УНІТРИКУТНІ АВТОМОРФІЗМИ КІЛЬЦЯ МНОГОЧЛЕНІВ ВІД ДВОХ ЗМІННИХ НАД ПОЛЕМ ХАРАКТЕРИСТИКИ $P > 0$

Жанна ДОВГЕЙ[1], *Віталій СУЩАНСЬКИЙ*[2]

[1] Чернівецький національний університет імені Юрія Федьковича, вул. Коцюбинського 2, Чернівці 58012,
[2] Інститут математики, Сілезький технічний університет, 44-100 Глівіце, Польща

e-mail: *janacucureac@mail.ru, Vitaliy.Sushchanskyy@polsl.pl*

Редакція отримала статтю 12 січня 2012 р.

Досліджується будова групи унітрикутних автоморфізмів кільця многочленів $K[x, y]$ від двох змінних над полем характеристики $p > 0$. Охарактеризовано її підгрупу p-тих степенів, знайдено ширину цієї вербальної підгрупи, наведено верхню оцінку енгелевої довжини всієї групи.

1 Вступ

Нехай K — фіксоване поле, $Aut\, K[x, y]$ — група автоморфізмів кільця многочленів $K[x, y]$ від змінних x, y над полем K. Довільний автоморфізм однозначно визначається образами твірних x, $y \in K[x, y]$, тобто парою многочленів

$$u = \langle a(x, y), b(x, y)\rangle, \tag{1}$$

УДК: 512.5; MSC 2010: 20E34,20E36
Ключові слова і фрази: група унітрикутних автоморфізмів, підгрупа p-тих степенів, ширина вербальної підгрупи, енгелева довжина групи

яка повинна бути такою, щоб відображення

$$x \to a(x, y), \quad y \to b(x, y),$$

продовжувалося до бієкції кільця $K[x, y]$ в себе, причому обернене відображення також повинно бути поліноміальним, тобто задаватися парою многочленів вигляду (1). Автоморфізм φ_u, який визначає пара (1), діє на довільний многочлен $f(x, y) \in K[x, y]$ таким чином

$$\varphi_u(f(x, y)) = f(a(x, y), b(x, y)). \tag{2}$$

В групі $Aut\, K[x, y]$ виділяється дві стандартні підгрупи.

1) Підгрупа афінних автоморфізмів $Aff_2(K)$. Автоморфізм φ_u називається афінним, якщо визначальна пара (1) для нього складається з лінійних многочленів. Інакше кажучи, для афінного перетворення φ_u маємо

$$\varphi_u(x) = ax + by + \alpha, \quad \varphi_u(y) = cx + dy + \beta, \tag{3}$$

де a, b, c, d, α, $\beta \in K$, $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$.

2) Підгрупа трикутних перетворень $J_2(K)$. Автоморфізм $\varphi_u \in AutK[x, y]$ називається трикутним, якщо він визначається перетвореннями вигляду

$$\varphi_u(x) = ax + b, \quad \varphi_u(y) = cy + d(x), \tag{4}$$

де a, b, $c \in K$, $a \neq 0$, $c \neq 0$, $d(x) \in K[x]$. Перетворення (4) називають трикутними або елементарними, а підгрупу $J_2(K)$ — підгрупою елементарних автоморфізмів кільця $K[x, y]$ або афінною групою Жонк'єра (детальніше див. [1], [2]). Перетин підгруп $Aff_2(K)$ і $J_2(K)$ складається з лінійних трикутних автоморфізмів

