תרגיל בית מס' 8

שאלה מס' 1

נסמן $\alpha = \sqrt{-6}$. נשים לב כי $(\alpha+1)(\alpha-1) = 2\cdot 3 = 6$ ולכן 6 אינו ראשוני.
נראה כי $\mathbb{Z}[\alpha] = \mathbb{Z}_{\alpha}$ הינו תחום פריקות יחידה.

תשובה

נשים לב כי $\alpha + 1$ הינו איבר בלתי פריק.
נעזר בטענה, הנובעת ישירות מהגדרת הנורמה, שכן נוכיח תחילה כי הנורמה היא כפלית ושונה מאפס עבור כל α שאינו איבר הפיך.
נראה תחילה שהנורמה שלנו הינה:
$$N(a+b\sqrt{-6}) = a^2 - 6b^2$$
נניח בשלילה שאכן α הינו פריק ונסיק כי קיים β שאינו הפיך ומחלק את α.
נראה תחילה כי β אינו ± 1.

$$N(1+\sqrt{-6}) = 1 - 6 = -5$$
$$N(-1+\sqrt{-6}) = 1 - 6 = -5$$

נשים לב כי $N(2\cdot 3) = 6$ ולכן נשים לב כי $N(2+\sqrt{-6}) = 4 - (-6) = 10$; $N(3+\sqrt{-6}) = 9 - (-6) = 15$
$N(3-\sqrt{-6}) = 9 - (-6) = 15$
$(2+\sqrt{-6})\cdot(3-\sqrt{-6}) = 1+\sqrt{-6}$
$(-2+\sqrt{-6})\cdot(3+\sqrt{-6}) = 1+\sqrt{-6}$

ולכן:
$$(\sqrt{-6}+3)(\sqrt{-6}+2)(\sqrt{-6}-3)(\sqrt{-6}+2) = (\sqrt{-6}+1)(\sqrt{-6}-1) = 6$$

ומכאן נובעת כי $2\cdot 3$ אינה יחידה.

~~$\frac{3}{-3+\sqrt{-6}} = -2+\sqrt{-6}$~~ ; $\frac{2}{-3}$

$\frac{3}{2+\sqrt{-6}} = -2+\sqrt{-6}$; $\frac{2}{3+\sqrt{-6}} = (3+\sqrt{-6})$

וכיוצ"ב: $(\sqrt{-6}+2)(\sqrt{-6}-2)\cdot(\sqrt{-6}+3)(\sqrt{-6}+3) = 2\cdot 3 = 6$
ולכן אינו פריק.

Scanned by CamScanner

שאלה מס' 2 ②

נגדיר: שדה מרוכבים: הוא: $\Theta_{-6} = \mathbb{Z}[\sqrt{-6}]$

$3 \cdot -2 = \sqrt{-6}\sqrt{-6}$

לא הפירוק פה: איברים אינם הפיכים ואינם כאשונים.

הוכחה

הוא: $\Theta_{-7} = \mathbb{Z}[\sqrt{-7}]$, הנורמה ל- $\mathbb{Z}[\sqrt{-7}]$ הינה:

$$\|a+b\sqrt{-7}\| = a^2+7b^2$$

כלל, כפל שאינו כ- 1 ו- a הינורמה גדלה.

דוגמה שלנו

2- אי פריק. למה? הנורמה שלו $\|-2\| = 4$

~~הוכחה לפריקות~~

נניח ש- 2 פריק: $A \cdot B = -2$. אז: $\|-2\| = \|A\| \cdot \|B\|$.

כי הנורמה של A חייבת לחלק את 4.

A - אז יכול להיכתב $a+b\sqrt{-7}$ כך

לכן A מכיל רק איברי חוגיות a.

יוצא ש- -2, אי פריק (אז גם 2 ו- (-1) כי -1 הפיך), כי 2 לא פריק. (1- שאר כמו 1, כי הפיכים אינם פריקים ולכן גם לא שאר פריקים).

3 אי פריק

למה? הנורמה שלו $\|3\| = 9$

נניח ש- 3 פריק: $A \cdot B = 3$.

אז: $\|3\| = \|A\| \cdot \|B\|$ ולכן: $\|A\|$ או $\|B\|$.

אחד הפריקים (נניח A) מכיל $a+b\sqrt{-7} = A$ (סוגה א-ס)

ל- $\sqrt{-7}$, כי שאחד הפריקים מכיל $\sqrt{-7}$ כמכפלה, ולכן נקבל 3.

Scanned by CamScanner

$\|A\| \geq 6$
$\|B\| \geq 6$
$\Downarrow$
$\|A\|\,\|B\| \geq 36 > 9 = |B|$

ולכן מתקיים עפ"י ט': $A \cdot B = 3$

ומכך ש A מכיל מספר שלם של $\sqrt{-6}$ ($A = u + v\sqrt{-6}$).

אחרת A ניתן לחלק ב 3 ולכן: $A = 3$ ו- $b = 1$ (אז כבר סיימנו ומכך ש $A + B$) ומכך 3 הוא פרי.

$\sqrt{-6}$ הוא פרי

נניח שהוא פרי. ואז הוא מחלק את $A \cdot B = \sqrt{-6}$.

$\|\sqrt{-6}\| = 6$

ומכך ש פרי $\|A\| < 6$ ולכן $\|B\| < 6$.

אחרת נניח כי אומר שיתכן A ולכן B הוא מכפלת מספרים (כלומר A, B לא יחידות) שאינם $\sqrt{-6}$.

אחרת מכפלה של $a_A \to a_{AB}$ הוא מחלק את $\sqrt{-6}$.

לכן $\sqrt{-6}$ אי פרי.

שני הראשונים אינם חברים

נניח ש u הוא הפרי כך ש:

$3 \cdot u = 2$
$\Downarrow$
$u = \frac{2}{3} \notin \mathcal{O}_{-6}$

נניח ש u הוא פרי כך ש:

$3 \cdot u = \sqrt{-6}$
$\Downarrow$
$u = \frac{1}{3}\sqrt{-6} \notin \mathcal{O}_{-6}$

נניח ש u הוא פרי כך ש:

$2 \cdot u = \sqrt{-6}$
$\Downarrow$
$u = \frac{1}{2}\sqrt{-6} \notin \mathcal{O}_{-6}$

לכן הם אינם חברים.

