מבוא לחוגים ומודולים - תרגול 3

תזכורת:

$I\subseteq R$ <u>אידאל</u> אם הוא תת-חבורה חיבורית ו- $IR,RI\subseteq I$.

$\varphi:R\to S$ <u>הומומורפיזם</u> אם

$$\varphi(x+y)=\varphi(x)+\varphi(y)$$
$$\varphi(xy)=\varphi(x)\varphi(y)$$
$$\varphi(1_R)=1_S$$

תרגיל:

תני דוגמה לחוגים R,S, הומומורפיזם $\varphi:R\to S$ ואידאל $I\lhd R$ כך ש- $\varphi(I)$ אינו אידאל של S.

פתרון:

$R=\mathbb{Z}$, $S=\mathbb{Q}$, $\varphi:R\to S$ ההכלה, $I=\mathbb{Z}$.

$I\lhd\mathbb{Z}$, אבל $\varphi(I)=\mathbb{Z}\ntriangleleft\mathbb{Q}$ כי ב- $\mathbb{Q}$ אין אידאלים לא טריוויאליים.

פעולות על אידאלים

הגדרה:

יהיו $I,J\lhd R$ אידאלים.

א. $I\cap J$ הוא אידאל. זה האידאל המקסימלי שמוכל ב- I וב- J.

ב. $I+J=\{i+j \mid i\in I, j\in J\}$ הוא אידאל. זה האידאל המינימלי המכיל את I ואת J.

דוגמה:

ב- $\mathbb{Z}$,

$$a\mathbb{Z}\cap b\mathbb{Z}=\mathrm{lcm}(a,b)\mathbb{Z}$$
$$a\mathbb{Z}+b\mathbb{Z}=\gcd(a,b)\mathbb{Z}$$

$$\begin{tikzcd} & I+J \arrow[dl, dash] \arrow[dr, dash] & \\ I \arrow[dr, dash] & & J \arrow[dl, dash] \\ & I\cap J & \end{tikzcd}$$

הגדרה:

אם $\{I_j\}_{j\in\Lambda}$ משפחת אידאלים,

$\bigcap_{j\in\Lambda} I_j$ אידאל

$\sum_{j\in\Lambda} I_j = \{$סכומים סופיים של איברים מ-I_j-ים$\}$ האידאל המינימלי שמכיל את כולם

הגדרה:

יהי R חוג ויהי $a\in R$. <u>האידאל שנוצר ע"י a</u> הוא האידאל המינימלי של R שמכיל את a:

$$\langle a\rangle = RaR = \left\{\sum_{i=1}^{n} r_i a s_i \,\middle|\, n\in\mathbb{N},\ r_i,s_i\in R\right\}$$

דוגמה: ב-$\mathbb{Z}$, $\langle n\rangle = n\mathbb{Z}$

אם R חילופי, $RaR=Ra=aR$.

אם R לא חילופי, יתכן ששלוש הקבוצות האלו שונות זו מזו.

נסמן $\langle x_1,\dots,x_k\rangle = \langle x_1\rangle+\dots+\langle x_k\rangle$

למשל: ב-$\mathbb{Z}[x]$ $\langle 2,x\rangle = \{2f(x)+x\cdot g(x) \mid f(x),g(x)\in\mathbb{Z}[x]\} \subsetneq \mathbb{Z}[x]$,

ב-$\mathbb{Z}$, $\langle 3,14\rangle = \{3m+14n \mid m,n\in\mathbb{Z}\} = \mathbb{Z} = \langle 1\rangle$

הגדרה:

יהיו $I,J\lhd R$. <u>המכפלה</u> שלהם היא

$$IJ = \left\{\sum_{k=1}^{n} i_k j_k \,\middle|\, i_k\in I,\ j_k\in J,\ n\in\mathbb{N}\right\}$$

דוגמה:

המכפלה ה"נקודתית" של אידאלים אינה בהכרח אידאל. למשל, $R=\mathbb{Z}[x]$, $I=\langle 2,x\rangle$, $J=\langle 3,x\rangle$. פה $\{ij \mid i\in I, j\in J\}$ לא אידאל ($6+x^2$ לא נמצא בה)

$$\begin{tikzcd}[column sep=small] & I+J \arrow[dl, dash] \arrow[dr, dash] & \\ I \arrow[dr, dash] & & J \arrow[dl, dash] \\ & I\cap J \arrow[d, dash] & \\ & IJ & \end{tikzcd}$$

תמיד $IJ \subseteq I \cap J$.

