमूह है।

E2) किसी भी $A \in \wp(X)$ के लिए, $A \Delta A = \emptyset$, $(A \Delta A) \Delta A = A, \ldots .$

अतः $A^n = \emptyset$ यदि n सम है, और $A^n = A$ यदि n विषम है।

इस प्रकार, $< A > = \{\emptyset, A\}$.

अतः, यदि $A = \{x_1\}$, तो $< A >$, $\wp(X)$ का एक उचित अतुच्छ चक्रीय उपसमूह है।

E3) सत्य है। क्योंकि $xyxy = xxyy \ \forall \ x, y \in G$. दाएँ और बाएँ पक्षों पर निरसन द्वारा, हम $yx = xy \ \forall \ x, y \in G$ प्राप्त करते हैं। अर्थात्, G आबेली है।

E4) $\mathbb{Z}[\sqrt{n}] \subseteq \mathbb{C}$ तथा $\mathbb{Z}[\sqrt{n}] \neq \emptyset$.

अब, यदि $a + b\sqrt{n}, c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, तो

$(a + b\sqrt{n}) - (c + d\sqrt{n}) = (a - c) + (b - d)\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$.

अतः, $\mathbb{Z}[\sqrt{n}] \leq \mathbb{C}$. इस प्रकार, $(\mathbb{Z}[\sqrt{n}], +)$ एक समूह है।

E5) के लिए $n \in \mathbb{N}, n\begin{bmatrix} \overline{1} & \overline{0} \\ \overline{1} & \overline{1} \end{bmatrix} = \begin{bmatrix} \overline{n} & \overline{0} \\ \overline{n} & \overline{n} \end{bmatrix}$.

इस प्रकार, न्यूनतम n, जिसके लिए $nA = \mathbf{0}$ है, $n = 7$ है।

$\therefore \mathbb{M}_2(\mathbb{Z}_7)$ में $o(A) = 7$ है।

$A \in GL_2(\mathbb{Z}_7)$ भी है, क्योंकि $\det(A) = \overline{1} \neq \overline{0}$.

अब, $A = I + \begin{bmatrix} \overline{0} & \overline{0} \\ \overline{1} & \overline{0} \end{bmatrix}$.

अतः, $A^n = I + \begin{bmatrix} \overline{0} & \overline{0} \\ \overline{n} & \overline{0} \end{bmatrix}, n \in \mathbb{N}$ के लिए।

$\therefore GL_2(\mathbb{Z}_7)$ में $o(A) = 7$ है, क्योंकि $7 \cdot \overline{1} = \overline{0}$.

E6) क्योंकि $R_{120} \in D_6$ और $R_{120} \notin D_8$, इसलिए $D_6 \not\subset D_8$. अतः, $D_6 \not< D_8$.

E7) i) सर्वप्रथम, $e \in T$. अतः, $T \neq \emptyset$.

आगे, $g \in T$ के लिए, $o(g^{-1}) = o(g) < \infty$. अतः, $g^{-1} \in T$.

अंत में, यदि $g_1, g_2 \in T$, तो $o(g_1 g_2) \leq o(g_1)o(g_2) < \infty$.

अतः,, $g_1 g_2 \in T$.

इस प्रकार, $T \leq G$.

ii) ध्यान दीजिए कि $o(a, b) = \max(o(a), o(b))\ \forall\ a \in \mathbb{Z}, b \in K_4$.

साथ ही, $\mathbb{Z}$ में परिमित कोटि वाला अवयव सिर्फ़ 0 है, और $o(x) < \infty\ \forall\ x \in K_4$. अतः, $T = \{(0, x) \mid x \in K_4\} = \{0\} \times K_4$.

E8) i) यदि G आबेली है, तो यह सत्य है, अन्यथा नहीं। S_3 और $n = 3$ को लेकर अन्आबेली G के लिए एक प्रति-उदाहरण दीजिए।

ii) असत्य। पुनः, $G = S_3$ और $n = 2$ लेकर एक प्रति-उदाहरण दीजिए।

iii) सत्य। 45 के प्रत्येक धनात्मक भाजक के लिए, $\mathbb{Z}_{45}$. का एक अद्वितीय उपसमूह है। ये भाजक 1, 3, 5, 9, 15, 45 हैं।

iv) असत्य। उदाहरणार्थ, $\mathbb{Z}_8 = <\overline{1}>$ पर विचार कीजिए।

तब, $o(\overline{2}) = 4$ और $o(\overline{4}) = 2$. अर्थात्, $o(\overline{2} \cdot \overline{2}) = 2 \neq [4, 4]$.

v) असत्य। उदाहरणार्थ, $\mathbb{Z} = <1> \neq <2>$, परंतु $o(2)$ अपरिमित है।

E9) मान लीजिए कि $X = \{x_1, x_2, \ldots\}$.

