תורת החוגים - תרגול 1

guy.blachar@gmail.com

שקלול הקבלה: בתרגולים מוצג

80% בחינה, 20% בתנים - תרגילים נפוצים שבהם בהרצה

הגדרה:

חוג בלי יחידה $(R,+,\cdot)$ הוא מבנה אלגברי המקיים: (rng, non-unital ring)

1. $(R,+,0)$ הוא חבורה אבלית - חבורה חילופית או חוג.
2. $(R,\cdot)$ הוא חבורה למחצה.
3. מתקיים חוק הפילוג

$$a\cdot(b+c)=a\cdot b+a\cdot c$$
$$(b+c)\cdot a=b\cdot a+c\cdot a$$

הגדרה:

א. R הוא חילופי אם $(R,\cdot)$ חבורה למחצה חילופית.

ב. R חוג (חוג עם יחידה) אם $(R,\cdot)$ מונואיד. היחידה של המונואיד נקראת היחידה של החוג.

ג. R חוג עם חילוק אם $(R\setminus\{0\},\cdot,1)$ חבורה.

ד. R שדה אם $(R\setminus\{0\},\cdot,1)$ חבורה אבלית.

דוגמאות:

1. $(\mathbb{Z},+,\cdot)$ חוג חילופי.
2. $(2\mathbb{Z},+,\cdot)$ חוג בלי יחידה חילופי.
3. $(n\mathbb{Z},+,\cdot)$ חוג חילופי. $n\mathbb{Z}$ שדה $\Leftrightarrow$ n ראשוני.
4. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ שדות.

ג. $M_n(R)$ כאשר R חוג הוא חוג לא חילופי לכל $n>1$.

1. $R[x_1,x_2,\dots]$ חוג הפולינומים ב-∞ משתנים. R חילופי $\iff R[x_1,x_2,\dots,x_n]$ חילופי.

למה כזה לא חילופי?

$$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}$$
$$\begin{pmatrix}0&0\\1&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&1\end{pmatrix}$$

ה. חוג הקווטרניונים $\mathbb{H}=\mathbb{R}+\mathbb{R}i+\mathbb{R}j+\mathbb{R}k$

$i^2=j^2=k^2=-1$

$ij=k$

$ji=-k$

$$ijk=(ij)k=k\cdot k=k^2=-1$$

$\mathbb{H}$ חוג לא חילופי.

למה? לכל איבר $a+bi+cj+dk$ נגדיר "צמוד" $\overline{a+bi+cj+dk}=a-bi-cj-dk$

לכל $z\in\mathbb{H}$ מקיים $z\cdot\bar{z}\in\mathbb{R}$, $z\cdot\bar{z}=0\iff z=0$.

$$z^{-1}=\frac{\bar{z}}{(z\cdot\bar{z})}$$

ו. $(P(X),\Delta,\cap)$ חוג חילופי לא יחידה. הוא לא שדה. חוג בוליאני.

הגדרה:

יהי R חוג. אומרים שאיבר $a\in R$ הפיך משמאל אם קיים $b\in R$ כך ש-$ba=1$.

מ"מ

a הפיך אם הוא הפיך משמאל ומימין.

$$R^\times=\{\text{איברים הפיכים}\}$$

$R^\times$ הוא לכו חוג!

תרגיל:

יהי R חוג חילופי. $A \in M_n(R)$ הפיכה $\iff$ $\det(A)$ הפיכה.

תכונה:

בדיוק כמו בהוכחה שהדטרמיננטה כפלית מעל כל חוג חילופי. אנחנו שוב שבה נזכר.

$\Leftarrow$ אם A הפיכה, יש B כך ש- $AB = BA = I_n$

$$1 = \det(I_n) = \det(AB) = \det(A)\cdot\det(B) = \det(B)\cdot\det(A)$$

(R חילופי)

$\Rightarrow$ נזכר מהשיעור שלכל $A \in M_n(R)$,

$$A \cdot \mathrm{adj}(A) = \mathrm{adj}(A)\cdot A = \det(A)\cdot I_n$$

לכן אם $\det(A)$ הפיכה אז $(\det(A))^{-1}\cdot\mathrm{adj}(A)$ ההופכית של A □

דוגמה:

$A \in M_n(\mathbb{Z})$ הפיכה $\iff \det(A) = \pm 1$.

