תורת החוגים - תרגול 1

guy.blachar@gmail.com

שעות קבלה: בתיאום מראש

80% בחינה, 20% בחנים - תאריכים נכון שכתוב בהרצאה

הגדרה:

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

א. $(R,+,0)$ הוא חבורה אבלית - החבורה החיבורית של החוג.

ב. $(R,\cdot)$ הוא חבורה למחצה.

ג. 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:

א. $(\mathbb{Z},+,\cdot)$ חוג חילופי.

ב. $(2\mathbb{Z},+,\cdot)$ חוג בלי יחידה חילופי.

ג. $(\mathbb{Z}_n,+,\cdot)$ חוג חילופי. $\mathbb{Z}_n$ שדה $\Longleftrightarrow$ n ראשוני.

ד. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ שדות.

ה. $M_n(R)$ כאשר R חוג הוא חוג לא חילופי אם $n>1$.

ו. $R[x_1,x_2,\dots]$ חוג הפולינומים ב-$\aleph_0$ משתנים. R חילופי $\Leftarrow$ $R[x_1,x_2,\dots]$ חילופי.

למה זה לא חילופי?

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

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

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

$k=ij=-ji$

$$ijk=(ij)k=kk=k^2=-1$$

$\mathbb{H}$ חוג עם חילוק.

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

אז לכל $z\in\mathbb{H}$ נקבל $z\cdot\bar{z}\in\mathbb{R}$, $z\cdot\bar{z}=0 \Leftrightarrow z=0$.

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

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

<u>הגדרה:</u>

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

<u>מימין</u> $ab=1$.

a <u>הפיך</u> אם הוא הפיך משמאל ומימין.

$R^\times=\{$ אוסף האיברים ההפיכים $\}$

$R^\times$ הוא לא חוג!

תרגיל:

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

$$\det: M_n(R)\longrightarrow R$$

הוכחה:

צריך לבדוק שהדטרמיננטה כפלית מעל R חוג חילופי. אנחנו נניח שזה נכון.

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

$$1=\det(I_n)=\det(AB)=\det(A)\cdot\det(B)\underset{R\text{ חילופי}}{=}\det(B)\cdot\det(A)$$

$\boxed{\Rightarrow}$ ניזכר במטריצה של $A\in M_n(R)$,

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

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

דוגמה:

$A\in M_n(\mathbb{Z})$ הפיכה $\Longleftrightarrow$ $\det(A)=\pm1$.

דוגמה:

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

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

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

(אכן $a^2-2b^2\neq0$ 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!

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

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

<u>דוגמה:</u>

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

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

זה חוג ביחס לחיבור והרכבה. העובדה ש- f הומומורפיזם מתבטאת בפילוג $a\cdot(b+c)=a\cdot b+a\cdot c$.

באופן דומה, אם V מרחב וקטורי גם $End(V)=\{T: V\to V \mid T \text{ ה"ל}\}$ חוג ביחס לפעולות הנ"ל.

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

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

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

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

$f,g\in End(G)$

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

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

<u>הגדרה:</u>

יהי R חוג. איבר $0\neq a\in R$ נקרא <u>מחלק אפס</u> שמאלי (ימני) אם קיים $0\neq b\in R$ כך ש- $ab=0$ ($ba=0$).

<u>הגדרה:</u>

חוג בלי מחלקי אפס נקרא <u>תחום</u> (domain). תחום חילופי נקרא תחום שלמות (integral domain).

דוגמה:

א. $\mathbb{Z}, \mathbb{Z}_p$ כש-p ראשוני - תחומי שלמות. F שדה הוא תחום שלמות.

ב. $\mathbb{Z}_{12}$ אינו תחום שלמות כי $3\cdot 4\equiv 0 \pmod{12}$. הוא גם 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 $0\neq a\in R$ מחלק אפס אז הוא לא יכול להיות הפיך. אחרת, נניח $ab=0$ ($b\neq 0$) ו-a הפיך

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

בסתירה (כי חייבים ש-$b\neq 0$ כדי ש-a יהיה מחלק אפס).

הגדרה:

יהי R חוג. חוג הפולינומים ב-n משתנים מתחלפים מסומן $R[x_1,\dots,x_n]$.

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

R חילופי $\iff$ $R[x_1,\dots,x_n]$ חילופי.

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

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

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

לכן $1-x$ אינו הפיך ב-$R[x]$.

הוכחה מלאה:
נניח בשלילה שיש הופכי
$a_0+a_1x+\dots+a_nx^n$

$(1-x)(a_0+a_1x+\dots+a_nx^n)=$
$=a_0+(a_1-a_0)x+(a_2-a_1)x^2+\dots+(a_n-a_{n-1})x^n-a_nx^{n+1}=1$
$\Rightarrow a_0=a_1=\dots=a_n=1,\ a_n=0$
אבל התוצאה לא תצא 1
וכך "יתן" סתירה

דוגמה:

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

הגדרה:

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

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

תת-חוגים

הגדרה:

יהי R חוג. תת-קבוצה $S\subseteq R$ היא <u>תת-חוג</u> (<u>subring</u>) של R אם S היא חוג ביחס לפעולות שמושרות מ-R, ומכילה את איבר היחידה של R.

$S\subseteq R$ נקראת <u>תת-חוג בלי יחידה</u> (<u>subrng</u>) אם S היא חוג בלי יחידה ביחס לפעולות שמושרות מ-R.

טענה:

$\phi\neq S\subseteq R$ היא תת-חוג בלי יחידה של R $\iff$ לכל $a,b\in S$, $a-b,ab\in S$.

דוגמה:

א. $n\mathbb{Z}$ תת-חוג בלי 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 $1_S=1_R$.

לפעמים ל-S יש יחידה אחרת:

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

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

ד. $\mathbb{H}$ $\leftarrow$ 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 בלי יחידה, ויהי $0\neq a\in R$. הוכח כי aRa הוא תת-חוג בלי יחידה של R.

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

הוכחה:

$0\in aRa$ לכן $aRa\neq\emptyset$. מהקריטריון המקוצר, יהיו $axa,aya\in aRa$.

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

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

תרגיל:

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

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

הוכחה:

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

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

$$(eae)e=ea(ee)=eae \qquad \square$$

$$R=\mathbb{Z}[x_1,\dots,x_{n^2},y_1,\dots,y_{n^2}] \subseteq F=\mathbb{Q}(x_1,\dots,x_{n^2},y_1,\dots,y_{n^2})$$

שדה הפונקציות הרציונליות

$$A=\begin{pmatrix} x_1 & \cdots & x_n \\ x_{n+1} & \cdots & x_{2n} \\ \vdots & & \vdots \\ x_{n^2-n+1} & \cdots & x_{n^2}\end{pmatrix} \qquad B=\begin{pmatrix} y_1 & \cdots & y_n \\ \vdots & & \vdots \\ y_{n^2-n+1} & \cdots & y_{n^2}\end{pmatrix} \qquad A,B\in M_n(R)\subseteq M_n(F)$$

$$p(x_1,\dots,x_{n^2},y_1,\dots,y_{n^2})=\det(AB)-\det(A)\det(B)=0$$

כי זה נכון מעל F

לכן כפולינומים ב הביטוי $\det(AB)-\det(A)\det(B)$ מתאפס ושווה 0.