Scanned by CamScanner

נוכיח שהאידיאלים הראשוניים שמצאנו הראשוניים - הם הראשיים.

א. נוכיח עבור $\langle -2 \rangle$:

$$\langle -2 \rangle = -2a - 2b\sqrt{-6}$$

כאשר $a, b \in \mathbb{Z}$.

נשים לב:

$$3\sqrt{-6} \notin \langle -2 \rangle$$

$$(3 \cdot \sqrt{-6}) \cdot (3\sqrt{-6}) = -54 \in \langle -2 \rangle$$

$\Downarrow$

$\langle -2 \rangle \Rightarrow$ לא ראשוני -2 לא ראשוני.

ב. נוכיח עבור $\langle 3 \rangle$:

$$\langle 3 \rangle = 3a + 3b\sqrt{-6}$$ כאשר $a, b \in \mathbb{Z}$

נוכיח: $2 \cdot \sqrt{-6} \notin \langle 3 \rangle$

$$(2 \cdot \sqrt{-6}) \cdot (2\sqrt{-6}) = -24 \in \langle 3 \rangle$$

$\Downarrow$

$\langle 3 \rangle$ - לא ראשוני

$\Downarrow$

3 - לא ראשוני.

ג. נוכיח עבור $\sqrt{-6}$:

~~$\langle \sqrt{-6} \rangle = a\sqrt{-6} + (b\sqrt{-6}) \cdot \sqrt{-6}$~~

$$\langle \sqrt{-6} \rangle = (a + b\sqrt{-6}) \cdot \sqrt{-6} = -6b + a\sqrt{-6}$$

נוכיח:

$3 \notin \sqrt{-6}$

$2 \notin \sqrt{-6}$

$$2 \cdot 3 = 6 = \sqrt{-6} \cdot (\sqrt{-6}) \in \langle \sqrt{-6} \rangle$$

$\Downarrow$

$\langle \sqrt{-6} \rangle$ - לא ראשוני.

$\Downarrow$

$\sqrt{-6}$ - לא ראשוני.

Scanned by CamScanner

שאלה מס' 3

(5)

יהי F שדה. הוכיחו שהחוג הבא הוא תחום:

$$F[x,y,z]/\langle z^2-xy\rangle$$

שימו לב שהאידיאל הראשי הוא

הפתרון

$$(z+x)(z-x)\in F[x,y,z]$$

$$(z+x)(z-x)=z^2-x^2$$

$$x(x-y)=x^2-xy \text{ modulo } \langle z^2+xy\rangle \text{ שווה ל } (z+x)(z-x)$$

כלומר הוא שווה ל-

$$\frac{F[x,y,z]}{\langle z^2-xy\rangle}$$

יש לנו

2 פתרונות לפולינום זהה:

$$x(x-y) \qquad -1\cdot(z-x)(z+x)$$

יש לפולינום שהוא הוא מעל F (א) ו (ב) פולינום אחר

ב x של $(z+x)$

ב x של $(z-x)$.

עכשיו אנחנו הולכים להראות:

$$\frac{F[x,y,z]}{\langle z^2-xy\rangle}\cong F[x,y,\sqrt{xy}]$$

כלומר $F[x,y,\sqrt{xy}]$ הוא תחום כי הוא משוכן ב-

$$\sqrt{xy}\ y\ x$$

ולכן x הוא שורש של פולינום, כי

נסיון לפרק x מכפלת פולינומים יתן

Scanned by CamScanner

(6)

שלכל שדה F מעל $\mathbb{Q}$ ומספר טבעי $n-1$ שדה F / $\mathbb{Q}$ שדה מעל $\mathbb{Q}$ ומספר טבעי $n-1$ שלכל

$(k_1, k_2) \cdot (x_1, x_2)$ נגדיר: $k_1, k_2 \in F$.

שדה F מעל $\mathbb{Q}$ שבו $x \neq (x+z)$ ו- $x \neq (x-z)$.

הוכחה:

נגדיר הצמדה:

$$x+z \longmapsto x+\sqrt{xy}$$
$$x-z \longmapsto x-\sqrt{xy}$$

$$\frac{x \pm \sqrt{xy}}{x} = 1 \pm \sqrt{\frac{y}{x}}$$

נראה כי $\sqrt{\frac{y}{x}}$ אינו איבר של $F[x, y, \sqrt{xy}]$

נניח: $x = (x+z)$

נפתח כי מתקיים:

$$(x+z)(x-z) = x(x-y)$$

יש 2 פתרונות שונים.

סתירה

Scanned by CamScanner

הוכיחו ש-x הוא $\sqrt{y}$-פרימיטיבי ב-$F[x,\sqrt{xy}]$

כל פולינום $p(x)$, שהוא מעל $F[x,\sqrt{xy}]$,

שהוא גם מעל $F[x^{1/2}, y^{1/2}]$

הוא מקיים פירוק יחיד.

נראה כעת, ש-x הוא פרימיטיבי:

(עד כאן מהכלים הרגילים) $x = x^{1/2}\cdot x^{1/2}$

קבוע = מחלק משותף.

הפירוק שהפרימיטיבי $x = x^{1/2}\cdot x^{1/2}$ לא שייך

ל-x: $F[x,\sqrt{xy}]$, כיוון שהוא פירוק ל-x

ב- $F[x,\sqrt{xy}]$ (מלבד: $x\cdot(x^{-1})$),

שכיוון שלפי ההגדרה של פירוק יחיד כך, הוא

הפירוק פרימיטיבי שמספיק לי. $F[x^{1/2}, y^{1/2}]$

וכך לכל ימין.

Scanned by CamScanner

כל איבר y:

⑦

שאלה מס' 4

יהי R תחום. נגדיר פונקציה נורמה אוקלידית

N על R באופן הבא: $N(0)=0$ ולכל $a\in R$ $a\neq 0$:

$N(a)=\left|\frac{R}{\langle a\rangle}\right|=$ (מספר איברי חוג המנה)

טענה א'

הוכיחו שאם R תחום שלמים אז N היא פונקציה נורמה.

הוכחה

יהיו איברים לא אפסים $a,b\in R$

נשים לב ש $\langle a\rangle$

יש עוד לפחות $\langle b\rangle$

ויש עוד לפחות $\langle ab\rangle$.

