

ז. שנויים למשל כיתח-כוכ

ז. שדה פונקציות רציונליות

כסול זה ... נכונה לקבץ את השדה ואת החלקה הקוונטית של

שדה פונקציות רציונליות  $F = K(t)$  מעל שדה  $K$  מאגמה ז

כאשר נעיר  $e$  א  $e$  סגור אלגברית  $F > K$  ואכן יוני  $u \in F$  אגד

אלגברי מעל  $K$  את  $u$  נכל לנסב לזכרה  $u = \frac{f(t)}{g(t)}$  כאשר  $f, g \in K[t]$

פולינומים. נניח לשלילה  $u \notin K$  אזל שמתל של השוויון  $f(t) - u g(t) = 0$

שלינו יוכל להיות שדה לאפס כאשר נחווה בפולינום  $g$  לכן  $t$  אלגברי מעל

$(u)K$ . לכן  $t$  אלגברי מעל  $K$ , כשתיבה להנחה

כאילו נכר יש  $F$  שט סגורים של החלקים האסותיים. כאשיות

החלקים  $q$  והמאמים לפולינומים האסותיים  $P(t)$  נחקה זה

$F_p \cong K[t] / P(t)K[t]$  ולכן  $\deg p = \deg P(t)$  שיה החתולן  $p_\infty$  החתולן

לפולינום האס פריק  $t^r$   $K[t]$  ואת מקולים  $e$   $\deg p_\infty = 1$  אכ

$f(t)$  הוא פונקציה רציונלית כלשהי וסכומם של פולינומים האס של יוני

$$f(t) = p_1(t)^{e_1} \dots p_r(t)^{e_r} \quad e_i \geq 0$$

אז החתולן הוא החתולן לה נון של יוני

$$(f(t)) = \sum_{i=1}^r e_i p_i - \deg f(t) \cdot p_\infty$$

כשר  $p_i$  הוא החתולן הרחב האס  $P_i(t)$  החתולן  $- \deg f(t)$  של  $p_\infty$

או כאמור  $\sum_{p_\infty} v_{p_\infty}(f(t))$  מסומה זו אכ מקולים שמתל  $L(n p_\infty)$

עבור  $n$  סדרים מוכנסים לבין מכל הפולינומים שהם  $n \geq 0$  זכרים להיחל

יש הוא  $1, t, t^2, \dots, t^n$  לבן  $\dim(nP_\infty) = n+1$  אם  $n$

$\dim(nP_\infty) = n \deg P_\infty + 1 - g$   $2g-2 > n$  מקבל המשט הימן כן  $e$

לומר  $n+1 = n+1 - g$  ולכן  $g=0$

אילו  $-2P_\infty$   $\deg(-2P_\infty) = -2 = 2g-2$   $g=0$

היה ממלך קומי היינו מקבלים  $\dim(-2P_\infty) = g-1 = -1$  סגורה  $-2P_\infty$  לבן הוא ממלך קומי

הוכחנו אפוא את המשט הנ"ל

משט 17: אם  $F = K(t)$  הונו שדה פונקציות רציונליות מעל שדה  $K$  ו- $g=0$

$-2P_\infty$  הוא המלך הקומי.

הוכחה: הוכח שם  $f(t) \in K[t]$  הוא פולינום ו- $\deg(f(t))_0 = \deg f$

2.2. עבור פונקציות ממעלה 2 נחזק שדות פונקציות רציונליות.

אם  $v_p(\alpha) \neq 0$  אז  $\alpha$  מתחלק במכונה  $p$  המכונה  $v_p(\alpha) \neq 0$  או נאמר

יש מתחלק  $\alpha$  ב  $v_p(\alpha) \neq 0$  אם אין קיים מתחלק המכונה  $p$  המכונה  $v_p(\alpha) \neq 0$

$v_p(\alpha) > 0$   $\Leftrightarrow \alpha \in p$

למה 2.2: יהי  $F/K$  שדה פונקציות, יהי  $x \in F$  ונא קבוע  $v_p(x) = \frac{f_1(x)}{f_2(x)}$  אם

