(שאלה: מדוע ניתן להניח שהגורמים מתוקנים?)

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

את ההוכחה:

כל הגורמים הלינאריים כאלה. אך, לפי (כמה תצרוכת על) הלמה של הנגלה, ניתן להניח

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

כאלו.

בתכורה הכללית $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ כ"ו מסדר $p-1$. לכן $a^{p-1} = 1$ לכל $a \in \mathbb{F}_p^*$.

$$k = \mathbb{Z}_p[x]/p\mathbb{Z}_p[x] \simeq \hat{R}/\hat{I} = \mathbb{Z}[x]/\mathbb{Z} \times R/I = \mathbb{F}_p$$

$\mathbb{Z}_p$ שלם לכו, ה-$p\mathbb{Z}_p$-יחידי. לתכונן בפלינום $f(x) = x^{p-1} - 1$

טכניקה:

ב-$\mathbb{Z}_p$ יש $p-1$ שורשים $(p-1)$-יים של 1.

תוצאה:

1) $hg = f$

2) $g = \bar{h}$, $r = \bar{g}$

3) $\deg r = \deg g$

ואפשר לבחר את גורמים פרים). $r = \deg g$, $n-r = \deg h$. וכי $h \in R[x]$, g כך ש:

נניח כי: $g r = \bar{f}$, כאשר $g, r \in k[x]$ פולינומים פרים ($k[x]$ תחום אוקלידי, לכן תפ"י,

כי: $f \in R[x]$ פולינום כך ש $f \notin I[x]$. כלומר, $\bar{f} \neq 0$. (נשים לב שיתכן $\deg f \geq \deg \bar{f}$)

כאשי. כי: $k = R/I$ שדה השאריות. $\left(\begin{array}{c} \text{תכורת, יש התאמה טבעית} \\ f \longmapsto \bar{f} \end{array} \; k[x] \leftarrow R[x] \right)$

כי: R תחום שלמות אקוא', (אקוא' = יש רק ויכוח אקסיומטי אחד) ו$I \neq R$ אידאל אקסיומטי.

I. נניח כי: R שלם שהכור הטופולוגיה ה-I אדית וכי $\bigcap_{n=1}^{\infty} I^n = (0)$. נניח כי: I אידאל

משפט (הלמה של הנגלה):

מקבלים שורשים $c_1, c_2, \dots, c_{p-1} \in \mathbb{Z}_p$ של הפולינום $x^{p-1} - 1$. כלומר, שורשים $(1-p)$-ים של 1. הרקורסיות שייכות לאיברים שונים של $\mathbb{F}_p$.

מסקנה:

לכל איבר לא אפסי x של $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}$ יש בדיוק שורש $(1-p)$-י של 1.

נקרא לו $[x]$. הוא נקבע ביחידות כאיבר הקבוצתי של נציגים של איברי,

קבוצת הנציגים סגורה לכפל. $[fx] = [f]\cdot[x]$ לכל $f, x \in \mathbb{F}_p$

(הכוונה של Teichmüller)

הערות על הלמה של הנזל:

לא חייבים להניח כי I ראשי, אבל אז צריך להניח כי המקדם המוביל של f הוא הפיך.

כלומר, $\deg \bar{f} = \deg f$

הוכחה של המשפט:

בכדי הוא להניח סדרות של h, g אלא יכי קירובים מועילים. כלומר נבנה סדרות

$g_0, g_1, g_2, \dots \in R[x]$ $\quad h_0, h_1, h_2, \dots$

כך שלכל n מתקיים:

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

2) $g_n = \bar{g}$ ו$\deg g_n = r$ $\quad g_{n+1} - g_n \in I^n[x]$

3) $h_n = \bar{h}$ ו$\deg h_n \le \deg f - r$ $\quad h_{n+1} - h_n \in I^n[x]$

4) $\deg g_n = r$;

נראה שסדרות כאלה אכן קיימות, כי הסדרה של המקדמים של x^k ב-g_n תהיה סדרת קושי של איברים של R. לכן ניתן להגדיר "פולינום גבול" $g = \lim_{n\to\infty} g_n$. כאשר $\deg g = r$.

באופן דומה נגדיר גבול $h = \lim_{n\to\infty} h_n$. (לכה המקום היחיד בהוכחה בו נשתמש בהנחה כי R שלם). כאשר $f = \bar{h}, x = \bar{g}$. בנוסף, $f - gh \in \bigcap_{n=1}^{\infty} I^n = (0)$. לפי (1) נשאר להבנות את הסדרות g_n, h_n.

$\deg g_0 = r$

$\deg h_0 = \deg f - r$

נשים לב כי המקדם המוביל של g_0 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. נרצה למצוא g_n, h_n.

