מבוא לחוגים ומודולים - תרגול 13

תחומי דדקינד

הגדרה:

יהי R חוג. נקרא R ***תחום דדקינד*** אם:

א. R תחום שלמות

ב. R נותרי (כל שרשרת עולה של אידאלים מתייצבת)

ג. $\dim R=1$ (כל אידאל ראשוני לא אפסי הוא מקסימלי)

ד. R סגור בשלמות בתוך שדה השברים שלו.

תרגיל:

הראו שכל תחום ראשי הוא תחום דדקינד.

הוכחה:

יהי R תחום ראשי.

א. כל תחום ראשי הוא תחום שלמות.

ב. משפט מההרצאה.

[רעיון: אם $I_1\subseteq I_2\subseteq\dots$ אידאלים, אז $J=\bigcup_{n=1}^{\infty} I_n$ אידאל,
אבל R ראשי לכן $J=\langle j\rangle$ $\Leftarrow$ קיים $n\in\mathbb{N}$ כך ש- $j\in I_n$
$\Leftarrow$ $J=I_n$.]

ג. משפט מההרצאה.

[רעיון: אם $0\neq P\triangleleft R$ אידאל ראשוני, נניח בשלילה ש-P לא
מקסימלי. $P\subsetneq M\subsetneq R$, M אידאל מקסימלי. R תחום ראשי,
לכן $P=\langle p\rangle$, $M=\langle m\rangle$. $P\subseteq M$ $\Leftarrow$ $m|p$.
P ראשוני $\Leftarrow$ p איבר ראשוני $\Leftarrow$ p אי-פריק $\Leftarrow$ m הפיך $\Leftarrow$ $M=R$
או $m\sim p$ $\Leftarrow$ $M=P$ בסתירה.]

ד. R תחום ראשי ⇐ R תפ"י, וראינו בהרצאה שכל תפ"י סגור בשלמות בשדה השברים שלו.

[רעיון: אם $\frac{\alpha}{\beta}$ (שבר מצומצם) שורש של $a_nx^n + a_{n-1}x^{n-1} + \dots + a_0$,
אז $\beta | a_n$ ו- $\alpha | a_0$. אבל אם $\frac{\alpha}{\beta}$ שלם מעל R,
אפשר לבחור $a_n = 1$ ⇐ β הפיך ⇐ $\frac{\alpha}{\beta} \in R$] □

__הגדרה:__

__שדה מספרים__ הוא שדה $\mathbb{Q} \subseteq F$ ו- F ממימד סופי כמו"ו מעל $\mathbb{Q}$.

הסגור השלם של $\mathbb{Z}$ ב- F מסומן $\mathcal{O}_F$.

__משפט:__

לכל שדה מספרים F, $\mathcal{O}_F$ הוא תחום דדקינד.

__הוכחת סגירות בשלמות:__ (השאר - בהרצאה)

$$\begin{array}{c} S \\ | \\ T \\ | \\ R \end{array} \qquad T = \text{הסגור השלם}$$

הוכחנו בתרגול הקודם שאם $R \subseteq S$ תחומי שלמות, אז הסגור השלם של R ב- S סגור בשלמות ב- S.

לכן $\mathcal{O}_F$ סגור בשלמות ב- F.

בפירוט: נניח $a \in F$ שלם מעל $\mathcal{O}_F$. אנחנו יודעים ש- $\mathcal{O}_F$ הרחבה שלמה של $\mathbb{Z}$, ולכן מתרגיל מהתרגול הקודם a שלם מעל $\mathbb{Z}$.