$$x \to ax + b, \quad y \to cy + dx + e, \tag{5}$$

a, b, c, d, $e \in K$, $a \neq 0$, $c \neq 0$. Група автоморфізмів вигляду (5) позначається $T_2(K)$. Ще з сорокових років минулого століття відомо (див., напр., [3], [4], [5]), що група $Aut\, K[x, y]$ розкладається на амальгамований вільний добуток своїх підгруп $Aff_2(K)$ та $J_2(K)$ над об'єднаною підгрупою $T_2(K)$. Це означає, що дослідження будови $Aut\, K[x, y]$ в певному сенсі зводиться до вивчення будови її підгруп $J_2(K)$ і $Aff_2(K)$. Проте підгрупа $J_2(K)$ досліджувалася з точки зору теорії груп зовсім мало, в основному, вивчалася динаміка дії автоморфізмів трикутного вигляду. Група Жонк'єра $J_2(K)$ містить підгрупу унітрикутних автоморфізмів $UJ_2(K)$, тобто автоморфізмів вигляду (4), для яких $a = 1$, $c = 1$. Унітрикутне перетворення φ_u, задане рівностями

$$\varphi_u(x) = x + a, \quad \varphi_u(y) = y + b(x) \tag{6}$$

однозначно визначається набором даних $[a, b(x)]$, де $a \in K$, $b(x) \in K[x]$. Суперпозиція перетворень $u = [a_1, b_1(x)]$, $v = [a_2, b_2(x)]$ визначається рівністю

$$uv = [a_1 + a_2, b_1(x) + b_2(x + a_1)]. \tag{7}$$

А тому групу $UJ_2(K)$ можна ототожнити з групою наймождивіших наборів вигляду $[a, b(x)]$, $a \in K$, $b(x) \in K[x]$, з правилом множення, що задається рівністю (7). При цьому нейтральному елементу відповідає пара $e = [0, 0]$, а оберненою до пари $[a, b(x)]$ є пара $[-a, -b(x - a)]$. Підгрупа $UJ_2(K)$ є нормальною в $J_2(K)$, причому фактор-група $J_2(K)/UJ_2(K)$ ізоморфна $K^* \times K^*$, де K^* — мультиплікативна група поля K.

В роботах [6], [7], [8] розпочато дослідження груп $J_2(K)$ і $UJ_2(K)$ над полями характеристики нуль. Метою даної статті є вивчення властивостей групи $UJ_2(K)$ над полями характеристики $p > 0$. Ми розвиваємо теорію різницевих операторів в кільцях многочленів над такими полями, виділяємо нормальний дільник, що задається так званими p-многочленами, досліджуємо підгрупу p-тих степенів, оцінюємо енгелеву довжину групи $UJ_2(K)$.

2 Різницевий оператор в кільці многочленів над полем характеристики p

В полі характеристики p для біноміальних коефіцієнтів $C_{p^s}^k$ виконується співвідношення

$$C_{p^s}^k = \begin{cases} 0, & \text{якщо } 0 < k < p^s, \\ 1, & \text{якщо } k = 0, p^s. \end{cases}$$

А тому, біноміальна тотожність для показника p^s ($s \in \mathbb{N}$) над таким полем записується у вигляді

$$(x + y)^{p^s} = x^{p^s} + y^{p^s}. \tag{8}$$

Із (8) випливає, що для довільного многочлена $a(x) \in K[x]$, $charK = p$, рівність

$$a(x)^{p^s} = a(x^{p^s}) \tag{9}$$

виконується при будь-якому натуральному s. Рівність (9) означає, що відповідність $x \to x^{p^s}$ при довільному $s \in \mathbb{N}$ продовжується до ізоморфного занурення кільця $K[x]$ в себе. Образом $K[x]$ при такому зануренні буде підкільце $K[x^{p^s}]$. Таким чином, маємо нескінченну послідовність ізоморфних кілець

$$K[x] \to K[x^p] \to K[x^{p^2}] \to \ldots,$$

причому має місце рівність

$$\bigcap_{s=0}^{\infty} K[x^{p^s}] = K.$$

Ми використовуватимемо далі деякі факти з різницевого числення в кільці многочленів над полем характеристики p. Різницевий оператор в кільці $K[x]$ визначається для елемента $a \in K$ як відображення $\Delta_a : K[x] \to K[x]$, яке задається рівністю

$$\Delta_a f(x) = f(x + a) - f(x), \quad f(x) \in K[x]. \tag{10}$$

Відображення Δ_a є лінійним, тобто для довільних многочленів f, $g \in K[x]$ і будь-яких $\alpha, \beta \in K$ виконується співвідношення

$$\Delta_a(\alpha f + \beta g) = \alpha \Delta_a f + \beta \Delta_a g. \tag{11}$$

