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

R חוג חילופי, אידיאל $I \triangleleft R$ הינו תת-קבוצה סגורה לחיבור $a,b\in I \Rightarrow a+b\in I$

וסגורה לכפל עם כל איבר של R. $a\in I$, $r\in R \Rightarrow ra\in I$

האידיאל הראשי הנוצר ע"י $a\in R$ הוא $Ra=(a)=\{ra : r\in R\}$

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

$a=qb+r$ וגם

ב) $r=0$ או $N(r)<N(b)$

דוגמאות:

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

אם $a,b\in F$ $(b\neq 0)$ $\Rightarrow$ $q=ab^{-1}$, $r=0$

2) $R=\mathbb{Z}$ $N(a)=|a|$ (ערך מוחלט רגיל)

למדנו את אלגוריתם אוקלידס לחילוק עם שארית.

3) $R=\mathbb{F}[x]$ לכל שדה F. $N(P)=\deg P$. $N(a_nx^n+\dots+a_0)=n$

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

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

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

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 $\beta\neq 0$. איך מחלקים?

יהי $\gamma=\frac{\alpha}{\beta}\in\mathbb{C}$. נבחר שלמים $m,n\in\mathbb{Z}$ כך ש $|m-\mathrm{Re}\,\gamma|\leq\frac{1}{2}$

$|n-\mathrm{Im}\,\gamma|\leq\frac{1}{2}$

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

צריך להוכיח ש $N(r)<N(\beta)$ (במקרה הזה $\beta\neq 0 \Rightarrow N(\beta)\neq 0$)

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

טענה:

כל תחום אוקלידי הוא תחום ראשי

הוכחה:

יהי R תחום אוקלידי, ויהי $I \triangleleft R$ אידאל. 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)

נראה ש $I=(d)$

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

יהי $a\in I$. קיימים q,r כך ש $a=qd+r$ וגם $N(r)<N(d)$ או $r=0$.

אבל $r=\underbrace{a}_{\in I}-\underbrace{qd}_{\in I}\in I$. אם $r\neq 0$ אז $N(r)<N(d)$ בסתירה למינימליות של $N(d)$

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

תוצאה:

החוג $\mathbb{Z}[x]$ אינו תחום אוקלידי

הוכחה:

הוכחנו כבר ש $\mathbb{Z}[x]$ אינו תחום ראשי.

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

$b\in(a) \Longleftrightarrow ac=b$

הגדרה: $a,b\in R$ נקראים חברים אם קיים $u\in R$ הפיך כך ש $a=bu$

הגדרות: יהי R חוג תילופי

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

ב) $0\neq a\in R$ לא הפיך נקרא אי פריק אם $a=bc \Leftarrow b$ הפיך או c הפיך

ג) $0\neq a\in R$ לא הפיך נקרא ראשוני אם (a) הוא אידאל ראשוני $\Longleftrightarrow bc\in(a)$,

אז $b\in(a)$ או $c\in(a)$

טענה:

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

הוכחה:

לפי ההנחה (a) ראשוני. יהי $a=bc$. אזי $bc\in(a) \Leftarrow b\in(a)$ או $c\in(a)$.

בלי הגבלת הכלליות נניח $c\in(a)$. אזי $c=ra$

קיבלנו $a=bc=bra \Leftarrow a-bra=(1-br)a=0$

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

דוגמא:

איבר אי-פריק - לא בהכרח ראשוני $R=\mathbb{Z}[\sqrt{-5}]=\{a+ib\sqrt{5} \mid a,b\in\mathbb{Z}\}\subseteq\mathbb{C}$

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 $\alpha=2+\sqrt{-5}$. נראה ש-α אי-פריק. אכן, יהי $\alpha=\beta\gamma$. אז
$N(\beta)N(\gamma)=N(\alpha)=2^2+5\cdot 1^2=9$

נשים לב שלא ניתן להציג את $3=a^2+5b^2$, אז אין $\beta\in R$ עם $N(\beta)=3$.

לכן בהכרח $N(\beta)=9, N(\gamma)=1$ (או להיפך) ואז $N(\gamma)=1 \Leftarrow \gamma=\pm 1 \Leftarrow$
$\Leftarrow \gamma$ הפיך $\Leftarrow \alpha$ אי-פריק

מצד שני, α לא ראשוני. אכן $(2+\sqrt{-5})(2-\sqrt{-5})=9 \Leftarrow 9=3\cdot 3\in(\alpha)$.

