

## אלגברה ב2

© ארזים

14 ביוני 2017

### 1 הרחבות אי־פרידות טהורות

יש לנו הרחבה  $L/K$  סופית. המעלה שלה היא  $[L : K] = \dim_K L$ , מעלת הפרידות שלה היא  $[L : K]_s = |\text{Emb}_K(L, \bar{K})|$ . נוסיף עוד מושג כזה:

**הגדרה 1.1** מעלת האי־פרידות של ההרחבה היא

$$[L : K]_i = \frac{[L : K]}{[L : K]_s}$$

ראינו בשיעור שעבר שזה תמיד חזקה של  $p = \text{char} K$  (אם המציין הוא אפס אז זה בוודאות 1).

הגדרנו גם שההרחבה  $L/K$  תיקרא אי־פרידה טהורה אם  $[L : K]_i = [L : K]$ .

**טענה 1.2** יהי  $K$  שדה עם איפיון  $p > 0$ . התנאים הבאים שקולים לכך שההרחבה  $L/K$  אי־פרידה טהורה.

1. לכל  $\alpha \in L$  יש  $\nu > 0$  עם  $\alpha^{p^\nu} \in K$ .

2. לכל  $\alpha \in L$  מתקיים  $\text{irr}(\alpha, K) = x^{p^n} - a$  עבור  $a \in K$ ,  $n \geq 0$ .

3. יש יוצרים של  $L/K$ ,  $\alpha_1, \dots, \alpha_r$ , שעבורם  $\alpha_i^{p^{\nu_i}} \in K$ .

**הוכחה:**  $3 \Rightarrow 1$ : ברור.

$1 \Rightarrow 3$ : אם יש  $\alpha \in L$ , נקבל  $\alpha = f(\alpha_1, \dots, \alpha_r)$ , באשר  $f$  פולינום עם מקדמים מתוך  $K$ . ניקח  $\nu = \max \nu_i$ , ואז  $\alpha^{p^\nu} = f(\alpha_1^{p^\nu}, \dots, \alpha_r^{p^\nu})$  ועכשיו

$$\alpha^{p^\nu} \in K \text{ ולכן } \alpha_i^{p^\nu} = \left(\alpha_i^{p^{\nu_i}}\right)^{p^{\nu-\nu_i}} \in K$$

$1 \Rightarrow 2$ : אם  $\nu \geq 0$  הוא מינימלי עם  $\alpha^{p^\nu} \in K$ , אזי  $g(x) = x^{p^\nu} - \alpha^{p^\nu} \in K[x]$ . כל המחלקים שלו הם מהצורה  $(x - \alpha)^r$ , שהוא לא פולינום בשדה אם  $r \neq 0$  בשדה. לכן  $p \mid r$ . מצד שני, אם  $r = pr'$  כאשר  $p \nmid r'$  אזי  $(x - \alpha)^r = (x^p - \alpha^p)^{r'}$  וזה שוב בשדה אם ורק אם  $\alpha^p \in K$ . באינדוקציה, אם  $\alpha^p \in K$  וכן  $p \nmid r'$ , אזי בהכרח  $\alpha^{p^k} \in K$  לכן הפולינום המינימלי של  $\alpha$ , שמחלק את  $(x - \alpha)^{p^\nu}$ , חייב להיות מהצורה  $(x - \alpha)^{p^n}$  כנדרש.  $2 \Rightarrow 1$ : ברור.

לבסוף נוכיח שקילות בין 1 לבין אי פרידות טהורה. ראינו שאם  $\nu$  גדול מספיק אזי  $KL^{p^\nu}/K$  פרידה. לכן אם  $L/K$  אי פרידה טהורה אזי עבור  $\nu$  גדול מספיק  $KL^{p^\nu} = K$ . לכן 1 אכן שקול לאי פרידות טהורה. ■

**מסקנה 1.3** אם  $L_1/K, L_2/K$  הרחבות אי פרידה טהורות, אזי גם  $L_1L_2/K$  אי פרידה טהורה, וגם אם יש  $K \subseteq L \subseteq E$  אזי  $E/K$  אי פרידה טהורה אם ורק אם  $E/L, L/K$  אי פרידות טהורות.

