הרצאה 7

תזכורת מלפני החג: חוג חילופי R נקרא תחום שלמות אם אין מחלקי אפס: $ab=0 \Rightarrow a=0$ או $b=0$.

R חוג חילופי. אידיאל $I \trianglelefteq R$ הינו תת-קבוצה

סגורה לחיבור $a,b\in I \Rightarrow a+b\in I$.

סגורה לכפל עם כל איבר של R.

$a\in I$, $r\in R$ $\Rightarrow$ $ra\in I$

האידיאל הראשי הנוצר על ידי $a\in R$ הינו

$$Ra=(a)=\{ra : r\in R\}.$$

הגדרה תחום אוקלידי הינו תחום שלמות R כך שקיימת נורמה $N: R\to \mathbb{N}\cup\{0\}$

כך ש: 1) $N(0)=0$.

2) לכל $a,b\in R$ כך ש- $b\neq 0$ קיימים $q,r\in R$ כך ש:

א. $a=qb+r$

ב. $r=0$ או $N(r)<N(b)$.

<u>דוגמאות</u> 1) כל שדה F הינו תחום אוקלידי, $N(a)=0,\ \forall a\in R$.

אם $a,b\in F$, $b\neq 0$ $\Leftarrow$ $q=ab^{-1}$, $r=0$.

2) $R=\mathbb{Z}$ $\quad N(a)=\underbrace{|a|}_{\text{הערך המוחלט הרגיל}}$

למדנו אלגוריתם אוקלידס לחילוק עם שארית בבית ספר יסודי.

3) $R=F[x]$ לכל שדה F. $\quad N(P)=\deg P$

$N(a_nx^n+a_{n-1}x^{n-1}+\dots+a_0)=n$.

4) $R=\mathbb{Z}[i]$ $=\{a+bi : a,b\in\mathbb{Z}\}\subseteq\mathbb{C}$ השלמים של גאוס.

יהי $\alpha\in\mathbb{Z}[i]$. $\quad \alpha=|\alpha|^2=\alpha\bar{\alpha}$

$N(a+bi)=(a+bi)(a-bi)=a^2+b^2\in\mathbb{N}\cup\{0\}$.

הנורמה הינה כפלית: $N(\alpha\beta)=N(\alpha)N(\beta)$

לכל $\alpha,\beta\in\mathbb{Z}[i]$.

יהיו $\alpha,\beta\in\mathbb{Z}[i]$, נניח $\beta\neq 0$. אין מחלקים?

יהי $\gamma=\frac{\alpha}{\beta}\in\mathbb{C}$. נבחר שלמים

$m,n\in\mathbb{Z}$ כך ש-

$$|m-\mathrm{Re}\,\gamma|\le\frac{1}{2}$$
$$|n-\mathrm{Im}\,\gamma|\le\frac{1}{2}$$

יהי $q=m+ni\in R=\mathbb{Z}[i]$. נגדיר $r=\alpha-\beta q\in\mathbb{Z}[i]$.

צריך להוכיח כי $N(r)<N(\beta)$

(במקרה הזה, $\beta\neq 0 \Leftarrow N(\beta)\neq 0$).

$$|\gamma-q|^2\le\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2=\frac{1}{2}$$

$$|\beta\gamma-\beta q|^2=|\alpha-\beta q|^2=N(r)=N(\beta)|\gamma-q|^2\le \frac{1}{2}N(\beta)<N(\beta).$$

<u>טענה</u> כל תחום אוקלידי הינו תחום ראשי.

<u>הוכחה</u> יהי R תחום אוקלידי, יהי $I\triangleleft R$ אידיאל.

אם $I=(0)$, ברור שהוא ראשי.

נניח $I\neq(0)$, יהי $d\in I$ איבר לא-אפסי

בעל נורמה מינימלית (בין האיברים הלא-אפסיים של I).

אני טוען כי $I=(d)$.

$(d)\subseteq I \Leftarrow d\in I$.

יהי $a\in I$. קיימים q,r כך ש-

$a=qd+r$, וגם $N(r)<N(d)$ או $r=0$.

אך $r=\underbrace{a}_{a\in I}-\underbrace{qd}_{\in I}\in I$. אם $r\neq 0$, אזי

$N(r)<N(d)$ בסתירה למינימליות של $N(d)$.

אז בהכרח $a\in(d) \Leftarrow a=qd \Leftarrow r=0$.

לכן $I\subseteq(d)$.

<u>מסקנה</u> החוג $\mathbb{Z}[x]$ אינו תחום אוקלידי.

