אלגברה ב3

ⓒ ארזים

1 בנובמבר 2016

הקורס עוסק במבוא לאלגברה קומוטטיבית, ובעיקר בחוגים קומוטטיביים.

1 חוגים קומוטטיביים

כנגיד "יהי R חוג" אנחנו מתכוונים להגיד "יהי R חוג קומוטטיבי עם יחידה, בו $1 \neq 0$"

1.1 אידאלים

1. חיתוך כלשהו של אידאלים בחוג נתון R הוא אידאל.
2. סכום של אידאלים הוא גם כן אידאל:

$$\sum_{\alpha \in X} I_\alpha = \left\{ \sum_{i=1}^{n} r_{\alpha_i} \mid n \geq 0, \{\alpha_1, \ldots, \alpha_n\} \subseteq X, r_{\alpha_i} \in I_{\alpha_i} \right\}$$

3. נתונה קבוצה $S \subseteq R$. האידאל הנוצר על ידי S הוא

$$I(S) = \left\{ \sum_{i=1}^{n} a_i s_i \mid n \geq 0, \{a_1, \ldots, a_n\} \subseteq R, \{s_1, \ldots, s_n\} \subseteq S \right\}$$

זהו האידאל הקטן ביותר של R שמכיל את S. זהו חיתוך כל האידאלים שמכילים את S.
מקרה פרטי: $S = \{s\}$, ואז $I(S) = R \cdot s = \{a \cdot s \mid a \in R\}$ נקרא <u>אידאל ראשי</u>, ונאמר שהוא <u>נוצר</u> על ידי האיבר s.
חוג שבו כל האידאלים ראשיים יקרא <u>חוג ראשי</u>.
ניתן לכתוב גם

$$I(S) = \sum_{s \in S} Rs$$

4. מכפלה: יהיו I, J שני אידאלים בחוג R. נגדיר את האידאל

$$IJ = \left\{ \sum_{i=1}^{n} a_k b_k \mid n \geq 0, a_k \in I, b_k \in J \right\}$$

באופן דומה נגדיר $I_1, I_2, \ldots, I_n$.

סימון $R^* = \{a \in R \mid \exists b \in R . ab = 1\}$

R^* היא חבורה כפלית ביחס לכפל, שכן $(ab)\left(a^{-1}b^{-1}\right) = 1$.

טענה 1.1 1. יהי $0 \neq I \subseteq R$ אידאל. אזי $I = R$ אם ורק אם $I \cap R^* \neq \emptyset$.

2. חוג R שאין בו אידאלים לא טריוויאליים הוא שדה.

3. בשדה אין אידאלים לא טריוויאליים.

הוכחה:

1. נניח כי $I \neq 0$. אם $I = R$, $1 \in I \cap R^*$. להיפך, אם $a \in I \cap R^*$, אזי $a^{-1} \cdot a = 1 \in I$, ולכן לכל $r \in R$ מתקיים $r = r \cdot 1 \in I$, כלומר $I = R$.

2. נניח כי בחוג R אין אידיאלים לא טריוויאליים. יהי $0 \neq a \in R$. $Ra \subseteq R$ הוא אידאל, ולכן טריוויאלי. $Ra \neq 0$, שכן $a = 1 \cdot a \in Ra$, ולכן $Ra = R$. בפרט, $1 \in Ra$, כלומר קיים $b \in R$ כך שמתקיים $1 = ba$, ולכן a הפיך.

3. נניח כי R שדה. יהי $0 \neq I \subseteq R$ אידאל. בהכרח I מכיל איבר שונה מאפס, שבהכרח הפיך כי מדובר בשדה. לכן I מכיל איבר הפיך - ולכן הוא כל החוג.

■

הגדרה 1.2 נתונים שני אידאלים $I, J \subsetneq R$. נאמר כי האידאלים <u>זרים</u> אם $I + J = R$. תנאי שקול: ניתן לכתוב $1 = u + v$, כאשר $u \in I, v \in J$.

דוגמא נניח כי $m, n \in \mathbb{Z}$ זרים. אזי קיימים a, b שלמים כך שמתקיים $am + bn = 1$. זה אומר שהאידאלים הראשיים $\mathbb{Z} \cdot m, \mathbb{Z} \cdot n$ זרים.

הערה 1.3 $\mathbb{Z}$ הוא חוג ראשי.