**משפט 1.4** תהי  $L/K$  הרחבה סופית. אזי יש פירוק  $K \subseteq E \subseteq L$  כך שהרחבה  $L/E$  אי פרידה טהורה והרחבה  $E/K$  פרידה. ■

**הוכחה:** נסמן  $E$  את אוסף האיברים של  $L$  שהם פרידים מעל  $K$ . אזי זו הרחבה פרידה של  $K$ , וודאי. בנוסף, עבור  $\nu$  גדול מספיק,  $E \subseteq L^{p^\nu} E$  פרידה מעל  $E$ , ולכן פרידה גם מעל  $K$  - לכן מוכלת בתוך  $E$ . לכן  $E = EL^{p^\nu}$ , כלומר  $L/E$  אי פרידה טהורה, וסיימנו. ■

**משפט 1.5** תהי  $L/K$  הרחבה סופית ונורמלית. אזי יש  $K \subseteq K_i \subseteq L$  כך שהרחבה  $K_i/K$  אי-פרידה טהורה, והרחבה  $L/K_i$  פרידה (ולכן גלואה). ■

**הוכחה:** נסמן  $G = \text{Aut}_K(L)$ , ויהי  $K_i = L^G$ . אזי  $L/K_i$  גלואה עם חבורת גלואה  $G$  (מהלמה של ארטין ומכך שמתקיים  $[L : K_i] \geq [L : K_i]_s$ ). אם יש  $\sigma : K_i \rightarrow \bar{K}$  כן שמתקיים  $\sigma|_K = \text{Id}$ , נרחיב את  $\sigma$  להעתקה  $\hat{\sigma} : L \rightarrow K$ ,  $\hat{\sigma}|_{K_i} = \sigma$ . כיוון שהרחבה  $L/K$  נורמלית,  $\hat{\sigma} : L \rightarrow L$  ולכן  $G \rightarrow \hat{\sigma}$  ולכן  $G = \text{Id}$  ולכן  $\hat{\sigma}|_{K_i} = \text{Id}$ . קיבלנו כי  $\text{Emb}_K(K_i, \bar{K}) = \{\text{id}\}$  ואז  $K_i/K$  אי פרידה טהורה. ■

**הגדרה 1.6** שדה  $K$  נקרא משוכלל (perfect) אם כל הרחבה סופית שלו היא פרידה.

#### דוגמאות

1. שדות באיפיון אפס.
2. שדות סופיים.

## 2 עקומים אליפטיים

### 2.1 בעיית הלוגריתם הדיסקרטי

**הבעיה** ניקח חבורה  $G$  וניקח איבר  $g \in G$ . בהינתן איבר  $h \in \langle g \rangle$ , נרצה למצוא מספר  $n$  עבורו  $g^n = h$ . לרוב מסמנים  $m = \log_g h$ , או  $m = \text{ind}_g(h)$  עבור  $|m|$  המינימלי שמקיים את זה.

**דוגמה** פרוטוקול Diffie Hellman Key Exchange. כולם יודעים מה החבורה  $G$  ומה האיבר  $g \in G$  (כולל הסדר שלו,  $n$ ). שני הצדדים ייקראו אליס ובוב. אליס בוחרת את  $0 < a < n$ , ובוב בוחר  $0 < b < n$ . אליס מחשבת את  $A = g^a$ , ובוב מחשב את  $B = g^b$ . אליס מחליפה ביניהם את  $A, B$  בערוץ תקשורת גלוי. כעת, אליס מחשבת את  $B^a$ , ובוב מחשב את  $A^b$ , וכעת לשניהם יש את  $g^{ab}$ , ואי אפשר לגלות את המספר הזה רק מהאזנה לתקשורת הגלויה ולמידע הגלוי לכל (אם בעיית הלוגריתם הדיסקרטי בחבורה היא "קשה מספיק").  $g^{ab}$  הוא המפתח שתואם כאן בפרוטוקול.