לכן, לפי הגדרת הסגור השלם, $a \in \mathcal{O}_F$. לכן $\mathcal{O}_F$ סגור בשלמות. □

__דוגמה:__

$F = \mathbb{Q}[\sqrt{D}]$ ל- D חופשי מריבועים, אז

$$\mathcal{O}_{\mathbb{Q}[\sqrt{D}]} = \mathcal{O}_D = \begin{cases} \mathbb{Z}[\sqrt{D}], & D \equiv 2,3 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right], & D \equiv 1 \pmod 4 \end{cases}.$$

משפט:

יהי R תחום דדקינד, ויהי $0\neq I\triangleleft R$ אידאל. אז קיים פירוק $I=P_1^{e_1}\cdots P_r^{e_r}$ כאשר $P_1,\dots,P_r\triangleleft R$ אידאלים ראשוניים ו- $e_1,\dots,e_r\in\mathbb{N}$. בנוסף, הפירוק יחיד עד כדי סדר הגורמים.

איך זה עובד?

ניקח $0\neq I\triangleleft R$. אם I ראשוני, סיימנו.

אחרת, $I\subsetneq P$ עבור P מקסימלי (ובפרט, ראשוני). נגדיר

$$P^{-1}=\{x\in Frac(R)\mid xP\subseteq R\}$$

[למשל: אם $R=\mathbb{Z}$, $P=2\mathbb{Z}$, אז $P^{-1}=\frac{1}{2}\mathbb{Z}$]. מתקיים $PP^{-1}=R$.

$$I\subsetneq IP^{-1}=I_1$$

אם I_1 ראשוני, סיימנו. אחרת, בדומה נמצא אידאל ראשוני $I_1\subsetneq P_2$.

$$I\subsetneq IP^{-1}=I_1\subsetneq I_1P_2^{-1}=I_2$$

כך אפשר להמשיך ולקבל שרשרת אידאלים $I\subsetneq I_1\subsetneq I_2\subsetneq\cdots$.

כיוון ש-R נותרי, התהליך חייב להסתיים בשלב סופי - ואז נקבל אידאל ראשוני I_n. אם נוסיף את כל האידאלים שמצאנו בדרך יחד עם I_n וזה ייתן את הפירוק.

תרגיל:

יהי R תחום דדקינד, יהי $0\neq I\triangleleft R$ אידאל, ויהי $P\triangleleft R$ אידאל ראשוני. אז P מופיע בפירוק של I למכפלת אידאלים ראשוניים $\Longleftrightarrow I\subseteq P$.

הוכחה:

$\boxed{\Leftarrow}$ נניח $I=P^{e_1}P_2^{e_2}\cdots P_r^{e_r}$. לכן

$$I=P^{e_1}P_2^{e_2}\cdots P_r^{e_r}\subseteq P^{e_1}\subseteq P$$

$\boxed{\Rightarrow}$ נניח $I\subseteq P$ $=$ $P_1^{e_1}\cdots P_r^{e_r}$.

P ראשוני, לכן קיים $1\le i\le r$ כך ש- $P_i\subseteq P$.

R תחום דדקינד, לכן P_i מקסימלי (כי $P_i\neq 0$), לכן $P_i=P$. □

מסקנה:

בתנאים הנ"ל, P^e מופיע בפירוק של I $\iff I\subseteq P^e$.

אפשר להסיק ש- P מופיע בפירוק של I עם חזקה בדיוק e $\iff I\subseteq P^e$, $I\not\subseteq P^{e+1}$.

תרגיל:

נתבונן בחוג $R=\mathcal{O}_{-5}=\mathbb{Z}[\sqrt{-5}]$. כזכור, R לא תפ"י כי $6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$.

א. הראו שהאידיאלים $P_1=\langle 2,1+\sqrt{-5}\rangle$, $P_2=\langle 3,1+\sqrt{-5}\rangle$, $P_3=\langle 3,1-\sqrt{-5}\rangle$ ראשוניים.

ב. הראו ש- $6\mathcal{O}_{-5}=P_1^2P_2P_3$.

פתרון:

א. נוכיח $\mathbb{Z}/6\mathbb{Z}\cong\mathbb{Z}[\sqrt{-5}]/\langle 1-\sqrt{-5}\rangle\cong\mathbb{Z}[\sqrt{-5}]/\langle 1+\sqrt{-5}\rangle$.

