תזכורת:

הגדרה: תחום שלמות R נקרא תחום דדקינד אם:

א) R נתרי

ב) R סגור בשלמות (כל איבר ב-$\mathrm{Frac}R$ שהוא שלם מעל R מוכל ב-R)

ג) $k\text{-}\dim(R)=1$: כל אידאל ראשוני לא אפסי הוא מקסימלי. ויש אידאלים ראשוניים לא אפסיים. בפרט, R לא שדה

הערה: $\mathbb{Z}$ הוא תחום דדקינד

הגדרה: שדה k נקרא שדה מספרים אם $\mathbb{Q}\subseteq k$ וגם $\dim_{\mathbb{Q}} k$ סופי

למשל $\mathbb{Q}(\sqrt{d})$ הם שדות מספרים. $\mathbb{R},\mathbb{C}$ לא.

הגדרה: יהי k שדה מספרים. $O_k=\{\alpha\in k:$ α שלם מעל $\mathbb{Z}\}$

זה חוג, בנוסף $k=\mathrm{Frac}\,O_k$ (תרגיל)

טענה:

לכל שדה מספרים k, החוג O_k הוא תחום דדקינד?

עובדה:

יהי k שדה מספרים, יהי $n=\dim_{\mathbb{Q}}k$. אזי יש n איברים $\alpha_1,\dots,\alpha_n\in O_k$

כך ש O_k הוא $\mathbb{Z}$-מודול חופשי עם בסיס $\mathbb{Z}$

$O_k=\{b_1\alpha_1+\dots+b_n\alpha_n : b_i\in\mathbb{Z}\}$

וגם כל איבר של O_k ניתן לרשום באופן יחיד בצורה כזאת

הערה: אם $n=\dim_{\mathbb{Q}}k=2$, אזי $k=\mathbb{Q}(\sqrt{d})$, ואז α_1,α_2 הוא בסיס של O_k.

כאשר $\alpha_1=1$, $\alpha_2=\begin{cases}\sqrt{d} & d\equiv 2,3 \bmod 4\\ \frac{1+\sqrt{d}}{2} & d\equiv 1 \bmod 4\end{cases}$

הגדרה: יהיו $R\subset S$ חוגים חילופיים. S נקרא שלם מעל R $\Longleftrightarrow$ כל $s\in S$ שלם מעל R

דוגמא: O_k שלם מעל $\mathbb{Z}$

טענה:

יהי S שלם מעל R. יהי $0\neq P\lhd S$ אידאל ראשוני. אזי $P\cap R$ הוא אידאל ראשוני לא אפסי של R

הוכחה:

נשים לב כי R,P שניהם סגורים לחיבור וגם סגורים לכפל עם איברים של R.
לכן $P\cap R$ סגור לשתי הפעולות הללו, ולכן $P\cap R\lhd R$. יהיו $a,b\in R$ כך ש $ab\in P\cap R$
בפרט, $a,b\in S$ כך ש $ab\in P$. אך P ראשוני ולכן $a\in P\cap R$ או $b\in P\cap R$
לכן $P\cap R$ הוא אידאל ראשוני של R.
יהי $\alpha\in P$ ויהי $f_\alpha\in R[x]$ הפולינום המינימלי:

$$\alpha^n+r_{n-1}\alpha^{n-1}+\dots+r_1\alpha+r_0=0$$

$$r_0=-\alpha(r_1+r_2\alpha+\dots+\dots+r_{n-1}\alpha^{n-2}+r_n\alpha^{n-1})\in P$$

אבל $r_0\neq 0$, אחרת היינו יכולים לחלק ב-x ולקבל פול' ממעלה נמוכה יותר
עם שורש α. אז $0\neq r_0\in P\cap R$. ולכן $P\cap R\neq(0)$

טענה:

יהי k שדה מספרים. החוג O_k הוא תחום דדקינד.