Крім того, мають місце такі очевидні рівності:

(i) $\Delta_0 f = 0$, $\Delta_a(\text{const}) = 0$;

(ii) $\Delta_a \Delta_b f = \Delta_b \Delta_a f$;

(iii) $\Delta_a(f(x) \cdot g(x)) = f(x + a)\Delta_a g(x) + g(x)\Delta_a f(x)$.

Символом Δ_a^l позначатимемо l-тий степінь оператора Δ_a і нехай $cm.f(x)$ — степінь многочлена $f(x)$.

Лема 2.1. *Для довільного многочлена $f(x)$, ст.$f(x) = n$, при кожному натуральному l, $l \leq n$, має місце рівність*

$$\Delta_a^l f(x) = \sum_{k=0}^{l} (-1)^k C_l^k f(x + ka). \tag{12}$$

Якщо $l \geq n + 1$, то $\Delta_a^l f(x) = 0$.

Доведення рівності (12) легко здійснюється індукцією за числом l з урахуванням рівностей (10) і (11). Оскільки степінь многочлена $\Delta_a^r f(x)$ принаймні на 1 менший ніж степінь многочлена $\Delta_a^{r-1} f(x)$ $(1 \leq r \leq l)$, то $\Delta_a^{n+1} f = 0$.

Означення 2.1. *Многочлен $f(x) \in K[x]$, $\operatorname{char} K = p$, називається p-многочленом, якщо $f(x) \in K[x^p]$.*

Кожен p-многочлен має вигляд

$$f(x) = a_1 x^{p^{k_1}} + a_2 x^{p^{k_2}} + \cdots + a_s x^{p^{k_s}} + a_{s+1},$$

де $a_i \in K$, $1 \leq i \leq s + 1$, $k_1 > k_2 > \cdots > k_s \geq 1$.

Лема 2.2. *Нехай $f(x) \in K[x]$ є p-многочленом. Для довільного елемента $a \in K$ має місце рівність*

$$\Delta_a f(x) = f(a) - a_{s+1}. \tag{13}$$

Доведення. Якщо $a = 0$, то рівність (13) є окремим випадком рівності (i), що характеризує основні властивості різницевого оператора. Нехай $a \neq 0$. Тоді при довільному натуральному s отримаємо

$$\Delta_a(x^{p^s}) = (x + a)^{p^s} - x^{p^s} = x^{p^s} + a^{p^s} - x^{p^s} = a^{p^s}.$$

Звідси, враховуючи співвідношення (11), для p-многочлена $f(x)$ отримуємо

$$\Delta_a f(x) = a_1 a^{p^{k_1}} + a_2 a^{p^{k_2}} + \cdots + a_s a^{p^{k_s}} = f(a) - a_{s+1},$$

тобто має місце рівність (13).

□

З леми 2 випливає, що для будь-якого p-многочлена його образ при дії різницевим оператором є деякою константою, тобто має місце включення

$$\Delta_a(K[x^p]) \subseteq K. \tag{14}$$

Нехай натуральне число k має розклад

$$k = d_0 + d_1 p + \dots + d_s p^s, \quad d_s = 0, 0 \le d_i < p,$$

за основою p. Символом $\sigma_p(k)$ позначимо найменший індекс i ($0 \le i < s$) такий, що $d_i \ne 0$.