הוכחה:

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

עם הפעולות הרגילות. נניח ש$a + b\sqrt{2} \neq 0$, אז אם $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

(כאן $a^2 - 2b^2 \neq 0$ כי $a, b \in \mathbb{Q}$)

דוגמה:

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

חוג חילופי שאינו שדה, כי $\frac{1}{2} \notin \mathbb{Z}[\sqrt{2}]$. אבל יש בו אינסוף איברים הפיכים!

אכן, $(3+2\sqrt{2})(3-2\sqrt{2}) = 3^2 - 2\cdot 2^2 = 1$

לכן $3\pm 2\sqrt{2}$ הפיכים. אפשר גם לראות ש $(3+2\sqrt{2})^n$ איבר הפיך לכל $n\in\mathbb{Z}$.

דוגמה:

אם G חבורה אבלית, נסמן ב $End(G) = \{f: G\to G \mid f \text{ הומומורפיזם}\} = \{f: G\to G \mid f(x+y)=f(x)+f(y)\}$.

כלי חשוב בהוכחה ש f הומומורפיזם מתבטאת בפילוג $a\cdot(b+c)=a\cdot b+a\cdot c$.

באופן דומה, אם V מרחב וקטורי נסמן $End(V)=\{T:V\to V \mid T \text{ העתקה לינארית}\}$.

נניח $V=F^{\mathbb{N}}=\{(a_1,a_2,a_3,\dots) \mid a_i\in F\}$, ונגדיר $D, U\in End(V)$ ע"י

$$D((a_1,a_2,\dots)) = (a_2,a_3,\dots)$$
$$U((a_1,a_2,\dots)) = (0,a_1,a_2,\dots)$$

$$D\circ U = Id_V, \qquad U\circ D \neq Id_V$$

ולכן U הפיך משמאל ולא מימין, ו D הפיך מימין ולא משמאל.

$f,g\in End(G)$

$$(f+g)(x) = f(x)+g(x)$$
$$(f\cdot g)(x) = f(g(x))$$

$$\left(f\cdot(g+h)\right)(x) = f\left((g+h)(x)\right) = f(g(x)+h(x)) = f(g(x))+f(h(x)) = (f\cdot g + f\cdot h)(x)$$

הגדרה:

יהי R חוג. איבר $a\in R\setminus\{0\}$ נקרא מחלק אפס שמאלי אם קיים $b\in R\setminus\{0\}$ כך ש $ab=0$.

מחלק אפס ימני: $ba=0$.

הגדרה:

חוג בלי מחלקי אפס נקרא תחום (domain) תחום חילופי נקרא תחום שלם (integral domain).

דוגמאות:

א. $\mathbb{Z}, \mathbb{Z}_p$ כשקיים ראשוני – תחומי שלמות. כל שדה הוא תחום שלמות.

ב. $\mathbb{Z}_{12}$ אינו תחום שלמות כי $3\cdot 4 \equiv 0 \pmod{12}$. הוא שדה לא תחום.

ג. $\mathbb{H}$ תחום אבל לא תחום שלמות.

ד. $M_n(R)$ כש-$n<1$ הוא לא תחום, למשל $\begin{pmatrix}0&1\\0&0\end{pmatrix}^2=\begin{pmatrix}0&0\\0&0\end{pmatrix}$.

הערה:

אם R מתקיים אפס אין הוא לא תחום שלמות. אחרת, עבור $a\neq 0$ הפיך ו- $ab=0$ נסיק:

$$b=1\cdot b=(a^{-1}a)b=a^{-1}(ab)=0$$

מסתירה לכך ש- $b\neq 0$ כך ש- a הופכי מתקיים $ab=0$.