הוכחה: יהי $I \subseteq \mathbb{Z}$ אידאל. אם $I = 0$, אזי $I = \mathbb{Z} \cdot 0$. נניח $I \neq 0$. יהי n הטבעי המינימלי שמקיים $n \in I$. נראה כי $I = \mathbb{Z} \cdot n$. ראשית, $\mathbb{Z} \cdot n \subseteq I$, שכן I אידאל וכן $n \in I$. שנית, יהי $a \in I$. נחלק עם שארית:

$$a = ln + r$$

כאשר $0 \leq r < n$. כעת נקבל כי $r = a - ln \in I$. ממינימליות n, נקבל כי $r = 0$, ולכן $a = ln$. לכן $I \subseteq \mathbb{Z} \cdot n$, ובסך הכל $I = \mathbb{Z} \cdot n$. ■

הערה 1.4 באותו אופן, עבור שדה $\mathbb{F}$, חוג הפולינומים $\mathbb{F}[x]$ הוא חוג ראשי.

משפט 1.5 יהיו $I_1,\dots,I_n$ אידאלים בחוג R. נתבונן בחוגי המנה $R/I_1,\dots,R/I_n$, ובהומומורפיזם:

$$\begin{aligned}\phi:R &\to R/I_1\times\cdots\times R/I_n\\ \phi(x) &= (x+I_1,\dots,x+I_n)\end{aligned}$$

אזי:

1. ϕ הוא הומומורפיזם על $\iff$ האידאלים זרים בזוגות.
2. ϕ הוא הומומורפיזם חד־חד־ערכי $\iff$ חיתוך כל האידאלים הוא טריוויאלי.
3. נניח כי האידאלים זרים בזוגות. אזי

$$\bigcap_{j=1}^{n} I_j = \prod_{j=1}^{n} I_j$$

הוכחה:

1. נניח כי ϕ על. בפרט, לכל $1\le i\le n$ קיים $x_i\in R$ המקיים

$$\phi(x_i) = (I_1,\dots,I_{i-1},I_i+1,I_{i+1},\dots,I_n)$$

מההגדרה,

$$\phi(x_i) = (x+I_1,\dots,x+I_n)$$

ומכאן שמתקיים

$$\forall j\neq i \quad x\in I_j$$

וכן מתקיים $x_i\in 1+I_i$, כלומר קיים $u_i\in I_i$ כך שמתקיים

$$\begin{aligned}x_i &= 1+u_i\\ 1 &= x_i+(-u_i)\end{aligned}$$

כעת, $u_i\in I_i$, $x_i\in I_j$ כלשהו, ולכן I_i,I_j זרים לכל i,j.
בכיוון השני, נניח כי האידאלים זרים בזוגות. לכל $1\le i\neq j\le n$, נכתוב את 1 בתור

$$1 = u_{ij}+v_{ij}$$

כאשר $u_{ij}\in I_i, v_{ij}\in I_j$. נגדיר

$$x_i = \prod_{\substack{j=1\\ i\neq j}}^{n} v_{ij}$$

כמובן, $v_{ij} \in I_j$, ולכן $x_i \in I_j$ לכל $i \neq j$. כמו כן, ניתן לכתוב

$$x_i = \prod_{\substack{j=1 \\ i \neq j}}^{n} (1 - u_{ij})$$

כל גורם הוא בתוך $1 + I_i$, שהיא סגורה ביחס לכפל. כלומר, קיבלנו כי $x_i \in 1 + I_i$.
נסיק כי

$$\phi(x_i) = (I_1, \dots, I_{i-1}, 1 + I_i, I_{i+1}, \dots, I_n)$$

יהיו $y_1, \dots, y_n$ בחוג. כעת,

$$\begin{aligned} \phi\left(\sum_{i=1}^{n} x_i y_i\right) &= \sum_{i=1}^{n} \phi(x_i)\,\phi(y_i) = \sum_{i=1}^{n} (I_1, \dots, I_{i-1}, y_i + I_i, I_{i+1}, \dots, I_n) = \\ &= (y_1 + I_1, \dots, y_n + I_n) \end{aligned}$$

ולכן ϕ אכן על.

2. ϕ חד־חד־ערכי אם ורק אם $\ker\phi = 0$, ולפי ההגדרה

$$\begin{aligned} \ker\phi &= \{x \in R \mid (x + I_1, \dots, x + I_n) = (I_1, \dots, I_n)\} = \{x \in R \mid x \in I_1, \dots, x \in I_n\} = \\ &= \bigcap_{i=1}^{n} I_i \end{aligned}$$

בסך הכל ϕ חד־חד־ערכית אם ורק אם חיתוך כל האידאלים הוא טריוויאלי.

