הרצאה 5

ראינו בפעם שעברה כי

$$\mathbb{Z}[x]/(x^2) = \{a_0 + a_1x + \{\text{איברים ממעלה גבוהה יותר}\} \mid a_0, a_1 \in \mathbb{Z}\}$$

תזכורת: R חוג חילופי, $a\in R$, מסמנים $(a) = aR = Ra$.

תזכורת: שלמים של גאוס:

$$\mathbb{Z}[i] = \{a+bi \mid a,b\in\mathbb{Z}\}$$

איך נראה $\mathbb{Z}[x]/(x^2+1)$.

<u>טענה</u> $\mathbb{Z}[x]/(x^2+1) \simeq \mathbb{Z}[i]$

<u>הוכחה</u> נגדיר הומומורפיזם של חוגים

$$f: \mathbb{Z}[x] \longrightarrow \mathbb{Z}[i]$$

$$f(a_0 + a_1x + \dots + a_nx^n) = a_0 + a_1 i + a_2 i^2 + \dots + a_n i^n$$

אז

$$i^2 = -1$$
$$i^3 = -i$$
$$i^4 = 1$$

$i^a = i^b$ כאשר $a \equiv b \mod 4$

לכן $f(a_0 + \dots + a_nx^n) \in \mathbb{Z}[i]$.

f הינו מקרה פרטי של הומ' הצבה. לכן הומ'.

ברור כי f על, ולכן

$$f(a+bx) = a+bi$$

לכן, לפי משפט האיזו' הראשון $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(\ker f)$

גר-

טענה $\ker f = (x^2+1)$.

גר- הוכחה יהי $g(x)\in\mathbb{Z}[x]$. אם $g(x)\in(x^2+1)$, אזי

$$g(x) = (x^2+1)h(x)$$

$$f(g) = (i^2+1)f(h) = 0\cdot f(h) = 0$$

לכן $(x^2+1)\subseteq\ker f \Leftarrow g\in\ker f$.

בכיוון השני, נניח $g\in\ker f$. נחלק את g ב- (x^2+1) עם שארית (אפשרי לעשות את החילוק ולהישאר בתוך $\mathbb{Z}[x]$ כיוון ש- x^2+1 הינו פולינום מתוקן (המקדם העליון הינו 1). נקבל:

$$g(x) = (x^2+1)h(x) + r(x)$$

כאשר $\deg r < \deg(x^2+1)=2$

$$g(x) = (x^2+1)h(x) + a + bx$$

עבור $a,b\in\mathbb{Z}$.

$$f(g) = a+bi$$

אך הנחנו $g\in(x^2+1) \Leftarrow r(x)=0 \Leftarrow a=b=0 \Leftarrow g\in\ker f$.

ולכן $\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2+1)$

<u>תזכורת</u> יהי $f:R\to S$ הומ' של חוגים בלי יחידה.

אזי: 1) אם $I\subseteq S$ הינו אידיאל שמאלי/ימני/דו-צדדי, אזי $f^{-1}(I)=\{r\in R: f(r)\in I\}\subseteq R$ גם אידיאל שמאלי/ימני/דו-צדדי.

2) אם $S'\subseteq S$ תת-חוג-בלי-יחידה, אזי $f^{-1}(S')\subseteq R$ גם תת-חב"י,
(אם $f:R\to S$ הומ' של חוגים, אזי המקור של תת-חוג הינו תת-חוג).

3) אם $R'\subseteq R$ תת-חב"י, אזי $f(R')\subseteq S$
תת-חב"י (אם f הומ' של חוגים, $R'\subseteq R$ תת-חוג,
אזי $f(R')\subseteq S$ תת-חוג).

4) אם f <u>על</u>, ואם $I\subseteq R$ אידיאל שמאלי/ימני/דו-צדדי, אזי $f(I)\subseteq S$ גם אידיאל שמאלי/ימני/דו-צדדי.

הערה: אם f לא על, אזי הטענה 4) לא נכונה.
לדוגמא, ניקח $f:\mathbb{Z}\to\mathbb{Q}$ הומ' ההכלה, $I=2\mathbb{Z}$, $f(I)$ לא אידיאל של $\mathbb{Q}$.
(כי $2\in f(I)$, אך $\frac{3}{2}\cdot 2=3\notin f(I)$).