<u>הוכחה</u> הוכחנו כי $\mathbb{Z}[x]$ אינו תחום ראשי!

<u>הגדרה</u> יהי R חוג חילופי.

א) $a\in R$ נקרא הפיך אם קיים $b\in R$ כך ש- $ab=1=ba$.

ב) $a\in R$ נקרא אי-פריק אם $\Leftarrow a=bc$ b הפיך או c הפיך.

$a\neq 0$
a לא הפיך

ג) $a\in R$ נקרא ראשוני אם (a) הינו

$a\neq 0$
a לא הפיך

אידאל ראשוני $\iff$ $bc\in(a)$, אזי $b\in(a)$ או $c\in(a)$.

הגדרה: $a,b\in R$. אומרים כי $a|b$ (a מחלק את b) אם קיים c כך ש- $ac=b$ ($\iff b\in(a)$).

כלומר, $a\in R$ ראשוני אם $a|bc \Rightarrow a|b$ או $a|c$.

ב) $a,b\in R$ נקראים חברים אם קיים $u\in R$ הפיך כך ש- $a=bu$.

טענה: יהי R תחום שלמות, יהי $a\in R$ ראשוני. אזי a אי-פריק.

הוכחה: לפי ההנחה, (a) ראשוני, יהי $a=bc$.
אזי $bc\in(a) \Rightarrow b\in(a)$ או $c\in(a)$. בלי הגבלת הכלליות נניח $c\in(a)$. אזי $c=ra$.

קיבלנו $a = bc = bra$

$$a - bra = (1-br)a = 0$$

$a \neq 0$, R תחום שלמות $\Leftarrow$ $1-br=0$ $\Leftarrow$

$br=1 \Leftarrow b$ הפיך.

<u>דוגמא</u> איבר אי-פריק לא בהכרח ראשוני!

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5} : a,b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

יהי $\alpha = a + b\sqrt{-5}$. נגדיר נורמה

$$N(\alpha) = |\alpha|^2 = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2 + 5b^2.$$

ברור כי $N(\alpha\beta) = N(\alpha)N(\beta)$ לכל $\alpha,\beta \in R$.

יהי $\alpha = 2 + \sqrt{-5}$, אני טוען כי α אי-פריק. אכן, יהי $\alpha = \beta\gamma$. אזי

$$N(\beta)N(\gamma) = N(\alpha) = 2^2 + 5\cdot 1^2 = 9$$

נשים לב שלא ניתן להגיע $3 = a^2 + 5b^2$.

אז אין $\beta \in R$ עם $N(\beta)=3$. אז בהכרח

$N(\beta)=9$, $N(\gamma)=1$ ולכן הפיך אבל

γ הפיך $\Leftarrow \gamma = \pm 1 \Leftarrow N(\gamma)=1$

נגלה: α אי-פריק, מצד שני, α לא

ראשוני. אכן $\Leftarrow (2+\sqrt{-5})(2-\sqrt{-5}) = 9$

$9 = 3 \cdot 3 \in (\alpha)$. אבל אין כי $3 \notin (\alpha)$

ולכן (α) אינו אידאל ראשוני. נניח שבשלילה

כי $N(3) = 9 = N(\alpha)N(\delta) \Leftarrow 3 = \alpha\delta$

$3 = \pm \alpha \Leftarrow \delta = \pm 1 \Leftarrow N(\delta) = 1 \Leftarrow$

סתירה.

<u>הגדרה</u> תחום שלמות R נקרא תחום פריקות יחידה (תפ"י) (=UFD unique factorization domain)

אם לכל $a \in R$ כך ש-a לא הפיך וגם $a \neq 0$ מתקיים:

א) קיים פירוק $a = p_1 p_2 p_3 \cdots p_r$
למכפלה (סופית) של איברים אי-פריקים.

ב) הפירוק הינו יחיד במובן הבא. יהי
$a = q_1 q_2 \cdots q_s$ פירוק אחר.

אזי $s = r$, ועד כדי מספור מחדש של ה-q_i-ים
p_i ו-q_i חברים לכל $i = 1, 2, \ldots, r$.

<u>הערה</u> אם $p \in R$ אי-פריק, אזי up גם אי-פריק
לכל u הפיך.

<u>דוגמאות</u> א) כל שדה הינו תפ"י במובן הריק.
ב) $\mathbb{Z}$ הינו תפ"י (המשפט היסודי של האריתמטיקה).