$\varphi_1:\mathbb{Z}[\sqrt{-5}]\longrightarrow\mathbb{Z}/6\mathbb{Z}$ לפי $\varphi_1(a+\sqrt{-5}b)=a-b+6\mathbb{Z}$

$\varphi_2:\mathbb{Z}[\sqrt{-5}]\longrightarrow\mathbb{Z}/6\mathbb{Z}$ לפי $\varphi_2(a+\sqrt{-5}b)=a+b+6\mathbb{Z}$

אפשר לוודא ש- φ_1,φ_2 אפימורפיזמים עם גרעין $\ker\varphi_1=\langle 1+\sqrt{-5}\rangle$

$\ker\varphi_2=\langle 1-\sqrt{-5}\rangle$

אפשר לשים לב $P_1=\varphi_1^{-1}(2\mathbb{Z}/6\mathbb{Z})$, $P_2=\varphi_1^{-1}(3\mathbb{Z}/6\mathbb{Z})$, $P_3=\varphi_2^{-1}(3\mathbb{Z}/6\mathbb{Z})$,

ומשפט ההתאמה נקבל ש-P_1, P_2, P_3 אידאלים ראשוניים ב- $\mathcal{O}_{-5}$.

ב. רוצים להוכיח $6\mathcal{O}_{-5} = P_1^2 P_2 P_3$.

$$P_1^2 = \langle 2, 1+\sqrt{-5}\rangle\langle 2, 1+\sqrt{-5}\rangle = \langle 4, 2+2\sqrt{-5}, 2+2\sqrt{-5}, -4+2\sqrt{-5}\rangle =$$

בחוג חילופי,
$\langle a\rangle\cdot\langle b\rangle = \langle ab\rangle$
$\langle a_1,\dots,a_n\rangle\langle b_1,\dots,b_m\rangle = \langle a_1b_1, a_1b_2,\dots,a_nb_m\rangle$

$$= \langle 4, 2+2\sqrt{-5}, 2\rangle = \langle 2\rangle = 2\mathcal{O}_{-5}$$

מאופן דומה $P_2P_3 = 3\mathcal{O}_{-5}$. לכן

$$P_1^2 P_2 P_3 = (2\mathcal{O}_{-5})(3\mathcal{O}_{-5}) = 6\mathcal{O}_{-5}$$

הגדרה:

יהי R תחום דדקינד, ויהיו $J, I \trianglelefteq R \neq 0$. אומרים ש-$I$ מחלק את J, ומסמנים $I|J$, אם קיים $I' \trianglelefteq R$ ש- $II' = J$.

דוגמה:

ב- $\mathbb{Z}$, $m\mathbb{Z} | n\mathbb{Z} \iff m|n \iff n\mathbb{Z} \subseteq m\mathbb{Z}$.

תרגיל:

אם R תחום דדקינד, $I|J \iff J \subseteq I$.

הוכחה:

נכתוב $I = P_1^{e_1}\cdots P_r^{e_r}$, $J = P_1^{f_1}\cdots P_r^{f_r}$, $e_i, f_i \geq 0$.

$\boxed{\Leftarrow}$ $I|J \Leftarrow J = II' \subseteq I$.

$\boxed{\Rightarrow}$ מהתרגיל שהוכחנו קודם, נקבל $e_i \leq f_i$ לכל $1 \leq i \leq r$,

ולכן $J = P_1^{f_1}\cdots P_r^{f_r} = \underbrace{(P_1^{e_1}\cdots P_r^{e_r})}_{I}\underbrace{(P_1^{f_1-e_1}\cdots P_r^{f_r-e_r})}_{I'}$.

$\square$

תרגיל: (לבית)

יהי R תחום דדקינד, ויהיו $I = P_1^{e_1} \cdots P_r^{e_r}$, $J = P_1^{f_1} \cdots P_r^{f_r}$, $e_i, f_i \geq 0$

אז:

$$I + J = P_1^{\min\{e_1,f_1\}} \cdots P_r^{\min\{e_r,f_r\}}$$

$$IJ = P_1^{e_1+f_1} \cdots P_r^{e_r+f_r}$$

$$I \cap J = P_1^{\max\{e_1,f_1\}} \cdots P_r^{\max\{e_r,f_r\}}$$

תרגיל:

יהי R תחום דדקינד, יהי $0 \neq I \lhd R$, ויהי $0 \neq a \in I$. אז קיים $b \in I$ כך ש- $I = \langle a, b \rangle$. בפרט, כל אידאל נוצר ע"י לכל היותר שני איברים.

