28/11/18

$\boxed{\text{הרצאה 6}}$

__פתרון שאלה מתרגיל בית__

① נסמן $R=\mathbb{F}_q[t_1,\dots,t_n]$ ויהי $\nu\geq 1$. נחשב את $\#\mathrm{Hom}(R,\mathbb{F}_{q^\nu})$.

__פתרון:__ $q^{\nu n}$ (בוחרים תמונות של x_i, מוגדר מ"ב —)

② נתבונן בהומומורפיזם - $\Psi:\mathrm{Hom}_{\mathbb{F}_q}(R,\mathbb{F}_{q^\nu})\to \mathrm{spec}R$ המוגדר ע"י $\Psi(\alpha)=\ker\alpha$.

נחשב את $\mathrm{Im}(\Psi)$.

__פתרון:__ $\mathrm{Im}\,\Psi=\{\mathfrak{p}\mid K(\mathfrak{p})\subseteq\mathbb{F}_{q^\nu}\}$

במובן של יש שיכון

כי אם $\mathfrak{p}\in RHS$, אז $\alpha:R\to R/\mathfrak{p}\subseteq\mathbb{F}_{q^\nu}$ ($R/\mathfrak{p}=K(\mathfrak{p})$). להיפך, נבחר α כך ש- $\mathfrak{p}=\ker\alpha$, אזי נקבל - $\mathbb{F}_{q^\nu}\supseteq\mathrm{Im}(\alpha)\cong R/\ker\alpha=K(\mathfrak{p})$.

③ בהינתן $\mathfrak{p}$ כך ש $K(\mathfrak{p})\subseteq\mathbb{F}_{q^\nu}$, נחשב את $\#\Psi^{-1}(\mathfrak{p})$.

__פתרון:__ אם $\ker\alpha=\ker\beta=\mathfrak{p}$ אזי $\mathrm{Im}\,\alpha\cong R/\mathfrak{p}\cong\mathrm{Im}\,\beta$ ($=K(\mathfrak{p})$)

ולכן יש $\sigma:K(\mathfrak{p})\to K(\mathfrak{p})$ כך ש- $\sigma\alpha=\beta$, וגם, $\sigma|_{\mathbb{F}_q}=id$. וכן, מאידך שקל ההיפך נכון ($\sigma\alpha=\beta\Leftarrow\ker\alpha=\ker\beta$)

$\sigma\in\mathrm{Gal}(K(\mathfrak{p})/\mathbb{F}_q)$ $\quad \#\Psi^{-1}(\mathfrak{p})=\#\mathrm{Gal}(K(\mathfrak{p})/\mathbb{F}_q)=[K(\mathfrak{p}):\mathbb{F}_q]$

④ תחשב את $\#\mathrm{Im}\,\Psi$.

__פתרון:__ נסמן $F(\nu)=\#\mathrm{Hom}(R,\mathbb{F}_{q^\nu})$. כלומר, $F(\nu)=q^{n\nu}$

נסמן -

$$f^*(\nu)=\#\{\alpha\in\mathrm{Hom}(R,\mathbb{F}_{q^\nu})\mid\mathrm{Im}(\alpha)=\mathbb{F}_{q^\nu}\}$$

מש"כ - $q^{n\nu}=f(\nu)=\sum_{d|\nu}f^*(d)\Rightarrow f^*(\nu)=\sum_{d|\nu}\mu(\frac{\nu}{d})q^{nd}$

ולכן,

$$\#\mathrm{Im}\,\Psi=\sum_{d|\nu}f^*(d)\frac{1}{d}=\sum_{d|\nu}\sum_{r|d}\mu\left(\frac{d}{r}\right)\frac{q^{rn}}{d}$$

__חוגי דדקינד__

הגדרנו תחום שלמות שהוא נקרא דדקינד אם -

* הוא נתרי.
* הוא סגור בשלמות.
* הוא DVR מקומית (כלומר לכל $\mathfrak{p}\in\mathrm{spec}R$, $R_{\mathfrak{p}}$ הוא DVR)

היינו בדרך להוכיח הטענה, שבתחום דדקינד לכל אידיאל יש פירוק יחיד למכפלת ראשוניים.

תזכורת: אם p הינו חוג B ~~A~~ ראשוני מקסימלי,
אז יש k_i כך ש-

$$\prod p_i^{k_i} = 0$$

ממשפט השארית הסיני, $B \cong \prod_{i=1}^{n} B/p_i^{k_i}$ (השתמשנו בכך שאם P,Q זרים אז גם P^{α}, Q^{β})

<u>מסקנה:</u> $\operatorname{Spec} B = \biguplus \operatorname{Spec}(B/p_i^{k_i}) = \{p_1,\dots,p_n\}$.

