इग्नू
जन-जन का
विश्वविद्यालय

इंदिरा गांधी राष्ट्रीय मुक्त विश्वविद्यालय
विज्ञान विद्यापीठ

BMTC-134
बीजगणित

खंड
4
पूर्णांकीय प्रांत

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)

आभार:

i) **प्रो. पार्वती शास्त्री**, मुम्बई विश्वविद्यालय, और **डॉ. इन्द्राक्षी दत्ता**, जीज़स एंड मेरी कॉलेज, दिल्ली विश्वविद्यालय, के प्रति, उनकी विस्तृत टिप्पणियों के लिए।

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

खंड प्रस्तावना

इस खंड में हम वलय सिद्धांत पर अपनी चर्चा जारी रखेंगे। इकाई 14 में दो विशेष प्रकार के वलयों, यानी पूर्णांकीय प्रांत और क्षेत्र, के बारे में आप सीखेंगे। यहाँ हम इनके गुणों पर विस्तार से चर्चा करेंगे।

आगे, इकाई 15 में हम उन वलयों की चर्चा करेंगे जिनके अवयवों – एक चर में बहुपद – से शायद आप परिचित हों। हम किसी भी क्रमविनिमेय वलय पर बहुपदों के विभिन्न गुणों पर चर्चा करेंगे। क्षेत्र पर बहुपदों के सिद्धांत के अनेक अनुप्रयोग हैं, गणित के अलावा। वास्तव में, इसी कारण से आर्यभट्ट-I, श्रीधर, भास्कर-II और अन्य प्राचीन भारतीय गणितज्ञों ने $\mathbb{Q}$ पर रैखिक और द्विघात बहुपदों का गहराई से अध्ययन किया था, और इनसे संबंधित सिद्धांत को विकसित किया था। आजकल इस सिद्धांत का कूटलेखन सिद्धांत तथा सामाजिक विज्ञान व रासायनिक विज्ञान की समस्याओं के गणितीय निदर्श बनाने में प्रयोग होता है।

आख़िर में, इस पाठ्यक्रम की अंतिम इकाई, इकाई 16 में हम $\mathbb{Q}$, $\mathbb{R}$ और $\mathbb{C}$ पर उन बहुपदों पर विचार करेंगे जिनके उचित गुणनखंड सिर्फ़ मात्रक हैं। ऐसे बहुपदों को अखंडनीय बहुपद कहते हैं। इस इकाई में आप कई ऐसे परीक्षणों का अध्ययन करेंगे, और लागू करेंगे, जिनसे मालूम पड़ता है कि इन क्षेत्रों पर कोई बहुपद अखंडनीय है या नहीं।

पिछले खंडों की तरह, इस खंड के अंत में आप कई उदाहरण, उनके हलों समेत, पाएंगे। ये प्रश्न इस खंड में आपके द्वारा अध्ययन किये गए अवधारणाओं से जुड़े हैं। साथ ही, आपको हल करने के लिए विविध प्रश्न भी दिए गए हैं, उदाहरणों के बाद। इन्हें आप खुद हल करें, जिससे कि आप संबंधित अवधारणाओं को बेहतर समझ पाएंगे।

इस खंड के साथ ही हम इस पाठ्यक्रम को समाप्त करते हैं। इसकी पढ़ाई के बाद आप इस पाठ्यक्रम के सत्रीय कार्य को पूरा कीजिए। यह सत्रीय कार्य इस पाठ्यक्रम के चारों खंडों पर आधारित है।

संकेत और प्रतीक (खंड 4 में प्रयोग होने वाले)

पिछले खंडों में **दिए संकेतों और प्रतीकों को भी दोबारा देख लीजिए।**

char R	वलय R का?
R[x]	वलय R पर? x में सभी बहुपदों का वलय
$\mathbb{Z}[\sqrt{n}]$	$\mathbb{Z}+\sqrt{n}\mathbb{Z},\ n \in \mathbb{Z}$

इकाई 14

पूर्णांकीय प्राँत और क्षेत्र

इकाई की रूपरेखा **पृष्ठ संख्या**

14.1 प्रस्तावना

इकाई 10 में हमने वलयों से आपका परिचय कराया था, तथा फिर क्रमविनिमेय वलयों और तत्समकी वलयों जैसे कुछ विशिष्ट वलयों से परिचय कराया था। जैसा कि आपने वहाँ देखा था कि, इन वलयों की विशिष्टता इन पर परिभाषित गुणन के गुणों की वजह से है। आपने यह भी देखा था कि ऐसी विशिष्ट वलयों का एक प्रतिनिधिक उदाहरण $\mathbb{Z}$ है। अतः, किसी अर्थ में ये वलय $\mathbb{Z}$ के अमूर्तीकरण माने जा सकते हैं। फिर भी, ज़रूरी नहीं है कि ये $\mathbb{Z}$ के एक आवश्यक गुण, यानी गुणन के लिए निरसन नियम, को संतुष्ट करें। इस इकाई में आप उन वलयों के बारे में अध्ययन करेंगे, जो इस नियम को संतुष्ट करते हैं। ऐसे वलय पूर्णांकीय प्राँत कहलाते हैं। ये बीजगणित की अनेक शाखाओं और उनके अनुप्रयोगों के अध्ययन के लिए अति महत्वपूर्ण हैं।

इस पूरी इकाई में हम मानकर चलेंगे कि वलय क्रमविनिमेय हैं, जब तक कुछ और कहा न गया हो।

भाग 14.2 में हम यह चर्चा करते हुए प्रारंभ करेंगे कि एक शून्य का भाजक क्या होता है। फिर हम एक पूर्णांकीय प्राँत की परिभाषा की ओर बढ़ेंगे, और आप इसके अनेक

उदाहरणों का अध्ययन करेंगे। आप देखेंगे कि अभी तक आपने जो अनेक देखें हैं, उनमें से अनेक क्यों पूर्णांकीय प्रांतों के उदाहरण हैं तथा उनमें से अनेक क्यों पूर्णांकीय प्रांतों के उदाहरण नहीं हैं! हम इस भाग में पूर्णांकीय प्रांतों के विभिन्न गुणों की चर्चा भी करेंगे।

अगले भाग, भाग 14.3 में, हम एक ऐसी विशेषता पर ध्यान केन्द्रित करेंगे, जो किसी भी वलय का, तथा विशिष्ट रूप से एक पूर्णांकीय प्रांत का लक्षण है। यह प्रत्येक वलय से जुड़ा एक ऋणेतर पूर्णांक होता है, जो उसका अभिलक्षणिक कहलाता है। हम यहाँ पूर्णांकीय प्रांत के अभिलक्षणिक पर ख़ास ध्यान देंगे। आप पूर्णांकीय प्रांत का अभिलक्षणिक 0 या एक अभाज्य संख्या होने के कारणों का अध्ययन करेंगे।

भाग 14.4 में आप $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ और $\mathbb{Z}_p$ (जहाँ p एक अभाज्य संख्या है) जैसे वलयों के एक सार्व गुण का अध्ययन करेंगे। इन वलयों में शून्येतर अवयवों का समुच्चय गुणन के सापेक्ष एक आबेली समूह है। ऐसा वलय एक क्षेत्र कहलाता है। क्षेत्र अति उपयोगी बीजीय वस्तुएँ हैं, जिसका एक कारण है कि किसी भी क्षेत्र का प्रत्येक शून्येतर अवयव एक मात्रक है। इस भाग में आप क्षेत्रों के कुछ मौलिक गुणों का भी अध्ययन करेंगे।

आगे, भाग 14.5 में आप अध्ययन करेंगे कि कोई भी पूर्णांकीय प्रांत एक क्षेत्र में आविष्ट होता है। आप यह भी देखेंगे कि एक दिए हुए पूर्णांकीय प्रांत को आविष्ट करने वाले सबसे छोटे क्षेत्र को कैसे बनाया जाता है। जैसा कि आप देखेंगे, वास्तव में यही वह विधि है जिसके द्वारा $\mathbb{Z}$ से $\mathbb{Q}$ बनाया जाता है।

पूर्णांकीय प्रांतों और क्षेत्रों से संबंधित वलयों की कुछ विशिष्ट गुणजावलियाँ हैं, जो अभाज्य गुणजावलियाँ और उच्चिष्ठ गुणजावलियाँ कहलाती हैं। भाग 14.6 में आप ऐसी गुणजावलियों, तथा इनके पूर्णांकीय प्रांतों और क्षेत्रों के साथ संबंधों, का अध्ययन करेंगे।

जैसा कि आप देख सकते हैं, इस इकाई में आप अनेक नई संकल्पनाओं का अध्ययन करेंगे। शायद आपको इन्हें समझने में कुछ समय लगे। चिंता नहीं करें। जितना समय आपको चाहिए, लीजिए। परंतु जब भी आप इसका अध्ययन समाप्त कर लें, उम्मीद है कि आपने निम्नलिखित सीखने के उद्देश्यों को प्राप्त कर लिए होंगे।

उद्देश्य

इस इकाई की पढ़ाई के बाद, आपको निम्नलिखित कर में समर्थ हो जाना चाहिए:

- वलय में शून्य के भाजक को परिभाषित करना, तथा उसके उदाहरण देना;
- जाँच करना कि एक बीजीय निकाय एक पूर्णांकीय प्रांत है या नहीं;
- क्रमविनिमेय या अक्रमविनिमेय वलय का अभिलक्षणिक प्राप्त करना;
- जाँच करना कि एक बीजीय निकाय एक क्षेत्र है या नहीं;

- पूर्णांकीय प्राँतों और क्षेत्रों के सरल गुणों को सिद्ध करना, तथा उनका अनुप्रयोग करना;
- किसी पूर्णांकीय प्राँत के विभाग क्षेत्र को बनाना, या पहचान पाना;
- वलय की अभाज्य गुणजावलियों और उच्चिष्ठ गुणजावलियों को परिभाषित करना, तथा उनकी पहचान करना।

14.2 पूर्णांकीय प्राँत क्या होता है?

आइए इस चर्चा को दो शून्येतर पूर्णांकों के गुणनफल को लेते हुए प्रारंभ करें। आप जानते हैं कि यह एक शून्येतर पूर्णांक होता है, अर्थात्, यदि $m, n \in \mathbb{Z}$ ऐसे हैं कि $m \neq 0$ और $n \neq 0$, तो $mn \neq 0$.

अब, वलय $\mathbb{Z}_6$ लीजिए। यहाँ $\overline{2} \neq \overline{0}$ और $\overline{3} \neq \overline{0}$, फिर भी $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$. अतः, हम पाते हैं कि $\mathbb{Z}_6$ में दो शून्येतर अवयवों $\overline{2}$ और $\overline{3}$ का गुणनफल शून्य है। यह उदाहरण हमें निम्नलिखित परिभाषा पर ले जाता है।

परिभाषा: वलय R का शून्येतर अवयव r वलय R में **शून्य का भाजक (zero divisor)** कहलाता है यदि R में एक ऐसा शून्येतर अवयव b है जिससे कि $rb = 0$.

याद रखिए R क्रमविनिमेय है।

(ध्यान दीजिए कि b भी शून्य का भाजक होगा!)

अब, क्या आप मानते हैं कि $\mathbb{Z}_6$ में $\overline{2}$ शून्य का भाजक है? $\mathbb{Z}_4$ में $\overline{3}$ के बारे में आप क्या कह सकते हैं? क्योंकि $\mathbb{Z}_4$ में प्रत्येक शून्येतर x के लिए, $\overline{3} \cdot x \neq \overline{0}$, इसलिए $\mathbb{Z}_4$ में $\overline{3}$ शून्य का भाजक नहीं है।

नाम 'शून्य का भाजक' इस बात से है कि एक अवयव $x \in R$, $r \in R$ को भाग देता है यदि $\exists\, y \in R$ s.t. $xy = r$. अंतर केवल यह है कि यहाँ $r = 0$ है, परंतु x और y दोनों शून्येतर हैं। अतः, $\overline{2} \cdot \overline{3} = \overline{0}$ की स्थिति में, $\overline{2} \mid \overline{0}$ और $\overline{3} \mid \overline{0}$. इस प्रकार, $\mathbb{Z}_6$ में $\overline{2}$ और $\overline{3}$ दोनों शून्य के भाजक हैं।

आइए ऐसे वलयों के कुछ और उदाहरणों पर विचार करें जिनमें शून्य के भाजक हैं।

उदाहरण 1: जाँच कीजिए कि $\mathbb{Z}[\sqrt{3}]/<4>$ में शून्य के भाजक हैं या नहीं।

हल: ध्यान दीजिए कि $\mathbb{Z}[\sqrt{3}]/<4> = \{a + b\sqrt{3} + <4> \mid a, b \in \mathbb{Z}\}$, और $<4> = \{4a + 4b\sqrt{3} \mid a, b \in \mathbb{Z}\}$.

हमें देखना है कि क्या $\exists\ \bar{x}, \bar{y} \in \mathbb{Z}[\sqrt{3}]/<4>$ s.t. $\bar{x} \neq \bar{0}, \bar{y} \neq \bar{0}$ परंतु $\overline{xy} = \bar{0}$, अर्थात् क्या $\exists x, y \in \mathbb{Z}[\sqrt{3}]$ s.t. $x, y \notin <4>$, परंतु $xy \in <4>$.

अब $x = 2, y = 2$ पर विचार कीजिए। यहाँ $x \notin <4>, y \notin <4>$. (क्यों?)

परंतु $xy = 4 \in <4>$.

अतः, $\mathbb{Z}[\sqrt{3}]/<4>$ में $\bar{2}$ एक शून्य का भाजक है।

आप इस वलय में कई और क्यों नहीं आप एक और पता कर लेते हैं? शून्य के भाजक मालूम कर सकते हैं।

***

उदाहरण 2: $C[0,1]$ में शून्य के भाजक का एक उदाहरण, पुष्टि सहित, दीजिए।

हल: $f(x) = \begin{cases} x - \frac{1}{2}, & 0 \le x \le 1/2 \\ 0, & 1/2 \le x \le 1 \end{cases}$ द्वारा दिए जाने वाले फलन $f \in C[0,1]$ पर विचार कीजिए।

आइए $g(x) = \begin{cases} 0, & 0 \le x \le 1/2 \\ x - \frac{1}{2}, & 1/2 \le x \le 1 \end{cases}$ द्वारा $g : [0,1] \to \mathbb{R}$ को परिभाषित करें।

तब, 'कलन' से आप जानते हैं कि $f, g \in C[0,1]$.

साथ ही, $f \neq 0, g \neq 0$ और $(fg)(x) = f(x)g(x) = 0\ \forall\ x \in [0, 1]$.

इस प्रकार, fg शून्य फलन है।

अतः, $C[0,1]$ में f एक शून्य का भाजक है, और g भी शून्य का भाजक है।

***

उदाहरण 3: जाँच कीजिए कि दो अतुच्छ वलयों के अनुलोम गुणनफल में शून्य के भाजक हैं या नहीं।

हल: मान लीजिए A और B अतुच्छ वलय हैं। मान लीजिए कि $a \in A, a \neq 0$, तथा $b \in B,\ b \neq 0$.

तब, दोनों $(a, 0) \in A \times B$ और $(0, b) \in A \times B$ शून्येतर हैं।

परंतु, $(a, 0)(0, b) = (0, 0)$.

अतः, $A \times B$ में $(a, 0)$ और $(0, b)$ शून्य के भाजक हैं।

***

उदाहरण 4: जाँच कीजिए कि $\wp(X)$ में शून्य के भाजक हैं या नहीं, जहाँ X कम से कम दो अवयवों वाला समुच्चय है।

हल: X का प्रत्येक अरिक्त उचित उपसमुच्चय A शून्य का भाजक है, क्योंकि $A \cdot A^c = A \cap A^c = \emptyset$, जो $\wp(X)$ का शून्य अवयव है।

***

उदाहरण 5: मान लीजिए $\mathbb{Z}_n$ में $\overline{x}$ एक शून्य का भाजक है, जहाँ $n \in \mathbb{N}$. दिखाइए कि $(x, n) > 1$.

हल: मान लीजिए $\overline{y} \in \mathbb{Z}_n$ s.t. $\overline{y} \neq \overline{0}$ और $\overline{x}\,\overline{y} = \overline{0}$.

तब $n \nmid x, n \nmid y$, लेकिन $n | xy$.

मान लीजिए $(x, n) = 1$. तब $\exists\, m, r \in \mathbb{Z}$ s.t. $mx + nr = 1$.

अतः, $y = y \cdot 1 = mxy + nry$.

अब $n | xy$ और $n | nry$. अतः, $n | (mxy + nry)$, अर्थात्, $n | y$, जो एक अंतर्विरोध है।

इसलिए, $(x, n) \neq 1$.

अतः, $(x, n) > 1$.

***

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E1) $\mathbb{Z}$ में, तथा $\mathbb{Z}_{10}$ में, सभी शून्य के भाजक तथा सभी मात्रकों को लिखिए। क्या प्रत्येक वलय के शून्य के भाजकों और मात्रकों में कोई संबंध है? यदि है, तो क्या संबंध है? (यह E5 से जुड़ा है।)

E2) उदाहरण 5 में जो दिया है, उसका विलोम सिद्ध कीजिए।

E3) मान लीजिए R एक वलय है तथा $a \in R$ एक शून्य का भाजक है। दर्शाइए कि मुख्य गुणजावली Ra का प्रत्येक शून्येतर अवयव एक शून्य का भाजक है।

E4) जाँच कीजिए कि $\wp(X)$ में शून्य के भाजक हैं या नहीं, जहाँ $X = \{a\}$.

E5) मान लीजिए R एक तत्समकी वलय है तथा $a \in R, a \neq 0$.

i) यदि a शून्य का भाजक नहीं है, तो क्या $a \in U(R)$?

ii) यदि $a \in U(R)$, तो क्या R में a शून्य का भाजक हो सकता है?

अपने उत्तरों की पुष्टि कीजिए।

अभी तक आपने शून्य के भाजक वाले वलयों के अनेक उदाहरणों को देखा है। आप यह भी जानते हैं कि $\mathbb{Z}$ में कोई शून्य का भाजक नहीं है। वास्तव में, ऐसे अनेक वलय हैं जिनमें कोई शून्य के भाजक नहीं हैं। आइए ऐसे वलयों को परिभाषित करें।

परिभाषा: एक अतुच्छ वलय R एक **पूर्णांकीय प्रॉंत (integral domain)** कहलाता है, यदि

i) R क्रमविनिमेय है,

ii) R तत्समकी है, तथा

ii) R में कोई शून्य के भाजक नहीं हैं।

इस प्रकार, एक पूर्णांकीय प्रॉंत एक तत्समकी अतुच्छ क्रमविनिमेय वलय होता है जिसमें दो शून्येतर अवयवों का गुणनफल एक शून्येतर अवयव होता है।

इस प्रकार के वलय का नाम पूर्णांकों के समुच्चय से आया है, जो ऐसे वलयों का सबसे ज़्यादा जाना पहचाना उदाहरणों में से एक है। वस्तुतः, शुरू में पूर्णांकीय प्रॉंतों को $\mathbb{Z}$ का एक व्यापकीकृत रूप माना जाता था।

क्या आपके दिमाग़ में कोई और पूर्णांकीय प्रॉंत आता है? $\mathbb{Q}, \mathbb{R}$ और $\mathbb{C}$ के बारे में आप क्या कह सकते हैं? आपको इसकी जाँच करनी चाहिए कि ये परिभाषा में दिए प्रतिबंधों को संतुष्ट करते हैं।

अब, जिन उदाहरणों का अभी तक आपने अध्ययन किया है, उनमें से क्या आप को कोई ऐसा वलय दिखता है जो पूर्णांकीय प्रॉंत नहीं है? $C[0,1]$ के बारे में आप क्या कह सकते हैं? उदाहरण 2 में आप देख चुके हैं कि इसमें शून्य के भाजक होते हैं। इस प्रकार, $C[0,1]$ एक पूर्णांकीय प्रॉंत नहीं है।

इससे पहले कि हम आगे बढ़ें, शब्दावली के बारे में एक संक्षिप्त टिप्पणी को देखिए।

टिप्पणी 1: अनेक लेखक शब्द 'पूर्णांकीय प्रॉंत' को संक्षेप में 'प्रॉंत' ही लिख हैं। हम भी ऐसा ही करेंगे।

आइए अब $\mathbb{Z}_n$ पर दृष्टि डालें। E1 में आप सिद्ध कर चुके हैं कि $\mathbb{Z}_{10}$ एक प्रॉंत नहीं है। इससे पहले आप देख चुके हैं कि $\mathbb{Z}_6$ और $\mathbb{Z}_4$ प्रॉंत नहीं हैं। अतः, क्या किसी भी $n \in \mathbb{N}$ के लिए, $\mathbb{Z}_n$ एक प्रॉंत नहीं है? $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ लीजिए। क्योंकि $\overline{1} \cdot \overline{1} = \overline{1} \neq \overline{0}$, इसलिए $\mathbb{Z}_2$ एक प्रॉंत है।

$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ के बारे में आप क्या कह सकते हैं? आपको इसकी जाँच करनी चाहिए कि यह एक प्रॉंत है।

अतः, $\mathbb{Z}_2$ और $\mathbb{Z}_3$ के बारे में ऐसा क्या है जो इन्हें प्राँत बना देता है, जबकि $\mathbb{Z}_6$ और $\mathbb{Z}_4$ प्राँत नहीं हैं? शायद उस निष्कर्ष पर पहुंच गए होंगे जिसे अब हम सिद्ध करने जा रहे हैं।

प्रमेय 1: $\mathbb{Z}_p$ एक पूर्णांकीय प्राँत होता है यदि और केवल यदि p एक अभाज्य संख्या है।

उपपत्ति: आप जानते हैं कि $\forall\ n \geq 2, \mathbb{Z}_n$ एक अतुच्छ तत्समकी क्रमविनिमेय वलय है। अतः, हमें यह सिद्ध करने की आवश्यकता है कि $\mathbb{Z}_p$ में कोई शून्य के भाजक नहीं हैं यदि और केवल यदि p एक अभाज्य संख्या है।

एक वलय R **बिना शून्य के भाजक वाला** है, यदि $a, b \in R$ के लिए, $ab = 0 \Rightarrow a = 0$ या $b = 0$.

पहले, आइए मान लें कि p एक अभाज्य संख्या है।

मान लीजिए $\bar{a}, \bar{b} \in \mathbb{Z}_p$ ऐसे हैं कि $\bar{a}\,\bar{b} = \bar{0}$.

तब, $\overline{ab} = \bar{0}$, अर्थात् $p|ab$.

क्योंकि p एक अभाज्य संख्या है, इसलिए इकाई 1 से आप जानते हैं कि $p|a$ या $p|b$.

इस प्रकार, $\bar{a} = \bar{0}$ या $\bar{b} = \bar{0}$.

इस प्रकार, हमने सिद्ध कर लिया है कि $\mathbb{Z}_p$ में यदि $\bar{a} \neq \bar{0}$ और $\bar{b} \neq \bar{0}$, तो $\bar{a}\,\bar{b} \neq \bar{0}$.

पाठ्यक्रम 'वास्तविक विश्लेषण' के खंड 1 से आप जानते हैं कि यह इसे सिद्ध करने के तुल्य है कि $\bar{a}\bar{b} = \bar{0} \Rightarrow \bar{a} = \bar{0}$ या $\bar{b} = \bar{0}$.

इस प्रकार, $\mathbb{Z}_p$ में शून्य के भाजक नहीं हैं, तथा इसी लिए यह एक प्राँत है।

विलोमतः, हमें दिया है कि $\mathbb{Z}_p$ में कोई शून्य के भाजक नहीं हैं।

यदि $p = 1$, तो $\mathbb{Z}_p$ तुच्छ वलय है, जो एक प्राँत नहीं है।

यदि $p \neq 1$, मान लीजिए $m|p$ किसी $m \in \mathbb{N}$ के लिए। अतः, किसी $r \in \mathbb{N}$ के लिए, $p = mr$.

तब $1 \leq m \leq p, 1 \leq r \leq p$, और $\mathbb{Z}_p$ में $\bar{m}\,\bar{r} = \overline{mr} = \bar{p} = \bar{0}$.

क्योंकि $\mathbb{Z}_p$ के कोई शून्य के भाजक नहीं हैं, इसलिए $\bar{m} = \bar{0}$ या $\bar{r} = \bar{0}$.

इस प्रकार, $p|m$ या $p|r$.

यह तभी संभव है, जब $m = p$ या $r = p$.

यदि $m = p$, तो $r = 1$. यदि $r = p$, तो $m = 1$. अतः, p के गुणनखंड केवल 1 और p हैं।

अतः, p एक अभाज्य संख्या है। ■

प्रमेय 1 के अनुप्रयोग से आप तुरंत कुछ ऐसे निष्कर्ष निकाल सकते हैं जिन्हें आप पहले सिद्ध कर चुके हैं, जैसे कि $\mathbb{Z}_{10}, \mathbb{Z}_6$ और $\mathbb{Z}_4$ में शून्य के भाजक हैं!

आइए अब प्राँत के एक अन्य उदाहरण पर दृष्टि डालें।

उदाहरण 6: दर्शाइए कि $R = (D_1 \times D_2) / D_1 \times \{0\}$ एक पूर्णांकीय प्राँत है, जहाँ D_1 और D_2 प्राँत हैं।

हल: इकाई 13 से आप जानते हैं कि $(D_1 \times D_2) / D_1 \times \{0\} \simeq D_2$, जो एक प्राँत है। क्योंकि तुल्याकारी वलयों में पूरी तरह से समान बीजीय गुण होते हैं तथा R एक प्राँत के तुल्याकारी है, इसलिए R को प्राँत होना ही चाहिए। इस प्रकार, परिणाम प्राप्त हो जाता है।

***

उपरोक्त उदाहरण में एक रोचक तथ्य दिखता है। उदाहरण 4 से आप जानते हैं कि $D_1 \times D_2$ एक प्राँत नहीं है। परंतु $D_1 \times D_2$ का एक विभाग वलय प्राँत बन जाता है!

अब, कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E6) निम्नलिखित में से कौन-से वलय पूर्णांकीय प्राँत **नहीं** हैं? क्यों?
$\mathbb{Z}_{97}$, $2\mathbb{Z}$, $\mathbb{Z} + i\mathbb{Z}$, $\mathbb{R} \times \mathbb{R}$, $\{0\}$, $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\})$.

E7) क्या पूर्णांकीय प्राँत के उपवलय को एक प्राँत होना ही पड़ता है? क्या प्राँत के विभाग वलय को एक प्राँत होना ही पड़ता है? अपने उत्तरों के लिए कारण दीजिए।

E8) जाँच कीजिए कि $\mathbb{Q}[\sqrt{n}]$ एक पूर्णांकीय प्राँत है या नहीं, जहाँ n एक वर्ग-मुक्त पूर्णांक है।

अब, वलय R पर विचार कीजिए। हम जानते हैं कि R में योग के लिए निरसन नियम लागू होता है, अर्थात्, जब भी R में $a + b = a + c$, तो $b = c$. परंतु, क्या $ab = ac$ से $b = c$ प्राप्त होता है? यह आवश्यक नहीं है। उदाहरणार्थ, $\mathbb{Z}$ में $0 \cdot 1 = 0 \cdot 2$, परंतु $1 \neq 2$. अतः, यदि $a = 0$, तो $ab = ac$ का निहितार्थ $b = c$ नहीं है। परंतु, यदि $a \neq 0$ तथा $ab = ac$, तो क्या यह सत्य है कि $b = c$? हम सिद्ध करेंगे कि यह पूर्णांकीय प्राँतों के लिए सत्य है।

प्रमेय 2: वलय R में कोई शून्य के भाजक नहीं होते हैं यदि और केवल यदि R में गुणन के लिए निरसन नियम लागू होता है (अर्थात्, यदि $a, b, c \in R$ ऐसे हैं कि $a \neq 0$ और $ab = ac$ या $ba = ca$, तो $b = c$.)

उपपत्ति: पहले, आइए मान लें कि R में कोई शून्य के भाजक नहीं हैं। यह भी मान लीजिए कि $a, b, c \in R$ s.t. $a \neq 0$ और $ab = ac$. तब,

$a(b-c) = ab - ac$, इकाई 10 के प्रमेय 1 द्वारा।

$\qquad = 0.$

क्योंकि $a \neq 0$ तथा R में कोई शून्य के भाजक नहीं हैं, इसलिए हम $b - c = 0$, अर्थात् $b = c$ प्राप्त करते हैं।

इस प्रकार, यदि $ab = ac$ और $a \neq 0$, तो $b = c$.

इसी तरह यदि $ba = ca$ और $a \neq 0$, तो $b = c$.(ध्यान दीजिए कि यहाँ R को क्रमविनिमेय नहीं माना गया है।)

विलोमतः, मान लीजिए R में गुणन के लिए निरसन नियम लागू है। मान लीजिए $a \in R$ s.t. $a \neq 0$.

यह भी मान लीजिए कि किसी $b \in R$ के लिए, $ab = 0$.

तब, $ab = 0 = a0$.

गुणन के लिए निरसन नियम का उपयोग करने पर, $b = 0$ प्राप्त होता है।

अतः, ऐसा कोई शून्येतर b नहीं है s.t. $ab = 0$.

इसलिए, a शून्य का भाजक नहीं है, अर्थात् R में कोई शून्य के भाजक नहीं हैं। ■

इस प्रमेय का उपयोग करते हुए, हम तुरंत निष्कर्ष निकाल सकते हैं कि एक **पूर्णांकीय प्राँत में गुणन के लिए निरसन नियम लागू होता है।**

ध्यान दीजिए कि प्रमेय 2 केवल प्राँतों के लिए सत्य नहीं है। यह किसी भी ऐसे वलय के लिए भी सत्य है जो प्राँत नहीं है और बिना शून्य के भाजक वाला है, जैसे कि $2\mathbb{Z}$.

आइए प्रमेय 2 के उपयोग के कुछ उदाहरणों पर दृष्टि डालें।

उदाहरण 7: क्या $\mathbb{Z}[i]$ में गुणन के लिए निरसन नियम लागू होता है?

हल: क्योंकि $\mathbb{Z}[i]$, $\mathbb{C}$ का एक उपवलय है, इसलिए यह बिना शून्य के भाजक वाला वलय है। इस प्रकार, प्रमेय 2 द्वारा, $\mathbb{Z}[i]$ के लिए निरसन नियम लागू होता है।

***

उदाहरण 8: मान लीजिए कि R बिना शून्य के भाजक वाला एक अतुच्छ परिमित वलय है। दर्शाइए कि R तत्समकी होगा ही।

हल: मान लीजिए $a \neq 0 \in R$. तब, R का a^i एक शून्येतर अवयव $\forall\ i \in \mathbb{N}$.

परंतु, R में केवल परिमित संख्या में अवयव हैं।

अतः, किन्हीं $r, s \in \mathbb{N}, r \neq s$ के लिए, $a^r = a^s$.

मान लीजिए n सबसे छोटा ऐसा धनात्मक पूर्णांक है जिसके लिए s.t. $\exists\ m \in \mathbb{N}$ $a^m = a^n$, $m \neq n$. तब, $m > n$.

अतः, सभी $x \in R$ के लिए,

$x \cdot a^m = x \cdot a^n$

$\Rightarrow xa^{m-1} = xa^{n-1}$, प्रमेय 2 से, और a के निरसन द्वारा।

$\Rightarrow xa^{m-n} = x$, इसी प्रक्रिया का $(n-1)$ बार अनुप्रयोग करने पर।

इसी प्रकार, आप दर्शा सकते हैं कि $a^{m-n}x = x\ \forall\ x \in R$.

इस प्रकार, का a^{m-n}, R तत्समक है।

***

अब आपको निम्नलिखित प्रश्नों को हल, करना चाहिए, प्रमेय 2 के उपयोग से।

E9) जाँच कीजिए कि क्या $\mathbb{Z}[\sqrt{7}]$ और $5\mathbb{Z}$ में गुणन के लिए निरसन नियम लागू है या नहीं।

वलय R के अवयव r को **वर्गसम अवयव (idempotent)** कहते हैं यदि $r^2 = r$.

E10) दर्शाइए कि किसी भी प्राँत में, समीकरण $x^2 = x$ के हल केवल $x = 0$ और $x = 1$ हैं।

E11) सिद्ध कीजिए कि केवल 0 ही प्राँत का शून्यंभावी अवयव (इकाई 12 के उदाहरण 9 को देखिए) होता है।

E12) मान लीजिए R एक तत्समकी अतुच्छ परिमित वलय है तथा $a \in R$, $a \neq 0$. दर्शाइए कि या तो a शून्य का भाजक है या a, R का मात्रक है।

आइए अब किसी भी वलय से जुड़ा एक ऋणेतर पूर्णांक का परिचय दें। यह हमें पूर्णांकीय प्राँत के एक ख़ास लक्षण की ओर ले जाएगा।

14.3 एक वलय का अभिलक्षणिक

इस भाग में हम एक ऐसे ऋणेतर पूर्णांक पर ध्यान देंगे जो वलयों का एक लक्षण है। यदि वलय R परिमित है, तो आप देखेंगे कि यह पूर्णांक असल में आबेली समूह $(R,+)$ की कोटि का भाजक है। वलय के इस लक्षण को देने की हमारी वजह है कि इससे पूर्णांकीय प्राँतों का एक महत्त्वपूर्ण गुण मिलता है, जैसा कि आप देखेंगे।

ध्यान दीजिए कि इस भाग में हम **केवल क्रमविनिमेय वलयों तक ही चर्चा सीमित नहीं** रखेंगे।

आइए $\mathbb{Z}_4$ पर दृष्टि डालते हुए प्रारंभ करें। क्या $n \in \mathbb{N}$ है s.t. $\mathbb{Z}_4$ में $n \cdot \overline{2} = \overline{0}$? हाँ है। उदाहरणार्थ, $2 \in \mathbb{N}$ s.t. $2 \cdot \overline{2} = \overline{0}$. क्या कोई $n \in \mathbb{N}$ है s.t. $\mathbb{Z}_4$ में $n \cdot \overline{3} = \overline{0}$? यहाँ 4 के बारे में क्या कहा जा सकता है? $\mathbb{Z}_4$ में $4 \cdot \overline{3} = \overline{12} = \overline{0}$ । अतः, 4 कार्य करता है।

क्या कोई $n \in \mathbb{N}$ है s.t. $n \cdot x = \overline{0} \ \forall \ x \in \mathbb{Z}_4$? यहाँ पर भी 4 के बारे में क्या कहा जा सकता है? आप जानते हैं कि $4x = \overline{0} \ \forall \ x \in \mathbb{Z}_4$, क्योंकि $\overline{4} = \overline{0}$.

वस्तुतः, किसी भी $x \in \mathbb{Z}_4$ के लिए, $8x = \overline{0}$ और $12x = \overline{0}$ भी होता है। परंतु 4 इस गुण के साथ सबसे छोटा धनात्मक पूर्णांक है। अर्थात्, 4 समुच्चय $\{n \in \mathbb{N} \mid nx = \overline{0} \ \forall \ x \in \mathbb{Z}_4\}$ का लघुतम अवयव है। यह हमें बताता है कि 4, $\mathbb{Z}_4$ का अभिलक्षणिक है, जैसा कि अब आप देखेंगे।

परिभाषा: मान लीजिए R एक वलय है। सबसे छोटा धनात्मक पूर्णांक n जिससे कि $nx = 0 \ \forall \ x \in R$, R का **अभिलक्षणिक (characteristic)** कहलाता है।

यदि ऐसा कोई धनात्मक पूर्णांक n नहीं है जिससे कि $nx = 0 \ \forall \ x \in R$, तो **R के अभिलक्षणिक को शून्य परिभाषित किया जाता है।**

R के अभिलक्षणिक को **char R** द्वारा व्यक्त किया जाता है।

अतः, जैसा कि आप ऊपर देख चुके हैं, $\text{char } \mathbb{Z}_4 = 4$. वस्तुतः, आपको इसकी जाँच करनी चाहिए कि $\text{char } \mathbb{Z}_n = n$ तथा $\text{char } \mathbb{Z} = 0$.

आइए एक अन्य उदाहरण पर विचार करें।

उदाहरण 9: char $(m\mathbb{Z})$ ज्ञात कीजिए, जहाँ $m \in \mathbb{Z}, m \geq 2$.

हल: $m\mathbb{Z}$ का कोई भी अवयव $mn, n \in \mathbb{Z}$ के रूप का होता है। अब, यदि $r \in \mathbb{Z}$ s.t. $rmn = 0 \ \forall \ n \in \mathbb{Z}$, तो $rm = 0$, $n = 1$ रखने पर।

क्योंकि $m \neq 0$, इसलिए $r = 0$.

अतः, $\text{char } (m\mathbb{Z}) = 0$.

***

निम्नलिखित प्रश्नों को हल करने से आपको वलय के अभिलक्षणिक के बारे में एक बेहतर समझ प्राप्त होगी।

याद रखिए कि इस भाग में जरूरी नहीं कि वलय क्रमविनिमेय हों।

E13) पुष्टि सहित एक ऐसे वलय R का उदाहरण दीजिए जिसके लिए
$\text{char } R = 0,\ R \neq m\mathbb{Z},\ m \in \mathbb{N}.$

E14) char $\wp(X)$ ज्ञात कीजिए, जहाँ X एक अरिक्त समुच्चय है।

E15) मान लीजिए कि R एक वलय है तथा $\text{char } R = m$. $\text{char } (R \times R)$ क्या है?

E16) यदि R एक परिमित वलय है, तो char R को शून्येतर क्यों होना होगा?

E17) i) मान लीजिए R एक n अवयवों वाला परिमित वलय है। दर्शाइए कि n को char R विभाजित करता है।

ii) विशिष्ट रूप से, $R = \mathbb{M}_2(\mathbb{Z}_4)$ के लिए n और r क्या हैं?

iii) पुष्टि करते हुए, उपरोक्त (i) में $r = n$ वाले R का एक उदाहरण दीजिए।

अब, आइए एक तत्समकी वलय के अभिलक्षणिक के बारे में एक अच्छे परिणाम पर दृष्टि डालें। जब हम ऐसे वलय का अभिलक्षणिक प्राप्त करना चाहते हैं, तब इस परिणाम से हमें बहुत फ़ायदा होता है।

प्रमेय 3: मान लीजिए कि m एक धनात्मक पूर्णांक है तथा R एक तत्समकी वलय है। तब, निम्नलिखित प्रतिबंध तुल्य हैं:

i) $m \cdot 1 = 0.$

ii) सभी $a \in R$ के लिए, $ma = 0.$

उपपत्ति: हम सिद्ध करेंगे कि (i) $\Rightarrow$ (ii) तथा (ii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): हम जानते हैं कि $m \cdot 1 = 0.$

इस प्रकार, किसी भी $a \in R$ के लिए, $ma = m(1 \cdot a) = (m \cdot 1)a = 0 \cdot a = 0,$ अर्थात् (ii) सत्य है।

(ii) $\Rightarrow$ (i): यदि $ma = 0\ \forall\ a \in R$, तो निश्चित रूप से यह $a = 1$ के लिए भी सत्य है, अर्थात् $m \cdot 1 = 0.$ ■

प्रमेय 3 हमें बताता है कि **एक तत्समकी वलय R का अभिलक्षणिक ज्ञात करने के लिए,** हमें $nx\ \forall\ x \in R, n \in \mathbb{N}$ के बदले **केवल समुच्चय $\{n \cdot 1 \mid n \in \mathbb{N}\}$ को देखने की ज़रूरत है।**

आइए कुछ उदाहरणों को देखें।

i) $\text{char } \mathbb{Q} = 0,$ क्योंकि किसी भी $n \in \mathbb{N}$ के लिए $n \cdot 1 \neq 0.$

ii) इसी प्रकार, $\text{char } \mathbb{R} = 0$ तथा $\text{char } \mathbb{C} = 0.$

iii) आप पहले ही देख चुके हैं कि, $n \geq 2$ के लिए, $\text{char } \mathbb{Z}_n = n.$ यहाँ $n \cdot \overline{1} = \overline{0},$ तथा n ऐसी लघुतम प्राकृतिक संख्या है।

आप वलयों तथा उनके अभिलक्षणिकों के अनेक उदाहरण देख चुके हैं। इन उदाहरणों से आपने शायद यह निष्कर्ष निकाल लिया होगा कि एक अपरिमित वलय का अभिलक्षणिक शून्य होता है। परंतु, निम्नलिखित उदाहरण पर विचार कीजिए।

उदाहरण 10: $\mathbb{Z}_3$ से गुणांकों वाले x में बहुपदों के वलय $\mathbb{Z}_3[x]$ का अभिलक्षणिक ज्ञात कीजिए।

हल: $\mathbb{Z}_3[x]$ का कोई भी अवयव, गुणांकों $\overline{0}, \overline{1}$ या $\overline{2}$ वाला एक बहुपद है। इस वलय का एक तत्समक अर्थात् $\overline{1}$ है।

सबसे छोटा धनात्मक पूर्णांक 3 है जिसके लिए

क्योंकि $n \cdot \overline{1} n = \overline{0}$, इसलिए $\text{char } \mathbb{Z}_3[x] = 3,$ प्रमेय 3 द्वारा।

***

ध्यान दीजिए कि $\mathbb{Z}_3[x]$ एक अपरिमित वलय है, क्योंकि प्रत्येक $n \in \mathbb{N}$ के लिए, घात n वाला एक बहुपद होता है तथा ये सभी बहुपद भिन्न-भिन्न होते हैं। अतः, $\mathbb{Z}_3[x]$ एक ऐसे अपरिमित वलय का उदाहरण है जिसका शून्येतर अभिलक्षणिक है।

अब आप कुछ प्रश्न हल क्यों नहीं कर लेते?

E18) $\text{char } \mathbb{M}_n(\mathbb{C}), n \in \mathbb{N},$ तथा $\text{char } \mathbb{M}_n(\mathbb{Z}_m), n, m \in \mathbb{N},$ ज्ञात कीजिए।

E19) यदि R एक वलय है तथा R की I एक गुणजावली है, तो क्या $\text{char } R = \text{char } (R/I)$ होगा ही? क्यों, या क्यों नहीं?

E20) यदि R एक वलय है तथा R का S एक उचित उपवलय है, तो क्या $\text{char } S < \text{char } R$ हमेशा होगा? क्यों, या क्यों नहीं?

E21) क्या अभिलक्षणिक 1 वाला कोई वलय है? क्यों, या क्यों नहीं?

E22) मान लीजिए R और S तुल्याकारी वलय हैं। $\text{char } R - \text{char } S$ ज्ञात कीजिए।

आइए अब देखें कि प्रमेय 1 क्या कहता है। यह बताता है कि $\mathbb{Z}_n$ एक प्राँत है यदि और केवल यदि n एक अभाज्य संख्या है। अतः, यदि हम इसे $\text{char } \mathbb{Z}_n$ के साथ जोड़ें, तो हम

ज्ञात करते हैं कि $\mathbb{Z}_n$ एक प्राँत है iff char $\mathbb{Z}_n$ एक अभाज्य संख्या है। तो, प्रश्न यह उठता है कि क्या कोई प्राँत है जिसका अभिलक्षणिक एक अभाज्य संख्या नहीं है। क्या $\mathbb{Q}$ एक ऐसा प्राँत नहीं है, क्योंकि char $\mathbb{Q} = 0$. जो एक अभाज्य संख्या नहीं है? क्या char R, जहाँ R एक प्राँत है, कोई अन्य मान ग्रहण कर सकता है? निम्नलिखित प्रमेय इस प्रश्न का उत्तर देता है।

प्रमेय 4: एक पूर्णांकीय प्राँत का अभिलक्षणिक या तो शून्य होता है या एक अभाज्य संख्या होता है।

उपपत्ति: मान लीजिए R एक प्राँत है। हम सिद्ध करेंगे कि यदि R का अभिलक्षणिक शून्य नहीं है, तो यह एक अभाज्य संख्या है।

अतः, मान लीजिए char $R = m$, जहाँ $m \in \mathbb{N}$. तब, m ऐसा लघुतम धनात्मक पूर्णांक है कि $m \cdot 1 = 0$, प्रमेय 3 द्वारा।

हम अंतर्विरोध की विधि से दर्शाएँगे कि m एक अभाज्य संख्या है, अर्थात्, हम शुरू में मान लेंगे कि m एक अभाज्य संख्या नहीं है, तथा एक अंतर्विरोध पर पहुंचेंगे। यह दर्शाएगा कि हमारी परिकल्पना ग़लत थी।

अतः, मान लीजिए m अभाज्य संख्या नहीं है। तो $m = st$, जहाँ $s, t \in \mathbb{N}, 1 < s < m$ और $1 < t < m$.

तब, $m \cdot 1 = 0 \Rightarrow (st) \cdot 1 = 0 \Rightarrow (s \cdot 1)(t \cdot 1) = 0 \Rightarrow s \cdot 1 = 0$ या $t \cdot 1 = 0$, क्योंकि R में कोई शून्य के भाजक नहीं हैं।

परंतु s और t, m से छोटे हैं। लेकिन $m = \text{char } R$. अतः, प्रमेय 3 द्वारा, हम एक अंतर्विरोध पर पहुँचते हैं। अतः, हमारी परिकल्पना कि m अभाज्य संख्या नहीं है ग़लत होगी। अतः, m एक अभाज्य संख्या है। ■

अब, प्रमेय 4 के विलोम के बारे में क्या कहा जा सकता है? अर्थात्, यदि R अभिलक्षणिक 0 या अभाज्य अभिलक्षणिक वाला एक वलय है, तो क्या R को एक प्राँत होना चाहिए? आप 'अभिलक्षणिक' की अपनी समझ का उपयोग कर सकते हैं इसका उत्तर देने के लिए, तथा अन्य नीचे दिए प्रश्नों को हल करने के लिए।

E23) जाँच कीजिए कि प्रमेय 4 का विलोम सत्य है या नहीं।

(**संकेत:** क्या E15 इसमें सहायता करता है?)

E24) मान लीजिए R एक पूर्णांकीय प्राँत है, जिसका अभिलक्षणिक एक अभाज्य संख्या p है। सिद्ध कीजिए कि

i) $a, b \in R, (a+b)^p = a^p + b^p$ और $(a-b)^p = a^p - b^p$.

ii) $n \in \mathbb{N}$ और $a, b \in R$ के लिए, $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

iii) उपसमुच्चय $\{a^p \mid a \in R\}$, R का एक उपवलय है।

iv) फलन $\phi : R \to R : \phi(a) = a^p$ एक एकैक समाकारिता है।

v) यदि R एक परिमित पूर्णांकीय प्राँत है, तो उपरोक्त (iv) में ϕ एक तुल्याकारिता है।

E25) यदि $\text{char } R = 0$, तो E24 के कथनों में से कौन-से कथन सत्य हैं? क्यों?

E26) दर्शाइए कि वलय R के लिए, $(a+b)^6 = a^6 + b^6$ का सत्य होना आवश्यक नहीं, जहाँ $a, b \in R$, तथा $\text{char } R = 6$.

E27) मान लीजिए R एक तत्समक 1 वाला वलय है, तथा मान लीजिए कि char $R = m$. $f : \mathbb{Z} \to R : f(n) = n \cdot 1$ परिभाषित कीजिए। दर्शाइए कि f एक समाकारिता है। Ker f के लिए एक जनक भी दीजिए।

E28) $\mathbb{Z}_3 \times \mathbb{Z}_4$ का अभिलक्षणिक ज्ञात कीजिए। इस वलय को एक उदाहरण के रूप में उपयोग करके दर्शाइए कि प्रमेय 4 केवल पूर्णांकीय प्राँतों के लिए ही सत्य है।

अब तक आप पूर्णांकीय प्राँतों तथा उनके अभिलक्षणिक से परिचित हो गए होंगे। आइए अब अपनी चर्चा को एक अन्य बीजीय संरचना की ओर बढ़ाएँ। यह संरचना हमें एक प्राँत के गुणन पर कुछ प्रतिबंध लगाने से प्राप्त होता है।

14.4 क्षेत्र

इस भाग में आप कुछ विशिष्ट प्राँतों का अध्ययन करेंगे, जिनके उदाहरण $\mathbb{Q}, \mathbb{R}$ और $\mathbb{C}$ हैं। आइए देखें कि ये पूर्णांकीय प्राँत विशिष्ट क्यों हैं।

हम जिस संकल्पना की ओर बढ़ रहे हैं, उसे समझने के लिए एक वलय $(R, +, \cdot)$ लीजिए। आप जानते हैं कि $(R,+)$ एक आबेली समूह है। आप यह भी जानते हैं कि R में संक्रिया $\cdot$ साहचर्य है। परंतु $(R, \cdot)$ का आबेली समूह होना आवश्यक नहीं है। उदाहरणार्थ, $(\mathbb{Z}, \cdot)$ एक आबेली समूह नहीं है, क्योंकि $\mathbb{Z}$ में कई अवयवों का, जैसे कि 2 का कोई गुणनात्मक प्रतिलोम नहीं है।

इसी प्रकार, $(\mathbb{C}, \cdot)$ एक आबेली समूह नहीं है, क्योंकि ऐसा कोई अवयव $a \in \mathbb{C}$ नहीं है जिससे कि $a \cdot 0 = 1$. परंतु $(\mathbb{C}^*, \cdot)$ एक आबेली समूह है, जैसा कि आप जानते हैं। इसी प्रकार, गुणन के सापेक्ष $\mathbb{Q}^*$ और $\mathbb{R}^*$ भी आबेली समूह है। ये प्रेक्षण हमें एक नई बीजीय वस्तु को परिभाषित करने की ओर ले जा रहे हैं।

परिभाषा: वलय $(R, +, \cdot)$ को **क्षेत्र** कहते हैं यदि $(R \setminus \{0\}, \cdot)$ एक आबेली समूह है।

इस प्रकार, निकाय $(R, +, \cdot)$ को एक क्षेत्र होने के लिए आवश्यक है कि वह इकाई 10 में दिए वलय अभिगृहीतों R1 से R6 को संतुष्ट करे तथा निम्नलिखित अभिगृहीतों को भी संतुष्ट करे।

R7) गुणन क्रमविनिमेय है;

R8) R का एक शून्येतर तत्समक है (जिसे हम 1 द्वारा व्यक्त करते हैं); तथा

R9) R में प्रत्येक शून्येतर अवयव x का एक गुणनात्मक प्रतिलोम है, जिसे हम x^{-1} द्वारा व्यक्त करते हैं, अर्थात्, $U(R) = R \setminus \{0\}$.

इससे पहले कि हम आगे बढ़ें, निम्नलिखित संबंधित जानकारी पर विचार करें।

टिप्पणी 2: एक वलय जो R8 और R9 को संतुष्ट करता है, परंतु R7 को नहीं, एक **विभाजन वलय (division ring)**, या **विषम क्षेत्र (skew field)**, या **अक्रमविनिमेय क्षेत्र (non-commutative field)** कहलाता है। ऐसे वलयों का भी बीजगणित के अध्ययन में एक बहुत महत्वपूर्ण स्थान है। (एक उदाहरण $\mathbb{H}$ है, जो वास्तविक चतुष्टियों का वलय है, जिसका अध्ययन आपने इकाई 10 में किया था।) परंतु इस पाठ्यक्रम में हम विभाजन वलयों की चर्चा नहीं करेंगे।

आइए क्षेत्रों पर वापस आ जाएँ। क्षेत्र की धारणा 19वीं शताब्दी में बीजीय संख्या सिद्धांत में ने बनाया। शोध करते हुए जर्मन गणितज्ञों रिचर्ड डेडेकिंड तथा लियोपोल्ड क्रोनेकर। डडेकिंड ने जर्मन शब्द 'Körper' का इस संकल्पना के लिए उपयोग किया, जिसका अर्थ 'क्षेत्र' होता है। इसी कारण से आप प्रायः पाएँगे कि गणित की पुस्तकों तथा लेखों में व्यापक क्षेत्र को K द्वारा व्यक्त किया जाता है।

जैसा कि आप देख चुके हैं, $\mathbb{Q}, \mathbb{R}$ और $\mathbb{C}$ क्षेत्र हैं। परंतु $(\mathbb{Z}^*, \cdot)$ एक समूह नहीं है। अतः, $\mathbb{Z}$ एक क्षेत्र नहीं है।

आइए अब एक और क्षेत्र का उदाहरण, कुछ विस्तार में देखें।

उदाहरण 11: दर्शाइए कि $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$ एक क्षेत्र है।

हल: इकाई 10 से आप जानते हैं कि $F = \mathbb{Q}[\sqrt{2}]$ तत्समक $\left(1 + \sqrt{2} \cdot 0\right)$ वाला एक क्रमविनिमेय वलय है।

अब, मान लीजिए कि F का $a + \sqrt{2}b$ एक शून्येतर अवयव है। परिमेयकरण की प्रक्रिया से हम देखते हैं कि

$$(a + \sqrt{2}b)^{-1} = \frac{1}{a + \sqrt{2}b} = \frac{a - \sqrt{2}b}{(a + \sqrt{2}b)\,(a - \sqrt{2}b)} = \frac{a - \sqrt{2}b}{a^2 - 2b^2}$$

$$= \frac{a}{a^2 - 2b^2} + \sqrt{2}\,\frac{(-b)}{a^2 - 2b^2} \in F.$$

(ध्यान दीजिए कि $a^2-2b^2 \neq 0$, क्योंकि $\sqrt{2}$ परिमेय संख्या नहीं है तथा a और b में से कम से कम एक शून्येतर है।)

इस प्रकार, F के प्रत्येक शून्येतर अवयव का एक गुणनात्मक प्रतिलोम है।

अतः, $F = \mathbb{Q} + \sqrt{2}\mathbb{Q}$ एक क्षेत्र है।

***

अब तक, आप क्षेत्रों के अनेक उदाहरणों को देख चुके हैं। क्या आपने इस ओर ध्यान दिया कि ये सभी पूर्णांकीय प्रांत भी हैं? यह कोई संयोग नहीं है। वस्तुतः, हमें निम्नलिखित परिणाम यही बताता है।

प्रमेय 5: प्रत्येक क्षेत्र एक पूर्णांकीय प्रांत होता है।

उपपत्ति: मान लीजिए कि F एक क्षेत्र है। तब, $F \neq \{0\}$, F एक क्रमविनिमेय वलय है तथा $1 \in F$. हमें यह देखने की आवश्यकता है कि क्या F में शून्य के भाजक हैं या नहीं। अतः, मान लीजिए कि a और b, F के अवयव हैं, जहाँ $ab = 0$ और $a \neq 0$. क्योंकि $a \neq 0$ तथा F एक क्षेत्र है, इसलिए a^{-1} का अस्तित्व है।

तब, जैसा आपने E5(ii) में सिद्ध किया था, a शून्य का भाजक नहीं है।

अतः, F में शून्य के भाजक नहीं हैं।

इस प्रकार, F एक पूर्णांकीय प्रांत है। ■

हम प्रमेय 5 का उपयोग अनेक विधियों से कर सकते हैं। उदाहरणार्थ, प्रमेय 5 और प्रमेय 1 के अनुप्रयोग से आप जानते हैं कि $\mathbb{Z}_{10}$ एक क्षेत्र नहीं है, क्योंकि 10 एक अभाज्य संख्या नहीं है।

अब, क्या प्रमेय 5 का विलोम सत्य है? अर्थात्, क्या प्रत्येक प्राँत एक क्षेत्र होता है? ध्यान दीजिए कि $\mathbb{Z}$ एक प्राँत है, परंतु यह एक क्षेत्र नहीं है।

अब, आपको निम्नलिखित संबंधित प्रश्नों को हल करना चाहिए।

E29) निम्नलिखित वलयों में से कौन-से क्षेत्र नहीं हैं, और क्यों?