לכן מתקיים היחס הבא:

$$\frac{\frac{R}{\langle ab\rangle}}{\frac{\langle b\rangle}{\langle ab\rangle}}=\frac{R}{\langle b\rangle}$$

וזה שמגדיר חוג מנה אז כל הגרסאות חופשיות/חוג אלגי:

$$\frac{R}{\langle b\rangle}\ ,\ \frac{\langle b\rangle}{\langle ab\rangle}\ ,\ \frac{R}{\langle ab\rangle}$$

ולכן גם כפל אחד בשני שווה תכונה חלוקתית.

לכן, לפי משפט לגרנג' במתמטיקה תכונה חלוקתית:

$$\frac{\left|\frac{R}{\langle ab\rangle}\right|}{\left|\frac{\langle b\rangle}{\langle ab\rangle}\right|}=\left|\frac{R}{\langle b\rangle}\right|$$

$$\Downarrow$$

$$\left|\frac{R}{\langle ab\rangle}\right|=\left|\frac{\langle b\rangle}{\langle ab\rangle}\right|\cdot\left|\frac{R}{\langle b\rangle}\right|$$

משלים מס' 1

Scanned by CamScanner

נרצה למצוא את $\frac{\langle b\rangle}{\langle ab\rangle}$?

$$\langle b\rangle = R\cdot b$$
$$\langle ab\rangle = Rab$$

$$\frac{\langle b\rangle}{\langle ab\rangle} = (R\cdot b) \text{ modulo } (R\cdot ab)$$

כל איבר x:

$$x \in \frac{\langle b\rangle}{\langle ab\rangle}$$

אז נקבל:

$$x = r_1 b - r_2 ab = (r_1 - r_2 a)\cdot b$$

(כאשר $r_1, r_2 \in R$).

כל איבר y: $y \in \frac{R}{\langle a\rangle}$, אז נקבל:

$$y = (r_1 - r_2 a)$$

כאשר $r_1, r_2 \in R$.

לכן, לכל $x \in \frac{\langle b\rangle}{\langle ab\rangle}$ יש פתרון y אחד: $y \in \frac{R}{\langle a\rangle}$

כאשר מקבלים: $x = b\cdot y$.

ולכן מספר איברי y: $\left|\frac{R}{\langle a\rangle}\right|$, שהוא מספר איברי x: $\left|\frac{\langle b\rangle}{\langle ab\rangle}\right|$

$$\left|\frac{R}{\langle a\rangle}\right| \geq \left|\frac{\langle b\rangle}{\langle ab\rangle}\right|$$

כי איברי R- הם כפשהו.

תרגיל בבית.

R חוג חילופי שלם. הוכיחו בשלילה: שאם $x_1 \neq x_2$, אז:

$x_1 = b\cdot y_1$, $x_2 = b\cdot y_2$

$$\Downarrow$$

$$b\cdot y_2 = b\cdot y_1$$

מהשלם שלמד, נובע שמכאן ש- b וגם עבור $y_2 = y_1$.

בשורה הקודמת סתירה.

לכן:

$$\left|\frac{R}{\langle a\rangle}\right| = \left|\frac{\langle b\rangle}{\langle ab\rangle}\right|$$

Scanned by CamScanner

נניח כעת כי a, b זרים זה לזה.

$$\left|\frac{R}{\langle ab\rangle}\right| = \left|\frac{R}{\langle a\rangle}\right| \cdot \left|\frac{R}{\langle b\rangle}\right|$$

$$\Downarrow$$

$$N(ab) = N(a) \cdot N(b)$$

מש"ל

טענה ג'

תהי R חוג קומוטטיבי יחידה סופי ויהי a איבר הפיך בR. אזי a אינו מחלק של אפס.

הוכחה:

נניח כי a מחלק של אפס:

$R = \mathbb{Z}_4 = \{0,1,2,3,4,5\}$

$a = 3$; $b = 3$

$\langle a\rangle = \{0,3\}$

$\langle b\rangle = \{0,3\}$

$$N(a) = \left|\frac{R}{\langle a\rangle}\right| = 3$$

$$N(b) = \left|\frac{R}{\langle b\rangle}\right| = 3$$

$ab = 3 \cdot 3 = 3$

$\langle ab\rangle = \{0,3\}$

$$N(ab) = \left|\frac{R}{\langle ab\rangle}\right| = 3$$

זהו מספיק!

$$N(ab) = N(a) \cdot N(b)$$

Scanned by CamScanner

משפט. יהי R תחום שלמות בו כל אידיאל הוא עקרי. אז R הוא תחום פריק יחידה.

הגדרה

~~הגדרה~~ הנורמה ההרגילה שבשלם ריבועי.

$$N(a+b\sqrt{D}) = |a^2 - Db^2|$$

למה | יהי $D \bmod 4 = 2,3$

נסמן ב: $\left|\frac{\langle r \rangle}{R}\right|$

הוכחה: $\alpha = a+b\sqrt{D} = r$ עבור $\beta \in \mathbb{Z}$.

קיבלנו שאידיאל הגורם $\langle r \rangle$, נקרא "כפולות $\sqrt{D}$".

בפרט, ~~הוכחנו~~: הוכחנו: אם נסמן:

$$a+b\sqrt{D}$$

נקרא: $(a+b\sqrt{D}) \bmod (\sqrt{D}k+\ell) = a+b\sqrt{D} + (\sqrt{D}k+\ell)\cdot(\sqrt{D}y+x)$

למה | יהי $z \in \mathbb{Z}$ כך ש: יחלק ב $\sqrt{D}$ ויחלק גם ב a.

הוכחה:

$$\alpha x + \beta y = 1$$

נכפול ב q - נקבל שאידיאל αx כולל

$$\alpha x + \beta y = q$$

קיבלנו - שהשארית כן יכולה להיות r.

- אם $r=0$ נקבל שאנחנו "כפולות" של q.

- אם $r \neq 0$ נקבל ש q שונה. $q \mid g$ ויהיה גדול יותר

בסתירה. (g מקסימלי ב.ש.ג).

