פתרון תרגיל בית 1 מבוא לחוגים ומודולים
88-212 סמסטר ב' תשפ"א

שאלה 1 (רענון הגדרות)**.** נבדוק אלו תכונות נשמרות תחת תת־חוגים. יהי R חוג בלי יחידה, ויהי $S \subseteq R$ תת־חוג בלי יחידה. הוכיחו או הפריכו:

א. אם R עם יחידה, האם S עם יחידה? ולהפך?

ב. אם R חילופי, האם S חילופי? ולהפך?

ג. אם R תחום, האם S תחום? ולהפך?

ד. אם איבר x הפיך ב-R, האם הוא הפיך ב-S? ולהפך?

פתרון.

א. לא! לשאלה הראשונה אפשר לקחת $R = \mathbb{Z}$ ו-$S = 2\mathbb{Z}$ תת-חוג בלי יחידה שלו. לשאלה השנייה אפשר לקחת $R = \left\{ \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix} \right\} \subseteq M_2(\mathbb{C})$ חוג בלי יחידה ותת-חוג בלי יחידה שלו $S = \left\{ \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \right\}$.

ב. אם R חילופי אכן S חילופי גם הוא, ישירות מההגדרה. ההיפך אינו נכון; שוב ניתן לקחת $R = \left\{ \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix} \right\}$ ו-$S = \left\{ \begin{pmatrix} * & 0 \\ 0 & 0 \end{pmatrix} \right\}$.

ג. אם R תחום אז גם S הוא תחום. הכיוון ההפוך, שוב, אינו נכון, עם אותה הדוגמה. S הוא תחום כי $S \cong \mathbb{C}$, אבל R אינו תחום כי $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

ד. קודם כל צריך להניח פה ש-R עם יחידה ושגם S מכיל יחידה, אחרת אין משמעות למושג "הפיך". אם היחידה של R שונה מהיחידה של S, שני הכיוונים לא נכונים. אם S הוא תת-חוג ממש (כלומר מכיל את היחידה של R), אז כל איבר הפיך ב-S יהיה גם הפיך ב-R, אך לא להיפך.

שאלה 2. הוכיחו או הפריכו האם האובייקטים הבאים הם חוגים. במקרה שהם כן, האם הם תחומים?

א. $R = \left\{ \frac{m}{2n+1} \,\middle|\, n, m \in \mathbb{Z} \right\} \subseteq \mathbb{Q}$ עם חיבור וכפל רגילים.

ב. $R = \left\{ \frac{2n+1}{m} \,\middle|\, n \in \mathbb{Z}, m \in \mathbb{N} \right\} \subseteq \mathbb{Q}$ עם חיבור וכפל רגילים.

ג. $R = (\mathrm{End}(G), +, \circ)$ כאשר $(G, +, 0)$ היא חבורה אבלית, $\mathrm{End}(G)$ הוא אוסף האנדומורפיזמים של G (הומומורפיזמים מ-G לעצמה), הפעולה $+$ ב-R היא חיבור פונקציות המושרה מהפעולה של G והפעולה $\circ$ היא הרכבה. רמז: R הוא חוג.

ד. $R=(C[0,1],+,\circ)$ כאשר $C[0,1]$ הוא אוסף הפונקציות הממשיות הרציפות בקטע $[0,1]$, הפעולה $+$ היא חיבור פונקציות והפעולה $\circ$ היא הרכבה.

ה. $R=(C[0,1],+,\cdot)$ כאשר הפעולה $\cdot$ היא כפל פונקציות, כלומר $(f\cdot g)(x)=f(x)g(x)$.

פתרון. א. נראה כי R הוא תת-חוג של $\mathbb{Q}$. הוא לא ריק כמובן, סגור לחיסור כי

$$\frac{m}{2n+1}-\frac{m'}{2n'+1}=\frac{m\left(2n'+1\right)-m'\left(2n+1\right)}{\left(2n+1\right)\left(2n'+1\right)}=\frac{2mn'-2m'n+m-m'}{2\left(2nn'+n+n'\right)+1}\in R$$

וסגור לכפל כי

$$\frac{m}{2n+1}\cdot\frac{m'}{2n'+1}=\frac{mm'}{2\left(2nn'+n+n'\right)+1}\in R.$$

ב. זהו לא חוג, כי אין בו איבר ניטרלי לחיבור ($0\notin R$).

ג. ראיתם בהרצאה שזהו חוג.