$6\mathbb{Z},\ \mathbb{Z}_5,\ \mathbb{Z}_6,\ \mathbb{Z}[\sqrt{2}],\ \mathbb{Q}\times\mathbb{Q},\ \wp(\{a\}).$

E30) क्या क्षेत्र का उपवलय भी एक क्षेत्र होता है? क्यों?

E31) जाँच कीजिए कि $\mathbb{Z}[i]$ और $\mathbb{Q}[i]$ क्षेत्र हैं या नहीं।

E32) क्या $\mathbb{Z}[x]/<x^2>$ एक पूर्णांकीय प्राँत है? क्या यह एक क्षेत्र है? अपने उत्तरों के कारण दीजिए।

आप देख चुके हैं कि प्रत्येक प्राँत एक क्षेत्र नहीं होता। परंतु, यदि हम अपने को परिमित प्राँतों तक सीमित रखें, तो हम पाते हैं कि ये क्षेत्र हैं, जैसा अब आप देखेंगे।

प्रमेय 6: प्रत्येक परिमित पूर्णांकीय प्राँत एक क्षेत्र होता है।

उपपत्ति: मान लीजिए $R = \{a_0 = 0,\ a_1 = 1, a_2, \ldots, a_n\}$ एक प्राँत है। तब, परिभाषा द्वारा, R क्रमविनिमेय है। R को क्षेत्र दर्शाने के लिए $U(R) = R \setminus \{0\}$ दर्शाना होगा।

अतः, मान लीजिए कि R का $a = a_i$ एक शून्येतर अवयव है (अर्थात् $i \neq 0$). अवयवों $aa_1, \cdots, aa_n$ पर विचार कीजिए। प्रत्येक $j \neq 0$ के लिए $a_j \neq 0$, तथा क्योंकि $a \neq 0$, इसलिए हम $aa_j \neq 0$ प्राप्त करते हैं।

अतः, समुच्चय $\{aa_1, \ldots, aa_n\} \subseteq \{a_1, \ldots, a_n\}$.

साथ ही, $aa_1, aa_2, \ldots, aa_n$ सभी समुच्चय $\{a_1, \ldots, a_n\}$ के अलग-अलग अवयव हैं, क्योंकि $aa_j = aa_k \Rightarrow a_j = a_k$, प्रमेय 2 द्वारा।

इस प्रकार, $\{aa_1, \ldots, aa_n\} = \{a_1, \ldots, a_n\}$.

विशेष रूप में, $1 = a_1 = aa_j \;\; j = 1, \ldots, n$ के लिए किसी।

इस प्रकार, R में a व्युत्क्रमणीय है।

अतः, R के प्रत्येक शून्येतर अवयव का एक गुणनात्मक प्रतिलोम है।

इस प्रकार, R एक क्षेत्र है। ■

इस परिणाम का उपयोग करते हुए अब हम एक प्रमेय को सिद्ध करेंगे, जो क्षेत्रों के अनेक उदाहरणों को जनित करता है।

प्रमेय 7: $\mathbb{Z}_n$ एक क्षेत्र है यदि और केवल यदि n एक अभाज्य संख्या है।

उपपत्ति: प्रमेय 1 से आप जानते हैं कि $\mathbb{Z}_n$ एक प्राँत है यदि और केवल यदि n एक अभाज्य संख्या है। आप यह भी जानते हैं कि $\mathbb{Z}_n$ में केवल n अवयव हैं। अब, प्रमेय 6 से हमें परिणाम प्राप्त हो जाता है।

■

प्रमेय 7 से हमें क्षेत्रों के अनंततः अनेक उदाहरण मिलते हैं, जैसे $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$, इत्यादि। ये सभी उसके उदाहरण हैं, जिसे अब हम परिभाषित करने जा रहे हैं।

परिभाषा: एक क्षेत्र जिसका समुच्चय परिमित है, एक **परिमित क्षेत्र (finite field)** कहलाता है।

इस प्रकार, प्रत्येक अभाज्य p के लिए, $\mathbb{Z}_p$ एक परिमित क्षेत्र है। विज्ञान और प्रौद्योगिकी के विभिन्न क्षेत्रों, जैसे गूढ़लेखन (cryptography) में, परिमित क्षेत्रों के अनेक महत्वपूर्ण अनुप्रयोग हैं। आप ऊंचे के स्तर की पढ़ाई में इनका विस्तृत रूप से अध्ययन कर सकते हैं।

क्षेत्रों के सभी उदाहरणों को देखने हुए क्या आप क्षेत्र के अभिलक्षणिक के बारे में कुछ कह सकते हैं? हाँ, प्रमेयों 4 और 5 के उपयोग से।

प्रमेय 8: क्षेत्र का अभिलक्षणिक या तो शून्य होता है या एक अभाज्य संख्या होता है।

उपपत्ति: प्रमेयों 4 और 5 के अनुप्रयोग से, हमें यह परिणाम प्राप्त हो जाता है। ■

प्रमेय 7 और प्रमेय 8 से हम देखते हैं कि प्रत्येक अभाज्य p के लिए, हमें अभिलक्षणिक p वाला एक क्षेत्र, यानी $\mathbb{Z}_p$, प्राप्त होता है।

अभी तक आपने परिमित क्षेत्रों के जो उदाहरण देखे हैं उनमें किसी अभाज्य p के लिए p अवयव थे। निम्नलिखित प्रश्न में हम आपसे 4 अवयवों वाले एक परिमित क्षेत्र के उदाहरण की जाँच करने के लिए कह रहे हैं।

E33) मान लीजिए $R = \{0, 1, a, 1+a\}$. R में + और · को निम्नलिखित केली सारणियों के अनुसार परिभाषित कीजिए:

$+$	0	1	a	$1+a$
0	0	1	a	$1+a$
1	1	0	$1+a$	a
a	a	$1+a$	0	1
$1+a$	$1+a$	a	1	0

$\cdot$	0	1	a	$1+a$
0	0	0	0	0
1	0	1	a	$1+a$
a	0	a	$1+a$	1
$1+a$	0	$1+a$	1	a

दर्शाइए कि R एक क्षेत्र है। साथ ही, इस क्षेत्र का अभिलक्षणिक ज्ञात कीजिए।

E33 आपको बताता है कि n अवयवों वाले परिमित क्षेत्र भी हैं, जहाँ n एक अभाज्य संख्या नहीं है। परंतु, जैसा कि आप उच्चतर अध्ययन में देखेंगे, किसी अभाज्य p और किसी $r \in \mathbb{N}$ के लिए, $n = p^r$ होता है। उदाहरणार्थ, E33 में $n = 2^2$.

आइए अब क्षेत्र की गुणजावलियों पर विचार करें। अभी तक आपने जो क्षेत्रों के उदाहरण देखे हैं, उन पर विचार कीजिए। इकाई 12 में आप देख चुके हैं कि $\mathbb{Q}$, $\mathbb{R}$ और $\mathbb{C}$ की एक ही उचित गुणजावली है, यानी $\{0\}$. क्या यह अन्य क्षेत्रों के लिए भी सत्य है? इसका उत्तर निम्नलिखित प्रमेय में है।

प्रमेय 9: मान लीजिए R एक तत्समकी क्रमविनिमेय वलय है। तब, R एक क्षेत्र है यदि और केवल यदि R की गुणजावलियाँ केवल R और $\{0\}$ हैं।

उपपत्ति: आइए पहले मान लें कि R एक क्षेत्र है। मान लीजिए कि I, R की गुणजावली है I ।

यदि $I \neq \{0\}$, तो एक शून्येतर अवयव $x \in I$ है।

क्योंकि $x \neq 0$ तथा R एक क्षेत्र है, इसलिए किसी $y \in R$ के लिए $xy = 1$.

क्योंकि $x \in I$ तथा I एक गुणजावली है, इसलिए $xy \in I$, अर्थात्, $1 \in I$.

इस प्रकार, इकाई 12 के प्रमेय 2 द्वारा, $I = R$.

अतः, R की गुणजावलियाँ केवल $\{0\}$ और R हैं।

विलोमतः, मान लीजिए कि R की गुणजावलियाँ केवल R और $\{0\}$ हैं।

मान लीजिए कि $a \in R,\ a \neq 0$. मुख्य गुणजावली $Ra = \{ra \mid r \in R\}$ लीजिए।

यह R की शून्येतर गुणजावली है, क्योंकि $a \in Ra$.

अतः, $Ra = R$.

अब, $1 \in R = Ra$.

अतः, किसी $b \in R$ के लिए, $1 = ba$, अर्थात्, a^{-1} का अस्तित्व है।

क्योंकि a, R का कोई भी एक स्वेच्छिक शून्येतर अवयव था, इसलिए हमने सिद्ध कर लिया है कि ऐसे प्रत्येक अवयव का एक गुणनात्मक प्रतिलोम है।

अतः, R एक क्षेत्र है। ■

प्रमेय 9 और उदाहरण 11 से, आप जानते हैं कि $\mathbb{Q}[\sqrt{2}]$ की कोई अतुच्छ उचित गुणजावली नहीं है। वस्तुतः, $\mathbb{Q}[\sqrt{p}]$ की कोई अतुच्छ उचित गुणजावली नहीं होती, जहाँ p एक अभाज्य संख्या है। इसी प्रकार, आप अब यह भी जानते हैं कि $\mathbb{C}$, $\mathbb{R}$ और $\mathbb{Z}_p$ की कोई उचित अतुच्छ गुणजावलियाँ नहीं होती हैं। इस प्रकार, प्रमेय 9 बहुत उपयोगी है। आप पाएंगे कि आप इसका अनुप्रयोग इस खंड के शेष भाग में बार-बार करते रहेंगे।

प्रमेय 9 का उपयोग करते हुए, हम **क्षेत्र समाकारिताओं** (**field homomorphisms**) के कुछ रोचक गुण प्राप्त कर सकते हैं। हम निम्नलिखित प्रश्नों में आपसे इन्हें सिद्ध करने के लिए कह रहे हैं।

एक **क्षेत्र समाकारिता** एक क्षेत्र से दूसरे तक एक वलय समाकारिता होती है।

E34) मान लीजिए कि F और K क्षेत्र हैं तथा $f: F \to K$ एक क्षेत्र समाकारिता है। दर्शाइए कि या तो f शून्य फलन है या f एकैकी है।

E35) जाँच कीजिए कि

i) एक वलय से एक क्षेत्र तक कोई भी समाकारिता 1-1 है या नहीं,

ii) एक क्षेत्र समाकारिता को शून्य फलन या आच्छादक होना ज़रूरी है या नहीं।

E36) मान लीजिए R एक क्षेत्र F के तुल्याकारी एक वलय है। दर्शाइए कि R एक क्षेत्र होगा ही।

अब जब हम पूर्णांकीय प्राँतों और क्षेत्रों की चर्चा कर चुके हैं, आइए एक क्षेत्र में एक प्राँत को बैठाने की एक स्वाभाविक विधि पर बात करें।

14.5 विभाग क्षेत्र

आइए $\mathbb{Z}$ और $\mathbb{Q}$ के बीच संबंध पर विचार करें। आप जानते हैं कि $\mathbb{Q}$ का प्रत्येक अवयव $\frac{a}{b}$ के रूप का होता है, जहाँ $a \in \mathbb{Z}$ और $b \in \mathbb{Z}^*$. वास्तव में, हम $\frac{a}{b}$ को क्रमित युग्म $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ द्वारा भी व्यक्त कर सकते हैं। आइए इस बात के उपयोग से $\mathbb{Z} \times \mathbb{Z}^*$ पर एक ऐसे संबंध को परिभाषित करें जिसके अधीन अवयव $\mathbb{Q}$ के अवयव की तरह ही करें।के व्यवहार का अनुकरण करता हो।

याद कीजिए कि किसी वलय R के लिए, $R \setminus \{0\}$ को R^* व्यक्त करता है।

$\mathbb{Q}$ में आप जानते हैं कि $\frac{a}{b} = \frac{c}{d}$ iff $ad = bc$. आइए इसी प्रकार का एक संबंध ~, $\mathbb{Z} \times \mathbb{Z}^*$ के अवयवों पर रखें, अर्थात्, $(a,b) \sim (c,d)$ iff $ad = bc$.

तब, आपको इसकी जाँच करनी चाहिए कि ~ एक तुल्यता संबंध है।

आगे, आप जानते हैं कि $\mathbb{Q}$ में संक्रियाएँ निम्नलिखित तरह से परिभाषित हैं :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \text{ और } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \;\forall\; \frac{a}{b}, \frac{c}{d} \in \mathbb{Q}.$$

इकाई 1 से याद कीजिए कि ~ के सापेक्ष $\mathbb{Z} \times \mathbb{Z}^*$ के तुल्यता वर्गों के समुच्चय को $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$ द्वारा व्यक्त किया जाता है।

इन संक्रियाओं को ध्यान में रखते हुए, हम $\mathbb{Z} \times \mathbb{Z}^*$ में तुल्यता वर्गों पर द्वि-आधारी संक्रियाएँ निम्नलिखित रूप में परिभाषित करते हैं:

$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$, तथा

$[(a,b)] \cdot [(c,d)] = [(ac, bd)] \;\forall\; [(a,b)], [(c,d)] \in (\mathbb{Z} \times \mathbb{Z}^*)/\sim$.

ऐसा होता है कि इन तुल्यता वर्गों का समुच्चय इन संक्रियाओं के सापेक्ष एक वलय बन जाता है तथा यह $\mathbb{Q}$ के तुल्यताकारी एक क्षेत्र होता है।

साथ ही, $\mathbb{Z}$ से इस क्षेत्र तक एक आविष्टि होती है। अतः, हम $\mathbb{Z}$ को इस क्षेत्र का उपवलय मान सकते हैं।

आइए किसी दिए हुए पूर्णांकीय प्राँत को आविष्ट करने वाले एक क्षेत्र को प्राप्त करने की इस प्रक्रिया को व्यापकीकृत करें।

एक वलय R एक वलय S में **अतःस्थापित (embedded)** होता है, यदि R से S तक एक एकैक समाकारिता हो।

प्रमेय 10: मान लीजिए कि R एक पूर्णांकीय प्राँत है। तब, R को एक क्षेत्र F में अतःस्थापित किया जा सकता है, जहाँ F का प्रत्येक अवयव ab^{-1} के रूप का होता है $a, b \in R, b \neq 0$ के लिए।

उपपत्ति: क्रमित युग्मों के समुच्चय $K = \{(a,b) \mid a, b \in R$ और $b \neq 0\}$ पर विचार कीजिए।

आइए K में '$(a,b) \sim (c,d)$ यदि $ad = bc$' द्वारा एक संबंध ~ को परिभाषित करें।

~ स्वतुल्य है: $(a,b) \sim (a,b)\ \forall\ (a,b) \in K,$ क्योंकि R क्रमविनिमेय है। अतः, ~ स्वतुल्य है।

~ सममित है: मान लीजिए $(a,b), (c,d) \in K,$ जहाँ $(a,b) \sim (c,d).$

तब, $ad = bc.$ अर्थात् $cb = da.$

अतः, $(c,d) \sim (a,b).$

इस प्रकार, ~ सममित है।

~ संक्रामक है: मान लीजिए $(a,b), (c,d), (u,v) \in K$ ऐसे हैं कि $(a,b) \sim (c,d)$ तथा $(c,d) \sim (u,v).$

तब, $ad = bc$ और $cv = du.$

अतः, $(ad)v = (bc)v = b(cv) = bdu,$ अर्थात्, $avd = bud.$

क्योंकि $d \neq 0,$ इसलिए गुणन के निरसन नियम द्वारा, हम $av = bu,$ अर्थात् $(a,b) \sim (u,v)$ प्राप्त करते हैं।

इस प्रकार, ~ संक्रामक है।

अतः, ~ एक तुल्यता संबंध है।

आइए (a,b) को आविष्ट करने वाले तुल्यता वर्ग को $[a,b]$ द्वारा व्यक्त करें।

इस प्रकार, $[a,b] = \{(c,d) \mid c, d \in R,\ d \neq 0$ और $ad = bc\}.$

उदाहरणार्थ, $\mathbb{Z} \times \mathbb{Z}^*$ में $(2,6) \in [1,3]$ तथा $(1,2) \notin [1,3],$ क्योंकि $2 \cdot 3 = 6 \cdot 1$ और $1 \cdot 3 \neq 2 \cdot 1.$

साथ ही, ध्यान दीजिए कि **किसी भी प्राँत R के लिए, $[0,1] = \{0\} \times (R \setminus \{0\})$.**

मान लीजिए कि $F, \sim$ के सापेक्ष K के सभी तुल्यता वर्गों का समुच्चय है। अर्थात्, $\mathbf{F} = \mathbf{K}/\sim$.

जैसा कि हमने $(\mathbb{Z} \times \mathbb{Z}^*)/\sim$ के लिए किया था, आइए F में + और $\cdot$ को निम्नलिखित तरीके से परिभाषित करें:

$[a,b]+[c,d]=[ad+bc,bd]$, तथा

$[a,b]\cdot[c,d]=[ac,bd]$.

क्या आप इससे सहमत हैं कि F पर + और $\cdot$ द्वि-आधारी संक्रियाएँ हैं? ध्यान दीजिए कि यदि पूर्णांकीय प्राँत R में $b \neq 0$ और $d \neq 0$, तो $bd \neq 0$. अतः, संक्रियाओं को परिभाषित करने वाले समीकरणों के दाएँ पक्ष F में तुल्यता वर्ग हैं। इस प्रकार, F में दो अवयवों के योग और गुणनफल पुनः F के अवयव हैं। परंतु, हमें अभी भी यह सुनिश्चित करना है कि ये संक्रियाएँ सुपरिभाषित हैं।

अतः, मान लीजिए कि $[a,b]=[a',b']$ और $[c,d]=[c',d']$. हमें $[a,b]+[c,d]=[a',b']+[c',d']$ और $[a,b]\cdot[c,d]=[a',b']\cdot[c',d']$, दर्शाना है कि अर्थात्, $[ad+bc,bd]=[a'd'+b'c',b'd']$ तथा $[ac,bd]=[a'c',b'd']$.

अब, $(ad+bc)b'd'-(a'd'+b'c')bd$

$$= ab'dd' + cd'bb' - a'bdd' - c'dbb'$$

$$= (ab'-a'b)dd' + (cd'-c'd)bb'$$

$$= (0)dd' + (0)bb', \text{ क्योंकि } (a,b)\sim(a',b') \text{ तथा } (c,d)\sim(c',d').$$

$$= 0.$$

अतः, $[ad+bc,bd]=[a'd'+b'c',b'd']$, अर्थात्, + सुपरिभाषित है।

अब, आइए जाँच करें कि गुणन सुपरिभाषित है। निम्नलिखित पर विचार कीजिए:

$$(ac)(b'd')-(bd)(a'c') = ab'cd' - ba'dc'$$

$$= ba'cd' - ba'cd', \text{ क्योंकि } ab'=ba' \text{ और } cd'=dc'.$$

$$= 0.$$

अतः, $[ac,bd]=[a'c',b'd']$, अर्थात्, $\cdot$ सुपरिभाषित है।

आइए, अब सिद्ध करें कि F एक क्षेत्र है।

i) **+ साहचर्य है:** $[a,b],[c,d],[u,v] \in F$ के लिए,

$$([a,b]+[c,d])+[u,v] = [ad+bc,bd]+[u,v]$$

$$= [(ad+bc)v+ubd, bdv]$$

$$= [adv + b(cv + ud), bdv]$$

$$= [a, b] + [cv + ud, dv]$$

$$= [a, b] + ([c, d] + [u, v]).$$

ii) **+ क्रमविनिमेय है**: $[a, b], [c, d] \in F$ के लिए,

$[a, b] + [c, d] = [ad + bc, bd] = [cb + da, db] = [c, d] + [a, b].$

iii) **F के लिए [0,1] योज्य तत्समक है**: $[a, b] \in F$ के लिए,

$[0,1] + [a, b] = [0 \cdot b + 1 \cdot a, 1 \cdot b] = [a, b].$

iv) **$[a,b] \in F$ का योज्य प्रतिलोम $[-a,b]$ है:**

$[a, b] + [-a, b] = [ab - ab, b^2] = [0, b^2] = [0,1]$, क्योंकि $(0,1) \sim (0, b^2)$.

हम चाहेंगे कि F के क्षेत्र होने के लिए शेष ज़रूरी गुणों को आप सिद्ध करें (देखिए E37), जिसके बाद उपपत्ति जारी रहेगी।

E37) दर्शाइए कि F में $\cdot$ साहचर्य है, क्रमविनिमेय है, + बंटित है, तथा F के लिए [1, 1] गुणनात्मक तत्समक है।

आगे, दर्शाइए कि $F^* = \{[a, b] \in F \mid a, b \neq 0\}$ तथा $U(F) = F^*$.

अतः, हमने अपने मस्तिष्कों को एक साथ रख कर **सिद्ध कर लिय है कि F एक क्षेत्र है।**

अब, आइए $f: R \to F: f(a) = [a,1]$ परिभाषित करें। हम दर्शाना चाहते हैं कि f एक एकैकी समाकारिता है।

f सुपरिभाषित है: यदि R में $a = b$, तो F में $[a,1] = [b,1]$, अर्थात् F में $f(a) = f(b)$.

f एक समाकारिता है: a, $b \in R$ के लिए,

$f(a + b) = [a + b, 1] = [a,1] + [b,1] = f(a) + f(b)$, तथा

$f(ab) = [ab, 1] = [a,1] \cdot [b,1] = f(a) \cdot f(b).$

f एकैकी है: मान लीजिए $a, b \in R$ ऐसे हैं कि $f(a) = f(b)$. तब, $[a,1] = [b,1] \Rightarrow (a,1) \sim (b,1) \Rightarrow a = b.$

इस प्रकार, f एक एकैक समाकारिता है।

अतः, समाकारिता के मूल प्रमेय द्वारा, $\operatorname{Im} f = f(R)$, F का एक उपवलय है जो R के तुल्याकारी है।

जैसा कि आप जानते हैं, तुल्याकारी संरचनाएँ बीजीय रूप से एक समान होती हैं।

इसलिए, हम R और $f(R)$ को एक ही मान सकते हैं, तथा R को F का एक उपवलय सोच सकते हैं।

अब, F का कोई भी अवयव $[a,b]=[a,1][1,b]=[a,1][b,1]^{-1}=f(a)f(b)^{-1}$ के रूप का होता है, जहाँ $b \neq 0$.

इस प्रकार, $x \in R$ और $f(x) \in f(R)$ का एकीकरण करने पर, हम कह सकते हैं कि F का कोई भी अवयव ab^{-1} के रूप का होता है, जहाँ $a, b \in R, b \neq 0$.

अतः, F ही वाँछित क्षेत्र है, जिसमें R अंतःस्थापित है। ■

जिस क्षेत्र F के अस्तित्व को हमने अभी सिद्ध किया है, उसे R का **विभाग क्षेत्र (field of quotients,** या **quotient field**, या **field of fractions**) कहते हैं।

इस प्रकार, $\mathbb{Q}$, $\mathbb{Z}$ का विभाग क्षेत्र है।

इस संदर्भ में निम्नलिखित टिप्पणी पर विचार कीजिए।

टिप्पणी 3: याद रखिए कि प्राँत R के विभाग क्षेत्र के अवयव वास्तव में तुल्यता वर्गों का एक गुणनफल है। जब हम कहते हैं कि इस क्षेत्र F का कोई अवयव ab^{-1} के रूप का है, तो असल में हमारा मतलब है $[a,1][b,1]^{-1}$, जहाँ $a, b \in R$, $b \neq 0$. हम R को "अयाथर्थ रूप में" उसकी F में तुल्याकारी प्रति $f(R)$ के बराबर मान रहे हैं।

विभाग क्षेत्र के और उदाहरणों पर विचार करने से पहले, हम इस क्षेत्र के एक मौलिक गुण को सिद्ध करेंगे। इस गुण से आपको किसी प्राँत के विभाग क्षेत्र को प्राप्त करने में कुछ आसानी होगी।

प्रमेय 11: किसी पूर्णांकीय प्राँत R का विभाग क्षेत्र R को आविष्ट करने वाला सबसे छोटा क्षेत्र होता है।

उपपत्ति: इसे सिद्ध करने के लिए, हम प्रमेय 10 के $[a,1]$ को a के समान मानेंगे $\forall\, a \in R$. मान लीजिए कि F, R का विभाग क्षेत्र है।

तब, $R \subseteq F$, जैसी प्रमेय 10 में चर्चा की गई थी।

मान लीजिए कि R को आविष्ट करने वाला एक अन्य क्षेत्र K है।

F का कोई भी अवयव ab^{-1} के रूप का है, जहाँ $a, b \in R$ और $b \neq 0$.

क्योंकि $a, b \in R$, इसलिए $a, b \in K$.

क्योंकि $b \in K^*$ तथा K एक क्षेत्र है, इसलिए $b^{-1} \in K$.

अतः, $a, b^{-1} \in K$. इसलिए $ab^{-1} \in K$.

इस प्रकार, $F \subseteq K$.

अतः, R को आविष्ट करने वाला सबसे छोटा क्षेत्र F है। ■

आइए अब प्राँतों के एक बड़े वर्ग का विभाग क्षेत्र ज्ञात करने के लिए, प्रमेय 11 का उपयोग करें।

उदाहरण 12: क्षेत्र F का विभाग क्षेत्र ज्ञात कीजिए।

हल: क्योंकि F एक क्षेत्र है, इसलिए यह स्वयं को आविष्ट करने वाला लघुतम क्षेत्र है। इस प्रकार, F स्वयं अपना ही विभाग क्षेत्र है।

***

उदाहरण 12 से आप जानते हैं कि $\mathbb{Z}_p$ स्वयं अपना ही विभाग क्षेत्र है, जहाँ p एक अभाज्य संख्या है। इसी प्रकार, $\mathbb{Q}$ और $\mathbb{C}$ भी स्वयं अपने ही विभाग क्षेत्र हैं।

अब कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E38) क्या $\mathbb{R}$, $\mathbb{Z}+\sqrt{2}\mathbb{Z}$ का विभाग क्षेत्र है? या, क्या यह $\mathbb{C}$ है? या, क्या यह $\mathbb{Q}+\sqrt{2}\mathbb{Q}$ है? अपने उत्तरों के लिए कारण दीजिए।

E39) प्रमेय 10 में क्षेत्र F की रचना के किस स्तर पर यह मानना अति आवश्यक था कि R एक प्राँत है? क्यों?

E40) मान लीजिए R एक तत्समकी क्रमविनिमेय वलय है, परंतु एक पूर्णांकीय प्राँत नहीं है। क्या R को किसी क्षेत्र में अंतःस्थापित किया जा सकता है? क्यों, या क्यों नहीं?

इस भाग में आपने देखा कि किस प्रकार एक पूर्णांकीय प्राँत को स्वाभाविक रूप से एक क्षेत्र में अंतःस्थापित किया जा सकता है। आइए अब ऐसे विभाग वलयों पर दृष्टि डालें जो पूर्णांकीय प्राँत या क्षेत्र हैं, तथा उनके संगत विभाग क्षेत्रों को भी देखें।

14.6 अभाज्य और उच्छिष्ठ गुणजावलियाँ

आइए, पुनः $\mathbb{Z}_p$ पर विचार करते हुए प्रारंभ करें। आप जानते हैं कि $n \in \mathbb{N}$ के लिए, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. आप यह भी जानते हैं कि $\mathbb{Z}_n$ एक पूर्णांकीय प्राँत है iff n एक अभाज्य संख्या है। इस प्रकार, $\mathbb{Z}/n\mathbb{Z}$ एक प्राँत है iff n एक अभाज्य संख्या है। अभाज्य p का वह कौन-सा गुण है जिकसी वजह से $\mathbb{Z}/p\mathbb{Z}$ प्राँत बनता है?

आप जानते हैं कि यदि p एक अभाज्य संख्या है तथा p दो पूर्णांकों a और b के गुणनफल को विभाजित करता है, तब या तो a को p विभाजित करता है या b को p विभाजित करता है। दूसरे शब्दों में, यदि $ab \in p\mathbb{Z}$, तो या तो $a \in p\mathbb{Z}$ या $b \in p\mathbb{Z}$. यही वह गुण है जो $p\mathbb{Z}$ को $\mathbb{Z}$ की एक विशिष्ट गुणजावली बनाती है। अधिक व्यापक रूप में, निम्नलिखित परिभाषा पर विचार कीजिए।

परिभाषा: एक वलय R (ज़रूरी नहीं कि यह क्रमविनिमेय हो) की एक उचित गुणजावली P को एक **अभाज्य गुणजावली (prime ideal)** कहा जाता है यदि जब भी $a, b \in R$ के लिए $ab \in P$, तब या तो $a \in P$ या $b \in P$.

इस प्रकार, $2\mathbb{Z}, 3\mathbb{Z}, 11\mathbb{Z}$ सभी $\mathbb{Z}$ की अभाज्य गुणजावलियाँ है।

एक अन्य उदाहरण के रूप में, $\mathbb{R}$ की $\{0\}$ एक अभाज्य गुणजावली है, क्योंकि यह $\mathbb{R}$ की एक उचित गुणजावली है, तथा

$ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a = 0$ या $b = 0 \Rightarrow a \in \{0\}$ या $b \in \{0\}$, जहाँ $a, b \in \mathbb{R}$.

आइए अभाज्य गुणजवालियों के और उदाहरणों पर दृष्टि डालें।

उदाहरण 13: मान लीजिए R एक पूर्णांकीय प्राँत है। दर्शाइए कि $R \times R$ की $I = \{(0, x) | x \in R\}$ एक अभाज्य गुणजावली है।

हल: ध्यान दीजिए कि $I = \{0\} \times R$. है। इकाई 12 में आप देख चुके हैं कि I, $R \times R$ की एक गुणजावली है।

साथ ही, यह एक उचित गुणजावली है, क्योंकि $\{0\} \neq R$.

अब, आइए इसकी जाँच करें कि I एक अभाज्य गुणजावली है या नहीं। इसके लिए, आइए मान लें कि $(a_1, b_1), (a_2, b_2) \in R \times R$ s.t. $(a_1, b_1)(a_2, b_2) \in I$.

तब, किसी $x \in R$ के लिए, $(a_1a_2, b_1b_2) = (0, x)$.

$\therefore a_1a_2 = 0$, अर्थात्, $a_1 = 0$ या $a_2 = 0$, क्योंकि R एक प्राँत है।

अतः,, $(a_1, b_1) \in I$ या $(a_2, b_2) \in I$.

इस प्रकार, $R \times R$ की I एक अभाज्य गुणजावली है।

***

उदाहरण 14: जाँच कीजिए कि $\wp(X)$ की गुणजावली $\wp(Y)$ एक अभाज्य गुणजावली है या नहीं, जहाँ X एक अरिक्त समुच्चय है तथा X का Y एक उचित अरिक्त उपसमुच्चय है।

हल: मान लीजिए कि $A, B \in \wp(X)$ s.t. $AB \in \wp(Y)$, अर्थात्, $A \cap B \subseteq Y$. तब, यह आवश्यक नहीं है कि $A \subseteq Y$ या $B \subseteq Y$, अर्थात्, यह आवश्यक नहीं है कि $A \in \wp(Y)$ या $B \in \wp(Y)$.

उदाहरणार्थ, मान लीजिए कि $X = \{1, 2, 3\}$, $Y = \{1\}$, $A = \{1, 2\}$ और $B = \{1, 3\}$. तब, $A \cap B \subseteq Y$, परंतु न तो A और न ही B समुच्चय Y के उपसमुच्चय हैं।

इस प्रकार, $\wp(X)$ की $\wp(Y)$ एक अभाज्य गुणजावली नहीं है।

***

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए। ऐसा करने से आपको अभाज्य गुणजावलियों को बेहतर समझेंगे।

E41) जाँच कीजिए कि की समुच्चय $I = \{f \in C[0,1] \mid f(0) = 0\}$, $C[0,1]$ एक अभाज्य गुणजावली है या नहीं।

E42) दर्शाइए कि एक तत्समकी क्रमविनिमेय अतुच्छ वलय R एक पूर्णांकीय प्राँत है यदि और केवल यदि गुणजावली $\{0\}$, R की एक अभाज्य गुणजावली है।

E43) $\mathbb{C}$ की सभी अभाज्य गुणजावलियाँ ज्ञात कीजिए।

E44) जाँच कीजिए कि $\mathbb{Z}[\sqrt{5}]$ की $< 6 >$ एक अभाज्य गुणजावली है या नहीं।

अब, जैसा कि आप देख चुके हैं, $\mathbb{Z}/n\mathbb{Z}$ एक प्राँत है यदि और केवल यदि $n\mathbb{Z}$, की $\mathbb{Z}$ की एक अभाज्य गुणजावली है। क्या यह स्थिति केवल $\mathbb{Z}$ की अभाज्य गुणजावलियों के लिए ही सत्य है? वस्तुतः, यही संबंध किसी भी पूर्णांकीय प्राँत और उसकी अभाज्य गुणजावलियों के लिए सत्य है, जैसा कि अब हम सिद्ध करेंगे।

प्रमेय 12: एक तत्समकी क्रमविनिमेय वलय R की गुणजावली P एक अभाज्य गुणजावली होती है यदि और केवल यदि विभाग वलय R/P एक पूर्णांकीय प्राँत है।

उपपत्ति: आइए पहले मान कर चलें कि R की P एक अभाज्य गुणजावली है। क्योंकि R क्रमविनिमेय तथा तत्समकी है, इसलिए इकाई 12 से आप जानते हैं कि R/P क्रमविनिमेय तथा तत्समकी है।

साथ ही, क्योंकि R की P एक उचित गुणजावली है, इसलिए $(R/P) \neq \{\overline{0}\}$.

अब, मान लीजिए R/P में $a+P$ और $b+P$ ऐसे हैं कि $(a+P)(b+P)=P$, R/P का शून्य अवयव।

तब, $ab+P=P$, अर्थात्, $ab \in P$.

क्योंकि R की P एक अभाज्य गुणजावली है, इसलिए या तो $a \in P$ या $b \in P$.

अतः, या तो $a+P=P$ या $b+P=P$.

इस प्रकार, R/P में कोई शून्य के भाजक नहीं हैं।

अतः, R/P एक पूर्णांकीय प्राँत है।

विलोमतः, मान लीजिए कि R/P एक पूर्णांकीय प्राँत है।

मान लीजिए $a, b \in R$ ऐसे हैं कि $ab \in P$.

तब, R/P में $ab+P=P$, अर्थात्, R/P में $(a+P)(b+P)=P$.

क्योंकि R/P एक पूर्णांकीय प्राँत है, इसलिए या तो $a+P=P$ या $b+P=P$, अर्थात्, या तो $a \in P$ या $b \in P$.

इससे प्रदर्शित होता है कि R की P एक अभाज्य गुणजावली है। ■

आइए यह समझने के लिए कि प्रमेय 12 कितना उपयोगी है, कुछ उदाहरणों पर विचार करें।

उदाहरण 15: $\mathbb{Z}_{45}$ की सभी अभाज्य गुणजावलियाँ ज्ञात कीजिए।

हल: आप जानते हैं कि $\mathbb{Z}_{45} = \mathbb{Z}/45\mathbb{Z}$. अतः, इकाई 12 के प्रमेय 8 द्वारा, आप जानते हैं कि $\mathbb{Z}_{45}$ की गुणजावलियाँ $45\mathbb{Z}$ को अंतर्विष्ट करने वाली $\mathbb{Z}$ की गुणजावलियों के संगत हैं।

इस प्रकार, $\mathbb{Z}_{45}$ की गुणजावलियाँ $<\overline{n}>$ हैं, जहाँ $n|45$. अतः, $n = 1, 3, 5, 9, 15, 45$.

अतः, $<\overline{n}>$ क्रमशः $\mathbb{Z}_{45}, <\overline{3}>, <\overline{5}>, <\overline{9}>, <\overline{15}>, <\overline{0}>$ है।

क्योंकि एक अभाज्य गुणजावली उचित गुणजावली है, इसलिए $\mathbb{Z}_{45}$ अभाज्य गुणजावली नहीं है।

क्योंकि $\overline{3} \cdot \overline{3} \in <\overline{9}>$, लेकिन $\overline{3} \notin <\overline{9}>, <\overline{9}>$ अभाज्य गुणजावली नहीं है।

इसी तरह आपको दर्शाना चाहिए कि क्यों $<\overline{15}>$ एक अभाज्य गुणजावली नहीं है।

क्योंकि 45 अभाज्य नहीं है, $\mathbb{Z}_{45}$ प्राँत नहीं है। अतः, $<\overline{0}>$ एक अभाज्य गुणजावली नहीं है।

अब, $\mathbb{Z}_{45}/<\overline{3}> \simeq \mathbb{Z}_3$, तुल्याकारिता प्रमेयों से; और $\mathbb{Z}_3$ एक क्षेत्र है। अतः, $\mathbb{Z}_{45}/<\overline{3}>$ एक क्षेत्र है। इसलिए, प्रमेय 12 से, $<\overline{3}>$ वलय $\mathbb{Z}_{45}$ की अभाज्य गुणजावली है।

इसी तरह दर्शाइए कि $<\overline{5}>$, $\mathbb{Z}_{45}$ की अभाज्य गुणजावली है।

ध्यान दें कि केवल $<\overline{3}>$ और $<\overline{5}>$ ही $\mathbb{Z}$ की ऐसी अभाज्य गुणजावली हैं, जो $45\mathbb{Z}$ को आविष्ट करती हैं।

E47 में आप देखेंगे कि $\mathbb{Z}_n$ की अभाज्य गुणजावलियाँ $\mathbb{Z}$ के संगत हैं जो $n\mathbb{Z}$ को आविष्ट करती हैं।

इस प्रकार, $\mathbb{Z}_{45}$ की अभाज्य गुणजावलियाँ $45\mathbb{Z}$ को आविष्ट करने वाली $\mathbb{Z}$ की अभाज्य गुणजावलियों के संगत हैं, अर्थात्, $p\mathbb{Z}$ हैं, जहाँ $p|45$ और p एक अभाज्य संख्या है।

अर्थात्, $\mathbb{Z}_{45}$ की अभाज्य गुणजावलियाँ $<\overline{5}> = \{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}, \overline{30}, \overline{35}, \overline{40}\}$ और $<\overline{3}> = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}, \overline{21}, \overline{24}, \overline{27}, \overline{30}, \overline{33}, \overline{36}, \overline{39}, \overline{42}\}$ है।

***

उदाहरण 16: दर्शाइए कि की $<x+5>$, $\mathbb{R}[x]$ एक अभाज्य गुणजावली है। साथ ही, $\mathbb{R}[x]/<x+5>$ का विभाग क्षेत्र भी ज्ञात कीजिए।

हल: आइए, पहले $\mathbb{R}[x]/<x+5> \simeq \mathbb{R}$ सिद्ध करने के लिए समाकारिता के मूल प्रमेय का उपयोग करें।

मूल्यांकन फलन $\phi : \mathbb{R}[x] \to \mathbb{R} : \phi(f(x)) = f(-5)$ को परिभाषित कीजिए।

आप इकाई 13 के E2 से जानते हैं कि ϕ एक सुपरिभाषित वलय आच्छादक समाकारिता है। साथ ही,

$\text{Ker}\,\phi = \{f(x) \in \mathbb{R}[x] |$ (-5), $f(x)$ का एक मूल है$\}$ $= \{f(x) \in \mathbb{R}[x] | f(x)$ को $(x+5)$ विभाजित करता है$\}$, जैसा कि आप 'कलन' के खंड 1 से जानते हैं।

$= <x+5>.$

अतः, समाकारिता के मूल प्रमेय द्वारा, $\mathbb{R}[x]/<x+5> \simeq \mathbb{R}.$

क्योंकि $\mathbb{R}$ एक क्षेत्र है, इसलिए यह एक प्रांँत है।

अतः, $\mathbb{R}[x]/<x+5>$ एक प्रांँत है।

इस प्रकार, प्रमेय 12 के प्रयोग से, $<x+5>$, $\mathbb{R}[x]$ की अभाज्य गुणजावली है।

आगे, क्योंकि $\mathbb{R}[x]/<x+5> \simeq \mathbb{R}$ जो एक क्षेत्र है, इसलिए $\mathbb{R}[x]/<x+5>$ एक क्षेत्र है। अतः, यह स्वयं अपना ही विभाग क्षेत्र है।

***

उदाहरण 16 की ही तरह, आपको सिद्ध करना चाहिए कि $\mathbb{R}[x]$ की $<x+r>$ एक अभाज्य गुणजावली है $\forall\ r \in \mathbb{R}$.

अब, आइए किसी गुणजवाली की अभाज्यता की जाँच करने के लिए, तुल्याकारिता प्रमेयों और प्रमेय 12 के उपयोग के एक अन्य उदाहरण पर विचार करें।

उदाहरण 17: जाँच कीजिए कि $\mathbb{Z}_{49}$ की $<\overline{7}>$ एक अभाज्य गुणजावली है या नहीं। यदि है, तो $\mathbb{Z}_{49}/<\overline{7}>$ के विभाग क्षेत्र को ज्ञात कीजिए।

यदि नहीं है, तो एक ऐसा वलय दीजिए जिसमें $\mathbb{Z}_{49}/<\overline{7}>$ अंतःस्थापित है।

हल: हम तीसरे तुल्याकारिता प्रमेय का अनुप्रयोग करेंगे। इस प्रमेय को आपने इकाई 13 में सिद्ध किया था। यहाँ ध्यान दीजिए कि $49\mathbb{Z}$, $7\mathbb{Z}$ की गुणजावली है, तथा $7\mathbb{Z}$, $\mathbb{Z}$ की गुणजावली है। अब,

$$\mathbb{Z}/7\mathbb{Z} \simeq (\mathbb{Z}/49\mathbb{Z})/(7\mathbb{Z}/49\mathbb{Z}) \simeq \mathbb{Z}_{49}/<\overline{7}>.$$

क्योंकि आप देख चुके हैं कि $\mathbb{Z}/7\mathbb{Z}$ एक प्राँत है, इसलिए $\mathbb{Z}_{49}/<\overline{7}>$ भी एक प्राँत है।

अतः, $\mathbb{Z}_{49}$ की $<\overline{7}>$ एक अभाज्य गुणजावली है।

ध्यान दीजिए कि वाँछित विभाग क्षेत्र $\mathbb{Z}_7$ है। (क्यों?)

***

अब कुछ संबंधित प्रश्नों को हल करने का प्रयास कीजिए।

E45) जाँच कीजिए कि $\mathbb{Z}[x]$ की $<x+20>$ एक अभाज्य गुणजावली है या नहीं।

E46) मान लीजिए R एक ऐसा तत्समकी क्रमविनिमेय वलय है जिससे कि R/I एक प्राँत है वलय R की किसी गुणजावली I के लिए। क्या R एक प्राँत होगा ही? क्यों?

E47) $\mathbb{Z}_{30}$ की सभी अभाज्य गुणजावलियाँ मालूम कीजिए।

अब, $\mathbb{Z}$ में आप देख चुके हैं कि एक अभाज्य गुणजावली एक अभाज्य संख्या से जनित होती है। क्या इस बात को अन्य प्राँतों के लिए व्यापकीकृत किया जा सकता है?

इसके लिए, पहले हमें प्राँत में विभाज्यता और अभाज्य अवयवों के बारे में बात करनी होगी।

इकाई 10 के E29 से याद कीजिए कि हमने $\mathbb{Z}$ में 'b को a विभाजित करता है' की परिभाषा को किसी भी क्रमविनिमेय वलय R के लिए व्यापकीकृत किया था। आपने अध्ययन किया था कि R में एक अवयव a एक अवयव b को **विभाजित करता** है (जिसे $\mathbf{a}|\mathbf{b}$ द्वारा व्यक्त किया जाता है), यदि किसी $r \in R$ के लिए $b = ra$.

इस स्थिति में, हम यह भी कहते हैं कि b का a एक **गुणनखंड** है, या b का a एक **भाजक** है।

इस प्रकार, $\mathbb{Z}_7$ में $\bar{6}$ को $\bar{3}$ विभाजित करता है, क्योंकि $\bar{3} \cdot \bar{2} = \bar{6}$.

इसी प्रकार, $X = \{1, 2, 3\}$, $A = \{1, 2\}$ और $B = \{1\}$ के लिए, $\wp(X)$ में

क्योंकि $\exists\, C = \{1, 3\} \subseteq X$ s.t. $A \cap C = B$.

ध्यान दीजिए कि यदि R एक तत्समकी वलय है, तो $a|a\ \forall\, a \in R$. (क्यों?)

क्रमविनिमेय वलय के लिए 'भाजक' की इस परिभाषा के व्यापकीकरण से, अब आइए एक अभाज्य पूर्णांक की संकल्पना को व्यापकीकृत करें। हम देखेंगे कि किसी भी प्राँत में एक अभाज्य अवयव क्या होता है।

परिभाषा: पूर्णांकीय प्राँत R का एक शून्येतर अवयव p एक **अभाज्य अवयव** कहलाता है, यदि

i) p एक मात्रक नहीं है, तथा

ii) जब भी $a, b \in R$ और $p|ab$, तो $p|a$ या $p|b$.

इस प्रकार, $\mathbb{Z}$ के अभाज्य अवयव अभाज्य संख्याएँ और उनके संबंधित ऋणात्मक संख्याएं ही होते हैं। आप यह भी जानते हैं कि $\mathbb{Z}$ का अभाज्य अवयव एक अभाज्य गुणजावली जनित करता है। क्या यह अन्य प्राँतों के लिए भी सत्य है? निम्नलिखित प्रमेय इसका उत्तर देता है।

प्रमेय 13: मान लीजिए R एक पूर्णांकीय प्राँत है। तब, R का एक अभाज्य अवयव है यदि और केवल यदि Rp, R की एक अभाज्य गुणजावली है।

$x \in R$ का गुणनात्मक प्रतिलोम होता है iff $Rx = R$.

उपपत्ति: आइए पहले मान लें कि R का p एक अभाज्य अवयव है।

क्योंकि p का कोई गुणनात्मक प्रतिलोम नहीं है, इसलिए $1 \notin Rp$.

इस प्रकार, Rp, R की एक उचित गुणजावली है।

आगे, मान लीजिए $a, b \in R$ s.t. $ab \in Rp$. तब,

$ab = rp$, किसी $r \in R$ के लिए।

$\Rightarrow p|ab$

$\Rightarrow p|a$ या $p|b$, क्योंकि p एक अभाज्य अवयव है।

$\Rightarrow$ $a = xp$ या $b = xp$, किसी $x \in R$ के लिए।

$\Rightarrow a \in Rp$ या $b \in Rp$.

इस प्रकार, $ab \in Rp \Rightarrow a \in Rp$ या $b \in Rp$, अर्थात्, R की Rp एक अभाज्य गुणजावली है।

विलोमतः, मान लीजिए कि R की Rp एक अभाज्य गुणजावली है। तब, $Rp \neq R$, परिभाषा द्वारा। इस प्रकार, $1 \notin Rp$, तथा इसीलिए p का कोई गुणनात्मक प्रतिलोम नहीं है।

अब, मान लीजिए कि ab को p विभाजित करता है, जहाँ $a, b \in R$.

तब, किसी $r \in R$ के लिए, $ab = rp$, अर्थात्, $ab \in Rp$.

क्योंकि Rp एक अभाज्य गुणजावली है, इसलिए या तो $a \in Rp$ या $b \in Rp$.

अतः, या तो $p|a$ या $p|b$.

इस प्रकार, R में p एक अभाज्य अवयव है। ■

प्रमेय 13 इसकी जाँच करने के लिए अति उपयोगी है कि कोई अवयव अभाज्य है या नहीं। यह प्रमेय यह ज्ञात करने के लिए भी उपयोगी है कि एक मुख्य गुणजावली अभाज्य गुणजावली है या नहीं। उदाहरणार्थ, प्रमेय 13 और E42 हमें बताते हैं कि **R का 0 एक अभाज्य अवयव है iff R एक प्राँत है।**

अभाज्य गुणजावलियों के अनेक अन्य उपयोगी गुण हैं। निम्नलिखित प्रश्नों में हम आपसे इनमें से कुछ को सिद्ध करने के लिए कह रहे हैं।

याद रखिए कि यहाँ सभी वलयों को क्रमविनिमेय मान कर चल रहे हैं।

E48) मान लीजिए $f : R \to S$ एक वलय आच्छादक समाकारिता है जिसकी अष्टि N है। दर्शाइए कि

i) यदि S में J एक अभाज्य गुणजावली है, तो R में $f^{-1}(J)$ एक अभाज्य गुणजावली है।

ii) यदि I N को आविष्ट करने वाली R की एक अभाज्य गुणजावली है, तो S की $f(I)$ एक अभाज्य गुणजावली है।

iii) N को आविष्ट करने वाली R की अभाज्य गुणजावलियों के समुच्चय तथा S की अभाज्य गुणजावलियों के समुच्चय के बीच $\phi(I) = f(I)$ द्वारा दिया जाने वाला फलन ϕ एकैकी आच्छादक है।

E49) R से S तक एक ऐसे वलय समाकारिता f का उदाहरण दीजिए जिससे कि R की P एक अभाज्य गुणजावली है, परंतु S की $f(P)$ एक अभाज्य गुणजावली नहीं है।

E50) मान लीजिए P_1 और P_2 किसी वलय R की अलग अभाज्य गुणजावलियाँ हैं।

i) क्या $P_1 \cap P_2$ को R की अभाज्य गुणजावली होना ही होगा?

ii) क्या सभी स्थितियों में $P_1 + P_2$, R की अभाज्य गुणजावली होगी?

iii) क्या सभी स्थितियों में P_1P_2, R की अभाज्य गुणजावली होगी?

अपने उत्तरों के लिए कारण दीजिए।

E51) $\mathbb{Z} \times \mathbb{Z}$ की दो अलग अभाज्य गुणजावलियाँ दीजिए।

आइए अब एक विशेष प्रकार की अभाज्य गुणजावली को परिभाषित करें। यह वास्तव में एक वलय को एक ऐसे क्षेत्र से जोड़ेगी जो उसका विभाग वलय है।

आइए पुनः एक उदाहरण के तौर पर $\mathbb{Z}$ से प्रारंभ करें। $\mathbb{Z}$ की गुणजावली $2\mathbb{Z}$ लीजिए। मान लीजिए कि $\mathbb{Z}$ में $n\mathbb{Z}$ एक ऐसी गुणजावली है कि $2\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}$. तब, $n|2$. अतः, $n = \pm 1$ या $n = \pm 2$, जिससे कि $n\mathbb{Z} = \mathbb{Z}$ या $n\mathbb{Z} = 2\mathbb{Z}$.

यह बताता है कि $\mathbb{Z}$ की कोई भी गुणजावली $2\mathbb{Z}$ और $\mathbb{Z}$ के बीच नहीं हो सकती। अर्थात्, $2\mathbb{Z}$ को आविष्ट करने वाली $\mathbb{Z}$ की उचित गुणजावलियों में से $2\mathbb{Z}$ ही उच्चिष्ठ है। इससे हम निम्नलिखित परिभाषा तक पहुँचते हैं।

परिभाषा: वलय R की एक उचित गुणजावली M एक **उच्चिष्ठ गुणजावली (maximal ideal)** कहलाती है, यदि जब भी I, R की ऐसी गुणजावली है कि $M \subseteq I \subseteq R$, तो या तो $I = M$ या $I = R$.

इस प्रकार, एक उचित गुणजावली M एक उच्चिष्ठ गुणजावली होती है यदि R की कोई भी उचित गुणजावली उसे आविष्ट नहीं करती।

एक उदाहरण जो तुरंत आपके दिमाग में आ सकता है वह किसी भी क्षेत्र F में शून्य गुणजावली का है। यह उच्चिष्ठ है, क्योंकि आप जानते हैं कि F की अन्य गुणजावली केवल स्वयं F ही है। आप यह भी पहले देख चुके हैं कि $\{0\}$, F की अभाज्य गुणजावली है।

आपने अभी देखा कि क्षेत्रों की स्थिति में, उच्चिष्ठ गुणजावली एक अभाज्य गुणजावली होती है। क्या यह किसी भी वलय के लिए सत्य है? क्या वलय की अभाज्य गुणजावली और उच्चिष्ठ गुणजावली के बीच कुछ संबंध है? इनके उत्तर के लिए, उच्चिष्ठ गुणजावलियों की निम्नलिखित विशेषता पर विचार कीजिए।

प्रमेय 14: मान लीजिए R एक तत्समकी क्रमविनिमेय वलय है। R में M एक उच्चिष्ठ गुणजावली है यदि और केवल यदि R/M एक क्षेत्र है।

उपपत्ति: पहले, आइए मान लें कि R की M एक उच्चिष्ठ गुणजावली है। हम सिद्ध करना चाहते हैं कि R/M एक क्षेत्र है। आप पहले से जानते हैं कि R/M एक तत्समकी क्रमविनिमेय वलय है। अतः, यह सिद्ध करना काफ़ी है कि R/M की कोई अतुच्छ उचित गुणजावली नहीं है (प्रमेय 9 को देखिए)।

अतः, मान लीजिए कि R/M की I एक गुणजावली है। विहित समाकारिता $\eta : R \to R/M : \eta(r) = r + M$ पर विचार कीजिए।

तब, इकाई 13 से आप जानते हैं कि $\eta^{-1}(I)$, R की M को आविष्ट करने वाली एक गुणजावली है, और M, η की अष्टि है।

क्योंकि R की M एक उच्चिष्ठ गुणजावली है, इसलिए $\eta^{-1}(I) = M$ या $\eta^{-1}(I) = R$.