לסיכום: ~~הוכחנו~~ הוכחנו שכל $\sqrt{D} \in \{1-g, \dots, g\}$ שאינו מספר אי-פריק שכל

Scanned by CamScanner

משפט השארית הסיני

$(\alpha,\beta)=1$ אם"ם $(\beta,\alpha)=1$

$\exists \alpha+\beta=r$, α ו- β זרים $(\alpha,\beta)=1$.

נבחר ב"ל שלם n שמתלק ב r.

כמו כן:

$$\frac{0}{r}=0$$

וכמו כן:

$$\frac{n}{r}=\frac{n}{\alpha+\sqrt{D}\beta}=\frac{n(\alpha-\sqrt{D}\beta)}{(\alpha+\sqrt{D}\beta)(\alpha-\sqrt{D}\beta)}=\frac{n\alpha-n\sqrt{D}\beta}{\alpha^2-D\beta^2}=$$

$$=n\cdot\frac{\alpha}{\alpha^2-D\beta^2}-n\frac{\sqrt{D}\beta}{\alpha^2-D\beta^2}$$

נניח ש- $r=1-\beta$ זרים וכן גם α ו β זרים.

שלם: $\frac{\alpha}{\alpha^2-D\beta^2}$ לכן: $\frac{\beta}{\alpha^2-D\beta^2}$ גם כן שלם.

ולכן, כך ש- n המתקבל r , נקבל:

$$\|x\|=|\alpha^2-D\beta^2|=n$$

כלומר, יהי $(\alpha,\beta)=1$,

האיברים עד $\frac{R}{\sqrt{D}}$ מתוכם שלם. כאשר $\|x\|=n$.

כולל.

משפט שני – $(\alpha,\beta)=g\neq 1$

כאן הבדל"מ: $1-\frac{\alpha}{\alpha^2-D\beta^2}$ נשארים $\frac{\beta}{\alpha^2-D\beta^2}$

שמתחלקים ב- g.

ולכן מספר לנו: $n=\frac{\alpha^2-D\beta^2}{g}$

כלומר – האיברים (פחות מספיק) כולל $\frac{\alpha^2-D\beta^2}{g}$.

$\frac{\sqrt{D}}{\beta}$, אבל g מספרים נשארים פחות מ $\sqrt{D}$,

Scanned by CamScanner

כי צריך q כזה ש"ק". $q \mid g$.

ואכן, $\left|\frac{R}{\langle r\rangle}\right| = \frac{g}{g} = 1$.

כלומר, המרחק $\left|\frac{R}{\langle r\rangle}\right|$ מצמצם את הסריג הזה שכולו כבוי.

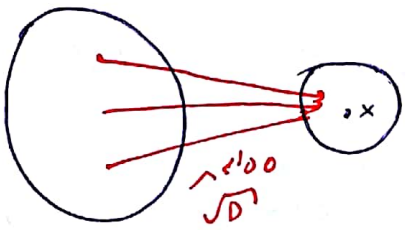
תרגיל

יש איזו פרמטריזציה שמכוונת בשני אופנים:

שיטת: $x \in (\text{חוג}, \sqrt{D})$

ורוצים שיש לו אחד

ר- $\mathbb{Z}[\sqrt{D}]$



פתרון:

$x = (0,x) \in \mathbb{Z}[\sqrt{D}]$

פתרון תרגיל $D \bmod 4 = 1$

נרצה לחשב את $\left|\frac{R}{\langle r\rangle}\right|$.

כזכור: $r = \alpha + \frac{\beta}{2} + \frac{\sqrt{D}}{2}$ כאשר $\alpha \in \mathbb{Z}$

שקול: $\frac{R}{\langle r\rangle}$ הוא חוג סופי של $\mathbb{Z}[\sqrt{D}]$.

כלומר, הוא שווה ל: $a + \frac{b}{2} + \frac{\sqrt{D}}{2}$

$\left(a + \frac{b}{2} + \frac{\sqrt{D}}{2}\right) \bmod \left(\alpha + \frac{\beta}{2} + \frac{\sqrt{D}}{2}\right) =$ נרצה.

$= (a + \frac{b}{2} + \frac{\sqrt{D}}{2}) \cdot (x + \frac{y}{2} + \frac{\sqrt{D}}{2})$

כלומר כ: $0 = (\frac{y}{2} + x) \cdot \frac{\beta}{2} + \frac{y}{2} \cdot (\frac{\beta}{2} + \alpha) + \frac{b}{2}$

$\Downarrow$

צריך למצוא y כך ש- $\sqrt{D}$ יתחלק,

Scanned by CamScanner

$$2b + (2\alpha+\beta)y + \beta(2x+y) = 0$$

$$\Downarrow$$

$$-2b = 2\alpha y + \beta(2x+2y)$$

$$-b = \alpha y + \beta(x+y)$$

אם $(\alpha,\beta)=1$ – נעזר בפתרון של $\sqrt{D}$

נזכיר: $(\alpha,\beta)=g \neq 1$,

אז נקבל: $g \mid b$ ו"מ.

פתרון של $\sqrt{D}$.

ובאשר נעסוק בהרבה "פתרונות מינימליים",

נעבוד בשיטת הפתרון של $\sqrt{D}$ הנ"ל.

$\{1-g, \dots, g\} \in$ מנדק של $\sqrt{D}$

הגדרה משלה הנ"ל: $(\alpha,\beta)=1$

$$r = \alpha + \frac{\beta}{2} + \frac{\beta}{2}\sqrt{D} \quad ; \quad (\alpha,\beta)=1$$

נבחין בקיצה שלפי n ~~מספיק~~ שבשבילו ~~כפולה~~ של $\frac{1}{2}$ ($\Leftarrow \theta_D$).