יש פונקציות רציונליות  $f_1, f_2$  ו  $f_2$  הם פולינומים שונים זה לזה אם

$$v_p(x) = (f_1(x))_0 - (f_2(x))_0 - \deg f_2(x) \cdot (x)_\infty$$

המתחלקים  $(f_1(x))_0, (f_2(x))_0, (x)_\infty$  שונים זה לזה

$$[K(x) : K(v_p(x))] = \max(\deg f_1, \deg f_2)$$

הוכחה: יהי

$$f(x) = a_0 + a_1x + \dots + a_nx^n \quad a_i \in K \quad a_n \neq 0$$

פולינום, יהי  $p$  מתחלק המכונה  $v_p(x) \geq 0$  אם  $v_p(f(x)) \geq 0$  אם

אם  $v_p(x) < 0$  אם  $v_p(f(x)) = n v_p(x)$  אם  $v_p(x) < 0$  אם  $v_p(x) < 0$

$$(f(x))_\infty = n(x)_\infty$$

$$v_p(x) = (f_1(x))_0 - (f_1(x))_\infty - (f_2(x))_0 + (f_2(x))_\infty$$

$$= (f_1(x))_0 - (f_2(x))_0 - \deg f_1(x) \cdot (x)_\infty + \deg f_2(x) \cdot (x)_\infty$$

$$= (f_1(x))_0 - (f_2(x))_0 - \deg f_2(x) \cdot (x)_\infty$$

אם  $v_p(x) < 0$  אם  $v_p(f(x)) = n v_p(x)$  אם  $v_p(x) < 0$  אם  $v_p(x) < 0$

$$g_1(x)f_1(x) + g_2(x)f_2(x) = 1 \quad \text{ע} \quad \text{כך} \quad g_1(x), g_2(x) \text{ פולינומים}$$

כדי להוכיח את השיון האחרון נבנה להיטה  $e$   $\deg f_1 \geq \deg f_2$  (אחרת)

נבנה להיטה  $e$   $\{r(x)^{-1}\}$  ו  $F = K(x)$  ו  $(r(x))_0 = (f_1(x))_0$  ו  $(f_2(x))_0$

$$[K(x) : K(r(x))] = \deg (r(x))_0 = \deg (f_1(x))_0 = \deg f_1$$

מהלכה נבנה  $e$   $K(x) = K(r(x))$  אם ורק אם  $\max(\deg f_1, \deg f_2) = 1$

אם  $r(x) = \frac{ax+b}{cx+d}$  כאשר  $a, b, c, d$  הם אגפים  $e$   $K$  ו  $ad - bc \neq 0$

ההיטה האחרון נבנה כדי שהמחנה והמכנה יהיו זרים זה לזה

נניח  $e$   $K$  הוא שדה  $e$   $\{x\}$  אגפיו  $\neq 2$ , יהיו  $x$  אגרי טרנסצנדנטי

$F$  יהיו  $K$  היחידה  $e$   $K(x)$  ממעלה  $\geq 2$ . נניח שיש קומה גרמיה אלגברית

$L$   $e$   $K$   $\geq L$   $L(x) = F$  אם  $K$  סגור אלגברית  $\geq F$

אם  $F$  נמן  $e$   $F = K(x, y)$  כאשר  $y$  מקיים משווא ריבועית או פריק

$$y^2 + b(x)y + c(x) = 0 \quad b(x), c(x) \in K[x]$$

זו יצי השלמה לריבוע נעשה להשווא

$$\left(y + \frac{b(x)}{2}\right)^2 + c(x) - \frac{b(x)^2}{4} = 0$$

ולכן נבנה להיטה  $e$   $y$  מקיים משווא מעברית  $y^2 = d(x)$  אם  $d(x)$

אפשר לפרק לריבועים וזו יצי השלמה כל המקרים הנושאים של פולינומים או

פריקים נמן להיטה  $e$   $d(x)$  הוא פולינום ממעלה  $\geq 2$  שאינו מתחלק לריבוע

של פולינום או פריק

$$\pi^{-1}(B_i) = \bigcup_j A_{ij}$$

$F_i$   
 $\downarrow$   
 $\varphi(x, y)$   
 $\downarrow$   
 $\varphi(x)$   
 $\downarrow$   
 $Q$

$K(x, y)$   
 $\downarrow$   
 $K(x)$

$$y^2 = d(x)$$

$$(\sigma z) = \sum \psi_p(\sigma z) P$$

$$z \in L(n(x)_\infty)$$

$$z = r_1(x) + y r_2(x)$$

$$\sigma z = r_1(x) - y r_2(x) \in L(n(x)_\infty)$$

$$z + \sigma z = 2r_1(x) \in L(n(x)_\infty)$$

$$(r_1(x)) + n(x)_\infty \geq 0$$

$$r_1(x) = \frac{f_1(x)}{g_1(x)}$$

$$(f_1(x))_0 - (g_1(x))_0 - (\deg f_1 - \deg g_1)(x)_\infty + n(x)_\infty \geq 0$$

$$\Rightarrow g_1 = \text{const.}$$

$$\deg f_1 \leq n.$$

$$z \cdot \sigma z = r_1(x)^2 - y^2 r_2(x)^2 = r_1(x)^2 - d(x) r_2(x)^2 \in L(n(x)_\infty).$$