अतः, $I = \eta(\eta^{-1}(I))$ या तो $\eta(M)$ है या $\eta(R)$.

अर्थात्, $I = \{\bar{0}\}$ या $I = R/M$.

इस प्रकार, R/M एक क्षेत्र है।

विलोमतः,मान लीजिए कि R की M एक ऐसी गुणजावली है कि R/M एक क्षेत्र है।

तब R/M की गुणजावलियाँ केवल $\{\bar{0}\}$ और R/M हैं।

मान लीजिए कि I, M को आविष्ट करने वाली R की एक गुणजावली है। तब, ऊपर की तरह, $\eta(I) = \{\bar{0}\}$ या $\eta(I) = R/M$.

$\therefore I = \eta^{-1}(\eta(I))$ या M है या R.

अतः, M, R की एक उच्चिष्ठ गुणजावली है। ■

प्रमेय 14 से (तथा कुछ अन्य प्रमेयों को भी) तुरंत एक निष्कर्ष निकलता है।

उपप्रमेय 1: एक तत्समकी क्रमविनिमेय वलय की प्रत्येक उच्चिष्ठ गुणजावली एक अभाज्य गुणजावली होती है।

■

हम आपसे एक प्रश्न के रूप में इस उपप्रमेय को सिद्ध करने के लिए कह रहे हैं (E52 देखिए)।

ध्यान दीजिए कि उपप्रमेय 1 एक एक-तरफ़ा कथन है। इसके विलोम के बारे में क्या कहा जा सकता है? अर्थात्, क्या प्रत्येक अभाज्य गुणजावली उच्चिष्ठ होती है? इस संदर्भ में, $\mathbb{Z}$ में शून्य गुणजावली के बारे में आप क्या कह सकते हैं? क्योंकि $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$ है ,

इसलिए $\{0\}$ एक उच्चिष्ठ गुणजावली नहीं है। परंतु, क्योंकि $\mathbb{Z}$ एक पूर्णांकीय प्राँत है, इसलिए $\{0\}$, $\mathbb{Z}$ की एक अभाज्य गुणजावली है।

अब, आइए प्रमेय 14 में दिए शक्तिशाली लक्षणकरण का उच्चिष्ठ गुणजावलियों के कुछ उदाहरणों को प्राप्त करने के लिए उपयोग करें।

उदाहरण 18: दर्शाइए कि $\mathbb{Z}$ की गुणजावली $m\mathbb{Z}$ उच्चिष्ठ है यदि और केवल यदि m एक अभाज्य संख्या है।

हल: प्रमेय 7 से आप जानते हैं कि $\mathbb{Z}_m$ एक क्षेत्र है iff m अभाज्य संख्या है। आप यह भी जानते हैं कि $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$.

इस प्रकार, E36 द्वारा, $\mathbb{Z}/m\mathbb{Z}$ एक क्षेत्र है iff m अभाज्य है।

अतः, प्रमेय 14 द्वारा, $\mathbb{Z}$ में $m\mathbb{Z}$ उच्चिष्ठ है iff m एक अभाज्य संख्या है।

***

उदाहरण 19: दर्शाइए कि $\mathbb{Z}_{12}$ की $\bar{2}\mathbb{Z}_{12}$ एक उच्चिष्ठ गुणजावली है, जबकि $\bar{4}\mathbb{Z}_{12}$ नहीं है।

हल: आप जानते हैं कि $\mathbb{Z}_{12} \simeq \mathbb{Z}/12\mathbb{Z}$ तथा $\bar{2}\mathbb{Z}_{12} \simeq 2\mathbb{Z}/12\mathbb{Z}$. इस प्रकार, इकाई 13 के तीसरे तुल्याकारिता प्रमेय द्वारा, हम देखते हैं कि
$\mathbb{Z}_{12}/\bar{2}\mathbb{Z}_{12} \simeq (\mathbb{Z}/12\mathbb{Z})/(2\mathbb{Z}/12\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}_2$, जो एक क्षेत्र है। अतः, $\mathbb{Z}_{12}$ में $\bar{2}\mathbb{Z}_{12} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$ उच्चिष्ठ है।

अब, $\bar{4}\mathbb{Z}_{12} \subsetneq \bar{2}\mathbb{Z}_{12} \subsetneq \mathbb{Z}_{12}$.

अतः, $\mathbb{Z}_{12}$ में $\bar{4}\mathbb{Z}_{12} = \{\bar{0}, \bar{4}, \bar{8}\}$ उच्चिष्ठ नहीं है।

***

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E52) उपप्रमेय 1 को सिद्ध कीजिए।

E53) दर्शाइए कि $\mathbb{Z}_{10}$ में $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ उच्चिष्ठ है।

E54) जाँच कीजिए कि $\mathbb{C}[x]$ में $< x - \pi >$ उच्चिष्ठ है या नहीं।

E55) दर्शाइए कि $C[0,1]$ में $\{f \in C[0,1] \mid f(\frac{1}{2}) = 0\}$ उच्चिष्ठ है।

अतः, आइए देखें कि इस भाग में आपने क्या अध्ययन किया है। आपका पहले एक वलय की एक विशिष्ट गुणजावली, से यानी अभाज्य गुणजावली परिचय कराया गया। इसकी विशिष्टता इस बात से है कि इसका संगत विभाग वलय एक पूर्णांकीय प्राँत होता है। इसके बाद, आपने एक विशेष अभाज्य गुणजावली, यानी उच्चिष्ठ गुणजावली के बारे में अध्ययन किया। हम ऐसी गुणजावली को दुगुनी विशिष्ट क्यों समझते हैं? क्योंकि इसका संगत विभाग वलय एक क्षेत्र है, और क्षेत्र एक बहुत उपयोगी बीजीय संरचना है।

हम पूर्णांकीय प्राँतों की चर्चा को यहीं समाप्त कर रहे हैं। आइए अब उन सभी धारणाओं को संक्षेप में देखें जिनका अध्ययन इस इकाई में आपने किया है।

14.7 सारांश

इस इकाई में, हमने निम्नलिखित बिंदुओं पर चर्चा की है।

1. वलय में शून्य के भाजक की परिभाषा, तथा उसके उदाहरण।
2. एक पूर्णांकीय प्राँत की परिभाषा, और उदाहरण।
3. $\mathbb{Z}_n$ एक क्षेत्र है iff n एक अभाज्य संख्या है।
4. एक पूर्णांकीय प्राँत में गुणन के लिए निरसन नियम लागू होता है।
5. वलय के अभिलक्षणिक की परिभाषा, और उदाहरण।
6. एक पूर्णांकीय प्राँत का अभिलक्षणिक या तो शून्य होता है या एक अभाज्य संख्या।
7. एक क्षेत्र की परिभाषा, और उदाहरण।
8. प्रत्येक क्षेत्र एक प्राँत होता है, परंतु विलोम सत्य नहीं है।
9. एक परिमित प्राँत एक क्षेत्र होता है।
10. एक क्षेत्र का अभिलक्षणिक या तो शून्य होता है। या एक अभाज्य संख्या
11. एक पूर्णांकीय प्राँत का विभाग क्षेत्र कैसे बनता है।
12. एक पूर्णांकीय प्राँत का विभाग क्षेत्र उस प्राँत की आविष्ट करने वाला लघुतम क्षेत्र है।
13. अभाज्य और उच्चिष्ठ गुणजावलियों की परिभाषाएँ, और उदाहरण।
14. इस परिणाम की उपपत्ति और प्रयोग, कि एक तत्समकी वलय R की एक उचित गुणजावली I अभाज्य (क्रमशः, उच्चिष्ठ) होती है यदि और केवल यदि R/I एक पूर्णांकीय प्राँत (क्रमशः, एक क्षेत्र) हो।
15. प्रत्येक उच्चिष्ठ गुणजावली एक अभाज्य गुणजावली होती है, परंतु इसका विलोम सत्य नहीं है।

16. एक पूर्णांकीय प्राँत R का एक अवयव p अभाज्य होता है यदि औद केवल यदि मुख्य गुणजावली pR, R की एक अभाज्य गुणजावली है।

14.8 हल / उत्तर

E1) $\mathbb{Z}$ में कोई शून्य के भाजक नहीं हैं, क्योंकि $m \neq 0, n \neq 0 \Rightarrow mn \neq 0 \ \forall \ m, n \in \mathbb{Z}$.
खंड 3 में आप यह भी देख चुके हैं कि $U(\mathbb{Z}) = \{-1, 1\}$.

अब, आइए $\mathbb{Z}_{10}$ में शून्य के भाजकों पर विचार करें।

$\overline{m} \in \mathbb{Z}_{10}$ एक शून्य का भाजक है

$\Leftrightarrow \exists \ \overline{n} \in \mathbb{Z}_{10}$ s.t. $\overline{m} \cdot \overline{n} = \overline{0}, \overline{m} \neq \overline{0}, \overline{n} \neq \overline{0}$.

$\Leftrightarrow \overline{m} = \overline{2}$ or $\overline{m} = \overline{5}$.

इस प्रकार, $\mathbb{Z}_{10}$ में शून्य के भाजक $\overline{2}, \overline{5}$ हैं।

साथ ही, खंड 3 में आप देख चुके हैं कि
$U(\mathbb{Z}_{10}) = \{\overline{m} \in \mathbb{Z}_{10} | (m, 10) = 1\} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$.

इन दो उदाहरणों से वलय में शून्य के भाजकों के समुच्चय A तथा मात्रकों के समुच्चय B के बारे में एक संभव निष्कर्ष जिस पर हम पहुँच सकते हैं, वह है कि $A \cap B = \emptyset$. परंतु, व्यापक रूप से वलयों के लिए, यह केवल एक अनुमान ही है। इसे सिद्ध या असिद्ध किए जाने की आवश्यकता है।

E2) आपको निम्नलिखित कथन सिद्ध करना है :

$n \in \mathbb{N}$ के लिए, यदि $x \in \mathbb{Z}_n$ s.t. $(x, n) > 1$, तब $\overline{x}$, $\mathbb{Z}_n$ में एक शून्य का भाजक है।

इसे सिद्ध करने के लिए, मान लीजिए $\overline{x}, \mathbb{Z}_n$ में शून्य का भाजक नहीं है।

तब दर्शाइए कि $\mathbb{Z}_n = \{\overline{m}\,\overline{x} | \overline{m} \in \mathbb{Z}_n\} = < \overline{x} >$.

अतः, $(x, n) = 1$, जो $(x, n) > 1$ का अंतर्विरोध है।

इस तरह, $\overline{x}$ को $\mathbb{Z}_n$ में शून्य का भाजक होना ही होगा।

E3) मान लीजिए कि R में $b \neq 0$ और $ab = 0$.

तब, किसी भी $r \in R$ के लिए,

$(ra)b = r(ab) = 0.$

इस प्रकार, Ra का प्रत्येक शून्येतर अवयव शून्य का भाजक है।

E4) $\wp(X)=\{\emptyset, X\}, X \neq \emptyset.$

क्योंकि $X \cdot X = X \cap X = X \neq \emptyset$ है, इसलिए $\wp(X)$ में कोई शून्य के भाजक नहीं हैं।

E5) i) नहीं। उदाहरणार्थ, $2 \in \mathbb{Z}$ शून्य का भाजक नहीं है। साथ ही, $2 \notin U(\mathbb{Z})$.

ii) नहीं। आइए इसे सिद्ध करें।

यदि $a \in U(R), \exists\ b \in R$ s.t. $ab = 1$.

मान लीजिए R में a शून्य का भाजक होता। तब, R में $\exists\ c \neq 0$ s.t. $ac = 0$.

इस प्रकार, $acb = 0$, अर्थात् $(ab)c = 0$, क्योंकि R क्रमविनिमेय है।

$\therefore c = 0$, जो एक अंतर्विरोध है।

अतः, यदि $a \in U(R)$, तो R में a शून्य का भाजक नहीं है।

E6) प्रमेय 1 द्वारा, $\mathbb{Z}_{97}$ एक प्राँत है, क्योंकि 97 एक अभाज्य संख्या है।

$2\mathbb{Z}$ एक प्राँत नहीं है, क्योंकि $1 \notin 2\mathbb{Z}$.

$\mathbb{Z} + i\mathbb{Z}$ एक तत्समकी अतुच्छ क्रमविनिमेय वलय है।

अब, मान लीजिए $a + ib \in \mathbb{Z}[i]$ s.t. $\exists\ c + id \in \mathbb{Z}[i], c + id \neq 0,$ तथा $(a+ib)(c+id) = 0.$

तब, $ac - bd = 0,$ तथा ...(1)

$ad + bc = 0.$ ...(2)

(1) से $\mathbb{Z}$ में $b(c^2 + d^2) = 0$ मिलता है, (2) के उपयोग से।

$\therefore b = 0$ या $c^2 + d^2 = 0.$

$c^2 + d^2 = 0 \Rightarrow c = 0$ और $d = 0,$ जो संभव नहीं है क्योंकि $c + id \neq 0.$

$\therefore b = 0.$

तब, (1) से $ac = 0,$ और (2) से $ad = 0$ मिलता है।

यदि $a \neq 0,$ तो $ac = 0$ जिससे $c = 0$ मिलता है; और $ad = 0 \Rightarrow d = 0.$

यह संभव नहीं है, पुनः क्योंकि $c + id \neq 0.$

अतः, $a = 0$ भी है।

इस प्रकार, $a + ib = 0.$

अतः, $\mathbb{Z}[i]$ में कोई शून्य के भाजक नहीं हैं, तथा इसीलिए यह एक प्राँत है।

उदाहरण 4 की ही तरह, $\mathbb{R} \times \mathbb{R}$ एक प्राँत नहीं है।

$\{0\}$ तुच्छ है, और इसीलिए, यह एक प्राँत नहीं है।

उदाहरण 6 की ही तरह, $(\mathbb{Z}\times\mathbb{Z})/(\mathbb{Z}\times\{0\}) \simeq \mathbb{Z}$, जो एक पूर्णांकीय प्राँत है।

अतः, $(\mathbb{Z}\times\mathbb{Z})/(\mathbb{Z}\times\{0\})$ एक प्राँत है।

E7) नहीं, उदाहरणार्थ आप देख चुके हैं कि $2\mathbb{Z}$ एक प्राँत नहीं है, हालांकि $\mathbb{Z}$ प्राँत।

विभाग वलय का एक प्राँत होना आवश्यक नहीं है। उदाहरणार्थ, आप जानते हैं कि $\mathbb{Z}$ एक प्राँत है, परंतु $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}_6$ नहीं है।

E8) इकाई 10 से आप जानते हैं कि $\mathbb{Q}[\sqrt{n}]$ एक तत्समकी क्रमविनिमेय वलय है। क्योंकि $\mathbb{C}$ का $\mathbb{Q}[\sqrt{n}]$ एक उपवलय है, तथा $\mathbb{C}$ के कोई शून्य के भाजक नहीं हैं, इसलिए $\mathbb{Q}[\sqrt{n}]$ में कोई शून्य के भाजक नहीं हैं। अतः, यह एक प्राँत है।

E9) ध्यान दीजिए कि $\mathbb{R}$ एक पूर्णांकीय प्राँत है। क्योंकि $\mathbb{Z}[\sqrt{7}]$, $\mathbb{R}$ का एक उपवलय है, इसलिए यह भी बिना शून्य के भाजकों का है। अतः, $\mathbb{Z}[\sqrt{7}]$ में गुणन के लिए निरसन नियम लागू होता है।

क्योंकि $\mathbb{Z}$ का $5\mathbb{Z}$ एक उपवलय है तथा $\mathbb{Z}$ में कोई शून्य के भाजक नहीं हैं, इसलिए $5\mathbb{Z}$ में भी ऐसा ही है।

अतः, $5\mathbb{Z}$ में निरसन नियम लागू होता है।

E10) $x^2 = x \Rightarrow x(x-1) = 0$

$\Rightarrow x = 0$ या $x - 1 = 0$

$\Rightarrow x = 0$ या $x = 1$.

E11) मान लीजिए R एक प्राँत है तथा $x \in R$ शून्यंभावी है।

तब, किसी $n \in \mathbb{N}$ के लिए, $x^n = 0$.

यदि $n = 1$, तो $x = 0$.

यदि $n > 1$, तो $x \cdot x^{n-1} = 0$.

क्योंकि R में कोई शून्य के भाजक नहीं हैं, इसलिए $x = 0$ या $x^{n-1} = 0$.

हम इसी तर्क का अनुप्रयोग बार-बार कर सकते हैं जब तक कि $x^2 = 0$ पर नहीं पहुँच जाएँ।

$\therefore x \cdot x = 0$, अर्थात्, $x = 0$.

E12) मान लीजिए $R = \{x_1, \ldots, x_n\}$.

मान लीजिए कि a शून्य का भाजक नहीं है।

अब, $ax_i \in R \;\forall\; i = 1, \ldots, n$.

साथ ही, क्योंकि a शून्य का भाजक नहीं है, इसलिए $ax_i = ax_j$ iff $x_i = x_j$, $i, j = 1, \ldots, n$ के लिए।

इस प्रकार, $R = \{ax_1, \ldots, ax_n\}$.

क्योंकि $1 \in R$, इसलिए किसी $i = 1, \ldots, n$ के लिए, $1 = ax_i$.

अतः, R में a एक मात्रक है।

E13) उदाहरणार्थ, $R = \mathbb{Q}$ पर विचार कीजिए। मान लीजिए कि $r = \text{char}\ \mathbb{Q}$.

तब, $r \cdot \frac{m}{n} = 0 \;\forall\; \frac{m}{n} \in \mathbb{Q}$.

विशेष रूप में, $r \cdot 1 = 0$, क्योंकि $1 \in \mathbb{Q}$.

यह तभी संभव है, जब $r = 0$.

E14) हम दर्शाएंगे कि $2A = \emptyset \;\forall\; A \subseteq X$, तथा कि 2 ऐसी लघुतम प्राकृतिक संख्या है।

पहले, किसी भी $A \subseteq X$ के लिए,

$2A = A \Delta A = (A \setminus A) \cup (A \setminus A) = \emptyset$.

साथ ही, क्योंकि $X \neq \emptyset$, इसलिए $1 \cdot X \neq \emptyset$. इस प्रकार, $\text{char}\ \wp(X) \neq 1$.

$\therefore \text{char}\ \wp(X) = 2$.

E15) मान लीजिए कि $\text{char}(R \times R) = n$.

हम जानते हैं कि $mr = 0 \;\forall\; r \in R$, तथा m ऐसा लघुतम ऋणेतर पूर्णांक है।

अब, मान लीजिए $R \times R$ का (r, s) कोई भी अवयव है।

तब, $m(r, s) = (mr, ms) = (0, 0)$, क्योंकि $r, s \in R$.

इस प्रकार, $n \leq m$. …(3)

दूसरी ओर, यदि $r \in R$, तो $(r, 0) \in R \times R$.

$\therefore n(r, 0) = (0, 0)$,

अर्थात्, $(nr, 0) = (0, 0)$,

अर्थात्, $nr = 0$.

यह किसी भी $r \in R$ के लिए सत्य है।

$\therefore\ m \le n.$ …(4)

इस प्रकार, (3) और (4) दर्शाते हैं कि $m = n$, अर्थात् $\text{char } R = \text{char } (R \times R)$.

E16) $(R, +)$ एक परिमित समूह है। यदि $o(R) = n$, तो r सभी $x \in R$ के लिए, r की कोटियों का ℓ.c.m है।

साथ ही, R में प्रत्येक x के लिए, n का $o(x)$ एक गुणनखंड है। इस प्रकार, $r \ne 0$.

E17) i) $(R, +)$ कोटि n वाला ऐसा समूह है s.t. $rx = 0\ \forall\ x \in R$, जहाँ $r = \text{char } R$.

E16 द्वारा, $r \ne 0$.

अतः, $o(x) | r\ \forall\ x \in R$, तथा r ऐसा लघुतम धनात्मक पूर्णांक है।

इसलिए, इकाई 4 से आप जानते हैं कि $r | n$.

ii) जब $R = \mathbb{M}_2(\mathbb{Z}_4)$, तब $n = 2^4$. अतः, $r = 2, 2^2, 2^3$ या 2^4.

वस्तुतः, $r = 4$ क्योंकि $4\begin{bmatrix} \bar{x}_1 & \bar{x}_2 \\ \bar{x}_3 & \bar{x}_4 \end{bmatrix} = \begin{bmatrix} 4\bar{x}_1 & 4\bar{x}_2 \\ 4\bar{x}_3 & 4\bar{x}_4 \end{bmatrix} = \mathbf{0}$, जहाँ $\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4 \in \mathbb{Z}_4$; और $2\begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix} = \begin{bmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix} \ne \mathbf{0}$.

iii) उदाहरणार्थ $\mathbb{Z}_n, n \in \mathbb{N}$. यहाँ $o(\mathbb{Z}_n, +) = n = \text{char } \mathbb{Z}_n$.

E18) यहाँ तत्समक है $I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & 0 \\ 0 & 0 & \dots & 1 \end{bmatrix} \in \mathbb{M}_n(\mathbb{C})$.

किसी भी $r \in \mathbb{N}$ के लिए, $r \cdot I = \begin{bmatrix} r & 0 & \dots & 0 \\ 0 & r & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & r \end{bmatrix} \ne \mathbf{0}$.

अतः, $\text{char } \mathbb{M}_n(\mathbb{C}) = 0$.

$\mathbb{M}_n(\mathbb{Z}_m)$ में तत्समक है $I = \begin{bmatrix} \overline{1} & \overline{0} & \dots & \overline{0} \\ \overline{0} & \overline{1} & \dots & \overline{0} \\ \vdots & \vdots & & \vdots \\ \overline{0} & \overline{0} & \dots & \overline{1} \end{bmatrix}$.

$\therefore mI = \begin{bmatrix} \overline{m} & \overline{0} & \dots & \overline{0} \\ \overline{0} & \overline{m} & \dots & \overline{0} \\ \vdots & \vdots & & \vdots \\ \overline{0} & \overline{0} & \dots & \overline{m} \end{bmatrix} = \mathbf{0},$ तथा m ऐसा लघुतम धनात्मक पूर्णांक है।

$\therefore$ char $\mathbb{M}_n(\mathbb{Z}_m) = m.$

E19) नहीं; उदाहरणार्थ, char $\mathbb{Z} = 0$ तथा char $(\mathbb{Z}/2\mathbb{Z}) = \text{char } \mathbb{Z}_2 = 2.$

E20) नहीं, उदाहरणार्थ, $\mathbb{Z} \subsetneq \mathbb{Q}$, परंतु char $\mathbb{Z}$ = char $\mathbb{Q} = 0.$

E21) मान लीजिए R का अभिलक्षणिक 1 है।

तब, किसी भी $r \in R$ के लिए, $1 \cdot r = 0$, अर्थात्, $r = 0.$

अतः, केवल तुच्छ वलय का अभिलक्षणिक 1 है।

E22) क्योंकि $R \simeq S$, इसलिए इनके एक समान ही बीजीय गुण हैं। अतः char R = char S. इसलिए char R − char S = 0.

E23) मान लीजिए D एक प्रांँत है। तब, char D या तो 0 है या एक अभाज्य संख्या है। अतः, E15 द्वारा, char $(D \times D)$ या तो 0 है या एक अभाज्य संख्या है।

परंतु, उदाहरण 4 से, $D \times D$ एक प्रांँत नहीं है।

इस प्रकार, प्रमेय 4 का विलोम सत्य नहीं है।

E24) i) द्विपर प्रसार द्वारा (इकाई 10 का E16 देखिए),

$(a+b)^p = a^p + {}^pC_1\, a^{p-1}b + \dots + {}^pC_{p-1}\, ab^{p-1} + b^p.$

क्योंकि $p \mid {}^pC_n \ \forall\, n = 1, \dots, p-1$, ${}^pC_n x = 0 \ \forall\ x \in R$ तथा $\forall\ n = 1, \dots, p-1.$

इस प्रकार, ${}^pC_1 a^{p-1}b = 0 = \dots = {}^pC_{p-1}\, ab^{p-1}.$

$\therefore (a+b)^p = a^p + b^p.$

इसी प्रकार आप दर्शा सकते हैं कि $(a-b)^p = a^p - b^p$. यहाँ, ध्यान दीजिए कि अभिलक्षणिक 2 वाले वलय में, $(-1) = 1$, क्योंकि $2 = 0.$

ii) $(a+b)^{p^m} = a^{p^m} + b^{p^m}$, $a, b \in R$, $P(m)$ को विधेय लेते हुए, आपको इसे आगमन द्वारा सिद्ध करना चाहिए। $m \in \mathbb{N}$ के लिए।

(i) में आप सिद्ध कर चुके हैं कि $P(1)$ सत्य है। अब, मान लीजिए कि किसी $k \in \mathbb{N}$ के लिए $P(k)$ सत्य है, और फिर सिद्ध कीजिए कि $P(k+1)$ सत्य है।

तब, $\forall\ n \in \mathbb{N}$, $P(n)$ सत्य होगा।

iii) मान लीजिए $S = \{a^p \mid a \in R\}$.

पहले तो, $S \neq \emptyset$, क्योंकि $R \neq \emptyset$.

दूसरे, मान लीजिए कि $\alpha, \beta \in S$. तब, किन्हीं $a, b \in R$ के लिए, $\alpha = a^p$, $\beta = b^p$.

तब, $\alpha - \beta = (a-b)^p \in S$, उपरोक्त (i) द्वारा,

तथा $\alpha\beta = (ab)^p \in S$.

इस प्रकार, R का S एक उपवलय है।

iv) पहले, आपको इसकी जाँच करनी चाहिए कि ϕ सुपरिभाषित है।

आगे, $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$, तथा

$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$.

इस प्रकार, ϕ एक वलय समाकारिता है।

ϕ एकैकी है, क्योंकि

$\phi(a) = \phi(b) \Rightarrow a^p = b^p \Rightarrow (a-b)^p = 0$, (i) से।

$\Rightarrow a - b = 0$, क्योंकि R बिना शून्य के भाजक वाला है।

$\Rightarrow a = b$.

v) हमें दर्शाना है कि यदि R परिमित है, तो ϕ आच्छादक है।

मान लीजिए R में n अवयव हैं। क्योंकि ϕ एकैकी है, इसलिए $\text{Im}\ \phi$ में भी n अवयव हैं।

साथ ही, $\text{Im}\ \phi \subseteq R$. इस प्रकार, $\text{Im}\ \phi = R$.

अतः, ϕ आच्छादक है।

E25) यह दर्शाते समय कि कोई भी कथन सत्य नहीं है, आपको इन तथ्यों का उपयोग करने की आवश्यकता है कि 0^0 परिभाषित नहीं है (पाठ्यक्रम 'कलन' को देखिए) तथा $a^0 = 1 \ \forall \ a \in R, \ a \neq 0$ (क्योंकि R एक प्रांत है)।

E26) $\mathbb{Z}_6$, और $\overline{2}, \overline{3} \in \mathbb{Z}_6$ लीजिए।

अब, $\overline{2}^6 = \overline{4}$ तथा $\overline{4}^6 = \overline{4}$.

अतः, $\overline{2}^6 + \overline{4}^6 = \overline{8} = \overline{2}$, $\mathbb{Z}_6$ में।

साथ ही, $(\overline{2} + \overline{4})^6 = \overline{0}^6 = \overline{0}$.

इस प्रकार, $(\overline{2} + \overline{4})^6 \neq \overline{2}^6 + \overline{4}^6$.

E27) आपको इसकी जाँच करनी चाहिए कि f एक सुपरिभाषित फलन है।

आगे, $m, n \in \mathbb{Z}$ के लिए,

$f(m+n) = (m+n) \cdot 1$

$= m \cdot 1 + n \cdot 1$, भाग 10.3, इकाई 10 के LI 2(i) से।

$= f(m) + f(n)$.

साथ ही, $f(mn) = (mn) \cdot 1 = (mn)(1 \cdot 1) = (m \cdot 1)(n \cdot 1)$, LI 2(v) से।

अतः, f एक वलय समाकारिता है।

$\text{Ker } f = \{n \in \mathbb{Z} \mid n \cdot 1 = 0\}$, $\mathbb{Z}$ की गुणजावली है।

अतः, किसी $\text{Ker } f = r\mathbb{Z}, \ r \in \mathbb{Z}$ के लिए जहाँ $r \cdot 1 = 0$.

क्योंकि char $R = m, \ m \cdot 1 = 0$.

अतः, $m\mathbb{Z} \subseteq r\mathbb{Z}$, अर्थात्, $r \mid m$.

परंतु $m = \text{char } R$. अतः, $r \geq m$.

इस प्रकार, $r = m$, अर्थात्, $\text{Ker } f = m\mathbb{Z}$.

E28) दिखाइए कि $\text{char } (\mathbb{Z}_3 \times \mathbb{Z}_4) = 12$.

इस प्रकार, $\mathbb{Z}_3 \times \mathbb{Z}_4$ का अभिलक्षणिक न तो शून्य है और न ही एक अभाज्य संख्या। ध्यान दीजिए कि $\mathbb{Z}_3 \times \mathbb{Z}_4$ एक प्रांत नहीं है, जैसा कि आप उदाहरण 4 में देख चुके हैं।

E29) $6\mathbb{Z}$ नहीं है, क्योंकि $6\mathbb{Z}$ का कोई तत्समक नहीं है।

$\mathbb{Z}_6$ नहीं है, क्योंकि यह एक प्रांत नहीं है।

$\mathbb{Z}[\sqrt{2}]$ नहीं है, क्योंकि इसमें प्रत्येक शून्येतर अवयव व्युत्क्रमणीय नहीं है।

$\mathbb{Q}\times\mathbb{Q}$ नहीं है, क्योंकि यह प्राँत नहीं है।

$\mathbb{Z}_5$ एक क्षेत्र है, क्योंकि प्रमेय 1 द्वारा यह एक प्राँत है तथा $(\mathbb{Z}_5^*, \cdot)$ एक समूह है।

$\wp(\{a\}) = \{\emptyset, \{a\}\}$ एक क्षेत्र है, क्योंकि यह $R1 - R9$ को संतुष्ट करता है (देखिए E4)।

E30) नहीं। उदाहरणार्थ, $\mathbb{Q}$ का $\mathbb{Z}$ एक उपवलय है और $\mathbb{Q}$ एक क्षेत्र है, परंतु $\mathbb{Z}$ क्षेत्र नहीं है।

E31) इकाई 10 से आप जानते हैं कि $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\} \neq (\mathbb{Z}[i])^*$.

अतः, $\mathbb{Z}[i]$ एक क्षेत्र नहीं है।

$\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$ एक तत्समकी क्रमविनिमेय वलय है। क्या इसमें प्रत्येक शून्येतर अवयव का एक गुणनात्मक प्रतिलोम है? उदाहरण 11 की ही तरह इसकी जाँच कीजिए।

E32) ध्यान दीजिए कि $\overline{x} = x + \mathbb{Z}[x] \neq \overline{0}$, क्योंकि $x \notin < x^2 >$. (क्यों?)

परंतु, $\overline{x} \cdot \overline{x} = \overline{x^2} = \overline{0}$.

अतः, $\mathbb{Z}[x]/< x^2 >$ एक प्राँत नहीं है।

इस प्रकार, प्रमेय 5 द्वारा, यह एक क्षेत्र नहीं है।

E33) सारणियों से आप देख सकते हैं कि R पर $+$ और $\cdot$ द्वि-आधारी संक्रियाएँ हैं। साथ ही, R इकाई 10 में दिए $R1 - R6$ को संतुष्ट करता है।

आगे, R एक तत्समकी क्रमविनिमेय वलय है तथा इसके प्रत्येक शून्येतर अवयव का एक प्रतिलोम है, अर्थात् $R7 - R9$ को R संतुष्ट करता है।

इस प्रकार, R एक क्षेत्र है।

यहाँ, $2x = 0 \ \forall \ x \in R$ तथा किसी $x \in R$ के लिए (जैसे $x = 1$), $1 \cdot x \neq 0$.

इस प्रकार, char $R = 2$.

E34) $\text{Ker } f$, F की गुणजावली है। इस प्रकार, प्रमेय 9 द्वारा,

$\text{Ker } f = \{0\}$ या $\text{Ker } f = F$.

यदि $\text{Ker } f = \{0\}$, तो f एकैकी है।

यदि $\text{Ker } f = F$, तो $f = \mathbf{0}$.

E35) i) यह आवश्यक नहीं है। उदाहरणार्थ, निम्नलिखित पर विचार कीजिए :

$$\pi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} : \pi(m) = \begin{cases} \bar{0}, \text{ यदि } m \text{ सम है,} \\ \bar{1}, \text{ यदि } m \text{ विषम है ।} \end{cases}$$

जाँच कीजिए कि π एक वलय समाकारिता है, जो 1-1 नहीं है।

आप यह भी जानते हैं कि $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$, जो एक क्षेत्र है।

ii) $\mathbb{Q}$ से $\mathbb{R}$ तक आविष्टि समाकारिता पर विचार कीजिए।

यह न तो **0** है, और न ही आच्छादक है।

E36) क्योंकि $R \simeq F$, तथा तुल्याकारी वलयों के पूरी तरह समान बीजीय गुण होते हैं, इसलिए R एक क्षेत्र है।

E37) आपको इन सभी गुणों को, R के संगत गुणों का उपयोग करते हुए, सिद्ध करना चाहिए। $\mathbb{Q}$ को दिमाग में रखने से शायद आपको सहायता मिले।

E38) पहले, E29 से आप जानते हैं कि $\mathbb{Z}[\sqrt{2}]$ एक क्षेत्र नहीं है। इस प्रकार, यह स्वयं अपना विभाग क्षेत्र नहीं हो सकता है।

आगे, $\mathbb{Z}[\sqrt{2}]$ के विभाग क्षेत्र का कोई भी अवयव $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$ के रूप का है, जहाँ $c + d\sqrt{2} \neq 0$ तथा $a, b, c, d \in \mathbb{Z}$.

अब,

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{(a+b\sqrt{2})\,(c-d\sqrt{2})}{c^2-2d^2} = \left(\frac{ac-2bd}{c^2-2d^2}\right) + \sqrt{2}\left(\frac{bc-ad}{c^2-2d^2}\right) \in \mathbb{Q} + \sqrt{2}\mathbb{Q}.$$

इस प्रकार, $F \subseteq \mathbb{Q} + \sqrt{2}\mathbb{Q}$.

ध्यान दीजिए कि $\mathbb{Q} + \sqrt{2}\mathbb{Q}$ एक क्षेत्र है, जैसा कि आपने उदाहरण 11 में देखा था।

साथ ही, $\mathbb{Q} + \sqrt{2}\mathbb{Q}$ का कोई भी अवयव $\frac{a}{b} + \sqrt{2}\,\frac{c}{d}$, $a, b, c, d \in \mathbb{Z}$, $b \neq 0$, $d \neq 0$ के रूप का होता है।

अब,, $\frac{a}{b} + \sqrt{2}\,\frac{c}{d} = \frac{ad + bc\sqrt{2}}{bd} = \frac{ad + bc\sqrt{2}}{bd + 0\sqrt{2}}$, और $ad, bc, bd \in \mathbb{Z}$, $bd \neq 0$.

इस प्रकार, $\frac{a}{b} + \sqrt{2}\,\frac{c}{d} \in F$.

अतः, $\mathbb{Q} + \sqrt{2}\mathbb{Q} \subseteq F$.

इस प्रकार, $F = \mathbb{Q} + \sqrt{2}\mathbb{Q}$.

ध्यान दीजिए कि $\mathbb{C} \supsetneq F$ (उदाहरणार्थ, $i \notin F$), तथा इसीलिए यह $\mathbb{Z}[\sqrt{2}]$ का विभाग क्षेत्र नहीं है।

इसी प्रकार, $\mathbb{Z}[\sqrt{2}]$ का $\mathbb{R}$ विभाग क्षेत्र नहीं है। (उदाहरणार्थ, $\sqrt{3} \in \mathbb{R}$, परंतु $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$. क्यों? आइए देखें।

मान लीजिए $\sqrt{3} \in \mathbb{Q}[\sqrt{2}]$.

तब, $\exists\ m \in \mathbb{Z}$ s.t. $m\sqrt{3} = a + b\sqrt{2}, a, b \in \mathbb{Z}$.

अतः, $3m^2 = a^2 + 2b^2 + 2ab\sqrt{2}$.

इसलिए, $a^2 + 2b^2 = 3m^2$ तथा $2ab = 0$. अतः, $a = 0$ या $b = 0$.

यदि $a = 0, m\sqrt{3} = b\sqrt{2} \Rightarrow m\sqrt{6} \in \mathbb{Z}$, जो एक अंतर्विरोध है।

इसी प्रकार, $b = 0$ से भी एक अंतर्विरोध तक पहुँचते हैं।)

E39) यदि R एक प्रांत नहीं है, तो संबंध ~ को संक्रामक होना ज़रूरी नहीं है, तथा इसी कारण से F परिभाषित नहीं है।

E40) मान लीजिए R एक तत्समकी क्रमविनिमेय वलय है। मान लीजिए कि यह एक क्षेत्र F में अंतःस्थापित है। तब, F बिना शून्य के भाजक वाला है, तथा F का R एक उपवलय है।

इस प्रकार, R को बिना शून्य के भाजकों वाला होना चाहिए। अर्थात्, R को एक प्रांत होना चाहिए।

E41) पहले, $C[0, 1]$ की I एक गुणजावली है, जैसा कि आप इकाई 12 से जानते हैं।

दूसरे, क्योंकि कोई भी शून्येतर अचर फलन (उदाहरणार्थ, फलन $h : [0, 1] \to \mathbb{R} : h(x) = 1$) $C[0, 1] \setminus I$ में है, इसलिए I एक उचित गुणजावली है।

अंत में, मान लीजिए $fg \in I$, जहाँ $f, g \in C[0, 1]$.

तब, $(fg)(0) = 0$, अर्थात् $\mathbb{R}$ में $f(0) \cdot g(0) = 0$.

इसलिए $f(0) = 0$ या $g(0) = 0$, क्योंकि $\mathbb{R}$ एक प्रांत, अर्थात् $f \in I$ या $g \in I$.

इस प्रकार, $C[0, 1]$ की I एक अभाज्य गुणजावली है।

E42) R एक तत्समकी क्रमविनिमेय वलय है। इस प्रकार, हमें यह दर्शाने की आवश्यकता है R बिना शून्य के भाजक वाला है यदि और केवल यदि R में $\{0\}$ एक अभाज्य गुणजावली है।

अब, R में $\{0\}$ एक अभाज्य गुणजावली है,

iff $ab \in \{0\} \Rightarrow a \in \{0\}$ या $b \in \{0\}$, $a, b \in R$ के लिए

iff $ab = 0 \Rightarrow a = 0$ या $b = 0$

iff R बिना शून्य के भाजक वाला है।

इस प्रकार, R में $\{0\}$ एक अभाज्य गुणजावली है iff R एक पूर्णांकीय प्रांँत है।

E43) क्योंकि $\mathbb{C}$ एक क्षेत्र है, इसलिए इसकी गुणजावलियाँ केवल $\{0\}$ और $\mathbb{C}$ हैं। क्योंकि $\mathbb{C}$ एक प्रांँत है, इसलिए E42 द्वारा, $\mathbb{C}$ की $\{0\}$ एक अभाज्य गुणजावली है। इस तरह, केवल $\{0\}$ ही $\mathbb{C}$ की एक अभाज्य गुणजावली है।

E44) यह नहीं है। उदाहरणार्थ, $2 \cdot 3 \in < 6 >$.

अब, यदि $2 \in < 6 >$, तो $\exists\, a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ s.t. $6(a + b\sqrt{5}) = 2$, अर्थात् $6a = 2, b = 0$.

परंतु ऐसा कोई $a \in \mathbb{Z}$ नहीं है s.t. $6a = 2$. अतः $2 \notin < 6 >$.

इसी प्रकार, $3 \notin < 6 >$.

E45) उदाहरण 16 की ही तरह, सिद्ध कीजिए कि $\mathbb{Z}[x]\big/ < x + 20 > \simeq \mathbb{Z}$, जो एक प्रांँत है। अतः, $\mathbb{Z}[x]$ की $< x + 20 >$ एक अभाज्य गुणजावली है।

E46) नहीं। उदाहरणार्थ, $\mathbb{Z} \times \mathbb{Z}$ एक प्रांँत नहीं है, परंतु $(\mathbb{Z} \times \mathbb{Z})\big/(\mathbb{Z} \times \{0\}) \simeq \mathbb{Z}$, जो एक प्रांँत है। अतः, $(\mathbb{Z} \times \mathbb{Z})\big/(\mathbb{Z} \times \{0\})$ एक प्रांँत है।

E47) आप इसे उदाहरण 15 की ही तरह हल कर सकते हैं।

$\mathbb{Z}_{30}$ की अभाज्य गुणजावलियाँ $< \bar{p} >$ हैं, जहाँ $p \mid 30$ और p अभाज्य है। इस प्रकार, ये $\bar{2}\mathbb{Z}_{30}, < \bar{3} >$ और $< \bar{5} >$ हैं।

E48) i) इकाई 13 के प्रमेय 4 से आप जानते हैं कि R की $f^{-1}(J)$ एक गुणजावली है। क्योंकि f आच्छादक है तथा $J \neq S$, इसलिए $f^{-1}(J) \neq R$.

अब, मान लीजिए $a, b \in R$ s.t. $ab \in f^{-1}(J)$.

$\Rightarrow f(ab) \in J$

$\Rightarrow f(a)\, f(b) \in J$

$\Rightarrow f(a) \in J$ या $f(b) \in J$, क्योंकि J एक अभाज्य गुणजावली है।

$\Rightarrow a \in f^{-1}(J)$ या $b \in f^{-1}(J)$.

इस प्रकार, R की $f^{-1}(J)$ एक अभाज्य गुणजावली है।

ii) पहले, क्योंकि f आच्छादक है, इसलिए आप जानते हैं कि S की $f(I)$ एक गुणजावली है। (इकाई 13 के प्रमेय 4 से)

साथ ही, क्योंकि $1 \notin I$ तथा $f^{-1}(f(I)) = I$ (इकाई 13 प्रमेय 5 से, क्योंकि $I \supseteq N$), इसलिए $f(1) \notin f(I)$. इस प्रकार, $f(I) \neq S$.

अंत में, मान लीजिए $x, y \in S$ s.t. $xy \in f(I)$.

क्योंकि $S = \text{Im } f$, इसलिए $\exists\, a, b \in R$ s.t. $x = f(a)$ और $y = f(b)$.

तब, $f(ab) = f(a)f(b) = xy \in f(I)$, अर्थात्, $ab \in f^{-1}(f(I)) = I$.

$\therefore a \in I$ या $b \in I$, क्योंकि I एक अभाज्य गुणजावली है।

अतः, $x \in f(I)$ या $y \in f(I)$.

इस प्रकार, S की $f(I)$ एक अभाज्य गुणजावली है।

iii) **ϕ एकैकी है:** $\phi(I) = \phi(J)$

$\Rightarrow f(I) = f(J)$

$\Rightarrow f^{-1}(f(I)) = f^{-1}(f(J))$

$\Rightarrow I = J$, क्योंकि I और J दोनों में N आविष्ट है।

ϕ आच्छादक है: मान लीजिए S की J एक अभाज्य गुणजावली है। तब, R की $f^{-1}(J)$ एक अभाज्य गुणजावली है तथा $\phi(f^{-1}(J)) = f(f^{-1}(J)) = J$ (इकाई 13 से)।

इस प्रकार, $J \in \text{Im } \phi$.

E49) आविष्टि फलन $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ और $P = 2\mathbb{Z}$ पर विचार कीजिए। तब, $\mathbb{Q}$ की $i(P) = 2\mathbb{Z}$ एक गुणजावली नहीं है, क्योंकि $\mathbb{Q}$ की गुणजावलियाँ केवल $\{0\}$ और $\mathbb{Q}$ हैं। इस तरह, $\mathbb{Q}$ की $2\mathbb{Z}$ एक अभाज्य गुणजावली नहीं है।

E50) i) मान लीजिए P_1 और P_2 वलय R की अभाज्य गुणजावलियाँ हैं s.t. $\exists\, x \in P_1 \setminus P_2$ तथा $y \in P_2 \setminus P_1$.

तब, $xy \in P_1$ और $xy \in P_2$, क्योंकि P_1 और P_2 गुणजावलियाँ हैं।

$\therefore xy \in P_1 \cap P_2$.

परंतु $x \notin P_1 \cap P_2$ तथा $y \notin P_1 \cap P_2$.

इस प्रकार, $P_1 \cap P_2$ अभाज्य नहीं है।

ii) नहीं। उदाहरणार्थ, $2\mathbb{Z}+3\mathbb{Z}=\mathbb{Z}$, क्योंकि $(2, 3)=1$. यहाँ $\mathbb{Z}$ की $2\mathbb{Z}$ और $3\mathbb{Z}$ अभाज्य गुणजावलियाँ हैं, परंतु $\mathbb{Z}$ में $\mathbb{Z}$ अभाज्य नहीं है। (क्यों?)

iii) नहीं। उदाहरणार्थ, $(2\mathbb{Z})(3\mathbb{Z})=6\mathbb{Z}$, जो $\mathbb{Z}$ में अभाज्य नहीं है।

E51) जैसा कि आप इकाई 12 से जानते हैं, $m\mathbb{Z}\times n\mathbb{Z}$, is an ideal of $\mathbb{Z}\times\mathbb{Z}$ की गुणजावली है, जहाँ $m, n\in\mathbb{Z}$.

अब, $\mathbb{Z}\times\mathbb{Z}/(m\mathbb{Z}\times n\mathbb{Z})\simeq\mathbb{Z}_m\times\mathbb{Z}_n$, जो एक प्राँत केवल तब होगा जब ($m=1$ और n एक अभाज्य है या $n=0$) या जब ($n=1$ और m एक अभाज्य है या $m=0$)।

अतः, $\mathbb{Z}\times 2\mathbb{Z}$ और $\mathbb{Z}\times 3\mathbb{Z}$, $\mathbb{Z}\times\mathbb{Z}$ के दो अभाज्य गुणजावलियाँ हैं।

ध्यान दीजिए कि ये अलग हैं क्योंकि उदाहरणार्थ, $(1, 2)\in\mathbb{Z}\times 2\mathbb{Z}$ लेकिन $(1, 2)\notin\mathbb{Z}\times 3\mathbb{Z}$.

E52) R में M उच्चिष्ठ है

$\Rightarrow R/M$ एक क्षेत्र है, प्रमेय 14 द्वारा।

$\Rightarrow R/M$ एक प्राँत है, प्रमेय 5 द्वारा।

$\Rightarrow R$ में M अभाज्य है, प्रमेय 12 द्वारा।

E53) $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}=\bar{2}\mathbb{Z}_{10}$ तथा $\mathbb{Z}_{10}/\bar{2}\mathbb{Z}_{10}\simeq\mathbb{Z}_2$, एक क्षेत्र।

इस प्रकार, $\mathbb{Z}_{10}$ में $\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\}$ उच्चिष्ठ है।

E54) उदाहरण 16 की ही तरह, दर्शाइए कि $\mathbb{C}[x]/<x-\pi>\simeq\mathbb{C}$, एक क्षेत्र।

अतः, $\mathbb{C}[x]$ में $<x-\pi>$ उच्चिष्ठ है।

E55) इकाई 13 में आप देख चुके हैं कि यह गुणजावली आच्छादक समाकारिता $\phi: C[0, 1]\to\mathbb{R}:\phi(f)=f\left(\frac{1}{2}\right)$ की अष्टि है।

$\therefore C[0,1]/\text{Ker}\,\phi\simeq\mathbb{R}$, एक क्षेत्र।

इस प्रकार, $C[0,1]$ में $\text{Ker}\,\phi$ उच्चिष्ठ है।

इकाई 15

बहुपद वलय

इकाई की रूपरेखा **पृष्ठ संख्या**

15.1 प्रस्तावना

अभी तक आपने अनेक वलयों के बारे में अध्ययन किया है। इनमें विशिष्ट गुणों वाले वलय भी शामिल हैं आपने 'कलन' के खंड 1 में $\mathbb{R}$ पर बहुपदों के बारे में भी कुछ विस्तार से अध्ययन किया है। इस पाठ्यक्रम की पिछली इकाइयों में आपने बहुपदों के विभिन्न वलयों से संबंधित अनेक उदाहरणों का अध्ययन किया था। इस इकाई में हमारा उद्देश्य है बहुपदों के आपके पिछले सभी अध्ययनों को एकत्रित करना और उन्हें कुछ और आगे ले जाना।

भाग 15.2 में आप उन समुच्चयों के बारे में अध्ययन करेंगे, जिनके अवयव $a_0+a_1x+\cdots+a_nx^n$ प्रकार के बहुपद हैं, जहाँ $a_0, a_1, \ldots, a_n$ किसी वलय R के अवयव हैं। आप देखेंगे कि यह समुच्चय, जिसे $R[x]$ द्वारा व्यक्त किया जाता है, भी एक वलय है।

भाग 15.3 में आप देखेंगे कि हम बहुपद वलयों की चर्चा प्राँतों और क्षेत्रों के खंड में क्यों कर रहे हैं। इस संबंध में आप $R[x]$ के अनेक गुणों का अध्ययन करेंगे। विशेष रूप में आप देखेंगे कि यदि R एक पूर्णांकीय प्राँत है, तो $R[x]$ भी एक पूर्णांकीय प्राँत होता है।

चर्चा को आगे ले जाते हुए, भाग 15.4 में आप देखेंगे कि किसी क्षेत्र पर बहुपदों का वलय कुछ हद तक $\mathbb{Z}$ की तरह है। यह एक ऐसे विभाजन ऐल्गोरिद्म को संतुष्ट करता है जो $\mathbb{Z}$ द्वारा संतुष्ट ऐल्गोरिद्म (इकाई 1 देखिए) की तरह है। हम इस गुण को, और उससे निकलने वाले कुछ परिणामों को, इस भाग में सिद्ध करेंगे।

अगले भाग, भाग 15.5 में, $F[x]$ की गुणजावलियों पर केन्द्रित होगा, जहाँ F एक क्षेत्र है। आप सीखेंगे कि क्यों $F[x]$ में प्रत्येक गुणजावली एक मुख्य गुणजावली होती है, जैसा कि $\mathbb{Z}$ में होता है। आप यह भी देखेंगे कि यह तथ्य इतना महत्वपूर्ण क्यों है।

अगली इकाई में हम बहुपदों पर अपनी चर्चा को जारी रखेंगे। इस इकाई में, और अगली इकाई में, जो आप अध्ययन करेंगे वह गणित की किसी भी शाखा में आपके अध्ययन के लिए बहुत ही मौलिक है। अतः, इस इकाई का ध्यानपूर्वक अध्ययन कीजिए। जैसे-जैसे आप किसी प्रश्न पर पहुंचे, वैसे-वैसे ही उसे हल करें। इससे आपको यह सुनिश्चित करने में सहायता मिलेगी कि आपने इस इकाई की निम्नलिखित सीखने की अपेक्षाओं को प्राप्त कर लिए हैं।

उद्देश्य

इस इकाई की पढ़ाई के बाद, आप निम्नलिखित करने में समर्थ हो जाएंगे:

- दिए हुए वलय पर बहुपदों को परिभाषित करना, तथा उनके उदाहरण देना;
- एक क्रमविनिमेय वलय R पर बहुपदों का समुच्चय वलय $(R[x], +, \cdot)$ होता है, इस परिणाम को सिद्ध करना और उसका उपयोग करना;
- $R[x]$ के कुछ गुणों को R के गुणों से जोड़ना;
- $F[x]$ के लिए विभाजन ऐल्गोरिद्म को सिद्ध करना, और उसका अनुप्रयोग करना, जहाँ F एक क्षेत्र है;
- क्षेत्र F के लिए, $F[x]$ में प्रत्येक गुणजावली एक मुख्य गुणजावली होती है इस परिणाम को सिद्ध करना और उसका अनुप्रयोग करना।

15.2 बहुपदों का वलय

आप $1+x,\ 2+3x+4x^2,\ x^5-1,\ 0,$ इत्यादि, जैसे अनेक बहुपदों को देख चुके हैं। ये $\mathbb{R}$ पर बहुपदों के उदाहरण हैं, क्योंकि इनके गुणांक $\mathbb{R}$ में हैं। परंतु ये $\mathbb{Z}$ पर भी बहुपद हैं, क्योंकि इनके गुणांक $\mathbb{Z}$ में हैं। क्या इस संक्षिप्त चर्चा से आपको कुछ संकेत मिलता है कि किसी भी वलय R पर एक बहुपद क्या होता है? आइए इस वस्तु को, तथा इससे संबंधित कुछ शब्दों को, परिभाषित करें।

परिभाषाएँ: मान लीजिए R एक वलय है तथा x एक **अनिर्धार्य (indeterminate)** है।

एक 'अनिर्धार्थ' एक औपचारिक प्रतीक है। यह एक चर **नहीं** है।

i) x में **R पर एक बहुपद** $a_0x^0+a_1x^1+a_2x^2+\cdots+a_nx^n$ के रूप का व्यंजक है, जहाँ n ऋणेतर पूर्णांक है तथा $a_0, a_1, \ldots, a_n \in R$.

ii) $i = 0, 1, \ldots, n$ के लिए, a_ix^i उपरोक्त (i) में दिए बहुपद का पद **(term)** कहलाता है। यदि $a_0 \neq 0$, तो a_0x^0 इस बहुपद का **अचर पद (constant term)** कहलाता है।

iii) $a_0, a_1, \ldots, a_n$ उपरोक्त (i) में दिए बहुपद के **गुणांक (coefficients)** कहलाते हैं। यदि $a_n \neq 0$, तो a_n इस बहुपद का **अग्रग गुणांक** (**leading coefficient**) कहलाता है, तथा n इस बहुपद की **घात (degree)** कहलाती है। हम इस तथ्य को **deg** $(\mathbf{a_0x^0+\cdots+a_nx^n}) = \mathbf{n}$ से दर्शाते हैं।

iv) यदि $a_0 \neq 0$, तो बहुपद a_0x^0 एक **अचर बहुपद (constant polynomial)** कहलाता है।

v) यदि $a_i = 0 \ \forall\ i = 0, 1, \ldots, n$, तो प्राप्त बहुपद 0 है, जिसे **शून्य बहुपद (zero polynomial)** कहते हैं। परिभाषा से ही **इसमें कोई अग्रग गुणांक नहीं होता है।** साथ ही, **शून्य बहुपद की घात परिभाषित नहीं है।**

उदाहरणार्थ, किसी भी वलय R तथा किसी भी $r \in R$ के लिए, rx^0 एक अचर बहुपद है (यदि $r \neq 0$) या शून्य बहुपद है (यदि $r = 0$).