<u>הוכחה:</u> שכן כל $B/p_i^{k_i}$ מקומי עם אידיאל יחיד P_i. (האידיאלים היחידים שמוכלים בו הם שמכילים את $P_i^{k_i}$; אם $j\neq i$, אז $P_j \supseteq P_i^{k_i}$, אבל $P_j \supseteq P_j + P_i^{k_i} = B$) □

<u>למה:</u> יהי P מקסימלי בחוג B, ויהי k טבעי. אז העתק ההכלה $i: B \hookrightarrow B_P$ משרה איזומורפיזם,

$$B/P^k \xrightarrow{\sim} B_P/P^kB_P$$

<u>הוכחה:</u> יודעים כי $P^k = B \cap P^k B_P$ (למה?). לכן, $B/P^k \to B_P/P^kB_P$ העתקה מוגדרת היטב. (בשביל זה צריך $\subseteq$) וגם היא חח"ע (בשביל זה צריך $\supseteq$).
נשאר להראות שהיא על. ניקח $s \in B\setminus P$, אז $\frac{1}{s} \in B_P$.
מספיק להראות שקיים $r \in B$ כך ש- $\frac{1}{s} \equiv r \pmod{P^kB_P}$ ← למה?
P מקסימלי $\Leftarrow$ $P+Bs=B$ $\Leftarrow$ $P^k+Bs=B$. לכן, יש $a\in B$, $x\in P$, כך ש- $x+as=1$ $\Leftarrow$ $as\equiv 1 \pmod{P^k}$. כנדרש. □

<u>מסקנה:</u> יהי B דדקינדי, $0\neq P\in\operatorname{Spec}B$. אז לכל k טבעי, האידיאלים של B/P^k הם חזקות של P/P^k. יתר על P, הם כנ"ל.

<u>הוכחה:</u> B_P הוא DVR.
$\Leftarrow$ כל אידיאל של B_P הוא חזקה של PB_P, והם: כמוש'.
$\Leftarrow$ כנ"ל לגבי אידיאלים של B_P/P^kB_P.
לפי הלמה - סיימנו. □

משפט: יהי R חוג דדקינד ויהי $0\neq a\trianglelefteq R$ אידיאל של R. אז
יש פירוק יחיד (עד כדי סדר) $a=p_1^{k_1}\cdots p_n^{k_n}$ כאשר
p_i ראשוניים שונים; סופית.

יתר על כן, ניתן למצוא את הראשוניים של a
מתוך הפירוק הסופי של ראשוניים, והם $p_1,\dots,p_n$. וה-k_i
שמקיימים ש- $aR_{p_i}=p_i^{k_i}R_{p_i}$.

<u>הוכחה:</u>

*קיום – נסמן $B=R/a$. כיוון שהאידיאלים של B מתאימים
לאידיאלים (של R) המכילים את a, נקבל ש-B הוא ארטיני
ראשוני – מסקנה!

⇐ קיימים $\bar{p}_1,\dots,\bar{p}_n$ ראשוניים של B, ו- $e_1,\dots,e_n$, כך
ש- $0=\prod \bar{p}_i^{e_i}$ ב-B
וכן $\bar{p}_i$ הם כל הראשוניים של B. ⇐ למה?
מתאימים לראשוניים של R המכילים את a. נקבל –
$\prod p_i^{e_i}\subseteq a$ וכן $p_1,\dots,p_n$ הם הראשוניים של R המכילים
את a. נסמן –

$$B'=R/\prod p_i^{e_i}\cong\prod R/p_i^{e_i}$$

לפי המשפט האידיאלים של $R/p_i^{e_i}$ הם בדיוק $p_i^{f_i}/p_i^{e_i}$.
לכן התמונה של a ב-B', שנסמנה a', היא
$a'=\prod p_i^{k_i}/p_i^{e_i}$. ולכן $a=\prod p_i^{k_i}$ – והמשך.

*יחידות – $a=\prod q_j^{r_j}$, כאשר r_j. אם q_j לא אחד
מה-p_i, אז $a\not\subseteq q_j$ – סתירה.
(למה? זה סתם תכונה הקודמת.)
לכן נניח כי $q_1,\dots,q_n=p_1,\dots,p_n$ ונסמן $r_j=$.

$$p_i^{k_i}R_{p_i}=\prod p_l^{k_l}R_{p_i}=aR_{p_i}=q_i^{r_i}R_{p_i}$$

לכן $r_j=k_i$. □

<u>הערה:</u> יכולנו להסתכל ב- $R/p_i^{k_i+r_j}$.