הוכחה:

נכתוב $I = P_1^{e_1} \cdots P_r^{e_r}$ עבור $P_1, \dots, P_r \lhd R$ ראשוניים ו- $e_i \geq 0$. כיוון ש- $\langle a \rangle \subseteq I$, לכן אפשר לכתוב $\langle a \rangle = P_1^{f_1} \cdots P_r^{f_r}$ עבור $f_i \geq e_i$, $f_i \geq 0$.

לכל $1 \leq i \leq r$ נבחר $b_i \in P_1^{e_1+1} \cdots P_i^{e_i} \cdots P_r^{e_r+1} \setminus P_1^{e_1+1} \cdots P_i^{e_i+1} \cdots P_r^{e_r+1}$ (קיים בגלל יחידות הפירוק)

נשים לב ש- $b_i \in P_i^{e_i} \setminus P_i^{e_i+1}$.

אחרת, $P_1^{e_1+1} \cdots P_i^{e_i+1} \cdots P_r^{e_r+1} \underset{\text{התרגיל לבית}}{=} P_i^{e_i+1} \cap (P_1^{e_1+1} \cdots P_i^{e_i} \cdots P_r^{e_r+1}) \ni b_i$.

נגדיר $b = b_1 + \cdots + b_r$. נשים לב ש- $b \in I$, ו- $b \notin P_i^{e_i+1}$ לכל i

נטען כי $I = \langle a, b \rangle$.

אכן, $\langle a, b \rangle \subseteq I$. מצד שני, $\langle a, b \rangle \subseteq P_i^{e_i}$, $\langle a, b \rangle \not\subseteq P_i^{e_i+1}$ לכל i. אם היינו כותבים $\langle a, b \rangle = P_1^{t_1} \cdots P_r^{t_r}$, אז $t_i = e_i$.

$\square$

הגדרה:

יהי R תחום דדקינד. <u>אידאל שברי</u> של R הוא תת-R-מודול של $\mathrm{Frac}(R)$ שנוצר סופית כ-R-מודול.

דוגמה:

א. $R=\mathbb{Z}$, $\frac{1}{2}\mathbb{Z}$ הוא אידאל שברי.

$\mathbb{Z}[\frac{1}{2}]$ לא אידאל שברי.

ב. כל אידאל רגיל ("אידאל שלם") של R הוא אידאל שברי.

טענה:

כל אידאל שברי $\underline{a}\neq 0$ של R אפשר לכתוב בצורה $\underline{a}=IJ^{-1}$, $I,J\trianglelefteq R$
לכן גם אותם אפשר לפרק למכפלת ראשוניים עם חזקות שלמות.

דוגמה:

$R=\mathbb{Z}$, $\underline{a}=\frac{14}{15}\mathbb{Z}$.

$$\underline{a}=(14\mathbb{Z})(15\mathbb{Z})^{-1}=(2\mathbb{Z})\cdot(7\mathbb{Z})\cdot(3\mathbb{Z})^{-1}\cdot(5\mathbb{Z})^{-1}$$

חוגים מקומיים

הגדרה:

חוג חילופי R הוא <u>מקומי</u> אם יש לו אידאל מקסימלי יחיד.

משפט:

התנאים הבאים שקולים:

א. R הוא חוג מקומי.

ב. אוסף האיברים הלא הפיכים הוא אידאל.

ג. לכל $a\in R$, a הפיך או $1-a$ הפיך.

ד. אם סכום סופי של איברים ב-R הוא הפיך, אז לפחות אחד מהמחוברים הפיך.