ध्यान दीजिए कि बहुपदों को लिखते समय हम **निम्नलिखित प्रथाओं** का अनुपालन करेंगे:

i) हम x^0 नहीं लिखेंगे। अतः, हम a_0x^0 के लिए a_0 ही लिखेंगे।

ii) हम x^1 को x लिखेंगे।

iii) हम $1 \cdot x^m$ के स्थान पर x^m लिखेंगे (अर्थात् जब $a_m = 1$), तथा यदि $a_m = (-a) \in R$, तो $-ax^m$ लिखेंगे।

iv) हम $0 \cdot x^m$ जैसे पदों को नहीं लिखेंगे।

इस प्रकार, $\mathbb{Z}$ पर बहुपद $2x^0 + 0 \cdot x^1 + 3x^2 + (-1)x^3$ को $2 + 3x^2 - x^3$ लिखा जाएगा, जिसमें (-1) इसका अग्रम गुणांक है तथा 2 इसका अचर पद है।

उदाहरण के तौर पर, $\mathbb{R}$ पर $\frac{1}{2} - \pi x^5 + \sqrt{2}x^{11}$ एक बहुपद है, जहाँ

$a_0 = \frac{1}{2}, a_5 = -\pi, a^{11} = \sqrt{2},$ तथा $i = 1, \ldots, 10, i \neq 5$ के लिए, $a_i = 0.$

इसी प्रकार, $\mathbb{R}$ पर $-\frac{1}{2} + \pi x^5 - \sqrt{2}x^{11}$ एक बहुपद है।

साथ ही, $A = \begin{bmatrix} 2 & 1 \\ -0.5 & \pi \end{bmatrix}$ और $B = \begin{bmatrix} \sqrt{3} & 0 \\ \sqrt{2} & 3 \end{bmatrix}$ के लिए, $Ax + Bx^4$, $\mathbb{M}_2(\mathbb{R})$ पर घात 4 वाला एक बहुपद है, जिसमें B इसका अग्रग गुणांक है तथा इसका कोई अचर पद नहीं है।

आइंदा, **जब भी हम शब्द 'बहुपद' का उपयोग करेंगे, तब हमारा तात्पर्य अनिर्धार्य x में एक बहुपद से होगा।** आगे, हम प्रायः बहुपद $a_0 + a_1x + \cdots + a_nx^n$ के लिए संक्षिप्त संकेत $\sum_{i=0}^{n} a_ix^i$ का उपयोग करेंगे।

याद कीजिए कि Σ यूनानी बड़ा अक्षर 'सिगमा' है, जो 'योग' को व्यक्त करता है।

अनिर्धार्य के उपयोग को स्पष्ट करने के लिए, यहाँ एक टिप्पणी है।

टिप्पणी 1: जैसा ऊपर बताया गया है, x को एक प्रतीक के रूप में उपयोग किया जाता है, जो अनिर्धार्य कहलाता है। प्रतीकों $x^0, x^1, x^2, \ldots$ को यहाँ क्रम में स्थान बताने का तरीक़ा सोचा जाना चाहिए। अतः, R पर बहुपद $a_0 + a_1x + \cdots + a_nx^n$ लिखने के स्थान पर, हम इसे एक अपरिमित अनुक्रम (sequence) के रूप में $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ लिख सकते थे ('वास्तविक विश्लेषण' से अनुक्रमों के अपने अध्ययन को याद कीजिए), जहाँ इस अनुक्रम में केवल परिमित संख्या में शून्येतर प्रविष्टियाँ हैं। इसी प्रकार, घात

m वाले एक बहुपद को $(b_0, b_1, \ldots, b_m, 0, 0, \ldots)$, $b_i \in R$, या $b_0 + b_1 x + \cdots + b_m x^m$ लिख सकते हैं।

ध्यान दीजिए कि $(0, 0, 2, 1, 5, 7, 9, 11, \ldots)$ एक बहुपद नहीं है, क्योंकि इसमें केवल परिमित संख्या में अनेक शून्येतर प्रविष्टियाँ नहीं हैं।

आइए x में बहुपदों के कुछ और उदाहरणों पर विचार करें।

i) $5 + 4x + 3x^2$ घात 2 वाला एक बहुपद है, जिसके गुणांक $\mathbb{Z}$ में हैं। इसका अग्रग गुणांक 3 है।

ii) $\overline{8} + \overline{6}x + x^2 + \overline{2}x^4$ घात 4 वाला एक बहुपद है, जिसके गुणांक $\mathbb{Z}_{10}$ में हैं। इसका अग्रग गुणांक $\overline{2}$ है।

और उदाहरण देने से पहले, हम कुछ और संकेतों को स्थापित करना चाहेंगे।

संकेतन: R[x] किसी **वलय R पर सभी बहुपदों के समुच्चय** को व्यक्त करेगा। (यहाँ वर्ग कोष्ठकों [ ] के उपयोग पर ध्यान दीजिए। अन्य प्रकार के किन्हीं कोष्ठकों का उपयोग नहीं करें, क्योंकि $R[x]$ और $R(x)$ अलग-अलग समुच्चयों को व्यक्त करते हैं, जैसा आप कुछ आगे जाकर देखेंगे।)

इस प्रकार, $R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in R \ \forall\ i = 0, 1, \ldots, n, \text{ जहाँ } n \geq 0, n \in \mathbb{Z} \right\}$.

हम प्रायः बहुपद $a_0 + a_1 x + \cdots + a_n x^n$ को $f(x), p(x), q(x)$, इत्यादि, द्वारा व्यक्त करेंगे।

इस प्रकार, $\mathbb{Z}_4[x]$ के एक अवयव का उदाहरण है $f(x) = \overline{1} + \overline{3}x + \overline{2}x^4$.

यहाँ $\deg f(x) = 4$ तथा $f(x)$ का अग्रग गुणांक $\overline{2}$ है।

आगे बढ़ने से पहले, आइए देखें कि दो बहुपद बराबर कब होते हैं। (पाठ्यक्रम 'वास्तविक विश्लेषण' से दो अनुक्रमों के बराबर होने के प्रतिबंध को याद कीजिए।)

परिभाषा: मान लीजिए R एक वलय है तथा $R[x]$ में $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ और $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ हैं। $f(x)$ और $g(x)$ **बराबर (equal)** कहलाते हैं यदि $a_i = b_i \ \forall\ i = 0, 1, \ldots, n.$ इसे $\mathbf{f(x) = g(x)}$ द्वारा व्यक्त किया जाता है।

इस प्रकार, यदि **दो बहुपद बराबर होते** हैं, तो उनके समान अग्रग गुणांक होते हैं, और इसी लिए इनकी **समान घात होती** हैं। क्या इसका विलोम सत्य है? नहीं। उदाहरणार्थ, $\mathbb{Z}[x]$ में दोनों $2x + 3x^4$ और $5 + 3x^4$ की घात 4 हैं, हालांकि ये बराबर नहीं हैं। इसका कारण यह है कि x^0 और x^1 के स्थानों में दोनों के संगत गुणांक अलग-अलग हैं।

अभी तक जो आपने अध्ययन किया है, उसे आप किस हद तक समझ गए हैं, इसे जाँचने के लिए निम्नलिखित प्रश्नों को हल कीजिए।

E1) निम्नलिखित व्यंजकों में से बहुपदों की पहचान कीजिए। इनमें से कौन-से $\mathbb{Z}[x]$ के अवयव हैं?

i) $1 + x + x^2 + x^4 + x^6$, ii) $\frac{2}{x^2} + \frac{1}{x} + x + x^2$,

iii) $\sqrt{2}x+\sqrt{3}x^2$, iv) $1+\frac{1}{2}x+\frac{1}{3}x^2+\frac{1}{4}x^3$,

v) $x^{1/2}+x+x^2$, vi) -5,

vii) $\sum_{i=0}^{\infty} ix^i$, viii) 0.

E2) यदि $\mathbb{R}[x]$ में $a_0+5x^2+\sqrt{3}x^3=\frac{1}{2}+b_1x+b_2x^2+b_3x^3+b_4x^{11}$, तो a_0, b_1, b_2, b_3, b_4 मालूम कीजिए।

E3) $\mathbb{R}[x]$ में निम्नलिखित में से प्रत्येक बहुपद की घात तथा अग्रग पद निर्धारित कीजिए।

i) $7+\sqrt{2}x$, ii) $1+3x-7x^3$, iii) $1+x^3+x^4+0\cdot x^5$,

iv) $\frac{1}{3}x+\frac{1}{5}x^2+\frac{1}{7}x^3$, v) 0.

अब किसी भी वलय R के लिए, आइए देखें कि $R[x]$ में योग और गुणन को किस प्रकार परिभाषित कर सकते हैं जिससे कि वे $R[x]$ पर सुपरिभाषित द्वि-आधारी संक्रियाएँ हो जाएँ। पहले बहुपदों के योग पर विचार कीजिए।

परिभाषा: मान लीजिए $f(x)=a_0+a_1x+\cdots+a_nx^n$ और $g(x)=b_0+b_1x+\cdots+b_mx^m$, $R[x]$ में हैं। मान लीजिए कि $m\geq n$. (ऐसी ही परिभाषा $n>m$ के लिए सत्य है।) तब, हम **R[x] में योग** को निम्नलिखित द्वारा परिभाषित करते हैं:

$$f(x)+g(x)=(a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n+b_{n+1}x^{n+1}+\cdots+b_mx^m$$

$$=\sum_{i=0}^{m}(a_i+b_i)x^i, \text{ जहाँ } i>n \text{ के लिए } a_i=0.$$

उदाहरणार्थ, $\mathbb{Z}[x]$ में $p(x)=1+2x+3x^2$, $q(x)=4+5x+7x^3$ द्वारा दिए जाने वाले दो बहुपदों $p(x), q(x)$ पर विचार कीजिए। तब,

$p(x)+q(x)=(1+4)+(2+5)x+(3+0)x^2+(0+7)x^3=5+7x+3x^2+7x^3$.

ध्यान दीजिए कि $p(x)+q(x)\in\mathbb{Z}[x]$, तथा इस स्थिति में

$\deg\,(p(x)+q(x))=3=\max\,(\deg p(x), \deg q(x))$.

ऊप दी हुई परिभाषा से ऐसा प्रतीत होता है कि

$\deg\,(f(x)+g(x))=\max\,(\deg f(x), \deg g(x))$. क्या यह सत्य है? आइए देखें।

$\mathbb{Z}[x]$ में, $p(x)=1+x^2$ और $q(x)=2+3x-x^2$ लीजिए।

तब, $p(x)+q(x)=(1+2)+(0+3)x+(1-1)x^2=3+3x$.

यहाँ, $\deg\,(p(x)+q(x))=1$; परंतु $\max(\deg p(x), \deg q(x))=\max(2, 2)=2$.

इस प्रकार, इस स्थिति में $\deg\,(p(x)+q(x))<\max(\deg p(x), \deg q(x))$.

अतः, जो हम कह सकते हैं, वह यह है कि

$\mathbf{deg\,(f(x)+g(x))\leq max\,(deg\,f(x), deg\,g(x))}$ $\forall\ f(x), g(x)\in R[x]$.

आइए अब $R[x]$ में गुणन को परिभाषित करें।

परिभाषा: मान लीजिए कि R एक वलय है। $R[x]$ में $f(x) = a_0 + a_1x + \cdots + a_nx^n$ तथा $g(x) = b_0 + b_1x + \cdots + b_mx^m$ के लिए, हम **R[x] में गुणन को** $f(x) \cdot g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}$, द्वारा परिभाषित करते हैं, जहाँ $c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_0b_i \; \forall \; i = 0, 1, \ldots, m+n.$
(यहाँ ध्यान दीजिए कि $i > n$ के लिए $a_i = 0,$ तथा $i > m$ के लिए $b_i = 0.$)

एक उदाहरण के रूप में, आइए $\mathbb{Z}[x]$ में निम्नलिखित बहुपदों का गुणा करें:
$p(x) = 1 - x + 2x^3,\; q(x) = 2 + 5x + 7x^2.$
यहाँ $m = 3, n = 2,$ इसलिए $m + n = 5.$ अब,
$a_0 = 1, a_1 = -1, a_2 = 0, a_3 = 2, a_4 = 0 = a_5,$
$b_0 = 2, b_1 = 5, b_2 = 7, b_3 = 0 = b_4 = b_5.$

इस प्रकार, $p(x) \cdot q(x) = \sum_{i=0}^{5} c_ix^i$, जहाँ

$c_0 = a_0b_0 = 2,$
$c_1 = a_1b_0 + a_0b_1 = 3,$
$c_2 = a_2b_0 + a_1b_1 + a_0b_2 = 2,$
$c_3 = a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 = -3,$
$c_4 = a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4 = 10,$
$c_5 = a_5b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 + a_0b_5 = 14.$
अतः, $p(x) \cdot q(x) = 2 + 3x + 2x^2 - 3x^3 + 10x^4 + 14x^5.$
ध्यान दीजिए कि $p(x) \cdot q(x) \in \mathbb{Z}[x]$, तथा
$\deg\,(p(x) \cdot q(x)) = 5 = (\deg\, p(x) + \deg\, q(x)).$

एक अन्य उदाहरण के रूप में, $p(x) = \overline{1} + \overline{2}x, q(x) = \overline{2} + \overline{3}x^2 \in \mathbb{Z}_6[x]$ पर विचार कीजिए।
तब, $p(x) \cdot q(x) = \overline{2} + \overline{4}x + \overline{3}x^2 + \overline{6}x^3 = \overline{2} + \overline{4}x + \overline{3}x^2$, क्योंकि $\overline{6} = \overline{0}.$
यहाँ, $\deg\,(p(x) \cdot q(x)) = 2 < (\deg\, p(x) + \deg\, q(x))$ (क्योंकि $\deg\, p(x) = 1,$ $\deg\, q(x) = 2$).

अतः, हम यह कह सकते हैं कि
$\mathbf{deg\,(f(x) \cdot g(x)) \leq deg\, f(x) + deg\, g(x)}$.

हमें इसकी जाँच करने की आवश्यकता है कि जिस तरह हमने $R[x]$ में योग और गुणन को परिभाषित किया है, ये $R[x]$ में संवृत हैं। पहले, आइए देखें कि क्या + सुपरिभाषित है। यदि

$f(x) = \sum_{i=0}^{n} a_ix^i,\; f'(x) = \sum_{i=0}^{m} a'_ix^i,\; g(x) = \sum_{i=0}^{r} b_ix^i$ तथा $g'(x) = \sum_{i=0}^{s} b'_ix^i$, तथा $R[x]$ में हैं s.t. $f(x) = f'(x)$ और $g(x) = g'(x)$, तो
$n = m,\; r = s,\; a_i = a'_i,\; b_j = b'_j \;\forall\; i = 0, \ldots, n,\; j = 0, \ldots, r.$

अतः, $f(x) + g(x) = \sum_{i=0}^{\max(n,r)} (a_i + b_i)x^i = \sum_{i=0}^{\max(m,s)} (a'_i + b'_i)x^i = f'(x) + g'(x).$
इस प्रकार, + सुपरिभाषित है।

इसी प्रकार से आपको दर्शाना चाहिए कि गुणन सुपरिभाषित है।

शेष भाग के लिए, नीचे दिए E4 को कीजिए। साथ ही, नीचे दिए अन्य प्रश्न भी कीजिए। इन्हें करने से आप बहुपदों पर इन संक्रियाओं के आदी हो जाएंगे।

E4) स्पष्ट कीजिए कि $R[x]$ पर योग और गुणन द्वि-आधारी संक्रियाएँ क्यों हैं।

E5) निम्नलिखित परिकलित कीजिए:

i) $\mathbb{Z}[x]$ में $(2+3x^2+4x^3)+(5x+x^3)$,

ii) $\mathbb{Z}_7[x]$ में $(\bar{6}+\bar{2}x^2)+(\bar{1}-\bar{2}x+\bar{5}x^3)$,

iii) $\mathbb{Z}[x]$ में $(1+x)\cdot(1+2x+x^2)$,

iv) $\mathbb{Z}_3[x]$ में $(\bar{1}+x)\cdot(\bar{1}+\bar{2}x+x^2)$,

v) $\mathbb{Q}[x]$ में $(2+x+x^2)\cdot(5x+x^3)$.

E6) किसी भी वलय R के लिए, स्पष्ट कीजिए कि बहुपद $a_0+a_1x+\cdots+a_nx^n \in R[x]$ का प्रत्येक पद भी R पर बहुपद क्यों है। इस प्रकार, $\sum_{i=0}^{n} a_ix^i$, R पर n बहुपदों का योग है।

केवल एक पद वाले बहुपद को **एकपद (monomial)** कहते हैं।

अब तक आप बहुपदों के योग और गुणन के आदी हो गए होंगे। आप यह भी देख चुके हैं कि $R[x]$ पर $+$ और $\cdot$ द्वि-आधारी संक्रियाएँ हैं। अब प्रश्न यह है कि $(R[x], +, \cdot)$ एक वलय है या नहीं। आइए देखें।

प्रमेय 1: यदि R एक वलय है, तो $R[x]$ भी एक वलय होता है, जहाँ x एक अनिर्धार्य है।

उपपत्ति: हमें $(R[x], +, \cdot)$ के लिए अभिगृहीतों $R1 - R6$ (इकाई 10 के) जांचने की आवश्यकता है।

R1 (योग क्रमविनिमेय है): मान लीजिए $R[x]$ में $p(x)=a_0+a_1x+\cdots+a_nx^n$ और $q(x)=b_0+b_1x+\cdots+b_mx^m$.
तब, $p(x)+q(x)=c_0+c_1x+\cdots+c_tx^t$,
जहाँ $t=\max(m, n)$ और $c_i=a_i+b_i \;\forall\; i=0, 1, \ldots, t$.
इसी प्रकार, $q(x)+p(x)=d_0+d_1x+\cdots+d_sx^s$,
जहाँ $s=\max(n, m)=t$, और $d_i=b_i+a_i \;\forall\; i=0, 1, \ldots, t$.
क्योंकि R में योग क्रमविनिमेय है, इसलिए $c_i=d_i \;\forall\; i\geq 0$.
अतः, $p(x)+q(x)=q(x)+p(x)$.

R2 (योग साहचर्य है): R में योग की साहचर्यता का उपयोग करते हुए, आपको इसकी जाँच करनी चाहिए कि किन्हीं $p(x), q(x), s(x) \in R[x]$ के लिए,
$\{p(x)+q(x)\}+s(x)=p(x)+\{q(x)+s(x)\}$.

R3 (योज्य तत्समक): $R[x]$ में शून्य बहुपद योज्य तत्समक है। इसका कारण यह है कि किसी भी $p(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ के लिए,

$$0 + p(x) = (0 + a_0) + (0 + a_1)x + \cdots + (0 + a_n)x^n$$
$$= a_0 + a_1x + \cdots + a_nx^n$$
$$= p(x).$$

R4 (योज्य प्रतिलोम): $p(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ के लिए, बहुपद $q(x) = -p(x) = -a_0 - a_1x - \cdots - a_nx^n$ पर विचार कीजिए, जहाँ R में a_i का योज्य प्रतिलोम $-a_i$ है। तब,

$$p(x) + q(x) = (a_0 - a_0) + (a_1 - a_1)x + \cdots + (a_n - a_n)x^n$$
$$= 0 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^n$$
$$= 0.$$

अतः, $q(x)(= -p(x))$ ही $p(x)$ का योज्य प्रतिलोम है।

R5 (गुणन साहचर्य है): मान लीजिए कि $R[x]$ में $p(x) = a_0 + a_1x + \cdots + a_nx^n$, $q(x) = b_0 + b_1x + \cdots + b_mx^m$, तथा $t(x) = d_0 + d_1x + \cdots + d_rx^r$. तब,

$p(x) \cdot q(x) = c_0 + c_1x + \cdots + c_sx^s$, जहाँ $s = m + n$ तथा

$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k \ \forall \ k = 0, 1, ..., s.$

अतः,

$\{p(x) \cdot q(x)\} \cdot t(x) = e_0 + e_1x + \cdots + e_tx^t$,

जहाँ $t = s + r = m + n + r$, और

$$e_k = c_kd_0 + c_{k-1}d_1 + \cdots + c_0d_k$$
$$= (a_kb_0 + \cdots + a_0b_k)d_0 + (a_{k-1}b_0 + \cdots + a_0b_{k-1})d_1 + \cdots + a_0b_0d_k.$$

इसी प्रकार, आपको जाँच करनी चाहिए कि $p(x) \cdot \{q(x) \cdot t(x)\}$ में x^k का गुणांक (किसी भी $k \geq 0$ के लिए), है।

$a_kb_0d_0 + a_{k-1}(b_1d_0 + b_0d_1) + \cdots + a_0(b_kd_0 + b_{k-1}d_1 + \cdots + b_0d_k)$

$= e_k$, R में $+$ और $\cdot$ के गुणों के उपयोग से।

अतः, $\{p(x) \cdot q(x)\} \cdot t(x) = p(x) \cdot \{q(x) \cdot t(x)\}$.

R6 (गुणन योग पर बंटित है): मान लीजिए कि $R[x]$ में $p(x) = a_0 + a_1x + \cdots + a_nx^n$, $q(x) = b_0 + b_1x + \cdots + b_mx^m$ और $t(x) = d_0 + d_1x + \cdots + d_rx^r$. किसी भी $k \geq 0$ के लिए, $p(x) \cdot (q(x) + t(x))$ में x^k का गुणांक $c_k = a_k(b_0 + d_0) + a_{k-1}(b_1 + d_1) + \cdots + a_0(b_k + d_k)$ है।

साथ ही, $p(x) \cdot q(x) + p(x) \cdot t(x)$ में x^k का गुणांक है

$$(a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k) + (a_kd_0 + a_{k-1}d_1 + \cdots + a_0d_k)$$
$$= a_k(b_0 + d_0) + a_{k-1}(b_1 + d_1) + \cdots + a_0(b_k + d_k)$$
$$= c_k.$$

अतः, $p(x) \cdot \{q(x) + t(x)\} = p(x) \cdot q(x) + p(x) \cdot t(x)$.

इसी प्रकार, आप सिद्ध कर सकते हैं कि

$\{q(x) + t(x)\} \cdot p(x) = q(x) \cdot p(x) + t(x) \cdot p(x)$.

इस प्रकार, $R[x]$ एक वलय है। ■

प्रमेय 1 हमें बताता है कि बहुपद वलयों के जिन उदाहरणों के साथ आप पहले कार्य कर चुके हैं, उनके अलावा $C[0, 1][x]$, $(3\mathbb{Z})[x]$, $\mathbb{M}_n(\mathbb{Z})[x]$, $\mathbb{H}[x]$ भी वलय ही हैं।

साथ ही, ध्यान दीजिए कि क्योंकि $(R[x], +)$ आबेली है, तथा E6 का उपयोग करते हुए, हम पाते हैं कि $a_0+a_1x+\cdots+a_nx^n$ को $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, या $a_nx^n+a_0+a_{n-1}x^{n-1}+a_1x+\cdots$ लिख सकते हैं।
अतः, उदाहरणार्थ, $-\pi+5x+5x^3\in\mathbb{R}[x]$ और $5x-\pi+5x^3$, या $5x+5x^3-\pi$, बराबर हैं।

आइए $R[x]$ के एक विस्तृत उदाहरण पर विचार करें।

उदाहरण 1: क्या $\mathbb{Z}_6[x]$ परिमित है? क्यों?

हल: $\mathbb{Z}_6$ में 6 अवयव हैं।
$\mathbb{Z}_6[x]=\{a_0+a_1x+\cdots+a_nx^n \mid a_i\in\mathbb{Z}_6\ \forall\ i=0,1,\ldots,n,\ n\in\mathbb{N}\cup\{0\}\}$.
अतः, a_0 कोई भी मान, $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$, ले सकता है।
इसी प्रकार, प्रत्येक a_i इन 6 मानों में से कोई भी एक मान ले सकता है।
अतः, $\overline{0}$ शून्य बहुपद है, तथा यहाँ 5 अचर बहुपद हैं। अब, घात 1 वाले $6\times5=30$ बहुपद हैं, क्योंकि a_0 द्वारा 6 मान लिए जा सकते हैं, परंतु $a_1\neq\overline{0}$ (क्योंकि हम $\overline{0}$ पहले ही गिन चुके हैं), जिससे a_1 5 मान ले सकता है।
इसी प्रकार, $\mathbb{Z}_6$ पर घात 2 वाले $6\times6\times5$ बहुपद हैं, इत्यादि।
क्योंकि n अपरिमित मान ले सकता है, इसलिए $\mathbb{Z}_6$ पर अनंततः अनेक बहुपद हैं।

***

आगे बढ़ने से पहले, आइए बहुपदों से संबंधित कुछ सामान्यतः उपयोग किए जाने वाले शब्दों को परिभाषित करें। हो सकता है आप अपने पिछले अध्ययनों से इन शब्दों से पहले से ही परिचित हों।

परिभाषा: i) घात 1 वाला बहुपद एक **रैखिक (linear) बहुपद** कहलाता है।

ii) घात 2 वाला बहुपद एक **द्विघात (quadratic) बहुपद** कहलाता है।

iii) घात 3 वाला बहुपद एक **त्रिघात (cubic) बहुपद** कहलाता है।

iv) घात 4 वाला बहुपद एक **चतुर्घात (bi-quadratic,** या **quartic) बहुपद** कहलाता है।

v) अग्रग गुणांक 1 वाला बहुपद **एकगुणांकी (monic) बहुपद** कहलाता है।

अतः, उदाहरणार्थ $3+5x^3\in\mathbb{Z}[x]$ एक त्रिघात बहुपद है, तथा $\frac{3}{5}+x^3$, $\mathbb{Q}$ पर एक त्रिघात एकगुणांकी बहुपद है।

अब कुछ प्रश्नों को हल करने का प्रयास कीजिए।

E7) निम्नलिखित में से कौन-से कथन सत्य हैं? अपने उत्तरों के लिए कारण दीजिए।

i) $R[x]$ में दो रैखिक बहुपदों का गुणनफल एक रैखिक बहुपद हो सकता है, जहाँ R एक वलय है।

ii) $\mathbb{Q}[x]$ में दो द्विघात बहुपदों का गुणनफल एक चतुर्घात बहुपद होता है।

iii) $\mathbb{C}[x]$ में दो द्विघात बहुपदों का योग एक द्विघात बहुपद होता है।

iv) यदि $R[x]$ में $p(x)$ एक एकगुणांकी बहुपद है, जहाँ R एक तत्समकी वलय है, तो $p(x)+q(x)$ एकगुणांकी है $\forall\, q(x) \in R[x]$.

E8) पुष्टि करते हुए, $\mathbb{M}_2(\mathbb{C})[x]$ में धनात्मक घात के दो अलग-अलग अवयव दीजिए।

E9) जाँच कीजिए कि R

i) $R[x]$ का एक उपवलय है या नहीं,

ii) $R[x]$ की एक गुणजावली है या नहीं।

E10) $\mathbb{Z}_4[x]$ में सभी द्विघात पदों की सूची बनाइए।

E11) मान लीजिए कि R एक वलय है, तथा $n \in \mathbb{N}$ के लिए, $\wp_n = \{f(x) \in R[x] \mid \deg f(x) \le n\} \cup \{0\}$. जाँच कीजिए कि $\wp_n$, $R[x]$ का उपवलय है या नहीं।

E12) मान लीजिए कि R एक वलय है तथा

$$A = \left\{ \sum_{i=0}^{n} a_i x^i \in R[x] \,\middle|\, a_i = 0 \text{ यदि } i \text{ विषम है} \right\}.$$

क्या A, $R[x]$ का उपवलय है? क्यों, या क्यों नहीं?

ध्यान दीजिए कि इस भाग में हमने जिन परिभाषाओं और प्रमेयों की चर्चा की है, वे **किसी भी वलय** के लिए सत्य हैं। परंतु, जिस स्थिति में हम वास्तव में रूचि रखते हैं, वह है एक प्राँत R की। अगले भाग में, हमारी चर्चा इसी स्थिति की ओर आगे बढ़ेगी।

15.3 बहुपद वलयों के कुछ गुण

पिछले भाग का अध्ययन करते समय आपको $R[x]$ के कुछ गुणों का अनुमान हो गया होगा। जैसे कि उदाहरण 1 से शायद आपको अंदाजा हो गया होगा कि यदि R एक परिमित अतुच्छ वलय है तो $R[x]$ अपरिमित वलय होता है। क्या आपने वलय R पर संक्रियाओं तथा $R[x]$ पर संक्रियाओं के बीच निकट रिश्ते के बारे में भी सोचा है? निस्संदेह, प्रमेय 1 को सिद्ध करते समय आप इस रिश्ते को देख चुके हैं। अब, आप R पर गुणन तथा $R[x]$ पर गुणन के बीच संबंध के और प्रमाण देखेंगे।

प्रमेय 2: मान लीजिए R एक तत्समकी क्रमविनिमेय वलय है। तब $R[x]$ भी एक तत्समकी क्रमविनिमेय वलय है।

उपपत्ति: पहले हम दर्शाएंगे कि $R[x]$ क्रमविनिमेय है।

मान लीजिए कि वलय $R[x]$ में $p(x) = a_0 + a_1x + \cdots + a_nx^n$ और

$q(x) = b_0 + b_1x + \cdots + b_mx^m$.

तब, $p(x) \cdot q(x) = c_0 + c_1x + \cdots + c_sx^s$, जहाँ $s = m + n$, तथा

$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k$

$\quad = b_ka_0 + b_{k-1}a_1 + \cdots + b_1a_{k-1} + b_0a_k$, क्योंकि R में योग और गुणन दोनों क्रमविनिमेय हैं।

$= q(x)\cdot p(x)$ में x^k का गुणांक।

इस प्रकार, प्रत्येक $i \ge 0$ के लिए, $p(x)\cdot q(x)$ में x^i का गुणांक $q(x)\cdot p(x)$ में x^iके गुणांक के बराबर है।

अतः, $p(x)\cdot q(x) = q(x)\cdot p(x)$, अर्थात्, $R[x]$ क्रमविनिमेय है।

आगे, हम जानते हैं R का तत्समक 1 है। हम सिद्ध करेंगे कि अचर बहुपद 1, $R[x]$ का तत्समक है।

$p(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ लीजिए।

तब, $1\cdot p(x) = c_0 + c_1x + \cdots + c_nx^n$ (क्योंकि $\deg 1 = 0$),

जहाँ $c_k = a_k\cdot 1 + a_{k-1}\cdot 0 + a_{k-2}\cdot 0 + \cdots + a_0\cdot 0 = a_k$.

इस प्रकार, $1\cdot p(x) = p(x)$.

अतः, $R[x]$ का तत्समक 1 है। ■

प्रमेय 2 से हम जानते है कि $\mathbb{Z}[x]$ एक तत्समकी क्रमविनिमेय वलय है। इसी तरह, किसी भी क्षेत्र F के लिए, $F[x]$ एक तत्समकी क्रमविनिमेय वलय है।

प्रमेय 2 के विलोम के बारे में आपका क्या ख़्याल है? इसी बात से निम्नलिखित प्रश्न जुड़े हैं।

E13) यदि R एक ऐसा वलय है कि $R[x]$ तत्समकी क्रमविनिमेय वलय है, तो

i) क्या R को क्रमविनिमेय होना ही होगा?

ii) क्या R को तत्समकी होना ही होगा?

अपने उत्तरों के लिए, कारण दीजिए।

E14) मान लीजिए कि R एक तत्समकी क्रमविनिमेय वलय है। दर्शाइए कि $U(R[x]) = U(R)$.

आइंदा, हम सभी वलयों को तत्समकी और क्रमविनिमेय मान कर चलेंगे।

अब, आइए देखें कि क्या R और $R[x]$ शून्य के भाजकों के संबंध में एक ही प्रकार का व्यवहार करते हैं। इसके लिए, पहले हम वह परिणाम सिद्ध करेंगे जिसका ज़िक्र हमने तब किया था जब हमने बहुपदों के गुणन को परिभाषित किया था। आपने इसका E7(ii) को हल करते समय भी अस्पष्ट रूप से उपयोग किया था।

प्रमेय 3: मान लीजिए R एक वलय है तथा $f(x)$ और $g(x)$, $R[x]$ के दो शून्येतर अवयव हैं। तब,

$\deg(f(x)g(x)) \le \deg f(x) + \deg g(x)$.

आगे, यह एक समता है यदि और केवल यदि R बिना शून्य के भाजकों का है।

उपपत्ति: मान लीजिए $f(x) = a_0 + a_1x + \cdots + a_nx^n,\ a_n \ne 0,$

तथा $g(x) = b_0 + b_1x + \cdots + b_mx^m,\ b_m \ne 0.$

तब, $\deg f(x) = n,\ \deg g(x) = m.$

अतः, $f(x)\cdot g(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}$, जहाँ

$c_k = a_kb_0 + a_{k-1}b_1 + \cdots + a_0b_k,\ k = 0, 1, \ldots, m+n.$

क्योंकि $a_{n+1}, a_{n+2}, \ldots, a_{n+m}$ तथा $b_{m+1}, b_{m+2}, \ldots, b_{m+n}$ सभी शून्य हैं, इसलिए

$c_{m+n} = a_n b_m$.
इस प्रकार, $\deg\ (f(x)\cdot g(x)) \le n+m = \deg\ f(x) + \deg\ g(x)$.

अब, यदि R बिना शून्य के भाजकों का है, तो $a_n b_m \neq 0$, क्योंकि $a_n \neq 0$ और $b_m \neq 0$.
इस प्रकार, इस स्थिति में,
$\deg\ (f(x)g(x)) = \deg\ f(x) + \deg\ g(x)$.

विलोमतः, मान लीजिए कि
$\deg\ (f(x)g(x)) = \deg\ f(x) + \deg\ g(x)\ \forall\ f(x), g(x) \in R[x]\setminus\{0\}$.
हम अंतर्विरोध द्वारा सिद्ध करेंगे कि R बिना शून्य के भाजकों का है। मान लीजिए कि, इसके विपरीत, R में शून्य के भाजक हैं और मान लीजिए $ab = 0$, जहाँ R में $a \neq 0, b \neq 0$.
मान लीजिए $R[x]$ में $f(x) = a_0 + ax$ और $g(x) = b_0 + bx$.
तब, $f(x)g(x) = a_0b_0 + (ab_0 + a_0b)x + abx^2 = a_0b_0 + (ab_0 + a_0b)x$.
इस स्थिति में, $\deg\ (f(x)g(x)) = 1 < 2 = \deg\ f(x) + \deg\ g(x)$, तथा हम एक अंतर्विरोध पर पहुँचते हैं।
इस प्रकार, R बिना शून्य के भाजकों का है। ■

प्रमेय 2 और 3 हमें निम्नलिखित महत्वपूर्ण परिणाम पर ले जाता हैं।

प्रमेय 4: $R[x]$ एक पूर्णांकीय प्राँत है $\Leftrightarrow$ R एक पूर्णांकीय प्राँत है।

उपपत्ति: प्रमेय 2 और E13 से आप जानते हैं कि R एक तत्समकी क्रमविनिमेय वलय है यदि और केवल यदि $R[x]$ एक तत्समकी क्रमविनिमेय वलय है। इस प्रकार, इस प्रमेय को सिद्ध करने के लिए, हमें यह सिद्ध करने की आवश्कता है कि R बिना शून्य के भाजकों का है यदि और केवल यदि $R[x]$ बिना शून्य के भाजकों का है।

अतः, आइए पहले मान लें कि R बिना शून्य के भाजकों का है।
मान लीजिए कि $R[x]$ में $p(x)$ और $q(x)$ क्रमशः घातों n और m के हैं।
तब, प्रमेय 3 से आप जानते हैं कि $\deg(p(x)q(x)) = m+n \ge 0$.
इस प्रकार, $p(x)q(x) \neq 0$.
इस प्रकार, $R[x]$ बिना शून्य के भाजकों का है।

विलोमतः, आइए मान लें कि $R[x]$ बिना शून्य के भाजकों का है। क्योंकि $R[x]$ का R एक उपवलय है, इसलिए R भी बिना शून्य के भाजकों का है।
अतः, हमने प्रमेय को सिद्ध कर लिया है। ■

इस भाग में अभी तक आपने देखा कि वलय R के अनेक गुण $R[x]$ के लिए भी सत्य हैं, तथा इसका विलोम भी सत्य है। इस प्रकार, यदि F एक क्षेत्र है, तो आप शायद अपेक्षा करें कि $F[x]$ भी एक क्षेत्र होगा। आइए देखें कि क्या ऐसा है।

उदाहरण 2: मान लीजिए F एक क्षेत्र है। दर्शाइए कि $F[x]$ एक क्षेत्र नहीं है।
हल: क्योंकि F एक क्षेत्र है, इसलिए यह एक पूर्णांकीय प्राँत है। अतः, प्रमेय 4 द्वारा, $F[x]$ एक पूर्णांकीय प्राँत है।
मान लीजिए कि $F[x]$ एक क्षेत्र है। तब, $U(F[x]) = F[x]^*$.
परंतु, E14 से आप जानते हैं कि $U(F[x]) = U(F) = F^* \neq F[x]^*$.
अतः, हम एक अंतर्विरोध पर पहुँचते हैं।
इसलिए, $F[x]$ एक क्षेत्र नहीं है।

***

अब आप निम्नलिखित प्रश्नों को क्यों नहीं हल कर लेते? ऐसा करने से आपको कुछ वलयों R के लिए, $R[x]$ की समझ बेहतर बनेगी।

E15) निम्नलिखित में से कौन-से बहुपद वलय बिना शून्य के भाजकों के हैं?

i) $R[x]$, जहाँ $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$,

ii) $\mathbb{Z}_7[x]$,

iii) $\mathbb{M}_2(\mathbb{Q})[x]$,

iv) $R[x]$, जहाँ $R = C[0, 1]$,

v) $\wp(X)[x]$, जहाँ X कम से कम दो अवयवों वाला समुच्चय है।

E16) यदि I किसी वलय R की गुणजावली है, तो दर्शाइए कि $R[x]$ की $I[x] = \left\{\sum_{i=0}^{n} a_i x^i \middle| a_i \in I, n \in \mathbb{N}, \cup \{0\}\right\}$ एक गुणजावली है। इसके आगे, दर्शाइए कि $\left(R/I\right)[x] \simeq R[x]/I[x]$.

E17) दर्शाइए कि $R[x]$ की $< x >$ एक उचित गुणजावली है, जहाँ R एक अतुच्छ क्रमविनिमेय वलय है। इसी से दर्शाइए कि $R[x]$ की प्रत्येक गुणजावली $I[x]$ के रूप की **नहीं** होती है, जहाँ R की I एक गुणजावली है।

E18) मान लीजिए R एक प्राँत है। दर्शाइए कि $\text{char } R = \text{char } R[x]$.

E19) मान लीजिए $f : R \to S$ एक वलय समाकारिता है। दर्शाइए कि $\phi : R[x] \to S[x] : \phi(a_0 + a_1x + \cdots + a_nx^n) = f(a_0) + f(a_1)x + \cdots + f(a_n)x^n$ एक वलय समाकारिता है।
इसके आगे, यदि f एक तुल्याकारिता है, तो क्या ϕ भी एक तुल्याकारिता होगी? क्यों, या क्यों नहीं?

E20) मान लीजिए R और S वलय हैं। $\phi : (R \times S)[x] \to R[x] \times S[x] : \phi\left(\sum_{i=0}^{n} (a_i, b_i)x^i\right) = \left(\sum_{i=0}^{n} a_i x^i, \sum_{i=0}^{n} b_i x^i\right)$ परिभाषित कीजिए। जाँच कीजिए कि ϕ एक वलय समाकारिता है या नहीं। क्या ϕ आच्छादक है? क्या ϕ एकैकी है?

आप देख चुके हैं कि यदि R एक प्राँत है, तो $R[x]$ भी एक प्राँत होता है; परंतु यदि F एक क्षेत्र है, तो $F[x]$ एक क्षेत्र नहीं होता है। अतः, प्रश्न उठता है कि क्या क्षेत्र F तथा $F[x]$ के विभाग क्षेत्र में कोई संबंध है। इसका उत्तर देने के लिए, आइए पहले निम्नलिखित परिभाषा पर विचार करें।

परिभाषा: किसी अनिर्धार्य x में एक क्षेत्र F पर एक **परिमेय फलन (rational function)** विभाग $p(x)/q(x)$ है, जहाँ $p(x), q(x) \in F[x], q(x) \neq 0$.
F पर x में परिमेय फलनों के समुच्चय को $\mathbf{F(x)}$ द्वारा व्यक्त किया जाता है। (यहाँ, गोल कोष्ठकों के उपयोग पर ध्यान दीजिए।)

$F[x] \neq F(x)$. इन अलग वलयों को दर्शाने के लिए अगल प्रकार के कोष्ठकों के उपयोग पर ध्यान दीजिए।

उदाहरणार्थ, $\mathbb{Q}(x)=\{f(x)/g(x) \mid f(x), g(x)\in\mathbb{Q}[x], g(x)\neq 0\}$.

आइए अब उस प्रश्न के उत्तर की ओर बढ़ें, जो हमने ऊपर उठाया है।

प्रमेय 5: मान लीजिए F एक क्षेत्र है। तब, $F(x)$, $F[x]$ का विभाग क्षेत्र है।

उपपत्ति: इकाई 14 से आप जानते हैं कि पूर्णांकीय प्रांत $F[x]$ का विभाग क्षेत्र है $\{p(x)[q(x)]^{-1} \mid p(x), q(x)\in F[x], q(x)\neq 0\}=F(x)$, परिभाषा द्वारा। ■

इस प्रकार, **किसी भी क्षेत्र F के लिए, $F(x)$ एक क्षेत्र है,** तथा यह F पर एक अनिर्धार्य में **परिमेय फलनों का क्षेत्र** (**field of rational functions**) कहलाता है।

उदाहरणार्थ, $\mathbb{Q}$ पर x में परिमेय फलनों का क्षेत्र $\mathbb{Q}(x)$ है।

अब, एक प्रांत R लीजिए। आप जानते हैं कि $R[x]$ एक प्रांत है। यदि R का विभाग क्षेत्र F है, तो क्या $R[x]$ का विभाग क्षेत्र $F(x)$ होगा? आइए एक उदाहरण के माध्यम से इसका उत्तर ढूंढें।

उदाहरण 3: निम्नलिखित के विभाग क्षेत्र ज्ञात कीजिए:

i) $\mathbb{Q}[x]$, ii) $\mathbb{Z}[x]$.

हल: i) प्रमेय 5 द्वारा, $\mathbb{Q}[x]$ का $\mathbb{Q}(x)$ विभाग क्षेत्र है।

ii) आप जानते हैं कि किसी प्रांत का विभाग क्षेत्र उसको आविष्ट करने वाला लघुतम क्षेत्र होता है। आप यह भी जानते हैं कि $\mathbb{Z}$ का विभाग क्षेत्र $\mathbb{Q}$ है। हम इन तथ्यों का उपयोग F ज्ञात करने के लिए करेंगे, जहाँ F, $\mathbb{Z}[x]$ का विभाग क्षेत्र है।
क्योंकि F, $\mathbb{Z}[x]$ को आविष्ट करने वाला एक क्षेत्र है, इसलिए यह $\mathbb{Z}$ को आविष्ट करता है।
अतः, $F\supseteq\mathbb{Q}$.
साथ ही, किसी भी $f(x)=\frac{r_0}{s_0}+\frac{r_1}{s_1}x+\cdots+\frac{r_n}{s_n}x^n\in\mathbb{Q}[x]$, $s_0s_1\ldots s_nf(x)\in\mathbb{Z}[x]$.
इस प्रकार, किसी भी $f(x)\in\mathbb{Q}[x]$ के लिए $\exists\, m\in\mathbb{Z}$ s.t. $mf(x)\in\mathbb{Z}[x]$.
अब, मान लीजिए ${f(x)}/{g(x)}\in\mathbb{Q}(x)$, जहाँ $f(x), g(x)\in\mathbb{Q}[x]$, $g(x)\neq 0$.
यदि $f(x)=0$, तो $\frac{f(x)}{g(x)}\in F$.
यदि $f(x)\neq 0$, तो किन्हीं $m, n\in\mathbb{Z}$ के लिए, जहाँ $m, n\neq 0$, $\mathbb{Z}[x]$ में $mf(x)$ और $ng(x)$ हैं।
अतः, ${f(x)}/{g(x)}=\left(\frac{n}{m}\right)\frac{mf(x)}{ng(x)}\in F$, क्योंकि $\mathbb{Q}\subseteq F$ तथा $\mathbb{Z}[x]$ का F विभाग क्षेत्र है।
अतः, $\mathbb{Q}(x)\subseteq F$.
साथ ही, किसी भी $p(x)\in\mathbb{Z}[x]$ के लिए, $p(x)\in\mathbb{Q}[x]\subseteq\mathbb{Q}(x)$.
अब $\mathbb{Q}(x)$, $\mathbb{Z}[x]$ को आविष्ट करने वाला एक क्षेत्र है, तथा यह F में आविष्ट है, और F, $\mathbb{Z}[x]$ का विभाग क्षेत्र है। इसलिए $\mathbb{Q}(x)=F$.
इस प्रकार, $\mathbb{Z}[x]$ का विभाग क्षेत्र वही है जो $\mathbb{Q}[x]$ का विभाग क्षेत्र है। यहाँ ध्यान दीजिए कि हमने इस तथ्य का उपयोग किया है कि $\mathbb{Q}$, $\mathbb{Z}$ का विभाग क्षेत्र है।

***

उपरोक्त उदाहरण की प्रक्रिया को अपनाते हुए, आइए उदाहरण 3 से पहले उठाए गए प्रश्न का उत्तर दें।

प्रमेय 6: मान लीजिए D एक पूर्णांकीय प्रांँत है जिसका विभाग क्षेत्र F है। तब, $D[x]$ का विभाग क्षेत्र $F(x)$ है, जो F पर परिमेय फलनों का क्षेत्र है।

उपपत्ति: पहले तो, $D \subseteq F \subseteq F(x)$. अतः, $D[x] \subseteq F[x] \subseteq F(x)$.
साथ ही, $F[x]$ को आविष्ट करने वाला $F(x)$ लघुतम क्षेत्र है।
मान लीजिए $D[x]$ को आविष्ट करने वाला K कोई क्षेत्र है।
तब, $K \supseteq D$, तथा इसी लिए $K \supseteq F$.
साथ ही, $F[x]$ में कोई भी बहुपद $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n$ के रूप का है,
जहाँ $a_i, b_j \in D, b_j \neq 0,\ i, j = 1, \ldots, n$ के लिए।
तब, उदाहरण 3(ii) की ही तरह, $\exists\, d \in D^*$ s.t. $df(x) \in D[x]$.
$\therefore\ f(x), K$ में है, क्योंकि $D[x]$ का प्रत्येक बहुपद K में है।
इस प्रकार, $K \supseteq F[x]$.
अतः, $K \supseteq F(x)$.
इस प्रकार, $D[x]$ को आविष्ट करने वाला लघुतम क्षेत्र $F(x)$ है, अर्थात् यह $D[x]$ का विभाग क्षेत्र है। ■

अब, आप कुछ संबंधित प्रश्नों को क्यों नहीं हल करते?

E21) निम्नलिखित प्रांँतों के विभाग क्षेत्र ज्ञात कीजिएः

i) $\mathbb{Z}[i][x]$, ii) $\mathbb{Q}[\sqrt{11}][x]$, iii) $\mathbb{Z}_p[x]$, जहाँ P अभाज्य संख्या है।

E22) पुष्टि करते हुए, $\mathbb{C}[x]$ के विभाग क्षेत्र के दो अलग अतुच्छ दीजिए।

E23) प्रत्येक अभाज्य संख्या p के लिए, अभिलक्षणिक p वाला एक अपरिमित क्षेत्र ज्ञात कीजिए।

इस भाग में आपने अनेक गुण देखे जो R और $R[x]$ दोनों के लिए सत्य हैं। आप कुछ ऐसे भी गुण देखे, जो दोनों के लिए अलग हैं – उदाहरणार्थ, F एक क्षेत्र है, परंतु $F[x]$ क्षेत्र नहीं है। परंतु, $F[x]$ स्वयं में एक अति रोचक बीजीय वस्तु है। इसमें अनेक रोचक गुण हैं जो $\mathbb{Z}$ के गुणों की तरह ही हैं। अगले भाग में हम ऐसे ही कुछ गुणों की चर्चा करेंगे जो विभाज्यता से संबंधित हैं।

15.4 बहुपद वलयों में विभाज्यता

इकाई 1 में आपने $\mathbb{Z}$ में विभाज्यता के विभिन्न गुणों का अध्ययन किया था। विशिष्ट रूप में, आपने पूर्णांकों के लिए विभाजन ऐल्गोरिद्म का अध्ययन किया था। अब हम एक क्षेत्र F पर बहुपदों के लिए विभाज्यता, तथा विभाजन ऐल्गोरिद्म, की चर्चा करेंगे। आगे बढ़ने से पहले आप इकाई 1 के प्रमेय 4 तथा संबंधित उदाहरणों पर दोबारा एक नज़र मार

लीजिए। इससे आपको पूर्णांकों द्वारा संतुष्ट होने वाले गुणों तथा F पर बहुपदों द्वारा संतुष्ट होने वाले गुणों में समानता देखेने में सहायता मिल सकती है।

आइए $\mathbb{Q}[x]$ में एक उदाहरण से प्रारंभ करें। आइए यह ज्ञात करने के लिए कि $3x^3+4$ को $2x^2+x$ से भाग देने पर क्या मिलता है भाग की लंबी प्रक्रिया का उपयोग करें।

$$\begin{array}{r l}
 & \frac{3}{2}x-\frac{3}{4} \longleftarrow \text{भागफल} \\
2x^2+x\,\big) & 3x^3+4 \\
 & 3x^3+\frac{3}{2}x^2 \\ \hline
 & -\frac{3}{2}x^2+4 \\
 & -\frac{3}{2}x^2-\frac{3}{4}x \\ \hline
 & \frac{3}{4}x+4 \longleftarrow \text{शेषफल}
\end{array}$$

अतः, ऊपर के विभाजन में हमने क्या किया है? हम $(2x^2+x)$ के अलग गुणजों को तब तक घटाते रहे जब तक कि हम 0 या $\deg(2x^2+x)$ से कम घात वाले बहुपद तक नहीं पहुँचे। यह बहुपद, अर्थात् $\frac{3}{4}x+4$, ही शेषफल है। $(2x^2+x)$ के गुणजों का योग, अर्थात् $\frac{3}{2}x-\frac{3}{4}$ भागफल है। वास्तव में यह वही प्रक्रिया है जो विभाजन ऐल्गोरिद्म में की जाती है, जैसा कि अब आप देखेंगे।

प्रमेय 7 (विभाजन ऐल्गोरिद्म): मान लीजिए F एक क्षेत्र है। मान लीजिए $F[x]$ में $f(x)$ और $g(x)$ बहुपद हैं, जहाँ $g(x)\neq 0$. तब

i) $F[x]$ में ऐसे बहुपद $q(x)$ और $r(x)$ हैं जिनसे कि $f(x)=q(x)g(x)+r(x)$, जहाँ $r(x)=0$ या $\deg r(x)<\deg g(x)$, तथा

ii) $q(x)$ और $r(x)$ अद्वितीय होते हैं।

उपपत्ति: i) यदि $\deg f(x)<\deg g(x)$, तो हम $q(x)=0$ चुन सकते हैं।
तब, $f(x)=0\cdot g(x)+f(x)$, जहाँ $\deg f(x)<\deg g(x)$.
अतः, इस स्थिति में, $r(x)=f(x)$ और $q(x)=0$.

अब, आइए मान लें कि $\deg f(x)\geq \deg g(x)$.
मान लीजिए $f(x)=a_0+a_1x+\cdots+a_nx^n$, $a_n\neq 0$, तथा
$g(x)=b_0+b_1x+\cdots+b_mx^m$, $b_m\neq 0$, जहाँ $n\geq m$.
हम $\deg f(x)$, अर्थात् n पर गणितीय आगमन नियम के शक्तिशाली रूप का अनुप्रयोग करेंगे (इकाई 1 देखिए)।
यदि $n=0$, तो $m=0$, क्योंकि $g(x)\neq 0$.
अतः, $f(x)=a_0$ और $g(x)=b_0$, F में हैं।
इसलिए, $f(x)=(a_0b_0^{-1})b_0+0=q(x)g(x)+r(x)$, जहाँ $q(x)=a_0b_0^{-1}$ तथा $r(x)=0$.
अतः, यह ऐल्गोरिद्म सत्य है जब $n=0$.

आइए मान लें कि यह ऐल्गोरिद्म n से छोटी घातों के सभी बहुपदों के लिए सत्य है, तथा फिर देखें कि क्या यह $f(x)$ के लिए सत्य है।

निम्नलिखित बहुपद पर विचार कीजिए:

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$$
$$= (a_0 + a_1 x + \cdots + a_n x^n) - (a_n b_m^{-1} b_0 x^{n-m} + a_n b_m^{-1} b_1 x^{n-m+1} + \cdots + a_n b_m^{-1} b_m x^n).$$

हमने $f_1(x)$ में x^n के गुणांक को शून्य बनाने के लिए, $g(x)$ से गुणा करने के लिए $a_n b_m^{-1} x^{n-m}$ को चुना है।

अतः, $\deg f_1(x) \le n-1$.

आगमन परिकल्पना द्वारा, $F[x]$ में ऐसे $q_1(x)$ और $r(x)$ हैं जिनसे कि

$f_1(x) = q_1(x)g(x) + r(x)$, जहाँ $r(x) = 0$ या $\deg r(x) < \deg g(x)$.

$f_1(x)$ के मान को प्रतिस्थापित करने पर, हम प्राप्त करते हैं:

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = q_1(x)g(x) + r(x),$$

अर्थात्, $f(x) = \{a_n b_m^{-1} x^{n-m} + q_1(x)\}g(x) + r(x)$

$= q(x)g(x) + r(x)$, जहाँ $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$ तथा

$r(x) = 0$ या $\deg r(x) < \deg g(x)$.

अतः, $f(x)$ के लिए (i) सत्य है।

इसलिए, आगमन नियम द्वारा, $F[x]$ में सभी बहुपदों के लिए (i) सत्य है।

ii) आइए अब दर्शाएं कि $q(x)$ और $r(x)$ अद्वितीय रूप से निर्धारित होते हैं।

मान लीजिए कि $f(x), g(x) \in F[x], g(x) \neq 0$.