Лема 2.3. *Для довільного елемента $a \in K$, $a \ne 0$, має місце рівність*

$$\text{ст.}\Delta_a(x^k) = k - p^{\sigma_p(k)}. \tag{15}$$

Доведення. Припустимо, що $\sigma_p(k) = t$. Тоді $d_0 = d_1 = \dots = d_{t-1} = 0$, $d_t \ne 0$, а тому

$$\Delta_a(x^k) = (x+a)^{d_t p^t}(x+a)^{d_{t+1}p^{t+1}} \dots (x+a)^{d_s p^s} - x^k =$$

$$= (x^{p^t} + a^{p^t})^{d_t}(x^{p^{t+1}} + a^{p^{t+1}})^{d_{t+1}} \dots (x^{p^s} + a^{p^s})^{d_s} - x^k.$$

Розкриваючи дужки в кожному множнику першого доданка останнього виразу і виділяючи в такому розкладі перші два доданки, дістанемо

$$\Delta_a(x^k) = (x^{p^t \cdot d_t} + C^1_{d_t} x^{p^t(d_t-1)} a^{p^t} + \dots)(x^{p^{t+1}d_{t+1}} + C^1_{d_{t+1}} x^{p^{t+1}(d_{t+1}-1)} a^{p^{t+1}} +$$

$$+ \dots) \dots (x^{p^s d_s} + C^1_{d_s} x^{p^s(d_s-1)} a^{p^s}) - x^k.$$

Одночлен найвищого степеня в цьому виразі дістанемо, вибираючи з першої дужки другий доданок, а з усіх інших дужок — перший, тобто цей одночлен дорівнює

$$a^{p^t} \cdot C^1_{d_t} x^{p^t(d_t-1)} \cdot x^{p^{t+1}d_{t+1}} \dots x^{p^s d_s} = a^{p^t} C^1_{d_t} x^{k-p^t}.$$

Оскільки $a \ne 0$, то $a^{p^t} \ne 0$, а з нерівності $0 < d_t < p$ випливає, що $C^1_{d_t} \ne 0$. Отже, вибраний одночлен входить в многочлен $\Delta_a(x^k)$ з ненульовим коефіцієнтом. Звідси й дістаємо рівність (15).

□

Із леми 3 випливає, що при знаходженні степеня многочлена $\Delta_a f(x)$, $f(x) \in K[x]$ потрібно:

1) знайти значення виразу (15) для кожного одночлена многочлена $f(x)$;

2) вибрати ті одночлени $f(x)$ (їх може бути кілька!), для яких значення виразу (15) є максимальним;

3) пересвідчитися, що сума відповідних одночленів у значенні різницевого оператора відмінна від нуля.

3 Підгрупа p-тих степенів групи $UJ_2(K)$

Лема 3.1. *Для довільного натурального k і довільного перетворення $u = [a, b(x)] \in UJ_2(K)$ має місце рівність*

$$u^k = \Big[ka, \sum_{i=0}^{k} b(x+ia)\Big]. \tag{16}$$

Доведення — індукція за числом k.

Лема 3.2. *Для довільного натурального l і будь-якого $a \in K$, $a \neq 0$, має місце співвідношення*

$$\sum_{k=1}^{p-1} (ka)^l = \begin{cases} -a^l, & \text{якщо } (p-1)/l, \\ 0, & \text{в інших випадках.} \end{cases}$$

Доведення. Нехай спочатку $(p-1)/l$, тобто при деякому натуральному m виконується рівність $l = (p-1)m$. Тоді

$$\sum_{k=1}^{p-1} (ka)^l = \sum_{k=1}^{p-1} (ka)^{(p-1)m} = a^{(p-1)m} \sum_{k=1}^{p-1} k^{(p-1)m}.$$

Оскільки елементи $1, 2, \ldots, p-1$ містяться в мультиплікативній групі простого підполя поля K, то $k^{p-1} = 1$, а отже, й $k^{(p-1)m} = 1$ ($k = 1, 2, \ldots, p-1$). А тому маємо

$$\sum_{k=1}^{p-1} k^{(p-1)m} = p - 1 = -1 \quad (\text{в полі } K).$$

Таким чином, в першому випадку шукана сума дорівнює $-a^{(p-1)m} = -a^l$, що й треба було встановити.