<u>טענה</u> יהי R תפ"י, יהי $a \in R$. אזי
a ראשוני $\iff$ a אי-פריק.

<u>הוכחה</u> $\Leftarrow$) נכון בכל תחום שלמות.

$\Rightarrow$) יהי a אי-פריק. יהי $a|bc$.

זה אומר $bc=ad$ עבור d מתאים.

יהיו

$$b = p_1p_2\cdots p_r$$

$$c = q_1q_2\cdots q_s$$

$$d = \pi_1\pi_2\cdots\pi_t$$

פירוקים לגורמים אי-פריקים. אזי

$$bc=ad \Leftrightarrow p_1p_2\cdots p_r q_1q_2\cdots q_s = a\pi_1\pi_2\cdots\pi_t$$

לפי יחידות הפירוקים, a הינו חבר של אחד ה-p_i-ים או אחד ה-q_i-ים.

נניח בלי הגבלת הכלליות כי a חבר של p_1.

$\Leftarrow$ $p_1=au$ כאשר u הפיך $\Leftarrow$

$$b = p_1p_2\cdots p_r = a(up_2p_3\cdots p_r) \Rightarrow a|b.$$

לכן a ראשוני.

<u>מסקנה</u> $\mathbb{Z}[\sqrt{-5}]$ לא תפ"י. (יש איברים אי-פריקים שאינם ראשוניים)

טענה כל תחום ראשי הינו תחום פריקות יחידה.

הגדרה חוג (חילופי) נקרא נתרי אם כל שרשרת עולה של אידאלים $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ מתייצבת, כלומר קיים N כך ש-$I_n = I_N$ לכל $n \geq N$. הוכחנו לפני שיעורים שכל תחום ראשי הינו נתרי.

תת-טענה יהי R תחום ראשי, $a \in R$. אזי a אי-פריק $\iff$ (a) מקסימלי.

הוכחה $\Leftarrow$) יהי a אי-פריק. נניח $(a) \subseteq I$, כאשר I אידאל אמיתי. אזי $I=(d)$ $\Leftarrow$ $a=bd$. אך I אמיתי $\Leftarrow$ d לא הפיך $\Leftarrow$ b הפיך $\Leftarrow$ a,d חברים $\Leftarrow$ $(a)=(d)=I$ $\Leftarrow$ (a) מקסימלי.

$\Rightarrow$) יהי (a) מקסימלי. אם $a=bc$, ואף אחד מן הגורמים אינו הפיך, אזי $(a) \subsetneq (b)$, בסתירה למקסימליות. (הכיוון הזה נכון בכל תחום שלמות)

הוכחה של המשפט: יהי R תחום ראשי.

יהי $0\neq a\in R$ איבר לא הפיך.

שלב 1 אני טוען שיש ל-a מחלק אי-פריק

הוכחה נניח שלא. אזי a בעצמו לא

אי-פריק $\Leftarrow$ $a=b_1c_1$, שני הגורמים
לא אי-פריקים
לא הפיכים

$c_1=b_2c_2$, כאשר b_2,c_2 לא הפיכים ולא
אי-פריקים

$c_2=b_3c_3$ ...

$c_3=b_4c_4$ ...

בפרט $(a)\subsetneq(c_1)\subsetneq(c_2)\subsetneq(c_3)\subsetneq\dots$

(כי b_1, $b_2,b_3,\dots$ לא הפיכים, לכן $a,c_1,c_2,\dots$
לא חברים). סתירה לנתריות.

שלב 2 יש ל-a פירוק לגורמים אי-פריקים.

הוכחה יש ל-a מחלק אי-פריק p_1

לפי שלב 1. $a=p_1b_1$. אם b_1 הפיך

סיימנו (כי a אי-פריק).

אחרת, ל-b_1 יש גורם אי-פריק p_2.

אזי $b_1=p_2b_2 \Leftarrow a=p_1p_2b_2$. אם

b_2 הפיך, סיימנו. ממשיכים

$$b_2=p_3b_3$$
$$b_3=p_4b_4$$

אם אף אחד מן ה-b_i-ים אינו הפיך, אזי

כל ה-p_i-ים לא חברים ומקבלים

$$(p_1)\subsetneq(p_2)\subsetneq(p_3)\subsetneq\cdots$$

בסתירה לנותריות. אזי מתישהו נקבל b_r הפיך.

אזי

$$a=p_1p_2p_3\cdots p_rb_r=p_1p_2\cdots p_{r-1}\underbrace{(p_rb_r)}_{\text{אי-פריק}}$$