הוכחה:

O_k הוא תת חוג של שדה ולכן אין בו מחלקי אפס (כי בשדה אין מחלקי אפס). לכן O_k
הוא תחום שלמות. לפי העובדה, O_k נוצר סופית מעל $\mathbb{Z}$. אבל $\mathbb{Z}$ נתרי, לכן כל
חוג נוצר סופית מעליו גם נתרי. יהי $(0)\neq P\lhd O_k$ אידאל ראשוני לא אפס.
לפי הטענה הקודמת, $P\cap\mathbb{Z}$ הוא אידאל ראשוני לא אפס של $\mathbb{Z}$. לכן $P\cap\mathbb{Z}=p\mathbb{Z}$
כאשר p ראשוני. זה אומר ש- $p\in P$. לכן לפי העובדה

$$pb_1\alpha_1+pb_2\alpha_2+\dots+pb_n\alpha_n\in P$$

לכל $b_i\in\mathbb{Z}$. לכן במנה O_k/p יש רק מספר סופי של מחלקות, כי כל איבר
$\beta\in O_k$ שקול מודולו P לאחד האיברים $c_1\alpha_1+\dots+c_n\alpha_n$, $(0\le c_i\le P-1)$

יש p^n איברים כאלה. אכן $\beta=\sum b_i\alpha_i$, יהי $c_i=b_i \bmod p$ לכל i

אז $\beta\equiv\sum c_i\alpha_i$ מודולו p. לכן O_K/p הוא תחום שלמות (כי p ראשוני)

סופי. כל תחום שלמות סופי הוא שדה (הוכחנו בעבר), לכן O_K/p שדה $\Leftarrow$ p מקסימלי

נשאר להוכיח כי O_K סגור בשלמות

תרגיל: יהיו $R\subset S\subset T$ חוגים חילופיים. נניח כי S שלם מעל R. יהי $t\in T$.

אזי t שלם מעל S $\Leftrightarrow$ t שלם מעל R

פתרון:

$(\Rightarrow)$ אם t שלם מעל R, אז הוא שורש של פולינום מתוקן עם מקדמים ב-R

אבל $R\subset S$ ולכן אותו פולינום הוא מתוקן ב-$S[x]$

$(\Leftarrow)$ נניח t שלם מעל S. זה אומר ש-$S[t]$ נוצר סופית כ-S מודול

יהי $S[t]=St_1+St_2+\dots+St_m$ $(t_1,\dots,t_m\in T)$. לכן

$t\in S[t] \Rightarrow t=s_1t_1+\dots+s_mt_m$

עבור $s_1,\dots,s_m\in S$ שהם כולם שלמים מעל R. לכן $R[s_i]$ נוצר סופית

כמודולים מעל R, לכן $R[s_1,\dots,s_m]$ גם R-מודול נוצר סופית. אז

$R[s_1,\dots,s_m]=Ru_1+\dots+Ru_l$

יהי $M\subset T$ ה-R-מודול הנוצר על ידי u_it_j $(1\le i\le l,\ 1\le j\le m)$ וגם על ידי 1.

M הוא R-מודול נאמן (בגלל איבר היחידה). M הוא R-מודול נוצר סופית. גם $t\in M$

כי $s_j=\sum r_{ij}u_i$, $r_{ij}\in R$ $\Leftarrow$ $t=s_1t_1+\dots+s_mt_m=\sum r_{ij}u_it_j\in M$.

∘∘∘ תרגיל: להשלים את ההוכחה

בחזרה ל-O_K. המצב שלנו הוא $\mathbb{Z}\subset O_K\subset K$, O_K שלם מעל $\mathbb{Z}$.

יהי $x\in K=\mathrm{Frac}\,O_K$ שלם מעל O_K. לפי הטענה הקודמת, x שלם מעל $\mathbb{Z}$, אז

$x\in O_K$ לפי ההגדרה של O_K. לכן O_K סגור בשלמות. ולכן O_K הוא תחום דדקינד

יהי R תחום דדקינד. לכל אידאל $I\trianglelefteq R$ הגדרנו

$$I^{-1}=\{x\in F=\mathrm{Frac}\,R : xI\subseteq R\}$$

לכל $a\in I$ $xa\in R$

כמובן $R\subseteq I^{-1}$ כי I אידאל. הוכחנו בסוף השיעור הקודם שלכל I מתקיים $R\subsetneq I^{-1}$

טענה:

יהי R תחום דדקינד. יהי $(0)\neq P\trianglelefteq R$ אידאל ראשוני לא אפסי אזי $PP^{-1}=R$

תזכורת:

$$PP^{-1}=\{a_1b_1+\dots+a_mb_m : a_i\in P,\ b_i\in P^{-1}\}$$

הוכחה:

ברור כי $PP^{-1}\subseteq R$ (לפי ההגדרה של P^{-1}, $a_ib_i\in R$). יותר מזה, PP^{-1} סגורה לחיבור וגם לכפל עם איברים של R (כי P סגור לכפל עם איברים של R)

לכן $PP^{-1}\trianglelefteq R$ אידאל (אולי לא אמיתי).

