

אלגברה ב2

© ארזים

15 במרץ 2017

1 הקדמות

1.1 חוגים

הגדרה 1.1 יהי R חוג ותהי $A \subseteq R$. נסמן את האידאל המינימלי של R שמכיל את A בתור (A) . אזי, איברי (A) הם כל הביטויים מהצורה

$$\sum_{i=1}^n a_i r_i$$

כאשר $r_i \in R, a_i \in A$ אם A סופית, עם $A = \{a_1, \dots, a_n\}$, נרשום

$$(A) = (a_1, \dots, a_n) = \sum_{i=1}^n a_i R$$

טענה 1.2 יהי $f : R \rightarrow S$ הומומורפיזם של חוגים. אזי $\ker f = \{r \in R \mid f(r) = 0\}$ הוא אידאל של R , ויתר על כן, f חד-חד-ערכית אם ורק אם $\ker f = 0$.

הוכחה: יהי $x \in R, y \in \ker f$. אזי

$$f(xy) = f(x)f(y) = f(x) \cdot 0 = 0$$

לכן $xy \in \ker f$. לפי ההגדרה, $f(0) = 0$, ולכן $\ker f$ לא ריק. כמו כן, אם $x, y \in \ker f$ אז

$$f(x+y) = f(x) + f(y) = 0 + 0 = 0$$

ולכן $\ker f$ אידאל. אם f חד-חד-ערכי אז יש פתרון יחיד עבור $f(x) = 0$, והוא $x = 0$. לכן $\ker f = 0$.

נניח כי $\ker f = 0$. נקח $x, y \in R$ ונניח כי $f(x) = f(y)$. אזי

$$f(x-y) = 0$$

$$x-y = 0$$

$$x = y$$

ולכן f חד־חד־ערכית. ■

הגדרה 1.3 אם ניקח $I \triangleleft R$ (סימון עבור I שהוא אידיאל בחוג $(R, +)$), בפרט $(I, +)$ תת חבורה נורמלית של $(R, +)$, ולכן יש מבנה של חבורה ביחס לחיבור על

$$R/I = \{r + I \mid r \in R\} = \{\{r + \alpha \mid \alpha \in I\} \mid r \in R\}$$

ניתן להגדיר עליה גם כפל:

$$(r_1 + I)(r_2 + I) = r_1 r_2 + I$$

נראה אי תלות בבחירת הנציגים. נניח כי $r_1 = r'_1 + \alpha, r_2 = r'_2 + \beta$ כאשר $\alpha, \beta \in I$ ואז

$$r_1 r_2 + I = r'_1 r'_2 + \alpha r'_2 + \beta r'_1 + \alpha \beta + I$$

אבל $\alpha r'_2, \beta r'_1, \alpha \beta \in I$ שייכים אל I מהגדרת האידיאל. כעת R/I הוא חוג עם $0 + I, 1 + I$ בתור היחידות, והפעולות שראינו.

משפט 1.4 (משפט האיזומורפיזם הראשון) אם $\varphi : R \rightarrow S$ הוא אפימורפיזם של חוגים, אזי φ משרה איזומורפיזם

$$R/\ker \varphi \cong S$$

על ידי

$$\bar{\varphi}(x + \ker \varphi) = \varphi(x)$$

הוכחה: מתורת החבורות, $\bar{\varphi}$ מוגדרת היטב. $\bar{\varphi}$ הומומורפיזם כי φ הומומורפיזם, וכך גם היא על משום שלקחנו φ אפימורפיזם. נותר להראות כי φ מונומורפיזם:

$$\ker \bar{\varphi} = \{x + \ker \varphi \mid \varphi(x) = 0\} = \{\ker \varphi\}$$

■

1.2 שדות

הגדרה 1.5 שדה הוא חוג (חילופי עם יחידה) שבו כל איבר שאינו 0 הוא הפיך, וכן היחידות שונות, כלומר $0 \neq 1$.

הגדרה 1.6 תת שדה הוא תת חוג שהוא גם שדה.

דוגמאות $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, כאשר p ראשוני. אוסף הפונקציות המרומורפיות מהמישור המרוכב למישור המרוכב.

תרגיל הומומורפיזם של שדות הוא תמיד חד־חד־ערכי.

1.2.1 מאפיין (קרקטריסטיקה) של שדה

יהי F שדה. מוגדרת העתקה $c: \mathbb{Z} \rightarrow F$ על ידי

$$c(n) = \underbrace{1 + 1 + \dots + 1}_n$$

זהו הומומורפיזם. לכל $n \in \mathbb{Z}$, מתקיים

$$c(-n) = -c(n)$$

נתבונן באידאל $\ker c \triangleleft \mathbb{Z}$.