הגדרה:

יהי R חוג. חוג הפולינומים ב- n משתנים מתקבלים מעל R הוא $R[x_1,\dots,x_n]$.

$$(2\cdot x_1)\cdot(3x_1^2x_2)\cdot(x_3x_1)=6x_1^4x_2x_3$$

R תחום שלמות $\iff$ $R[x_1,\dots,x_n]$ תחום שלמות.

R תחום שלמות $\iff$ $R[x_1,\dots,x_m]$ תחום שלמות

R שדה $\not\Rightarrow$ $R[x]$ שדה! למשל

$$\frac{1}{x-1}=1+x+x^2+\dots\notin R[x]$$

לכן $x-1$ אינו הפיך ב- $R[x]$.

דוגמה:

$2x+1\in\mathbb{Z}_4[x]$ הפיך, כי $(2x+1)(2x-1)=4x^2-1=1 \pmod 4$

הגדרה:

אפשר לגזור את חוג הפולינומים במשתנים לא מתחלפים $R\langle x_1,\dots,x_n\rangle$.

$$(2\cdot x_1)\cdot(3x_1^2x_2)\cdot(x_3x_1)=6x_1^3x_2x_3x_1\neq 6x_1^4x_2x_3$$

הוכחה אפשרית:

עבור פולינום $a_0+a_1x+\dots+a_nx^n$

$$(x-1)(a_0+a_1x+\dots+a_nx^n)=$$
$$=a_0+(a_1-a_0)x+(a_2-a_1)x^2+\dots+(a_n-a_{n-1})x^n-a_nx^{n+1}=1$$

$\Leftarrow a_0=-1, a_1=a_0=\dots=a_n=0$

אפשר להמציא גם הוכחה יותר סתירה

תת-חוגים

הגדרה:

יהי R חוג. תת-קבוצה $S \subseteq R$ היא **תת-חוג** (subring) של R אם S היא חוג ביחס לפעולות שאושרו ב-R, ומעלה את אותו היחידה של R.

$S \subseteq R$ נקראת **תת-חוג בעל יחידה** (subring) אם S היא חוג ביחס לפעולות שאושרו ב-R.

טענה:

$R \supseteq S \neq \emptyset$ היא תת-חוג בעל יחידה של R $\iff$ לכל $a,b \in S$, $a-b, ab \in S$.

דוגמאות:

א. $n\mathbb{Z}$ תת-חוג בעל יחידה של $\mathbb{Z}$.

ב. יהי R חוג. אם S תת-חוג של R, אז $M_n(S)$ תת-חוג של $M_n(R)$.

ג. אם איבר היחידה של R נמצא בתת-חוג S, אז $1_R = 1_S$.

לפעמים ל-S יש יחידה אחרת:

$$M_2(\mathbb{C}) \supseteq \left\{\begin{pmatrix} * & * \\ * & 0 \end{pmatrix}\right\} \supseteq \left\{\begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}\right\}$$

$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ תת-חוג בעל יחידה

$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ תת-חוג בעל יחידה שיש לו יחידה

ד. $\mathbb{H} \to$ תת-חוג של $M_2(\mathbb{C})$

$$\left\{\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \middle| a,b \in \mathbb{C}\right\}$$

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

תרגיל:

יהי R חוג כלשהו, ויהי $a\in R$. הוכיחו כי aRa הוא תת-חוג כלשהו של R.

$$aRa=\{axa\mid x\in R\}$$

הוכחה:

$aRa\neq\emptyset$ שכן $0\in aRa$. מהקיבוץ ויון הוא קבוצה, יהיו $axa, aya\in aRa$.

$$axa-aya=a(\underbrace{x-y}_{R})a\in aRa$$

$$(axa)(aya)=a(\underbrace{xaay}_{R})a\in aRa$$

□

תרגיל:

אבר $e\in R$ נקרא אידמפוטנטי (idempotent) אם $e=e^2$.

הוכיחו שאם $e\in R$ אידמפוטנטי אז e הוא איבר היחידה של eRe.

הוכחה:

$eee\in eRe$ כי $e=ee=eee$. נוודא שהוא יחידה:

$$e(eae)=(ee)ae=eae$$

$$(eae)e=ea(ee)=eae$$

□