נמצא: $\frac{Q}{r} = 0$

נזכיר:

$$\frac{h}{r} = \frac{h}{\alpha+\frac{\beta}{2}+\frac{\beta}{2}\sqrt{D}} =$$

$$= \frac{h\cdot(\alpha+\frac{\beta}{2}) - h\cdot\frac{\beta}{2}\sqrt{D}}{(\alpha+\frac{\beta}{2})^2 - D(\frac{\beta}{2})^2} =$$

$$= \frac{(4\alpha+2\beta)+(2\beta\sqrt{D})}{(2\alpha+\beta)^2 - \beta^2 D} \cdot h$$

נסמן: $\vec{D}$:

$$D = 4\vec{D}+1$$

ונמצא:

$$\text{שלם} = \frac{h}{r} = h\cdot\frac{(2\alpha+\beta)+\beta\sqrt{D}}{2\alpha^2+2\alpha\beta-\beta^2\vec{D}\cdot 2}$$

נזכיר ש- α,β קיים, כך שלפחות אחד מהשניים

$\frac{\beta}{2\alpha^2+2\alpha\beta-\beta^2\vec{D}\cdot 2}$ ו $\frac{2\alpha+\beta}{2\alpha^2+2\alpha\beta-\beta^2\vec{D}\cdot 2}$ לפחות אחד.

Scanned by CamScanner

ולכן, כדי לקבל התנגשות מספר [illegible] (שכנוע שיש θ_D נדרש).

$$n = \frac{2\alpha^2 + 2\alpha - \hat{D}^2\beta^2 \cdot 2 - \beta}{2} = \alpha^2 + \alpha - \beta\hat{D}^2$$

כלומר המספרים השלמים שעבורם נתון שהפרש
מולטיפלסים ב-$(n-1)$ הם.

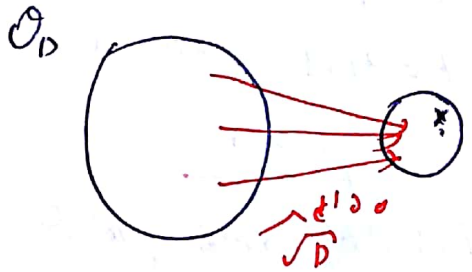
ראשית נבדוק מהי ההתנגשות שעבורה כולנו בכיתה:

$$\left\| \left(\alpha + \frac{\beta}{2}, \frac{\beta}{2}\right) \right\| = \left(\alpha + \frac{\beta}{2}\right)^2 - D\left(\frac{\beta}{2}\right)^2 = \alpha^2 + 2\alpha\frac{\beta}{2} + \left(\frac{\beta}{2}\right)^2 \cdot (1-D) =$$

$$= \alpha^2 + \alpha\beta + \beta^2 \cdot \frac{1}{4} - \beta^2\hat{D}\cdot\frac{1}{4} =$$

כדי לבדוק האם הנתון נכון

נבחר קבל $x \in (n-1, \dots, 0)$ יש מרחק



$$x \in (n-1, \dots, 0)$$
$$\Downarrow$$
$$x \in \theta_D$$

לדוגמה: $a=x, b=0$.

כשלפחות אחד - $g = (\alpha,\beta) \neq 1$

כלל המרחקים: $\frac{\alpha+\beta}{2\alpha^2+2\alpha\beta-\beta^2\hat{D}\cdot 2}$ $\frac{\beta}{2\alpha^2+2\alpha\beta-\beta^2\hat{D}\cdot 2}$ $1-$

נחלק במחלק המשותף הגדול ביותר g.

ולכן מספר הפעמים $\frac{1}{g}\cdot$

$$n = \frac{2\alpha^2+2\alpha\beta-\beta^2\hat{D}\cdot 2}{2}$$

כלומר - המתנגש (בפחות מספרים) הוא הראשון:

$$\frac{\alpha^2+\alpha\beta-\beta^2\hat{D}}{g}$$

כן 1 [illegible] מכל g מספרים נתחיל מהפעם

Scanned by CamScanner

שים לב: $\sqrt{D}$ הוא כפל של g, כי b כפולה של g מהגדרה.

$$\left|\frac{R}{\langle r\rangle}\right| = \frac{\alpha^2+\beta\alpha+\beta^2 D}{g} \cdot g =$$

$$= \alpha^2+\beta\alpha+\beta^2 D$$

כלומר, הנורמה של $\left|\frac{R}{\langle r\rangle}\right|$ שייכת לאידיאל $\langle r\rangle$.

שאלה מס' 5

א. הוכח/הפרך כי: $\frac{\mathbb{Z}}{10\mathbb{Z}} \simeq \frac{\mathbb{Z}[i]}{\langle 3+i\rangle}$

ב. הסבר: $3+i \in \mathbb{Z}[i]$ איננו הפיך.

ג. הבהר: $7 \in \mathbb{Z}[i]$ הפיך/לא הפיך?

פתרון

א. אומרים כי: $\frac{\mathbb{Z}[i]}{\langle 3+i\rangle}$ שקולה לכך: $a+bi$.

שיכולים שני מספרים שונים.

$$f : \left[\frac{\mathbb{Z}[i]}{\langle 3+i\rangle}\right] \to \frac{\mathbb{Z}}{10\mathbb{Z}}$$

$$f(a+bi) = (a-3b) \bmod 10$$

Scanned by CamScanner

מושגים לפתרון

בדיקת הכפלתיות של פונקציה: מציבים 2 איברים.

שלב א

מציבים הפרשים של j ו-i:

$$a+bi \equiv a+bi-b\cdot(3+i) = a-3b$$

קיבלנו: תמונה $\to \mathbb{Z}$.

שלב ב'

נבדוק מתוקנות של 10 לתמונה $\to \mathbb{Z}$, אחת זו $(3+i)$:

$$\frac{10}{3+i} = 3-i$$

א. יחידה בחוג המנה פיק

1. תחילה:

$$f(a_1+b_1i)+f(a_2+b_2i) = (a_1-3b_1+a_2-3b_2) \bmod 10 =$$

$$= [a_1+a_2-3(b_1+b_2)] \bmod 10$$

$$f[(a_1+b_1i)+(a_2+b_2i)] = f[a_1+a_2+b_1i+b_2i] =$$

$$= [a_1+a_2-3(b_1+b_2)] \bmod 10.$$

2. הכפל

$$f[(a_1+b_1i)(a_2+b_2i)] = f[a_1a_2-b_1b_2+(a_2b_1+a_1b_2)i] =$$

$$= [a_1\cdot a_2-b_1b_2-3(a_2b_1+a_1b_2)] \bmod 10$$

$$f(a_1+b_1i)\cdot f(a_2+b_2i) = [(a_1-3b_1)(a_2-3b_2)] \bmod 10 =$$

$$= [a_1a_2+9b_1b_2-3(b_1a_2+a_1b_2)] \bmod 10 =$$

$$= [a_1a_2-b_1b_2-3(a_2b_1+a_1b_2)] \bmod 10$$

3. $f(1)$

$$F(1+0i) = (1-3\cdot 0) \bmod 10 = 1$$

Scanned by CamScanner

ג. הוכיחו: תת"ר

יהיו $x_1=(a_1+b_1 i)$ ו-$x_2=(a_2+b_2 i)$ שני מספרים שלמים. נניח כי f היא הומומורפיזם ונגדיר f שמקיים שלושה תנאים: f היא העתקה על $\mathbb{Z}_{10}$, f היא חח"ע, ו-$(3+i)$ הוא גרעין f.