<u>אפיון של חוגי דדקינד</u>

טענה: יהי R חוג דדקינד עם מס' סופי של ראשוניים.
אז R הוא PID.

הוכחה: יהיו $P_1,\dots,P_k$ הראשוניים מ-CRT, יש $x\in R$ כך ש- $x\in P_1\setminus P_1^2$, $x\notin P_2,\dots,P_k$. אזי,

$$\langle x\rangle=\prod P_i^{e_i}=P_1^{e_1}=P_1$$

$x\notin P_1^2$, $x\notin P_2,\dots,P_k$

אז P_1 ראשוני - ראשי. יהי π_i יוצר של P_i, ויהי $P_1^{e_1}\cdots P_k^{e_k}=a$ אידיאל. אזי:

$$a=\langle \pi_1^{e_1}\cdots\pi_k^{e_k}\rangle$$

אידיאל ראשי.

∎

משפט: יהי R תחום שלמות שאינו שדה. התנאים הבאים שקולים:

1. R דדקינדי.
2. המקומיים של R בכל P מקסימלי, ולכל $0\neq a\in R$ יש מספר סופי של ראשוניים המכילים את aR.
3. R נותרי, סגור בשלמות ומימד קרול 1.

הוכחה:

$1\Rightarrow 2$ - רק צריך להראות שלכל $a\neq 0$, a נמצא בלכל היותר מספר סופי של ראשוניים. נפרק $aR=P_1^{e_1}\cdots P_m^{e_m}$: a הוא נמצא רק בהם.

$2\Rightarrow 3$ - נניח q מקסימלי, $P\subsetneq q$ ראשוני, נראה ש-$P=0$. אחרי לוקליזציה ב-q, $PR_q\subsetneq qR_q$.

ראשוני שלמה? מקסימלי

לכן $PR_q=0 \Leftarrow P=PR_q\cap R=0$.

עכשיו נוכיח סגירות בשלמות.

למה כללית - יהי R תחום, אזי $R=\bigcap_{P\text{ maximal}} R_P$.

הוכחה: אכן, ברור ש- $\subseteq$ מתקיים, ולהיפך, יהי $x\in RHS$, $a=\{y\in R\mid xy\in R\}$. זה אידיאל. נניח P מקסימלי. $x\in R_P$ לכן $x=\frac{r}{s}$, $r\in R$, $s\notin P$. אזי, $s\in a$. אז, $a\not\subseteq P$. זה נכון לכל P מקסימלי $\Leftarrow$ $a=R$.

לפי הלמה, $R=\bigcap_{P\text{ maximal}} R_P$. לפי הנחה, R_P הוא DVR ולכן סגור בשלמות. לכן, R סגור בשלמות. (אם $x\in \mathrm{Frac}R$ שלם מעל R, אז x שלם מעל R_P לכל P, לכן $x\in R_P$ לכל P, לכן $x\in R$!)

נוכיח נותריות – נשתמש שוב גם בעוד טענה כללית:

למה כללית: יהי R תחום, $a\subseteq b$ אידיאלים. אם לכל P מקסימלי, $aR_P=bR_P$, אזי $a=b$.

הוכחה: יהי $\beta\in b$. נגדיר $c=\{y\in R\mid \beta y\in a\}$. לכל P מקסימלי, $\beta\in aR_P=bR_P$, לכן $\beta=\frac{\alpha}{y}$ עם $\alpha\in a$, $y\notin P$. לכן $y\in R$. לכל P יש $y\in c$ כך ש-$y\notin P$ $\Leftarrow$ $c=R$ ואז סיימנו.

טענה: תחת תנאי ②, אם $0\neq\mathfrak{a}\subseteq R$ אידיאל, $0\neq\alpha\in\mathfrak{a}$,
אז יש $\beta\in\mathfrak{a}$ כך ש- $\mathfrak{a}=\alpha R+\beta R$. בפרט R נותרי.