נשים לב כי $1\in R\subseteq P^{-1}$. לכן $P\subseteq PP^{-1}$ (לכל $x\in P$, $x=x\cdot 1\in PP^{-1}$).

נניח בשלילה כי PP^{-1} אידאל אמיתי. אך P מקסימלי, לכן $PP^{-1}=P$.

יהי $x\in P^{-1}\setminus R$, לפי הטענה האחרונה של השיעור הקודם, x כזה קיים. לכן, לכל $a\in P$ מתקיים $ax\in PP^{-1}=P$, לכן P סגור לכפל עם כל איבר של תת-החוג $R[x]\subseteq F=\mathrm{Frac}\,R$. לכן, ל-$P$ יש מבנה טבעי של $R[x]$-מודול. יותר מזה, R נתרי.

לכן האידאל P נוצר סופית (כ-R-מודול)

בנוסף, P הוא $R[x]$-מודול נאמן. כי:

$$\mathrm{Ann}_{R[x]}(P)=\{y\in R[x]\subseteq F : ay=0\ \ \forall a\in P\}$$

אבל $P\neq(0)$ וגם הכל קורה בתוך השדה F, שאין בו מחלקי אפס. לכן $\mathrm{Ann}_{R[x]}(P)=0$.

לכן P הוא $R[x]$-מודול נאמן. לפי אפיון השלמות מהרצאה קודמת, x שלם מעל R. אבל R סגור בשלמות $\Leftarrow$ $x\in R$ בסתירה להנחה כי $x\notin R$ ולכן $PP^{-1}=R$

משפט:

יהי R תחום דדקינד. יהי $(0)\neq I \trianglelefteq R$ אידאל לא אפסי. אזי I מתפרק למכפלה של אידאלים ראשוניים (לא אפסיים) $I=P_1P_2\cdots P_r$. הפירוק יחיד עד כדי שינוי סדר הגורמים.

הוכחה:

קיום של הפירוק:

יהי $(0)\neq I\trianglelefteq R$, יהי P אידאל מקסימלי כך ש $I\subseteq P$. נניח בשלילה שאין ל-I פירוק לגורמים ראשוניים. נניח ש-I אידאל מקסימלי ביחס לתכונה הזאת ($I\subsetneq J \Rightarrow J$ מתפרק) אפשר להניח את זה כי R נתרי.

תת-טענה: $IP^{-1}\subsetneq R$ $\left(IP^{-1}=\{a_1b_1+\dots+a_mb_m : a_i\in I ,\ b_i\in P^{-1}\}\right)$

הוכחה:

כמו בהוכחה הקודמת, $I\subseteq IP^{-1}\trianglelefteq R$. נניח בשלילה כי $IP^{-1}=R\underset{\text{הטענה הקודמת}}{=}PP^{-1}$

I לא מתפרק, לכן לא ראשוני. לכן $I\neq P$. נתבונן ב-

$IP^{-1}P=\{a_1b_1c_1+\dots+a_nb_nc_n \mid a_i\in I ,\ b_i\in P^{-1},\ c_i\in P\}$

$$P=RP\underset{IP^{-1}=R \text{ מההנחה}}{=}(IP^{-1})P=IP^{-1}P=I(P^{-1}P)=IR=I$$

קיבלנו $P=I$ בסתירה

לכן $IP^{-1}\subsetneq R$.

בחזרה להוכחת המשפט:

אז $IP^{-1}\trianglelefteq R$ אידאל אמיתי וגם $I\subsetneq IP^{-1}$ (מוכיחים $I\subsetneq IP^{-1}$ בדיוק כמו בהוכחה של הטענה הקודמת. אם $I=IP^{-1}$, יהי $x\in P^{-1}\setminus R$, אז I הוא $R[x]$-מודול נוצר...)

לפי המקסימליות של I, IP^{-1} מתפרק. מכפלה של ראשוניים: $IP^{-1}=Q_1\cdot\ldots\cdot Q_r$

$I=IR=IP^{-1}P=Q_1\cdot\ldots\cdot Q_rP$

גם מתפרק, בסתירה להנחה שיש אידאלים שלא מתפרקים