כעת נרצה לדון בקושי של הבעיה. בחבורות כמו  $G = \mathbb{Z}/m\mathbb{Z}$  או  $\mathbb{R}^*$ ,  $\mathbb{C}^*$ , זה קל. יש חבורות שבהן זה קשה (או לפחות, לא יודעים שזה קל): למשל  $\mathbb{F}_p^*$  - האלגוריתם הטוב ביותר שידוע בחבורה זו הוא יותר גרוע מפולינומיאלי (אבל יותר טוב מאקספוננציאלי). אנחנו נבנה כעת עקום אליפטי  $E$ , ולכל שדה  $K$  תהיה לנו חבורה  $E(K)$  אבלית. בהינתן למשל  $P \in E(\mathbb{F}_p)$  קל לחשב את  $nP = \underbrace{P + \dots + P}_n$ , אבל אין אלגוריתם מהיר לחשב את  $n$  מתוך  $nP$ .

עקום אליפטי הוא עקום שהוא גם חבורה. חוק החבורה בו גיאומטרי, ואין קשר לאליפסות.

**הגדרה 2.1** נניח שכל השדות שלנו  $K$  הם מאיפיון שאינו 2 או 3. בהנתן  $f \in K[x]$ , ממעלה 3, המשוואה

$$E = \{y^2 = f(x)\}$$

מגדירה עקום אליפטי אם אין לפולינום  $f$  שורשים כפולים. לכל  $K \subseteq L$  נגדיר

$$E(L) = \{x, y \in L^2 \mid y^2 = f(x)\}$$

**דוגמה** נראה כמה עקומים, ואת המימוש שלהם על  $\mathbb{R}$ . נדבר על  $y^2 = x^3 - x$  על  $y^2 = x^3 + x$ , ועל  $y^2 = x^3 - 3x + 3$ . העקומים מוצגים באיורים 1, 2, 3.

נצטמצם מעתה למקרה  $y^2 = x^3 + Ax + B$  (שהוא למעשה המקרה הכללי דרך החלפת משתנים).

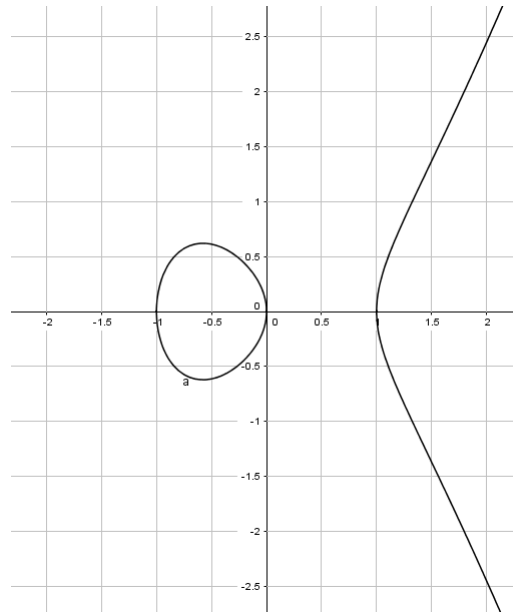
**טענה 2.2** לפולינום  $f$  אי שורשים כפולים  $\iff \Delta f = 4A^3 + 27B^2 \neq 0$   $\iff$  העקום  $\{(x, y) \mid y^2 = f(x)\} \subseteq \mathbb{C}^2$  הוא חלק, משמע הנגזרת שלו לא מתאפסת, כלומר אם  $y^2 = f(x)$  אזי לא מתקיים  $f'(x) = 0$  וגם  $y = 0$ .