$d(x) r_2(x)^2$  ist ein Polynom vom Grad  $\leq 2n$

$r_2(x)$  ist ein Polynom vom Grad  $\leq \deg n - \frac{m}{2}$

$\frac{d}{dx} \frac{1}{y}$   
 $\frac{d}{dx} \frac{1}{y^2}$   
 $\frac{d}{dx} \frac{1}{y^3}$   
 $\frac{d}{dx} \frac{1}{y^4}$

$$\sum_{\sigma P} (z) = \psi(\sigma^{-1} z)$$

48

$$z \in L(\alpha) \quad (z) + \alpha \geq 0$$

$$\sigma z \in L(\sigma \alpha)$$

$$\sigma(z) = (\sigma z)$$

$$(z) = \sum \psi_p(z) P$$

$$\sigma(z) = \sum_p \psi_p(z) (\sigma P) = \sum_{\sigma' P} \psi_{\sigma^{-1} P}(z) P$$

$$= \sum_p \psi(\sigma z) P$$

הוא פולינום מעלה  $n - \frac{m}{2}$

לפיכך, נכלול את  $r_1(x)$  ו-  $r_2(x)$  ונראה שהם פולינום מעלה  $n$

הוא פולינום מעלה  $n - \frac{m}{2}$  וכן  $r_1(x) + y r_2(x)$  (  $L(n(x)_\infty)$  )

לפיכך, נכלול את  $r_1(x)$  ו-  $r_2(x)$  ונראה שהם פולינום מעלה  $n$

הוא פולינום מעלה  $n - \frac{m}{2}$  וכן  $r_1(x) + y r_2(x)$  (  $L(n(x)_\infty)$  )

$$1, x, \dots, x^n, y, yx, \dots, yx^{n-\frac{m}{2}}$$

הוא פולינום מעלה  $n - \frac{m}{2}$  וכן  $r_1(x) + y r_2(x)$  (  $L(n(x)_\infty)$  )

הוא פולינום מעלה  $n - \frac{m}{2}$  וכן  $r_1(x) + y r_2(x)$  (  $L(n(x)_\infty)$  )

הוא פולינום מעלה  $n - \frac{m}{2}$  וכן  $r_1(x) + y r_2(x)$  (  $L(n(x)_\infty)$  )

$$2n + 2 - \frac{m}{2} = 2n + 1 - g$$

$$g = \frac{m-2}{2}$$

הוא פולינום מעלה  $n - \frac{m}{2}$  וכן  $r_1(x) + y r_2(x)$  (  $L(n(x)_\infty)$  )

$$1, x, \dots, x^n, y, yx, \dots, yx^{n-\frac{m+1}{2}}$$

הוא פולינום מעלה  $n - \frac{m+1}{2}$  וכן  $r_1(x) + y r_2(x)$  (  $L(n(x)_\infty)$  )

$$g = \frac{m-1}{2}$$

הוא פולינום מעלה  $n - \frac{m+1}{2}$  וכן  $r_1(x) + y r_2(x)$  (  $L(n(x)_\infty)$  )

משפט 2.3: יהי  $K$  שדה בעל אופיון  $m$  ויהי  $x$  איבר סגור על  $K$ .

נחלק  $K$  ויהי  $d(x)$  פולינום  $> 0$  מעל  $K$  המצליח חלוקה מלאה של  $x$  במתחם

קטן  $g$ , ויהי  $y$  איבר המקיים  $y^2 = d(x)$  ויהי  $F = K(x, y)$ .

$F$  הוא שדה פונקציות מעל  $K$ ,  $[F:K] = 2$ , והשדה  $F$  הוא  $g$  על  $K$ .

$$g = \begin{cases} \frac{m-2}{2} & \text{אם } m \text{ זוגי} \\ \frac{m-1}{2} & \text{אם } m \text{ אי-זוגי} \end{cases}$$

דוגמה:  $g=0$  עבור  $m=2, 7$ ,  $g=1$  עבור  $m=3, 4$ ,  $g=2$  עבור

5, 6

באופן כללי, אנו מקבלים דוגמאות לשדות פונקציות על שדה כללי.