נראה ש $3\notin(\alpha)$ (ולכן (α) אינו אידיאל ראשוני). נניח בשלילה כי $3=\alpha\delta$
$\Leftarrow N(3)=9=N(\alpha)N(\delta) \Leftarrow N(\delta)=1 \Leftarrow \delta=\pm 1 \Leftarrow 3=\pm\alpha$ סתירה.

הגדרה: תחום שלמות R נקרא תחום פריקות יחידה (תפ"י) (unique factorization domain - UFD) אם לכל $a\in R$ כך ש a לא הפיך וגם $a\neq 0$ מתקיים:

א) קיים פירוק $a=p_1p_2\dots p_r$ למכפלה (סופית) של איברים אי-פריקים

ב) הפירוק יחיד: אם $a=q_1\cdot\ldots\cdot q_s$ פירוק אחר, אזי $r=s$

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

הערה: אם $p\in R$ אי פריק, אזי pu גם אי פריק לכל u הפיך

דוגמאות:

1) כל שדה הוא תפ"י במובן הריק.

ב) $\mathbb{Z}$ הוא תפ"י (המשפט היסודי של האריתמטיקה)

טענה:

יהי R תפ"י, ויהי $a\in R$. אזי a ראשוני $\iff$ a אי פריק

הוכחה:

($\Leftarrow$) נכון בכל תחום שלמות

($\Rightarrow$) יהי a אי פריק. יהי $a|bc$. זה אומר $bc=ad$ עבור d מתאים

יהיו $b=p_1\cdot\ldots\cdot p_r$, $c=q_1\cdot\ldots\cdot q_s$, $d=\pi_1\cdot\ldots\cdot\pi_t$

פירוקים לגורמים אי פריקים. אזי

$$bc=ad \iff p_1p_2\cdot\ldots\cdot p_r\cdot q_1\cdot\ldots\cdot q_s = a\pi_1\cdot\ldots\cdot\pi_t$$

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 $\Leftarrow$ $b=p_1\cdot\ldots\cdot p_r=a(up_2\cdot\ldots\cdot p_r)$ $\Leftarrow$ $a|b$

לכן a ראשוני

תוצאה:

$\mathbb{Z}[\sqrt{-5}]$ לא תפ"י (יש איברים אי-פריקים שאינם ראשוניים)

טענה:

כל תחום ראשי הינו תחום פריקות יחידה

תזכורת: חוג (חילופי) נקרא נותרי אם כל שרשרת עולה של אידאלים
$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$

מתייצבת, כלומר קיים N כך ש $I_n = I_N$ לכל $n \geq N$.

הוכחנו לפני ב שיעורים שכל תחום ראשי הוא נותרי

נוח 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 $I = (d) \Leftarrow$

$\Leftarrow$ $a = bd$. ובגלל I אמיתי $\Leftarrow$ d לא הפיך $\Leftarrow$ b הפיך $\Leftarrow$ a,d חברים

$\Leftarrow$ $I = (d) = (a) \Leftarrow (a)$ מקסימלי

$(\Rightarrow)$ יהי (a) מקסימלי. אם $a = bc$, נניח אחד מהגורמים 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 I: נראה שיש ל- a מחלק אי פריק.

נניח שלא. אזי a בעצמו לא אי פריק $\Leftarrow$ $a = b_1 c_1$, שני הגורמים לא אי-פריקים ולא הפיכים

$c_1 = b_2 c_2$ שני הגורמים לא אי-פריקים ולא הפיכים

$c_2 = b_3 c_3$ שני הגורמים לא אי-פריקים ולא הפיכים

$\vdots$

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

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

שלב II: יש ל-a פירוק לגורמים אי פריקים.

יש ל-a מחלק אי פריק p_1 לפי שלב I. $a=p_1b_1$. אם b_1

היה הפיך סיימנו (כי a אי פריק)

אחרת, ל-b_1 יש גורם אי פריק p_2. אזי $a=p_1p_2b_2 \Leftarrow b_1=p_2b_2$.

אם b_2 הפיך, סיימנו. ממשיכים באופן הזה ($b_2=p_3b_3$, $b_3=p_4b_4$)

אם אף אחד מן ה-b_i-ים אינו הפיך, אזי כל ה-p_i-ים לא

חברים ומקבלים: $(p_1) \subsetneq (p_2) \subsetneq (p_3) \subsetneq \ldots$

בסתירה לנתריות. אז מתישהו נקבל b_r הפיך. לכן,

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