<u>דוגמא של הוכחה</u> 4) יהי I אידיאל שמאלי, f על.

אנחנו טוענים כי $f(I)$ הינה אידיאל שמאלי של S.

א) סגירות לחיבור: יהיו $s_1,s_2\in f(I)$. אזי קיימים $r_1,r_2\in I$ כך ש- $f(r_1)=s_1$, $f(r_2)=s_2$. אזי

$$f(r_1+r_2) \underset{f \text{ הומו׳}}{=} s_1+s_2$$

אך I סגור לחיבור, לכן $r_1+r_2\in I \Rightarrow s_1+s_2\in f(I)$.

ב) סגירות לכפל אם איברים של S.

יהיו $s_1\in f(I)$, $s\in S$. אזי קיימים $r_1\in I$, $f(r_1)=s_1$.

גם f על, לכן קיים $r\in R$ כך ש- $s=f(r)$.

לכן

$$f(\underbrace{rr_1}_{\in I}) \underset{f \text{ הומו׳}}{=} ss_1$$

כי I אידיאל שמאלי

לכן $ss_1\in f(I)$. לכן $f(I)$ אידיאל שמאלי של S.

<u>הגדרה</u> (משפט האיזו׳ הרביעי). יהי R חוג בלי יחידה. יהי $I\triangleleft R$ אידיאל. אזי יש

הגדרה

{אידיאלים שמאליים/ימניים/ דו-צדדיים/ תת-חבורות/ תת-חוגים של R שמכילים את I.} $\longleftrightarrow$ {אידיאלים שמאליים/ ימניים/ דו-צדדיים/ תת-חבורות/ תת-חוגים של R/I}

ויוניטליים אם R חוג

<u>הוכחה</u> נתבונן בהומו' הטבעי $f: R \to R/I$
ההומו' הזה הינו על. $f(r) = r+I$

זה תמיד הומו' של חוגים בלי יחידה. אם R חוג (ולכן R/I חוג), אזי זה הומו' של חוגים.

ההתאמה הינה

$$K \longmapsto f(K)$$
$$f^{-1}(J) \longleftarrow J$$

צריך <u>להוכיח</u> ששתי ההעתקות האלה הפכיות

כי של כיוון א) יהי K אידיאל/ תת-חוג של R,
נניח $I \subseteq K$.

צריך להוכיח $f^{-1}(f(K)) = K$. אכן, ברור כי
$f^{-1}(f(K)) \supseteq K$.

יהי $r \in f^{-1}(f(K))$. אזי $f(r) \in f(K)$.
לכן קיים $k \in K$ כך ש- $f(r) = f(k)$,

כלומר $r+I=k+I$ $\Leftarrow$ $r-k\in \underbrace{I\subseteq K}_{\text{הנחה}}$. לכן

לכן, $r=\underbrace{(r-k)}_{\in K}+\underbrace{k}_{\in K}\in K$ $\quad f^{-1}(f(K))=K$

<u>ב)</u> יהי J אידיאל/תת-חוג של R/I. צריך להוכיח $f(f^{-1}(J))=J$.

ברור מן ההגדרה כי $f(f^{-1}(J))\subseteq J$.

מצד שני יהי $r+I\in J$. אזי

$$r\in f^{-1}(J)$$

$$r+I=f(r)\in f(f^{-1}(J))$$

ולכן $f(f^{-1}(J))=J$ וקיבלנו את הדרוש.

<u>אבחנה</u> ההתאמה שומרת הכלה.

<u>הגדרה</u> חוג R נקרא פשוט אם אין לו אידיאלים דו-צדדיים מלבד $R,(0)$.

<u>טענה</u> יהי R חוג חילופי. אזי R פשוט אם ורק אם R שדה.

<u>הוכחה</u> $\Leftarrow$) נניח R פשוט. יהי $0\neq a\in R$. אזי

R חילופי $\Leftarrow$ $(a)\neq(0)$ אידיאל דו-צדדי!

R פשוט $\Leftarrow$ $(a)=R$ $\Leftarrow$ $1\in(a)$ $\Leftarrow$ קיים

$b\in R$ כך ש- $ab=ba=1$, לכן R שדה.

