הערה

אם יש בI איבר הפיך, אז $I = R$.

הוכחה

אם $i \in I$ איבר הפיך אז $i^{-1}i = 1_R$ ואז $1_R \in I$. על פי הגדרת אידיאל אם $i^{-1} \in R$ ו$i \in I$ אז $i^{-1} \cdot i \in I$ ולכן $1_R \in I$. אם $1_R \in I$ אז $R = I$ ($1_R \in I$ הראנו, אם $x \in R$ אז $x = x \cdot 1_R \in I$.

מסקנה

אם R חוג עם חילוק, אז יש לו רק שני אידיאלים - $I = \{0\}$ ו$I = R$, מכיוון שכל איבר בR הפיך חוץ מ0.

אם $I \neq \{0\}$ אז קיים $0 \neq x \in I$. R חוג עם חילוק ולכן x הפיך ועל פי ההערה $I = R$.

הגדרה

יהי R חגו כלשהו. אם $I = R$ או $I = \{0\}$ נאמר שI אידיאל טריוויאלי.

תרגיל

יהיו $m, n \in \mathbb{N}$. הוכח ש$n|m \Leftrightarrow m\mathbb{Z} \subseteq n\mathbb{Z}$

פתרון

$\Leftarrow$ נתון ש$n|m$, ז"א קיים $a \in \mathbb{Z}$ כך ש$na = m$.
יהי $b \in m\mathbb{Z}$. ז"א קיים $x \in \mathbb{Z}$ כך ש

$$b = mx = (na)\,x = n\,(ax) \in n\mathbb{Z}$$

$\Rightarrow$ נתון ש$m\mathbb{Z} \subseteq n\mathbb{Z}$. $m \in m\mathbb{Z}$ מכיוון ש$1 \in \mathbb{Z}$. $m = m \cdot 1 \in m\mathbb{Z}$ ולכן $m \in n\mathbb{Z}$, ז"א קיים $y \in \mathbb{Z}$ כך ש$m = ny$.

טענה

אם I, J אידאלים, אז $I \cap J$ אידאל.

הוכחה

יהיו $x \in I \cap J$, $y \in R$, צ"ל ש$xy \in I \cap J$

אם $x \in I \cap J$ אז $x \in I$. מכיוון שI אידאל, $xy \in I$. באותו אופן $xy \in J$, ולכן $xy \in I \cap J$.

הערה

באותו אופן ניתן להראות ש$I+J$ אידאל:

$$a\left(x_1+x_2\right)=ax_1+ax_2$$

הגדרה

יהי R חוג עם יחידה, $x\in R$, אז הקבוצה

$$\langle x\rangle:=\left\{\sum_{i=1}^{n}\alpha_i x\beta_i\middle|\alpha_i,\beta_i\in R,n\in\mathbb{N}\right\}$$

היא אידאל ונקראת האידאל הנוצר ע"י x.

מדוע $\langle x\rangle$ אידאל?

יהי $y\in R$.

$$y\cdot\sum_{i=1}^{n}\alpha_i x\beta_i=\sum_{i=1}^{n}\underbrace{\left(y\alpha_i\right)}_{\in R}x\beta_i\in\langle x\rangle$$

וזה האידאל המינימלי שמכיל את x.

טענה

$\langle x\rangle$ מינימלי, ז"א שאם $R\lhd I$ המכיל את x אזי $\langle x\rangle\subseteq I$.

רעיון

$$x\in I$$

$$\alpha x\in I$$

$$\alpha x\beta\in I$$

הערה

הראנו שאם I,J אידאלים, אז $I+J$ אידאל.

המשך הגדרה

אם ניקח קבוצת איברים $\{x_i\}_{i=1}^{r}$, $x_i \in R$, אז נגדיר

$$\langle x_1, \dots x_r \rangle = \langle x_1 \rangle + \cdots + \langle x_r \rangle$$

דוגמה

$$\langle 2, x \rangle = \{2f(x) + xg(x) | f(x), g(x) \in \mathbb{Z}[x]\}$$

שכן $\langle 2, x \rangle = \langle 2 \rangle + \langle x \rangle$, $\mathbb{Z}[x]$ חוג קומוטטיבי.

אם R חוג קומוטטיבי ו$x \in R$, אז $\langle x \rangle = xR$, כי

$$\langle x \rangle = \left\{ \sum_{i=1}^{n} \alpha_i x \beta_i \middle| \alpha_i, \beta_i \in R, n \in \mathbb{N} \right\}$$

$$\alpha_i x \beta_i = \alpha_i \beta_i x \overset{\beta_i = 1_R}{=} Rx = xR$$

ולכן

$$\langle 2, x \rangle = \langle 2 \rangle + \langle x \rangle$$

$$\langle 2 \rangle = \left\{ \sum_{i=1}^{n} \alpha_i 2 \beta_i \middle| \alpha_i, \beta_i \in \mathbb{Z}[x], n \in \mathbb{N} \right\}$$

$$\alpha_1 \cdot 2 \cdot \beta_1 = 2 \cdot \alpha_1 \cdot \beta_1 = 2 \cdot f(x) \qquad f(x) \in \mathbb{Z}[x]$$

הגדרה

יהיו I, J אידאלים. נגדיר:

$$IJ = \left\{ \sum_{\substack{\text{finite} \\ \text{sum}}} i_n j_n \middle| i_n \in I, j_n \in J \right\}$$

הראינו בהרצאה שהסכום הנ"ל הוא אידאל.

