http://math-wiki.com/images/b/bd/AA2class7.pdf

תזכורת

$S\times R$, סימון - $S^{-1}R$

$$\left(\underbrace{a}_{\in S},\underbrace{b}_{\in R}\right)\sim\left(\underbrace{a'}_{\in S},\underbrace{b'}_{\in R}\right)$$

$$\Updownarrow$$

$$ab'=ba'$$

$$\frac{b}{a}=\frac{b'}{a'}\qquad ba'=b'a$$

$$i:R\to S^{-1}R$$
$$i\left(x\right)=\frac{x}{1}$$

. ידוע ש$y\in S\subseteq R$ $\Leftarrow$ $i\left(y\right)=\frac{y}{1}$ $\Leftarrow$ $\frac{y}{1}\cdot\frac{1}{y}$

הערה

איבר ב$S^{-1}R$ הוא מהצורה (a,b). מיהו היחידה ב$S^{-1}R$? $(1,1)$, ואז ההפיך ל$(y,1)$ הוא $(1,y)$. יש לשים לב ש$(1,y)$ הפיך רק אם $y\in S$, כי אם $y\notin S$ אז $(y,1)\in S\times R$ ולכן $(y,1)\in S^{-1}R$.

דוגמה

יהי $p\in\mathbb{Z}$ ראשוני. אז הקבוצה $S=\mathbb{Z}\backslash p\mathbb{Z}$ סגורה לכפל. ואז נקבל שS מונואיד.
נתבונן ב$S^{-1}\mathbb{Z}$. איבר ב$S^{-1}\mathbb{Z}$ הוא מהצורה $S\times\mathbb{Z}$. ואז נקבל את $\mathbb{Z}_{(p)}$.

הסבר 2

נתבונן בשדה $\mathbb{F}$. $\mathbb{F}\left[x\right]$ הוא תחום שלמות. נסמן $S=\mathbb{F}\left[x\right]\setminus\{0\}$ ונתבונן ב$S^{-1}R$ כאשר $R=\mathbb{F}\left[x\right]$. האיברים ב$S^{-1}R$ הם (f,g) כך ש

$$\begin{gathered}(f,g)\sim(f',g')\\ \Updownarrow\\ g'f=f'g\end{gathered}\qquad f\neq0$$

אמנם

$$(x,2)\in S\times R\qquad\left(x^2,2x\right)\in S\times R$$

$(x,2)\sim\left(x^2,2x\right)$ ב$S^{-1}R$.

נסמן ב$S^{-1}R$ במקום (a,b).

$$\frac{b}{a}$$

$\mathbb{Z}$ תחום שלמות. $P\mathbb{Z} \lhd \mathbb{Z}$. נתבונן ב$S=\mathbb{Z}\backslash P\mathbb{Z}$ סגורה לכפל.
הסבר מדוע S סגורה לכפל:
נתון ש$P \lhd R$ ראשוני, ז"א ${}^{R}/_{P}$ תחום שלמות. ניקח $a+P, b+P$ כך ש$a,b \notin P$

$$(a+P)(b+P) \notin P$$

$$\Downarrow$$

$$ab \notin P$$

ולכן $S=R\backslash P$ הוא סגור לכפל.

המשך דוגמה

נקבל את $S^{-1}\mathbb{Z} = \mathbb{Z}_{(p)}$ - חוג מקומי. $S^{-1}\mathbb{Z}$ במקרה שלנו $\mathbb{Z}_{(p)}$ נקרא מיקום של $\mathbb{Z}$ באידיאל $p\mathbb{Z}$

הסבר התרגיל

$M \lhd R$ מקסימלי. R חוג קומוטטיבי עם יחידה. ${}^{R}/_{M^n}$ הוא חוג מקומי קומוטטיבי, ו${}^{M}/_{M^n}$ הוא האידאל המקסימלי.
שימו לב: ${}^{M}/_{M^n} \subseteq {}^{R}/_{M^n}$

$$\underbrace{x}_{\in M}+M^n \Rightarrow \underbrace{x}_{\in R}+M^n \in {}^{R}/_{M^n}$$

יותר מזה, ${}^{M}/_{M^n} \lhd {}^{R}/_{M^n}$

$$\left(\underbrace{y}_{\in R}+M^n\right)\left(\underbrace{x}_{\in M}+M^n\right) \in M+M^n$$

1. $\begin{matrix} M^n \subseteq \underbrace{I}_{\text{maximal}} \lhd R \\ \underbrace{I}_{\text{maximal}}/M^n \lhd {}^{R}/_{M^n} \end{matrix}$ - ממשפט ההתאמה.

2. $I \lhd R$ מקסימלי $\Leftarrow$ ${}^{R}/_{I}$ שדה $\Leftarrow$ ${}^{R}/_{I}$ תחום שלמות $\Leftarrow$ IU ראשוני

R תחום שלמות.
נאמר ש$a|b$ אם יש $k\in R$ כך ש$ak=b$.

הערות

1. $Rb\subseteq Ra\Leftrightarrow a|b$
2. יהיו $a,b\in R\backslash\left\{0\right\}$. אם $a|b$ ו$b|a$. אז קיים איבר הפיך u כך ש$a=bu$.