($\Leftarrow$) נניח R שדה. יהי $I \triangleleft R$ אידיאל
לא אפסי. יהי $0\neq a\in I$. לכן,
$1=aa^{-1}\in I$ $\Leftarrow$ לכל $r\in R$,
$r=r\cdot 1\in I$

ולכן $I=R$, ולכן R פשוט.

<u>הגדרה</u> יהי R חוג. איבר $a\in R$ נקרא הפיך
אם קיים $b\in R$ כך ש- $ab=ba=1$.

<u>הגדרה</u> חוג R נקרא חוג עם חילוק אם כל
איבר לא אפסי הינו הפיך.

דוגמאות של חוגים פשוטים:

1) כל שדה.

2) F שדה. $R=M_n(F)$.

R פשוט, כי הוכחנו בתרגילי הבית
שכל אידיאל דו-צדדי של R הינו מן הצורה
$M_n(I)$ כאשר $I \triangleleft F$ $\Leftarrow$ $I=F$, $I=(0)$

נשים לב כי ב- $M_n(F)$ יש אידיאלים
שמאליים/ימניים לא-טריוויאליים. כן, לא דו-צדדיים

משפט (Wedderburn) יהי R חוג פשוט,
ונניח שאין לו שרשרת יורדת אינסופית של
אידיאלים שמאליים. אזי קיימים חוג עם
חילוק D, ומספר טבעי n, כך ש- $R \simeq M_n(D)$.

נוכיח בהמשך.

תוצאה של ההתאמה יהי R חוג חילופי. יהי
$I \triangleleft R$ אידיאל. אזי I מקסימלי $\iff$ R/I שדה.

הוכחה R/I שדה $\overset{\text{הטענה הקודמת}}{\iff}$ האידיאלים היחידים של
R/I הם (0) ו- R/I

$\overset{\text{ההתאמה}}{\iff}$ האידיאלים היחידים של R שמכילים
את I הם:
$f^{-1}(R/I) = R$
$f^{-1}(0_{R/I}) = I$

$\iff$ $I \triangleleft R$ מקסימלי.

הגדרה יהי R חוג. איבר $0 \neq a \in R$ נקרא מחלק
אפס שמאלי אם קיים $0 \neq b \in R$ כך ש- $ab = 0$.
בהתאמה, a מחלק אפס ימני אם קיים $b \neq 0$ כך ש-
$ba = 0$.

הגדרה איבר $0 \neq a \in R$ נקרא רגולרי שמאלי/ימני
אם הוא לא מחלק אפס שמאלי/ימני.

דוגמא $R = \mathbb{Z}/6\mathbb{Z}$

$$[2] \cdot [3] = [0]$$

לכן $[2],[3]$ מחלקי אפס.

טענה יהי $a \in R$ רגולרי שמאלי, ויהיו $b,c \in R$
כך ש- $ab=ac$. אזי $b=c$.
(בהתאמה, אם a רגולרי ימני, $b=c \Leftarrow ba=ca$.)

הוכחה $0 = ab - ac = a(b-c) \Leftarrow ab=ac$.

a רגולרי שמאלי $b=c \Leftarrow b-c=0 \Leftarrow$.

הגדרה תחום שלמות הינו חוג **חילופי** ללא
מחלקי אפס. במילים אחרות, חוג חילופי R
הינו תחום שלמות אם ורק אם $\Leftarrow ab=0$
$a=0$ או $b=0$.

דוגמא $\mathbb{Z}$ תחום שלמות.

$\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$ תחום שלמות (כי זה תת-חוג
של השדה $\mathbb{C}$)

אבל $\mathbb{Z}[x]/(x^2)$ לא תחום שלמות כי

$$(x+(x^2))(x+(x^2)) = 0_{\mathbb{Z}[x]/(x^2)}.$$

הגדרה יהי R חוג חילופי. אידאל $I \triangleleft R$ נקרא ראשוני אם לכל $a,b\in R$:

$$ab\in I \iff a\in I \text{ או } b\in I.$$

טענה יהי R חוג חילופי. אזי R תחום שלמות $\iff$ האידאל (0) הינו ראשוני.