המשך הוכחה מההרצאה הקודמת:

(כל תחום ראשי הינו תפ"י)

כבר הוכחנו שקיימים פירוקים לאי פריקים. נשאר להוכיח את היחידות

תזכורת: R תחום ראשי. אזי: $a\in R$ אי פריק $\Longleftrightarrow$ (a) מקסימלי $\Longleftrightarrow$ (a) ראשוני $\Longleftrightarrow$ a ראשוני

יהי R תחום ראשי. $0\neq a\in R$ לא הפיך. נתונים שני פירוקים

$$a = p_1\cdot\ldots\cdot p_r = q_1\cdot\ldots\cdot q_s$$

באינדוקציה על r. אם $r=1$, $a=p_1$ אי פריק. אם $a=p_1=q_1\cdot\ldots\cdot q_s$

אזי a אי פריק $\Leftarrow$ a ראשוני (כי R תחום ראשי) לכן $a|q_i \Leftarrow a|q_1\cdot\ldots\cdot q_s$

עבור i מסוים. זה אומר ש $(q_i)\subseteq(a) \Leftarrow q_i\in(a)$

וכל גם q_i אי פריק. לכן $(a),(q_i)$ אידאלים מקסימליים $\Leftarrow$ $(q_i)=(a)$ $\Leftarrow$

$\Leftarrow$ q_i,a חברים

(ה-q-ים) $q_1\cdot\ldots\cdot q_r=q_i$, q_i מייצרים את אותו האידאל (a). לכן הם חברים

(שאר ה-q_i-ים הפיכה. אך מכפלה של קבוצה לא ריקה של אי פריקים לא

הפיכה, לכן זו מכפלה ריקה. לכן $s=1$, $a=p_1=q_1$.

נניח שיחידות הפירוק ידועה ל-r. יהי $a=p_1\cdot\ldots\cdot p_r\cdot p_{r+1}=q_1\cdot\ldots\cdot q_s$

אזי p_r ראשוני, לכן $p_{r+1}|q_i \Leftarrow p_{r+1}|q_1\cdot\ldots\cdot q_s$ לאיזשהו i. עד כדי מספור

מחדש, נניח $p_{r+1}|p_s$

כמו קודם $q_s=up_{r+1} \Leftarrow (q_s)=(p_{r+1}) \underset{\text{שניהם אי פריקים}}{\Leftarrow} (q_s)\subseteq(p_{r+1})$ עבור $u\in R$ הפיך

R תחום שלמות, אז אפשר לצמצם את p_{r+1}:

$$p_1\cdot\ldots\cdot p_r = q_1\cdot\ldots\cdot(q_{s-1}u)$$

באינדוקציה $r+1=s \Leftarrow r=s-1$, וגם p_i,q_i חברים לכל $1\le i\le\ldots\le r$ עד כדי

שינוי בסדר ה-q_i-ים.

הגדרה: יהי R חוג חילופי. תהי $S\subseteq R$ תת קבוצה כך ש:

1) $0\notin S$

2) S סגורה לכפל $(ab\in S \Leftarrow a,b\in S)$

3) $1\in S$

נגדיר את החוג $S^{-1}R=\{\frac{r}{s} : r\in R, s\in S\}$

פורמלית: נגדיר קודם יחס שקילות על $R\times S$ $\left((r,s) \rightsquigarrow \frac{r}{s}\right)$:

$(r_1,s_1)\sim(r_2,s_2) \iff$ ק"מ $t\in S$ כך ש $t(r_1s_2-r_2s_1)=0$

נב יחס שקילות:

רפלקסיביות - ברורה

סימטריות - ברורה

טרנזיטיביות - $(r_1,s_1)\sim(r_2,s_2)$, $(r_2,s_2)\sim(r_3,s_3)$ אז קיימים $t_1,t_2\in S$ כך ש

$$t_1(r_1s_2-r_2s_1)=0, \quad t_2(r_2s_3-r_3s_2)=0$$

לכן,

$$0=s_3t_2t_1(r_1s_2-r_2s_1)+s_1t_1t_2(r_2s_3-r_3s_2)=$$

$$=r_1s_2s_3t_1t_2-r_2s_1s_3t_1t_2+r_2s_1s_3t_1t_2-r_3s_1s_2t_1t_2=$$

$$=\underbrace{s_2t_1t_2}_{\in S}(r_1s_3-r_3s_1) \Rightarrow (r_1,s_1)\sim(r_3,s_3)$$