הנ"ל קובעים שדות פונקציות אינדיסל-אלימנטריים. במקרה  $g=1$  קובעים להם שדות פונקציות אלימנטריים.

הערה: סיבה אחרת חשובה להבחין בין שני המקרים היא שדה  $F$  הוא

מחלקים קומוניים של  $F$  למקרים השונים.

3. עזרו לי, עזרתי לכם

עזרו לי, עזרתי לכם.  $F/K$  שדה פונקציות על  $\mathbb{C}$  ו- $F=K(t)$  הוא שדה

פונקציות רציונליות מעל  $K$ , או  $F$  הוא הרחבה גדולה של  $K(t)$ . במקרה

אחרון זה, נרמזה והוספת  $\text{char } F \neq 2$  אפשר לתאר את  $F=K(t,u)$  בכורה

כאשר  $u^2 = at^2 + c$ ,  $a, c \in K$ ,  $a \neq 0$

הוכחה: נסמן  $w$  מרחב קטני של  $F/K$  ויש  $\deg w = -2$  לכן

לכן  $\dim(-w) = 3$  קיימים איברי  $x, y, z$  אינדיבידואליים של  $(-w)$  ו- $\deg(-w) = 2 > 2g - 2$

על ידי איברי  $x, y, z$  אינדיבידואליים של  $(-w)$  ו- $\deg(-w) > 2g - 2$

על ידי איברי  $x, y, z$  אינדיבידואליים של  $(-w)$  ו- $\deg(-w) > 2g - 2$

$$(z) = ((y) + w) - ((x) + w)$$

לכן  $(z)_\infty \leq (z) - w$  לכן  $(z) + w \geq 0$  ו- $(y) - w \geq 0$

$$[F:K(t)] = \deg(z)_\infty \leq \deg((z) + w) = 2$$

מכאן נמצא שהרחבה של המעלה

אם  $[F:K(t)] = 2$  ו- $\text{char}(F) \neq 2$  ויש לפי המשפט 3.1 נהיה לתאר את  $F$

ככורה  $F=K(t,u)$  כאשר  $u^2 = at^2 + bt + c$  ו- $a, b, c$  הם איברי  $K$  כך

אם  $a \neq 0$  על ידי השלמה לריבוע אפשר להגיע לכך  $b=0$

המשפט הבא יאפשר לנו להבחין בין שתי האפשרויות שמוצגו במשפט 3.1



משפט 5.5: הנאי הנכתי ומספיק לכן שדה פונקציות  $F/K$  גדל בצד אפס יהיה

שדה פונקציות רציונליות הוא שיהיה לו מחלק, כאשר  $q$  המעלה 1.

הוכחה: ברור שהנאי הנכתי נוכח שהוא עם מספיק ואכן, המשפט

כימין-יון נוצר  $e$   $\dim p = 1+1 = 2$  לכן קימים  $L(p)$  שני אלמנטים

$x, y$  שאינם גלויים לימנוריה מעל  $K$ . אימצ אהים, נאמר  $x$ , אינו קלוש. הטו

מקום  $0 \leq p(x) < \infty$  ולכן  $(x)_\infty = p$  (הוכחה) לכן

$$[F:K(x)] = \deg(x)_\infty = 1$$

כן  $e$   $F=K(x)$

הכרטיס: הוכח שאם  $F/K$  הוא שדה פונקציות גדל בצד אפס אזי כל מחלק

ל  $F/K$  מעלה אפס הוא ראשי.

4. עמוד 251

מעבר 3 (הוכחה) אם  $x$  הוא אזור סימפליקטיאלי מעל  $K$  על אופן

עמוד 2 נא  $y^2 = f(x)$  (א) כאשר  $f \in K[x]$  הוא פולינום ממעלה 3 על שדה

מכונות  $F = K(x, y)$  שיהי  $F = K(x, y)$  ויהי  $F = K(x, y)$  מהמשווא  $(x)$  נגזר

$\deg(x)_\infty = [F:K(x)] = 2$  ולכן יש  $(x)_\infty$  על אפסיות

$\deg p = 1$  כאשר  $p$  מחלק ראשוני  $(x)_\infty = 2p$

$\deg p = 2$  כאשר  $p$  מחלק ראשוני  $(x)_\infty = p$

כאשר  $p, q$  מחלקים ראשוניים ממעלה 1  $(x)_\infty = p + q$

מאונך המישור  $(x)$  אם  $v_p(x) < 0$  אם  $v_p(y) < 0$  ומקרה כזה

אם  $v_p(x) < 0$  ו  $v_p(y) < 0$   $2(y)_\infty = 3(x)_\infty$  נגזר מהאפסיות (א) ו (ב)