तब, $(x_i\ x_{i+1}) \in S(X)\ \forall\ i \in \mathbb{N}$.

साथ ही, $(x_i\ x_{i+1}) \neq (x_j\ x_{j+1})$ जब तक $i = j$ नहीं हो, क्योंकि $(x_i\ x_{i+1})$ या तो x_j को नियत करता है या x_{j+1} को नियत करता है, या दोनों को, यदि $i \neq j$; परंतु $(x_j\ x_{j+1})$, x_j और x_{j+1} दोनों को हिलाता है।

अतः, $S(X)$ में $(x_i\ x_{i+1}), i \in \mathbb{N}$, के रूप के अनन्ततः अनेक पक्षांतरण हैं।

इसलिए, $S(X)$ अपरिमित है।

E10) i) $\sigma^2 = (1\ 3\ 5)(2\ 4\ 6)$, $\sigma^3 = (1\ 4)(2\ 5)(3\ 6)$,

$\sigma^4 = (1\ 5\ 3)(2\ 6\ 4)$, $\sigma^5 = (1\ 6\ 5\ 4\ 3\ 2)$,

$\sigma^6 = I$, $\sigma^7 = \sigma$, इत्यादि।

इस प्रकार, σ^n केवल तभी 6-चक्र है जबकि $n = 1, 5, 1+6, 5+6, \ldots$, यानी

$n \in \{1+6k, 5+6k \mid k \in \mathbb{N}\}$.

ध्यान दीजिए कि σ^n एक 6-चक्र होगा iff $o(\sigma^n) = 6 = o(\sigma)$.

परंतु, $o(\sigma^2) = \frac{o(\sigma)}{2} \neq o(\sigma)$. इसी प्रकार, $o(\sigma^3) = \frac{o(\sigma)}{3}$.

व्यापक रूप से, $o(\sigma^n) = \frac{6}{(6, n)}$ होता है।

ii) σ^n एक m-चक्र है iff $o(\sigma^n) = m$.

साथ ही, $o(\sigma^n) = \frac{m}{(n, m)}$.

$\therefore \sigma^n$ एक m-चक्र है iff $\frac{m}{(n, m)} = m$, अर्थात्, $(n, m) = 1$.

E11) आप इस कथन के प्रतिधनात्मक को सिद्ध कर सकते हैं। अर्थात्, सिद्ध कर सकते हैं कि यदि G में कोटि n वाला एक अवयव x है, तो $G = < x >$ होगा।

यहाँ नोट करें कि $< x > \leq G$, और दोनों समूह समान कोटि के हैं।

E12) $(3\ 5\ 7)(1\ 3\ 5)(5\ 7) = (5\ 3\ 7\ 1)$, एक 4-चक्र.

क्योंकि $(5\ 3\ 7\ 1) = (5\ 1)(5\ 7)(5\ 3)$, जो 3 पक्षांतरणों का एक गुणनफल है, इसलिए यह एक विषम क्रमचय है।

E13) $o(\overline{1}) = 36$, क्योंकि $35 \cdot \overline{1} \neq \overline{0}$ और $36 \cdot \overline{1} = \overline{0}$; $o(-\overline{1}) = 36$;

$o(\overline{5}) = 36$, क्योंकि $(5, 36) = 1$; $o(\overline{6}) = 6$, $o(\overline{13}) = 36$, $o(-\overline{13}) = o(\overline{23}) = 36$.

E14) जाँच कीजिए कि $\mathbb{Z}$ पर $*$ एक द्वि-आधारी संक्रिया है।

क्योंकि $(\mathbb{Z}, *)$ एक समूह है, इसलिए $\mathbb{Z}$ पर $*$ साहचर्य है।

इससे दर्शाइए कि c को शून्य होना चाहिए।

तब, जोड़ का तत्समक 0 होना चाहिए।

परंतु, तब $\mathbb{Z}^*$ के किसी भी अवयव का $*$ के सापेक्ष प्रतिलोम नहीं होगा। (क्यों?)

इस प्रकार, किसी भी c के लिए, $(\mathbb{Z}, *)$ एक समूह नहीं है।

E15) $GL_2(\mathbb{Z}_4) = \left\{ \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} \in \mathbb{M}_2(\mathbb{Z}_4) \middle| \overline{a}\,\overline{d} - \overline{b}\,\overline{c} \neq \overline{0} \right\}$.