ד. זהו לא חוג. מתקיימות כל האקסיומות של חוג, למעט פילוג מצד ימין:

$$f\circ(g+h)\neq f\circ g+f\circ h.$$

כדוגמה אפשר לקחת $g\left(x\right)=h\left(x\right)=x$ ו-$f\left(x\right)=x^2$, ואכן

$$\left(f\circ(g+h)\right)(x)=f\left(\left(g+h\right)\left(x\right)\right)=f\left(2x\right)=4x^2$$
$$\left(f\circ g+f\circ h\right)(x)=f\left(g\left(x\right)\right)+f\left(h\left(x\right)\right)=f\left(x\right)+f\left(x\right)=2x^2.$$

ה. זהו חוג. איבר האפס הוא הפונקציה $f\left(x\right)=0$, איבר היחידה הוא הפונקציה $f\left(x\right)=1$. ניתן לעבור על כל האקסיומות ולוודא שהן מתקיימות.

שאלה 3. הוכיחו שהאקסיומה של חילופיות החיבור נובעת משאר האקסיומות האחרות של חוג. כלומר, אם $(R,+,\cdot)$ מקיים ש-$(R,+,0)$ חבורה, $(R,\cdot,1)$ מונואיד ומתקיים חוק הפילוג משני הצדדים, אז בהכרח $x+y=y+x$ לכל $x,y\in R$. (רמז: $\left(1+x\right)\left(1+y\right)$).

הוכחה. נסתכל על הביטוי $\left(1+x\right)\left(1+y\right)$, ונפתח אותו באמצעות חוק הפילוג. בדרך הראשונה נפעיל פילוג מצד ימין ואז פילוג מצד שמאל:

$$\left(1+x\right)\left(1+y\right)=\left(1+x\right)1+\left(1+x\right)y=1+x+y+xy$$

ובפעם השנייה נפעיל פילוג מצד שמאל ואז פילוג מצד ימין:

$$\left(1+x\right)\left(1+y\right)=1\left(1+y\right)+x\left(1+y\right)=1+y+x+xy.$$

לכן קיבלנו שלכל $x,y\in R$ מתקיים

$$1+x+y+xy=1+y+x+xy.$$

נחבר את הנגדיים של 1 מצד שמאל ושל xy מצד ימין ונקבל

$$x+y=y+x$$

כנדרש. $\square$

שאלה 4. יהיו R,S חוגים בלי יחידה. נגדיר את המכפלה הישרה $R\times S$ עם הפעולות רכיב-רכיב.

א. הוכיחו כי $R\times S$ חוג בלי יחידה, ושאם R,S הם חוגים (עם יחידה), אז גם $R\times S$.

ב. הגדירו מבנה של חוג בלי יחידה על המכפלה הישרה $\prod_{i\in I}R_i$ למשפחה $\{R_i\}_{i\in I}$ של חוגים בלי יחידה, והוכיחו:

(i) אם R_i חילופי לכל $i\in I$, אז גם $\prod_{i\in I}R_i$ חילופי.

(ii) אם כל R_i הוא חוג עם יחידה, אז גם $\prod_{i\in I}R_i$ הוא חוג עם יחידה.

ג. נגדיר את **הסכום הישר** $\bigoplus_{i\in I}R_i$ של משפחת חוגים $\{R_i\}_{i\in I}$ להיות אוסף האיברים ב-$\prod_{i\in I}R_i$ שיש להם תומך סופי (כלומר רק מספר סופי של קואורדינטות שונות מ-0). (במקרה שבו קבוצת האינדקסים I סופית, ההגדרה מתלכדת עם זו של המכפלה הישרה).

(i) הוכיחו כי $\bigoplus_{i\in I}R_i$ הוא תת-חוג בלי יחידה של $\prod_{i\in I}R_i$.

(ii) מתי $\bigoplus_{i\in I}R_i$ הוא חוג עם יחידה?

פתרון.

א. אפשר לעבור על כל האקסיומות ולוודא, הן מתקיימות ב-$R\times S$ כי הן מתקיימות בכל רכיב. אם ב-R וב-S יש יחידה, ב-$R\times S$ איבר היחידה הוא $1_{R\times S}=(1_R,1_S)$.

