

11/3/09

אלגברה ק' 2 - שיעור 3

הצדקה: פולינום $f(x) \in F[x]$ מתפלג מעל F אם הוא מכיל את גורמים אינאריות ב- $F[x]$.

משפט 30 (קרונקר): יהי $f(x) \in F[x]$ כאשר F שדה, אז קיים שדה E המכיל את F (קיים $F \subseteq F' \subseteq E$) שבו $f(x)$ מתפלג.

הוכחה

באינדוקציה על דרגת $f(x)$. אם הדרגה של f היא 1, אזי $E = F$.

אם הדרגה גדולה מ-1, אז נרשום $f(x) = p(x)g(x)$ ($p, g \in F[x]$) ו- $p(x)$ אי-פריק מעל F . ממסקנה 29 נקבל כי קיים שדה B המכיל את F וקיים $\theta \in B$ כך ש- θ הינו שורש של $p(x)$. לכן ב- $B[x]$ ניתן לרשום $p(x) = (x - \theta)h(x)$. באינדוקציה, קיים שדה E המכיל את B שעבורו $h(x)g(x)$ מתפלג. לכן $f(x) = (x - \theta)h(x)g(x)$ מתפלג ב- E . $\square$

נעשה במשפט של קרונקר כדי לקנות שדה עם מספר סופי של איברים. בתרגיל הוכחנו:

למה 32: יהי F שדה כך ש- $\text{char}(F) = p > 0$. אז:

- (1) לכל $a \in F$, $a^p = a$.
 - (2) לכל $a, b \in F$, $(a+b)^p = a^p + b^p$.
 - (3) לכל $a, b \in F$, $a^k = a$ לכל $k \geq 1$.
- $(a+b)^{p^k} = a^{p^k} + b^{p^k}$

הערה: נראה כי נקבל כי אם F הינו שדה ממצין p , ו- $q = p^k$ אזי $a \mapsto a^q$ היא הפעקה של חוסר.

יהי E שדה, ו- F תת-שדה שלו. אז ניתן לחשוב על E כעל מרחב וקטורי מעל השדה F . E הינו מרחב וקטורי עם פדאל החיבור כפי שהיא מוגדרת בשדה, ואם $c \in F$, E נשזיר ככל סקלר c בהתאם לכלל השדה.

יהי E שדה סופי, אז המצין שלו $p < \infty$. לכן השדה הראשוני שלו הוא $\mathbb{Z}_p$. נבחר בסיס למרחב הוקטורי E מעל השדה $\mathbb{Z}_p$: $\alpha_1, \dots, \alpha_n$. אז כל $a \in E$ ניתן לרשום בצורה יחידה $a = c_1\alpha_1 + \dots + c_n\alpha_n$ כאשר $c_i \in \mathbb{Z}_p$. לכן $|E| = p^n$.

משפט 33 (גלואה): יהי p ראשוני ו- $n \geq 1$. אז קיים שדה שיש בו בדיוק p^n איברים.

$$g \in \mathbb{Z}_p[x]$$

נגדיר $g(x) = x^q - x$ כאשר $q = p^n$. נחשב קריינר קיים שזה E המכל

$$F = \{\alpha \in E : g(\alpha) = 0\}$$

כל $\mathbb{Z}_p$ שבו $g(x)$ מתבטל. נגדיר: $(g, g') = 1$ מכיוון ש $g'(x) = qx^{q-1} - 1 = -1$ מכיוון ש $q \equiv -1 \pmod p$.

אין שורשים חיצוניים באל שדה. לכן F יש בדיוק q איברים.

נראה כי F שדה: יהי $a, b \in F$ כל $a^q = a, b^q = b$ לכן:

$$(ab)^q = a^q b^q = ab$$

$$ab \in F$$

$$(a+b)^q = a^q + b^q = a + b$$

כל $a, b \in F$ נראה 32 :

$$a+b \in F$$

$$a^q - a = a(a^{q-1} - 1) = 0 \quad \text{לכן} \quad a^{q-1} - 1 = 0 \quad \text{כאשר} \quad a \neq 0$$

$$a^{q-2} = a^{-1}$$

קל לראות כי $a^{-1} \in F$ מכיוון ש $a \in F$ שדה. $\square$

דוגמה: נבנה שדה $q = 4$ איברים: $4 = 2^2$. נפרק את $x^4 - x$ מעל $\mathbb{Z}_2$:

$$x^4 - x = x(x-1)(x^2+x+1)$$

מבטא 7 במצב 2. נקבל שכל אחד מהפולינומים האלו הוא א-פריק מעל $\mathbb{Z}_2$. יהי α שורש של x^2+x+1 בשדה הרחבה כלשהו.

כל איברי השדה $\mathbb{F}_4$ יהיו $0, 1, \alpha, \alpha+1$ והפעולה המבוצעת

$$\alpha^2 = \alpha + 1$$

הן מוצאנו $\mathbb{Z}_2$, נחבר שורש α של $x^2+x+1=0$.