תהי $S^{-1}R$ קבוצת מחלקות השקילות. נגדיר חיבור וכפל:

$$\frac{r_1}{s_1}+\frac{r_2}{s_2}=\frac{r_1s_2+r_2s_1}{s_1s_2}, \quad \frac{r_1}{s_1}\cdot\frac{r_2}{s_2}=\frac{r_1r_2}{s_1s_2}$$

כלומר,

$$(r_1,s_1)+(r_2,s_2)=(r_1s_2+r_2s_1, s_1s_2)$$

$$(r_1,s_1)\cdot(r_2,s_2)=(r_1r_2, s_1s_2)$$

תרגיל:

הפעולות מוגדרות היטב על $S^{-1}R$, וגם $S^{-1}R$ הוא חוג חילופי עם הפעולות הללו.

דוגמאות:

1) R תחום שלמות, $S=R\setminus\{0\}$ סגור לכפל. במקרה הזה $S^{-1}R$ הוא שדה

$$\frac{r}{s}=\frac{0}{1} \iff rt=t(r\cdot 1-0\cdot s)=0 \Rightarrow r=0$$

לכן, אם $0\neq\frac{r}{s}\in S^{-1}R$ אזי $r\neq 0$, אז $\frac{r}{s}\cdot\frac{s}{r}=\frac{rs}{rs}=\frac{1}{1}$

במקרה הזה, $S^{-1}R$ נקרא שדה השברים של R, ומסומן $\mathrm{Frac}R$ $(\mathrm{Frac}\,\mathbb{Z}=\mathbb{Q})$

2) R חוג חילופי. $S=\{$כל האיברים הרגולריים$\}$

$S^{-1}R=$ חוג השברים של R

הערה: אם R תחום שלמות, $S=R\setminus\{0\}$, ומקבלים $\mathrm{Frac}R$.

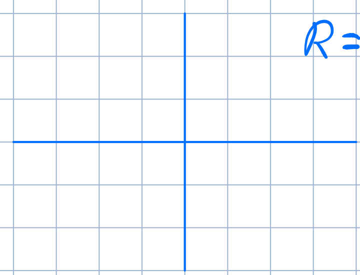
3) $R=\mathbb{Z}$, $S=\{1,2,4,8,16,32,\dots\}$, $S^{-1}R=\{\frac{a}{b}\in\mathbb{Q} : b=2^k\}$

$S^{-1}R$ נקרא המיקום של R ב-S

4) R חוג חילופי, P אידיאל ראשוני. $S=R\setminus P$. $S^{-1}R=\{\frac{r}{s} : s\notin P\}$

$R=\mathbb{R}^2$

$\mathbb{R}[x,y] \longleftrightarrow$



$P=I(V)=(x,y) \longleftrightarrow (0,0)$

ראשוני

V אי פריקה

$S=\mathbb{R}[x,y]\setminus P$, אזי $S^{-1}R=\left\{\begin{array}{c}\text{פונקציות רציונליות } \frac{f(x,y)}{g(x,y)} \\ \text{מעל } \mathbb{R} \\ \text{שמוגדרות ב-}(0,0)\end{array}\right\}$

יש הומ' של חוגים $R\to S^{-1}R$, $r\mapsto\frac{r}{1}$. אם R לא תחום שלמות, ההומ' הנ"ל עלול לא להיות חח"ע.

הגדרה: R תחום תלוקי. יהי $a,b\in R$. d הוא מחלק משותף של a,b אם $d|a$ וגם $a,b\in(d)\Leftrightarrow d|b$

הוא נקרא מחלק משותף מקסימלי (gcd) אם לכל מחלק משותף c אחר של a,b מתקיים $c|d$.

כלומר, (d) הוא האידיאל הראשי המינימלי, שמכיל את $I=(a,b)$

תוצאה:

אם R תחום שלמות, אזי gcd של שני איברים מוגדר היטב עד כדי חברות, אם הוא קיים.