<u>הגדרה:</u>

$I,J \lhd R$ הם <u>קו-מקסימליים</u> אם $I+J=R$.

באופן שקול: $1 \in I+J$.

<u>תרגיל:</u>

אם I,J בחוג חילופי, קו-מקסימליים אז $IJ = I \cap J$.

<u>הוכחה:</u>

$\boxed{\subseteq}$ נכון תמיד. אם $\sum_{k=1}^{n} i_k j_k \in IJ$

$$i_k \in I \overset{\text{בליעה}}{\Longrightarrow} i_k j_k \in I \overset{\text{סגירות לחיבור}}{\Longrightarrow} \sum_{k=1}^{n} i_k j_k \in I$$

בדומה ל-J. לכן $\sum_{k=1}^{n} i_k j_k \in I \cap J$.

$\boxed{\supseteq}$ I,J קו-מקסימליים, לכן קיימים $i \in I$ ו- $j \in J$ כך ש- $1 = i+j$.

כעת לכל $a \in I \cap J$,

$$a = a \cdot 1 = a \cdot (i+j) = ai + aj \underset{\text{חילופי } R}{=} \underset{I}{i}\,\underset{J}{a} + \underset{I}{a}\,\underset{J}{j} \in IJ$$

$\square$

<u>דוגמה:</u>

$R=\mathbb{Z}$, $I = 2\mathbb{Z}$, $J = 3\mathbb{Z}$, $I+J = \gcd(2,3)\mathbb{Z} = \mathbb{Z}$

$I \cap J = \operatorname{lcm}(2,3)\mathbb{Z} = 6\mathbb{Z} = (2\mathbb{Z})\cdot(3\mathbb{Z})$

<u>דוגמה:</u>

ב-$\mathbb{Z}[x]$, $\langle x-1 \rangle$ ו- $\langle 2x-1 \rangle$ קו-מקסימליים. למה?

$$(-2)\cdot(x-1) + 1 \cdot (2x-1) = -2x+2+2x-1 = 1$$

לכן 1 שייך לסכום האידיאלים.

משפטי האיזומורפיזם

משפט: (משפט האיזומורפיזם הראשון)

אם $\varphi: R\to S$ הומומורפיזם, אז $R/\ker\varphi \cong \operatorname{Im}\varphi$.

בפרט, אם φ אפימורפיזם, אז $R/\ker\varphi \cong S$.

דוגמאות:

א. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

שלמים מודולו n

$\varphi:\mathbb{Z}\to\mathbb{Z}_n$, $\varphi(a)=a \pmod n$

ב. יהי R חוג חילופי, ויהי $a\in R$. (מספיק לקחת R חוג ו- $a\in Z(R)$).

$$\begin{aligned}\varphi_a: R[x] &\to R\\ 1 &\mapsto 1\\ x &\mapsto a\\ f(x) &\mapsto f(a)\end{aligned}$$ ההומומורפיזם ההצבה

$\ker\varphi_a=\langle x-a\rangle$, φ_a אפימורפיזם

$$R[x]/\langle x-a\rangle \cong R$$

ג. $\varphi_i: \mathbb{R}[x]\to\mathbb{C}$

$f(x)\mapsto f(i)$

אפימורפיזם, $\ker\varphi_i=\langle x^2+1\rangle$, לכן $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$.

הגדרה:

יהי R חוג, $R_0\subseteq R$ תת-חוג, $X\subseteq R$ קבוצה. תת-החוג שנוצר ע"י X (מעל R_0) הוא חיתוך כל תת-החוגים של R שמכילים את R_0 ואת X. נסמן אותו $R_0[X]$. אם $R_0[X]=R$, נאמר ש-R נוצר ע"י X מעל R_0.