ראשית, $1 \notin \ker c$, שכן $1 \neq 0$ בשדה. תתי החבורות של $\mathbb{Z}$ הן $n\mathbb{Z}$, עבור $n > 0$, ואלה גם האידאלים.

מקרה ראשון: $\ker c = 0$. אזי נזהה את $\mathbb{Z}$ עם תמונתו בתוך F . כיוון שזהו שדה, לכל $n \in \mathbb{Z}$ גם $\frac{1}{n} \in F$. לכן $\mathbb{Q} \subseteq F$.

מקרה שני: $\ker c = (n) = n\mathbb{Z}$. ראשית, נטען כי n ראשוני. אחרת, נכתוב $n = a \cdot b$, ואז

$$0 = c(n) = c(ab) = c(a)c(b) \neq 0$$

שכן F שדה, וכן $a, b < n$. זוהי סתירה. לכן n ראשוני. לפי משפט האיזומורפיזם הראשון מתקיים

$$c(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

לכן F מכיל את $\mathbb{F}_p$. במקרה כזה נאמר שהמאפיין של F הוא p , ונסמן $\text{char } F = p$. השדות $\mathbb{Q}, \mathbb{F}_p$ עבור p ראשוני - נקראים השדות הראשוניים.

סיכום כל שדה F מכיל בדיוק שדה ראשוני 1.

טענה 1.7 אם F שדה ממאפיין $0 < p$, אזי ההעתקה $x \mapsto x^p$ היא הומומורפיזם.

הוכחה: הדבר היחיד שאינו מיידי היא שההעתקה שומרת על חיבור. ואכן

$$(x+y)^p = x^p + \cancel{px^{p-1}y} + \dots + \cancel{\binom{p}{k}x^k y^{p-k}} + \dots + y^p = x^p + y^p$$

הביטולים הם משום שמספרים k קטנים יותר מאשר p , וזו טענה כללית על מקדמים בינומיים - $p \mid \binom{p}{k}$. זה נכון כי המקדם הבינומי שלם וכן מקיים

$$\binom{p}{k} = \frac{p(p-1)!}{k!(p-k)!}$$

ואין דבר שיצמצם את p במכנה - כל הגורמים שם קטנים יותר מאשר p . ■

הגדרה 1.8 ההומומורפיזם $x \mapsto x^p$ במאפיין p נקרא אנדומורפיזם פרובניוס ומסומן Fr .

"זה נקרא אנדומורפיזם פרובניוס, כי פרובניוס באיטלקית זה 'להעלות בחזקה' - המרצה.

דוגמאות

1. נקיח

$$\begin{aligned}\text{Fr} : \mathbb{F}_p &\rightarrow \mathbb{F}_p \\ \text{Fr}(x) &= x^p \bmod p = x \bmod p\end{aligned}$$

לכן זוהי העתקת הזהות, ולכן היא חד-חד-ערכית ועל.

2. ניקח $\mathbb{F}_p(t)$, שדה הפונקציות הרציונאליות מעל $\mathbb{F}_p$ (כלומר מנות בין פולינומים). אזי

$$\text{Fr} : \mathbb{F}_p(t) \rightarrow \mathbb{F}_p(t)$$

העתקה לא על, שכן t לא בתמונה. תמונת ההומומורפיזם היא $\mathbb{F}_p(t^p)$, פונקציות רציונאליות במשתנה t^p .

טענה 1.9 אם R תחום שלמות, אזי R הוא תת חוג של שדה כלשהו.

הוכחה: נרצה "להוסיף" איברים מהצורה $\frac{r}{s}$, כאשר $r, s \in R$, $s \neq 0$. נגדיר יחס שקילות על $R \times R \setminus \{0\}$

$$(r_1, s_2) \sim (r_2, s_1) \iff r_1 s_2 = r_2 s_1$$

זהו אכן יחס שקילות - נבדוק טרנזיטיביות. אם

$$r_1 s_2 = r_2 s_1 \tag{1}$$

$$r_2 s_3 = r_3 s_2 \tag{2}$$

אזי נכפול אותם ונקבל

$$r_1 s_2 r_2 s_3 = r_2 s_1 r_3 s_2$$

אם $r_2 \neq 0$ מותר לצמצם ואז

$$r_1 s_3 = r_3 s_1$$

ולכן נקבל טרנזיטיביות. אילו $r_2 = 0$, מהשוויון הראשון $r_1 = 0$, ומהשוויון השני $r_2 = 0$. לכן