यदि संभव है, तो मान लीजिए कि $F[x]$ में $q_1(x), q_2(x), r_1(x), r_2(x)$ ऐसे हैं कि

$f(x) = q_1(x)g(x) + r_1(x)$, जहाँ $r_1(x) = 0$ या $\deg r_1(x) < \deg g(x)$, तथा

$f(x) = q_2(x)g(x) + r_2(x)$, जहाँ $r_2(x) = 0$ या $\deg r_2(x) < \deg g(x)$.

तब,

$q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$, जिससे

$\{q_1(x) - q_2(x)\}g(x) = r_2(x) - r_1(x)$ प्राप्त होता है। …(1)

यदि $r_1(x) = r_2(x)$, तो (1) से, $q_1(x) = q_2(x)$, क्योंकि $g(x) \neq 0$.

अतः, मान लीजिए कि $r_1(x) - r_2(x) \neq 0$. तब, $q_1(x) \neq q_2(x)$.

अतः, $\deg \{q_1(x) - q_2(x)\} \ge 0$, तथा इसी लिए

$\deg [\{q_1(x) - q_2(x)\}g(x)] \ge \deg g(x)$. …(2)

दूसरी ओर,

$\deg \{r_2(x) - r_1(x)\} < \deg g(x)$, …(3)

क्योंकि $r_1(x) - r_2(x) \neq 0$, तथा इसी लिए, $r_1(x) \neq 0$ या $r_2(x) \neq 0$.

(2) और (3) से, हमें (1) का अंतर्विरोध प्राप्त होता है।

अतः, (1) केवल तभी मान्य होगा जब $r_2(x) - r_1(x) = 0$. और फिर,

$q_1(x) - q_2(x) = 0$.

अर्थात्, $q_1(x) = q_2(x)$ और $r_1(x) = r_2(x)$.

इस तरह, हमने व्यंजक $f(x) = q(x)g(x) + r(x)$ में $q(x)$ और $r(x)$ की अद्वितीयता को सिद्ध कर लिया है। ■

प्रमेय 7 के ऐल्गोरिद्म के लिए, हमें कुछ शब्दों को परिभाषित करने की आवश्यकता है, जैसे $\mathbb{Z}$ के लिए किया था।

परिभाषाएँ: i) प्रमेय 7 में $r(x)$ को $q(x)$ से भाग देने पर प्राप्त बहुपद $g(x)$ **भागफल** कहलाता है तथा $f(x)$ **शेषफल** कहलाता है।

ii) यदि $r(x)=0$, तो $f(x)=g(x)q(x)$. इस स्थिति में हम कहते हैं कि $f(x)$ को $g(x)$ **विभाजित करता है (divides),** या यह कि $f(x)$ का $g(x)$ एक **गुणनखंड (factor)** है, या यह कि $g(x)$ द्वारा $f(x)$ विभाज्य **(divisible)** है। हम '$f(x)$ को $g(x)$ विभाजित करता है' दर्शाने के लिए $\mathbf{g(x)\mid f(x)}$ लिखते हैं, तथा '$f(x)$ को $g(x)$ विभाजित नहीं करता है' के लिए $\mathbf{g(x)\nmid f(x)}$ लिखते हैं।

आइए अब विभाजन ऐल्गोरिद्म का कुछ स्थितियों में अनुप्रयोग करें।

उदाहरण 4: $\mathbb{Q}[x]$ में $x^4+x^3+5x^2-x$ को (x^2+x+1) द्वारा भाग देने पर प्राप्त भागफल और शेषफल ज्ञात कीजिए।

हल: हम इस प्रश्न को हल करने के लिए बहुपदों के लिए विभाजन की लंबी प्रक्रिया का उपयोग करेंगे। यहाँ $f(x)=x^4+x^3+5x^2-x$ और $g(x)=x^2+x+1$.

$$
\begin{array}{rl}
 & x^2 \qquad\quad +4 \quad \leftarrow \text{भागफल } q(x)\\
(x^2+x+1) \big) & \overline{x^4+x^3+5x^2-x}\\
 & \underline{x^4+x^3+x^2} \quad \leftarrow x^2g(x)\\
 & \qquad 4x^2-x \quad \leftarrow (f(x)-x^2g(x))\\
 & \qquad \underline{4x^2+4x+4} \quad \leftarrow 4g(x)\\
 & \qquad\quad -5x-4 \quad \leftarrow (f(x)-x^2g(x)-4g(x))
\end{array}
$$

अब, क्योंकि $\deg(-5x-4)=1<\deg(x^2+x+1)$, हम प्रक्रिया को रोक लेते हैं। अतः, शेषफल $r(x)=-5x-4$. अतः, हम प्राप्त करते हैं
$x^4+x^3+5x^2-x=(x^2+x+1)(x^2+4)-(5x+4)$.
यहाँ, भागफल x^2+4 है तथा शेषफल $-(5x+4)$ है।

***

उदाहरण 5: जाँच कीजिए कि $\mathbb{R}[x]$ में $(3x^4+2x^2+2)$ को (x^2+2) विभाजित करता है या नहीं, तथा को $\mathbb{Z}_5[x]$ में $(\bar{3}x^4+\bar{2}x^2+\bar{2})$ $(x^2+\bar{2})$ विभाजित करता है या नहीं।

हल: आइए पहले $\mathbb{R}[x]$ में भाग करें।

$$
\begin{array}{rl}
 & 3x^2-4\\
(x^2+2)\big) & \overline{3x^4+2x^2+2}\\
 & \underline{3x^4+6x^2}\\
 & \quad -4x^2+2\\
 & \quad \underline{-4x^2-8}\\
 & \qquad\quad 10
\end{array}
$$

इस प्रकार, $\mathbb{R}[x]$ में $3x^4+2x^2+2=(x^2+2)(3x^2-4)+10$. ...(4)
क्योंकि शेषफल शून्य नहीं है, इसलिए $\mathbb{R}[x]$ में $(x^2+2)\nmid(3x^4+2x^2+2)$.

आइए, अब $\mathbb{Z}_5[x]$ के प्रश्न पर दृष्टि डालें। ध्यान दीजिए कि बहुपद वही हैं जो $\mathbb{R}[x]$ के सवाल में थे। साथ ही, ध्यान दीजिए कि $\mathbb{Z}[x]$ में भी (4) सत्य है। अतः, यदि हम (4) को $\mathbb{Z}_5[x]$ में देखें, तो हम प्राप्त करते हैं:

$\bar{3}x^4+\bar{2}x^2+\bar{2}=(x^2+\bar{2})(\bar{3}x^2+\bar{1})$, क्योंकि $\mathbb{Z}_5$ में $-\bar{4}=\bar{1}$ तथा $\overline{10}=\bar{0}$.

अतः, $\mathbb{Z}_5[x]$ में $(x^2+\bar{2})\,\big|\,(\bar{3}x^4+\bar{2}x^2+\bar{2})$.

***

अब, क्यों नही आप कुछ स्थितियों में विभाजन ऐल्गोरिद्म का उपयोग कर लेते?

E24) निम्नलिखित में से प्रत्येक स्थिति में $f(x)$ को $g(x)q(x)+r(x)$ के रूप में व्यक्त कीजिए, जहाँ $r(x)=0$ या $\deg r(x)<\deg g(x)$.

i) $\mathbb{Q}[x]$ में $f(x)=x^4+1,\ g(x)=\frac{1}{7}-x^3$,

ii) $\mathbb{Z}_3[x]$ में $f(x)=x^3+\bar{2}x^2-x+\bar{1},\ g(x)=\bar{2}x+\bar{1}$,

iii) $\mathbb{R}[x]$ में $f(x)=x^3-3\sqrt{3},\ g(x)=x-\sqrt{3}$.

इन स्थितियों में से किन में $f(x)$ को $g(x)$ विभाजित करता है?

अब, आइए $F[x]$ में संबंध 'विभाजित करता है' के कुछ गुणों को सिद्ध करें। (इनका अध्ययन करते समय $\mathbb{Z}$ के साथ समानता को नोट करते जाएँ। ऐसा करते समय, आप पूर्णांकों की स्थिति में 'घात' के स्थान पर 'निरपेक्ष मान' को ले सकते हैं।)

प्रमेय 8: मान लीजिए F एक क्षेत्र है तथा के साथ, $f(x), g(x), h(x)\in F[x]$, जहाँ $f(x)\neq 0$.

i) यदि $f(x)\,|\,g(x)$, जहाँ $g(x)\neq 0$, तो $\deg f(x)\leq \deg g(x)$.

ii) $f(x)\,|\,f(x)$.

iii) यदि $f(x)\,|\,g(x)$ तथा $a\in F^*$, तो $af(x)\,|\,ag(x)$.

iv) यदि $g(x)\neq 0$ s.t. $f(x)\,|\,g(x)$ और $g(x)\,|\,h(x)$, तो $f(x)\,|\,h(x)$.

v) यदि $g(x)\neq 0$ s.t. $f(x)\,|\,g(x)$ और $g(x)\,|\,f(x)$, तो किसी $a\in F^*$ के लिए $f(x)=ag(x)$.

vi) यदि $f(x)\,|\,g(x)$ और $f(x)\,|\,h(x)$, तो $f(x)\,|\,(g(x)+h(x))$.

vii) यदि $f(x)\,|\,g(x)$, तो $f(x)\,|\,g(x)h(x)$.

उपपत्ति: हम यहाँ (i) और (v) को सिद्ध करेंगे, तथा शेष अभ्यास के लिए आपको सिद्ध करने के लिए छोड़ देंगे (E25) देखिए।

i) यदि $f(x)\,|\,g(x)$, तो $\exists\ q(x)\in F[x]$ s.t. $f(x)q(x)=g(x)$.
अतः, $\deg f(x)+\deg q(x)=\deg g(x)$.
क्योंकि $g(x)\neq 0,\ q(x)\neq 0$.
अतः, $\deg q(x)\geq 0$.
इसलिए, $\deg f(x)\leq \deg g(x)$.

v) मान लीजिए $f(x)q(x) = g(x)$ और $g(x)r(x) = f(x)$ किन्हीं $q(x), r(x) \in F[x]$ के लिए, जहाँ $q(x) \neq 0, r(x) \neq 0.$
तब, $g(x)r(x)q(x) = g(x).$
अतः, $r(x)q(x) = 1,$ क्योंकि $F[x]$ में निरसन नियम लागू होता है।
इस प्रकार, $r(x) \in U(F[x]) = U(F) = F^*$, जैसा आपने E14 में सिद्ध किया है।
अतः, $r(x) = r_0 \in F^*.$
इस प्रकार, $f(x) = r_0 g(x), r_0 \in F^*.$ ■

उपरोक्त प्रमेय की उपपत्ति तब पूरी होगी, जब आप निम्नलिखित प्रश्न को हल कर लेंगे।

E25) (i) और (v) को छोड़ कर प्रमेय 8 को सिद्ध कीजिए।

आइए अब देखें कि क्या हम प्रमेय 8 के आधार पर, इकाई 1 के उदाहरण 3 के अनुरूप किसी तुल्यता संबंध को परिभाषित कर सकते हैं।

उदाहरण 6: मान लीजिए F एक क्षेत्र है तथा $h(x) \in F[x], h(x) \neq 0.$ संबंध $R = \{(f(x), g(x)) \mid h(x),$
$[f(x) - g(x)]$ को विभाजित करता है, जहाँ $f(x), g(x) \in F[x]\}$ पर विचार कीजिए। जाँच कीजिए कि $F[x]$ पर R एक तुल्यता संबंध है या नहीं। यदि है, तो 0 के तुल्यता वर्ग में दो अलग-अलग अवयव ज्ञात कीजिए। यदि यह नहीं है, तो $f[x]$ पर एक तुल्यया संबंध परिभाषित कीजिए।

हल: ध्यान दीजिए कि R संबंध ~ है जो '$F[x]$ में $f(x) \sim g(x)$ iff $h(x) \mid [f(x) - g(x)]$' द्वारा दिया जाता है।
R स्वतुल्य है: किसी भी $f(x) \in F[x]$ के लिए, $f(x) \sim f(x),$ क्योंकि $h(x) \mid 0.$
R सममित है: मान लीजिए $f(x) \sim g(x).$ तब $\exists\, r(x) \in F[x]$ s.t.
$f(x) - g(x) = h(x)r(x).$
अतः, $g(x) - f(x) = h(x)[-r(x)],$ तथा $-r(x) \in F[x].$
इसलिए, $g(x) \sim f(x).$
R संक्रामक है: मान लीजिए $F[x]$ में $f(x) \sim g(x)$ तथा $g(x) \sim s(x).$
तब, $h(x) \mid [f(x) - g(x)]$ तथा $h(x) \mid [g(x) - s(x)].$
इस प्रकार, प्रमेय 8(vi) द्वारा, $h(x) \mid [f(x) - g(x) + g(x) - s(x)],$ अर्थात्,
$h(x) \mid [f(x) - s(x)].$
अतः, $f(x) \sim s(x).$

इस प्रकार, हमने सिद्ध कर लिया है कि R एक तुल्यता संबंध है। अतः, $F[x]$ को R तुल्यता वर्गों में विभाजित कर देता है, जैसा कि आप इकाई 1, भाग 1.3, से जानते हैं।
$[0] = \{f(x) \in F[x] \mid h(x),\ [f(x) - 0]$ को विभाजित करता है $\} = \{f(x) \in F[x] \mid h(x),$ $f(x)\}$ को विभाजित करता है

$$= \{h(x)g(x) \mid g(x) \in F[x]\}$$
$$= < h(x) > .$$

इस प्रकार, [0] के दो अवयव $h(x)$ और $xh(x)$ हैं, उदाहरण के तौर पर ये अलग-अलग हैं क्योंकि इनकी घातें अलग-अलग हैं।

***

अब, आप क्यों नहीं $F[x]$ में विभाज्यता की अपनी समझ की जाँच कर लेते?

E26) प्रमेय 8 में यदि $F[x]$ को $R[x]$ द्वारा प्रतिस्थापित कर दिया जाए, जहाँ R एक पूर्णांकीय प्राँत है, तो कौन-से कथन सत्य रह जाते हैं, और क्यों?

E27) दर्शाइए कि यदि जहाँ R एक प्राँत है और $f(x), g(x) \in R[x]$ ऐसे एकगुणांकी बहुपद हैं कि $f(x) \mid g(x)$ तथा $g(x) \mid f(x)$, तो $f(x) = g(x)$.

E28) मान लीजिए कि F एक क्षेत्र है। जाँच कीजिए कि '$f(x) \sim g(x)$ iff $f(x) \mid g(x)$' द्वारा दिया जाने वाला $F[x]$ में संबंध ~ एक तुल्यता संबंध है या नहीं।

E29) मान लीजिए कि F एक क्षेत्र है तथा मान लीजिए कि $f(x), g(x), h(x) \in F[x]$ s.t. $f(x) \neq 0$ तथा $f(x) \mid g(x)$, $f(x) \mid h(x)$. दर्शाइए कि $f(x) \mid [g(x)r(x) + h(x)s(x)]$, किसी भी $r(x), s(x) \in F[x]$ के लिए।

आइए अब $\mathbb{Z}$ के एक अन्य गुण की बात करें, तथा देखें कि क्या यह $F[x]$ के लिए सत्य है। इकाई 1 में आप देख चुके हैं कि किन्हीं दो शून्येतर पूर्णांकों a और b का एक महत्तम समापवर्तक d होता है, तथा $\mathbb{Z}$ में किन्हीं n, m के लिए $d = an + bm$. क्या हम इसी प्रकार से $F[x]$ में दो शून्येतर बहुपदों के लिए g.c.d. को परिभाषित कर सकते हैं? क्या $F[x]$ में 'सापेक्षतः अभाज्य' की संकल्पना के बारे में भी सोचा जा सकता है? आइए देखें।

$\mathbb{Q}[x]$ में कोई भी दो बहुपदों, मान लीजिए $x^2 + 3x$ तथा $x^3 + 27$ को लीजिए। अब, $x^2 + 3x = x(x+3)$ तथा $x^3 + 27 = (x+3)(x^2 - 3x + 9)$.
अतः, $x^2 + 3$ तथा $x^3 + 27$ दोनों को $x+3$ विभाजित करता है। इस प्रकार, नीचे दी परिभाषाओं के अनुसार, $x+3$ इन दोनों बहुपदों का सार्वभाजक है।

परिभाषाएँ: मान लीजिए कि F एक क्षेत्र है तथा $F[x]$ के $f(x), g(x)$ शून्येतर अवयव हैं।

i) $f(x)$ और $g(x)$ का $h(x) \in F[x]$ एक **सार्वभाजक** (या **समापवर्तक**) कहलाता है, यदि $h(x) \mid f(x)$ और $h(x) \mid g(x)$.

ii) $f(x)$ और $g(x)$ का $d(x) \in F[x]$ **महत्तम समापवर्तक** (संक्षिप्त में, **g.c.d**) कहलाता है, तथा **(f(x), g(x))** द्वारा व्यक्त किया जाता है, यदि
D1) $f(x)$ और $g(x)$ का $d(x)$ एक सार्वभाजक है;
D2) जब भी $f(x)$ और $g(x)$ का $h(x)$ एक सार्वभाजक है, तब $h(x) \mid d(x)$;
D3) $d(x)$ एक गुणांकी बहुपद है।

iii) $f(x)$ और $g(x)$ **असहभाज्य** (या **सापेक्षतः अभाज्य**) कहलाते हैं, यदि $(f(x), g(x)) = 1$.

उदाहरणार्थ, $\mathbb{Q}[x]$ में $(x^2 + 3x, x^3 + 27) = (x+3)$, इनके गुणनखंडों को देखते हुए।

g.c.d. की अद्वितीयता के बारे में निम्नलिखित टिप्पणी पर विचार कीजिए।

टिप्पणी 2: मान लीजिए कि $F[x]$ में $f(x)$ और $g(x)$ के $d(x)$ और $d'(x)$ दो g.c.d हैं, जहाँ F एक क्षेत्र है। तब, D2 से $d(x) \mid d'(x)$ और $d'(x) \mid d(x)$.

अतः, प्रमेय 8 द्वारा, किसी $a \in F^*$ के लिए, $d(x) = ad'(x)$. अतः, यदि हम $d(x)$ को अद्वितीय चाहते हैं, तो हमें $a = 1$ की आवश्यकता है। यह E27 से सुनिश्चित हो जाता है यदि प्रतिबंध D3 संतुष्ट हो जाए। अतः, g.c.d के अद्वितीय होने के लिए, D3 एक आवश्यक प्रतिबंध है।

अब, $\mathbb{Z}$ की स्थिति में आप जानते हैं कि किन्हीं दो शून्येतर पूर्णांकों का g.c.d होता है। क्या $F[x]$ में किन्हीं दो शून्येतर बहुपदों का g.c.d होता हैं? आइए देखें।

प्रमेय 9: मान लीजिए F एक क्षेत्र है। F पर किन्हीं दो शून्येतर बहुपदों का g.c.d होता है। इसके आगे, $f(x), g(x) \in F[x] \setminus \{0\}$ के लिए,
$(f(x), g(x)) = f(x)r(x) + g(x)s(x)$, किन्हीं $r(x), s(x) \in F[x]$ के लिए।

उपपत्ति: मान लीजिए कि $F[x]$ में $f(x), g(x)$ दो शून्येतर बहुपद हैं। मान लीजिए कि S, $F[x]$ में उन सभी **एकगुणांकी** बहुपदों का समुच्चय है जो $f(x)r(x) + g(x)s(x)$ के रूप के हैं, किन्हीं $r(x), s(x) \in F[x]$ के लिए।
मान लीजिए कि $f(x)$ का अग्रग गुणांक a_n है।
तब $a_n^{-1}f(x)$ एकगुणांकी है, तथा $a_n^{-1}f(x) = a_n^{-1} \cdot f(x) + 0 \cdot g(x) \in S$.
इस प्रकार, $S \neq \emptyset$.
अब, $A = \{n \in \mathbb{N} \cup \{0\} \mid n = \deg h(x)$ किसी $h(x) \in S$ के लिए$\}$.
तब, $A \neq \emptyset$, क्योंकि $S \neq \emptyset$. अतः, सुक्रमण सिद्धांत द्वारा, जिसका अध्ययन आपने इकाई 1 में किया था, A का एक लघुतम अवयव, मान लीजिए, m है।
मान लीजिए $d(x) \in S$ s.t.
क्योंकि $d(x) \in S$, $d(x)$ एक एकगुणांकी बहुपद है तथा $\exists\, \alpha(x), \beta(x) \in F[x]$ s.t.
$d(x) = f(x)\alpha(x) + g(x)\beta(x)$. …(5)
अब, $f(x)$ और $d(x)$ पर विभाजन ऐल्गोरिद्म लागू करने से, $F[x]$ में ऐसे $q(x)$ और $r(x)$ हैं कि
$f(x) = d(x)q(x) + r(x)$, …(6)
जहाँ $r(x) = 0$ या $\deg r(x) < \deg d(x)$.
अब, मान लीजिए $r(x) \neq 0$ तब

$$
\begin{aligned}
r(x) &= f(x) - d(x)q(x), \text{ (6) से।} \\
&= f(x) - [f(x)\alpha(x) + g(x)\beta(x)]q(x), \text{ (5) से।} \\
&= f(x)[1 - \alpha(x)q(x)] + g(x)[-\beta(x)q(x)].
\end{aligned}
$$

मान लीजिए कि $r(x)$ का अग्रग गुणांक a है। तब,
$a^{-1}r(x) = f(x)[a^{-1} - a^{-1}\alpha(x)q(x)] + g(x)[-a^{-1}\beta(x)q(x)]$.
इस प्रकार, $a^{-1}r(x) \in S$ तथा $\deg a^{-1}r(x) = \deg r(x) < \deg d(x)$.
यह $d(x)$ के चुनने की विधि का अंतर्विरोध करता है।
अतः, हमारी परिकल्पना कि $r(x) \neq 0$ ग़लत होगी।
इस प्रकार, $r(x) = 0$.
अतः, (6) से, $d(x) \mid f(x)$.
इसी प्रकार, आप दर्शा सकते हैं कि $d(x) \mid g(x)$.
इस प्रकार, g.c.d की परिभाषा के D1 और D3 को $d(x)$ संतुष्ट करता है।

अब, मान लीजिए कि $f(x)$ और $g(x)$ का $h(x)$ एक सार्वभाजक है। तब, E29 द्वारा, $h(x) \mid d(x)$. अतः, $d(x)$ परिभाषा के D2 को भी संतुष्ट करता है।
अतः, $d(x) = (f(x), g(x))$.

इस प्रकार, (5) द्वारा, किन्हीं $\alpha(x), \beta(x) \in F[x]$ के लिए,
$(f(x), g(x)) = f(x)\alpha(x) + g(x)\beta(x).$ ■

इस संदर्भ में, निम्नलिखित टिप्पणी पर विचार कीजिए।

टिप्पणी 3: प्रमेय 9 बताता है कि $(f(x), g(x))$, $F[x]$ में $f(x)$ और $g(x)$ का वह **एकघात संचय (linear combination)** है जो एकगुणांकी है तथा ऐसे सभी संचयों में सबसे कम घात वाला है।
ध्यान दीजिए कि $f(x)$ और $g(x)$ का प्रत्येक एकघात संचय $(f(x), g(x))$ नहीं होता। उदाहरणार्थ, $\mathbb{Q}[x]$ में (x^3-1) और (x^2+2) लीजिए। विभाजन ऐल्गोरिद्म द्वारा,
$x^3-1 = (x^2+2)x + (-2x-1).$
अतः, $-2x-1 = (x^3-1) - x(x^2+2)$, जो $\mathbb{Q}[x]$ में (x^3-1) और (x^2+2) का एक एकघात संचय है। परंतु $\mathbb{Q}[x]$ में $-2x-1$ न तो (x^3-1) का भाजक है और न ही (x^2+2) का।

$\mathbb{Z}$ की स्थिति की ही तरह, यदि $f(x)$ और $g(x)$ सापेक्षतः अभाज्य हैं, तो हमें प्रमेय 9 का निम्नलिखित उपप्रमेय प्राप्त होता है।

उपप्रमेय 2: मान लीजिए F एक क्षेत्र है तथा $f(x), g(x) \in F[x] \setminus \{0\}$. तब, $f(x)$ और $g(x)$ सापेक्षतः अभाज्य हैं **यदि और केवल यदि** $1 = f(x)r(x) + g(x)s(x)$, किन्हीं $r(x), s(x) \in F[x]$ के लिए।

उपपत्ति: हम उपपत्ति आपके लिए छोड़ रहे हैं (देखिए E30)। ■

प्रमेय 9 हमें बताता है कि किन्हीं दो शून्येतर बहुपदों का एक g.c.d होता है।

आइए एक उदाहरण पर विचार करें।

उदाहरण 7: $\mathbb{R}[x]$ में $(x-5, 2x+1)$ ज्ञात कीजिए।

हल: क्योंकि $2(x-5) - (2x+1) = -11$, इसलिए
$$1 = \frac{(-2)}{11}(x-5) + \frac{1}{11}(2x+1).$$
अतः, उपप्रमेय 2 द्वारा, $(x-5, 2x+1) = 1.$
इस प्रकार, $\mathbb{R}[x]$ में $(x-5)$ और $(2x+1)$ सापेक्षतः अभाज्य हैं।

***

ध्यान दीजिए कि g.c.d की उपरोक्त परिभाषा का n बहुपदों के लिए निम्नलिखित तरीक़े से व्यापकीकरण किया जा सकता है।

परिभाषा: मान लीजिए F एक क्षेत्र है तथा $F[x]$ के $f_1(x), f_2(x), \ldots, f_n(x)$ शून्येतर अवयव हैं।**एकगुणांकी** बहुपद $g(x) \in F[x]$, $f_1(x), \ldots, f_n(x)$ का **महत्तम समापवर्तक** कहलाता है, यदि

i) $g(x) \mid f_i(x)\ \forall\ i = 1, \ldots, n$, तथा

ii) जब भी $h(x) \mid f_i(x)\ \forall\ i = 1, \ldots, n$, तो $h(x) \mid g(x)$.

आगे, जैसा कि प्रमेय 9 में दिया गया है, $\mathbf{f_1(x),\ldots,f_n(x)}$ **के g.c.d** का अस्तित्व है, तथा यह $\sum_{i=1}^{n} \mathbf{f_i(x)h_i(x)}$ के रूप का होता है, किन्हीं $h_i(x) \in F[x]$ के लिए, $i = 1,\ldots,n.$

उदाहरणार्थ, $2x^2 + x(2\sqrt{3}+\sqrt{2}) + \sqrt{6}$, $x^3 + 3\sqrt{3}$ और $7x^4 + 7\sqrt{3}x^3 + 5x^2 + 5\sqrt{3}x \in \mathbb{R}[x]$ का g.c.d बहुपद $x+\sqrt{3}$ है, क्योंकि $x+\sqrt{3}$ इनका एक सार्वभाजक है जो एकगुणांकी है, तथा अन्य सार्वभाजक केवल $\mathbb{R}^*$ के अवयव हैं।

अब, जैसा कि $\mathbb{Z}$ की स्थिति में है, सापेक्षतः अभाज्य बहुपदों के अति उपयोगी गुण होते हैं। आइए हम कुछ को सिद्ध करें।

प्रमेय 10: मान लीजिए F एक क्षेत्र है, तथा $f(x) \in F[x], f(x) \neq 0.$ यदि $g(x), h(x) \in F[x]$ सापेक्षतः अभाज्य हैं, तथा दोनों $f(x)$ के भाजक हैं, तो $f(x)$ को $g(x)h(x)$ विभाजित करता है।

उपपत्ति: हम जानते हैं कि किन्हीं $\alpha(x), \beta(x) \in F[x]$ के लिए,
$1 = g(x)\alpha(x) + h(x)\beta(x).$
अतः, $f(x) = f(x)g(x)\alpha(x) + f(x)h(x)\beta(x).$ …(7)
क्योंकि $g(x) \mid f(x)$, और $h(x) \mid f(x)$, $f(x) = g(x)r(x)$ और $f(x) = h(x)s(x)$, किन्हीं $r(x), s(x) \in F[x]$ के लिए।
इस प्रकार, $f(x)$ के इन मानों को (7) में प्रतिस्थापित करने पर, हम प्राप्त करते हैं:

$$\begin{aligned} f(x) &= h(x)s(x)g(x)\alpha(x) + g(x)r(x)h(x)\beta(x) \\ &= g(x)h(x)[s(x)\alpha(x) + r(x)\beta(x)]. \end{aligned}$$

अतः, $g(x)h(x) \mid f(x)$ in $F[x]$. ■

अब, आप कुछ संबंधित गुणों को सिद्ध क्यों नहीं कर लेते?

E30) उपप्रमेय 2 को सिद्ध कीजिए।

E31) सिद्ध कीजिए कि यदि F एक क्षेत्र है तथा $a, b \in F, a \neq b$ के साथ, तो $F[x]$ में $x+a$ और $x+b$ असहभाज्य हैं।

E32) पुष्टि करते हुए, $\mathbb{Z}_{13}[x]$ में एक ऐसे त्रिघात बहुपद और चतुर्थघात बहुपद का उदाहरण दीजिए जो असहभाज्य हैं।

E33) मान लीजिए F एक क्षेत्र है तथा $f(x), g(x), h(x) \in F[x]$. सिद्ध कीजिए कि

i) यदि $f(x)$ और $g(x)$ सापेक्षतः अभाज्य हैं, तथा $f(x)$ और $h(x)$ सापेक्षतः अभाज्य हैं, तो $f(x)$ और $g(x)h(x)$ सापेक्षतः अभाज्य होते हैं।

ii) यदि $f(x) \neq 0, f(x) \mid g(x)h(x)$ तथा $(f(x), g(x)) = 1$, तो $f(x) \mid h(x).$
(यह इकाई 1 के प्रमेय 6 में $\mathbb{Z}$ के लिए दिए गुण के अनुरूप है।)

अब, यदि आपको $\mathbb{Q}[x]$ में $(3x^5 - \frac{1}{3}x^4 + 5x^2 + x + \frac{7}{5})$ और $(\frac{2}{7}x^3 - 3x^2 + 1)$ का g.c.d ज्ञात करने को कहा जाए, तो आप ऐसा करने के लिए क्या करेंगे? आप सार्वभाजकों को ढूंढने का प्रयास कर सकते हैं, जो आसान काम नहीं होगा। परंतु क्या आपको इकाई 1 का $\mathbb{Z}$ के लिए यूक्लिडीय ऐल्गोरिद्म याद है? ऐसा ही एक ऐल्गोरिद्म $F[x]$

के लिए भी है, जो विभाजन ऐल्गोरिद्म के बार-बार अनुप्रयोग करने पर आधारित है। आइए एक सरल उदाहरण के माध्यम से देखें कि यह क्या है। इससे इस विधि के बारे में आपकी कुछ समझ बन जाएगी।

उदाहरण 8: $\mathbb{Q}[x]$ में (x^3-1) और (x^2-x) का g.c.d ज्ञात कीजिए।

हल: पहले हम (x^3-1) और (x^2-x) पर विभाजन ऐल्गोरिद्म लागू करते हैं। हम प्राप्त करते हैं:

$$x^3-1=(x^2-x)(x+1)+(x-1). \qquad \ldots(8)$$

अब, हम (x^2-x) और (8) के शेषफल, यानी $(x-1)$, पर विभाजन ऐल्गोरिद्म का अनुप्रयोग करते हैं। हम प्राप्त करते हैं:

$$x^2-x=(x-1)x+0. \qquad \ldots(9)$$

हम एक ऐसे चरण पर पहुँच गए हैं, जब शेषफल शून्य है। अतः, इस चरण पर प्राप्त भाजक बहुपद, यानी $(x-1)$, ही g.c.d है। ध्यान दीजिए कि यह बहुपद एकगुणांकी है।

***

ध्यान दीजिए कि यदि उदाहरण 8 के अंतिम चरण पर भाजक बहुपद एकगुणांकी नहीं होता, तो हम उसे एकगुणांकी बनाने के लिए उसके अग्रग गुणांक के प्रतिलोम से गुणा कर लेते, और फिर यह बहुपद g.c.d होता।

अब, निम्नलिखित ऐल्गोरिद्म को ध्यान से देखिए। ऐसे करते हुए ऊपर के उदाहरण को दिमाग़ में रखिए। हम इस पाठ्यक्रम में इस ऐल्गोरिद्म को सिद्ध नहीं करेंगे।

यूक्लिडीय ऐल्गोरिद्म (Euclidean Algorithum): मान लीजिए कि F एक क्षेत्र है, तथा $F[x]$ के $f(x)$ और $g(x)$ दो शून्येतर अवयव हैं। $F[x]$ में $f(x)$ और $g(x)$ पर विभाजन ऐल्गोरिद्म का अनुप्रयोग कीजिए, फिर $g(x)$ और $r_1(x)$ पर कीजिए और फिर $r_1(x)$ और $r_2(x)$ पर करिए, इत्यादि, जब तक कि शेषफल शून्य न आ जाए, जैसा नीचे दिया गया है:

$f(x)=g(x)q_1(x)+r_1(x)$, जहाँ $\deg r_1(x)<\deg g(x)$;

$g(x)=r_1(x)q_2(x)+r_2(x)$, जहाँ $\deg r_2(x)<\deg r_1(x)$;

$r_1(x)=r_2(x)q_3(x)+r_3(x)$, जहाँ $\deg r_3(x)<\deg r_2(x)$;

$\vdots$

$r_{n-2}(x)=r_{n-1}(x)q_n(x)+r_n(x)$, जहाँ $\deg r_n(x)<\deg r_{n-1}(x)$;

$r_{n-1}(x)=r_n(x)q_{n+1}(x)$.

तब, $f(x)$ और $g(x)$ का g.c.d, $a^{-1}r_n(x)$ है, जहाँ $r_n(x)$ का अग्रग गुणांक a है। ■

अब आपकी यूक्लिडीय ऐल्गोरिद्म की कुछ समझ बन गई होगी। आइए इसके अनुप्रयोग के कुछ और उदाहरण देखें।

उदाहरण 9: $(f(x), g(x))$ ज्ञात कीजिए, जहाँ $\mathbb{Z}_3[x]$ में $f(x)=x^4+\bar{2}x^3+x+\bar{2}$ और $g(x)=\bar{2}x^2+\bar{1}$.

हल: पहले, $x^4+\bar{2}x^3+x+\bar{2}=(\bar{2}x^2+\bar{1})(\bar{2}x^2+x+\bar{2})+\bar{0}$.

पहले ही चरण में हमें शेषफल $\bar{0}$ प्राप्त हो गया है, तथा भागफल है $\bar{2}x^2+\bar{1}$. अतः, $\mathbb{Z}_3[x]$ में g.c.d है $\bar{2}^{-1}(\bar{2}x^2+\bar{1})$.

क्योंकि $\bar{2}^{-1} = \bar{2}$, इसलिए g.c.d है $\bar{2}(\bar{2}x^2 + \bar{1})$, अर्थात्, $x^2 + \bar{2}$.

***

उदाहरण 10: $\mathbb{Q}[x]$ में $f(x) = 2x^5 - 3x + 1$ और $g(x) = 2x^3 + 1$ का g.c.d ज्ञात कीजिए।

हल: हम $f(x)$ और $g(x)$ पर विभाजन ऐल्गोरिद्म का अनुप्रयोग करते हैं, तथा प्राप्त करते हैं:

$2x^5 - 3x + 1 = (2x^3 + 1)(x^2) + (-x^2 - 3x + 1).$

आगे, हम $2x^3 + 1$ और $(-x^2) - 3x + 1)$ पर विभाजन ऐल्गोरिद्म लागू करते हैं। हम प्राप्त करते हैं :

$2x^3 + 1 = (-x^2 - 3x + 1)(-2x + 6) + (20x + 7).$

इसी तरह हम विभाजन ऐल्गोरिद्म लागू करते जाते हैं, जैसे नीचे दिया गया है।

$$-x^2 - 3x + 1 = (20x + 7)\left(-\frac{1}{20}x - \frac{53}{400}\right) + \frac{771}{400},$$

$$20x + 7 = \frac{771}{400}\left(\frac{8000}{771}x + \frac{2800}{771}\right).$$

$\therefore$ g.c.d है $\left(\frac{771}{400}\right)\left(\frac{771}{400}\right)^{-1}$, क्योंकि इसे एकगुणांकी होना चाहिए।

अर्थात्, $(f(x), g(x)) = 1.$

***

अब आप कुछ स्थितियों में स्वयं ही g.c.d क्यों नहीं ज्ञात कर लेते?

E34) $\mathbb{Q}[x]$ में $x^{10} - 3x^9 + 3x^8 - 11x^7 + 11x^6 - 11x^5 + 19x^4 - 13x^3 + 8x^2 - 9x + 3$ और $x^6 - 3x^5 + 3x^4 - 9x^3 + 5x^2 - 5x + 2$ का g.c.d ज्ञात कीजिए।

E35) $\mathbb{Z}_5[x]$ में $\bar{4}x^4 + \bar{2}x^2 - \bar{4}x + \bar{2}$ और $\bar{2}x^2 + \bar{2}x - \bar{1}$ का g.c.d ज्ञात कीजिए।

आइए अब $\mathbb{Z}$ के एक गुण से मिलते-जुलते $F[x]$ के एक और गुण की चर्चा करें।

15.5 बहुपद वलयों में गुणजावलियाँ

आइए अब $F[x]$ में गुणजावलियों की बीजीय संरचना की चर्चा करें, जहाँ F एक क्षेत्र है। आप जानते हैं कि $\mathbb{Z}$ में कोई भी गुणजावली एक मुख्य गुणजावली होती है। आप यह भी जानते हैं कि यह किसी भी क्षेत्र के लिए सत्य है। क्या यह $F[x]$ के लिए भी सत्य है, जहाँ F एक क्षेत्र है? इसका उत्तर हाँ है, जैसा कि अब आप देखेंगे।

प्रमेय 11: $F[x]$ की प्रत्येक गुणजावली एक मुख्य गुणजावली होती है, जहाँ F एक क्षेत्र है।

उपपत्ति: मान लीजिए $F[x]$ की I एक गुणजावली है। यदि $I = \{0\}$, तब $I = \langle 0 \rangle$, जो एक मुख्य गुणजावली है।

अतः, मान लीजिए कि $I \neq \{0\}$.

मान लीजिए $S = \{n \in \mathbb{N} \cup \{0\} \mid \text{किसी } f(x) \in I \text{ के लिए } \deg f(x) = n\}$.

क्योंकि $I \neq \{0\}$, इसलिए $S \neq \emptyset$. अतः, सुक्रमण सिद्धांत द्वारा, S का एक लघुतम अवयव, मान लीजिए, m होगा, तथा किसी $g(x) \in I$ के लिए $\deg g(x) = m$.
अतः, $< g(x) > \subseteq I$.

हम दर्शाएँगे कि $I = < g(x) >$.
इसके लिए, मान लीजिए $f(x) \in I$. तब, विभाजन ऐल्गोरिद्म द्वारा $\exists\, q(x), r(x) \in F[x]$
s.t. $f(x) = g(x)q(x) + r(x)$, जहाँ $r(x) = 0$ या $\deg r(x) < \deg g(x)$.
मान लीजिए यदि संभव है तो, कि $r(x) \neq 0$. तब,
$r(x) = f(x) - g(x)q(x) \in I$, क्योंकि $f(x), g(x) \in I$.
परंतु $\deg r(x) < \deg g(x)$, जो उस विधि का अंतर्विरोध करता है जिससे $g(x)$ को चुना गया है।
अतः, $r(x) \neq 0$ संभव नहीं है।
इस प्रकार, $r(x) = 0$.
अतः, $f(x) \in < g(x) >$, अर्थात्, $I \subseteq < g(x) >$.

इस प्रकार, $I = < g(x) >$. ■

प्रमेय 11 के संदर्भ में, आपको इसमें दी गई महत्वपूर्ण बात पर ध्यान देना चाहिए।

टिप्पणी 4: $F[x]$ में कोई भी गुणजावली I उसके में न्यूनतम घात वाले किसी बहुपद द्वारा जनित होती है।

आइए अब $F[x]$ में गुणजावलियों के कुछ उदाहरणों पर विचार करें।

उदाहरण 11: मान लीजिए $\mathbb{R}$ पर शून्य अचर पद वाले बहुपदों का समुच्चय S है। जाँच कीजिए कि $\mathbb{R}[x]$ की S एक उच्चिष्ठ गुणजावली है या नहीं।

हल: पहले आपको इसकी जाँच करनी चाहिए कि $S \neq \emptyset$.
आगे, आपको जाँच करनी चाहिए कि $\mathbb{R}[x]$ का S एक उपवलय है। यहाँ, ध्यान दीजिए कि किसी भी $f(x) \in S$ के लिए,
$f(x) = a_1x + a_2x^2 + \cdots + a_nx^n = x(a_1 + a_2x + \cdots + a_nx^{n-1})$. इस प्रकार,
$f(x) \in < x >$.
$\therefore S \subseteq < x >$.

अब, किसी भी $f(x) \in S$ और $g(x) \in \mathbb{R}[x]$ के लिए
$f(x)g(x) = x(a_1 + a_2x + \cdots a_nx^{n-1})g(x)$ में कोई अचर पद नहीं है।
अतः, $f(x)g(x) \in S$.
इस प्रकार, $\mathbb{R}[x]$ की S एक गुणजावली है।
साथ ही, $x \in S$, जिससे कि $< x > \subseteq S$.

इस प्रकार, $S = < x >$.

आगे, $\phi : \mathbb{R}[x] \to \mathbb{R} : \phi\left(\sum_{i=0}^{n} a_ix^i\right) = a_0$ परिभाषित कीजिए।
तब, आपको जाँच करनी चाहिए कि ϕ एक सुपरिभाषित वलय समाकारिता है,
$\operatorname{Im} \phi = \mathbb{R}$ तथा $\operatorname{Ker} \phi = < x >$.
इस प्रकार, समाकारिता के मूल प्रमेय द्वारा, $\mathbb{R}[x] \big/ < x > \simeq \mathbb{R}$, जो एक क्षेत्र है।

अतः, इकाई 14 के प्रमेय 14 से, $\mathbb{R}[x]$ की $<x>$ एक उच्चिष्ठ गुणजावली है, अर्थात् $\mathbb{R}[x]$ की S एक उच्चिष्ठ गुणजावली है।

***

उदाहरण 12: पुष्टि करते हुए, $F[x]$ (जहाँ F एक क्षेत्र है) में एक गुणजावली का उदाहरण दीजिए, जो

i) एक अभाज्य गुणजावली है परंतु उच्चिष्ठ गुणजावली नहीं है;

ii) अभाज्य गुणजावली नहीं है।

हल: i) क्या $<0>$ इस प्रतिबंध को संतुष्ट करता है? इसका उत्तर देने के लिए, जाँच कीजिए कि $F[x]/<0>$ एक प्रांत और/या एक क्षेत्र है या नहीं। यहाँ, इकाई 13 से याद कीजिए कि किसी भी वलय R के लिए, $R/<0> \simeq R$.

ii) $I = <x(x+1)>$ लीजिए।
मान लीजिए $x \in I$. तब, किसी $f(x) \in F[x]$ के लिए, $x = x(x+1)f(x)$.
अतः, निरसन नियम द्वारा, $(x+1)f(x) = 1$.
दोनों पक्षों में घातों की तुलना करने पर, हम पाते हैं
$1 + \deg f(x) = 0$.
परंतु, $\deg f(x) \geq 0$. अतः, हम एक अंतर्विरोध पर पहुँचते हैं। अतः, $x \notin I$.
इसी प्रकार, आपको दर्शाना चाहिए कि $x+1 \notin I$.
इस प्रकार, $x(x+1) \in I$ परंतु $x \notin I, x+1 \notin I$.
अतः, $F[x]$ की I एक अभाज्य गुणजावली नहीं है।

***

अब शायद आप सोच रहे होंगे कि क्या प्रमेय 11 क्षेत्रों के अलावा किसी भी पर बहुपदों के वलय के लिए भी सत्य है। एक उदाहरण पर विचार कीजिए।

उदाहरण 13: दर्शाइए कि $\mathbb{Z}[x]$ में गुणजावली $<x, 2>$ एक मुख्य गुणजावली नहीं है।

$\mathbb{Z}[x]$ की प्रत्येक गुणजावली मुख्य गुणजावली नहीं है।

हल: आप जानते हैं कि $\mathbb{Z}[x]$ एक प्रांत है, क्योंकि $\mathbb{Z}$ एक प्रांत है। हम अंतर्विरोध द्वारा दर्शाएँगे कि किसी $f(x) \in \mathbb{Z}[x]$ के लिए, $<2, x> \neq <f(x)>$.
अतः, मान लीजिए, यदि संभव हो तो, $\exists\, f(x) \in \mathbb{Z}[x]$ s.t. $<2, x> = <f(x)>$.
क्योंकि $2 \in <f(x)>$, $f(x) \neq 0$.
साथ ही, $\exists\, g(x), h(x) \in \mathbb{Z}[x]$ s.t.
$2 = f(x)g(x)$ और $x = f(x)h(x)$.
इस प्रकार, $\deg f(x) + \deg g(x) = \deg 2 = 0$, तथा …(10)
$\deg f(x) + \deg h(x) = \deg x = 1$. …(11)
(10) से प्रदर्शित होता है कि $\deg f(x) = 0$, अर्थात्, $f(x) \in \mathbb{Z}^*$, मान लीजिए $f(x) = n$.
तब, (11) से प्रदर्शित होता है कि $\deg h(x) = 1$. मान लीजिए $h(x) = ax + b$.
$a, b \in \mathbb{Z}$ के लिए, $a \neq 0$.
तब, $x = f(x)h(x) = n(ax+b)$.
समीकरण के दोनों पक्षों में गुणांकों की तुलना करने पर हम देखते हैं कि
$na = 1$ तथा $nb = 0$.
इस प्रकार, $\mathbb{Z}$ में n एक मात्रक है, अर्थात् $n = \pm 1$.
अतः, $1 \in <f(x)> = <x, 2>$. इस प्रकार,
$1 = x(a_0 + a_1 x + \cdots + a_r x^r) + 2(b_0 + b_1 x + \cdots + b_s x^s)$, जहाँ
$a_i, b_j \in \mathbb{Z}\ \forall\ i = 0, 1, \ldots, r$ और $j = 0, 1, \ldots, s$.

अब, दोनों पक्षों में अचर पदों की तुलना करने पर हम देखते हैं कि $1 = 2b_0$. यह संभव नहीं है, क्योंकि $\mathbb{Z}$ में 2 व्युत्क्रमणीय नहीं है। अतः, हम एक अंतर्विरोध पर पहुँचते हैं। इस प्रकार, $< x, 2 >$ एक मुख्य गुणजावली नहीं है।

***

अब, आइए एक अन्य गुण पर विचार करें जो $\mathbb{Z}$ और $F[x]$ दोनों में है। यह प्रमेय 11 से संबंधित है।

प्रमेय 12: मान लीजिए F एक क्षेत्र है तथा $F[x]$ के $f(x), g(x)$ शून्येतर अवयव हैं। तब, $< f(x), g(x) > = < d(x) >$, जहाँ $d(x) = (f(x), g(x))$.

उपपत्ति: प्रमेय 11 द्वारा, आप जानते हैं कि किसी $h(x) \in F[x]$ के लिए,
$< f(x), g(x) > = < h(x) >$. अतः, $f(x) \in < h(x) >$ और $g(x) \in < h(x) >$,
अर्थात्, $h(x) \mid f(x)$ और $h(x) \mid g(x)$.
$\therefore h(x) \mid d(x)$. ...(12)
साथ ही, क्योंकि $d(x) \mid f(x)$ और $d(x) \mid g(x)$ है, इसलिए $< f(x), g(x) >$ के प्रत्येक अवयव को $d(x)$ विभाजित करता है, E29 द्वारा।
$\therefore d(x) \mid h(x)$. ...(13)
(12) और (13) द्वारा, $d(x) = ah(x)$, जहाँ $a \in F^*$, प्रमेय 8 के अनुप्रयोग से।
$\therefore < f(x), g(x) > = < a^{-1}d(x) > = < d(x) >$. ■

प्रमेय 12 बहुत उपयोगी है। जैसे कि, इससे और उदाहरण 8 से आप जानते हैं कि $\mathbb{Q}[x]$ में $< x^3 - 1, x^2 - x > = < x - 1 >$.
इसी प्रकार, उदाहरण 9 से आप जानते हैं कि $\mathbb{Z}_3[x]$ में
$< x^4 + \overline{2}x^3 + x + \overline{2}, \overline{2}x^2 + \overline{1} > = < x^2 + \overline{2} >$.

अब आपको कुछ प्रश्न हल करने चाहिए।

E36) जाँच कीजिए कि $\mathbb{C}[x]$ की $< x^2 + 1 >$ एक उच्चिष्ठ गुणजावली है या नहीं।

E37) $\mathbb{Q}[x]$ में $< 3x + x^2 + 2, -\frac{1}{2}x^3 + x^5 + 1 >$ का एक जनक ज्ञात कीजिए। क्या यह गुणजावली $\mathbb{Q}[x]$ की एक अभाज्य गुणजावली है? क्यों, या क्यों नहीं?

E38) दर्शाइए कि $< x, x^2, x^3, \ldots, x^{n-1}, x^n - 1 > = F[x]$, जहाँ $n \geq 2$ तथा F एक क्षेत्र है।

E39) $\mathbb{Z}_{11}[x]$ में ऐसे $f(x)$ और $g(x)$ ज्ञात कीजिए जहाँ प्रत्येक की घात ≥ 2 और $< f(x), g(x) > = \mathbb{Z}_{11}[x]$.

इसके साथ ही हम बहुपद वलयों पर अपनी परिचयात्मक चर्चा के अंत पर पहुँच गए हैं। अगली इकाई में आप इस विषय पर कुछ और गहराई में जाएँगे। आप एक क्षेत्र पर बहुपदों के मूलों और गुणनखंडों के बारे में अध्ययन करेंगे।

आइए अब देखें कि इस इकाई में हमने किन बिंदुओं पर चर्चा की है।

15.6 सारांश

इस इकाई में आपने निम्नलिखित बिंदुओं का अध्ययन किया है।

1) वलय पर बहुपद की परिभाषा, और उदाहरण।

2) वलय R पर बहुपदों का समुच्चय, R[x] की वलय संरचना।

3) R एक तत्समकी क्रमविनिमेय वलय है यदि ओर केवल यदि R[x] एक तत्समकी क्रमविनिमेय वलय है।

4) R एक पूर्णांकीय प्राँत है यदि और केवल यदि R[x] एक पूर्णांकीय प्राँत है।

5) मान लीजिए F एक क्षेत्र है। तब,

   i) F[x] एक क्षेत्र नहीं है,

   ii) F[x] का विभाग क्षेत्र F(x) है।

6) मान लीजिए D एक प्रॉंत है, जिसका विभाग क्षेत्र F है। तब D[x] का विभाग क्षेत्र F(x) है, जो F पर परिमेय फलनों का क्षेत्र है।

7) F[x] में विभाजन ऐल्गोरिद्म, जहाँ F एक क्षेत्र है। यह कहता है कि यदि $f(x), g(x) \in F[x],\ g(x) \neq 0,$ तो अद्वितीय $q(x), r(x) \in F[x]$ का अस्तित्व है, जिससे कि $f(x) = q(x)g(x) + r(x)$, जहाँ $r(x) = 0$ या $\deg r(x) < \deg g(x)$.

8) F[x] में एक बहुपद $g(x)$ को एक बहुपद $f(x)$ विभाजित करता है iff $f(x)h(x) = g(x)$ किसी $h(x) \in F[x]$ के लिए।

9) मान लीजिए कि F एक क्षेत्र है। F पर किन्हीं दो बहुपदों का एक अद्वितीय g.c.d होता है। साथ ही, $f(x), g(x) \in F[x] \setminus \{0\}$ के लिए, $(f(x), g(x)) = f(x)r(x) + g(x)s(x)$. किन्हीं $r(x), s(x) \in F[x]$, के लिए।

10) F[x] में दो शून्येतर बहुपदों का g.c.d ज्ञात करने के लिए यूक्लिडीय ऐल्गोरिद्म, जहाँ F एक क्षेत्र है।

11) F[x] में प्रत्येक गुणजावली एक मुख्य गुणजावली होती है, जहाँ F एक क्षेत्र है। यह D[x] के लिए सत्य नहीं है, जहाँ D एक प्राँत है, परंतु क्षेत्र नहीं है।

12) मान लीजिए F एक क्षेत्र है, तथा F[x] के $f(x), g(x)$ शून्येतर अवयव हैं। तब, $< f(x), g(x) > = < d(x) >,$ जहाँ $d(x) = (f(x), g(x))$.

15.7 हल / उत्तर

E1) (i), (iii), (iv), (vi) और (viii) बहुपद हैं।
(ii) और (v) बहुपद नहीं हैं, क्योंकि इनमें x के ऋणात्मक और भिन्नात्मक घात शामिल हैं; (vii) एक बहुपद नहीं है, क्योंकि इसमें अनंततः अनेक शून्येतर पद हैं।
(i), (vi) और (viii), $\mathbb{Z}[x]$ में हैं।

E2) $a_0 = \frac{1}{2}, b_2 = 5, b_3 = \sqrt{3}, b_1 = 0 = b_4.$

E3) घात क्रमशः 1, 3, 4, 3 और अपरिभाषित हैं।

प्रथम चार के अग्रग गुणांक क्रमशः $\sqrt{2}, -7, 1, \frac{1}{7}$ हैं।

0 का कोई अग्रग गुणांक नहीं है।

E4) आप देख चुके हैं कि $R[x]$ में योग सुपरिभाषित है। आगे, यदि

$f(x) = \sum_{i=0}^{n} a_i x^i, \ g(x) = \sum_{i=0}^{m} b_i x^i$, तो $f(x) + g(x) = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$,

एक परिमित योग।

क्योंकि $a_i, b_i \in R, a_i + b_i \in R \ \forall \ i = 0, 1, \ldots, \max(n, m).$

$\therefore f(x) + g(x) \in R[x].$

जैसा योग के लिए किया था, यदि $R[x]$ में $f(x) = f'(x)$ और $g(x) = g'(x)$, तो दर्शाइए कि $f(x) \cdot g(x) = f'(x) \cdot g'(x)$ क्यों है, अर्थात् क्यों गुणन सुपरिभाषित है।

तब, स्पष्ट कीजिए कि यदि $f(x), g(x) \in R[x]$, तो क्यों $f(x) \cdot g(x) \in R[x]$.