$$f(a_2+b_2 i)=f(a_1+b_1 i)$$
$$(a_2-3b_2)\bmod 10=(a_1-3b_1)\bmod 10$$
$$\Downarrow$$
$$[(a_2-3b_2)-(a_1-3b_1)]\bmod 10=0$$
$$\Downarrow$$
$$[(a_2-a_1)-3(b_2-b_1)]\bmod 10=0$$

כלומר $(3+i)$ מחלק את 10.

כלומר $(3+i)$ מחלק את $[(a_2-a_1)+3(b_2-b_1)]$

$$\Downarrow$$

נוסיף $(b_2-b_1)\cdot(3+i)$

$$(3+i)\mid[(a_2-a_1)+(b_2-b_1)\cdot i]$$
$$\Downarrow$$
$$(3+i)\mid[x_2-x_1]$$

כלומר $x_2 \bmod (3+i)=x_1 \bmod (3+i)$

ד. מה

שדה המנה $\frac{\mathbb{Z}[i]}{\langle 3+i\rangle}$ הוא איזומורפי ל-

$0,1,\dots,9$

$\{0,1,\dots,9\}\in(a+bi)$

לכל k יש נציג מהצורה k.

$$f(k)=(k-3\cdot 0)\bmod 10=k\bmod 10=k$$

קיבלנו שכל איבר הוא אחד מ-$0,1,\dots,9$.

Scanned by CamScanner

א. הסיבה כי $\mathbb{Z}[i] \ni 3+i$ אינו הפיך

כל איבר הפיך שווה $\langle 3+i \rangle$ אז קיים איבר הפיך
הנקי ל- 0.
לדוגמה: $2 \to 2$ ו- $5 \to 5$!

$2 \cdot 5 = 10 \bmod 10 = 0$

לדוגמה: 2 איברים שונים ב$\mathbb{Z}[i]$ ו$\mathbb{Z}$ שאינם
איבר הפיך
לכן הפיך ב$\mathbb{Z}[i]$. $\langle 3+i \rangle$ אינו הפיך

ב. האם $\frac{\mathbb{Z}[i]}{\langle 7 \rangle} \cong \mathbb{Z}_7$ הפיך?

איבר $\langle 7 \rangle$ שייך ~~[illegible]~~ הפיך ~~[illegible]~~ הפיך!

$f: \frac{\mathbb{Z}[i]}{\langle 7 \rangle} \to \frac{\mathbb{Z}}{7\mathbb{Z}} + i\frac{\mathbb{Z}}{7\mathbb{Z}}$

$f:(a+bi) = (a \bmod 7) + i(b \bmod 7)$

א. הוכיח הומומורפיזם

1. חיבור

$f(a_1+b_1 i) + f(a_2+b_2 i) = (a_1+a_2) \bmod 7 + i(b_1+b_2) \bmod 7$

$f[(a_1+b_1 i) + (a_2+b_2 i)] = f[(a_1+a_2) + i(b_1+b_2)] =$

$= (a_1+a_2) \bmod 7 + i(b_1+b_2) \bmod 7$

2. כפל

$f[(a_1+b_1 i)\cdot(a_2+b_2 i)] = f[a_1 a_2 - b_1 b_2 + i(b_1 a_2 + a_1 b_2)] =$

$= (a_1 a_2 - b_1 b_2) \bmod 7 + i \cdot (b_1 a_2 + a_1 b_2) \bmod 7$

$f[(a_1+b_1 i)] \cdot f(a_2+b_2 i) = [(a_1 \bmod 7 + i b_1 \bmod 7) \cdot$

$\cdot (a_2 \bmod 7 + i b_2 \bmod 7)] \bmod 7 = [(a_1 \cdot a_2 - b_1 b_2) \bmod 7 + i(b_1 a_2 + a_1 b_2) \bmod 7]$

3. איבר יחידה

$f(1+0i) = 1 \bmod 7 + i \cdot 0 \bmod 7 = 1$

Scanned by CamScanner

נניח ש- $x_1 = (a_1 + b_1 i)$ $x_2 = (a_2 + b_2 i)$

$f(x_1) = f(x_2)$

$a_2 \bmod 7 + i \cdot (b_2 \bmod 7) = a_1 \bmod 7 + i (b_1 \bmod 7)$

$(a_2 - a_1) \bmod 7 + i (b_2 - b_1) \bmod 7 = 0$

$(x_2 - x_1) \bmod 7 = 0$

$x_2 \bmod 7 = x_1 \bmod 7$

2. סעיף

נניח ש- $a+bi$ מקיים $a, b \in \{0, \dots, 6\}$

ואז

$f(a+bi) = \alpha + \beta i$

כאשר

$\alpha = 0, \dots, 6$

$\beta = 0, \dots, 6$

נראה שכל איבר ב- $\langle 7 \rangle$ שהוא מהצורה f של איבר בשדה $\mathbb{Z}_7[i]$.

יהי $f(x_1) = a_1 + b_1 i$; $f(x_2) = a_2 + b_2 i$

כאשר $a_1 \neq 0$ ו- $b_1 \neq 0$, $a_2 \neq 0$, $b_2 \neq 0$.

$f(x_1) \cdot f(x_2) = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1)$

נשים לב ש- $f(x_1) \cdot f(x_2) \in |7|$

כלומר $\|f(x_1)\| \cdot \|f(x_2)\| = 7^2$

כלומר $\|f(x_1)\|$ או $\|f(x_2)\|$ מתחלק ב- 7.

