הרצאה 22

משפט (הלמה של הנזל). יהי R תחום שלמות מקומי (מקומי = יש רק אידיאל מקסימלי אחד) עם אידיאל מקסימלי I. נניח כי R שלם עבור הטופולוגיה ה-I-אדית וכי $\bigcap_{n=1}^{\infty} I^n=(0)$.

נניח כי I אידיאל ראשי. יהי $K=R/I$ שדה השאריות. (בנוסף, יש העתקה טבעית

$$R[x]\longrightarrow K[x]$$
$$(\ f\longmapsto \bar{f}$$

יהי $f\in R[x]$ פולינום כך ש- $f\notin I[x]$, כלומר $\bar{f}\neq 0$. (נשים לב שמתקיים $\deg\bar{f}\le\deg f$) נניח כי $\bar{f}=\gamma\delta$, כאשר $\gamma,\delta\in K[x]$ פולינומים זרים ($K[x]$ תחום אוקלידי, לכן גפיי ואפשר לדבר על איברים זרים). יהי $\deg\gamma=r$, $\deg\delta=n-r$. אזי קיימים $g,h\in R[x]$ כך ש-

1) $f=gh$

2) $\bar{g}=\gamma,\ \bar{h}=\delta$

3) $\deg g=r=\deg\gamma$.

<u>מסקנה</u> ב- $\mathbb{Z}_p$ יש $p-1$ שורשים $(p-1)$-יים שונים של 1.

<u>הוכחה</u> $\mathbb{Z}_p$ שלם לטופ' ה-$p\mathbb{Z}_p$-אדית. נתבונן בפולינום $f(x) = x^{p-1}-1$.

$$K = \mathbb{Z}_p / p\mathbb{Z}_p = \hat{R}/\hat{I} \simeq R/I = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

החבורה הכפלית $\mathbb{F}_p\setminus\{0\} = \mathbb{F}_p^*$ הינה מסדר $p-1$.

לכן, $\alpha^{p-1}=1$ לכל $\alpha\in\mathbb{F}_p^*$. לכן,

$$\bar{f} = \prod_{\alpha\in\mathbb{F}_p^*}(x-\alpha) \in \mathbb{F}_p[x]$$

כל הגורמים הלינאריים זרים, אז לפי (כמה חזרות על) הלמה של הנזל ניתן להרים את הפירוק:

$$f = \prod_{i=1}^{p-1}(x-c_i)$$

(<u>שאלה</u> מדוע ניתן לומר שהגורמים מתוקנים?)

מקבלים שורשים $c_1, c_2, \dots, c_{p-1} \in \mathbb{Z}_p$ של הפולינום

$x^{p-1}-1$, כלומר שורשים $(p-1)$-יים של 1.
הרדוקציות שייכים למחלקות שונות של $\mathbb{F}_p$.

<u>מסקנה</u> לכל מחלקה לא-אפסית של $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$
יש נציג יחיד שהוא שורש $(p-1)$-י של 1.
נקרא לו $[x]$. אם נגדיר $[0]=0$.
קיבלנו בחירה קנונית של נציגים של מחלקות, קבוצת הנציגים סגורה לכפל:

$[x]\cdot[y]=[xy]$ לכל $x,y\in\mathbb{F}_p$.
הרמוני של Teichmüller.

<u>הערות על הלמה של הנזל</u> לא חייבים להניח כי I ראשי, אבל אין צורך להניח כי המקדם המוביל של f הוא הפיך, כלומר $(\deg f = \deg \bar{f})$.

<u>הוכחה</u> הרעיון הוא לבנות את g,h על ידי קירובים חוזרים. כלומר, נבנה סדרות
$g_0,g_1,g_2,\ldots \quad h_0,h_1,h_2,\ldots \in R[x]$

כך שלכל $0 \le n$ מתקיים:

1) $f - g_n h_n \in I^{n+1}[x]$

2) $\bar{g}_n = \gamma$ וגם $g_n - g_{n-1} \in I^n[x]$.

3) $\bar{h}_n = \delta$ וגם $h_n - h_{n-1} \in I^n[x]$.

4) $\deg g_n = r$, $\deg h_n \le (\deg f) - r$.

אם נמצא סדרות כאלו, אזי לכל k, הסדרה של המקדמים של x^k ב- g_n תהיה סדרת קושי של איברים של R, לכן ניתן להגדיר פולינום גבולי $g = \lim_{n\to\infty} g_n$ - כמובן $\deg g = r$. באופן דומה מגדירים גבול $h = \lim_{n\to\infty} h_n$. (זה המקום היחיד בהוכחה בו נשתמש בהנחה כי R שלם). כמובן $\bar{g} = \gamma, \bar{h} = \delta$. בנוסף

$$f - gh \in \bigcap_{n=1}^{\infty} I^n[x] = (0)$$ לפי 1)

נשאר לבנות את הסדרות $\{g_n\}, \{h_n\}$.

יהיו $g_0,h_0\in R[x]$ הרמות כלשהן של γ,δ

($\bar{g}_0=\gamma,\ \bar{h}_0=\delta$) כך ש- $\deg g_0 = r$

$\deg h_0 = (\deg f) - r$.

נשים לב כי המקדם המוביל של g_0 הינו

הפיך ב-R, כי $\deg \bar{g}_0 = \deg g$.