הנחנו כי g, x זרים. לכן, ($K[x]$ תחום כאשי) קיימים $\alpha\beta \in K[x]$ כך ש $1 = \alpha g + \beta x$

תה"נ $a, b \in R[x]$ הדרושים של α, β מאותן המעלות. לכן $1 - bh_0 - ag_0 \in I[x]$.

הנחנו כי I ראשי. נבחר $I \ni \pi$ יוצר. לפי האינדוקציה, $f - g_{n-1}h_{n-1} \in I^n[x]$. אבל

$(\pi^n) = I^n$ לכן כל מקדם של $f - g_{n-1}h_{n-1}$ מתחלק ב-π^n לכן קיים $f_n \in R[x]$ כך ש:

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

אם I לא היה ראשי לא היינו יכולים לבנות את f_n

נשים לב כי $1 - ah_{n-1} - bg_{n-1} \in I[x] \Rightarrow f_n - af_n h_{n-1} - bf_n g_{n-1} \in R[x] \triangleright I[x]$

---

* כלל:

נגסה: $g_n = g_{n-1} + \pi^n b f_n$, $h_n = h_{n-1} + \pi^n a f_n$

נכון כי $f_n - af_n h_{n-1} - bf_n g_{n-1} \in I^n[x]$. במילים קומה $f_n \in I^n[x]$ $f - g_{n-1}h_{n-1} = \pi^n a f_n$. כנ"ש את הנ"מ:

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

$$\pi^n f_n (1 - bh_{n-1} - ag_{n-1}) \in \pi^n I \cdot I[x] = I^{1+n}[x]$$

ולכן יש (1) מתקיים

הבעיה היא שיכול להיות $\deg g_{n-1} + \deg f_n$ $\deg$

לכן $\deg g_n < \deg g$ (במקביל הגדלנו את g_n שתלקו ב-π^n)

נחלק את f_n ב-g_0 עם שארית על ידי תלוק אוקלידי. $f_n = q_n g_0 + h_n$

($R[x]$ לא בהכרח תחום אוקלידי, או אפילו ת.ק', אבל בגלגורית היבוץ למילוק פול.נומ

בונים את g_n באופן אינדוקטיבי. האלגוריתם בהוכחה נותן אותו ל"שום מחשב

כיוון ש:

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

$$= \tilde{q}_n p_{n_2} \pi - (r_n \tilde{q}_{r-n} g + r_{-n} h_n p_n) u_n \pi - r_{-n} h g - f = r_n h_n g - f$$

$$= \underbrace{\tilde{q}_n p_{n_2} \pi}_{\in I^{n+1}[x] \ni [x] I^{n_2}} - \underbrace{(r_n \tilde{q}_{r-n} g - r_{-n} h_n p_n - r_f) u_n \pi}_{\in I[x] \text{ ע"י } (*)}$$

נשאר להבהיר את (1):

$r_n = r_f \deg p > r_n \deg p$. נרצה להגדיר $g_n = g_{n-1} + \pi^{n_1} p_n$. צ"ל את"מ

אכן $r = r_f \deg p > r_n \deg p$. נרצה להגדיר $g_n = g_{n-1} + \pi^{n_1} p_n$. צ"ל את"מ

$((4)', (2))$

איך נגדיר h_n?

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

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

$$r_f - (r_n h_0 + a f_n + h_0 q_n) g_0 - r_f$$

כך ש: $\tilde{q}_n \in R[x]$ כפולינום שמתקבל מ- $r_n h_0 + a f_n + h_0 q_n$ אחרי שאומרים זה כל המונומים עם מקדמים ב- I. ברור כי

$$(*) \quad f \equiv g_0 (a f_n + h_0 q_n) + h_0 p_n \bmod I[x] \equiv g_0 \tilde{q}_n + h_0 p_n \bmod I[x] \equiv r_f h_0 + r_f p_n \bmod I[x]$$

ברור גם כי $\deg f_n \le \deg f$ (אכן $f_n \pi^n = f - \underbrace{r_{-n} g_{-n}}_{\deg = \deg f}$)

בנוסף, $\deg f > \underbrace{\deg p_n}_{>1} + \underbrace{\deg h_0}_{< \deg f - 1} = \deg r_f h_0 p_n$

לכן, $\deg f \ge \deg \tilde{q}_n g = \deg \tilde{q}_n + \deg g$ כי המקדמים המוביליים של g_0 ושל $\tilde{q}_n$ הכפיים.

לכן $\deg \tilde{q}_n \le \deg f - r$

לגדיר $g_n = g_{n-1} + r_n \pi^n$, $h_n = h_{n-1} + \tilde{q}_n \pi^n$. ברור כי $1, 3, 4$ את"מ.

נשאר להבהיר את (1):