3. תמיד מתקיים כי

$$\prod_{j=1}^{n} I_j \subseteq I_j$$

לכל j, ולכן

$$\prod_{j=1}^{n} I_j \subseteq \bigcap_{j=1}^{n} I_j$$

את ההכלה בכיוון השני נוכיח באינדוקציה על n. הבסיס הוא $n = 2$:

$$I_1 \cap I_2 = R(I_1 \cap I_2) = (I_1 + I_2)(I_1 \cap I_2) \subseteq I_1 \cdot I_2$$

זאת משום שאם ניקח $a \in I_1, b \in I_2, u \in I_1 \cap I_2$, נקבל

$$(a + b)\,u = au + bu$$

כאשר $au \in I_1I_2, bu \in I_2I_1$.
עבור הצעד, נסמן

$$J = \prod_{i=1}^{n-1} I_i$$

באינדוקציה, מתקיים

$$J = \bigcap_{k=1}^{n-1} I_k$$

כעת נראה כי J זר לאידאל I_n. נתבונן באיבר

$$x_n = \prod_{j=1}^{n-1} v_{nj}$$

מתוך הוכחת הסעיף הראשון. מבניית x_n נובע כי מתקיים $x_n \in J$. כמו כן, ראינו כי $x_n \in 1 + I_n$. לכן קיים $a \in I_n$ כך שמתקיים

$$1 = x_n + (-a)$$

לכן I_n, J זרים, וכעת ממקרה הבסיס $n = 2$ מתקבל כי

$$\begin{aligned} J \cap I_n &= JI_n \\ \bigcap_{i=1}^{n} I_j &= \prod_{j=1}^{n} I_j \end{aligned}$$

■

מסקנה 1.6 נניח, בסימונים הקודמים, כי $I_1, \ldots, I_n$ אידאלים זרים בזוגות. אזי ϕ משרה איזומורפיזם של חוגים

$$\begin{aligned} R/\left(\prod_{j=1}^{n} I_j\right) &\cong R/I_1 \times \cdots \times R/I_n \\ x + \prod_{j=1}^{n} I_j &\to (x + I_1, \ldots, x + I_n) \end{aligned}$$

משום שמתקיים

$$\ker \phi = \bigcap_{j=1}^{n} I_j = \prod_{j=1}^{n} I_j$$

שכן האידאלים זרים בזוגות, וכן ϕ על.

כאשר $R=\mathbb{Z}$, נסמן

$$I_i=\mathbb{Z}m_i$$

כעת הם זרים בזוגות, כלומר $m_1,\ldots,m_n$ זרים בזוגות (נניח כי הם טבעיים). כעת המסקנה אומרת לנו כי

$$\mathbb{Z}/\mathbb{Z}m_1m_2\ldots m_n\cong\mathbb{Z}/\mathbb{Z}m_1\times\cdots\times\mathbb{Z}/\mathbb{Z}m_n$$

וזה מוכר לנו כמשפט השאריות הסיני, מתורת המספרים.

1.2 אידאלים ראשוניים, אידאלים מקסימליים והרדיקל הנילי

הגדרה 1.7 החוג R ייקרא <u>תחום שלמות</u> אם לכל $a,b\in R$ מתקיים

$$ab=0\Rightarrow a=0\vee b=0$$

טענה 1.8 נניח כי R תחום שלמות. אזי גם $R[x]$ - חוג הפולינומים במשתנה אחד מעל R - הוא תחום שלמות.

הוכחה: נניח כי $f(x),g(x)\neq 0$. נסמן

$$\begin{aligned} f(x) &= \sum_{i=0}^{n}a_ix^i \\ g(x) &= \sum_{i=0}^{m}b_ix^i \end{aligned}$$

כאשר $a_n,b_m\neq 0$. כעת מתקיים כי

$$f(x)\,g(x)=a_nb_mx^{n+m}+h(x)$$

כאשר $h(x)$ הוא פולינום כלשהו מדרגה שקטנה ממש מאשר $m+n$. משום שנתון שהתחום R הוא תחום שלמות, $a_nb_m\neq 0$, ולכן קיבלנו בסך הכל כי $\deg(fg)=\deg f+\deg g$ (כאשר $\deg 0=-\infty$).