מחלקים ראשוניים (2 מחלק ראשוני 3 או 2 מחלק ראשוני 1 להחמיר)

$(x)_\infty = 2p$  ו  $(y)_\infty = 3p$  כאשר  $p$  הוא מחלק ראשוני ממעלה 1

כיוון הגבוה יש לנו המעבר והוא המקביל למעבר 5

מעבר 6: יהי  $F/K$  שיהי טורקציוני על שדה  $F$  ויהי  $\text{char } K \neq 2, 3$

יהי  $F/K$  מחלק מישור  $\Delta$  ממעלה 1. אם  $\Delta$  מתן להיבט או  $F$  לבורה

$F = K(x, y)$  כאשר  $y^2 = f(x)$  ו  $f(x)$  הוא פולינום ממעלה 3 מעל  $K$

עמוד 251

הוכחה:

ממש  $\dim K = n$  נניח  $\dim K = n$  ונניח  $\dim K = n$  ונניח  $\dim K = n$

$\dim K = 2$  לכן קיים  $L(K)$  מסדר 2 ונניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$

נניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$

נניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$

נניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$

נניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$

נניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$  ונניח  $L(K) = K[x]$

(1)  $y^2 + a_1xy + a_2y = a_3x^3 + a_4x^2 + a_5x + a_6$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$

נניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$  ונניח  $y = \frac{p(x)}{q(x)}$



5 ע : עקרונות אלגוריתמים

נשאר כסימונים של משפט 5.6. יהי  $\mathcal{P}$  מחלק באגודת  $F/K$  המעלה  $n$

ד. ס. א.  $(a, b) = (\varphi_p(x), \varphi_p(y))$  הוא זוג שקריות של  $K$  המקיים את השוויון  
(אזינו גלוי גמיש המיוצר  $\varphi$  על  $\mathcal{P}$ , נגזר  $\varphi$  ממוחלט)

לפיכך, אם  $(a, b)$  הוא זוג אכזבי של  $K$  המקיים את השוויון  $b^2 = f(a)$

ה'ג' א"י ההצטרף  $(a, b) \rightarrow (x, y)$  נחמד להיחשב להומומורפיזם- $K$  של  $K[x, y]$

של  $K[a, b]$ . אפשר להראות שהמושג המקומו של ההומומורפיזם, נהיה  $F/K$

$$\left\{ \frac{g(x, y)}{h(x, y)} \mid g, h \in K[x, y] \text{ ו- } h(a, b) \neq 0 \right\}$$

הוא זוג הצרובה. לכן אפשר להכניס את ההומומורפיזם כאן יחיד לאגד  $\varphi$

המעלה המיונה של  $F/K$  המחלק הראשוני  $\mathcal{P}$  המתאים לאגד זה יהיה  $\mathcal{P}(a, b)$

אפילו מסווג ומקיים את ד. (זוג  $(\infty, \infty)$  מקבל התאמה חד-חד ערכית הפוך אל כל המחלקים

הראשוניים המעלה 1 של  $K$  (נשמך אל זוג  $(P, \infty)$  זכין אל כל התקוצות ה- $K$ -

כפולותיו,  $\mathcal{E}(K)$  של העקרונות האלגוריתמי  $\mathcal{E}$  המושבר על יזי המשוואה האסימטרית

$$y^2 = f(x)$$

נשמך צמד ומקיים את  $P_1$  אל כל מחלקות המחלקים המעלה  $n$  עם של

$F/K$  מחלק המיוני  $\mathcal{P} \in P_1$  מתאים את המחלקה של המחלק  $\mathcal{P} - \mathcal{D}$  קבוע  $\mathcal{D}$

יהא  $\mathcal{P}$  מחלק המחלקים הנחשבים לפיכך, יהי  $\mathcal{Q}$  מחלק המעלה  $n$  אפס. א"י

$\deg(\alpha + \mathcal{D}) = 1$  (זכין, לפי משפט שיימן-כיון,  $\dim(\alpha + \mathcal{D}) = 1$  ק"י אפסו  $\mathcal{E}$

$F > \mathcal{E}$  כך  $\mathcal{E} + \alpha + \mathcal{D} > 0$ . המעלה של אגד נשמך היא 1 ולכן

$$\mathcal{P}' = \mathcal{P} + (\mathcal{Z})$$

קיים  $P \in P_1$  כך  $e$   $(z) + \alpha + \beta = P$  אם  $z' = z$  הוא אנו מניחים

אנו של  $F$  המקיים  $(z) + \alpha + \beta \neq 0$  ויש  $z' = cz$  כאשר  $c \in K$  ולכן

$(z') = (z)$  כך  $e$   $P$  מקבל באופן מסווגי על ידי התהליך הנ"ל

ע"פ  $P - \beta$  מקיף מופנה מתקופה האסות  $\alpha$  וכן התאמה הנ"ל היא התאמה

היא מסווגת של  $P_1$  על  $C_0$ .