אם $X=\{a_1,\dots,a_n\}$, נסמן $R_0[X]=R_0[a_1,\dots,a_n]$.

אם R נוצר ע"י קבוצה סופית מעל R_0, נאמר שהוא נוצר סופית מעל R_0.

דוגמה:

$\mathbb{Q}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{2}]$ הם מהצורה הנ"ל.

הערה:

אם $a\in Z(R)$, אז $=R_0[a]$ הפולינומים עם מקדמים ב-R_0 שמוצבים בהם a.

$$\mathbb{Z}[\sqrt[3]{2}]=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}\mid a,b,c\in\mathbb{Z}\}$$

$R=\mathbb{Q}$
$R_0=\mathbb{Z}$
$X=\{\frac{1}{3}\}$

$$\mathbb{Z}[\tfrac{1}{3}]=\{a+\tfrac{b}{3}+\tfrac{c}{9}+\dots+\tfrac{\xi}{3^n}\mid n\in\mathbb{Z},a,b,\dots,\xi\in\mathbb{Z}\}=\{\tfrac{a}{3^n}\mid a\in\mathbb{Z},n\in\mathbb{N}\}$$

דוגמה:

$R[x_1,\dots,x_n]$ נוצר סופית מעל R עבור $X=\{x_1,\dots,x_n\}$.

דוגמה:

$\mathbb{Z}$ נוצר סופית מעל $n\mathbb{Z}$ $(n\neq0)$, כי הוא פשוט נוצר ע"י $\{1\}$.

תרגיל:

חוג חילופי שנוצר סופית מעל R_0 הוא (איזומורפי) למנה של חוג הפולינומים $R_0[x_1,\dots,x_n]$ ל-n כלשהו.

הוכחה:

נניח ש-R חילופי ונוצר מעל R_0 ע"י $X=\{a_1,\dots,a_n\}$.

נגדיר $\pi:R_0[x_1,\dots,x_n]\longrightarrow R$ ע"י $\pi(x_i)=a_i$ ונרחיב ע"י החיבוריות והכפליות

$$\pi(f(x_1,\dots,x_n))=f(a_1,\dots,a_n).$$

זה הומומורפיזם כי R חילופי.

למה הוא על? כי כל איבר של R הוא פולינום מעל R_0 ב-$a_1,\dots,a_n$.

לכן $R\cong{}^{R_0[x_1,\dots,x_n]}/_{\ker\pi}$.

$\square$

דוגמה:

$$\varphi: \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\sqrt[3]{2}]$$
$$x \longmapsto \sqrt[3]{2}$$
$$\ker\varphi = \langle x^3-2 \rangle$$

$$\Longrightarrow \mathbb{Q}[x]/\langle x^3-2\rangle \cong \mathbb{Q}[\sqrt[3]{2}]$$

דוגמה:

$$\mathbb{Z}\left[\tfrac{1}{3}\right] \cong \mathbb{Z}[x]/\langle 3x-1 \rangle$$

דוגמה:

$$\mathbb{Q}[\pi] \cong \mathbb{Q}[x]$$

משפט: (משפט האיזומורפיזם השני)

יהי R חוג, יהי $S\subseteq R$ תת-חוג, ויהי $I \triangleleft R$ אידיאל. אזי

$$S/S\cap I \cong S+I/I$$

(יש פה כמה טענות שמסתתרות:

א. $I \triangleleft S+I$

ב. $S\cap I \triangleleft S$

ג. יש איזומורפיזם)

דוגמה:

$R=\mathbb{Z}$, $S=a\mathbb{Z}$, $I=b\mathbb{Z}$

$$a\mathbb{Z}/\mathrm{lcm}(a,b)\mathbb{Z} = S/S\cap I \cong S+I/I = \gcd(a,b)\mathbb{Z}/b\mathbb{Z}$$

תרגיל:

יהי R חוג, $S\subseteq R$ תת-חוג ו- $I\triangleleft R$ אידאל. אז יש שיכון $R/I \hookleftarrow S/S\cap I$.