$$(r_1, s_1) = (0, s_1) \sim (0, s_3) = (r_3, s_3)$$

כעת נסמן

$$F = \text{Frac}(R) = R \times (R \setminus \{0\}) / \sim$$

בקבוצה זו נגדיר כפל וחיבור: נסמן $\frac{r}{s}$ את מחלקת השקילות של (r, s) . כעת נגדיר

$$\begin{aligned} \frac{r_1}{s_1} + \frac{r_2}{s_2} &= \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \\ \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} &= \frac{r_1 r_2}{s_1 s_2} \end{aligned}$$

נגדיר גם $\frac{0}{1} = 0, \frac{1}{1} = 1$.
ההגדרות לא תלויות בבחירת הנציגים: נבדוק את הכפל, החיבור נשאר כתרגיל. נניח כי

$$\begin{aligned} \frac{r'_1}{s'_1} &= \frac{r_1}{s_1} \\ \frac{r'_2}{s'_2} &= \frac{r_2}{s_2} \end{aligned}$$

וכעת יש להראות כי

$$\frac{r_1 r_2}{s_1 s_2} = \frac{r'_1 r'_2}{s'_1 s'_2}$$

נבדוק:

$$r_1 r_2 s'_1 s'_2 = (r_1 s'_1) (r_2 s'_2) = (r'_1 s_1) (r'_2 s_2) = r'_1 r'_2 s_1 s_2$$

ולכן קיבלנו אי תלות בנציגים.
נשאר להראות כי F שדה. נראה רק קיום הופכי: עבור $r \neq 0$,

$$\left(\frac{r}{s}\right)^{-1} = \frac{s}{r}$$

כמובן שזה עובד.
נזהה את R עם תת החוג של F שנתון על ידי

$$\left\{ \frac{r}{1} \mid r \in R \right\}$$

■

הגדרה 1.10 השדה שבנינו, $\text{Frac}(R)$, נקרא שדה השברים של R .

1.3 חוגי פולינומים

הגדרה 1.11 יהי F שדה. חוג הפולינומים מעל השדה F במשתנה x , שיסומן $F[x]$, מוגדר להיות המרחב הווקטורי ממימד $\aleph_0$ הנפרש על ידי הבסיס הפורמלי

$$\{1, x, x^2, \dots\}$$

עם כפל שמוגדר באופן הבא:

$$\left(\sum_{i=0}^n a_i x^i\right) \left(\sum_{j=0}^m b_j x^j\right) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j\right) x^k$$

עם יחידה 1, ואפס 0. מקבלים כאן מבנה של חוג.

תכונות

1. לכל חוג R שמכיל את $\mathbb{F}$ ולכל $\alpha \in R$, יש הומומורפיזם

$$S_\alpha : \mathbb{F}[x] \rightarrow R$$

$$S_\alpha(f(x)) = f(\alpha)$$

2. קיימת פונקציית המעלה:

$$\deg : \mathbb{F}[x] \rightarrow \mathbb{N} \cup \{-\infty\}$$

$$\deg(f) = \begin{cases} \max\{i \mid a_i \neq 0\} & f = \sum_{i=0}^n a_i x^i \neq 0 \\ -\infty & f = 0 \end{cases}$$

3. **משפט 1.12** בחוג $\mathbb{F}[x]$ יש חלוקה עם שארית: לכל $f, g \in \mathbb{F}[x]$, עם $g \neq 0$, קיימים $q, r \in \mathbb{F}[x]$ כך שמתקיים

$$f = gq + r$$

$$\deg r < \deg g$$

יתר על כן, q, r נקבעים ביחידות.

מסקנה 1.13 1. כל אידאל של החוג $\mathbb{F}[x]$ נוצר על ידי איבר אחד (כלומר זהו תחום ראשי).

2. קיים מחלק משותף מקסימלי, כלומר לכל f, g קיים d כך שהוא מחלק את f, g וכל מחלק משותף אחר e מקיים $e \mid d$.

3. לכל $f, g \in \mathbb{F}[x]$ קיימים $a, b \in \mathbb{F}[x]$ כך שמתקיים

$$af + bg = \gcd(f, g)$$

יתרה מכך, יש אלגוריתם למציאת $\gcd$ והמקדמים a, b - אלגוריתם אוקלידס.