ב. נכתוב כל איבר של $\prod_{i\in I}R_i$ בתור $(r_i)_{i\in I}$ כאשר $r_i\in R_i$ לכל $i\in I$. נגדיר את הפעולות רכיב-רכיב:

$$(r_i)_{i\in I}\cdot(r'_i)_{i\in I}=(r_i\cdot r'_i)_{i\in I}\qquad(r_i)_{i\in I}+(r'_i)_{i\in I}=(r_i+r'_i)_{i\in I}\,.$$

(i) נניח שכל R_i חילופי. אזי

$$(r'_i)_{i\in I}\cdot(r_i)_{i\in I}=(r'_i\cdot r_i)_{i\in I}=(r_i\cdot r'_i)_{i\in I}=(r_i)_{i\in I}\cdot(r'_i)_{i\in I}\,.$$

(ii) נניח שבכל R_i יש יחידה. אז $(1_{R_i})_{i\in I}$ הוא איבר היחידה של $\prod_{i\in I}R_i$, כי

$$(r_i)_{i\in I}\cdot(1_{R_i})_{i\in I}=(r_i\cdot 1_{R_i})_{i\in I}=(r_i)_{i\in I}$$

ובדומה מהכיוון השני.

ג.

(i) כדי להראות שהסכום הישר הוא תת-חוג בלי יחידה של המכפלה הישרה, צריך לוודא שהוא סגור לחיסור ולכפל. אבל קבוצת האינדקסים שבהן הפרש או מכפלה של שני איברים מהמכפלה הישרה שונה מאפס מוכל באיחוד קבוצות האינדקסים שבהם כל איבר בנפרד שונה מאפס. אם שני האיברים היו מהסכום הישר, זהו איחוד של שתי קבוצות סופיות, ולכן סופי.

(ii) בסכום הישר יש יחידה אם ורק אם I סופית ובכל R_i יש יחידה. מצד אחד, אם I סופית ובכל R_i יש יחידה אז הסכום הישר מזדהה עם המכפלה הישרה, ולכן אנחנו יודעים מי היחידה בו. מצד שני, אם I אינסופית אז בכל איבר של הסכום הישר יש קואורדינטה שהיא 0 (אינסוף מהן, בפרט יש אחת), ולכן באותו רכיב המכפלה תמיד תהיה 0, ולא נקבל איבר יחידה (בהנחה ש-$R_i\neq\{0\}$ לכל $i\in I$).

שאלה 5. יהי R חוג חילופי, ויהיו $x,y\in R$. הוכיחו שאם xy הפיך, אז גם x וגם y הפיכים. הפריכו זאת במקרה הלא חילופי (רמז: אנדומורפיזמים).

פתרון. נניח ש-R חילופי, ויהיו $x,y\in R$ כך ש-xy הפיך ב-R. נוכיח ש-x הפיך (ולכן גם y, כי $xy=yx$):

$$x\left(y\left(xy\right)^{-1}\right)=\left(xy\right)\left(xy\right)^{-1}=1$$

ומהחילופיות גם $\left(y\left(xy\right)^{-1}\right)x=1$. לכן x הפיך.

נראה שהטענה אינה נכונה כאשר R אינו חילופי. ניקח $R=\operatorname{End}\left(F^{\mathbb{N}}\right)$ לשדה F כלשהו, ונשתמש בשני האיברים שראינו בתרגול:

$$\begin{aligned}D\left(\left(x_1,x_2,\dots\right)\right)&=\left(x_2,x_3,\dots\right)\\U\left(\left(x_1,x_2,\dots\right)\right)&=\left(0,x_1,x_2,\dots\right)\end{aligned}$$

אזי $D\circ U=\mathrm{id}$, ולכן $D\circ U$ איבר הפיך. אבל D,U אינם הפיכים. אחרת, היינו מקבלים $U\circ D=\mathrm{id}$, אבל

$$\left(U\circ D\right)\left(\left(x_1,x_2,\dots\right)\right)=\left(0,x_2,x_3,\dots\right)$$

בסתירה.

שאלה 6. יהי R תחום. הוכיחו $\left(R[x]\right)^{\times}=R^{\times}$. כלומר לא מקבלים איברים הפיכים "חדשים" בחוג הפולינומים.

פתרון. יהי $f\left(x\right)=\sum_{i=0}^{n}a_ix^i\in R\left[x\right]$ איבר הפיך כאשר $a_n\neq 0$. לכן קיים לו איבר הופכי $f^{-1}\left(x\right)=\sum_{j=0}^{m}b_jx^j$ ($b_m\neq 0$). נקבל

$$f\left(x\right)f^{-1}\left(x\right)=\sum_{k=0}^{m+n}\left(\sum_{i+j=k}a_ib_j\right)x^k=1.$$

כיוון ש-R הוא תחום, $a_nb_m\neq 0$, ולכן החזקה הגבוהה בסכום באגף שמאל היא $a_nb_mx^{m+n}$. כיוון שהביטוי כולו שווה ל-1, בהכרח $m+n=0$, כלומר $m=n=0$, ולכן $f\left(x\right)=a_0$ ו-$g\left(x\right)=b_0$. כמו כן, $a_0b_0=b_0a_0=1$, ולכן $a_0\in R^{\times}$. זה מראה שהאיברים ההפיכים ב-$R\left[x\right]$ הם רק הפולינומים הקבועים שהמקדם שלהם הוא איבר הפיך ב-R.