דוגמה:

ה-gcd של שני איברים לא בהכרח קיים

$R=\mathbb{Z}[\sqrt{-5}]$ כב תחום שלמות. $\alpha=6$, $\beta=2(1+\sqrt{-5})$.

$N(a+b\sqrt{-5})=a^2+5b^2=|a+b\sqrt{-5}|^2$, $N(\alpha)=36$, $N(\beta)=24$

$c=2$
$d=1\pm\sqrt{-5}$ שניהם מחלקים משותפים של α,β $(\alpha=(1-\sqrt{-5})(1+\sqrt{-5}))$

נסמן את ה-gcd של α,β ב-g. אזי $c|g$, $d|g$ $\Leftarrow$

$\Leftarrow$ $4=N(c)|N(g)$, $6=N(d)|N(g)$ $\Leftarrow$ $12=lcm(4,6)|N(g)$

מצד שני, $g|\alpha$, $g|\beta$ $\Leftarrow$ $N(g)|N(\alpha)=24$, $N(g)|N(\beta)=36$ $\Leftarrow$ $N(g)=gcd(24,36)=12$

לכן $N(g)=12$. אבל $12\neq a^2+5b^2$ לכל $a,b\in\mathbb{Z}$

לכן ב-$\mathbb{Z}[\sqrt{-5}]$ אין איברים עם נורמה 12. ל-α,β אין gcd

תרגיל:

אם R הוא תפ"י, אזי לכל זוג α,β של איברים לא אפסיים יש gcd

$\left(\alpha=p_1^{e_1}\cdot\ldots\cdot p_r^{e_r},\ \beta=p_1^{f_1}\cdot\ldots\cdot p_r^{f_r}\right.$

$\left.gcd(\alpha,\beta)=p_1^{\min\{e_1,f_1\}}\cdot\ldots\cdot p_r^{\min\{e_r,f_r\}}\right)$ p_i אי פריקים לא חברים, $e_i f_i\geq 0$.

$\{\text{שדות}\} \subsetneq \{\text{תחומים אוקלידיים}\} \subsetneq \{\text{תחומים ראשיים}\} \subsetneq \{\text{תפ"י}\} \subsetneq \{\text{תחומי gcd}\} \subsetneq \{\text{תחומי שלמות}\} \subsetneq \{\text{חוגים חילופיים}\}$

הערות:

1) R תחום שלמות $\iff$ $R[x]$ תחום שלמות

כי: $(\Rightarrow)$ אם $ab=0$, אז נחשוב על a,b כעל פולינומים קבועים

$(\Leftarrow)$ $f(x)g(x)=0$, $f(x)=ax^n+\{\text{חזקות יותר גבוהות}\}$ $(a\neq 0)$

ו- $g(x)=bx^m+O(x^{m+1})$ $(b\neq 0)$

$$f(x)g(x)=abx^{m+n}+O(x^{m+n+1}) \Rightarrow ab=0$$

2) יהי $I\triangleleft R$, יהי $I[x]\triangleleft R[x]$ האידיאל של כל הפולינומים עם מקדמים ב- I. נזכור שבהינתן הומ' $f:R\to S$ מקבלים הומ' $f:R[x]\to S[x]$

$\left(f(a_nx^n+\dots+a_0)=f(a_n)x^n+\dots+f(a_0)\right)$

בפרט, אם $f:R\to R/I$, $f(r)=r+I$. אז מקבלים $f:R[x]\to (R/I)[x]$ על

$\ker f=I[x]$. לפי משפט האיזו' הראשון, $R[x]/I[x]\simeq (R/I)[x]$

תוצאה:

$I\triangleleft R$ אידיאל ראשוני $\iff$ $I[x]\triangleleft R[x]$ אידיאל ראשוני

הוכחה:

$I\triangleleft R$ ראשוני $\iff$ R/I תחום שלמות $\iff$ $(R/I)[x]$ תחום שלמות $\iff$ $R[x]/I[x]$ תחום שלמות $\iff$ $I[x]$ ראשוני