

אלגברה ב2

© ארזים

6 ביוני 2017

1 חבורות גלואה

למה 1.1 יהי $f \in \mathbb{Z}[x]$ מתוקן אי פריק, ונסמן את שורשיו $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ נסמן $R = \mathbb{Z}[\alpha_1, \dots, \alpha_n]$. יהי p ראשוני, ויהי P אידאל ראשוני של R שמכיל את p . נניח בנוסף כי $p \nmid \Delta f$. אזי יש $\sigma \in \text{Gal}(f)$ כך שמתקיים

$$\sigma(x) = x^p (P)$$

לכל $x \in R$.

מסקנה 1.2 יהי f אי פריק מתוקן מעל \mathbb{Z} , ויהי p ראשוני כך שמודולו p הפולינום f מתפרק בתור

$$\bar{f} = g_1 \cdots g_k$$

כאשר g_i אי פריקים שונים מדרגה d_i . אז בתוך $\text{Gal}(f)$ יש איבר עם מבנה מעגלים (d_1, \dots, d_k) .

הוכחה: נניח כי שורשי f הם $\alpha_1, \dots, \alpha_n$, והרוקציות שלהם מודולו P (האידאל) הן $\bar{\alpha}_i$. הפירוק של f מודולו p הוא

$$\bar{f} = g_1 \cdot g_2 = \left(\prod_{i=1}^t (x - \bar{\alpha}_i) \right) \left(\prod_{i=t+1}^n (x - \bar{\alpha}_i) \right)$$

נרצה למצוא $\sigma \in \text{Gal}(f)$ עם מבנה מעגלים $(t, n-t)$ (הנחנו לשם הנוחות $k=2$). ניקח את σ שמובטח לנו מהלמה. נבחין כי

$$\sigma^t(\alpha_1) \equiv \text{Frob}(\alpha_1) \equiv \alpha_1 (P)$$

■ ומכאן $\sigma^t(\alpha_1) = \alpha_1$ באופן דומה נקבל את המעגל השני.

דוגמה נסתכל על $x^4 - x - 1$. הוא אי פריק מודולו 2, ולכן יש בחבורת גלואה מעגל באורך 4. כמו כן, הדיסקרימיננטה אינה ריבוע, ולכן $\text{Gal}(f) \neq A_4$, ועל כן $|\text{Gal}(f)| = 24$. נסתכל מודולו 7. הפירוק הוא מהצורה של פולינום לינארי כפול פולינום ממעלה 3. לכן יש בחבורת גלואה מעגל בגודל 3. לכן החבורה היא S_4 .

דוגמא נסתעל על $x^4 + 8x + 12$. מודולו 5 ומודולו 17 הפירוקים הם מהצורה $(2, 2)$, $(1, 3)$ בהתאמה. לכן f אי פריק בהכרח (כי יש סוגי פירוק שונים). מכאן $4 \mid \text{Gal}(f)$. הדיסקרימיננטה היא ריבוע, ולכן החבורה היא תת חבורה של A_4 . אבל ראינו שחייב להיות איבר מסדר 3 - לכן $\text{Gal}(f) = A_4$.

דוגמא $x^5 - x - 1$. נשים לב שאם α שורש שלו בתוך $\overline{\mathbb{F}}_p$, אזי $\alpha^5 = \alpha + 1$, וברור שרק $\alpha^{5^5} = \alpha$ (כלומר יש לו חמישה צמודי גלואה). לכן הפולינום אי פריק. מודולו 2, טיפוס הפירוק הוא $(2, 3)$, ולכן מחלק את הסדר של G - 5 מחלק, וגם 6 מחלק. הדיסקרימיננטה אינה ריבוע, ולכן נותרנו עם הסדרים 30, 120. נשים לב שאין תת חבורה מסדר 30 בתוך S_5 . לכן החבורה היא S_5 . נשים לב שזה אומר שהמשוואה לא פתירה.

טענה 1.3 לכל n יש פולינום $f_n(x) \in \mathbb{Z}[x]$ עם $\text{Gal}(f/\mathbb{Q}) = S_n$.

הוכחה: נשתמש בטענת עזר:

טענה 1.4 תת חבורה של S_n שמכילה חילוף, מעגל באורך n ומעגל באורך $n - 1$ היא כל S_n .

נשאר את ההוכחה כתרגיל בתורת החבורות. כעת, נחפש ראשוניים שיראו לנו על תמורות כאלו. ניקח ראשוניים p_1, p_2, p_3 עם $p_3 > n$. ניקח פולינום $f_3 \in \mathbb{Z}/p_3\mathbb{Z}[x]$ עם טיפוס פירוק $(2, 1, 1, \dots, 1)$, ובדומה נבחר f_2 עם טיפוס פירוק $(n - 1, 1)$ מעל p_2 ועוד f_1 אי פריק מודולו p_1 . כעת, ממשפט השאריות הסיני, יש פולינום $f \in \mathbb{Z}[x]$ עם $f \equiv f_i \pmod{p_i}$. ■