כעת נדון בחוק החבורה. בהינתן שתי נקודות  $P, Q \in E$ , נעביר ביניהן קו ישר  $L$ , ובגלל המשוואה שנתונה לנו ממעלה שלישית, הוא יחתוך את העקום בנקודה אחת נוספת בדיוק. נסמנה  $R$ . נשקף אותה סביב ציר  $x$ , ונקבל נקודה  $R'$ . כעת נגדיר  $P + Q = R'$  (כמו באיור 4). כדי לחבר את  $P$  עם עצמה נעביר את המשיק ונעשה את אותה פעולה (מוצג באיור 5). מה נעשה כעת אם שתי הנקודות שנרצה לחבר הן באותו ערך  $x$ ? נצטרך לשנות משהו. נוסף נקודה  $O$  "באינסוף" ואז

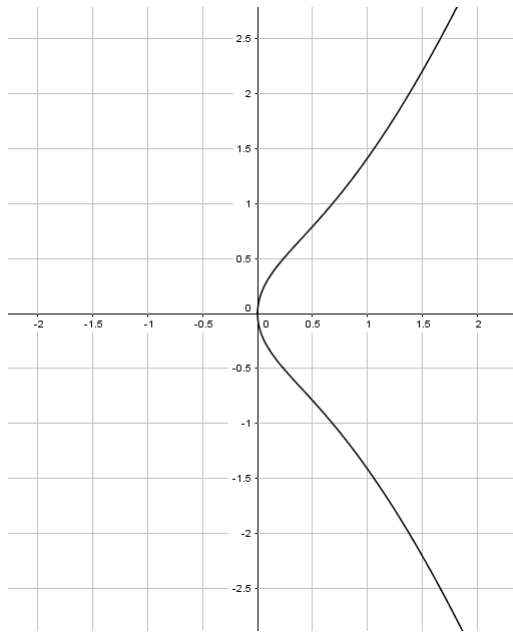
$$E(K) = \{(x, y) \mid y^2 = f(x)\} \cup \{O\}$$

נגדיר את  $O$  להיות האפס של החבורה, ואז החוקים שהגדרנו  $P + Q + R = O$  וכן  $P + (-P) = O$  כאשר  $-P$  היא השיקוף של  $P$  סביב ציר  $x$  (במקום  $(x, y)$  זה הנקודה  $(x, -y)$ ). בקורס בפונקציות מרוכבות 2 רואים:

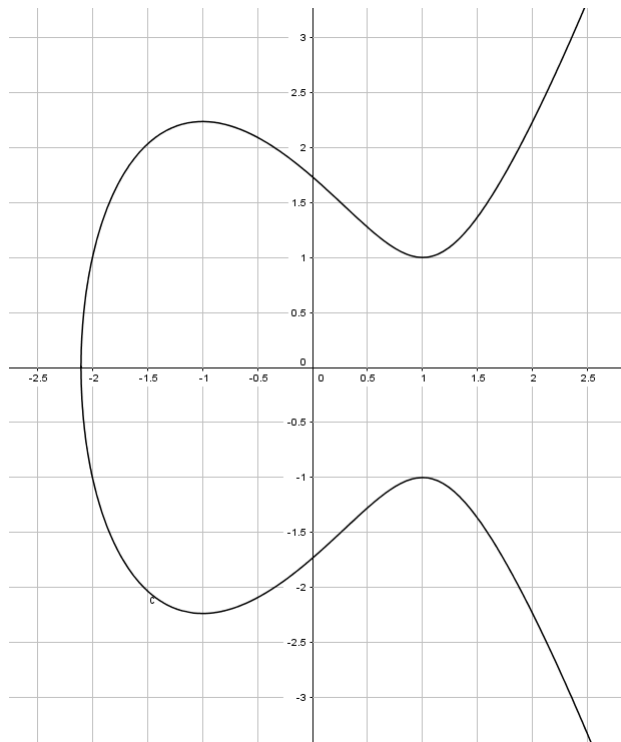
$$E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z}^2 \cong \mathbb{T}^2$$