שאלה 7. יהי R חוג בלי יחידה.

א. נאמר כי R בוליאני אם לכל איבר $x\in R$ מתקיים $x^2=x$. הוכיחו שאם R בוליאני, אז הוא חילופי.

ב. רשות: הוכיחו שאם לכל $x\in R$ מתקיים $x^3=x$, אז R הוא חילופי. הדרכה:

(i) הראו כי לכל $x,y\in R$, אם $xy=0$, אז $yx=0$.

(ii) הראו כי אם $x\in R$ מקיים $x^2=x$, אז $x\in Z\left(R\right)$.

(iii) הסיקו כי לכל $x\in R$, $x^2,x+x^2\in Z\left(R\right)$, ומכאן הסיקו את הדרוש.

ג. העשרה (ג'ייקובסון, 1945): אם לכל $x\in R$ קיים מספר שלם $n(x)>1$ כך ש-$x^{n(x)}=x$, אז R הוא חילופי.

פתרון. א. נחשב

$$x+y=(x+y)^2=x^2+xy+yx+y^2=x+y+xy+yx$$
$$0=xy+yx$$

נשים לב שבמקרה $x=y$ נקבל שלכל $x\in R$ מתקיים $x+x=x^2+x^2=0$, ולכן $x=-x$ לכל $x\in R$. לסיום נשים לב כי

$$xy=-yx=yx$$

ב. אציג את אחת הדרכים לפתור את השאלה. לדרך אחרת, מוזמנים להיכנס לקישור הזה. שימו לב לכל המקומות שבהם אנחנו משתמשים בתכונה של R.

(i) נניח ש-$xy=0$. לכן

$$yx=(yx)^3=y(xy)^2x=y\cdot 0\cdot x=0.$$

(ii) נניח ש-$x=x^2$, ויהי $y\in R$. מתקיים

$$x(xy-y)=x^2y-xy=xy-xy=0.$$

לפי תת-הסעיף הקודם,

$$(xy-y)x=xyx-yx=0.$$

זה מראה שמתקיים

$$(xy-yx)x=xyx-yx^2=xyx-yx=0$$

ושוב לפי תת-הסעיף הקודם מתקיים

$$x(xy-yx)=xy-xyx=0.$$

בסך הכל הראינו ש-$yx=xyx=xy$ לכל $y\in R$. לכן $x\in Z(R)$.

(iii) יהי $x\in R$. נראה ש-x^2 אידמפוטנט:

$$\left(x^2\right)^2=x^4=x^3\cdot x=x\cdot x=x^2.$$

לכן $x^2\in Z(R)$ לכל $x\in R$.
כעת נתבונן באיבר $x+x^2$. מצד אחד,

$$2\left(x+x^2\right)=x^2+2x^3+x^4=\left(x+x^2\right)^2\in Z(R).$$

מצד שני, לפי התכונה של R,

$$x+x^2=\left(x+x^2\right)^3=x^3+3x^4+3x^5+x^6=x+3x^2+3x+x^2=4\left(x+x^2\right)$$

ולכן $3\left(x+x^2\right)=0$. בסך הכל $x+x^2=3\left(x+x^2\right)-2\left(x+x^2\right)\in Z(R)$ לכל $x\in R$.
כיוון ש-$Z(R)$ תת-חוג, $x=\left(x+x^2\right)-x^2\in Z(R)$ לכל $x\in R$, ולכן R חילופי.

ג. המקור הוא Jacobson, N. "Structure Theory for Algebraic Algebras of Bounded Degree." Annals of Mathematics, Second Series, 46, no. 4 (1945): 695-707. doi:10.2307/1969205. עוד כאן https://math.stackexchange.com/questions/360958/prove-that-r-is-a-commutative-ring-if-x3-x/360968#360968, כאן http://math.stackexchange.com/a/360980 או כאן https://www-fourier.ujf-grenoble.fr/~marin/une_autre_crypto/articles_et_extraits_livres/Herstein-Wedderburn.pdf.

בהצלחה!