E5) i) $2 + 5x + 3x^2 + (4+1)x^3 = 2 + 5x + 3x^2 + 5x^3.$

ii) $(\overline{6} + \overline{1}) - \overline{2}x + \overline{2}x^2 + \overline{5}x^3 = -\overline{2}x + \overline{2}x^2 + \overline{5}x^3$, क्योंकि $\overline{7} = \overline{0}$.

$= \overline{5}x + \overline{2}x^2 + \overline{5}x^3$, क्योंकि $-\overline{2} = \overline{5}$.

iii) $(1 \cdot 1) + (1 \cdot 2 + 1 \cdot 1)x + (1 \cdot 1 + 1 \cdot 2 + 0 \cdot 1)x^2 = 1 + 3x + 3x^2 + x^3.$

iv) $\overline{1} + x^3$, क्योंकि $\overline{3} = \overline{0}$.

v) $10x + 5x^2 + 7x^3 + x^4 + x^5.$

E6) प्रत्येक पद $a_i x^i$ एक परिमित योग है, तथा $a_i \in R$. इस प्रकार, $a_i x^i \in R[x]$.

E7) i) सत्य; उदाहरणार्थ, $\mathbb{Z}_6[x]$ में $(\overline{2}x)(\overline{3}x + 1) = \overline{0} \cdot x^2 + \overline{2}x = \overline{2}x$.

ii) सत्य; मान लीजिए कि $\mathbb{Q}[x]$ में $f(x) = a + bx + cx^2$ और $g(x) = p + qx + rx^2$ हैं, जहाँ $c \neq 0, r \neq 0$. क्योंकि $\mathbb{Q}$ एक क्षेत्र है, इसलिए $cr \neq 0$.

साथ ही, उच्चतम घात वाला पद crx^4 है।

इस प्रकार, $f(x)g(x)$ एक चतुर्थघात बहुपद है।

iii) असत्य; उदाहरणार्थ, यदि $f(x) = a + bx + cx^2 \in \mathbb{C}[x]$, तो $f(x) + (-f(x)) = 0$, जो एक द्विघात बहुपद नहीं है।

iv) असत्य; उदाहरणार्थ, यदि $\mathbb{Z}[x]$ में $p(x) = x$ और $q(x) = 2x^2$, तो $p(x)$ एक एकगुणांकी बहुपद है, परंतु $p(x) + q(x)$ का अग्रग गुणांक 2 है।

E8) ऐसे अनंततः अनेक युग्म हैं। एक $\mathbb{M}_2(\mathbb{C})$ पर $f(x)=\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}x$ और

$g(x)=\begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}x$ है।

क्योंकि $f(x)$ और $g(x)$ दोनों रैखिक हैं, तथा इनके अलग-अलग अग्रग गुणांक हैं, इसलिए ये अलग-अलग हैं।

E9) i) R को $R[x]$ में अचर बहुपदों और 0 का समुच्चय माना जा सकता है।
अतः, $R \subset R[x]$.
साथ ही, R और $R[x]$ दोनों समान संक्रियाओं के सापेक्ष वलय हैं।
इस प्रकार, $R[x]$ का R एक उपवलय है।

ii) यह सत्य नहीं है।
उदाहरणार्थ, मान लीजिए $R=\mathbb{Z}$, तथा $x\in\mathbb{Z}[x]$ लीजिए।
तब, किसी भी $r\in\mathbb{Z}^*$ के लिए, $rx\notin\mathbb{Z}$.
अतः, $\mathbb{Z}[x]$ की $\mathbb{Z}$ एक गुणजावली नहीं है।

E10) $\mathbb{Z}_4=\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.
$\mathbb{Z}_4$ पर कोई भी द्विघात बहुपद $a_0+a_1x+a_2x^2$ के रूप का होता है, जहाँ $a_0, a_1, a_2\in\mathbb{Z}_4$.
इस प्रकार, यहाँ $4\times4\times3=48$ संभावनाएँ हैं।
ऐसे बहुपदों के साथ कार्य करने के अभ्यास के लिए, आपको इन सभी की सूची बनानी चाहिए।

E11) नहीं। उदाहरणार्थ, मान लीजिए $R=\mathbb{Q}$ और $n=1$.
तब, $1+x\in\wp_1$, परंतु $(1+x)^2\notin\wp_1$. अतः, $\wp_1$ एक वलय नहीं है, तथा इसी लिए यह $\mathbb{Q}[x]$ का उपवलय नहीं है।

E12) ध्यान दीजिए कि यदि $f(x)\in A$, तो $f(x)=\sum_{i=0}^{n}a_ix^{2i}$, क्योंकि x^{2i-1} का गुणांक $=0$ है $\forall\, i\in\mathbb{N}$.
साथ ही, $f(x)\in A\Rightarrow -f(x)\in A$. (क्यों?)
अब, मान लीजिए कि $f(x)=\sum_{i=0}^{n}a_ix^{2i}, g(x)=\sum_{i=0}^{m}b_ix^{2i}$.
तब, आपको जाँच करनी चाहिए कि $f(x)-g(x)$ तथा $f(x)g(x)$ के विषम घात वाले गुणांक भी शून्य होंगे।
अतः, $f(x)-g(x)\in A$ और $f(x)g(x)\in A$.
इस प्रकार, $R[x]$ का A एक उपवलय है।

E13) i) $R[x]$ का R एक उपवलय है। अतः, R में गुणन भी क्रमविनिमेय है।

ii) $R[x]$ का तत्समक R का अवयव है, तथा इसी लिए यह R का तत्समक है।

E14) मान लीजिए $f(x)\in R[x]$ एक मात्रक है।
तब, $\exists\, g(x)\in R[x]$ s.t. $f(x)g(x)=1$. अतः,
$\deg f(x)+\deg g(x)=\deg 1=0$.

क्योंकि $\deg f(x) \geq 0, \deg g(x) \geq 0$, इसलिए हम $\deg f(x) = 0, \deg g(x) = 0$ प्राप्त करते हैं।

अतः, $f(x) \in R$, तथा यह एक मात्रक है। इस प्रकार, $U(R[x]) \subseteq U(R)$.

अब, क्योंकि $R[x]$ का R एक उपवलय है, इसलिए $U(R) \subseteq U(R[x])$.

इस प्रकार, $U(R) = U(R[x])$.

E15) (i) और (ii), क्योंकि $\mathbb{Z}[\sqrt{-5}]$ और $\mathbb{Z}_7$ प्राँत हैं।

इकाई 14 में आप देख चुके हैं कि $\mathbb{M}_2(\mathbb{Q})$, $C[0, 1]$ और $\wp(X)$ में शून्य के भाजक होते हैं। अतः (iii), (iv) और (v) में शून्य के भाजक हैं।

E16) मान लीजिए $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i \in I[x]$ तथा

$h(x) = \sum_{j=0}^{t} c_j x^j \in R[x]$.

तब, $f(x) - g(x) = f(x) + (-g(x)) = \sum_{i=0}^{\max(m, n)} (a_i - b_i) x^i \in I[x]$, तथा

$f(x)h(x) = \sum_{i=0}^{n+t} (a_i c_0 + a_{i-1} c_1 + \cdots + a_0 c_i) x^i \in I[x]$,

क्योंकि R की I एक गुणजावली है।

इसी प्रकार, $h(x)f(x) \in I[x]$.

अतः, $I[x]$, $R[x]$ की गुणजावली है।

आइए $\phi : R[x] \to (R/I)[x] : \phi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \bar{a}_i x^i$ परिभाषित करें, जहाँ

$\bar{a} = a (\bmod I) \forall a \in R$.

ϕ सुपरिभाषित है: मान लीजिए कि $R[x]$ में $\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} b_i x^i$.

तब, $n = m$ तथा $a_i = b_i \ \forall\ i = 0, 1, \ldots, n$.

अतः, $\bar{a}_i = \bar{b}_i \ \forall\ i = 0, \ldots, n$.

$\therefore (R/I)[x]$ में $\sum_{i=0}^{n} \bar{a}_i x^i = \sum_{i=0}^{m} \bar{b}_i x^i$.

ϕ एक वलय समाकारिता है: मान लीजिए कि $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i$.

तब, $\phi(f(x) + g(x)) = \phi\left(\sum_{i=0}^{t} (a_i + b_i) x^i\right)$, जहाँ $t = \max(m, n)$.

$$= \sum_{i=0}^{t} \overline{(a_i + b_i)} x^i$$

$$= \left(\sum_{i=0}^{n} \bar{a}_i x^i\right) + \left(\sum_{i=0}^{m} \bar{b}_i x^i\right)$$

$$= \phi(f(x)) + \phi(g(x)), \text{ तथा}$$

$\phi(f(x)g(x)) = \phi\left(\sum_{i=0}^{r} c_i x^i\right)$, जहाँ $r = m + n$ और $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

$$= \sum_{i=0}^{r} \bar{c}_i x^i$$

$$= \sum_{i=0}^{r} (\bar{a}_i \bar{b}_0 + \bar{a}_{i-1} \bar{b}_1 + \cdots + \bar{a}_0 \bar{b}_i) x^i$$

$$= \left(\sum_{i=0}^{n} \bar{a}_i x^i \right) \left(\sum_{i=0}^{m} \bar{b}_i x^i \right)$$

$$= \phi(f(x)) \phi(g(x)).$$

ϕ **आच्छादक है:** किसी भी $h(x) = \sum_{i=0}^{n} \bar{a}_i x^i \in (R/I)[x]$ के लिए,

$\exists\, f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ s.t. $\phi(f(x)) = h(x)$.

इस प्रकार, $\text{Im}\, \phi = (R/I)[x]$.

$$\textbf{Ker}\ \phi = \left\{ \sum_{i=0}^{n} a_i x^i \in R[x] \,\middle|\, \sum_{i=0}^{n} \bar{a}_i x^i = \bar{0} \right\}$$

$$= \left\{ \sum_{i=0}^{n} a_i x^i \in R[x] \,\middle|\, \bar{a}_i = \bar{0}\ \forall\ i = 0, \ldots, n \right\}$$

$$= \left\{ \sum_{i=0}^{n} a_i x^i \in R[x] \,\middle|\, a_i \in I\ \forall\ i = 0, \ldots, n \right\}$$

$$= I[x].$$

अब, परिणाम प्राप्त करने के लिए FTH का अनुप्रयोग कीजिए।

E17) मान लीजिए कि $r \in R^*$. मान लीजिए, यदि संभव है, कि $r \in \langle x \rangle$. तब, $r = xf(x)$ किसी $f(x) \in R[x]$, के लिए।
$\therefore 0 = \deg r = \deg x + \deg f(x) \geq 1$, जो एक अंतर्विरोध है।
अतः, $\langle x \rangle \neq R[x]$.

मान लीजिए, यदि संभव है, कि R की किसी उचित गुणजावली I के लिए, $\langle x \rangle = I[x]$.
मान लीजिए $a \in R \setminus I$. तब, $ax \in \langle x \rangle = I[x]$, जो एक अंतर्विरोध है।
इस प्रकार, $\langle x \rangle \neq I[x]$.

E18) मान लीजिए $\text{char}\, R = n$. इकाई 14 के प्रमेय 3 से, आप जानते हैं कि n सबसे छोटा धनात्मक पूर्णांक है जिससे कि $n \cdot 1 = 0$. क्योंकि 1, $R[x]$ का भी तत्समक है, इसलिए इकाई 14 के वही प्रमेय आपको बताता है कि
$\text{char}\, R[x] = n = \text{char}\, R$.

E19) मान लीजिए
$p(x) = a_0 + a_1 x + \cdots + a_n x^n,\ q(x) = b_0 + b_1 x + \cdots + b_m x^m \in R[x]$.

तब, $\phi(p(x) + q(x)) = \phi\left(\sum_{i=0}^{t} (a_i + b_i) x^i \right)$, जहाँ $t = \max(m, n)$.

$$= \sum_{i=0}^{t} f(a_i + b_i) x^i$$

$$= \sum_{i=0}^{t} [f(a_i) + f(b_i)]x^i$$

$$= \sum_{i=0}^{t} f(a_i)\, x^i + \sum_{i=0}^{t} f(b_i) x^i$$

$= \phi(p(x)) + \phi(q(x))$, क्योंकि $f(a_i) = 0 = f(b_j)$

जब भी $a_i = 0,\ b_j = 0.$

साथ ही,, $\phi(p(x)\cdot q(x)) = \phi\left(\sum_{i=0}^{m+n} c_i x^i\right)$, जहाँ $c_i = a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_i$.

$$= \sum_{i=0}^{m+n} f(c_i) x^i$$

$= \sum_{i=0}^{m+n} [f(a_i) f(b_0) + f(a_{i-1}) f(b_1) + \ldots + f(a_0) f(b_i)] x^i$,

क्योंकि f एक वलय समाकारिता है।

$$= \phi(p(x))\phi(q(x)).$$

इस प्रकार, ϕ एक समाकारिता है।

अब, यदि f एक तुल्याकारिता है, तो किसी भी $h(x) = \sum_{i=0}^{n} a_i x^i \in S[x]$ के लिए,

$h(x) = \sum_{i=0}^{n} f(b_i) x^i$, जहाँ $a_i = f(b_i)\ \forall\ i$ क्योंकि f आच्छादक है।

$$= \phi\left(\sum_{i=0}^{n} b_i x^i\right).$$

इस प्रकार, $\text{Im}\ \phi = S[x]$.

दर्शाइए कि $\text{Ker}\ \phi = (\text{Ker}\ f)[x] = \{0\}$, क्योंकि f एकैकी है।

इस प्रकार, ϕ एक तुल्याकारिता है।

E20) पहले, दर्शाइए कि ϕ सुपरिभाषित है।

आगे, यदि $(R \times S)[x]$ में $f(x) = \sum_{i=0}^{n} (a_i, r_i) x^i$ and $g(x) = \sum_{i=0}^{m} (b_i, s_i) x^i$,

तो $\phi(f(x) + g(x)) = \phi\left(\sum_{i=0}^{t} [(a_i, r_i) + (b_i, s_i)] x^i\right)$, $t = \max(m, n)$.

$$= \phi\left(\sum_{i=0}^{t} (a_i + b_i, r_i + s_i) x^i\right)$$

$$= \left(\sum_{i=0}^{t} (a_i + b_i) x^i, \sum_{i=0}^{t} (r_i + s_i) x^i\right)$$

$$= \left(\sum_{i=0}^{t} a_i x^i, \sum_{i=0}^{t} r_i x^i\right) + \left(\sum_{i=0}^{t} b_i x^i, \sum_{i=0}^{t} s_i x^i\right)$$

$$= \phi(f(x)) + \phi(g(x)).$$

इसी प्रकार, दर्शाइए कि $\phi(f(x)g(x)) = \phi(f(x))\phi(g(x))$.

आगे, मान लीजिए कि $(f(x), g(x)) \in R[x]\times S[x]$, जहाँ $\deg f(x) = n$ तथा $\deg g(x) = m$. Suppose $m \ge n$.

तब, $f(x) = \sum_{i=0}^{m} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i$, जहाँ $i > n$ के लिए $a_i = 0$.

तब $\phi\left(\sum_{i=0}^{m}(a_i, b_i)x^i\right) = (f(x), g(x))$.

इस प्रकार, ϕ आच्छादक है।

$$\text{Ker } \phi = \left\{\sum_{i=0}^{n}(a_i, b_i)x^i \in (R\times S)[x] \,\middle|\, a_i = 0 = b_i \;\forall\; i = 0,\ldots,n\right\}$$
$$= \{0\}.$$

इस प्रकार, ϕ एक तुल्याकारिता है।

$\therefore (R\times S)[x] \simeq R[x]\times S[x]$.

E21) i) $\mathbb{Z}[i]$ का विभाग क्षेत्र $\left\{\frac{a+ib}{c+id}\,\middle|\, a, b, c, d \in \mathbb{Z}, c+id \ne 0\right\}$ है।

अब $\frac{a+ib}{c+id} = \frac{(a+ib)(c-id)}{c^2+d^2} = p+iq$, किन्हीं $p, q \in \mathbb{Q}$ के लिए।

इस प्रकार, $\mathbb{Z}[i]$ का विभाग क्षेत्र $\mathbb{Q}[i]$ है।

$\therefore \mathbb{Z}[i][x]$ का विभाग क्षेत्र $\mathbb{Q}[i](x)$ है।

ii) $\mathbb{Q}[\sqrt{11}]$ एक क्षेत्र है, जैसा कि आप इकाई 14 में दर्शा चुके हैं।

$\therefore \mathbb{Q}[\sqrt{11}](x)$ ही वाँछित क्षेत्र है।

iii) $\mathbb{Z}_p(x)$.

E22) $\mathbb{C}[x]$ का कोई भी अवयव $\mathbb{C}(x)$ में भी है। इन अवयवों के अलावा यहाँ

$(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m)^{-1}$, जहाँ $\sum_{i=0}^{m} b_i x^i \ne 0$,

$a_i, b_j \in \mathbb{C}\;\forall\; i = 1,\ldots n;\; j = 1,\ldots,m$ के रूप के सभी अवयव हैं।

इनमें से कोई दो चुनिए, और दर्शाइए कि वे अलग-अलग क्यों हैं।

E23) E18 में आप सिद्ध कर चुके हैं कि $\text{char } \mathbb{Z}_p[x] = \text{char } \mathbb{Z}_p = p$.

अब, $\mathbb{Z}_p(x)$ पर विचार कीजिए। इसका तत्समक $\overline{1}$, जहाँ $p\cdot\overline{1} = \overline{0}$.

इस प्रकार, $\text{char } \mathbb{Z}_p(x) = p$.

साथ ही, $\mathbb{Z}_p(x)$ अपरिमित है, क्योंकि $\mathbb{Z}_p[x]$ अपरिमित है।

E24) i)

$$\begin{array}{r|l} -x^3+\frac{1}{7} & \overline{x^4+1}\;(-x \\ & x^4-\frac{1}{7}x \\ \hline & \frac{1}{7}x+1 \end{array}$$

हम यहाँ रूक जाते हैं, क्योंकि $\deg\left(\frac{1}{7}x+1\right) < \deg\left(-x^3+\frac{1}{7}\right)$.

अतः, $f(x) = (-x)g(x) + \left(\frac{1}{7}x+1\right)$.

यहाँ $q(x) = -x$ और $r(x) = \frac{1}{7}x + 1$.

ii)
$$
\begin{array}{r|l}
 & \bar{2}x^2 \qquad + \bar{1} \\
\hline
\bar{2}x+\bar{1} & x^3+\bar{2}x^2-x+\bar{1} \\
 & \underline{x^3+\bar{2}x^2} \qquad \text{(क्योंकि यहाँ } \bar{4}=\bar{1}) \\
 & \qquad -x+\bar{1} \\
 & \qquad \underline{\bar{2}x+\bar{1}} \\
 & \qquad\qquad \bar{0} \quad \text{(क्योंकि यहाँ } -\bar{1}=\bar{2})
\end{array}
$$

इस प्रकार, $f(x) = (\bar{2}x^2 + \bar{1})\,g(x)$.

$\therefore g(x) \mid f(x)$.

iii) $f(x) = (x^2 + \sqrt{3}x + 3)\,g(x)$.

$\therefore g(x) \mid f(x)$.

E25) ii) क्योंकि $f(x) = 1 \cdot f(x)$ तथा $1 \in F[x]$, इसलिए $f(x) \mid f(x)$.

iii) $f(x) \mid g(x) \Rightarrow \exists\, p(x) \in F[x]$ s.t. $g(x) = f(x)p(x)$

$\Rightarrow ag(x) = af(x)p(x)$, किसी भी $a \in F^*$ के लिए।

$\Rightarrow af(x) \mid ag(x)$.

iv) $g(x) = f(x)p(x)$ and $h(x) = g(x)q(x)$, किन्हीं $p(x), q(x) \in F[x]$ के लिए।

$\therefore h(x) = f(x)p(x)q(x)$, तथा $p(x)q(x) \in F[x]$.

अर्थात्, $f(x) \mid h(x)$.

vi) किन्हीं $p(x), q(x) \in F[x]$ के लिए, $g(x) = f(x)p(x)$ और $h(x) = f(x)q(x)$.

अतः, $g(x) + h(x) = f(x)(p(x) + q(x))$, तथा $p(x) + q(x) \in F[x]$.

$\therefore f(x) \mid (g(x) + h(x))$.

vii) किसी $p(x) \in F[x]$ के लिए, $g(x) = f(x)p(x)$.

$\therefore g(x)h(x) = f(x)p(x)h(x)$, तथा $p(x)h(x) \in F[x]$.

$\therefore f(x) \mid g(x)h(x)$.

E26) $F[x]$ और $R[x]$ के बीच अंतर इनके मात्रकों में है। परंतु उपपत्तियों में, (v) को छोड़ कर, कहीं भी हमने इस तथ्य का उपयोग नहीं किया है, कि F^* का प्रत्येक अवयव एक मात्रक है। (v) की स्थिति में इसे इस प्रकार लिखा जा सकता है: 'यदि $g(x)$ ऐसा है कि $g(x) \neq 0$, $f(x) \mid g(x)$ और $g(x) \mid f(x)$, तो किसी $a \in U(R)$ के लिए, $f(x) = ag(x)$.'

E27) E26 से, किसी $a \in U(R)$ के लिए, $f(x) = ag(x)$.

इस प्रकार, $\deg f(x) = \deg g(x)$.

क्योंकि $f(x)$ और $g(x)$ दोनों के अग्रग गुणांक 1 हैं, इसलिए $a=1$.
इस प्रकार, $f(x)=g(x)$.

E28) ~ सममित नहीं है। उदाहरणार्थ, $\mathbb{Q}[x]$ में $(x-2) \mid (x^2-4)$, परंतु $(x^2-4) \nmid (x-2)$. (क्यों?)

E29) इसे सिद्ध करने के लिए, प्रमेय 8 के (vi) और (vii) का उपयोग कीजिए।

E30) यदि $f(x)$ और $g(x)$ सापेक्षतः अभाज्य हैं, तो $(f(x), g(x))=1$. अतः, किन्हीं $r(x), s(x) \in F[x]$ के लिए $1=f(x)r(x)+g(x)s(x)$.

विलोमतः, हम जानते हैं कि 1, $f(x)$ और $g(x)$ का एकघात संचय है। मान लीजिए $d(x)=(f(x), g(x))$.
क्योंकि $d(x) \mid f(x)$ और $d(x) \mid g(x)$, इसलिए
$d(x) \mid (f(x)r(x)+g(x)s(x))$, अर्थात्, $d(x) \mid 1$, E29 द्वारा।
$\therefore \deg d(x)=0$.
साथ ही, $d(x)$ एकगुणांकी है।
अतः, $d(x)=1$.

E31) $1=\dfrac{1}{(a-b)}(x+a)-\dfrac{1}{(a-b)}(x+b)$. अतः, उपप्रमेय 2 द्वारा, ये असहभाज्य हैं।

E32) उदाहरणार्थ, $f(x)=x^3, g(x)=x^4+\overline{1}$. क्योंकि
$(-x)f(x)+g(x)=\overline{1}$, इसलिए $(f(x),g(x))=\overline{1}$.
ऐसे अनेक उदाहरण हो सकते हैं। कुछ और उदाहरणों को ढूंढिए।

E33) i) $1=f(x)r(x)+g(x)s(x)$ …(14)
$1=f(x)p(x)+h(x)q(x)$ …(15)
किन्हीं $r(x), s(x), p(x), q(x) \in F[x]$ के लिए।
(15) से, हम प्राप्त करते हैं:
$g(x)=f(x)g(x)p(x)+g(x)h(x)q(x)$.
अतः, इसे (14) में रखने पर, हम प्राप्त करते हैं।
$1=f(x)[r(x)+g(x)p(x)s(x)]+g(x)h(x)q(x)s(x)$
$\therefore (f(x), g(x)h(x))=1$.

ii) $1=f(x)r(x)+g(x)s(x)$ …(16)
किन्हीं $r(x), s(x) \in F[x]$ के लिए।
साथ ही, $g(x)h(x)=f(x)p(x)$ …(17)
किसी $p(x) \in F[x]$ के लिए।
अब, (16) से हम प्राप्त करते हैं:
$h(x)=f(x)h(x)r(x)+g(x)h(x)s(x)$
$=f(x)h(x)r(x)+f(x)p(x)s(x)$, (17) से।
$=f(x)\alpha(x)$, जहाँ $\alpha(x)=h(x)r(x)+p(x)s(x) \in F[x]$.
$\therefore f(x) \mid h(x)$.

E34) $x^{10}-3x^9+3x^8-11x^7+11x^6-11x^5+19x^4-13x^3+8x^2-9x+3$
$=(x^6-3x^5+3x^4-9x^3+5x^2-5x+2)(x^4-2x)+(-x^4-3x^3-2x^2-5x+3)$.

तब, $x^6-3x^5+3x^4-9x^3+5x^2-5x+2$
$=(-x^4-3x^3-2x^2-5x+3)(-x^2+6x-19)+(-59x^3-118x+59).$

आगे, $-x^4-3x^3-2x^2-5x+3=(-59x^3-118x+59)\left(\frac{1}{59}x+\frac{3}{59}\right).$

$\therefore$ वाँछित g.c.d $-\frac{1}{59}(-59x^3-118x+59)$ है, क्योंकि g.c.d को एकगुणांकी होना चाहिए।

इस प्रकार, g.c.d (x^3+2x-1) है।

E35) $f(x)=\overline{4}x^4+\overline{2}x^2+x+\overline{2},\ g(x)=\overline{2}x^2+\overline{2}x+\overline{4}$, क्योंकि $-\overline{1}=\overline{4}$.

$\overline{4}x^4+\overline{2}x^2+x+\overline{2}=(\overline{2}x^2+\overline{2}x+\overline{4})(\overline{2}x^2+\overline{3}x+\overline{4})+(x+\overline{3})$,

$\overline{2}x^2+\overline{2}x+\overline{4}=(x+\overline{3})(\overline{2}x+\overline{1})+\overline{1}$,

$(x+\overline{3})=\overline{1}(x+\overline{3})$.

$\therefore (f(x),\ g(x))=\overline{1}$.

E36) $\mathbb{C}[x]$ में $x^2+1=(x+i)(x-i)$.

अतः, $x^2+1\in<x+i>\subsetneq\mathbb{C}[x]$, क्योंकि $1\notin<x+i>$.

मान लीजिए, यदि संभव है, कि $x+i\in<x^2+1>$.

तब $(x+i)=(x^2+1)f(x)$, किसी $f(x)\in\mathbb{C}[x]$ के लिए।

अतः, $1=\deg\,(x+i)=\deg\,(x^2+1)+\deg\,f(x)\geq 2$, जो एक अंतर्विरोध है।

इस प्रकार, $x+i\notin<x^2+1>$.

$\therefore <x^2+1>\neq<x+i>$.

$\therefore <x^2+1>\subsetneq<x+i>\subsetneq\mathbb{C}[x]$.

$\therefore <x^2+1>$, $\mathbb{C}[x]$ उच्चिष्ठ गुणजावली नहीं है।

E37) आपको दिखाना चाहिए कि x^2+3x+2 और $x^5-\frac{1}{2}x^3+1$ असहभाज्य है।

$\therefore <3x+x^2+2,\ -\frac{1}{2}x^3+x^5+1> = <1> = \mathbb{Q}[x].$

इस प्रकार, दी हुई गुणजावली एक उचित गुणजावली नहीं है। अतः, यह एक अभाज्य गुणजावली नहीं है।

E38) $x, x^2,\ldots,x^{n-1}$ का g.c.d x है।

$\therefore$ $x, x^2,\ldots,x^{n-1},\ x^n-1$ का g.c.d वहीं है जो $x,\ x^n-1$ का g.c.d है; और यह 1 है (क्योंकि $x\cdot x^{n-1}-(x^n-1)=1$).

$\therefore <x, x^2,\ldots,x^{n-1},\ x^n-1> = <1> = F[x].$

E39) यहाँ अनेक उत्तर हो सकते हैं। हमारा है $x^2+\overline{10}$, और x^2.

यहाँ $\overline{1}=(\overline{10})^{-1}(x^2+\overline{10}-x^2)$.

अतः, $x^2+\overline{10}$ और x^2 असहभाज्य है।

$\therefore <x^2+\overline{10},\ x^2> = <\overline{1}> = \mathbb{Z}_{11}[x].$

इकाई 16

बहुपदों के मूल और गुणनखंड

इकाई की रूपरेखा

पृष्ठ संख्या

16.1 प्रस्तावना

पिछली इकाई में आपने विभिन्न वलयों पर बहुपदों के साथ कार्य किया है। आपने $F[x]$ में विभाजन ऐल्गोरिद्म का भी अध्ययन किया है, जहाँ F एक क्षेत्र है। इस संदर्भ में आपने भागफलों, शेषफलों तथा एक बहुपद को दूसरे बहुपद से भाग देने की धारणा के साथ भी काम किया है। इस इकाई में हम इस समझ को आगे बढ़ाने में आपकी सहायता करेंगे। ध्यान दीजिए कि **इस इकाई में हम वलयों को क्रमविनिमेय मान कर चल रहे हैं।**

भाग 16.2 में आप अध्ययन करेंगे सीखेंगे कि बहुपद का मूल क्या होता है, तथा यह किस प्रकार बहुपद के गुणनखंड से जुड़ा है। आप यह भी देखेंगे कि एक बहुपद की घात किस प्रकार उसके मूलों की संख्या से संबंधित है। यह संबंध शेषफल प्रमेय से प्राप्त होता है, जैसा कि आप देखेंगे।

अगले भाग, भाग 16.3 में हम आपको किसी क्षेत्र पर खंडनीय और अखंडनीय बहुपदों की धारणा से परिचित कराऐंगे। यहाँ, आप देखेंगे कि $F[x]$ में एक अखंडनीय बहुपद $F[x]$ की एक उच्चिष्ठ गुणजावली जनित करता है। आप यह भी देखेंगे कि $F[x]$ के अखंडनीय अवयव वही हैं जो $F[x]$ के अभाज्य अवयव हैं।

आगे, भाग 16.4 में आप $F[x]$ पर बहुपद के अखंडनीय होने के लिए निकषों का अध्ययन करेंगे, जब F क्षेत्र $\mathbb{Q}, \mathbb{R}$ या $\mathbb{C}$ है। उदाहरणार्थ, आप पाएंगे कि $\mathbb{Q}$ पर अखंडनीय बहुपद किसी भी घात का हो सकता है, जबकि $\mathbb{C}$ पर ऐसे बहुपद केवल घात 1 का हो सकता है।

इकाई 15 में आप देख चुके हैं कि पूर्णांकों के गुणों में तथा किसी क्षेत्र पर बहुपदों के गुणों में बहुत समानता है। भाग 16.5 में हम एक और ऐसी ही समानता, अर्थात् अद्वितीय गुणनखंडन पर विचार करेंगे। आप पाएंगे कि क्षेत्र पर अखंडनीय बहुपद वही भूमिका अदा करते हैं जो $\mathbb{Z}$ में अभाज्य संख्याएँ अदा करती हैं। इसी भाग में आप $F[x]$ में अद्वितीय गुणनखंडन के कुछ निष्कर्षों का भी अध्ययन करेंगे।

इस इकाई को निम्नलिखित सीखने की अपेक्षाओं को ध्यान में रखते हुए बनाया गया है। कृपया इसे ध्यानपूर्वक पढ़ें, तथा जब भी आप किसी प्रश्न पर पहुंचे, उसे उसी समय हल करें।

उद्देश्य

इस इकाई की पढ़ाई के बाद, आप निम्नलिखित करने में समर्थ हो जाएंगेः

- वलय R पर बहुपद के मूल (या शून्यक) को परिभाषित करना, तथा उसके उदाहरण देना;
- शेषफल प्रमेय का कथन देना, उसे सिद्ध करना तथा उसका अनुप्रयोग करना;
- बहुपद के किसी भी मूल के संगत उसके गुणनखंड को परिभाषित करना, तथा उसके उदाहरण देना;
- $F[x]$ के अखंडनीय अवयवों तथा अभाज्य अवयवों को परिभाषित करना, तथा उनके उदाहरण देना, जहाँ F एक क्षेत्र है;
- यह सुनिश्चित करने के लिए कि $\mathbb{C}, \mathbb{R}$ या $\mathbb{Q}$ पर एक दिया हुआ बहुपद अखंडनीय है या नहीं विभिन्न निकषों का अनुप्रयोग करना;
- $F[x]$ के लिए अद्वितीय गुणनखंडन प्रमेय का कथन देना, उसे सिद्ध करना तथा उसका अनुप्रयोग करना, जहाँ F एक क्षेत्र है।

16.2 मूल

'कलन' में, तथा स्कूली गणित में, आप बहुपदों के मूल ज्ञात करते रहे हैं। उदाहरणार्थ, आप जानते हैं कि यदि $x+1=0$, तो $x=-1$. अतः, (-1) बहुपद $x+1$ का एक मूल है। इसी प्रकार, आप जानते हैं कि यदि $\mathbb{C}$ पर ax^2+bx+c एक द्विघात बहुपद है, तो इसके मूल द्विघात सूत्र $\dfrac{-b\pm\sqrt{b^2-4ac}}{2a}$ द्वारा दिए जाते हैं। इस संकल्पना को व्यापकीकृत करने के लिए, आइए औपचारिक रूप से एक पद परिभाषित करें उस प्रक्रिया के लिए जिसका उपयोग आप पहले अनेक बार कर चुके हैं।

परिभाषा: मान लीजिए R एक वलय है तथा $f(x)=a_0+a_1x+\cdots+a_nx^n \in R[x]$. तब, किसी भी $r\in R$ के लिए, हम कहते हैं कि $f(r)=a_0+a_1r+\cdots+a_nr^n \in R$, **$f(x)$ के मान है जो x के स्थान पर r प्रतिस्थापित करने से प्राप्त होता है।**

इस प्रकार, यदि $f(x)=1+x+x^2\in\mathbb{Z}[x]$, तो $f(2)=1+2+4=7$, तथा $f(0)=1+0+0=1$.

आइए, अब एक मूल को, व्यापक रूप में, परिभाषित करें।

परिभाषा: मान लीजिए R एक वलय है। R का अवयव r बहुपद $f(x) \in R[x]$ का एक **मूल (root)** (या एक **शून्यक (zero)**) कहलाता है यदि $f(r) = 0$.

उदाहरणार्थ, यदि $2\mathbb{Z}[x]$ में $f(x) = 12 - 2x - 2x^2$, तो $f(2) = 12 - 4 - 8 = 0$.
अतः, $2\mathbb{Z}$ में $12 - 2x - 2x^2$ का एक मूल 2 है।
साथ ही, क्योंकि $f(-2) = 12 + 4 - 8 \neq 0$, इसलिए $2\mathbb{Z}$ में $12 - 2x - 2x^2$ का (-2) एक मूल नहीं है।

एक अन्य उदाहरण के रूप में, यदि $f(x) = 2x^3 + (1 - 2\pi)x^2 + (5 - \pi)x - 5\pi \in \mathbb{R}[x]$, तो $f(\pi) = 0$. अतः, $\mathbb{R}$ में π, $f(x)$ का एक शून्यक है।

किसी क्षेत्र F पर बहुपदों के लिए, मूल की संकल्पना $F[x]$ में विभाजन ऐल्गोरिद्म से निकट रूप से जुड़ा हुआ है। इसे समझने के लिए, निम्नलिखित महत्वपूर्ण प्रमेय पर विचार कीजिए, जो वास्तव में इकाई 15 में दिए गए विभाजन ऐल्गोरिद्म का उपप्रमेय है।

प्रमेय 1 (शेषफल प्रमेय): मान लीजिए F एक क्षेत्र है। यदि $f(x) \in F[x]$ और $b \in F$, तो एक ऐसा अद्वितीय बहुपद $q(x) \in F[x]$ जिससे कि $f(x) = (x - b)q(x) + f(b)$.

उपपत्ति: मान लीजिए $g(x) = x - b$. तब, $f(x)$ और $g(x)$ पर विभाजन ऐल्गोरिद्म का अनुप्रयोग करने से, $F[x]$ में ऐसे अद्वितीय $q(x)$ और $r(x)$ हैं जिनसे कि

$$\begin{aligned} f(x) &= q(x)g(x) + r(x) \\ &= q(x)(x - b) + r(x), \text{ जहाँ } r(x) = 0 \text{ या } \deg r(x) < \deg g(x) = 1. \end{aligned}$$

अतः, या तो $r(x) = 0$, या $r(x)$, F^* का एक अवयव है।
इस प्रकार, किसी $a \in F$ के लिए, $r(x) = a$.
अतः, $f(x) = (x - b)q(x) + a$.
x के लिए b प्रतिस्थापित करने पर हम प्राप्त करते हैं:
$f(b) = (b - b)q(b) + a = 0 \cdot q(b) + a = a$.
इस प्रकार, $a = f(b)$.
अतः, $f(x) = (x - b)q(x) + f(b)$.
इस प्रकार, शेषफल x के लिए b प्रतिस्थापित करने पर प्राप्त $f(x)$ का मान है।

ध्यान दीजिए कि प्रमेय 1 में $\deg f(x) = \deg\,(x - b) + \deg q(x) = 1 + \deg q(x)$. ■
अतः, $\deg q(x) = \deg f(x) - 1$.

प्रमेय 1 से एक परिणाम तुरंत निकलता है, जो निम्नलिखित है।

उपप्रमेय 1: मान लीजिए F एक क्षेत्र है तथा $f(x) \in F[x]$, जहाँ $\deg f(x) \geq 1$. तब, $f(x)$ का $a \in F$ एक मूल है iff $(x - a) \mid f(x)$.

उपपत्ति: हम उपपत्ति आपके लिए अभ्यास के तौर पर छोड़ रहे हैं (देखिए E1)। ■

आइए देखें कि उपप्रमेय 1 किस प्रकार उपयोगी है। उदाहरणार्थ, अब आप जानते हैं कि $x(x + 1) \in \mathbb{Z}[x]$ के मूल केवल 0 और 1 हैं, क्योंकि केवल x और $x + 1$ इसके रैखिक गुणनखंड हैं।

एक अन्य उदाहरण के रूप में $f(x) = 6x^2 - x - 1 \in \mathbb{Q}[x]$ पर विचार कीजिए। द्विघात सूत्र द्वारा आप जानते हैं कि इसके मूल $\frac{1}{2}$ और $\frac{-1}{3}$ हैं। इस प्रकार, उपप्रमेय 1 द्वारा, $(x - \frac{1}{2})$ और $(x + \frac{1}{3})$, $f(x)$ के गुणनखंड हैं।

अब, क्योंकि $\mathbb{Q}$ में 2 एक मात्रक है, इसलिए $(x - \frac{1}{2}) = (2^{-1})2(x - \frac{1}{2})$. अतः, $2(x - \frac{1}{2})$ भी $f(x)$ का एक गुणनखंड है, अर्थात् $(2x - 1)$, $f(x)$ का एक गुणनखंड है।
इसी प्रकार, $(3x + 1)$, $f(x)$ का एक गुणनखंड है।
क्या आपने इस ओर ध्यान दिया कि $f(x)$ के ये दोनों गुणनखंड $\mathbb{Z}[x]$ में हैं?

अब $(x - 1)^2(x - 2) \in \mathbb{Q}[x]$ पर विचार कीजिए। यहाँ $(x - 1)$ एक दोहरा गुणनखंड है। अतः, 1 दो बार इस बहुपद का मूल है। यह एक उदाहरण है उस अवधारणा की जिसे अब हम परिभाषित करने जा रहे हैं।

परिभाषा: मान लीजिए R एक वलय है तथा $f(x) \in R[x]$. $m \in \mathbb{N}$ के लिए, हम कहते हैं कि $a \in R$, $f(x)$ का **बहुकता (multiplicity) m वाला एक मूल है,** यदि $(x - a)^m \mid f(x)$, परंतु $(x - a)^{m+1} \nmid f(x)$.

उदाहरणार्थ, बहुपद $(x - 3)^2(x + 2) \in \mathbb{Q}[x]$ का 3 बहुकता 2 वाला मूल है, तथा इसी बहुपद का (-2) बहुकता 1 वाला मूल है।

अब, आपको कुछ प्रश्नों को हल करना चाहिए।

E1) उपप्रमेय 1 को सिद्ध कीजिए।

E2) निम्नलिखित बहुपदों के, मूल उनकी बहुकताओं के साथ, ज्ञात कीजिए।

i) $\frac{1}{2}x^2 - \frac{5}{2}x + 3 \in \mathbb{Q}[x]$,

ii) $x^2 + x + \overline{1} \in \mathbb{Z}_3[x]$,

iii) $x^4 + \overline{2}x^3 - \overline{2}x - \overline{1} \in \mathbb{Z}_5[x]$,

iv) $(5x + 3)^2(\sqrt{2} - 4x)^3(ix + 1 - \sqrt{3}i)^{11} \in \mathbb{C}[x]$.

E3) $\mathbb{Z}_{11}$ पर ऐसे बहुपद का उदाहरण दीजिए, जिसके केवल दो अलग-अलग मूल क्रमशः बहुकता 3 और 2 वाले, हैं। अपने उदाहरण की पुष्टि भी कीजिए।

E4) मान लीजिए F एक क्षेत्र है तथा $a \in F$. फलन $\phi : F[x] \to F : \phi(f(x)) = f(a)$ परिभाषित कीजिए। (यह फलन **a पर मूल्यांकन फलन** है, जैसा कि इकाई 13 से जानते हैं।)
दर्शाइए कि

i) ϕ एक आच्छादक वलय समाकारिता है,

ii) $\phi(b) = b \ \forall \ b \in F$,

iii) Ker ϕ, $F[x]$ में उन सभी बहुपदों का समुच्चय है जिनका एक शून्यक a है। साथ ही, Ker ϕ का एक जनक ज्ञात कीजिए।

इस स्थिति में, समाकारिता का मूल प्रमेय क्या कहता है।

E5) मान लीजिए F एक क्षेत्र है। सिद्ध कीजिए कि
$F[x]/\langle x-a\rangle \simeq F[x]/\langle x\rangle \ \forall\, a\in F^*.$

E6) मान लीजिए F एक क्षेत्र है तथा $a_0+a_1x+\cdots+a_nx^n\in F[x]$ का $a\in F^*$ एक मूल है। दर्शाइए कि $a_n+a_{n-1}x+\cdots+a_0x^n\in F[x]$ का a^{-1} एक मूल है। क्या यह तब भी सत्य होगा यदि F के बदले एक ऐसा प्रांँत D लें जो क्षेत्र नहीं है? क्यों?

आइए अब देखें कि हम F[x] में दिए एक बहुपद के सभी मूलों को किस प्रकार प्राप्त कर सकते हैं। जैसा कि आप जानते हैं, यह एक रैखिक या द्विघात बहुपद के लिए संभव है। उच्चतर घातों के बहुपदों के लिए, हम कुछ मूलों को प्रयास- और -भूल विधि (trial-and-error method) द्वारा प्राप्त कर सकते हैं, जैसे आपने E2(iii) में किया था। एक अन्य उदाहरण के रूप में, $f(x)=x^5-2x+1\in\mathbb{R}[x]$ पर विचार कीजिए। हम x के लिए 1 रखकर प्रयास करते हैं, तथा $f(1)=0$ ज्ञात करते हैं। इस प्रकार, हम पाते हैं कि f(x) का 1 एक शून्यक है। परंतु इस विधि से हमें $\mathbb{R}$ में f(x) के सभी मूल शायद न मिल पाएं।

साथ ही, ध्यान दीजिए कि हो सकता है F[x] में किसी बहुपद का F में कोई भी शून्यक न हो। (उदाहरणार्थ, $x^2+1\in\mathbb{R}[x]$ का $\mathbb{R}$ में कोई शून्यक नहीं है, क्योंकि इसके शून्यक i और $-i$ हैं, जो दोनों $\mathbb{C}\setminus\mathbb{R}$ में हैं।)
परंतु हम F[x] में किसी भी बहुपद के F में **मूलों की संख्या** के लिए एक उपरि सीमा दे सकते हैं।

प्रमेय 2: क्षेत्र F पर घात n वाले एक शून्येतर बहुपद के F में अधिकतम n मूल होते हैं।

उपपत्ति: यदि $n=0$, तो घात 0 वाला कोई भी बहुपद एक शून्येतर अचर बहुपद होता है। इस प्रकार, इसके कोई मूल नहीं हैं, तथा इसी लिए इसके F में अधिकत $0(=n)$ मूल हैं।
अतः, आइए मान लें कि $n\ge 1$. हम n पर आगमन नियम का उपयोग करेंगे।
$n\in\mathbb{N}$ के लिए, मान लीजिए कि P(n) विधेय, 'यदि $f(x)\in F[x]$ की घात n है, तो F में f(x) के अधिकतम n मूल होते हैं' है।
हम पहले जाँच करेंगे कि कथन P(1) सत्य है या नहीं।
यदि $f(x)\in F[x]$ s.t. $\deg f(x)=1$, तो $f(x)=a_0+a_1x$, जहाँ $a_0,\ a_1\in F$, तथा $a_1\neq 0$.
अतः, f(x) का एक मूल, अर्थात् $(-a_1^{-1}a_0)\in F$ है क्या इसके और मूल हो सकते हैं?
उपप्रमेय 1 से आप जानते हैं कि इसके और मूल नहीं हो सकते, क्योंकि
$\deg f(x)=1=\deg\,(x+a_1^{-1}a_0)$.
अतः, $n=1$ के लिए, f(x) का ठीक 1 मूल है, तथा यह F में है।
इस प्रकार, P(1) सत्य है।

अब, मान लीजिए कि किसी $m\in\mathbb{N}$ के लिए, P(m) सत्य है।
हम दर्शाएँगे कि $P(m+1)$ सत्य है।
मान लीजिए $f(x)\in F[x]$ s.t. $\deg f(x)=m+1$. हम दर्शाएँगे कि F में f(x) के मूलों की संख्या अधिकतम $m+1$ है।

अब, यहाँ दो संभावनाएँ हैं – या तो $f(x)$ का F में कोई शून्यक नहीं है, या F में $f(x)$ का शून्यक है।
यदि F में $f(x)$ का कोई मूल नहीं है, तो F में $f(x)$ के मूलों की संख्या $0 \le m+1$ है। इस प्रकार, तुच्छ रूप से, F में $f(x)$ के अधिकतम $m+1$ मूल हैं।

आगे, मान लीजिए $f(x)$ का एक मूल $a \in F$ है।
तब, $f(x) = (x-a)g(x)$, जहाँ $\deg g(x) = (m+1)-1 = m$, और $g(x) \in F[x]$.
अतः, आगमन परिकल्पना द्वारा, F में $g(x)$ के अधिकतम m मूल हैं। मान लीजिए कि F में $g(x)$ के भिन्न-भिन्न मूल $a_1, \ldots, a_s$ हैं, जहाँ $s \le m$.
अब, a_i, $g(x)$ का एक मूल है
$\Rightarrow g(a_i) = 0$
$\Rightarrow f(a_i) = (a_i - a)g(a_i) = 0$
$\Rightarrow a_i$ में $f(x)$ काएक मूल है, $F \; \forall \; i = 1, \ldots, s$.
इस प्रकार, $g(x)$ का प्रत्येक मूल $f(x)$ का एक मूल है।
इस प्रकार, F में $f(x)$ के कम से कम $s+1$ मूल $a, a_1, \ldots, a_s$ हैं, जहाँ $s+1 \le m$.
क्या $f(x)$ में F के कोई और मूल हैं? आइए देखें।
अब, $f(x)$ का $b \in F$ एक मूल है
$\Leftrightarrow f(b) = 0$
$\Leftrightarrow (b-a)g(b) = 0$
$\Leftrightarrow b - a = 0$ या $g(b) = 0$, क्योंकि F एक पूर्णांकीय प्रांत है।
इस प्रकार, $f(x)$ का b एक मूल है
$\Leftrightarrow b = a$ या $g(x)$ का b एक मूल है
$\Leftrightarrow b = a, a_1, \ldots, a_s$.
अतः, $f(x)$ के मूल केवल a और $a_1, \ldots, a_s$ हैं।
इस प्रकार, F में $f(x)$ के अधिकतम $m+1$ मूल हैं।
$\therefore P(m+1)$ एक सत्य कथन है।

अतः, $\forall \; n \in \mathbb{N}$ के लिए $P(n)$ सत्य है। अर्थात्, सभी $n \ge 1$ के लिए प्रमेय सत्य है। ■

यहाँ, प्रमेय 2 के बारे में एक महत्वपूर्ण बिंदु पर विचार कीजिए।

टिप्पणी 1: प्रमेय 2 के उपयोग से, आप जानते हैं कि $x^3 - 1 \in \mathbb{Q}[x]$ के $\mathbb{Q}$ में 3 से अधिक मूल नहीं हो सकते हैं। परंतु, इसका $\mathbb{Q}$ में केवल एक ही मूल है, यानी 1. अन्य मूल $\omega = \dfrac{-1+i\sqrt{3}}{2}$ तथा ω^2 हैं जो $\mathbb{C} \setminus \mathbb{Q}$ में हैं। इस प्रकार, प्रमेय 2 के कथन में 'अधिकतम' शब्द महत्वपूर्ण है।

प्रमेय 2 में हमने मूलों की बहुकता की बात नहीं की है। यही बात प्रमेय 2 की निम्नलिखित उपप्रमेय में की गई है।

उपप्रमेय 2: यदि $f(x) \in F[x]$ की घात n है, तो F में $f(x)$ के अधिकतम n अलग-अलग मूल होते हैं, जहाँ F एक क्षेत्र है। ■

हम उपप्रमेय 2 का उपयोग निम्नलिखित महत्वपूर्ण प्रमेय को सिद्ध करने के लिए करेंगे।

प्रमेय 3: मान लीजिए $f(x)$ और $g(x)$ एक क्षेत्र F पर घात n वाले शून्येतर बहुपद हैं। यदि F में $n+1$ ऐसे भिन्न-भिन्न अवयव $a_1, \ldots, a_{n+1}$ है जिनसे कि
$f(a_i) = g(a_i) \ \forall \ i = 1, ..., n+1$, तो $f(x) = g(x)$.

उपपत्ति: बहुपद $h(x) = f(x) - g(x)$ पर विचार कीजिए।
तब $\deg h(x) \le n$, परंतु F में $h(x)$ के $n+1$ भिन्न-भिन्न मूल $a_1, ..., a_{n+1}$ हैं। (क्यों?)
उपप्रमेय 2 द्वारा, यह असंभव है, जब तक कि $h(x)$ शून्य बहुपद न हो, अर्थात्
$f(x) = g(x)$. ■

ध्यान दीजिए कि प्रमेय 3 सत्य नहीं होगा यदि सभी a_i भिन्न-भिन्न नहीं हैं। उदाहरणार्थ, $\mathbb{R}[x]$ में $f(x) = (x-2)^2 (x-3)$ और $g(x) = (x-2)(x-3)^2$ को लीजिए। ये दोनों घात 3 के हैं, परंतु $\mathbb{R}$ में ऐसे 4 अवयव 2, 2, 3, 3 हैं जिन पर $f(x)$ और $g(x)$ के समान मान, 0 हैं।
साथ ही, $f(x) \ne g(x)$.

अब, प्रमेय 2 द्वारा आप जानते हैं कि यदि आपको $\mathbb{R}$ पर घात 25 वाला (मान लीजिए) बहुपद दिया जाए, तो आप $\mathbb{R}$ में इस बहुपद के अधिकतम 25 शून्यक ज्ञात कर सकते हैं। क्या यह, मान लीजिए, $\mathbb{Z}$ के लिए भी सत्य है? या ऐसे वलय के लिए सत्य है जो प्राँत नहीं है? आइए एक उदाहरण को देखें।

उदाहरण 1: सिद्ध कीजिए कि $x^3 + \bar{5}x \in \mathbb{Z}_6[x]$ के 3 से अधिक शून्यक हैं।

हल: क्योंकि $\mathbb{Z}_6$ परिमित है, इसलिए हम इसके सभी अवयवों को एक-एक करके जाँच कर सकते हैं कि इनमें से कौन से $f(x) = x^3 + \bar{5}x$ के मूल हैं।
अतः, प्रतिस्थापन द्वारा, हम प्राप्त करते हैं कि
$f(\bar{0}) = 0 = f(\bar{1}) = f(\bar{2}) = f(\bar{3}) = f(\bar{4}) = f(\bar{5})$.
वस्तुतः, $\mathbb{Z}_6$ का प्रत्येक अवयव $f(x)$ का एक शून्यक है। अतः $f(x)$ के 6 शून्यक हैं, जबकि $\deg f(x) = 3$. इस प्रकार, $\mathbb{Z}_6[x]$ के लिए प्रमेय 2 (तथा इसी लिए प्रमेय 3) सत्य नहीं है।

***

उदाहरण 1 से आप देख सकते हैं कि एक वलय के लिए, जो प्राँत नहीं है, प्रमेय 2 और 3 सत्य नहीं है। परंतु ये प्रमेय एक प्राँत के लिए सत्य हैं, जैसा कि अब आप देखेंगे।

प्रमेय 4: $D[x]$ में घात n वाले शून्येतर बहुपदके D में अधिकतम n मूल होते हैं, जहाँ D एक पूर्णांकीय प्राँत है।

उपपत्ति: मान लीजिए $f(x) \in D[x]$ की घात n है। मान लीजिए कि D का विभाग क्षेत्र F है। तब, $f(x) \in F[x]$. अतः, F में $f(x)$ के अधिकतम n मूल हैं, प्रमेय 2 द्वारा। साथ ही, D में $f(x)$ का कोई भी मूल F में भी एक मूल होगा। इस प्रकार, D में $f(x)$ के n से अधिक मूल नहीं हो सकते। ■

अब, निम्नलिखित प्रश्नों को हल करने का प्रयास कीजिए।

E7) उपप्रमेय 2 को सिद्ध कीजिए।

E8) क्षेत्र F को एक पूर्णांकीय प्राँत D से प्रतिस्थापित करते हुए, प्रमेय 3 के अनुरूप एक कथन दीजिए, तथा उसे सिद्ध कीजिए।

E9) मान लीजिए F एक क्षेत्र है तथा $f(x) \in F[x] \setminus \{0\}$. दर्शाइए कि $F[x]$ में $f(x)$ के अधिकतम n रैखिक गुणनखंड हो सकते हैं।

E10) मान लीजिए p एक अभाज्य संख्या है। $x^{p-1} - \overline{1} \in \mathbb{Z}_p[x]$ पर विचार कीजिए। यह दर्शाने के लिए कि $\mathbb{Z}_p$ का प्रत्येक शून्येतर अवयव $x^{p-1} - \overline{1}$ का एक मूल है, इस तथ्य का उपयोग कीजिए कि $\mathbb{Z}_p$ कोटि p वाला एक समूह है। इस प्रकार, दर्शाइए कि

i) $x^{p-1} - \overline{1} = (x - \overline{1})\,(x - \overline{2}) \ldots (x - \overline{p-1})$, तथा

ii) $(p-2)! \equiv 1 (\text{mod } p)$.

