<u>אלגברה מופשטת 2 – תרגיל כיתה 1</u>

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

הגדרה:

חוג הוא שלשה הכוללת קבוצה ושתי פעולות בינאריות "חיבור" ו"כפל" $(R,+,\cdot)$, כך ש

1. $(R,+)$ זו חבורה אבלית. איבר היחידה מסומן ב0.
2. $(R^*,\cdot)$ זו חבורה למחצה. [$R^* = R \setminus \{0\}$] והפעולה • אסוציאטיבית.
3. מתקיים חוק הפילוג $a(b+c)=ab+ac$, $(a+b)c=ac+bc$.

חוגים מיוחדים:

- "חוג קומוטטיבי" אם $(R^*,\cdot)$ היא אבלית.
- "חוג עם יחידה" אם $(R^*,\cdot)$ היא מונואיד. במקרה זה איבר היחידה מסומן ב1.

  במונואיד איבר a הוא "הפיך מימין" אם קיים c כך ש $ac=1$ ו"הפיך משמאל" אם קיים b כך ש $ba=1$. אם איבר הוא הפיך גם מימין וגם משמאל אז יש לו הופכי יחיד מימין השווה להופכי משמאל שגם הוא יחיד, איבר כזה נקרא ההופכי של a ומסומן ע"י a^{-1}.
- "חוג עם חילוק" אם $(R^*,\cdot)$ היא חבורה. במקרה זה, ההפכי של a לפעולת הכפל מסומן ב a^{-1}.
- "שדה" אם $(R^*,\cdot)$ היא חבורה אבלית.

דוגמאות:

- $(\mathbb{Z},+,\cdot)$ הוא חוג קומוטטיבי עם יחידה.
- $(2\mathbb{Z},+,\cdot)$ הוא חוג קומוטטיבי (בלי יחידה).

- $\left(\mathbb{Z}_n,+,\cdot\right)$ הוא חוג קומוטטיבי עם יחידה. עבור n ראשוני הוא אף שדה.
- $\mathbb{R},\mathbb{C},\mathbb{Q}$ הם שדות.

תרגיל: יהי R חוג קומוטטיבי עם יחידה. הוכח כי $A\in M_n(R)$ הפיכה אם ורק אם $\det(A)\in R$ הפיכה.

הוכחה: [צריך להוכיח שהתכונות המוכרות של מטריצות מעל שדות כגון הכפליות של הדטרמיננטה והמטריצה הנלווית נכונות עבור מטריצות מעל חוגים קומוטטיביים עם יחידה. אולם, נניח שהעבודה הזו כבר נעשתה] $\Leftarrow$ נניח שקיימת B כך ש $AB=BA=I$. אזי

$1=\det(I)=\det(AB)=\det(A)\det(B)$ וגם

$1=\det(I)=\det(BA)=\det(B)\det(A)$ ולכן $\det(A)$ הפיכה.

$\Rightarrow$

$$A\cdot adj(A)=\det(A)\cdot I\rightarrow\left(A\cdot adj(A)\right)\left(\det\left(A\right)\right)^{-1}=I$$

$$A\cdot\left(adj\left(A\right)\det\left(A\right)^{-1}\right)=I$$

באותו אופן ניתן להוכיח ש A הפיכה משמאל.

דוגמא: נסמן $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}:a,b\in\mathbb{Q}\}$. זהו שדה. רוב הבדיקות הן קלות. נראה רק סגירות להפכי

$$\frac{1}{a+b\sqrt{2}}=\frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2+2b^2}=\frac{a}{a^2+2b^2}-\frac{b}{a^2+2b^2}\sqrt{2}.$$

$\mathbb{Z}[\sqrt{2}]$ לעומת זאת איננו שדה, משום ש $\frac{1}{2}\notin\mathbb{Z}[\sqrt{2}]$.

תרגיל: הראה כי ישנם אינסוף מספרים הפיכים ב $\mathbb{Z}[\sqrt{2}]$.

הוכחה: $(3+2\sqrt{2})(3-2\sqrt{2})=1$ ולכן $3+2\sqrt{2}$ ו $3-2\sqrt{2}$ הם הפיכים. מכיוון ש $3+2\sqrt{2}>1$, קבוצת החזקות השלמות שלו היא אינסופית, ולכל חזקה $(3+2\sqrt{2})^n$ הוא מספר הפיך משום ש $(3+2\sqrt{2})^n(3-2\sqrt{2})^n=1$. משמע, ישנם אינסוף הפיכים.

דוגמא: $\mathbb{Q}[i]$ הוא שדה. $\mathbb{Z}[i]$ הוא חוג קומוטטיבי עם יחידה שהאיברים ההפיכים היחידים בו הם $\pm 1, \pm i$.

דוגמא: יהיה V מרחב וקטורי מעל שדה F. נסמן ב $End(V)$ את מרחב ההעתקות הליניאריות $\varphi : V \to V$. זהו חוג עם פעולות חיבור והרכבה, כאשר האפס זו פונקציית האפס $\varphi \equiv 0$ והיחידה היא פונקציית הזהות $\varphi = id$.