מכאן כמובן שמתקיים $f(x)\,g(x)\neq 0$. ■

כך נוכל לייצר הרבה תחומי שלמות: למשל נתחיל עם שדה $\mathbb{F}$. ניקח את החוג $\mathbb{F}[x_1]$, שהוא תחום שלמות. כעת גם החוג $(\mathbb{F}[x_1])[x_2]$ הוא תחום שלמות, ואפשר להתייחס אליו בתור $\mathbb{F}[x_1,x_2]$ - פולינומים בשני משתנים מעל השדה $\mathbb{F}$. כך נמשיך להגדיר את $\mathbb{F}[x_1,\ldots,x_n]$ ולקבל תחום שלמות. אם נחליף את $\mathbb{F}$ בתחום שלמות R נקבל עדיין תחומי שלמות.

יהי $I\subsetneq R$ אידאל (כאשר R חוג). נבדוק מתי R/I הוא תחום שלמות. נשים לב כי

$$(x+I)(y+I)=I\iff xy\in I$$

וכן

$$y+I=I\vee x+I=I \iff y\in I\vee x\in I$$

כדי לקבל תחום שלמות, נרצה שהתנאים הללו יהיו שקולים (מההגדרה). לכן בסך הכל מתקיים כי R/I תחום שלמות אם ורק אם מתקיים

$$xy\in I \iff x\in I\vee y\in I$$

הגדרה 1.9 אידאל שמקיים תכונה זו נקרא ראשוני.

דוגמא יהי $I\subsetneq\mathbb{Z}$ אידאל ראשוני. נסמן $I=\mathbb{Z}\cdot n$, כאשר n טבעי. מתקיים

$$\begin{aligned} xy\in\mathbb{Z}\cdot n &\Rightarrow x\in\mathbb{Z}\cdot n\vee y\in\mathbb{Z}\cdot n\\ n\mid xy &\Rightarrow n\mid x\vee n\mid y\end{aligned}$$

כלומר n הוא מספר ראשוני. בחוג הפולינומים מעל שדה היינו מקבלים כי האידאל חייב להיווצר על ידי פולינום אי פריק.

הגדרה 1.10 אידאל $I\subsetneq R$ נקרא מקסימלי אם האידאל היחיד שמכיל את I ממש הוא R.

טענה 1.11 $I\subsetneq R$ אידאל מקסימלי אם ורק אם חוג המנה R/I הוא שדה.

הוכחה: נניח כי I אידאל מקסימלי. אידאל בחוג R/I הוא מהצורה J/I, כאשר $I\subseteq J\subseteq R$ אידאל של R. ממקסימליות I נובע כי $J=I$ או $J=R$, כלומר J/I הוא אידאל טריוויאלי של חוג המנה. לכן לחוג המנה אין אידאלים לא טריוויאליים, ומכאן שהוא שדה.

כעת נניח כי R/I הוא שדה. יהי $I\subseteq J\subseteq R$ אידאל של R. J/I הוא אידאל של השדה R/I, ולכן בהכרח טריוויאלי. מכאן בהכרח כי $J=I$ או $J=R$. לכן I אידאל מקסימלי.$\blacksquare$

מסקנה 1.12 אידאל מקסימלי הוא ראשוני (כי שדה הוא +תחום שלמות).

טענה 1.13 יהי R תחום שלמות ראשי. אזי כל אידאל ראשוני לא טריוויאלי של R הוא מקסימלי.

הוכחה: יהי $I\subsetneq R$ אידאל ראשוני לא טריוויאלי. יהי $I\subsetneq J\subseteq R$ אידאל של R, ונראה כי בהכרח $J=R$. R תחום ראשי, ולכן נכתוב $I=Ra, J=Rb$. הנחנו כי $I=Ra\subsetneq J=Rb$. בפרט, $a\in J$, כלומר ניתן לכתוב, עבור $r\in R$ כלשהו, $a=br\in I$. I ראשוני, ולכן בהכרח $b\in I$ או $r\in I$. $b\notin I$ שכן אחרת $J\subseteq I$, בסתירה. לכן $r\in I$. לכן קיים $s\in R$ כלשהו עבורו $r=sa$. בסך הכל נקבל כי $a=br=bsa$. בתחום שלמות אנחנו יכולים לצמצם איברים שאינם 0 - I אינו טריוויאלי, ולכן $a\neq 0$. בסך הכל קיבלנו כי $sb=1$, כלומר b הפיך - ולכן $J=R$. $\blacksquare$