הגדרה: חוג בלי יחידה: כמו חוג, אבל לא דורשים את הקיום של 1 (אומרים פחות, חג)

הגדרה: תת חוג - R חוג. $S \subseteq R$ תת קבוצה ה"י תת חוג אם:

1) סגורה לחיסור

2) סגורה לכפל

3) $1 \in S$

הגדרה: תת חוג בלי יחידה - אם (1), (2) מתקיימים

דוגמאות:

1) $R = \mathbb{Z}$, $S = n\mathbb{Z}$, אז' S תת חוג בלי יחידה. תת חוג $\Leftrightarrow n=1$

אבחנה: אלה כל תתי החוגים בלי יחידה של $\mathbb{Z}$

2) $R = M_2(\mathbb{R})$, $S = \{\begin{pmatrix} a & a \\ b & b \end{pmatrix} : a,b \in \mathbb{R}\}$

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix} - \begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} a-c & a-c \\ b-d & b-d \end{pmatrix}$$

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} a(c+d) & a(c+d) \\ b(c+d) & b(c+d) \end{pmatrix}$$

יהי $\begin{pmatrix} x & x \\ y & y \end{pmatrix} \in S$ כאשר $x+y=1$. לכל $\begin{pmatrix} a & a \\ b & b \end{pmatrix}$ מתקיים

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} x & x \\ y & y \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix}$$

לכן $\begin{pmatrix} x & x \\ y & y \end{pmatrix}$ יחידה מימין

הוא לא יחידה משמאל כי $\begin{pmatrix} x & x \\ y & y \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 2x & 2x \\ 2y & 2y \end{pmatrix}$

בדרך כלל לא $\begin{pmatrix} 2 & 2 \\ 0 & 0 \end{pmatrix}$

הגדרה: הומומורפיזם של חוגים הוא העתקה $f: R \to S$ כך ש:

1) $f(a+b) = f(a) + f(b)$

2) $f(ab) = f(a)f(b)$

3) $f(1_R) = 1_S$

הגדרה: הומומורפיזם של חוג בלי יחידה - לא קורסים (3)

דוגמאות:

1) R חוג, S תת חוג (בלי יחידה) שאינה תת חוג. ההכלה $f: S \hookrightarrow R$ היא הומו' של חבורות

2) R חוג כלשהו. קיים הומו' יחיד (של חוגים) $f: \mathbb{Z} \to R$.

$f(1) = 1_R$, $f(n) = \underbrace{1_R + \ldots + 1_R}_{n \text{ פעמים}}$

נסמן $n_R = f(n)$

טענה:

$f: R \to S$ הומומורפיזם של חוגים בלי יחידה (חב"י) אזי:

1) $f(0_R) = 0_S$

2) $f(-a) = -f(a)$ לכל $a \in R$

הוכחה:

$f: (R,+) \to (S,+)$ הומו' של חבורות

3) $f: \mathbb{Z} \to \mathbb{Z}_n$ $f(a) = [a]$

הגדרה: המאפיין של R הינו $n \in \mathbb{N}$ המינימלי כך ש $n_R = 0_R$. אם אין n כזה, אומרים $\text{char} R = 0$

$\text{char}\, \mathbb{Z}_n = n$

4) R חוג חילופי. יהי $b \in R$. הומו' ההצבה $ev_b: R[x] \to R$

$a_n x^n + \ldots + a_1 x + a_0 \longmapsto a_n b^n + \ldots + a_1 b + a_0$

אם R לא חילופי זה עלול לא לשמור כפל כי:

$ev_b(ax)\, ev_b(ax) = abab \overset{?}{=} a^2 b^2 = ev_b(a^2 x^2)$

5) $f: R \to S$ הומו' של חוגים. $M_n(f): M_n(R) \to M_n(S)$

$a_{ij} \in R$ $\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \longmapsto \begin{pmatrix} f(a_{11}) & \cdots & f(a_{1n}) \\ \vdots & & \\ f(a_{n1}) & \cdots & f(a_{nn}) \end{pmatrix}$

$$(AB)_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj}$$

$$(M_nf(A)M_nf(B))_{ij}=\sum_{k=1}^{n}f(a_{ik})f(b_{kj})=f\left(\sum_{k=1}^{n}a_{ik}b_{kj}\right)=M_nf(AB)_{ij}$$

טענה:

$f:\mathbb{Z}\to\mathbb{Z}_p$, p ראשוני (שדה $\mathbb{Z}_p$), $M_n(f):M_n(\mathbb{Z})\to M_n(\mathbb{Z}_p)$

אזי $M_n(f)(A)$ הפיכה $\iff p\nmid \det A$

6) אין הומ׳ של חוגים $f:\mathbb{Z}_n\to\mathbb{Z}$

הוכחה: נניח שיש $f([1])=1$, $f([n])=f([1]+\dots+[1])=1+\dots+1=n$, $f([0])=0$

f לא מוגדר היטב

7) $f:R\to S$ הומ׳ של חוגים בלי יחידה $f(a)=0_S$ ההומ׳ הטריוויאלי

8) $f:\mathbb{C}\to\mathbb{C}$ הצמדה, $f(a+bi)=a-bi$

9) R,S חוגים $f(r,s)=r$ $f:R\times S\to R$

$g(r,s)=s$ $g:R\times S\to S$

10) לא בהכרח קיים הומ׳ $f:R\to R\times S$

הוכחה: ההרכבה של הומ׳ של חוגים היא הומ׳ של חוגים $R\to R\times S\xrightarrow{g}S$