נזכר ש- $\|a+bi\|$ מספרים טבעיים שמתחלקים ב- 7 כאשר:

$a \in \{0, \dots, 6\}$

$b \in \{0, \dots, 6\}$ כאשר $a \neq 0$, $b \neq 0$ שאחד מהם שונה מ-0.

$\|f(a+bi)\|$ מתחלק ב- 7.

סה"כ - כאשר

יהי R תחום פרינציפי. נזכיר שלכל $a \in R \setminus \{0\}$ את $u(a)$ נסמן מספר הגורמים הלא-פריקים הפריים q ב a. נזכיר כמה מפרידי של R הינו תחום פרינציפי.

יהיו $a, b \in R \setminus \{0\}$ כך ש: a/b. הוכיחו:

$u(a) \geq u(b)$ ושוויון אמ"מ a ו b שווים.

רמז: a הפיך אמ"מ $u(a) = 0$.

פתרון

סעיף א'

$a \nmid b \Leftarrow u(a) \geq u(b)$.

b נסמן כמכפלת גורמים לא-פריקים:

$$b = p_1 \cdot p_2 \cdots p_n \cdot u_1$$

כאשר u_1 איבר הפיך.

a נסמן כמכפלת גורמים לא-פריקים:

$$a = q_1 \cdots q_m \cdot u_2$$

כאשר u_2 איבר הפיך.

$a \mid b$ אזי קיים x כך ש:

$$b = xa$$
$$\Downarrow$$
$$p_1 \cdot p_2 \cdots p_n \cdot u_1 = q_1 \cdots q_m \cdot x \cdot u_2$$

מכיוון שכל הגורמים לא-פריקים, הרי ש q_1 שמופיע בצד שמאל חייב להופיע גם בצד שמאל.

לפחות קיים p_i כך ש:

$$q_1 \sim p_i$$

מכיוון שכל האיברים אינם שייכים ל u_1 לפחות.

$$\frac{p_i}{u_1} = \hat{u}_1 \leftarrow \text{איבר הפיך}$$

~~לפחות~~ לפחות הגורם הראשון שקיבל ש: p_i יהיה p_1 ול- p_1 יהיה p_i ונמצא:

Scanned by CamScanner

$$p_2 \cdot p_3 \cdot \ldots \cdot p_m \cdot \hat{u}_1 \cdot u_1 = q_2 \cdot q_3 \cdot \ldots \cdot q_m \cdot x \cdot u_2$$

כאן אי אפשר עוד לצמצם q_i לפחות אחד.

$$p_{m+1} \cdot \ldots \cdot p_n \cdot \hat{u}_1 \hat{u}_2 \ldots \hat{u}_m u_1 = x \cdot u_2$$

אלא שמתקיים ש: $n = m$

$$\hat{u}_1 \cdot \hat{u}_2 \ldots \hat{u}_m u_1 = x \cdot u_2$$

מסקנה שלישית:

$\mu(a) = m$ ו $\mu(b) = n$ אזי:

$n \geq m$

$\Downarrow$

$\mu(a) \leq \mu(b)$

משל ל:

$a \sim b \iff \mu(a) = \mu(b)$ עבור μ שמוגדרת כך שהיא מקיימת את 2 התכונות!

משל $a \sim b$

$\Downarrow$

a/b ולכן b/a

$\Downarrow$ $\Downarrow$

$\mu(a) \geq \mu(b)$ — No משל ל $\mu(b) \geq \mu(a)$

$\Downarrow$

$\mu(b) = \mu(a)$

מ"ש

משל $\mu(a) = \mu(b)$

אזי כל הפולינומים של a מתאחדים עם $b \Leftarrow a/b$

כמו כן כל הפולינומים של b מתאחדים עם $a \Leftarrow b/a$

ולכן: a/b ולכן b/a

$\Downarrow$

$a \sim b$

ל"ש

סימון ב'

נסמן $\mu(a)=0$ אם a יחידה.

הגדרה

איבר פרוק של סדר ב'.

a פרוק

$\Updownarrow$

$1 \sim a$

$\Updownarrow$

$\mu(a)=\mu(1)$

$\Updownarrow$

$\mu(a)=0$

שאלה מסוג ז

יהי F שדה. לכל $n \in \mathbb{N}$ נגדיר: $R_n = F[x^{1/n!}]$.

למשל: $R_1 = F[x]$ ו- $R_2 = F[x^{1/2}]$

הוכח כי שרשרת: $R_1 \subseteq R_2 \subseteq R_3 \subseteq \cdots$

נסתכל על הטענה שקיבלנו בהרצאה:

$$R = \bigcup_n R_n$$

סדר ב'

הוכיחו: לכל $r \in \mathbb{Q}$ כך ש $r > 0$, ולכל $x \in R$.

שלכל R הם סכומים סופיים מהצורה: $\sum a_i x^{r_i}$

כך ש: $a_i \in F$ ו- $r_i \in \mathbb{Q}$ כך ש $r_i > 0$.

פתרון

$r \in \mathbb{Q}$, נצטרך כאשר r נתון שקיים $\frac{a}{b}$.

כאשר הוא מהצורה - b - שהוא מספיק לחלק בו שני מספרים:

$b = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$

$$B = \max(p_1^{k_1}, p_2^{k_2}, \dots p_n^{k_n})$$

$$x^{\frac{1}{13!}} \in F[x^{\frac{1}{13!}}] = R_{13}$$

$$\Downarrow$$

$$x^{\frac{1}{13!}} \in R_{13} \subseteq R$$

$$\Downarrow$$ ← אינטואיציה לכפל

$$x^{\frac{1}{b}} = x^{\frac{1}{p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_n^{k_n}}} \subseteq R$$

[דוגמא למחשבה:

$$b = 9 \cdot 8 \cdot 7 = 2^3 \cdot 3^2 \cdot 7$$

$$x^6 = x^{\frac{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6}{9!}} = \left(x^{\frac{1}{9!}}\right)^{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6}$$

]

ואינטואיציה לכפל:

$$x^{\frac{a}{b}} \in R$$

ולכן:

$$x^r \in R$$

Scanned by CamScanner

תרגיל 26,

כל איבר $\to R$, יהיה שייך ל R_n כלשהו ($R_n \to$

ונניח גם שאנחנו באיחוס,

ולכן נקבל $F[x^{\frac{1}{n!}}] = \sum a_i (x^{\frac{1}{n!}})^k =$ יהיה: $R_n \to$

$$= \sum a_i x^{\frac{k}{n!}} \in \sum a_i x^{r_i}$$

כאשר $a \in r_i > 0$.