अब, $\begin{bmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{2} \end{bmatrix} \in GL_2(\mathbb{Z}_4)$. मान लीजिए कि $\begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix}$ इसका प्रतिलोम है। तब,

$$\begin{bmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{2} \end{bmatrix} \begin{bmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{bmatrix} = \begin{bmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{bmatrix}.$$

अतः, $\mathbb{Z}_4$ में $\overline{2d} = \overline{1}$. अतः, $4 \mid (1-2d)$. अर्थात्, किसी $x \in \mathbb{Z}$ के लिए, $4x = 1-2d$. अतः, $\mathbb{Z}$ में $2d + 4x = 1,$ यानी $2(d+2x) = 1,$ जो संभव नहीं है। इस प्रकार, $GL_2(\mathbb{Z}_4)$ में प्रत्येक अवयव का प्रतिलोम नहीं है। अतः, यह आव्यूह गुणन के सापेक्ष एक समूह नहीं है।

परंतु, $(GL_2(\mathbb{Z}_5), \cdot)$ एक समूह है, जिसकी आपको जाँच करनी चाहिए।

शब्दावली

Abelian (Non-abelian)	आबेली (अन्‌आबेली)
Action	क्रिया
Additive identity	योज्य तत्समक
Additive inverse	योज्य प्रतिलोम
Algorithm	कलन विधि, ऐल्गोरिद्‌म
Anti-clockwise	वामावर्त
Axiom	अभिगृहीत
Cancellation law	निरसन नियम
Centered	केंद्रक
Centre	केंद्र
Closed	संवृत
Column vector	स्तंभ सदिश
Common divisor	सार्वभाजक, समापवर्तक
Common Multiple	सार्वगुणज, समापवर्त्य
Commutative	क्रमविनिमेय
Commute	क्रमविनिमय करना
Composite number	भाज्य संख्या
Congruence	समशेषता
Conjugate	संयुग्मी
Co-prime	असहभाज्य
Curly bracket	धनुःकोष्ठक
Cycle	चक्र
Cyclic (Non-cyclic)	चक्रीय (अचक्रीय)
Determinant	सारणिक
Diagonal	विकर्ण
Dihedral group	द्वितल समूह
Direct product	अनुलोम गुणनफल
Disjoint	असंयुक्त
Distributive law	बंटन नियम
Divisibility	विभाज्यता
Divisor	भाजक
Empty (Non-empty)	रिक्त (अरिक्त)
Entry (of a matrix)	प्रविष्टि
Equivalence class	तुल्यता वर्ग
Equivalence relation	तुल्यता संबंध
Exponent	घातांक
External (Internal)	बाह्‌य (आंतरिक)
Factor	गुणनखंड
Finite (Infinite)	परिमित (अपरिमित)
Finitely generated	परिमिततः जनित
Fix (by a function)	नियत करना
Fundamental	मूलभूत

General linear group	व्यापक रैखिक समूह
Generate	जनित करना
Greatest common divisor	महत्तम समापवर्तक
Group	समूह
Identity element	तत्समक अवयव
Indexing set	समुच्चय से सूचित
Induction	आगमन
Infinitely many	अनंततः अनेक
Integral power	घात
Klein 4-group	क्लाइन 4-समूह
Least common multiple	लघुतम समापवर्त्य
Lemma	प्रमेयिका
Line of symmetry	सममिति रेखा
Matrix	आव्यूह
Move (by a function)	गतिमान करना
Multiple	गुणज
Operation table/Cayley table	संक्रिया सारणी/केली सारणी
Order	कोटि
Partition	विभाजन
Permutation	क्रमचय
Predicate	विधेय
Prime number	अभाज्य संख्या
Primitive	पूर्वग
Proper subgroup	उचित उपसमूह
Quaternion	चतुष्टयी
Quotient	भागफल
Reflection	परावर्तन
Regular polygon	सम बहुभुज
Relatively prime	सापेक्षतः अभाज्य
Remainder	शेषफल
Rotation	घूर्णन
Row vector	पंक्ति सदिश
Scalar	अदिश
Semigroup	सामिसमूह
Set of generators	जनक समुच्चय
Special linear group	विशिष्ट रैखिक समूह
Square brackets	गुरूकोष्ठक
Square matrix	वर्ग आव्यूह
Subgroup	उपसमूह
Subgroup diagram	उपसमूह आरेख
Substitution	प्रतिस्थापन
Symmetric group	सममित समूह
Symmetry	सममिति
Torsion subgroup	विमोटन उपसमूह

Translation	स्थानांतरण
Transpose of a matrix	आव्यूह का परिवर्त
Transposition	पक्षांतरण
Trivial (Non-trivial)	तुच्छ (अतुच्छ)
Unit circle	एकक वृत्त
Unity	एक / तत्समक
Well-ordering	सुक्रमण