11) ההומ׳ האלכסוני $f(a)=(a,\dots,a)$ $f:R\to R^n=R\times\dots\times R$

12) $f:R\to R\times S$ $f(r)=(r,0)$

זה הומ׳ של חוגים בלי יחידה

13) $f_1:R\to S_1$, $f_2:R\to S_2$

$f:R\to S_1\times S_2$ $f(a)=(f_1(a),f_2(a))$

הגדרה: הומו $f:R\to S$ נקרא איזומורפיזם אם הוא חח"ע ועל

תרגיל: $f^{-1}:S\to R$ גם איזו'

הגדרה: יהי $I\subseteq R$ תת חוג בלי יחידה. I נקרא אידיאל שמאלי אם $ra\in I$ לכל $r\in R,\ a\in I$

I נקרא אידיאל ימני אם $ar\in I$ לכל $r\in R,\ a\in I$

I נקרא אידיאל דו-צדדי אם I אידיאל ימני ושמאלי

טענה:

אם R חילופי, אז אידיאל ימני $\iff$ אידיאל שמאלי

רעיון: אידיאלים $\leftrightarrow$ תת חבורות נורמליות

טענה:

יהי $f:R\to S$ הומו' של חוגים (או חוגים בלי יחידה)

הגרעין $\ker f=\{r\in R: f(r)=0_S\}$ הוא אידיאל דו צדדי

הוכחה:

$(a\in\ker f)$ $(r\in R)$

$ra\in\ker f \Leftarrow f(ra)=f(r)f(a)=f(r)0_S=0_S$

$ar\in\ker f \Leftarrow f(ar)=0_S f(r)=0_S$

הגדרה: יהי R חוג, $I\subseteq R$ אידיאל דו צדדי. נגדיר יחס על R: $x,y\in R$

$x-y\in I \iff x\sim y$

זה יחס שקילות. (זה בדיוק היחס של החבורה $(R,+)$ שמגדיר את המחלקות של I)

תהי R/I הקבוצה של מחלקות השקילות

הגדרה: נסמן $a+I\in R/I$ את המחלקה של $a\in R$

נגדיר חיבור וכפל של מחלקות שקילות

$$(a+I)+(b+I)=(a+b)+I$$

$$(a+I)(b+I)=ab+I$$

הערה:

הפעולות מוגדרות היטב, ו-R/I עם הפעולות האלה היא חוג

הוכחה:

$a_1+I=a_2+I$, $b_1+I=b_2+I$ (שני נציגים למחלקה)

$$a_2=a_1+c_1 \qquad b_2=a_2+c_2 \qquad (c_1,c_2\in I)$$

מחילופיות החיבור:

$$a_2+b_2-(a_1+b_1)=(a_2-a_1)+(b_2-b_1)=c_1+c_2\in I$$

לכן

$$(a_2+b_2)+I=(a_1+b_1)+I$$

כמו כן,

$$a_2b_2=(a_1+c_1)(b_1+c_2)=a_1b_1+\underbrace{c_1b_1+a_1c_2+c_1c_2}_{\text{שייך ל-}I\text{ כי }I\text{ אידיאל דו צדדי}} \Rightarrow a_1b_1+I=a_2b_2+I$$

דוגמא:

האידיאלים של החוג $\mathbb{Z}$ הם $n\mathbb{Z}$ לכל $n\geq 0$

$$R/I=\mathbb{Z}_n \Leftarrow I=n\mathbb{Z},\ R=\mathbb{Z}$$

הערה:

יהי R חוג, I אידיאל. אזי $I=R \Leftrightarrow 1\in I$

הוכחה:

($\Leftarrow$) ברור. ($\Rightarrow$) $1\in I$ אז I מכיל כל איבר ב-R

דוגמא:

R חוג, $R, \{0_R\}$ אידיאלים דו צדדיים

הערה:

I מכיל איבר הפיך של R $\Leftrightarrow I=R$

הערה:

יהי $f:R\to S$ הומו' של חוגים. יהי $s\in f(R)$. יהי $r\in R$ כך ש $f(r)=s$. אזי:

$$f^{-1}(s)=r+(\ker f)$$

הוכחה:

$$a\in r+(\ker f) \iff a-r\in \ker f \iff f(a-r)=0_S \iff f(a)=f(r) \iff a\in f^{-1}(S)$$

משפט האיזומורפיזם הראשון:

יהי $f:R\to S$ הומו' של חוגים. אזי קיים איזו' $R/(\ker f) \xrightarrow{\sim} f(S)$

$$\left(r+(\ker f) \longmapsto f(r)\right)$$