לכל איבר: $r \in R$, קיימת $\sum$ סופית, כך שיהיה שייך ל- R_n מינימלי כלשהו.

טענה:
הוכיחו כי R אינו חוגים איחוס (משפט בחינה).

הוכחה:

$$X \in F[x] = R_1 \subseteq R$$

$$x = x^{1/2} \cdot x^{1/2} = (x^{\frac{1}{2}})^2$$

כלומר: $x^{1/2} \in R_2 \subseteq R$

נשים לב כי: $x = (x^{\frac{1}{2}\cdot\frac{1}{3}})^{2\cdot 3} = (x^{\frac{1}{3!}})^{3!}$

$$\vdots$$

$$x = (x^{\frac{1}{n!}})^{n!} \subset R$$

ובאופן: $x^{\frac{1}{n!}}$ נשים לב כי:

$$x^{\frac{1}{n!}} = x^{\frac{1}{(n+1)!}(n+1)}$$

$$x = (x^{\frac{1}{(n+1)!}})^{(n+1)!} \subset R$$

~~לכן לא קיים~~

ולכן אין כזו סדרה שמכפלת איבריה - כיצד, שם x.

Scanned by CamScanner

טענה ב'

יהי R שלם כך שלכל $m \in \mathbb{N}$, קיימים R_m ו- R_n איזומורפים, אזי R שדה איזומורפי לשלמים.

הוכחה

נסמן R_1 איזומורפי ל- R.

נגדיר: $y = x^{\frac{1}{m}}$

$$R_n = f\left[x^{\frac{1}{m}}\right] = F[y] \simeq F[x] = R_1$$

ולכן לכל m:

$$R_m \simeq R_1$$

ולכן:

$$R_n \simeq R_m$$

כלומר כל הפולינומים R_n ו- R_m איזומורפים ל- R_1 ו- R.

$$R_1 = F[x]$$

תחום פריקות יחידה.

שדה R אזי תחום פריקות ולכן שדה R איזומורפי ל- R.

שאלה מס' 4

יהי R תחום. שקיים פונקציית נורמה שמאיברים שונים מאפס:

לכל: $N(0) = 0$ ולכל: $a \neq 0 \in R$:

$$N(a) = \left|\frac{R}{\langle a \rangle}\right| = (\text{מספר איברי תחום המנה})$$

טענה א'

תהי R תחום שלמות, אזי N פונקציית נורמה כפלית.

הוכחה

יהי: $a/b \in R$

ושני אידיאלים $\langle a \rangle$.

ושני אידיאלים $\langle b \rangle$

ושני אידיאלים (גם) משניהם: $\langle ab \rangle$

Scanned by CamScanner

שאלה מס' 8

משפט: יהי F שדה. הפולינום שדרגתו n ב$F[x]$ יש לכל היותר n שורשים.

הוכחה:

F - שדה ולכן $F[x]$ תחום פריקות יחידה ולכן, תחום אוקלידי כאשר $(\deg)$ ולכן: אוקלידי כאשר לכל a,b - פרוק יש אותו דבר בתוך שדה.

לכן, נובעת שיש אלגוריתם אוקלידי ל- a,b פרוקים.

נניח בשלילה שיש יותר מ n אוקלידים ל- a,b פרוקים.

נסמן אותם:

$$p_1, p_2, \dots, p_M$$

ידוע שמתוכם האוקלידי: $r = p_1 \cdot p_2 \cdots p_N + 1$.

שהוא הפחות אוקלידי ולכן ה- $\deg$ הכי קטן ה- G.C.D.

לכן r פרוק לגורמים מהצורה של אוקלידים ל- a,b פרוקים, אך כבר כולם האוקלידי הם n.

ולכן נשארים ⇒ אוקלידים ל- a,b פרוקים, כך ש- r מתחלק באחד מהם.

אבל r לא מתחלק לאף אוקלידי: $p_j, \dots, p_M$.

$$r = p_1 \cdot p_2 \cdots p_N + 1$$

לכל p_i

$$\frac{r}{\langle p_i \rangle} = 1$$

לכן סתירה שמספר האוקלידים גדול M.

מש"ל

Scanned by CamScanner

שאלה מס' 9

משפט: תהי $\alpha \in \mathbb{C}$ שורש של פולינום לא קבוע, אז קיים פולינום $f(x) \in \mathbb{Z}[x]$ כך ש: $f(\alpha)=0$ ולכל פולינום כזה קיים A כך ש: $A \mid f$.

טענה 1/

נוכיח כי A הוא יחיד מתוך כל $\mathbb{Z}$.

הוכחה

1) $0 \in A$ כי $x=f(x)=0$ הפולינום שבו כולו x.

2) יהי x שייך ל-A כך ש- $-x$ שייך ל-A כי:

$$a_0+a_1x+a_2x^2+a_3x^3+\dots=0$$

$$\downarrow$$

$$a_0-a_1x+a_2(-x)^2-a_3(-x)^3+\dots=0$$

3) הפולינום הראשון - קבוע ושווה a_0.

4) הפולינום השני - שווה ל-x.

טענה 2/

נוכיח שלכל: $\alpha \in A$, גם $A \ni \sqrt{\alpha}$.

הוכחה

נניח כי α שורש של f.

$$a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+\dots=0$$

$$\Downarrow$$

$$a_0+a_1(\sqrt{\alpha})^2+a_2(\sqrt{\alpha})^4+a_3(\sqrt{\alpha})^6+\dots=0$$

$$\downarrow$$

$$\sqrt{\alpha} \in A$$

טענה 3/

נוכיח כי A יחיד. תהי g אחרת.

טענה 4/

כל $\alpha \in A$ ניתן לפירוק ל: $\sqrt{\alpha} \cdot \sqrt{\alpha}$

ו $\sqrt{\alpha}$ שוב ניתן לפירוק ל-$\sqrt{\alpha} \cdot \sqrt{\alpha}$ וכך עד אינסוף

ניתן לפרק לגורמים.

Scanned by CamScanner