נעשה אינדוקציה על n. נניח שמצאנו

g_{n-1}, h_{n-1} עם התכונות הנ"ל. רוצים לבנות

g_n, h_n. הנחנו כי γ,δ זרים. לכן,

($K[x]$ תחום ראשי) קיימים $\alpha,\beta\in K[x]$ כך

ש- $\alpha\gamma+\beta\delta=1$. תהיינה $a,b\in R[x]$ הרמות

של α,β מאותן המעלות. לכן

$$ag_0+bh_0-1\in I[x]$$

הנחנו כי I ראשי, נבחר $\pi\in I$ יוצר.

לפי האינדוקציה, $f-g_{n-1}h_{n-1}\in I^n[x]$. אך

$I^n=(\pi^n)$, לכן כל מקדם של $f-g_{n-1}h_{n-1}$

מתחלק ב-π^n. לכן קיים $f_n\in R[x]$

כך ש- $f - g_{n-1}h_{n-1} = \pi^n f_n$.

אם I לא היה ראשי לא היינו יכולים לבחור את f_n. נשים לב כי

$$a g_{n-1} + b h_{n-1} - 1 \in I[x]$$

$$a g_{n-1} f_n + b h_{n-1} f_n - f_n \in I[x] \triangleleft R[x]$$

<u>רעיון</u> ננסה

$$g_n = g_{n-1} + \pi^n b f_n$$

$$h_n = h_{n-1} + \pi^n a f_n$$

ברור כי $g_n - g_{n-1} = \pi^n b f_n \in I^n[x]$ 2) מתקיים

באופן דומה, $h_n - h_{n-1} = \pi^n a f_n \in I^n[x]$ 3) מתקיים.

בנוסף,

$$f - g_n h_n =$$

$$\underbrace{f - g_{n-1}h_{n-1} - \pi^n\left(b f_n h_{n-1} + a f_n g_{n-1}\right)}_{\underbrace{\underbrace{\pi^n}_{\in I^n} f_n \left(\underbrace{1 - b h_{n-1} - a g_{n-1}}_{\in I[x]}\right)}_{\in I^{n+1}[x]}} - \underbrace{\pi^{2n} a b f_n^2}_{\in I^{n+1}[x]}$$

לכן 1) גם מתקיים.

הבעיה היא שיכול להיות $\deg bf_n > \deg g_{n-1}$,

לכן $\deg g_n > \deg g_{n-1}$ (המקדמים העליונים של g_n ויחלקו ב-π^n)

נחלק את bf_n ב-g_0 עם שארית על ידי חילוק אוקלידי:

$$bf_n = g_0 q_n + p_n$$

(ב-$R[x]$ לא בהכרח אחוב אוקלידי או אפילו חפ"י, אבל באלגוריתם הידוע לחילוק פולינומים צריך לחלק רק במקדם המוביל של g_0, והמקדם הזה הפיך, לכן עובדים.)

עכשיו, $\deg p_n < \deg g_0 = r$. אני רוצה להגדיר $g_n = g_{n-1} + \pi^n p_n$. מתאים (2),(4).

איך להגדיר h_n?

$$f_n - (g_0 a + h_0 b) f_n \in I[x]$$

$$f_n - g_0 a f_n - h_0 (g_0 q_n + p_n) \in I[x]$$

$$f_n - g_0 (a f_n + h_0 q_n) - h_0 p_n$$

יהי $\tilde{q}_n \in R[x]$ הפולינום שמתקבל מ- $af_n + h_0 q_n$

אחרי שמוחקים את כל המונומים עם

מקדמים ב-I. ברור כי

$$f_n \equiv g_0(af_n + h_0 q_n) + h_0 p_n \mod I[x]$$

$$\equiv g_0\tilde{q}_n + h_0 p_n \mod I[x] \quad (*)$$

ברור כי $\deg f_n \le \deg f$

(אכן [illegible] $f_n = f - \underbrace{g_{n-1}h_{n-1}}_{\deg = \deg f}$)

בנוסף, $\deg h_0 p_n = \underbrace{\deg h_0}_{\le \deg f - r} + \underbrace{\deg p_n}_{< r} < \deg f$

לכן, $\deg \overline{g_0 \tilde{q}_n} \le \deg f$

$$\deg \overline{g_0 \tilde{q}_n} = \deg g_0 \tilde{q}_n$$

כי המקדמים המובילים של g_0 ושל $\tilde{q}_n$ הפיכים. לכן $\deg \tilde{q}_n \le \deg f - r$.

נגדיר $g_n = g_{n-1} + \pi^n p_n$

$h_n = h_{n-1} + \pi^n \tilde{q}_n$

ברור כי 2,3,4 מתקיימים. נשאר

להוכיח את 1)

$$f - g_n h_n = f - g_{n-1} h_{n-1} - \pi^n (p_n h_{n-1} + g_{n-1}\tilde{q}_n) - \pi^{2n} p_n \tilde{q}_n =$$

$$\underbrace{\pi^n}_{\in I^n}\underbrace{(f_n - p_n h_{n-1} - g_{n-1}\tilde{q}_n)}_{\in I[x] \text{ לפי (*)}} - \underbrace{\pi^{2n} p_n \tilde{q}_n}_{\in I^{2n}[x] \subseteq I^{n+1}[x]}$$

לכן $f - g_n h_n \in I^{n+1}[x]$ כמו שרצינו.

<u>פואנטה</u> בנייה של g,h באופן מפורש מאוד. האלגוריתם בהוכחה נוח מאוד ליישום במחשב.