E11) $\mathbb{Z}_5[x]$ में बहुपद $x^4 + \overline{4}$ को रैखिक गुणनखंडों में गुणनखंडित किया जा सकता है। इस गुणनखंडन को ज्ञात कीजिए।

E12) $x^n - 1 \in \mathbb{C}[x]$ के सभी शून्यकों को ज्ञात कीजिए, जहाँ $n \in \mathbb{N}$.

E12 में आपने शायद ध्यान दिया होगा कि $\mathbb{C}[x]$ पर बहुपद के सभी शून्यक $\mathbb{C}$ में स्थित होते हैं। जैसा कि आप जानते हैं, अन्य क्षेत्रों F के लिए, इसका $F[x]$ में बहुपदों के लिए सत्य होना आवश्यक नहीं है। उदाहरणार्थ, यह $F = \mathbb{R}$ के लिए सत्य नहीं है।

आइए अब $F[x]$ के उन अवयवों पर विचार करें जिनके F में मूल नहीं हैं। ये बहुपद कुछ हद तक $\mathbb{Z}$ में अभाज्य संख्याओं के अनुरूप हैं।

16.3 अखंडनीय बहुपद

इकाई 1 से आप जानते हैं कि अभाज्य संख्या $\mathbb{Z}$ का ऐसा 1 के अतिरिक्त शून्येतर अवयव है जो मात्रक नहीं है और जिसका 1 और स्वयं के अतिरिक्त कोई गुणनखंड नहीं है। आप यह भी जानते हैं कि यदि $\mathbb{Z}$ में p एक अभाज्य संख्या है, तो $\mathbb{Z}$ की $p\mathbb{Z}$ एक उच्चिष्ठ गुणजावली है। अतः, क्या इस गुण को $F[x]$ के अभाज्य अवयव भी संतुष्ट करते हैं, जहाँ F एक क्षेत्र है? इकाई 14, प्रमेय 13, से हम जानते हैं कि एक अभाज्य अवयव एक अभाज्य गुणजावली ज़रूर जनित करता है। यह गुणजावली $F[x]$ में उच्चिष्ठ हो सकती है, और नहीं भी। इस भाग में आप सीखेंगे कि ये अभाज्य अवयव क्या हैं। आप यह भी सीखेंगे कि ये $F[x]$ में उच्चिष्ठ गुणजावलियाँ जनित करते हैं।

पहले तो इकाई 15 से याद कीजिए कि $F[x]$ के मात्रक F^* के अवयव हैं। इस प्रकार, **F[x] के मात्र वही हैं जो F[x] में अचर बहुपद हैं।** अतः, $F[x]$ का शून्येतर अवयव, जो मात्रक नहीं है, घात ≥ 1 वाला बहुपद है।

आगे, यदि $F[x]$ में $f(x) \mid g(x)$, तो $\deg f(x) \leq \deg g(x)$. अतः, यदि $g(x)$ का मात्रक और स्वयं के अतिरिक्त कोई गुणनखंड नहीं हैं, तो $g(x) = af(x)$, किसी $a \in F^*$ के लिए।
इसका अर्थ है कि $\deg f(x) = \deg g(x)$.

उदाहरणार्थ, $g(x)=3x+5$ का धनात्मक घात वाला कोई गुणनखंड नहीं है, क्योंकि $\deg g(x)=1$. साथ ही, $\mathbb{R}[x]$ में $x^2+1 \in \mathbb{R}[x]$ का कोई रैखिक गुणनखंड नहीं है, उपप्रमेय 1 द्वारा। परंतु, x^2-1 के $\mathbb{R}[x]$ में गुणनखंड $(x-1)$ और $(x+1)$ हैं, पुनः उपप्रमेय 1 द्वारा। इस पृष्ठभूमि के साथ, आइए $F[x]$ में एक ऐसी संकल्पना को परिभाषित करें जिसमें बहुत कुछ वैसे ही गुण होते हैं जो $\mathbb{Z}$ में एक अभाज्य संख्या के होते हैं।

परिभाषा: मान लीजिए F एक क्षेत्र है। तब शून्येतर बहुपद $p(x) \in F[x]$, जो एक मात्रक नहीं है,

i) $F[x]$ में **अखंडनीय (irreducible)** कहलाता है यदि जब भी $F[x]$ में $p(x)=f(x)g(x)$, तो $\deg f(x)=0$ या $\deg g(x)=0$.

ii) $F[x]$ में **खंडनीय (reducible)** कहलाता है यदि यह $F[x]$ में **अखंडनीय नहीं है।**

उदाहरणार्थ, $\mathbb{Q}[x]$ में तथा $\mathbb{R}[x]$ में (x^2-1) खंडनीय है, क्योंकि $x^2-1=(x-1)(x+1)$ तथा $\deg (x-1)=1=\deg (x+1)$.

आइए अखंडनीय बहुपदों के एक उदाहरण पर विस्तार से विचार करें। यह वास्तव में उदाहरणों का एक वर्ग है।

उदाहरण 2: मान लीजिए F एक क्षेत्र है। दर्शाइए कि $F[x]$ में कोई भी रैखिक बहुपद $F[x]$ में अखंडनीय होता है।

हल: मान लीजिए $f(x)=ax+b \in F[x], a \neq 0$. मान लीजिए $F[x]$ में,
$f(x)=g(x)h(x)$,
तब, $1=\deg f(x)=\deg g(x)+\deg h(x) \geq 0$.
यह तभी संभव है, जब या तो $\deg g(x)=0$ हो या $\deg h(x)=0$, अर्थात् या तो $g(x) \in F^*$, या $h(x) \in F^*$.
इस प्रकार, परिभाषा द्वारा, $F[x]$ में $f(x)$ अखंडनीय है।

***

अतः, F पर एक रैखिक बहुपद अखंडनीय होता है। $F[x]$ में अरैखिक बहुपदों के बारे में क्या कहा जा सकता है? आप देख चुके हैं कि $\mathbb{R}$ पर x^2-1 खंडनीय है। निम्नलिखित उदाहरण पर विचार कीजिए।

उदाहरण 3: जाँच कीजिए कि $x^2+1 \in \mathbb{R}[x]$ अखंडनीय है या नहीं।

हल: मान लीजिए $\mathbb{R}[x]$ में $x^2+1=f(x)g(x)$. तब, $\deg f(x) \leq 2$.
मान लीजिएयदि संभव है तो, कि $\deg f(x)=1$.
क्योंकि $f(x) \mid (x^2+1)$, इसलिए उपप्रमेय 1 द्वारा हम पाते हैं कि $\mathbb{R}$ में x^2+1 का एक मूल है। यह एक अंतर्विरोध है।
अतः, $\deg f(x) \neq 1$.
$\therefore \deg f(x)=0$ या $\deg f(x)=2$.
यदि $\deg f(x)=2$, तो $\deg g(x)=0$.
अतः, (x^2+1) अखंडनीय है।

***

निम्नलिखित प्रमेय में आप अरैखिक बहुपदों की अखंडनीयता और मूलों के बीच के संबंध को देख सकते हैं।

प्रमेय 5: मान लीजिए F एक क्षेत्र है तथा $p(x) \in F[x]$, जहाँ $\deg p(x) \geq 2$. यदि $F[x]$ में $p(x)$ अखंडनीय है, तो F में $p(x)$ के कोई मूल नहीं हैं।

उपपत्ति: हम सिद्ध किए जाने वाले कथन के प्रतिधनात्मक (contrapositive), अर्थात्, 'यदि F में $p(x)$ का एक मूल है, तो $p(x)$ खंडनीय है', को सिद्ध करेंगे।

मान लीजिए कि $p(x)$ का एक मूल $a \in F$ है। तब, उपप्रमेय 1 द्वारा, $(x-a) \mid p(x)$.
अतः, $F[x]$ में $p(x) = (x-a)g(x)$, जहाँ $\deg g(x) = \deg p(x) - 1 \geq 1$.
इस प्रकार, $F[x]$ में $p(x)$ खंडनीय है।
अतः, प्रमेय सिद्ध हो जाता है। ■

अब, क्या प्रमेय 5 का विलोम सत्य है? अर्थात्, यदि $p(x)$ की घात ≥ 2 है तथा F में इसका कोई मूल नहीं है, तो क्या $F[x]$ में $p(x)$ अखंडनीय होगा ही? आइए देखें।
$f(x) = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ पर विचार कीजिए। यह खंडनीय है, क्योंकि $\mathbb{R}[x]$ में, $f(x) = (x^2+1)(x^2+1)$, तथा $\deg(x^2+1) = 2 \neq 0$. परंतु $\mathbb{R}$ में $f(x)$ के कोई मूल नहीं हैं, क्योंकि इसके मूल हैं $\pm\sqrt{-1} \in \mathbb{C} \setminus \mathbb{R}$.
इस प्रकार, प्रमेय 5 का विलोम सत्य नहीं है।

उपरोक्त प्रतिउदाहरण में ध्यान दीजिए कि $\deg f(x) = 4$. अतः, अब प्रश्न है — क्या प्रमेय 5 का विलोम सत्य है यदि $\deg f(x) = 2$ या 3? इसी सवाल का उत्तर निम्नलिखित प्रमेय देता है।

प्रमेय 6: मान लीजिए F एक क्षेत्र है, तथा F पर $p(x)$ एक द्विघात या त्रिघात बहुपद है। यदि F में $p(x)$ के कोई मूल नहीं हैं, तो $F[x]$ में $p(x)$ अखंडनीय है।

उपपत्ति: हम सिद्ध किए जाने वाले कथन का प्रतिधनात्मक सिद्ध करेंगे। इस प्रकार, हमारा उद्देश्य यह सिद्ध करना है कि यदि $F[x]$ में $p(x)$ खंडनीय है, तो F में $p(x)$ का एक है।
अतः, मान लीजिए $F[x]$ में $p(x) = f(x)g(x)$ जहाँ $\deg f(x) \geq 1$, $\deg g(x) \geq 1$ है।
अब, $\deg p(x) = \deg f(x) + \deg g(x)$, तथा $\deg p(x) = 2$ या 3. अतः, $\deg f(x) = 1$ या $\deg g(x) = 1$.
मान लीजिए $f(x)$ रैखिक है, और $f(x) = ax + b$, जहाँ $a \neq 0$.
तब, $f(-a^{-1}b) = 0$. अतः, $p(-a^{-1}b) = 0$. इस प्रकार, $-a^{-1}b \in F$, $p(x)$ का एक मूल है।

इसी प्रकार, यदि $g(x)$ रैखिक है, तो F में $p(x)$ का एक मूल होगा।

इस प्रकार, हमने सिद्ध कर लिया है कि यदि $p(x)$ खंडनीय है, तो इसका F में मूल है; जो कथन 'यदि F में $p(x)$ का कोई मूल नहीं है, तो F पर $p(x)$ अखंडनीय है' के तुल्य है। ■

अब, क्यों नहीं आप कुछ प्रश्न हल कर लेते?

E13) निम्नलिखित में से कौन-से बहुपद अखंडनीय हैं? अपने उत्तरों के कारण दीजिए।

i) $x^2 - 2x + 1 \in \mathbb{R}[x]$,

ii) $x^2 + x + 1 \in \mathbb{C}[x]$,

iii) $ix + 2 \in \mathbb{C}[x]$,

iv) $x^4 + 3x^2 + 2 \in \mathbb{R}[x]$,

v) $x^2 + a^2 \in \mathbb{R}[x] \ \forall \ a \in \mathbb{R}^*$.

E14) जाँच कीजिए कि $\mathbb{Z}_5[x]$ में $x^3 + \bar{3}x^2 + \bar{2}$ अखंडनीय है या नहीं।

E15) यदि F में $f(x) \in F[x]$ का जहाँ मूल है $\deg f(x) \leq 3$, तो $F[x]$ में $f(x)$ खंडनीय है। सत्य, या असत्य? क्यों?

E16) दो ऐसी अभाज्य संख्याएँ p ज्ञात कीजिए जिनसे कि $\mathbb{Z}_p[x]$ में
$(x + \bar{2}) \mid (x^4 + x^3 + x^2 - x + \bar{1})$.

E17) किन $n \in \mathbb{N}$ के लिए, $x^n - 1 \in \mathbb{Q}[x]$ अखंडनीय है, तथा क्यों?

अभी तक आपने $F[x]$ में $f(x)$ के अखंडनीय होने, तथा F में $f(x)$ के मूलों, के बीच के संबंध के बारे में अध्ययन किया है। आइए अब उस बात पर वापस आ जाएँ जिसका हमने इस भाग के शुरू में ज़िक्र किया था, अर्थात् $\mathbb{Z}$ में अभाज्य अवयव के अनुरूप $F[x]$ में संकल्पना। इकाई 14 में आपने देखा था कि यदि p एक अभाज्य संख्या है, तो $\mathbb{Z}$ की $p\mathbb{Z}$ एक उच्चिष्ठ गुणजावली है। अब आप देखेंगे कि यदि F एक क्षेत्र है, तो $F[x]$ के अखंडनीय अवयवों में यही गुण होता है।

प्रमेय 7: मान लीजिए F एक क्षेत्र है तथा $f(x) \in F[x]$, $F[x]$ में अखंडनीय है। $F[x]$ की गुणजावली $< f(x) >$ एक उच्चिष्ठ गुणजावली है।

उपपत्ति: मान लीजिए $F[x]$ की I एक ऐसी गुणजावली है कि $< f(x) > \subseteq I \subseteq F[x]$.
भाग 15.5, इकाई 15 से आप जानते हैं कि $F[x]$ में प्रत्येक गुणजावली एक मुख्य गुणजावली होती है।
$\therefore I = < g(x) >$, किसी $g(x) \in F[x]$ के लिए।
तब, $f(x) \in < g(x) > \Rightarrow \exists \ h(x) \in F[x]$ s.t. $f(x) = g(x)h(x)$.
क्योंकि $f(x)$ अखंडनीय है, इसलिए या तो $g(x) \in F^*$ या $h(x) \in F^*$.
यदि $g(x) \in F^*$, मान लीजिए $g(x) = c$, तो $< g(x) > = < c > = F[x]$.
यदि $h(x) \in F^*$, मान लीजिए $h(x) = a$, तो $g(x) = a^{-1} f(x) \in < f(x) >$, जिससे $< g(x) > = < f(x) >$ प्राप्त होता है।
अतः, $F[x]$ की $< f(x) >$ एक उच्चिष्ठ गुणजावली है। ■

प्रमेय 7 से तुरंत निकलने वाले दो उपप्रमेय निम्नलिखित हैं।

उपप्रमेय 3: यदि $f(x) \in F[x]$ अखंडनीय है, तो $F[x]/< f(x) >$ एक क्षेत्र है।

उपपत्ति: क्योंकि $F[x]$ की $< f(x) >$ एक उच्चिष्ठ गुणजावली है, इसलिए $F[x]/< f(x) >$ एक क्षेत्र है, इकाई 14 के प्रमेय 14 द्वारा। ■

उपप्रमेय 4: यदि $f(x) \in F[x]$ अखंडनीय है, तो $F[x]$ का $f(x)$ एक अभाज्य अवयव है।

उपपत्ति: क्योंकि $<f(x)>$ एक उच्चिष्ठ गुणजावली है, इसलिए यह $F[x]$ की एक अभाज्य गुणजावली है। अतः, $F[x]$ का $f(x)$ एक अभाज्य अवयव है, इकाई 14 के प्रमेय 13 द्वारा। ■

आइए प्रमेय 7 के उपयोग के एक उदाहरण पर विचार करें।

उदाहरण 4: मान लीजिए कि p एक अभाज्य संख्या है। क्या $\mathbb{Q}[x]/<x^3-p>$ एक क्षेत्र है? क्यों, या क्यों नहीं?

हल: प्रमेय 7 से आप जानते हैं कि किसी भी क्षेत्र F के लिए, यदि $F[x]$ में $f(x)$ अखंडनीय है, तो $F[x]$ की $<f(x)>$ एक उच्चिष्ठ गुणजावली है।

अब, x^3-p के मूल $p^{1/3}$, $p^{1/3}\omega$ और $p^{1/3}\omega^2$ हैं, जहाँ ω एक का $\mathbb{C}\setminus\mathbb{R}$ में एक घनमूल है। साथ ही, $p^{1/3}\in\mathbb{R}\setminus\mathbb{Q}$. इस प्रकार, x^3-p का कोई भी मूल $\mathbb{Q}$ में नहीं है। अतः, प्रमेय 6 द्वारा, x^3-p अखंडनीय है।

इसलिए, $\mathbb{Q}[x]$ की $<x^3-p>$ एक उच्चिष्ठ गुणजावली है।

इस प्रकार, $\mathbb{Q}[x]/<x^3-p>$ एक क्षेत्र है।

***

अब, आइए उपप्रमेय 4 पर वापस जाएँ। इस उपप्रमेय में आपने देखा था कि $F[x]$ का प्रत्येक अखंडनीय अवयव एक अभाज्य अवयव होता है। क्या इसका विलोम भी सत्य है? आइए देखें।

प्रमेय 8: मान लीजिए F एक क्षेत्र है तथा $f(x)\in F[x]$ एक अभाज्य अवयव है। तब, $F[x]$ में $f(x)$ अखंडनीय है।

उपपत्ति: मान लीजिए $F[x]$ में $f(x)=g(x)h(x)$. तब, $f(x)\mid g(x)h(x)$.

अतः, अभाज्य अवयव की परिभाषा से, $f(x)\mid g(x)$ या $f(x)\mid h(x)$.

मान लीजिए $f(x)\mid g(x)$.

क्योंकि $f(x)=g(x)h(x)$, इसलिए हम देखते हैं कि $g(x)\mid f(x)$ भी है।

अतः, इकाई 15, प्रमेय 8 द्वारा, किसी $a\in F^*$ के लिए, $f(x)=ag(x)$.

इस प्रकार, $ag(x)=g(x)h(x)$.

अतः, निरसन नियम द्वारा, $h(x)=a$, अर्थात्, $\deg h(x)=0$.

इसी प्रकार, यदि $f(x)\mid h(x)$, तो $\deg g(x)=0$.

इस प्रकार, $f(x)$ अखंडनीय है। ■

प्रमेय 8 और उपप्रमेय 4 आपको क्या बताते हैं? क्या ये नहीं कहते कि **$f(x)\in F[x]$ एक अभाज्य अवयव है iff यह अखंडनीय है**?

अब, क्यों नहीं आप कुछ संबंधित प्रश्नों को हल कर लेते?

E18) मान लीजिए F एक क्षेत्र है तथा $F[x]$ में $p(x)$ अखंडनीय है। यदि $p(x)\mid f_1(x)f_2(x)\ldots f_n(x)$, तो दर्शाइए कि किसी $i=1,\ldots,n$ के लिए, $p(x)\mid f_i(x)$, जहाँ $f_j(x)\in F[x]\ \forall\ j=1,\ldots,n$.

E19) निम्नलिखित में से कौन-से कथन सत्य हैं? अपने उत्तरों के लिए कारण दीजिए।

i) यदि F_1 और F_2 क्षेत्र हैं s.t. $F_1 \subseteq F_2$, तथा F_1 पर $f(x) \in F_1[x]$ अखंडनीय है, तो F_2 पर $f(x)$ अखंडनीय है।

ii) $\mathbb{Z}_5[x]$ में $x^3+\bar{2}x^2+\bar{2}$ एक अभाज्य अवयव होगा।

iii) यदि $F[x]$ का $p(x)$ एक अभाज्य अवयव है, तो $F[x]$ की किसी भी गुणजावली I के लिए, $\overline{p(x)}$, $F[x]$ का एक अभाज्य अवयव है, जहाँ F एक क्षेत्र है।

अब तक आपने क्षेत्र पर अखंडनीयता के धारणा की काफ़ी समझ बन ली होगी। आइए इस संकल्पना को सम्मिश्र, वास्तविक और परिमेय क्षेत्रों पर बहुपदों की विशिष्ट स्थितियों में अधिक गहराई से देखें।

16.4 $\mathbb{C}, \mathbb{R}$ और $\mathbb{Q}$ पर अखंडनीयता

अभी तक आपने किसी भी क्षेत्र F पर अखंडनीयता का अध्ययन किया है। अब हम, विशिष्ट रूप से $\mathbb{C}$, $\mathbb{R}$ या $\mathbb{Q}$ पर अखंडनीयता की बात करेंगे।

16.4.1 $\mathbb{C}$ और $\mathbb{R}$ पर अखंडनीयता

आप देख चुके हैं कि किसी भी क्षेत्र F के लिए, $F[x]$ में रैखिक बहुपद अखंडनीय होते हैं। अतः, $\mathbb{C}$ पर भी रैखिक बहुपद अखंडनीय होते हैं। परंतु $\mathbb{C}$ के लिए हमें एक और अधिक शक्तिशाली परिणाम मिलता है, जो वास्तव में बीजगणित के लिए मौलिक है।

प्रमेय 9 (बीजगणित का मूल प्रमेय): $\mathbb{C}[x]$ में घात $n \geq 1$ वाले बहुपद के सभी n मूल $\mathbb{C}$ में होते हैं, जहाँ पुनरावर्ती वाले मूलों की गिनती उनकी बहुकताओं के साथ होती है। ■

1799 में महान गणितज्ञ गाउस ने बीजगणित के मूल प्रमेय **(The fundamental Therorm of Algebra)** को सिद्ध किया था।

यह प्रमेय सरल प्रतीत होता है, परंतु बहुत गहरा है। हम इस पाठ्यक्रम में इसे सिद्ध नहीं करेंगे, क्योंकि उपपत्ति में सम्मिश्र विश्लेषण की कुछ समझ की आवश्यकता है। परंतु, आइए देखें कि इस प्रमेय से तुरंत क्या निष्कर्ष निकलता है।

उपप्रमेय 5: $\mathbb{C}$ पर घात $n \geq 1$ वाले प्रत्येक बहुपद को $\mathbb{C}[x]$ में n रैखिक बहुपदों के गुणनफल के रूप में लिखा जा सकता है। ■

दूसरे शब्दों में, उपप्रमेय 5 कहता है कि **C[x] में अखंडनीय बहुपद केवल रैखिक बहुपद ही हैं।**

इस प्रकार, $\mathbb{C}[x]$ में (x^2+1) अखंडनीय नहीं है, जबकि $\mathbb{R}[x]$ में यह अखंडनीय है, जैसा कि आप पहले देख चुके हैं।

बीजगणित के मूल प्रमेय द्वारा आप अब जानते हैं कि, उदाहरणार्थ, $(2+3i)x^{10}+(-5+i\sqrt{5})x^7+\pi x^5+i$ के $\mathbb{C}$ में 10 मूल हैं। निस्संदेह, इन मूलों का भिन्न-भिन्न होना ज़रूरी नहीं है।

आगे, आइए $\mathbb{R}[x]$ में अखंडनीय बहुपदों पर दृष्टि डालें। हम यह कैसे जानें कि $\mathbb{R}[x]$ में घात ≥ 2 वाला कोई बहुपद अखंडनीय है या नहीं? वैसे, प्रमेय 5 और प्रमेय 6 द्वारा आप जानते हैं कि यदि बहुपद घात 2 या 3 का है, तो यह अखंडनीय है यदि और केवल यदि इसका $\mathbb{R}$ में कोई मूल नहीं है। परंतु, इसके बारे में हमें एक अधिक परिशुद्ध परिणाम है, जो वास्तव में प्रमेय 9 से निकलता है।

प्रमेय 10: यदि $p(x) \in \mathbb{R}[x]$ अखंडनीय है, तो $p(x)$ या तो एक रैखिक बहुपद है, या एक द्विघात बहुपद है।

उपपत्ति: मान लीजिए $\deg p(x) = n$. क्योंकि $\mathbb{R}[x]$ में $p(x)$ अंखडनीय है, इसलिए इसके कोई वास्तविक मूल नहीं हैं।
यदि $n = 1$, तो $p(x)$ रैखिक है, तथा इसी लिए अखंडनीय है।
मान लीजिए $n \geq 2$. ध्यान दीजिए कि $p(x) \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$.
अतः, प्रमेय 9 द्वारा, $p(x) = a_n(x - z_1)(x - z_2)\ldots(x - z_n)$, जहाँ $a_n \in \mathbb{R}$ तथा $z_i \in \mathbb{C} \ \forall \ i = 1, ..., n$.
साथ ही, $p(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{R} \ \forall \ i = 0, \ldots, n$.
अब, यदि किसी $z \in \mathbb{C}$ के लिए, $p(z) = 0$, तो $\mathbb{C}$ में $a_0 + a_1z + \cdots + a_nz^n = 0$.
अतः, $\mathbb{C}$ में $p(\bar{z}) = a_0 + a_1\bar{z} + \cdots + a_n\bar{z}^n = \overline{p(z)} = 0$, जहाँ $\mathbb{C}$ में $\bar{z}$, z का संयुग्मी है।
ध्यान दीजिए कि $a_i = \bar{a}_i$, क्योंकि $a_i \in \mathbb{R} \ \forall \ i = 0, 1, \ldots, n$.
अतः, यदि $p(x)$ का $(x - z)$ एक गुणनखंड है, तो $\mathbb{C}$ में $p(x)$ का $(x - \bar{z})$ भी एक गुणनखंड होना चाहिए, अर्थात् यदि $\mathbb{C}$ में z, $p(x)$ का एक मूल है, तो $\bar{z}$ भी एक मूल होगा। ध्यान दीजिए कि $z \neq \bar{z}$, क्योंकि $z \notin \mathbb{R}$.
इस प्रकार, $p(x)$ **के अवास्तविक सम्मिश्र मूल युग्मों में प्रकट होते हैं।**
अतः, यदि $p(x) \in \mathbb{R}[x]$ का एक अवास्तविक सम्मिश्र मूल है, तो इसके कम से कम दो ऐसे मूल होने चाहिए।
इसी प्रकार, यदि $p(x)$ के 3 अवास्तविक सम्मिश्र मूल हैं, तो इसके न्यूनतम चार ऐसे मूल होंगे, इत्यादि।

अब दो स्थितियाँ उठती हैं: $\deg p(x)$ विषम है, या $\deg p(x)$ सम है।
यदि $\deg p(x)$ विषम है, तो $p(x)$ का कम से कम एक वास्तविक मूल होना चाहिए, क्योंकि $\mathbb{C} \setminus \mathbb{R}$ में कोई भी मूल युग्मों में प्रकट होते हैं। इस प्रकार, इस स्थिति में, $\mathbb{R}$ पर $p(x)$ खंडनीय है।

आगे, दूसरी स्थिति लीजिए, अर्थात् $\deg p(x)$ सम है, मान लीजिए $\deg p(x) = 2m$, $m \in \mathbb{N}$, अर्थात् यहाँ $n = 2m$.
$p(x)$ के प्रत्येक अवास्तविक सम्मिश्र मूलों के युग्म $a + ib$ और $a - ib$ के लिए,

$$[x - (a + ib)][x - (a - ib)] = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]. \qquad \ldots(1)$$

अतः, अवास्तविक सम्मिश्र मूलों के प्रत्येक युग्म के लिए, आपको $p(x)$ का घात 2 वाला एक गुणनखंड प्राप्त होता है। क्योंकि $p(x)$ का कोई वास्तविक मूल नहीं है, तथा $p(x)$ के अवास्तविक मूल युग्मों में प्रकट होते हैं, इसलिए $\mathbb{C} \setminus \mathbb{R}$ में $p(x)$ के मूलों के m युग्म हैं। अतः, $p(x)$ के $\mathbb{R}[x]$ में (1) में दर्शाए रूप के m गुणनखंड होंगे।
अतः, इस स्थिति में, $p(x)$ तभी अखंडनीय हो सकता है जब $m = 1$ हो, अर्थात् $\deg p(x) = 2$.

इस प्रकार, हमने सिद्ध कर दिया है कि यदि $p(x) \in \mathbb{R}[x]$ अखंडनीय है, तो $\deg p(x) = 1$ या $\deg p(x) = 2$. ■
अब, आप क्यों नहीं कुछ प्रश्नों को हल कर लेते?

E20) यदि $\mathbb{R}[x]$ में $p(x)$ एक रैखिक बहुपद या द्विघात बहुपद है, तो यह अखंडनीय होता है। सत्य, या असत्य? क्यों?

E21) यदि $p(x) \in \mathbb{R}[x]$ की घात 6 है, तो $\mathbb{C}[x]$ में इसके कितने रैखिक गुणनखंड होंगे? और, $\mathbb{R}[x]$ में $p(x)$ के कितने अखंडनीय गुणनखंड हो सकते हैं?

अतः, आपने देखा कि $\mathbb{C}$ या $\mathbb{R}$ पर अखंडनीयता बहुपदों की घातों से साफ़ साफ़ जुड़ा है। आइए देखें कि क्या यही स्थिति $\mathbb{Q}[x]$ में है।

16.4.2 $\mathbb{Q}$ पर अखंडनीयता

आइए अब $\mathbb{Q}$ पर अखंडनीय बहुपदों पर विचार करें। आश्चर्य की बात यह हैं कि यदि $p(x) \in \mathbb{Q}[x]$ अखंडनीय है, तो हम इसकी घात के बारे में कुछ नहीं कर सकते हैं जैसे आप आगे देखेंगे। इसका कारण समझने के लिए, हमें पहले $\mathbb{Z}[x]$ में अखंडनीयता को परिभाषित करने की आवश्यकता है।

परिभाषा: मान लीजिए $f(x) \in \mathbb{Z}[x], f(x) \neq 0, 1, -1$. **$\mathbb{Z}[x]$ में $f(x)$ अखंडनीय** कहलाता है यदि जब भी $\mathbb{Z}[x]$ में $f(x) = g(x)h(x)$, तब $g(x) = \pm 1$ या $h(x) = \pm 1$.

आपको याद होगा कि

$U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{1, -1\}$.

उदाहरणार्थ, $\mathbb{Z}[x]$ में $x+9$ अखंडनीय है, परंतु $3x+9$ खंडनीय है क्योंकि $3x+9 = 3(x+3)$, तथा ये दोनों गुणनखंड $\mathbb{Z}[x]$ में मात्रक नहीं हैं।

इससे जुड़ी निम्नलिखित टिप्पणी देखिए।

टिप्पणी 1: ध्यान दीजिए कि एक बहुपद जो $\mathbb{Z}[x]$ में खंडनीय है, $\mathbb{Q}[x]$ में अखंडनीय हो सकता है (उदाहरणार्थ, $3x+9$)।

अब, $\mathbb{Q}$ पर कोई बहुपद, मान लीजिए $f(x) = \frac{3}{2}x^3 + \frac{1}{5}x^2 + 3x + \frac{1}{3}$ लीजिए। यदि हम इसमें सभी हरों का, अर्थात्, $2, 5, 1$ और 3 का l.c.m लें, जो 30 है, तथा $f(x)$ को उससे गुणा करें, तो हमें क्या प्राप्त होता है? हमें $30f(x) = 45x^3 + 6x^2 + 90x + 10$ प्राप्त होता है, तथा यह $\mathbb{Z}[x]$ में है।

इसी प्रक्रिया का उपयोग करते हुए हम किसी भी $f(x) \in \mathbb{Q}[x]$ को एक उपयुक्त पूर्णांक d से गुणा कर सकते हैं, जिससे $df(x) \in \mathbb{Z}[x]$ हो जाए। वस्तुतः, आप इकाई 15 के प्रमेय 6 को सिद्ध करने के लिए इस प्रक्रिया का उपयोग कर चुके हैं। इसी प्रक्रिया के उपयोग से हम निम्नलिखित प्रमेय को सिद्ध करेंगे।

प्रमेय 11: यदि $\mathbb{Z}[x]$ में $f(x) \in \mathbb{Z}[x]$ अखंडनीय है, तो यह $\mathbb{Q}[x]$ में भी अखंडनीय होता है। ■

आकृति 1: फ़र्डिनंड गौटहोल्ड मैक्स आइसनस्टाइन (Ferdinand Gotthold Max Eisenstein) (1823-1852) गाउस के शिष्य थे।

हम इस प्रमेय को यहाँ सिद्ध नहीं करेंगे, क्योंकि इसके लिए कुछ और संकल्पनाओ से और गाउसीय प्रमेयिका (Gauss' Lemma) से आपका परिचय कराना होगा। (यदि आप इसके बारे में सीखना चाहते हैं, तो 'पाठ्यक्रम के परिचय' में दी गई पुस्तकों मे से किसी भी पुस्तक में इस प्रमेयिका के बारे में पढ़ लें।) परंतु, आइए देखें कि यह प्रमेय महत्वपूर्ण क्यों है। यह बताता है कि $\mathbb{Q}[x]$ में बहुपद की अखंडनीयता की जाँच करने के लिए, $\mathbb{Z}[x]$ में इसकी जाँच करना काफ़ी है। तथा, $\mathbb{Z}[x]$ में इसकी जाँच करने के लिए हमारे पास एक बढ़िया परीक्षण है, जिसे जर्मन गणितज्ञ थियोडोर राउनमान (Theodor Schönemann) (1812-1868) ने रूप दिया था, और बाद में जर्मन गणितज्ञ आइसनस्टाइन ने 1850 में सिद्ध किया था। यह आइसनस्टाइन के नाम से लोकप्रिय है, तथा राउनमान का नाम छुप सा गया है। हम इसका यहाँ कथन देंगे, परंतु इस पाठ्यक्रम में इसे सिद्ध नहीं करेंगे।

प्रमेय 12 (आइसनस्टाइन निकष): मान लीजिए $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$, और किसी अभाज्य संख्या p के लिए,

i) $p\nmid a_n$,

ii) $p|a_0, p|a_1,\ldots, p|a_{n-1}$, तथा

iii) $p^2\nmid a_0$.

तब $\mathbb{Z}[x]$ में $f(x)$ अखंडनीय होता है (तथा इसी लिए $\mathbb{Q}[x]$ में अखंडनीय होता है)। ■

अब, प्रमेयों 11 और 12 को साथ रखने पर, आप देख सकते हैं कि आइसनस्टाइन निकष हमें बताता है कि कब $\mathbb{Z}[x]$ का बहुपद $\mathbb{Q}[x]$ में अखंडनीय होता है। आइए इस निकष के उपयोग को देखें।

उदाहरण 5: क्या $\mathbb{Q}[x]$ में $2x^7+3x^5-6x^4+3x^3+12$ अखंडनीय है?

हल: $\mathbb{Z}[x]$ में दिया हुआ बहुपद घात 7 का है। इसके गुणांक हैं:

$a_0=12,\ a_1=0=a_2,\ a_3=3,\ a_4=-6,\ a_5=3,\ a_6=0,\ a_7=2.$

गुणांकों को देखने पर, हम पाते हैं कि अभाज्य संख्या 3 आइसनस्टाइन निकष में दिए प्रतिबंधों को संतुष्ट करती है:

i) $3\nmid 2$,

ii) $3|12,\ 3|0,\ 3|3,\ 3|(-6)$, तथा

iii) $3^2\nmid 12$.

अतः, दिया हुआ बहुपद $\mathbb{Z}[x]$ में अखंडनीय है, तथा इसी लिए $\mathbb{Q}[x]$ में अखंडनीय है।

***

अब, आइए देखें कि हम कैसे अप्रत्यक्ष रूप से प्रमेय 12 का उपयोग करते हुए एक बहुपद की अखंडनीयता की जाँच कर सकते हैं।

उदाहरण 6: मान लीजिए p एक अभाज्य संख्या है। दर्शाइए कि $\mathbb{Q}[x]$ में $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ अखंडनीय है। ($f(x)$ को **pवाँ वृत्तभाजनिक बहुपद (pth cyclotomic polynomial)** कहते हैं।)

हल: सबसे पहले ध्यान दीजिए कि $\mathbb{Z}[x]$ में $f(x)=g(x)h(x)$ iff $\mathbb{Z}[x]$ में $f(x+1)=g(x+1)h(x+1)$.

इस प्रकार, $\mathbb{Z}[x]$ में $f(x)$ अखंडनीय है iff $\mathbb{Z}[x]$ में $f(x+1)$ अखंडनीय है।

अब, $(x-1)f(x)=x^p-1$.

$\therefore [(x+1)-1]f(x+1)=(x+1)^p-1,$

अर्थात्, $xf(x+1)=x^p+{}^pC_1x^{p-1}+\cdots+{}^pC_{p-1}x+1-1$ (द्विपद प्रमेय द्वारा)

$$=x(x^{p-1}+px^{p-2}+{}^pC_2x^{p-3}+\cdots+{}^pC_{p-2}x+p)$$

$\therefore f(x+1)=x^{p-1}+px^{p-2}+{}^pC_2x^{p-3}+\cdots+{}^pC_{p-2}x+p$, निरसन द्वारा, क्योंकि $x\neq 0$.

अब, अभाज्य संख्या p को लेते हुए, आइसनस्टाइन निकष को लागू कीजिए। तब आप देख सकते हैं कि $\mathbb{Z}[x]$ में $f(x+1)$ अखंडनीय है।

अतः, $\mathbb{Z}[x]$ में 'तथा इसी लिए $\mathbb{Q}[x]$ में' $f(x)$ अखंडनीय है।

***

अब, आपको निम्नलिखित प्रश्नों को हल करना चाहिए।

$\mathbb{Q}[x]$ में किसी भी घात के अखंडनीय बहुपद होते है।

E22) किसी भी $n \in \mathbb{N}$ और अभाज्य संख्या p के लिए, दर्शाइए कि $\mathbb{Q}[x]$ में $x^n - p$ अखंडनीय है।

E23) यदि $\mathbb{Q}[x]$ में $a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ अखंडनीय है, तो क्या आप हमेशा एक ऐसा अभाज्य p प्राप्त कर सकते हैं, जो प्रमेय 12 के प्रतिबंधों (i), (ii) और (iii) को संतुष्ट करे? क्यों, या क्यों नहीं?

E24) $\mathbb{Z}[x]$ के निम्नलिखित अवयवों में से कौन-से अवयव $\mathbb{Q}$ पर अखंडनीय हैं?
i) $x^2 - 12$, ii) $8x^3 + 6x^2 - 9x + 24$, iii) $5x + 1$, iv) $5x^2 + 5$.

E25) दर्शाइए कि किसी भी $\bar{a} \in \mathbb{Z}_p$ के लिए, $x^p + \bar{a} \in \mathbb{Z}_p[x]$ अखंडनीय नहीं है।

E26) जाँच कीजिए कि $\forall\ n \geq 2$ $\mathbb{Q}[x]$ में $x^{n-1} + x^{n-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ अखंडनीय है या नहीं।

E27) यदि $\mathbb{Q}$ पर $f(x) \in \mathbb{Z}[x]$ अखंडनीय है, तो यह $\mathbb{Z}$ पर अखंडनीय होता है। सत्य, या असत्य? क्यों?

E28) क्या $\mathbb{Z}[x]$ के लिए प्रमेय 7 सत्य है? क्यों?

यह हमेशा करना मालूम आसान नहीं होता कि $\mathbb{Q}[x]$ में कोई दिया हुआ बहुपद अखंडनीय है या नहीं। निस्संदेह, आइसनस्टाइन निकष कुछ स्थितियों में हमारी सहायता करता है। परंतु E23 से आप जानते हैं कि $\mathbb{Q}[x]$ में ऐसे अखंडनीय बहुपद हैं जो इस निकष को संतुष्ट नहीं करते। परंतु, कुछ और ऐसे प्रमेय हैं, जो इसमें हमारी सहायता कर सकते हैं। आइए अब इनकी चर्चा करें।

प्रमेय 13 (परिमेय मूल प्रमेय): मान लीजिए $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, जहाँ $a_n \neq 0$. यदि $f(x)$ का $\frac{p}{q} \in \mathbb{Q}$ एक मूल है, जहाँ $(p, q) = 1$, तो $p | a_0$ और $q | a_n$.

उपपत्ति: क्योंकि $f(\frac{p}{q}) = 0$, इसलिए $a_0 + a_1\frac{p}{q} + \cdots + a_n\frac{p^n}{q^n} = 0$.

अतः, $a_0q^n + a_1pq^{n-1} + \cdots + a_{n-1}p^{n-1}q + a_np^n = 0$.

अब, $q \mid (a_0q^n + \cdots + a_{n-1}p^{n-1}q)$.

अतः, $q \mid (-a_np^n)$.

इस प्रकार, $q \mid a_n$, क्योंकि $(p, q) = 1$.

इसी प्रकार, क्योंकि $p \mid (a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_np^n)$, इसलिए $p \mid a_0$.

अतः, परिणाम प्राप्त हो जाता है। ■

ध्यान दीजिए कि यदि $\mathbb{Q}$ में $f(x) \in \mathbb{Z}[x]$ का कोई मूल नहीं है, तो भी यह अखंडनीय हो सकता है (जैसे कि $x+1$)। अतः, किसी घात ≥ 4 वाले बहुपद की अखंडनीयता की जाँच करने के लिए, प्रमेय 13 की भूमिका बहुत ही सीमित है।

आइए प्रमेय 13 के अनुप्रयोग के एक उदाहरण पर विचार करें।

उदाहरण 7: जाँच कीजिए कि $\mathbb{Q}[x]$ में $f(x) = 8x^3+9x^2-5x-2$ अखंडनीय है या नहीं।

हल: इस स्थिति में ऐसी कोई अभाज्य संख्या नहीं है जिसके प्रयोग से हम आइसनस्टाइन निकष को लागू कर सकते हैं। तो आइए देखें कि क्या $f(x)$ का कोई परिमेय मूल है।

यदि $(p, q) = 1$ के साथ $\frac{p}{q}$ एक मूल है, तो प्रमेय 13 द्वारा, $p \mid (-2)$ और $q \mid 18$.

अतः, p और q के लिए संभावनाएँ हैं: $p = \pm 1, \pm 2$, और
$q = \pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$.
अगला चरण है कि प्रयास-और-भूल विधि का उपयोग किया जाए। वाह! हमें $f\left(-\frac{1}{3}\right) = 0$ मिलता है। अतः, $\mathbb{Q}[x]$ में $f(x)$ का एक गुणनखंड $\left(x+\frac{1}{3}\right)$ है।
$\therefore$ $\mathbb{Q}$ पर $f(x)$ अखंडनीय नहीं है।

***

जैसा कि आप उपरोक्त उदाहरण से देख सकते हैं, परिमेय मूल प्रमेय को लागू करना इतना सरल नहीं है। इसका कारण यह है कि $\frac{p}{q}$ कई सारी संभावनाओं में से एक हो सकती है, तथा इनमें से प्रत्येक की जाँच करना होगा, जब तक कि आप एक मूल प्राप्त कर लेते हैं – या नहीं कर पाते!
आगे, यदि किसी बहुपद की घात ≥ 4 है, तो हो सकता है कि $\mathbb{Q}$ में इसका कोई भी मूल न हो और फिर भी खंडनीय हो, जैसा कि आप देख चुके हैं। अतः, यह प्रमेय वास्तव में केवल तब सहायक है, जब घात 2 या 3 की स्थिति हो या जब गुणांकों a_n और a_0 के गुणनखंडों की संख्या छोटी हो।

अब, आइए $\mathbb{Q}$ पर अखंडनीयता की एक अन्य निकष पर चर्चा करें। प्रमेय 12 की तरह, यह भी प्रमेय 11 पर आधारित है।

प्रमेय 14 (Mod p अखंडनीयता परीक्षण): मान लीजिए $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. यदि कोई अभाज्य संख्या p है s.t. $p \nmid a_n$ और s.t. $\mathbb{Z}_p[x]$ में $\overline{f(x)} = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n$ अखंडनीय है, तो $\mathbb{Q}[x]$ में $f(x)$ अखंडनीय है।

उपपत्ति: हम इसे अंतर्विरोध द्वारा सिद्ध करेंगे। मान लीजिए, यदि संभव हो तो, कि $\mathbb{Q}$ पर $f(x)$ खंडनीय है। तब प्रमेय 11 द्वारा, $\mathbb{Z}$ पर $f(x)$ खंडनीय है।
अतः, $f(x) = g(x)h(x)$, जहाँ $g(x), h(x) \in \mathbb{Z}[x], g(x) \neq \pm 1, h(x) \neq \pm 1$.
इसलिए, $\mathbb{Z}_p[x]$ में, हमें $\overline{f(x)} = \overline{g(x)} \cdot \overline{h(x)}$ प्राप्त होता है।
यहाँ $\deg \overline{g(x)} \leq \deg g(x) < \deg \overline{f(x)}$, तथा $\deg \overline{h(x)} < \deg \overline{f(x)}$.
यह हमारी परिकल्पना, कि $\mathbb{Z}_p$ पर $\overline{f(x)}$ अखंडनीय है, का अंतर्विरोध करता है।
इसलिए, $\mathbb{Q}[x]$ में $f(x)$ अखंडनीय है। ■

आइए प्रमेय 14 के एक अनुप्रयोग पर विचार करें।

उदाहरण 8: क्या $\mathbb{Q}[x]$ में $6x^3 - 7x^2 + 8x + 2$ अखंडनीय है? अपने उत्तर के लिए कारण दीजिए।

हल: यहाँ कोई अभाज्य संख्या नहीं है जिससे कि हम आइसनस्टाइन निकष लागू कर सकें। अतः, आइए प्रमेय 14 से करें।

मान लीजिए $f(x) = 6x^3 - 7x^2 + 8x + 2$.

हम $p = 7$ लेकर देखते हैं, क्योंकि $7 \nmid 6$. इसलिए, हम $\mathbb{Z}_7[x]$ में $\overline{f(x)}$ को देखेंगे।

हम $\overline{f(x)} = \overline{6}x^3 + x + \overline{2}$ पाते हैं।

प्रमेय 6 द्वारा, यह खंडनीय है iff $\mathbb{Z}_7$ में $\overline{f(x)}$ का कोई मूल है।

अब $x = \overline{0}, \overline{1}, \ldots, \overline{6}$ प्रतिस्थापित करने पर, आप देख सकते हैं कि इनमें से कोई भी $\overline{f(x)} = \overline{0}$ नहीं देता।

अतः, $\mathbb{Z}_7[x]$ में $\overline{f(x)}$ अखंडनीय है।

इस प्रकार, प्रमेय 14 द्वारा, $\mathbb{Q}[x]$ में $f(x)$ अखंडनीय है।

दिखाइए कि इस उदाहरण में आप $p = 5$ भी ले सकते हैं। क्यों? आप यहाँ भी पाएंगे $\mathbb{Z}_5[x]$ में $\overline{f(x)}$ अखंडनीय है।

***

आइए घात > 3 वाले बहुपद के एक उदाहरण पर भी विचार करें।

उदाहरण 9: मान लीजिए $f(x) = \frac{3}{7}x^4 - \frac{2}{7}x^2 + \frac{9}{35}x + \frac{3}{5} \in \mathbb{Q}[x]$. जाँच कीजिए कि $\mathbb{Q}$ पर $f(x)$ अखंडनीय है या नहीं।

हल: ध्यान दीजिए कि $g(x) = 35f(x) = 15x^4 - 10x^2 + 9x + 21 \in \mathbb{Z}[x]$. साथ ही, $\mathbb{Q}$ पर $f(x)$ अखंडनीय होगा यदि और केवल यदि $\mathbb{Q}$ पर $g(x)$ अखंडनीय होगा।

अब प्रमेय 14 में $p = 2$ लीजिए। हम $\overline{g(x)} = x^4 + x + \overline{1} \in \mathbb{Z}_2[x]$ प्राप्त करते हैं।

अब, $\mathbb{Z}_2$ में $\overline{g(x)}$ का कोई मूल नहीं है।

आइए देखें कि क्या इसके कोई द्विघात गुणनखंड हैं।

ऐसे कोई भी गुणनखंड $x^2 + \overline{1}$ या $x^2 + x + \overline{1}$ होगा।

क्योंकि $\mathbb{Z}_2$ में $x^2 + \overline{1}$ का एक शून्यक है, इसलिए यह $\overline{g(x)}$ का एक गुणनखंड नहीं हो सकता। साथ ही, $\mathbb{Z}_2[x]$ में $(x^2 + x + \overline{1}) \nmid (x^4 + x + \overline{1})$. (क्यों?).

अतः, $\mathbb{Z}_2[x]$ में $\overline{g(x)}$ अखंडनीय है।

इस प्रकार, प्रमेय 14 से, $\mathbb{Q}[x]$ में $g(x)$ अखंडनीय है।

अतः, $\mathbb{Q}[x]$ में $f(x)$ अखंडनीय है।

***

आइसनस्टाइन निकष तथा प्रमेयों 13 और 14 के होते हुए भी हमारे पास $\mathbb{Q}$ पर अखंडनीयता की जाँच करने के लिए पर्याप्त साधन नहीं हैं। उदाहरणार्थ, कोई ऐसा भी बहुपद हो सकता है जिसका $\mathbb{Q}$ में कोई मूल नहीं हो। या, कोई ऐसा भी बहुपद हो सकता है जिसके लिए, प्रमेय 14 को लागू करने के लिए कोई स्पष्ट p उपलब्ध नहीं हो। तब, हम कुछ स्थितियों में निरीक्षण की अपनी पुरानी विधि चला सकते हैं। उदाहरणार्थ, यदि आप $x^4 + 4x^2 + 2$ को देखते हैं, तो आप इसको देख कर कह सकते हैं कि यह $(x^2 + 2)^2$ है, तथा इसी लिए यह $\mathbb{Q}$ पर खंडनीय है।

साथ ही, कम्प्यूटर बीजगणित (Computer Algebra) में परिमित क्षेत्रों पर या $\mathbb{Q}$ पर जाँच करने के लिए, अनेक गुणनखंडन ऐल्गोरिद्म उपलब्ध हैं। आप इनमें से कुछ का अध्ययन उच्चतर पढ़ाई में कर सकते हैं।

अब, आप क्यों नहीं कुछ प्रश्नों को हल कर लेते?

E29) निम्नलिखित में से कौन-से कथन सत्य हैं? अपने उत्तरों की पुष्टि कीजिए।

i) $\mathbb{Q}[x] \big/ \langle x^7 + 7x^6 - 14 \rangle$ एक क्षेत्र है।

ii) $\mathbb{R}[x] \big/ \langle x^7 + 7x^6 - 14 \rangle$ एक क्षेत्र है।

iii) $Q[x] \big/ \langle 21x^3 - 3x^2 + 2x + 9 \rangle$ एक क्षेत्र नहीं है।

E30) पुष्टि करते हुए, घात 10 वाले एक ऐसे बहुपद का उदाहरण दीजिए जो $\mathbb{Q}$ पर अखंडनीय है, परंतु $\mathbb{Z}_{11}[x]$ में उसे लेने पर वह खंडनीय है।

E31) जाँच कीजिए कि निम्नलिखित बहुपद $\mathbb{Q}$ पर अखंडनीय हैं या नहीं।

i) $2x^3 + 3x^2 + 6x + 2,$

ii) $6x^3 + x + 9,$

iii) $x^5 + 2x + 4,$

iv) $8x^3 - 6x + 1$ (आप यहाँ उदाहरण 6 में उपयोग की गई विधि को लागू कर सकते हैं)।

आइए अब देखें कि $F[x]$ में अखंडनीय बहुपद क्यों महत्वपूर्ण हैं।

16.5 अद्वितीय गुणनखंडन

इकाई 1 में आपने अंकगणित के मूल प्रमेय का अध्ययन कियाण था। जैसा कि आप जानते हैं, इसी प्रमेय के आधार पर हम कहते हैं कि अभाज्य संख्याएँ वे परमाणु हैं जो किसी भी पूर्णांक को बनाते हैं। साथ ही, आप अभाज्य संख्याओं तथा $F[x]$ में अंखडनीय बहुपदों के बीच अनेक पहलुओं में एक समांतरता को देख चुके हैं। आइए देखें कि, अंकगणित के मूल प्रमेय के समांतर क्या हम $F[x]$ में किसी भी बहुपद को बनाने के लिए अखंडनीय बहुपदों को रचना खंडों के रूप में, सोच सकते हैं।

अब, बीजगणित के मूल प्रमेय से आप जानते हैं कि यदि $f(x) \in \mathbb{C}[x]$ s.t. $\deg f(x) = n \geq 1$, तो $f(x) = p_1(x)p_2(x)\ldots p_n(x)$, जहाँ $\mathbb{C}[x]$ में $p_i(x)$ एक रैखिक बहुपद है $\forall\ i = 1, \ldots, n$. इस प्रकार, $\mathbb{C}[x]$ में $f(x)$ अखंडनीय बहुपदों के एक गुणनफल के रूप में पूरी तरह गुणनखंडित हो जाता है। उदाहरणार्थ, $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$, जहाँ ω, 1 का एक अवास्तविक घनमूल है।

अब, आप देख चुके हैं कि $\mathbb{R}[x]$ में अखंडनीय बहुपद घात 1 या घात 2 के होते हैं। क्या हम $\mathbb{R}[x]$ में किसी बहुपद को अखंडनीय बहुपदों के गुणनफल के रूप में पूरी तरह गुणनखंडित कर सकते हैं? निम्नलिखित प्रमेय हमें बताता है कि हम ऐसा, बल्कि इससे अधिक भी, कर सकते हैं!

प्रमेय 15 (अद्वितीय गुणनखंडन): मान लीजिए F एक क्षेत्र है, तथा $f(x) \in F[x]$ s.t. $\deg f(x) = n \geq 1.$

i) $F[x]$ में ऐसे अखंडनीय बहुपद $p_1(x), p_2(x),\ldots,p_m(x)$ हैं जिनसे कि $f(x) = p_1(x)p_2(x)\ldots p_m(x)$.

ii) यदि $f(x) = q_1(x)q_2(x)\ldots q_r(x)$ भी है, जहाँ $q_i(x) \in F[x]$ अखंडनीय है $\forall\ i = 1,\ldots,r$ के लिए, तो $m = r$ तथा प्रत्येक $p_i = c_i q_j$, किन्हीं $j = 1,\ldots,m$ और $c_i \in F^*$ के लिए। ■

प्रमेय 15 को उपप्रमेय 4 का उपयोग करके, तथा फिर m पर आगमन का अनुप्रयोग करके, सिद्ध किया जा सकता है। परंतु, इस पाठ्यक्रम में हम इसे सिद्ध नहीं करेंगे, लेकिन अनेक स्थितियों में इसका अनुप्रयोग करेंगे। आइए एक उदाहरण पर विचार करें।

उदाहरण 10: $\mathbb{R}[x]$ तथा $\mathbb{C}[x]$ में $f(x) = x^5 - 4x$ को अखंडनीय बहुपदों के गुणनफल के रूप में व्यक्त कीजिए।

हल: अब, $f(x) = x^5 - 4x = x(x^4 - 4) = x(x^2 - 2)(x^2 + 2)$

$$= x(x - \sqrt{2})(x + \sqrt{2})(x^2 + 2). \qquad \ldots(2)$$

क्योंकि $x^2 + 2$ के कोई वास्तविक मूल नहीं हैं, इसलिए $\mathbb{R}[x]$ में $f(x) = x(x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)$ एक वाँछित गुणनखंडन है।

परंतु, $\mathbb{C}[x]$ में $x^2 + 2 = (x + i\sqrt{2})(x - i\sqrt{2})$.

