

## אלגברה ב2

© ארזים

25 באפריל 2017

**הגדרה 0.1** יהי  $K$  שדה ויהי  $f \in K[x]$  אי פריק ומתוקן.  $f$  ייקרא פריד אם מתקיימות התעונות השקולות הבאות:

1.  $\gcd(f, f') = 1$ .

2. לכל שדה הרחבה  $E/K$ , אין שורש כפול של  $f$  בתוך  $E$ .

3. מתפרק למכפלת גורמים לינאריים שונים מעל  $\bar{K}$ .

**הגדרה 0.2** אם  $E/K$  הרחבה,  $\alpha \in E$  אלגברי מעל  $K$ , אזי  $\alpha$  נקרא פריד אם הפולינום האי פריק שלו פריד.

**הגדרה 0.3** הרחבה אלגברית  $E/K$  נקראת פרידה אם כל  $\alpha \in E$  פריד מעל  $K$ . כאשר  $E/K$  סופית. פרידות שקולה לכך שמתקיים

$$[E : K]_s = [E : K]$$

**טענה 0.4**  $f$  אינו פריד אם ורק אם  $\text{char}K = p > 0$ , ויש פולינום  $g \in K[x]$  כאשר  $f(x) = g(x^p)$ .

**הוכחה:** נניח כי לא פריד, כלומר  $\gcd(f, f') \neq 1$ . אזי  $\gcd(f, f') = f$ , כי הוא מחלק את  $f$ , שהוא אי פריק. נובע כי  $f' \mid f$ , ולכן  $f' = 0$  - כי הנגזרת ממעלה קטנה מאשר  $f$ . לכן ברור כי המצויין הוא  $p > 0$ , וכל מקדמי הנגזרת מתחלקים בו - כלומר כל המונומים של  $f$  הם חזקות של  $x^p$ . לכן  $f(x) = g(x^p)$ . להפך, אם  $f(x) = g(x^p)$ , אזי  $f'(x) = 0$ , ולכן  $\gcd(f, f') = f \neq 1$  ולכן הפולינום לא פריד. ■

**הגדרה 0.5** שדה ייקרא מושלם אם כל הרחבה אלגברית שלו הינה פרידה.

**טענה 0.6** שדה  $K$  הוא מושלם אם ורק אם  $\text{char}K = 0$ , או  $\text{char}K = p > 0$  ולכל  $x \in K$  יש  $y \in K$  עם  $y^p = x$ .

**הוכחה:** נניח את צד שמאל. אם  $\text{char}K = 0$ , זה נובע מהטענה הקודמת. נניח את התנאי השני. יהי  $f \in K[x]$  שאינו פריד (בשליה). לפי הטענה, יש  $g \in K[x]$  עם

$$f(x) = g(x^p) = \sum_{i=0}^n a_i x^{ip} = \sum_{i=0}^n (b_i)^p (x^i)^p = \left( \sum_{i=0}^n b_i x^i \right)^p$$

בסתירה לאי פריקות של  $f$ . לכן כל הפולינומים מעל  $K$  פרידים, ולכן הוא מושלם. בכיוון השני, נניח כי  $K$  מושלם וכי  $\text{char}K = p > 0$  (אם המצויין הוא 0 סיימנו). יהי  $a \in K$ , ונמצא  $b$  עבורו  $b^p = a$ . נגדיר

$$f(x) = x^p - a$$

יהי  $t$  שורש של  $f$ , כלומר  $t^p = a$ . לכן

$$f(x) = x^p - t^p = (x - t)^p$$

מכאן שאם  $g$  גורם אי פריק כלשהו של  $f$ , אז מצד אחד, כל שורשי  $g$  שונים (מפרידות - כי  $K$  מושלם), ומצד שני,  $g(x) = (x - t)^r$  עבור  $r \leq p$ . בסך הכל נקבל כי  $r = 1$ , כלומר  $g(x) = x - t$ , ובפרט  $t \in K$ . לכן סיימנו. ■

**הגדרה 0.7** בהנתן משפחת פולינומים  $\{f_i\}_{i \in I} \subseteq K[x]$ , עבור שדה  $K$  כלשהו, מגדיר את שדה הפיצול של המשפחה להיות השדה הנוצר על ידי שורשי  $\{f_i\}_{i \in I}$  בתוך  $\bar{K}$ .

**הגדרה 0.8** הרחבה אלגברית  $E/K$  תקרא נורמלית אם מתקיימות התכונות השקולות הבאות:

1.  $E$  הינו שדה פיצול.

2. כל  $f \in K[x]$  אי פריק שיש לו שורש בתוך  $E$  מתפצל לחלוטין מעל  $E$ .

3. לכל  $\bar{E}$  ולכל שיכון  $\sigma$  של  $E$  מעל  $K$  לתוך  $\bar{E}$ , מתקיים

$$\sigma(E) \subseteq E$$

**הערה 0.9**  $K(\alpha)/K$  פרידה אם ורק אם  $\alpha$  פריד מעל  $K$ .

**הערה 0.10** יהי  $\alpha$  אלגברי מעל  $K$ , ונסמן  $f = \text{irr}(\alpha, K)$ . אזי  $K(\alpha)/K$  נורמלית אם ורק אם כל שורש של  $f$  הינו פולינום במשתנה  $\alpha$  עם מקדמים מתוך  $K$  (בתוך סגור אלגברי נתון  $\bar{K}$ ).

**דוגמאות** אם  $K$  שדה עם  $\text{char}K \neq 2$ , אזי כל הרחבה ריבועית היא נורמלית. זה נכון כי כל הרחבה כזו נראית כמו  $K(\sqrt{a})/K$ , ושורשי הפולינום  $x^2 - a = 0$  הם  $\pm\sqrt{a}$ . ההרחבה  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  אינה נורמלית - יש שורשים מרוכבים, שאינם פולינומים רציונליים במספר  $\sqrt[3]{2}$ .

ההרחבה  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  נורמלית - כל שורשי הפולינום האי פריק של  $\zeta_n$  הם שורשי יחידה מסדר  $n$  בעצמם, ולכן חזקות שלו.

ההרחבה  $\mathbb{F}_{p^n}/\mathbb{F}_p$  נורמלית - מהגדרתו בתור  $\{x \in \bar{\mathbb{F}}_p \mid x^{p^n} = x\}$

**הגדרה 0.11** הרחבה אלגברית נורמלית ופרידה נקראת הרחבת גלואה. מגדירים

$$\text{Gal}(L/K) = \text{Aut}_K(L)$$

**דוגמא** ההרחבה  $\mathbb{F}_{p^n}/\mathbb{F}_p$  היא גלואה. נגדיר את האוטומורפיזם פרובניוס:

$$x \mapsto x^p$$

נקבל את האוטומורפיזמים הבאים:

$$\left\{ x \mapsto x^p, x \mapsto x^{p^2}, \dots, x \mapsto x^{p^n} = \text{id} \right\} \cong \mathbb{Z}/n\mathbb{Z} \leq \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$$

כעת, ידוע לנו כי

$$\text{Aut}_K(L) = \text{Hom}_K(L, \bar{L})$$

היות וזו הרחבת גלואה. כלומר כמות האוטומורפיזמים הוא מעלת הפרידות של ההרחבה, שהיא לכל היותר מעלת ההרחבה - שהיא  $n$ . לכן

$$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$