תרגיל:

בחוג מקומי אין אידמפוטנטים לא טריוויאליים.

(איבר $e\in R$ הוא אידמפוטנט אם $e^2=e$; טריוויאלי $\Leftarrow$ $e=0,1$)

פתרון:

אם $e\neq 0,1$ אידמפוטנט אז $e^2=e$ $\Leftarrow$ $e(1-e)=0$ $\Leftarrow$ $e,1-e$ מחלקי אפס, ובפרט לא הפיכים. בסתירה. $\square$

תרגיל:

יהי M אידאל מקסימלי בחוג R. אז לכל $n\in\mathbb{N}$, החוג R/M^n מקומי עם אידאל מקסימלי יחיד M/M^n.

פתרון:

לפי משפט ההתאמה, כל אידאל מקסימלי של R/M^n הוא מהצורה I/M^n ל-$I\trianglelefteq R$ אידאל מקסימלי כך ש- $M^n\subseteq I$. יהי I כזה. I מקסימלי, לכן הוא ראשוני, לכן $M\subseteq I$. אבל M מקסימלי, לכן $I=M$. הראינו שהאידאל המקסימלי היחיד ב-R/M^n הוא M/M^n. $\square$

דוגמה:

$R=\mathbb{Z}$, $M=p\mathbb{Z}$. אז $\mathbb{Z}/p^n\mathbb{Z}$ מקומי עם אידאל מקסימלי $p\mathbb{Z}/p^n\mathbb{Z}$.

דוגמה:

$R=F[x]$, $M=\langle x\rangle$ (M מקסימלי כי $R/M\cong F$ שדה).

אז $F[x]/\langle x^n\rangle$ חוג מקומי עם אידאל מקסימלי $xF[x]/\langle x^n\rangle$.

דוגמה:

$R=F[[x]]$ הוא חוג מקומי עם אידאל מקסימלי יחיד $\langle x\rangle$.

תרגיל:

יהי R חוג חילופי, ויהי M אידאל מקסימלי של R. הראו שאם כל האיברים של M נילפוטנטיים, אז R מקומי עם אידאל מקסימלי יחיד M.

(תזכורת: a נילפוטנטי אם $a^n=0$ לאיזשהו n)

הוכחה:

דיון א' - אילו היה $I\neq M$ מקסימלי, ניקח $a\in M\setminus I$ ואז $a+I$ נילפוטנטי בשדה R/I, בסתירה.

דיון ב' - נראה שכל $a\notin M$, a הפיך. ידוע ש-M מקסימלי, לכן

$$M+Ra=R$$

לכן קיימים $m\in M$, $r\in R$ שעבורם $m+ra=1$.

לכן $ra=1-m$, m נילפוטנטי $\Leftarrow$ ra הפיך

(כי $1-m$ יהיה הפיך)

אם $m^k=0$

$$(1-m)(1+m+m^2+\dots+m^{k-1})=1-m^k=1$$

$R \xLeftarrow{\text{חילופי}}$ a הפיך. $\square$

תרגיל:

יהי F שדה ממאפיין שונה מ-2. הראו שמתקיים $F[x]/\langle x^2\rangle \not\cong F[x]/\langle x^2-1\rangle$.

פתרון:

$F[x]/\langle x^2\rangle$ מקומי. נסתכל על אגף ימין. נשים לב שהאידאלים $\langle x+1\rangle$ ו-$\langle x-1\rangle$ הם קו-מקסימליים, כי $2=(x+1)-(x-1)$ הפיך ב-F (מאפיין $\neq 2$).

ממשפט השאריות הסיני,

$$F[x]/\langle x^2-1\rangle = F[x]/\langle x+1\rangle\langle x-1\rangle \cong F[x]/\langle x+1\rangle \times F[x]/\langle x-1\rangle \cong F\times F.$$

אבל בחוג $F\times F$ יש שני אידאלים מקסימליים - $F\times\{0\}$ ו- $\{0\}\times F$, לכן הוא לא מקומי, ונקבל שהחוגים אינם איזומורפיים.