הוכחה:

$$S/S\cap I \underset{\text{איזו 2}}{\cong} S+I/I \underset{\text{הכלה}}{\hookrightarrow} R/I$$

$$x+I \mapsto x+J$$

$\square$

תרגיל:

יהיו $I\subseteq J$ אידאלים של R. הוכיחו שקיימת העתקה $R/I \longrightarrow R/J$.

(אפימורפיזם)

הוכחה:

רוצים להגדיר $\varphi: R/I \longrightarrow R/J$. נגדיר, בלית ברירה,

$\varphi(r+I)=r+J$.

φ מוגדרת היטב: אם $r+I=s+I$, אז $r-s\in I\subseteq J$ $\Leftarrow$ $r-s\in J$ $\Leftarrow$ $r+J=s+J$.

φ מכבדת חיבור:

$$\varphi((r+I)+(s+I))=\varphi((r+s)+I)=(r+s)+J=(r+J)+(s+J)=\varphi(r+I)+\varphi(s+I)$$

φ מכבדת כפל - בדומה.

$\varphi(1_{R/I})=\varphi(1+I)=1+J=1_{R/J}$.

$\Leftarrow$ φ הומומורפיזם.

למה φ על? כי $r+J\in R/J$, $\varphi(r+I)=r+J$. לכן φ אפימורפיזם. $\square$

משפט: (משפט האיזומורפיזם השלישי)

יהיו $I\subseteq J$ אידאלים של חוג R. אזי $R/I \big/ J/I \cong R/J$.

משפט השאריות הסיני

משפט:

יהיו $I_1,\dots,I_n \triangleleft R$ קו-מקסימליים בזוגות. אז $R/_{I_1\cap\dots\cap I_n} \cong R/_{I_1} \times \dots \times R/_{I_n}$.

מסקנה:

אם ניקח $R=\mathbb{Z}$, $I_1=m_1\mathbb{Z},\dots,I_n=m_n\mathbb{Z}$, $m_1,\dots,m_n$ זרים בזוגות, אז

$$\mathbb{Z}/_{m_1\cdots m_n\mathbb{Z}} \cong \mathbb{Z}/_{m_1\mathbb{Z}} \times \dots \times \mathbb{Z}/_{m_n\mathbb{Z}}$$

איך נראית ההופכית?

אם רוצים
$$x \equiv a \pmod{m_1}$$
$$x \equiv b \pmod{m_2}$$

$\gcd(m_1,m_2)=1 \Leftarrow 1=sm_1+tm_2 \Leftarrow x=bsm_1+atm_2$. למה?

$$x \equiv atm_2 = a(1-sm_1)=a-asm_1\equiv a \pmod{m_1}$$

ובדומה ל- m_2.

דוגמה:

מצא $x\in\mathbb{Z}$ המקיים
$$x\equiv 1 \pmod 3$$
$$x\equiv 2 \pmod 5$$

$\gcd(3,5)=1$, ואכן $1=\underbrace{2}_{s}\cdot 3\underbrace{-1}_{t}\cdot 5$. לכן ה-$x$ המתאים הוא

$$x=2\cdot 2\cdot 3+1\cdot(-1)\cdot 5=7$$

וה-x הזה יחיד מודולו 15.

דוגמה:

$R=\left(\mathbb{Z}/_{3\mathbb{Z}}\right)[x]$.

$$R/_{\langle x^2-x\rangle} \cong ?$$

$$x^2-x=x(x-1)$$

$$\langle x^2-x\rangle=\langle x\rangle\cdot\langle x-1\rangle$$

$\langle x\rangle$, $\langle x-1\rangle$ הם ק-מקסימליים, כי $1\cdot x-1\cdot(x-1)=1$. לכן

$$\langle x^2-x\rangle=\langle x\rangle\cap\langle x-1\rangle$$

$$R/\langle x^2-x\rangle = R/\langle x\rangle\cap\langle x-1\rangle \underset{\uparrow\ \text{CRT}}{\cong} R/\langle x\rangle\times R/\langle x-1\rangle\cong \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$$