Нехай тепер $(p-1) \not| l$. Тоді існують числа q, r такі, що

$$l = (p-1)q + r, \quad 0 < r < p-1.$$

Оскільки

$$k^l = k^{(p-1)q+r} = k^r \quad (1 \leq k \leq p-1),$$

то має місце рівність

$$\sum_{k=1}^{p-1} k^l = \sum_{k=1}^{p-1} k^r.$$

При $r = 1, 2, \ldots, p-1$ остання сума дорівнює нулю (див. [9, с.198–207]) і лему доведено. □

Нагадаємо, що підгрупою n-тих степенів у групі G називається підгрупа, породжена n-тими степенями всіх елементів із G (n — деяке натуральне число). Ця підгрупа є окремим прикладом вербальних підгруп в G, а тому вона є цілком характеристичною (ендоморфно допустимою) підгрупою G. Шириною підгрупи n-тих степенів в G називається найменше натуральне число m таке, що будь-який елемент цієї підгрупи розкладається на добуток не більше ніж m n-тих степенів елементів із G, а якщо таке число m не існує, то вважається, що ширина цієї підгрупи дорівнює ∞.

Теорема 3.1. *Нехай K — довільне поле характеристики p. Група $UJ_2(K)$ має експоненту p^2, а її підгрупа p-тих степенів збігається з центром і складається з перетворень вигляду $[0, c]$, $c \in K$. Ширина підгрупи p-тих степенів дорівнює 1.*

Доведення. 1) Пересвідчимося, що центр $Z(UJ_2(K))$ групи UJ_2 складається з перетворень вигляду $[0, c]$, $c \in K$. Нехай перетворення $u = [a, b(x)] \in UJ_2(K)$ міститься в $Z(UJ_2(K))$. Припустимо, що $a \neq 0$. Тоді для перетворення $v = [0, x]$ маємо

$$uv = [a, b(x) + x + a], \quad vu = [a, x + b(x)].$$

Оскільки $b(x) + x + a \neq x + b(x)$, то перетворення u, v не комутують. Отже, повинна виконуватися рівність $a = 0$, тобто $u = [0, b(x)]$.

Припустимо тепер, що $cm.b(x) \geq 1$. Тоді для перетворення $w = [1, 0]$ маємо

$$uw = [1, b(x)], \quad wu = [1, b(x+1)].$$

Оскільки $cm.b(x) \geq 1$, то $b(x) \neq b(x+1)$, тобто і в цьому випадку перетворення u, v не комутують. З іншого боку, довільне перетворення вигляду $[0, c]$, $c \in K$, комутує з будь-яким перетворенням із групи $UJ_2(K)$, а це й означає, що $Z(UJ_2(K))$ має потрібний вигляд.

2) Для довільного перетворення $[a, b(x)] \in UJ_2(K)$ за лемою 3.1 маємо

$$[a, b(x)]^p = \left[p \cdot a, \sum_{i=0}^{p} b(x + ia)\right] = [0, d(x)],$$

$d(x) \in K[x]$, а враховуючи рівність

$$[0, d(x)]^p = [0, p \cdot d(x)] = [0, 0],$$

звідси отримуємо, що

$$[a, b(x)]^{p^2} = [0, 0],$$

тобто група $UJ_2(K)$ має експоненту p^2.