ניקח את המרחב הוקטורי $V = F^{\mathbb{N}} = \{(x_1, x_2, \ldots) : x_n \in F \forall n \in \mathbb{N}\}$. ונביט בשתי ההעתקות $U((x_1, x_2, \ldots)) = (0, x_1, x_2, \ldots)$ ו $D((x_1, x_2, \ldots)) = (x_2, x_3, \ldots)$.

במקרה זה $D \circ U = id$ אולם $U \circ D \neq id$ ולכן D הפיכה מימין אך לא משמאל.

הגדרות:

1. $a \neq 0$ נקרא "מחלק אפס" שמאלי (ימני) אם קיים b כך ש $ab = 0$ ($ba = 0$).
2. חוג ללא מחלקי אפס נקרא "תחום". תחום קומוטטיבי נקרא "תחום שלמות".

דוגמאות:

1. $\mathbb{Z}$ הוא תחום שלמות.
2. $\mathbb{Z}_6$ איננו תחום משום שהוא מכיל מחלקי אפס 2 ו3.
3. לכל חוג קומוטטיבי עם יחידה R ו $n > 1$, $M_n(R)$ איננו תחום.
4. חוג עם חילוק הוא תמיד תחום.

הגדרה:

בהינתן חוג קומוטטיבי עם יחידה R נסמן את חוג הפולינומים ב $R[x]$. זהו גם כן חוג קומוטטיבי עם יחידה.אם R תחום שלמות אז גם $R[x]$ תחום שלמות. אולם, אם R שדה

אין זה אומר ש$R[x]$ שדה, משום שהאיבר $1-x$ איננו הפיך. [לפי פיתוח לטור טיילור,

$\frac{1}{1-x}=1+x+x^2+\cdots$. אולם הטור שמימין למשוואה איננו סופי ולכן אינו פולינום].

נגדיר לעומת זאת את חוג טורי טיילור $R[[x]]$. בחוג זה $1-x$ הוא אכן הפיך. אולם, x עצמו איננו הפיך, ולכן זה עדיין לא שדה.

תרגיל: הוכיחו כי $1+2x$ הפיך ב $\mathbb{Z}_4[x]$.

פיתרון: $(1+2x)(1-2x)=1-4x^2=1$.

הגדרה: תת-חוג $R\supseteq S$ הוא תת-קבוצה שמהווה חוג ביחס לפעולות המקוריות.

משפט: $S\neq\phi$ תת-חוג של R אם ורק אם לכל $a,b\in S$ מתקיים $a\cdot b,a-b\in S$.

דוגמאות:

1. לכל $n\in\mathbb{N}$, $n\mathbb{Z}$ הוא תת-חוג של $\mathbb{Z}$.
2. אם S תת-חוג של R אז $M_n(S)$ תת-חוג של $M_n(R)$.
3. תת-הקבוצה $A=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}:a\in\mathbb{R}\right\}$ של $M_2(\mathbb{R})$ היא תת-חוג, אע"פ שהיחידה בA היא $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ולא $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ [כלומר תת-החוג, גם אם יש לו יחידה, לא בהכרח יורש אותה מהחוג הגדול]. אולם, באופן כללי, אם היחידה של R שייכת גם ל S אז היא איבר היחידה ב S.
4. אם $k\mid n$ אזי $k\mathbb{Z}_n$ הוא תת-חוג של $\mathbb{Z}_n$.

תרגיל:

1. יהי חוג R (לאו דוקא עם יחידה) ויהי $0\neq q\in R$. הוכח כי qRq תת-חוג של R.
2. נניח ש $q^2=q$ [איבר כזה נקרא אידמפוטנט]. הוכח כי q הוא היחידה ב qRq.

פתרון

1. יהיו $a,b\in qRq$ ז"א קיימים $t,s\in R$ כך ש $a=qtq,b=qsq$ מפעולת האסוציאטיביות נקבל ש $a-b=qtq-qsq=q\left(t-s\right)q$ ומכיוון ש $t-s\in R$ נקבל ש $q\left(t-s\right)q\in qRq$ ז"א $a-b\in qRq$. $a\cdot b=qtqqsq$ מכיוון ש $tqqs\in R$ נקבל ש $a\cdot b=qtqqsq\in qRq$.
2. יהי $a\in qRq$ ז"א קיים $t\in R$ כך ש $a=qtq$.
$aq=qtq^2=qtq=a,qa=q^2tq=qtq=a$.

הגדרות:

יהי חוג R. המרכז שלו מסומן ב $Z(R)=\{y\in R: xy=yx\forall x\in R\}$. המרכז של תת-קבוצה $S\subseteq R$ הוא $C_R(S)=\{y\in R: xy=yx\forall x\in S\}$.

דוגמא: אם R חוג עם יחידה אזי $Z(M_n(R))=Z(R)\cdot I$.

תכונות:

1. $Z(R)$ תת-חוג קומוטטיבי של R.
2. R קומוטטיבי אם ורק אם $R=Z(R)$.
3. $C_R(S)$ תת-חוג של R.
4. אם R קומוטטיבי אז $C_R(S)=R$.
5. $S\subseteq C_R(C_R(S))$.
6. $C_R(S)=C_R(C_R(C_R(S)))$.