הוכחה: יהיו $P_1,\dots,P_n$ ~~הראשוניים~~ המקסימליים המכילים את $\mathfrak{a}$. נניח
ש- R_{P_i} הוא DVR, $\mathfrak{a}R_{P_i}=r_iR_{P_i}$, $r_i\in\mathfrak{a}$. נגדיר:

$$c=R\alpha+Rr_1+\dots+Rr_n\subseteq\mathfrak{a}$$

נראה שוויון מקומי בין $\mathfrak{a},c$. אם $P\neq P_i$, לכל i,

$$R_P\underset{?למה}{=}\alpha R_P\subseteq cR_P\subseteq\mathfrak{a}R_P\subseteq R_P$$

ולכן יש שוויון. אם $P=P_i$, אז,

$$r_iR_{P_i}\subseteq cR_{P_i}\subseteq\mathfrak{a}R_{P_i}\subseteq\mathfrak{a}R_{P_i}=r_iR_{P_i}$$

ושוב יש שוויון. □

(נסמן) CRT על האיברים. יש $\beta\in\mathfrak{a}$ כך ש- $\beta\equiv r_i\,(P_i^2)$.
נסמן - $d=R\alpha+R\beta\subseteq\mathfrak{a}$. נראה - $d=\mathfrak{a}$. די לבדוק
שוויון מקומי, אם $P\neq P_i$ - אותו דבר. נניח $P=P_i$.

$$r_i=\beta+(r_i-\beta)\in dR_{P_i}+P_i\mathfrak{a}R_{P_i}$$

$$\Leftarrow\quad dR_{P_i}+P_i\mathfrak{a}R_{P_i}\subseteq\mathfrak{a}R_{P_i}=r_iR_{P_i}\subseteq dR_{P_i}+P_i\mathfrak{a}R_{P_i}$$

$$\Leftarrow\quad \mathfrak{a}R_{P_i}=dR_{P_i}+P_i\mathfrak{a}R_{P_i}$$

לפי נקיימה, $N\subseteq M$, $M=N+P_iM\Rightarrow M=N$, לכן,
$\mathfrak{a}R_{P_i}=dR_{P_i}$ וסיימנו את ③ ⇐ ②.

<u>③ ⇐ ①</u>: P ראשוני $0\neq$ הוא מקסימלי ב- R, אז גם ב- R_P,
PR_P הוא הראשוני $0\neq$ היחיד. גם R_P נותרי ולכן
בשלמות נוכל להגביל ש- R_P - PID, לכל P מקסימלי.

טענה: יהי (A, m) חוג מקומי, תחום שלמות (נותרי), וכי m הראשוני $\neq 0$ היחיד. אז A הוא PID.

הוכחה: נבחר $a \in m \neq 0$, נסתכל על $M = A/aA$, ונו-
$m \in M$, $ann(m) = \{x \in A \mid xm = 0\} \supseteq aA$

-אידיאל
בקבוצת אידיאלים אלו יש מקסימלי, מנותריות, נניח q,
כסימון -

$$q = ann(m) = ann(b + aA) = \{c \in A \mid cb \in aA\}$$
$m = b + aA$ - ?!

כיוון ש- $q \neq 0$ נראה ש q ראשוני ⇒ $q = m$.
נניח, $xy \in q$, $y \notin q$ ⇒

$$x(yb + aA) = xy(b + aA) \subseteq aA$$

$$\Rightarrow ann(b + aA) \subsetneq ann(yb + aA) \ni x$$
סתירה למקסימליות ⇒ $q = m$.

משמעות הכוונה - $Ab \not\subseteq aA$, $mb \subseteq aA$. נרצה להוכיח $m = \frac{a}{b}A$. נסמן $\pi = \frac{a}{b}$. שים לב, כי $\frac{b}{a} = \pi^{-1} \notin A$,
אך $m\pi^{-1} \subseteq A$. אם $m\pi^{-1} \subset m$ אז ההעתקה $m \to m$
של כפל ב-π^{-1} מגדיר A ⇒ מראה ש-A סגורה בשלמות, $\pi^{-1} \in A$ וזו סתירה. אז $m\pi^{-1} = A$ כפי שרצינו.
ניקח $0 \neq a \in A$ כלשהו, $\pi \cdot a \subseteq \pi$ ⇒ $a \subseteq \pi^{-1} a$.
נקבל סדרה עולה ממש של A-מודולים,
$$a \subseteq a\pi^{-1} \subsetneq a\pi^{-2} \subsetneq \dots$$
כי אם $a\pi^{-i} = a\pi^{-i-1}$ אז $a = a\pi^{-1}$ וזה לא יכול
שאז כמו קודם, π^{-1} שלם ⇒ $\pi^{-1} \in A$ וזו סתירה.
כיוון ש-A נותרי ה.נ.מ. $a\pi^{-1} \not\subseteq A$. ונקבל: k מקסימלי
כך ש- $a\pi^{-k} \subseteq A$. אז $a\pi^{-k} \not\subseteq m$ ⇒ $a\pi^{-k} = A$ ⇒ $a = \pi^k A$ □
⇒ A הוא PID.