3) Пересвідчимося, що для довільного перетворення $u = [a, b(x)] \in UJ_2(K)$ має місце включення $u^p \in Z(UJ_2(K))$. Згідно з доведеним в п. 2) маємо

$$u^p = \left[0, \sum_{i=0}^{p-1} b(x + ia)\right].$$

Нехай $b(x) = \sum_{j=0}^{m} a_j x^j$. Тоді дістаємо

$$\sum_{i=0}^{p-1} b(x + ia) = \sum_{i=0}^{p-1} \sum_{j=0}^{m} a_j (x + ia)^j = \sum_{j=0}^{m} a_j \sum_{i=0}^{p-1} (x + ia)^j.$$

Перетворимо внутрішню суму, використовуючи біном Ньютона:

$$\sum_{i=0}^{p-1} (x + ia)^j = \sum_{i=0}^{p-1} \sum_{r=0}^{j} C_j^r x^{j-r} (ia)^r.$$

Змінюючи порядок сумування дістаємо вираз

$$\sum_{r=0}^{j} C_j^r x^{j-r} \sum_{i=0}^{p-1} (ai)^r.$$

За лемою 3.2 внутрішня сума в цьому виразі відмінна від нуля лише при $(p-1)/r$. А тому дістаємо:

$$\sum_{i=0}^{p-1} (x+ia)^j = \begin{cases} -a^{p-1} & \text{при } j \equiv p-1 (\operatorname{mod} p), \\ 0 & \text{в інших випадках.} \end{cases}$$

Враховуючи це співвідношення, маємо

$$\sum_{i=0}^{p-1} b(x+ia) = -\sum_{j=0,\, j\equiv p-1(\operatorname{mod} p)}^{m} a_j a^{p-1}.$$

Отже, $u^p = [0, c]$, де

$$c = -\sum_{j=0,\, j\equiv p-1(\operatorname{mod} p)}^{m} a_j a^{p-1}.$$

Згідно з попереднім, для перетворення $[1, cx^{p-1}]$ маємо

$$[1, cx^{p-1}]^p = [0, c],$$

а тому довільне перетворення з центру $Z(UJ_2(K))$ є p-тим степенем деякого перетворення з групи $UJ_2(K)$.

Це означає, що підгрупа p-тих степенів групи $UJ_2(K)$ має ширину 1, тобто має місце рівність

$$[UJ_2(K)]^p = Z(UJ_2(K)).$$

Теорему повністю доведено.

□

4 Фактор-група за підгрупою p-многочленних перетворень

Многочлен $f(x)$ над полем K характеристики p називатимемо p'-многочленом, якщо він не містить одночленів вигляду ax^{p^k}, $k \in \mathbb{N} \cup \{0\}$.

Множину всіх p'-многочленів із $K[x]$ позначимо $K_0[x]$. Як і множина $K[x^p]$ всіх p-многочленів, $K_0[x]$ утворює підкільце кільця $K[x]$. Кожен многочлен із $K[x]$ розкладається на суму двох доданків, один з яких є p-многочленом, а другий — p'-многочленом, причому розклад однозначний з точністю до порядку доданків. Це означає, що кільце $K[x]$ розпадається на пряму суму підкілець:

$$K[x] = K[x^p] \oplus K_0[x].$$

Лема 4.1. *Множина P перетворень вигляду $[a, b(x)]$, $a \in K$, $b(x) \in K[x^p]$, утворює підгрупу в $UJ_2(K)$. Підгрупа групи P перетворень вигляду $[0, b(x)]$, $b(x) \in K[x^p]$ буде нормальною в $UJ_2(K)$.*

Доведення. Якщо $b(x) \in K[x^p]$, то при будь-якому $a \in K$ многочлен $b(x+a)$ також міститься в $K[x^p]$. Позначимо через Q — підгрупу унітрикутних перетворень вигляду $[0, b(x)]$, де $b(x)$ належить $K[x^p]$. А тому, якщо перетворення $u = [a_1, b_1(x)]$ і $v = [a_2, b_2(x)]$ належать до P, то многочлен $b_1(x) + b_2(x + a_1)$ є p-многочленом як сума двох p-многочленів, тобто $u \cdot v \in$P. Оскільки група $UJ_2(K)$ має експоненту p^2, то звідси дістаємо, що P — підгрупа в $UJ_2(K)$. Для довільного перетворення $u = [a, b(x)] \in UJ_2(K)$ і перетворення $v = [0, c(x)] \in Q$ маємо

$$u^{-1}vu = [0, c(x - a)],$$

а тому Q — нормальна підгрупа в $UJ_2(K)$.