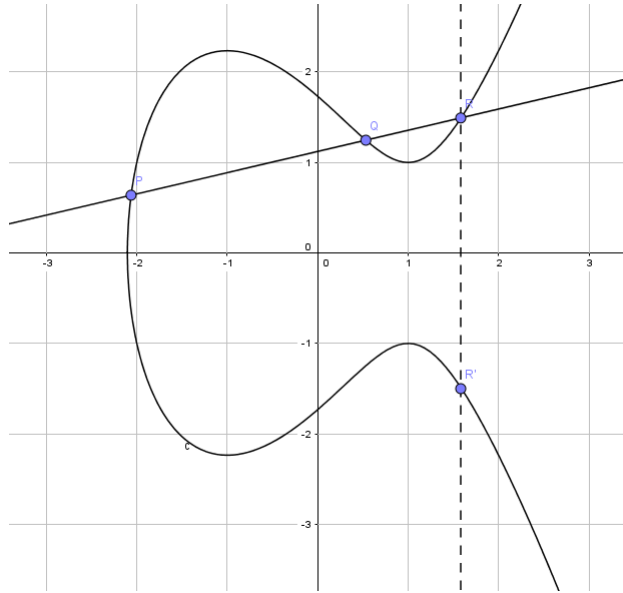
איור 1: העקום האליפטי  $y^2 = x^3 - x$



איור 2: העקום האליפטי  $y^2 = x^3 + x$



איור 3: העקום האליפטי  $y^2 = x^3 - 3x + 3$



איור 4: חוק החבורה:  $P + Q = R'$

נוסחאות אם  $P_1 = (x_1, y_1)$ ,  $P_2 = (x_2, y_2)$  (כאשר  $x_2 \neq x_1$ ) ואז הישר  $L$  הוא

$$y - y_1 = \underbrace{\frac{y_2 - y_1}{x_2 - x_1}}_{\lambda} (x - x_1)$$

נחתוך בין  $L, E$ :

$$(\lambda(x - x_1))^2 - x^3 + Ax + B = (x - x_1)(x - x_2)(x - x_3)$$

וכעת צריך להשוות מקדמים כדי למצוא את  $x_3$  מהמקדם של  $x^2$ :

$$-\lambda^2 = x_1 + x_2 + x_3$$

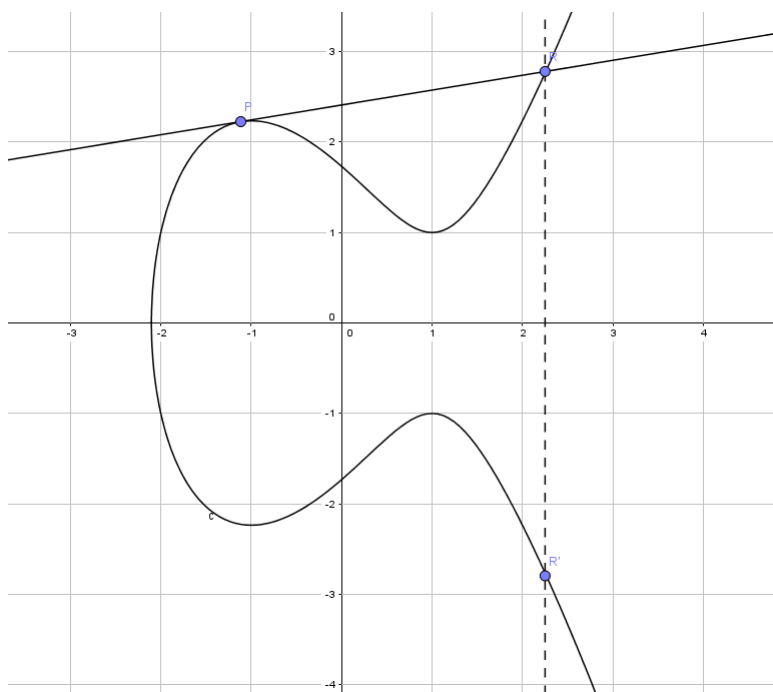
והנה לנו

$$x_3 = -x_1 - x_2 - \lambda^2$$

מכאן כמובן

$$y_3 = y_1 + \lambda(x_3 - x_1)$$

ומכאן  $R = (x_3, y_3)$  לכן  $P + Q = (x_3, -y_3)$ .



איור 5: חוק החבורה:  $P + P = R'$