अतः, (2) से हमें $\mathbb{C}[x]$ में अखंडनीय गुणनखंडों के गुणनफल के रूप में $f(x) = x(x - \sqrt{2})(x + \sqrt{2})(x + i\sqrt{2})(x - i\sqrt{2})$ प्राप्त होता है।

***

अब, आपको निम्नलिखित प्रश्नों को हल करना चाहिए।

E32) दर्शाइए कि $\bar{3}x^2 + \bar{4}x + \bar{3} \in \mathbb{Z}_5[x]$ के $(\bar{3}x + \bar{2})(x + \bar{4})$ तथा $(\bar{4}x + \bar{1})(\bar{2}x + \bar{3})$, दो गुणनखंडन हैं। क्या यह प्रमेय 15(ii) का अंतर्विरोध करता है? अपने उत्तर के लिए कारण दीजिए।

E33) $\mathbb{Q}[x]$ में $2x^4 + x^3 + 4x^2 + x + 2$ को अखंडनीय बहुपदों के गुणनफल के रूप में लिखिए।

E34) $\mathbb{R}[x]$ में $2x^4 - 3x^3 - 8x^2 + 9x + 6$ को अखंडनीय बहुपदों के गुणनफल के रूप में लिखिए।

E35) यदि $f(x) \in \mathbb{R}[x]$ ऐसा है कि $\deg f(x) = 5$, तो $f(x)$ के कितने वास्तविक मूल हो सकते हैं? अपने उत्तर की पुष्टि के लिए उदाहरण दीजिए।

E36) दर्शाइए कि $\mathbb{Z}_8[x]$ में प्रमेय 15 में दिया गया गुणनखंडन का अद्वितीय होना, कम के अलावा, आवश्यक नहीं है। ध्यान दीजिए कि $\mathbb{Z}_8$ एक क्षेत्र नहीं है। (इस प्रकार, यदि F एक क्षेत्र नहीं है, तो प्रमेय 15 का सत्य होना आवश्यक नहीं है।)

इसके साथ ही हम एक क्षेत्र F के लिए, $F[x]$ में गुणनखंडन तथा अखंडनीयता की अपनी चर्चा समाप्त करते हैं। आइए उसे संक्षिप्त में देखें कि हमने इस इकाई में क्या चर्चा की है।

16.6 सारांश

इस इकाई में आपने निम्नलिखित बिंदुओं पर अध्ययन किया है।

1. वलय R पर एक बहुपद के मूल (या शून्यक) की परिभाषा, तथा किसी मूल की बहुकता की परिभाषा।

2. **(शेषफल प्रमेय):** मान लीजिए F एक क्षेत्र है। यदि $f(x) \in F[x]$ और $b \in F$, तो एक अद्वितीय बहुपद $q(x) \in F[x]$ का अस्तित्व है ताकि $f(x) = (x-b)q(x) + f(b)$.
3. मान लीजिए F एक क्षेत्र है तथा $f(x) \in F[x]$, जहाँ $\deg f(x) \geq 1$. तब, $a \in F$, $f(x)$ का एक मूल है iff $(x-a) \mid f(x)$.
4. किसी भी क्षेत्र F पर घात n वाले शून्येतर बहुपद के F में अधिकतम n मूल होते हैं।

5. $D[x]$ में घात n वाले शून्येतर बहुपद के D में अधिकतम n मूल होते हैं, जहाँ D एक पूर्णांकीय प्राँत है।

6. मान लीजिए कि किसी क्षेत्र F (क्रमशः, प्राँत D) पर $f(x)$ और $g(x)$ घात n वाले शून्येतर बहुपद हैं। यदि F (क्रमशः D) में $n+1$ भिन्न-भिन्न अवयव $a_1, \ldots, a_{n+1}$ हैं ताकि $f(a_i) = g(a_i)\ \forall\ i = 1, \ldots, n+1$, तो $f(x) = g(x)$.

7. एक क्षेत्र F पर, तथा $\mathbb{Z}$ पर, अखंडनीय बहुपद की परिभाषा, तथा उसके उदाहरण।

8. मान लीजिए F एक क्षेत्र है तथा $p(x) \in F[x]$, जहाँ $\deg p(x) \geq 2$. यदि $F[x]$ में $p(x)$ अखंडनीय है, तो F में $p(x)$ के कोई मूल नहीं हैं।

9. मान लीजिए F एक क्षेत्र है तथा F पर $p(x)$ एक द्विघात या त्रिघात बहुपद हैं। यदि F में $p(x)$ के कोई मूल नहीं हैं, तो $F[x]$ में $p(x)$ अखंडनीय है।

10. **बीजगणित का मूल प्रमेय:** $\mathbb{C}[x]$ में घात $n \geq 1$ वाले बहुपद के सभी मूल, उनकी बहुकता के साथ उन्हें गिनते हुए, $\mathbb{C}$ में होते हैं।

11. यदि $p(x) \in \mathbb{R}[x]$ अखंडनीय है, तो $p(x)$ एक रैखिक या एक द्विघात बहुपद होता है।

12. यदि $\mathbb{Z}[x]$ में $f(x) \in \mathbb{Z}[x]$ अखंडनीय है, तो यह $\mathbb{Q}[x]$ में अखंडनीय होता है।

13. **आइसनस्टाइन-निकष:** मान लीजिए $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. यदि किसी अभाज्य संख्या p के लिए,

    i) $p \nmid a_n$,

    ii) $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$, तथा

    iii) $p^2 \nmid a_0$,

    तब, $\mathbb{Z}[x]$ में $f(x)$ अखंडनीय होता है (और इसलिए $\mathbb{Q}[x]$ में भी अखंडनीय होता है)।

14. मान लीजिए F एक क्षेत्र है तथा $f(x) \in F[x]$ अखंडनीय है। तब, $F[x]$ में $< f(x) >$ एक उच्चिष्ठ गुणजावली होगी।

15. मान लीजिए F एक क्षेत्र है तथा $f(x) \in F[x]$ एक अभाज्य अवयव है। तब, $F[x]$ में $f(x)$ अखंडनीय होता है।

16. **परिमेय मूल प्रमेय:** मान लीजिए $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x], a_n \neq 0.$ यदि $f(x)$ का $\frac{p}{q} \in \mathbb{Q}$ एक मूल है, जहाँ $(p, q) = 1,$ तब, $p \mid a_0$ तथा $q \mid a_n$.

17. **(Mod p अखंडनीय परीक्षण):** मान लीजिए $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. यदि कोई अभाज्य संख्या p है s.t. $p \nmid a_n$ तथा s.t. $\mathbb{Z}_p[x]$ में $\overline{f(x)} = \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n$ अखंडनीय है, तो $\mathbb{Q}[x]$ में $f(x)$ अखंडनीय होता है।

18. **अद्वितीय गुणनखंडन:** मान लीजिए F एक क्षेत्र है तथा $f(x) \in F[x]$, $\deg f(x) = n \geq 1.$
    i) $F[x]$ में ऐसे अखंडनीय बहुपद $p_1(x), p_2(x), \ldots, p_m(x)$ हैं ताकि $f(x) = p_1(x)p_2(x)\ldots p_m(x).$
    ii) यदि $f(x) = q_1(x)q_2(x)\ldots q_r(x)$ भी है, जहाँ $q_i(x) \in F[x]$ अखंडनीय है $\forall\ i = 1, \ldots, r$ के लिए, तो $m = r$ तथा प्रत्येक $p_i = c_iq_j$, किसी $j = 1, \ldots, m$ और $c_i \in F^*$ के लिए।

16.7 हल / उत्तर

E1) $f(x) \in F[x]$ का $a \in F$ एक मूल है।
iff $f(a) = 0$
iff किसी $q(x) \in F[x]$ के लिए, $f(x) = (x - a)q(x)$, प्रमेय 1 द्वारा।
iff $(x - a) \mid f(x)$, परिभाषा द्वारा।

E2) i) द्विघात सूत्र द्वारा, मूल 3 और 2 हैं, जिनमें से प्रत्येक की बहुकता 1 है। इस प्रकार, दिया हुआ बहुपद $\frac{1}{2}(x-3)(x-2) \in \mathbb{Q}[x]$ ही है। आपको इसकी जाँच करनी चाहिए।

ii) $x^2 + x + \bar{1} = (x - \bar{1})^2$, क्योंकि $\mathbb{Z}_3$ में $-\bar{2} = \bar{1}$.
इस प्रकार, केवल $\bar{1}$ ही शून्यक है। इसकी बहुकता 2 है क्योंकि $(x - \bar{1})^2$ दिए हुए बहुपद का गुणनखंड है, तथा $(x - \bar{1})^3$ इसका गुणनखंड नहीं है।

iii) प्रयास-और-भूल विधि द्वारा, एक शून्यक $\bar{1}$ है। अब, लंबे विभाजन विधि हम $x^4 + \bar{2}x^3 - \bar{2}x - \bar{1} = (x - \bar{1})(x^3 + \bar{3}x^2 + \bar{3}x + \bar{1})$ पाते हैं।
पुनः, प्रयास-और-भूल विधि द्वारा, हम पाते हैं कि $x^3 + \bar{3}x^2 + \bar{3}x + \bar{1}$ का $x + \bar{1}$ एक गुणनखंड है।
लंबे विभाजन विधि से, हम देखते हैं कि $x^3 + \bar{3}x^2 + \bar{3}x + \bar{1} = (x + \bar{1})^3.$
इस प्रकार, $x^4 + \bar{2}x^3 - \bar{2}x - \bar{1} = (x - \bar{1})(x + \bar{1})^3.$

इससे प्रदर्शित होता है कि $\overline{1}$ बहुकता 1 वाला एक मूल है तथा $-\overline{1}(=\overline{4})$ बहुकता 3 वाला एक मूल है।

iv) ध्यान दीजिए कि $5x+3=5(x+\frac{3}{5})$, $\sqrt{2}-4x=(-4)(x-\frac{1}{2\sqrt{2}})$ तथा $(ix+1-i\sqrt{3})=i[x-(\sqrt{3}+i)]$.

अतः, $\frac{-3}{5}, \frac{1}{2\sqrt{2}}$ और $(\sqrt{3}+i)$ ही दिए हुए बहुपद के मूल हैं।

क्योंकि बहुपद इन रैखिक बहुपदों के गुणनफल के रूप में दिया है, इसलिए आप देख सकते हैं कि इनकी बहुकताएँ क्रमशः 2, 3 और 11 हैं।

E3) उदाहरणार्थ, $x^3(x-\overline{10})^2 \in \mathbb{Z}_{11}[x]$.

यहाँ $\overline{0}$ की बहुकता 3 है, तथा $\overline{10}$ की बहुकता 2 है, और केवल ये ही मूल हैं। ऐसे ही अनेक उदाहरण हो सकते हैं।

E4) i) इसे उसी प्रकार सिद्ध कीजिए जैसे आपने इकाई 13 में किया था।

ii) क्योंकि b एक अचर बहुपद है, इसलिए x के लिए a रखने पर इसके मान में कोई परिवर्तन नहीं आएगा।

iii) $f(x) \in \text{Ker}\,\phi$ iff $\phi(f(x))=0$ iff $f(a)=0$ iff $f(x)$ का a एक शून्यक है।

अब, उपप्रमेय 1 द्वारा, $f(x) \in \text{Ker}\,\phi$.

iff $(x-a) \mid f(x)$

iff $f(x) \in \langle x-a \rangle$.

इस प्रकार, $\text{Ker}\,\phi = \langle x-a \rangle$.

समाकारिता का मूल प्रमेय कहता है कि $(F[x]/\langle x-a \rangle) \simeq F$.

E5) E4 से, $F[x]/\langle x-a \rangle \simeq F$ तथा $F[x]/\langle x \rangle \simeq F$. अतः, परिणाम प्राप्त हो जाता है।

E6) मान लीजिए $f(x)=a_0+a_1x+\cdots+a_nx^n$.

तब, $a_0+a_1a+\cdots+a_na^n=0$, क्योंकि $a \in F^*$, $f(x)$ का एक मूल है।

अतः, $a^n(a_0a^{-n}+a_1a^{-(n-1)}+\cdots+a_n)=0$.

क्योंकि $a^n \neq 0$ तथा F एक प्राँत है, इसलिए

$a_n+a_{n-1}a^{-1}+\cdots a_1(a^{-1})^{n-1}+a_0(a^{-1})^n=0$, यह ध्यान में रखते हुए कि $a^{-m}=(a^{-1})^m \;\forall\; m \in \mathbb{Z}$.

$\therefore a^{-1}$, $a_n+a_{n-1}x+\cdots+a_1x^{n-1}+a_0x^n \in F[x]$ का एक मूल है।

नहीं, क्योंकि हो सकता है कि a^{-1}, D में नहीं हो। उदाहरणार्थ, $x^2-4 \in \mathbb{Z}[x]$ का एक मूल 2 है। परंतु $\mathbb{Z}$ में $4x^2-1 \in \mathbb{Z}[x]$ का कोई मूल नहीं है।

E7) प्रमेय 2 द्वारा, F में $f(x)$ के अधिकतम n मूल हैं। अतः, F में $f(x)$ के अधिकतम n भिन्न-भिन्न मूल हैं।

E8) **कथन:** मान लीजिए एक पूर्णांकीय प्राँत D पर $f(x)$ और $g(x)$ घात n वाले दो शून्येतर बहुपद हैं। यदि D में ऐसे $n+1$ भिन्न-भिन्न अवयव $a_1,\ldots,a_{n+1}$ हैं कि $f(a_i)=g(a_i)\;\forall\; i=1,\ldots,n+1$, तो $f(x)=g(x)$.

उपपत्ति: प्रमेय 3 की उपपत्ति के तर्क अनुसार, तथा प्रमेय 4 और E7 के अनुप्रयोग से, परिणाम प्राप्त कीजिए।

E9) दर्शाइए कि यह निष्कर्ष किस प्रकार उपप्रमेय 1 और प्रमेय 2 से प्राप्त होता है।

E10) i) आप जानते हैं कि $(\mathbb{Z}_p^*, \cdot)$ एक समूह है, तथा $o(\mathbb{Z}_p^*) = p-1$.
इस प्रकार, इकाई 4 से, आप जानते हैं कि $x^{p-1} = \overline{1} \ \forall\ x \in \mathbb{Z}_p^*$,
अर्थात्, $\mathbb{Z}_p^*$ के $p-1$ अवयवों में से प्रत्येक $x^{p-1} - \overline{1}$ का एक मूल है।
अतः, $(x-\overline{1}) \ldots (x-\overline{p-1}) \Big| (x^{p-1}-\overline{1})$.
क्योंकि $\mathbb{Z}_p$ में $x^{p-1} - \overline{1}$ के अधिकतम $p-1$ मूल हो सकते हैं (प्रमेय 2 द्वारा), इसलिए हम पाते हैं कि केवल $\mathbb{Z}_p^*$ के $(p-1)$ अवयव ही $x^{p-1} - \overline{1}$ मूल हैं।
अब, $x^{p-1} - \overline{1}$ और $\prod_{i=1}^{p-1}(x-\overline{i})$ के अग्रग गुणांकों तथा घातों की तुलना करने पर, हम देखते हैं कि $x^{p-1} - \overline{1} = (x-\overline{1})(x-\overline{2})\ldots(x-\overline{p-1})$.

ii) (i) में x के लिए $\overline{0}$ प्रतिस्थापित करने पर, हम $-\overline{1} = (-1)^{p-1}\overline{(p-1)!}$, प्राप्त करते हैं अर्थात्, $\overline{p-1} = (-1)^{p-1}\overline{(p-1)!}$ प्राप्त करते हैं, क्योंकि $\mathbb{Z}_p$ में $\overline{p-1} = -\overline{1}$.
अर्थात्, $(-1)^{p-1}(p-2)! \equiv 1 (\text{mod}\, p)$.
अब, प्रत्येक अभाज्य संख्या p के लिए, $(-1)^{p-1} \equiv 1 (\text{mod}\, p)$. (क्यों?)
अतः, हमें परिणाम प्राप्त हो जाता है।

E11) $\mathbb{Z}_5[x]$ में बहुपद $x^4 + \overline{4}$ और $x^4 - \overline{1}$ समान हैं, क्योंकि $\overline{4} = -\overline{1}$.
अतः, E10 के परिणाम का अनुप्रयोग करने पर, हम
$x^4 + \overline{4} = (x-\overline{1})(x-\overline{2})(x-\overline{3})(x-\overline{4})$ प्राप्त करते हैं।

E12) समूह सिद्धांत के अध्ययन से आपको एक के nवें मूलों का समूह $U(n)$ याद होगा। एक का प्रत्येक nवाँ मूल $\mathbb{C}$ में $x^n - 1$ का एक शून्यक है। साथ ही, $\mathbb{C}$ में $x^n - 1$ के अधिकतम n शून्यक हैं। अतः, $\mathbb{C}$ में $U(n)$ के अवयव ही $x^n - 1$ के शून्यक हैं।

E13) i) नहीं, क्योंकि $x^2 - 2x + 1 = (x-1)(x-1)$.

ii) नहीं, क्योंकि $x^2 + x + 1 = (x-\omega)(x-\omega^2)$, जहाँ ω एक का अवास्तविक घनमूल है।

iii) हाँ, उदाहरण 2 द्वारा।

iv) नहीं, क्योंकि $x^4 + 3x^2 + 2 = (x^2+1)(x^2+2)$.

v) नहीं, प्रमेय 6 द्वारा।

E14) मान लीजिए $f(x) = x^3 + \overline{3}x^2 + \overline{2}$. अब, क्योंकि $f(x)$ एक त्रिघात बहुपद है, इसलिए प्रमेय 6 द्वारा आपको यह देखने की आवश्यकता है कि किसी भी $a \in \mathbb{Z}_5$ के लिए, क्या $f(a) = \overline{0}$. आप पाएंगे कि $f(a) \neq \overline{0}\ \forall\ a \in \mathbb{Z}_5$.
इस प्रकार, $\mathbb{Z}_5$ पर $f(x)$ अखंडनीय है।

E15) असत्य। उदाहरणार्थ, F पर एक रैखिक बहुपद अखंडनीय होता है तथा इसका मूल F में है। परंतु, प्रमेय 5 द्वारा, यह अन्य स्थितियों के लिए सत्य है।

E16) मान लीजिए $\mathbb{Z}[x]$ में $f(x) = x^4 + x^3 + x^2 - x + 1$.
तब, $f(-2) = 16 - 8 + 4 + 2 + 1 = 15.$
इस प्रकार, $\mathbb{Z}_p[x]$ में $p = 3$ या $p = 5$ के लिए, $f(-\overline{2}) = \overline{0}$.
$\therefore \mathbb{Z}_p[x]$ में $(x + \overline{2}) \mid f(x)$, यदि $p = 3$ या $p = 5$.

E17) $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1) \; \forall \; n \geq 2.$
इस प्रकार, $x^n - 1$ खंडनीय है $\forall \; n \geq 2.$
परंतु, $n = 1$ के लिए, उदाहरण 2 द्वारा $x = 1$ अखंडनीय है।

E18) क्योंकि F पर $p(x)$ अखंडनीय है, इसलिए उपप्रमेय 4 द्वारा, यह $F[x]$ में अभाज्य है। आपको यह सिद्ध करने की आवश्यकता है कि $\forall \; n \in \mathbb{N}, P(n)$ सत्य है जहाँ
$P(n)$: यदि $p(x) \mid f_1(x) \ldots f_n(x)$, तो $p(x) \mid f_i(x)$, किसी $i = 1, \ldots, n$ के लिए।
$P(1)$ तुच्छ रूप से सत्य है। (क्यों?)
मान लीजिए कि किसी $m \in \mathbb{N}$ के लिए, कथन $P(m)$ सत्य है।
आपको सिद्ध करना चाहिए कि $P(m+1)$ सत्य है। (आप $f_1(x) \ldots f_{m+1}(x) = [f_1(x) \ldots f_m(x)] f_{m+1}(x)$ लिख सकते हैं, तथा अभाज्य अवयव की परिभाषा का उपयोग कर सकते हैं।)
अतः, $\forall \; n \in \mathbb{N}$, $P(n)$ सत्य है।

E19) i) उदाहरणार्थ, $\mathbb{Q}[x]$ में, और $\mathbb{R}[x]$ में, $x^3 - 5$ लीजिए। यह कथन क्यों असत्य है दर्शाने के लिए, उदाहरण 4 और प्रमेय 6 का उपयोग कीजिए।

ii) यह असत्य है। क्योंकि $\mathbb{Z}_5$ में $\overline{1}$ एक शून्यक है, इसलिए दिया हुआ बहुपद खंडनीय है, तथा इसी लिए, $\mathbb{Z}_5[x]$ में यह अभाज्य नहीं है।

iii) सत्य नहीं है; उदाहरणार्थ, $F[x]$ का x एक अभाज्य अवयव है, परंतु $\overline{x}$, $F[x]/< x >$ में शून्य है, तथा इसी लिए यह अभाज्य अवयव नहीं है।

E20) यदि $p(x)$ रैखिक है, तो यह अखंडनीय है। परंतु, यदि यह द्विघात है, तो इसका अखंडनीय होना आवश्यक नहीं है। उदाहरणार्थ, $\mathbb{R}[x]$ में $x^2 - 1$ द्विघात है तथा खंडनीय है।

E21) प्रमेय 9 द्वारा, $\mathbb{C}[x]$ में $p(x)$ के 6 रैखिक गुणनखंड हैं, जिनका भिन्न-भिन्न होना आवश्यक नहीं है।

$p(x) \in \mathbb{R}[x]$ के लिए, हमें निम्नलिखित स्थितियाँ प्राप्त हैं:

i) $p(x)$ के सभी मूल $\mathbb{R}$ में हैं। तब, $\mathbb{R}[x]$ में $p(x)$ के 6 अखंडनीय (रैखिक) गुणनखंड हैं।

ii) $p(x)$ के 4 मूल $\mathbb{R}$ में हैं तथा 2 मूल $\mathbb{C} \setminus \mathbb{R}$ में हैं। तब, $p(x)$ के $\mathbb{R}[x]$ में 5 अखंडनीय गुणनखंड हैं जिनमें से 4 रैखिक और 1 द्विघात हैं जैसा कि प्रमेय 10 में था।

iii) $p(x)$ के $\mathbb{R}[x]$ में 2 मूल हैं और $\mathbb{C} \setminus \mathbb{R}$ में 4 मूल हैं। तब, $p(x)$ के $\mathbb{R}$ में 4 अखंडनीय गुणनखंड हैं, जिनमें 2 रैखिक और 2 द्विघात हैं।

iv) $p(x)$ के कोई वास्तविक मूल नहीं हैं तथा 6 मूल $\mathbb{C} \setminus \mathbb{R}$ में हैं। तब, $p(x)$ के $\mathbb{R}[x]$ में 3 अखंडनीय गुणनखंड हैं, तथा ये सभी द्विघात हैं।

E22) $x^n - p$ में गुणांक $a_n = 1, a_{n-1} = 0 = \cdots = a_1, a_0 = -p$ हैं।
$\therefore p \mid a_i,\ i = 0, 1, \ldots, n-1$ के लिए, $p \nmid a_n$ तथा $p^2 \nmid a_0$.
अतः, आइसनस्टाइन-निकष द्वारा, $\mathbb{Z}[x]$ में, तथा इसी लिए $\mathbb{Q}[x]$ में, $x^n - p$ अखंडनीय है।

E23) ऐसा नहीं है; $(x^2 + 1)$ एक प्रतिउदाहरण है। (क्यों?)

E24) i) यह अखंडनीय है, क्योंकि इसके मूल $\mathbb{Q}$ में नहीं हैं (या इसे $p = 3$ लेकर, आइसनस्टाइन-निकष का उपयोग करते हुए, दर्शाइए)।

ii) यह अखंडनीय है, $p = 3$ लेकर, आइसनस्टाइन-निकष के उपयोग से।

iii) यह अखंडनीय है, क्योंकि यह एक रैखिक बहुपद है।

iv) ध्यान दीजिए कि यह $\mathbb{Z}$ पर अखंडनीय है क्योंकि यह $5(x^2 + 1)$ है। यह $\mathbb{Q}$ पर अखंडनीय है क्योंकि $\mathbb{Q}$ में इसका कोई मूल नहीं है।

E25) क्योंकि $(\mathbb{Z}_p^*, \cdot)$ कोटि $p - 1$ का समूह है, इसलिए
$\bar{a}^{p-1} = \bar{1}\ \forall\ \bar{a} \in \mathbb{Z}_p^*$.
$\therefore \bar{a}^p = \bar{a}\ \forall\ \bar{a} \in \mathbb{Z}_p^*$.
साथ ही, $\bar{0}^p = \bar{0}$.
$\therefore \bar{a}^p = \bar{a}\ \forall\ \bar{a} \in \mathbb{Z}_p$.
अतः, $\overline{p-a}^p + \bar{a} = \overline{p-a} + \bar{a} = \bar{p} = \bar{0}\ \forall\ \bar{a} \in \mathbb{Z}_p$.
इस प्रकार, $x^p + \bar{a}$ का $\mathbb{Z}_p$ में $\overline{p-a}$ एक शून्यक है।
$\therefore \mathbb{Z}_p$ पर $x^p + \bar{a}$ खंडनीय है।

E26) उदाहरण 6 से आप जानते हैं कि यदि n एक अभाज्य संख्या है, तो यह $\mathbb{Q}[x]$ में अखंडनीय है।
परंतु, यदि आप एक विषम भाज्य पूर्णांक, मान लीजिए $n = 9$ लें, तो $\sum_{i=0}^{9} x^i$ का एक मूल (-1) होता है।
$\therefore$ यह $\mathbb{Q}[x]$ में खंडनीय है।

E27) असत्य। उदाहरणार्थ, $\mathbb{Q}$ पर $3(x + 5)$ अखंडनीय है, परंतु $\mathbb{Z}$ पर नहीं है।

E28) $\mathbb{Z}$ पर x अखंडनीय है। परंतु, $\mathbb{Z}[x] / \langle x \rangle \simeq \mathbb{Z}$, जो एक क्षेत्र नहीं है। अतः, $\mathbb{Z}[x]$ में $\langle x \rangle$ उच्चिष्ठ नहीं है।

E29) i) आइसनस्टाइन-निकष द्वारा दर्शाइए कि $\mathbb{Z}[x]$ पर $x^7 + 7x^6 - 14$ अखंडनीय है, तथा इसी लिए $\mathbb{Q}[x]$ पर भी अखंडनीय है।
$\therefore \mathbb{Q}[x]$ में $\langle x^7 + 7x^6 - 14 \rangle$ उच्चिष्ठ है।
इसलिए, दिया हुआ विभाग वलय एक क्षेत्र है।

ii) प्रमेय 10 द्वारा, $\mathbb{R}[x]$ में x^7+7x^6-14 खंडनीय है।
अतः, $\mathbb{R}[x]$ में $<x^7+7x^6-14>$ उच्चिष्ठ नहीं है।
इसलिए दिया हुआ विभाग वलय एक क्षेत्र नहीं है।

iii) असत्य। यह दर्शाने के लिए कि $\mathbb{Q}$ पर $21x^3-3x^2+2x+9$ अखंडनीय है, Mod p अखंडनीयता परीक्षण का, $p=2$ लेकर, उपयोग कीजिए।

E30) उदाहरणार्थ, $x^{10}-11$ लीजिए। स्पष्ट कीजिए कि यह उदाहरण क्यों यहाँ चल जाता है।

E31) i) यहाँ आइसनस्टाइन-निकष का अनुप्रयोग नहीं किया जा सकता है। आइए $p=3$ के लिए, प्रमेय 14 का अनुप्रयोग करें। हमें $\mathbb{Z}_3[x$ पर बहुपद $\overline{2}x^3+\overline{2}$ प्राप्त होता है।
परंतु इसका एक मूल $\overline{2}$ है।
अतः, $p=3$ लेने पर कोई सहायता नहीं मिलती है।
आइए $p=5$ लेकर प्रयास करें। तब, हमें बहुपद
$\overline{2}x^3+\overline{3}x^2+x+\overline{2}\in\mathbb{Z}_5[x]$ प्राप्त होता है।
आपको इसकी जाँच करनी चाहिए कि $\mathbb{Z}_5$ में इसका कोई शून्यक नहीं है।
इस प्रकार, $\mathbb{Z}_5$ पर यह अखंडनीय है।
अतः, प्रमेय 14 द्वारा, $\mathbb{Q}[x]$ पर $2x^3+3x^2+6x+2$ अखंडनीय है।

ii) इसी प्रकार, यहाँ भी $p=5$ लेकर प्रमेय 14 का अनुप्रयोग कीजिए।

iii) यहाँ $p=3$ लेकर प्रमेय 14 का अनुप्रयोग कीजिए। इस तरह इस पर पहुंचिए कि $\mathbb{Z}_3[x]$ में इसका कोई रैखिक गुणनखंड नहीं है। तब, द्विघात गुणनखंडों के लिए जाँच कीजिए।
मान लीजिए ऐसा एक गुणनखंड $x^2+\overline{a}x+\overline{b}\in\mathbb{Z}_3[x]$ है।
तब, इसका $\mathbb{Z}_3$ में कोई शून्यक नहीं होना चाहिए। अतः, ऐसे गुणनखंडों के लिए केवल संभावनाएँ x^2+1, $x^2+x+\overline{2}$ और $x^2+\overline{2}x+\overline{2}$ हैं।
लंबे विभाजन विधि द्वारा आपको जाँच करनी चाहिए कि इनमें से कोई भी $\mathbb{Z}_3[x]$ में $x^5+\overline{2}x+\overline{1}$ को विभाजित नहीं करता है।
$\therefore \mathbb{Z}_3[x]$ में $x^5+\overline{2}x+\overline{1}$ अखंडनीय है।
अतः, दिया हुआ बहुपद $\mathbb{Q}$ पर अखंडनीय है।

iv) यदि $p(x)=8x^3-6x+1$, तो आप $p(x+1)$ पर आइसनस्टाइन-निकष के उपयोग से दर्शा सकते हैं कि यह $\mathbb{Q}$ पर अखंडनीय है। आप इसे $p=5$ लेकर, प्रमेय 14 का उपयोग करके भी सिद्ध कर सकते हैं।

E32) आपको इसकी जाँच करनी चाहिए कि
$(\overline{3}x+\overline{2})(x+\overline{4})=\overline{3}x^2+\overline{4}x+\overline{3}=(\overline{4}x+\overline{1})(\overline{2}x+\overline{3})$.
साथ ही, ध्यान दीजिए कि $x+\overline{4}=\overline{4}(\overline{4}x+\overline{1})$ तथा $\overline{3}x+\overline{2}=\overline{4}(\overline{2}x+\overline{3})$, जहाँ $\overline{4}\in\mathbb{Z}_5^*$.
अतः, यह प्रमेय 15(ii) का उदाहरण है; यह इसका अंतर्विरोध नहीं करता है।

E33) यहाँ निरीक्षण से काम हो जाता है। आपको इसकी जाँच करनी चाहिए कि दिया हुआ बहुपद $\mathbb{Q}$ पर अखंडनीय बहुपदों के गुणनफल के रूप में $(2x^2+x+2)(x^2+1)$ है।

E34) प्रयास-और-भूल विधि द्वारा, तथा प्रमेय 13 की सहायता से, हमें एक रैखिक गुणनखंड $(x-2)$ प्राप्त होता है।
तब, लंबे विभाजन विधि द्वारा, आप प्रमेय 13 के पुनः अनुप्रयोग से, या निरीक्षण द्वारा, प्राप्त करेंगेः $2x^4-3x^3-8x^2+9x+6=(x-2)(2x^3+x^2-6x-3)$

$$=(x-2)(2x+1)(x-\sqrt{3})(x+\sqrt{3}).$$

यही वाँछित गुणनखंडन है।

E35) सभी पाँच मूल वास्तविक हो सकते हैं, जैसे कि $\prod_{i=1}^{5}(x-a_i)$ में, जहाँ $a_i \in \mathbb{R}$.
इसके 3 वास्तविक और 2 अवास्तविक मूल हो सकते हैं, जैसा कि $(x^2+1)(x+1)^3$ में, या इसका केवल 1 वास्तविक मूल हो सकता है, जैसा कि $(x^2+1)^2(x+1)$ में।

E36) उदाहरणार्थ, $(\bar{2}x+\bar{3})(\bar{4}x+\bar{1})=\bar{3}(\bar{2}x+\bar{1})$.
अतः, $\mathbb{Z}_8$ में $\bar{3}$ एक मात्रक है, क्योंकि $(3, 8)=1$.
अतः, LHS दो अखंडनीय बहुपदों का गुणनफल है, जबकि RHS में केवल एक ही अखंडनीय बहुपद है।

शब्दावली

यह शब्दावली पिछले खंडों में दी हुई शब्दावलियों से आगे बढ़ती है। इसलिए, इस खंड की पढ़ाई करते समय आप उन शब्दावलियों को भी ध्यान में रखिए।

Bi-quadratic/quartic polynomial	चतुर्घात बहुपद
Characteristic	अभिलक्षणिक
Coefficient	गुणांक
Constant term	अचर पद
Cubic polynomial	त्रिघात बहुपद
Cyclotomic polynomial	वृत्तभाजनिक बहुपद
Degree	घात
Division ring	विभाजन वलय
Eisenstein's criterion	आइसनटाइन निकष
Embedded	अंतःस्थापित
Field	क्षेत्र
Idempotent	वर्गसम अवयव
Indeterminate	अनिर्धार्य
Integral domain	पूर्णांकीय प्राँत
Inverse (invertible)	व्युत्क्रम (व्युत्क्रमणीय)
Irreducible	अखंडनीय
Leading coefficient	अग्रग गुणांक
Linear combination	एकघात संचय
Linear polynomial	रैखिक बहुपद
Maximal ideal	उच्चिष्ठ गुणजावली
Monic polynomial	एकगुणांकी बहुपद
Monomial	एकपद
Multiplicity	बहुकता
Multiplicity	बहुकता
Polynomial	बहुपद
Prime ideal	अभाज्य गुणजावली
Primitive	पूर्वग
Quadratic Polynomial	द्विघात बहुपद
Quotient field (field of fractions)	विभाग क्षेत्र
Quotient	भागफल/विभाग
Rational function	परिमेय फलन
Root	मूल
Skew field	विषम क्षेत्र

Term (of a polynomial)	पद (बहुपद का)
Unit	मात्रक
Upper bound	उपरिसीमा
Zero (of a polynomial)	शून्यक (बहुपद का)
Zero divisor	शून्य का भाजक
Zero Polynominal	शून्य बहुपद

विविध उदाहरण और प्रश्न

पिछले खंडों की तरह, नीचे दिए हुए कुछ उदाहरण और प्रश्न इस खंड में आपके द्वारा अध्ययन की गई संकल्पनाओं तथा प्रक्रियाओं पर आधारित हैं। इन उदाहरणों के अध्ययन से तथा इन प्रश्नों को हल करने से, आपको संबंधित संकल्पनाओं के बारे में बेहतर समझ प्राप्त होगी। इससे आपको इस प्रकार के सवालों को हल करने का अधिक अभ्यास भी प्राप्त होगा।

उदाहरण 1: $\mathbb{Z}_{16}$ की सभी अभाज्य गुणजावलियाँ तथा उच्चिष्ठ गुणजावलियाँ ज्ञात कीजिए।

हल: $\mathbb{Z}_{16}$ की गुणजावलियाँ $\overline{m}\mathbb{Z}_{16}$ के रूप की होती है, जहाँ $m|16$.
अतः, $m = 1, 2, 4, 8$ और 16 है।
इस प्रकार, उचित गुणजावलियाँ $\{0\}, <\overline{2}>, <\overline{4}>$ और $<\overline{8}>$ है।
क्योंकि 16 एक अभाज्य संख्या नहीं है, इसलिए $\mathbb{Z}_{16}$ एक प्राँत नहीं है। अतः, $\{\overline{0}\}$ एक अभाज्य गुणजावली नहीं है।
आगे, तुल्याकारिता प्रमेयों द्वारा, $\mathbb{Z}_{16}/<\overline{2}> \simeq \mathbb{Z}_2$ है, जो एक क्षेत्र है।
अतः, $\mathbb{Z}_{16}$ की $<\overline{2}>$ एक उच्चिष्ठ गुणजावली है, तथा इसीलिए यह $\mathbb{Z}_{16}$ की एक अभाजय गुणजावली है।
अब, आइए $<\overline{4}>$ पर विचार करें। क्योंकि $\overline{4} \in <\overline{4}>$ है s.t. $(\overline{4})^2 = \overline{16} = \overline{0}$ है और $\overline{4} \neq \overline{0}$ है, इसलिए $\mathbb{Z}_{16}$ की $<\overline{4}>$ एक अभाज्य गुणजावली नहीं है।
इसी प्रकार, दर्शाइए कि $\mathbb{Z}_{16}$ की $<\overline{8}>$ एक अभाज्य गुणजावली क्यों नहीं है।
इस प्रकार, $\mathbb{Z}_{16}$ की केवल अभाज्य गुणजावली $<\overline{2}>$ है, तथा यही इसकी केवल उच्चिष्ठ गुणजावली है।

***

उदाहरण 2: सिद्ध कीजिए कि $\mathbb{Z}_n$ की अभाज्य गुणजावलियाँ $n\mathbb{Z}$ को अंतर्विष्ट करने वाली $\mathbb{Z}$ की अभाज्य गुणजावलियों के संगत हैं, जहाँ $n \in \mathbb{N}$.

हल: हमें प्राकृतिक आच्छादक समाकारिता $\pi : \mathbb{Z} \to \mathbb{Z}_n : \pi(m) = m + n\mathbb{Z} = \overline{m}$ प्राप्त हैं यहाँ, $\text{Ker } \pi = n\mathbb{Z}$.
इकाई 14 के E47(iii) द्वारा, अब आपको परिणाम प्राप्त हो जाता है।

***

उदाहरण 3: यदि R और S दो वलय हैं तथा $f: R \to S$ एक समाकारिता तो R की प्रत्येक उच्चिष्ठ गुणजावली M के लिए, S की $f(M)$ एक उच्चिष्ठ गुणजावली होती है। सत्य या असत्य? क्यों?

हल: प्राकृतिक map $\pi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ पर विचार कीजिए।
अब, $\mathbb{Z}$ में $5\mathbb{Z}$ उच्चिष्ठ है, परंतु $\pi(5\mathbb{Z}) = \mathbb{Z}/6\mathbb{Z}$ है, क्योंकि $(5, 6) = 1$.
अतः, $\pi(5\mathbb{Z})$ एक उचित गुणजावली नहीं है। इस प्रकार, यह $\mathbb{Z}/6\mathbb{Z}$ की एक उच्चिष्ठ गुणजावली नहीं है। अतः, दिया हुआ कथन असत्य है।

***

उदाहरण 4: यदि R एक तत्समकी क्रमविनिमय वलय है, तो क्या $R[x]$ एक क्षेत्र हो सकता है? क्यों या क्यों नहीं?

हल: मान लीजिए कि $R[x]$ एक क्षेत्र है। तब, $x^{-1} \in R[x]$ मान लीजिए
$x^{-1} = f(x) \in R[x]$.
अतः, $xf(x) = 1$. …(1)
साथ ही, क्योंकि $R[x]$ बिना शून्य के भाजकों का है, इसलिए R बिना शून्य के भाजको का है।
इस प्रकार, (1) द्वारा, $1 + \deg f(x) = 0$ है, जो एक अंतर्विरोध है।
अतः, $R[x]$ एक क्षेत्र नहीं है।

***

उदाहरण 5: सिद्ध कीजिए कि यदि किसी वलय का अभिलक्षणिक शून्य है, तो उसे अपरिमित होना चाहिए।

हल: मान लीजिए कि R एक वलय है, जिसका अभिलक्षणिक शून्य है।
यदि कोई $a \in R$ है s.t. $o(a)$ अपरिमित है, तो R का $\{na \mid n \in \mathbb{Z}\}$ एक अपरिमित उपसमुच्चय है। इस प्रकार, R को अपरिमित होना चाहिए।

अब, उस स्थिति पर विचार कीजिए कि R के प्रत्येक अवयव की परिमित कोटि है। मान लीजिए कि, यदि संभव है तो, मान लीजिए $R = \{a_1, a_2, \ldots, a_n\}$ है।
मान लीजिए कि $o(a_i) = m_i \forall i = 1, \ldots, n$ है।
तब, $m = m_1 m_2 \ldots m_n$ के लिए, $ma_i = 0 \ \forall i = 1, \ldots, n$ है।
अतः, char R परिमित है, जो हमारी परिकल्पना का एक अंतर्विरोध है।
इसलिए, R को अपरिमित होना चाहिए।

***

उदाहरण 6: $\mathbb{Z}_2$ पर एक उपयुक्त अखंडनीय बहुपद का उपयोग करते हुए, 8 अवयवों के एक क्षेत्र की रचना चाहिए।

ध्यान दीजिए कि उदाहरण 6 के क्षेत्र में p^r अवयव हैं, जहाँ $p = 2$ और $r = 3$.

हल: हम 2^3 अवयवों वाले एक क्षेत्र की खोज कर रहे हैं। इसलिए, हम इकाई 16 की प्रमेय 6 और उपप्रमेय 3 का उपयोग करते हैं, तथा $\mathbb{Z}_2$ पर एक अखंडनीय **त्रिघात** बहुपद की खोज करने का प्रयास करते हैं।
आइए $f(x) = x^3 + x + 1$ पर विचार करें।
आपको इसकी जाँच करनी चाहिए कि $\mathbb{Z}_2$ पर $f(x)$ अखंडनीय है।
अतः, $\mathbb{Z}_2[x] / \langle x^3 + x + 1 \rangle = \{ax^2 + bx + c + \langle x^3 + x + 1 \rangle \mid a, b, c \in \mathbb{Z}_2\}$ एक क्षेत्र हैं।
क्योंकि a, b, c दो 2 मानों को ग्रहण कर सकते हैं, इसलिए इस क्षेत्र में अवयवों की संख्या 8 है।
अतः, यही वाँछित क्षेत्र है।

***

उदाहरण 7: मान लीजिए कि F एक क्षेत्र है तथा $f(x) \in \langle x \rangle$ है। मान लीजिए कि $K = \{\alpha \in F \mid f(\alpha) = 0\}$ है। क्या F और K का एक उपवलय है? अपने उत्तर के लिए कारण दीजिए।

हल: $f(x) = x(x-1) \in \mathbb{R}[x]$ पर विचार कीजिए। यहाँ, $K = \{0, 1\}$ अतः $\mathbb{R}$ का K एक उपवलय नहीं है।

***

विविध प्रश्न

E1) यदि R और S तत्समकी वलय हैं तथा $f: R \to S$ एक एकैक समाकारिता है, तो दर्शाइए कि $\text{char } R = \text{char } S$ है।

E2) मान लीजिए कि F एक क्षेत्र है तथा R एक वलय है s.t. $f: F \to R$ एक वलय समाकारिता है। दर्शाइए कि f शून्य map है या f एकैकी है।

E3) मान लीजिए कि R एक प्रॉंत है। दर्शाइए कि $o(r) = o(s) \ \forall \ r, s \in R$ है, जहाँ $o(x)$ समूह $(R, +)$ के एक अवयव x की कोटि को व्यक्त करता है।

E4) मान लीजिए कि R एक क्रमविनिमय वलय है s.t. $(R, +)$ की कोटि 10 है। क्या R एक पूर्णांकीय प्रॉंत हो सकता है? क्यों या क्यों नहीं?

E5) मान लीजिए कि R एक पूर्णांकीय प्रॉंत ळें यदि $\text{char } R = 0$ है, तो दर्शाइए कि प्रत्येक शून्येतर अवयव की कोटि अपरिमित है। यदि $\text{char } R = p$ है, तो दर्शाइए कि प्रत्येक शून्येतर अवयव की कोटि p है।

E6) क्या $\mathbb{Q}[x]$ पर $3x^5 + 15x^4 - 20x^3 + 10x + 20$ अखंडनीय है? क्या यह $\mathbb{R}[x]$ पर अखंडनीय है? अपने उत्तरों के कारण दीजिए।

E7) मान लीजिए कि F एक क्षेत्र है, $f(x) \in F[x]$ तथा $a \neq 0, a \in F.$

i) यदि F पर $af(x)$ अखंडनीय है, तो सिद्ध कीजिए कि F पर $f(x)$ अखंडनीय है।

ii) यदि F पर $f(ax)$ अखंडनीय है, तो सिद्ध कीजिए कि F पर $f(x)$ अखंडनीय है।

iii) यदि F पर $f(x+a)$ अखंडनीय है, तो सिद्ध कीजिए कि F पर $f(x)$ अखंडनीय है।

E8) 25 अवयवों वाले एक क्षेत्र की रचना कीजिए।

E9) जाँच कीजिए कि निम्नलिखित बहुपद अखंडनीय है या नहीं:

i) $\mathbb{Q}$ पर $\dfrac{5}{2}x^5 + \dfrac{9}{4}x^4 + \dfrac{15}{4}x^3 + \dfrac{3}{5}x^2 + \dfrac{6}{7}x + \dfrac{3}{10}$

ii) $\mathbb{Z}_{11}$ पर $x^2 + x + 4$

iii) $\mathbb{Z}_{11}$ पर $x^4 + 1$

iv) $\mathbb{Q}$ पर $x^4 + 15x^3 + 7$

v) $\mathbb{Z}$ पर $x^3 + (5m+1)x + (5n+1)$, जहाँ $m, n \in \mathbb{Z}.$

E10) मान लीजिए कि $f(x) \in F[x]$ है, जबकि F एक क्षेत्र है। दर्शाइए कि किसी $a \in F$ के लिए, $(x-a) \mid [f(x) - f(a)].$

E11) मान लीजिए कि $f(x) \in \mathbb{Z}[x]$ एक एकगुणांकी बहुपद है। मान लीजिए कि $\alpha \in \mathbb{Q}$ s.t. $f(\alpha) = 0$ है। दर्शाइए कि $\alpha \in \mathbb{Z}.$

E12) मान लीजिए कि F एक परिमित क्षेत्र है। F पर एक ऐसा बहुपद ज्ञात कीजिए, जिसका F में कोई मूल नहीं है।

हल / उत्तर

E1) मान लीजिए कि $f: R \to S$ एक एकैक समाकारिता है, तथा यह भी मान लीजिए कि $\text{char } R = m, \text{ char } S = n.$
अब, m न्यूनतम धनात्मक पूर्णांक है s.t.
R में $m \cdot 1 = 0$ है। …(2)
साथ ही, S में $f(1)$ तत्समक है। अतः, परिभाषा द्वारा n न्यूनतम (लघुतम) धनात्मक पूर्णांक है s.t.
S में $n \cdot f(1) = 0$ है। …(3)
S में (2) हमें $m \cdot f(1) = f(0) = 0$ प्रदान करता है। …(4)
(3) और (4) से, हम $m \geq n$ प्राप्त करते हैं।
इसी प्रकार, आपको देखना चाहिए कि $n \geq m$ क्यों है।
इस प्रकार, $m = n$.

E2) मान लीजिए कि $f \neq \mathbf{0}$ है। क्योंकि F की Ker f एक गुणजावली है तथा Ker $f \neq F$ है, इसलिए हम Ker $f = \{0\}$ प्राप्त करते हैं। इस प्रकार, f एकैकी $(1\text{-}1)$ है।

E3) मान लीजिए कि $o(r) = m$ और $o(s) = n$ है।
तब, $mr = 0, ns = 0$ तथा m और n ऐसे न्यूनतम धनात्मक पूर्णांक हैं।
अब, $mr = 0 \Rightarrow (mr)s = 0$
$\Rightarrow r(ms) = 0$
$\Rightarrow ms = 0$, क्योंकि $r \neq 0$ है।
$\therefore n|m.$ …(5)
इसी प्रकार, आपको दर्शाना चाहिए कि $m|n$ है। …(6)
(5) और (6) से, हमें $m = n$, प्राप्त होता है। अर्थात् $o(r) = o(s)$ है।

E4) क्योंकि 10 को विभाजित करने वाली अभाज्य संख्याएँ 2 और 5 हैं, इसलिए परिमित आबेली समूहों के लिए कौशी प्रमेय द्वारा (इकाई 7 को देखिए), $a, b \in R$ s.t. $o(a) = 2$ और $o(b) = 5$ प्राप्त करते हैं।
अब $o(a) = 2 \Rightarrow 5a = a \neq 0.$
साथ ही, $o(b) = 5 \Rightarrow 2b \neq 0.$
परंतु, $(5a)(2b) = 10ab = 0$ है, क्योंकि $o(R) = 10.$
इस प्रकार, R में 5a और 2b शून्य के भाजक हैं।
अतः, R एक पूर्णांकीय प्राँत नहीं है।

E5) E3 द्वारा, $o(r) = o(1) \ \forall \ r \in R^*$ है। …(7)
यदि $\text{char } R = 0$, तो $o(1)$ अपरिमित है।
अतः, (7) द्वारा, $\forall \ r \in R^*$, $o(r)$ अपरिमित है।

यदि $\text{char } R = p$, तो (7) द्वारा, $o(1) = p = o(r) \ \forall \ r \in R^*$ है।

E6) मान लीजिए कि $p(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$ है।
अब,, x^4, x^3, x^2, x^1 और x^2 में से प्रत्येक के गुणांक $15, -20, 0, 10$ और 20 को 5 विभाजित करता है।
साथ ही, $5 \nmid 3$, जो अग्रग गुणांक है तथा $5^2 \nmid 20$, जो अचर पद है।

अतः, आइन्सटाइन-निकष द्वारा, $\mathbb{Q}$ पर $p(x)$ अखंडनीय है।

क्योंकि $\deg p(x) > 2$ है, इसलिए यह $\mathbb{R}$ पर खंडनीय है।

E7) i) इसके विपरीत मान लीजिए कि F पर $f(x)$ खंडनीय है।
तब, $F[x]$ में, $f(x) = g(x)h(x)$ है, जहाँ $\deg g(x) \geq 1$ और $\deg h(x) \geq 1$ है।
$\Rightarrow af(x) = [ag(x)]h(x)$, जबकि $\deg ag(x) \geq 1$ है और $\deg h(x) \geq 1$ है।
इस प्रकार, $F[x]$ में $af(x)$ खंडनीय है, जो एक अंतर्विरोध है।

आप (i) की तरह की प्रक्रिया अपना कर (ii) और (iii) को हल कर सकते हैं।

E8) ध्यान दीजिए कि $25 = 5^2$ है। अतः, कोटि 25 के एक क्षेत्र की रचना के लिए, हम $\mathbb{Z}_5$ पर एक अखंडनीय द्विघात बहुपद की खोज करने का प्रयास कर सकते हैं। आप हल को पूरा करने के लिए उदाहरण 6 को देख सकते हैं।

E9) i) मान लीजिए कि $f(x)$ दिया हुआ बहुपद है तथा $g(x) = 140f(x)$ है।
तब, $g(x) = 350x^5 + 315x^4 + 525x^3 + 84x^2 + 120x + 42$ है।
अब, $p = 3$ लेकर तथा आइन्सटाइन-निकष के अनुप्रयोग से आपको यह निष्कर्ष निकालने में समर्थ हो जाना चाहिए कि $\mathbb{Q}$ पर $g(x)$ अखंडनीय है।
अतः, $\mathbb{Q}$ पर $f(x)$ अखंडनीय है (E7(i) के उपयोग से)।

ii) आपको इसकी जाँच करनी चाहिए कि $\mathbb{Z}_{11}$ का कोई भी अवयव दिए हुए बहुपद का मूल नहीं है। अतः, यह अखंडनीय है।

iii) पुनः, (ii) की ही तरह, दर्शाइए कि यह अखंडनीय है।

iv) $p = 3$ के लिए, $\bmod p$ टेस्ट का उपयोग करते हुए, आपको दर्शाना चाहिए कि यह अखंडनीय है।

v) $p = 5$ के लिए $\bmod p$ टेस्ट का उपयोग कीजिए तथा इसे सिद्ध कीजिए।

E10) मान लीजिए कि $g(x) = f(x) - f(a) \in F[x]$ है। तब, $g(a) = 0$ है। अर्थात्, $g(x)$ का a एक मूल है। अतः, $(x-a) | g(x)$ है। इससे परिणाम प्राप्त हो जाता है।

E11) मान लीजिए कि $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ है तथा मान लीजिए कि $(p, q) = 1$ के साथ, $\alpha = \frac{p}{q}$ है।

तब, $p^n + a_{n-1}p^{n-1}q + \cdots + a_1pq^{n-1} + a_0q^n = 0$ है।
यदि $q = \pm 1$, तो $\alpha \in \mathbb{Z}$ है।
मान लीजिए कि $q \neq \pm 1$ है तथा q को विभाजित करने वाली अभाज्य संख्या r_1 है। तब, $[-q(a_{n-1}p^{n-1} + \cdots + a_1pq^{n-2} + a_0q^{n-1})] = p^n$ को r_1 विभाजित करता है।
अतः, $r_1 | p$ है (देखिए इकाई 1)।
हम एक अंतर्विरोध पर पहुँच जाते हैं, क्योंकि $(p, q) = 1$ है।

अतः, q के कोई अभाज्य गुणनखंड नहीं हैं।
इसलिए, $q = \pm 1$ है। अर्थात्, $\alpha \in \mathbb{Z}$ है।

E12) मान लीजिए कि $F = \{a_1, a_2, \ldots, a_n\}$ है। तब,

$$f(x) = 1 + \prod_{i=1}^{n} (x - a_i) \in F[x] \text{ है।}$$

साथ ही, $f(a_i) = 1 \ \forall \ i = 1, \ldots, n$ है।
इस प्रकार, F का कोई भी अवयव $f(x)$ का एक मूल नहीं है।
अतः, $f(x)$ दिए हुए प्रतिबंधों (अवरोधों) को संतुष्ट करता है।