זהו  $C_0$  היא תלויה ולכן התאמה הנ"ל משנה את תלויה על  $P_1$

ע"פ  $D$  מורה את  $e$  האם: התאמה של  $P_1$  על  $\xi(K)$  משנה של

תלויה על  $\xi(K)$  שבה  $(\infty, \infty)$  הוא אזור האם

התאמה המפורטת של המספר  $\xi(K)$  מתקבלת בעזרת

למה  $z \in K$ : המספרים והמספרים  $(\alpha_i, \beta_i)$   $i=1,2,3$  של  $\xi(K)$

מקיימים  $(a_1, b_1) + (a_2, b_2) + (a_3, b_3) = 0$  (כאשר  $+$  מוקן כמספרות המספר

המספר  $C_0$  הוא של התאמה על ישר אחד.

הוכחה: נניח  $(a_i, b_i)$  ין תקופות סופיות ויהיו  $P_i$  התחלקים

המסויים של  $F/K$  התאמה  $P_i$  נניח קודם של תקופות המסויים על ישר אחד

למה  $P_i$  מקיימת המסויים

(7)  $\alpha a_i + \beta b_i + \delta = 0$   $\alpha, \beta, \delta \in K$   $i=1,2,3$

לכן  $P_1, P_2, P_3$  הם אפסים של האנו  $z = \alpha x + \beta y + \delta$  של  $F$  מסוי

$(z)_\infty = 3D$   $\deg(z)_\infty = 3$   $e$   $(z)_\infty = P_1 + P_2 + P_3$



ע)  $\mathcal{E}(K)$  וז"ל  $(x_i, y_i) \in \mathcal{E}(K)$  ,  $i=1,2,3$  ,  $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

אם  $(x_1, y_1) \neq (x_2, y_2)$  אז

$$x_3 = \left( \frac{y_1 - y_2}{x_1 - x_2} \right)^2 - x_1 - x_2$$

$$y_3 = \frac{y_1 - y_2}{x_1 - x_2} x_3 + \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}$$

אם  $y^2 = f(x)$  ,  $f(x)$  הוא פולינום  $\mathbb{Z}$  או  $\mathbb{Q}$  , אז  $\mathcal{E}(K)$  הוא קבוצת נקודות

על  $K[x, y]$  ,  $K = \mathbb{Z}$  או  $\mathbb{Q}$

אם  $a, b \in K$  , אז  $(a, b) \in \mathcal{E}(K)$  ,  $(a, b) \rightarrow (a, b)$  ,  $(a, b) \in \mathcal{E}(K)$

אם  $f: F \rightarrow K$  , אז  $f(x) = y^2$  ,  $f(x) = y^2$

אם  $(a, b) \in \mathcal{E}(K)$  , אז  $(a, -b) \in \mathcal{E}(K)$

אם  $(a, b) \in \mathcal{E}(K)$  , אז  $(a, b) \in \mathcal{E}(K)$

אם  $(a, b) \in \mathcal{E}(K)$  , אז  $(a, -b) \in \mathcal{E}(K)$  ,  $(a, b) = (a, -b)$  ,  $(a, b) \in \mathcal{E}(K)$

אם  $(a, b) \in \mathcal{E}(K)$  , אז  $(a, b) \in \mathcal{E}(K)$  ,  $(a, b) \in \mathcal{E}(K)$

אם  $(a, b) \in \mathcal{E}(K)$  , אז  $(a, b) \in \mathcal{E}(K)$  ,  $(a, b) \in \mathcal{E}(K)$

אם  $(a, b) \in \mathcal{E}(K)$  , אז  $(a, b) \in \mathcal{E}(K)$  ,  $(a, b) \in \mathcal{E}(K)$

אם  $(a, b) \in \mathcal{E}(K)$  , אז  $(a, b) \in \mathcal{E}(K)$  ,  $(a, b) \in \mathcal{E}(K)$