הערה

שימו לב שאם I, J אידאלים, לא בהכרח שהקבוצה $\{i \cdot j | i \in I, j \in J\}$ אידאל.

למשל

נתבונן בחוג $\mathbb{Z}[x]$.

$$I = \langle 2, x\rangle \qquad J = \langle 3, x\rangle$$

נוכיח שהקבוצה $S = \{f \cdot g | f \in I, g \in J\}$ אינה אידאל.
נתבונן ב$f_1, f_2, g_1, g_2 \in \mathbb{Z}[x]$, כך ש

$$f = 2f_1 + xf_2 \in I \qquad g = 3g_1 + xg_2 \in J$$

עבור $f = 2, g = 3$ נקבל ש$6 \in S$. אם ניקח $f = g = x$ נקבל $x^2 \in S$.
נוכיח ש$6 + x^2 \notin S$. נניח בשלילה ש$6 + x^2 \in S$, ז"א קיים $f \in I, g \in J$ כך ש$f \cdot g = 6 + x^2$. כלומר

$$(2f_1 + xf_2)(3g_1 + xg_2) = 6f_1g_1 + 2xf_1g_2 + 3xf_2g_1 + x^2f_2g_2$$

שני אפשרויות:

1. $f_1g_1 = 1 \Leftarrow 1_R = f_1g_1 \in S \Leftarrow S$ אינה אידאל
2. $f_1g_1 = -1 \Leftarrow$אותו דבר

הגדרה

יהי R חוג עם יחידה, $I, J \lhd R$.
נאמר שI, J קו־מקסימלים אם $I + J = R$.

טענה

אם R חוג קומוטטיבי עם יחידה, I, J אידאלים קו־מקסימלים, אז $IJ = I \cap J$.

הוכחה

$IJ \subseteq I \cap J$ - מיידי(נכון תמיד).
נוכיח ש$I \cap J \subseteq IJ$. יהי $a \in I \cap J$.
מכיוון שI, J קו־מקסימלים נקבל ש$I + J = R$, ז"א $1_R \in I + J$, ז"א קיימים i, j כך ש$i_{\in I} + j_{\in J} = 1_R$.

$$a = a \cdot 1 = a \cdot (i + j) = a \cdot i + a \cdot j = \underbrace{i_{\in I} \cdot a_{\in J}}_{\in IJ} + \underbrace{a_{\in I} \cdot j_{\in J}}_{\in IJ} \in IJ$$

הגדרה

I נקרא אידאל ראשי אם קיים $x \in R$ כך ש$I = \langle x\rangle$.
R הוא חוג ראשי אם כל אידאל בR הוא ראשי.

שימו לב

שאם R חוג קומוטטיבי אז $Rx = \langle x \rangle$. אם R לא קומוטטיבי השוויון הנ"ל לא (בהכרח) נכון.

תרגיל

הוכיחו כי $\mathbb{Z}[x]$ אינו ראשי.

פתרון

נסתכל על האידאל $\langle 2,x \rangle$. כדי להוכיח ש$\langle 2,x \rangle$ לא ראשי, יש להראות שלכל $y \in \mathbb{Z}[x]$, $\langle y \rangle \neq \langle 2,x \rangle$.

$$h(x) = 2f(x) + xg(x) \in \langle 2,x \rangle$$

$$h(0) = 2f(0) \in 2\mathbb{Z}$$

נניח שקיים $q \in \mathbb{Z}[x]$ כך ש$\langle q \rangle = \langle 2,x \rangle$. ז"א $x \in \langle q \rangle$ וגם $2 \in \langle q \rangle$.

מכיוון ש$x \in \langle q \rangle$ ז"א קיים פולינום, נקרא לו n, כך ש$x = qn$.

מכיוון ש$2 \in \langle q \rangle$ קיים פולינום m כך ש$2 = qm$.

ז"א 2 הוא מחלק משותף ב$\mathbb{Z}[x]$ של 2 וx, ולכן $q = \pm 1$, ז"א $\langle q \rangle = \mathbb{Z}[x]$.

הראינו מקודם שאם $h \in \mathbb{Z}[x]$ אז $h(0) \in 2\mathbb{Z}$, ז"א הפולינום $h(x) \notin \langle 2,x \rangle$ בסתירה לכך ש$\langle q \rangle = \mathbb{Z}[x]$.