הגדרה

נאמר ש$a,b\in R$ חברים אם $a|b$ ו$b|a$. נסמן $a\sim b$.

ניתן להוכיח יחס שקילות

מי הם מחלקות השיקלות בשלמים?

$$\left\{1,-1\right\},\left\{2,-2\right\},\left\{3,-3\right\},\ldots$$

הערה

- $Ra=Rb\Leftrightarrow a\sim b$
- $a\sim 1\Leftrightarrow a$ הפיך

תרגיל

מה הם ההפיכים ב$\mathbb{Z}\left[i\right]$?

פתרון

כבר יודעים ±1, $\pm i$.

$$a+bi\in\mathbb{Z}\left[i\right]$$

נגדיר

$$\underset{a+bi\mapsto a^{2}+b^{2}}{\left|\cdot\right|:\mathbb{Z}\left[i\right]\to\mathbb{N}\cup\left\{0\right\}}$$

$\mathbb{C} \leftarrow\subseteq \mathbb{Z}[i]$. אנחנו יודעים שב$\mathbb{C}$

$$|\mathbb{Z}_1 \cdot \mathbb{Z}_2| = |\mathbb{Z}_1|\,|\mathbb{Z}_2|$$

ולכן גם ב$\mathbb{Z}[i]$. אם

$$a_2 + b_2 i \in \mathbb{Z}[i] \ \underbrace{a_i + b_1}_{\text{reversable}} \ i \in \mathbb{Z}[i]$$

אזי

$$1 = |(a_1 + b_1 i)(a_2 + b_2 i)| = |a_2 + b_2 i| \cdot |a_1 + b_1 i| \Rightarrow a_1^2 + b_1^2 = 1$$

מכיוון ש$a_1, b_1 \in \mathbb{Z}$ וגם $a_1^2 + b_1^2 = 1$, נקבל שהאפשרויות הן

$$(b = 0, a = \pm 1) \vee (a = 0, b = \pm 1)$$

הגדרה

יהי $D \in \mathbb{Z}$ חופשי מריבועים(לכל $a \in \mathbb{Z}$, $a^2 \neq D$)
[למשל 7 חופשי מריבועים, מכיוון שלא קיים $a \in \mathbb{Z}$ כך ש$a^2 = 7$]
עבור השדה $\left\{a + b\sqrt{D} \middle| a, b \in \mathbb{Q}\right\} = \mathbb{Q}\left[\sqrt{D}\right]$, נגדיר את

$$O_D = \begin{cases} \mathbb{Z}\left[\sqrt{D}\right] & D = 2, 3 \pmod 4 \\ \mathbb{Z}\left[\dfrac{1 + \sqrt{D}}{2}\right] & D = 1 \pmod 4 \end{cases}$$

תרגיל

מי האיברים ההפיכים ב $\mathbb{Z}\left[\dfrac{1 + \sqrt{-3}}{2}\right]$?

פתרון

הרעיון הוא כמו בתרגיל עבור $\mathbb{Z}[i]$.

הגדרה

$0 \neq a \in R$ נקרא אי פריק אם a אינו הפיך, ולכל $b, c \in R$ כך ש$a = bc$ אז b או c הפיכים.
$0 \neq a \in R$ נקרא פריק אם a אינו הפיך וקיימים $b, c \in R$ לא הפיכים כך ש$a = bc$.

דוגמאות

1. בחוג הפולינומים $\mathbb{F}[x]$ נקבל ש־$x \in \mathbb{F}[x]$ הוא אי פריק. אם $x = f(x) \cdot g(x)$ אזי $f(x) = 1$ או $g(1) = 1$
2. ב־$\mathbb{Z}$ כל מספר אי ראשוני הוא פריק
3. בשדה אין משמעות, כי כל האיברים(פרט ל0) הפיכים.

תרגיל

יהי $p \in R$ אי פריק, ונניח $p \sim q$. אזי q אי פריק.

הוכחה

$p \sim q$ ולכן קיים איבר הפיך u כך ש־$p = q \cdot u$. נתון ש־p אי פריק. נניח ש־q פריק, ז"א קיימים a, b לא הפיכים כך ש־$q = 0 \cdot b$, ואז

$$p = (a \cdot b) \cdot u = a \cdot (b \cdot u)$$

a לא הפיך, נשאר להראות ש־$b \cdot u$ לא הפיך.

אם $b \cdot u$ הפיך, אז קיים c כך ש־$(b \cdot u) \cdot c = 1$. ז"א $b \cdot (u \cdot c) = 1$, ולכן b הפיך בסתירה לכך ש־b לא הפיך.

קיבלנו סתירה לאי פריקות של p.

תרגיל

כל איבר ראשוני הוא אי פריק.

פתרון

נניח בשלילה ש־$0 \neq p \in R$ ראשוני פריק. אזי $p = ab$ כך ש־a, b לא הפיכים, ולכן $p|ab$. נניח בה"כ ש־$p|a$, ז"א קיים $0 \neq c \in R$ כך ש־$a = pc$, ולכן

$$p = ab = (pc)\, b$$

$$\Downarrow$$

$$p\,(1 - cb) = 0$$

$$\Downarrow$$

$$cb = 1$$

$\Leftarrow$ b הפיך, וקיבלנו סתירה.