□

Символом (u, v) позначатимемо комутатор перетворень $u, v \in UJ_2(K)$, тобто $(u, v) = u^{-1}v^{-1}uv$.

Лема 4.2. *Для довільних перетворень $u = [a_1, b_1(x)]$, $v = [a_2, b_2(x)]$ має місце рівність*

$$(u, v) = [0, \Delta_{-a_2} b_1(x - a_1) - \Delta_{-a_1} b_2(x - a_2)]. \tag{17}$$

Доведення. Перемножаючи перетворення у виразі $u^{-1}v^{-1}uv$, дістаємо

$$(u, v) = [0, -b_1(x - a_1) - b_2(x - a_1 - a_2) + b_1(x - a_1 - a_2) + b_2(x - a_2)].$$

Оскільки

$$-b_1(x-a_1)+b_1(x-a_1-a_2) = -\Delta_{-a_2}b_1(x-a_1),$$

$$-b_2(x-a_1-a_2)+b_2(x-a_2) = -\Delta_{-a_1}b_2(x-a_2),$$

то з попередньої рівності отримуємо рівність (17).

□

Лема 4.3. *Довільне перетворення* $[a, b(x)] \in UJ_2(K)$ *розкладається на добуток двох множників:*

$$[a, b(x)] = [0, g(x)][a, h(x)], \tag{18}$$

де $g(x)$ *—* p*-многочлен,* $h(x)$ *—* p'*-многочлен, причому* $b(x) = g(x) + h(x)$.

Доведення. Розкладемо многочлен $b(x)$ на суму p-многочлена і p'-многочлена в $K[x]$ і нехай $b(x) = g(x) + h(x)$ — такий розклад. Тоді для перетворень $[0, g(x)]$ і $[a, h(x)]$ має місце рівність (18).

Зауважимо, що при фіксованому порядку множників (перший належить до нормального дільника Q) розклад (18) є однозначним.

Нехай $\pi\colon K[x] \to K_0[x]$ — проектор, тобто для довільного многочлена $f(x) \in K[x]$ такого, що $f(x) = g(x)+h(x)$, $g(x) \in K[x^p]$, $h(x) \in K_0[x]$ маємо $\pi(f(x)) = h(x)$. Для довільних $a \in K$ і $f(x) \in K[x]$ покладемо

$$f^a(x) = \pi(f(x+a)). \tag{19}$$

Безпосередньо перевіряється, що множина G всіх пар вигляду $[a, b(x)]$, $a \in K$, $b(x) \in K_0[x]$, утворює групу відносно дії множення, визначеної рівністю

$$[a_1, b_1(x)][a_2, b_2(x)] = [a_1 + a_2, b_1(x) + b_2^{a_1}(x)],$$

де $[a_1, b_1(x)], [a_2, b_2(x)] \in G$, а $b_2^{a_1}(x)$ визначене рівністю (19).

□

Теорема 4.1. 1) *Взаємний комутант* $[Q, UJ_2(K)]$ *збігається з центром* $Z(UJ_2(K))$.

2) *Фактор-група* $UJ_2(K)/Q$ *ізоморфна групі* G.

Доведення. 1) Згідно з рівністю (17) комутатор (u, v), $u \in UJ_2(K)$, $v \in Q$ є перетворенням вигляду $[0, c(x)]$, де $c(x)$ — різниця двох многочленів вигляду $\Delta_a f$. Для одного з них $a = 0$, а для другого f є p-многочленом. Враховуючи властивість (i) різницевого оператора і лему 2, звідси дістаємо, що $(u, v) = [0, a]$, $a \in K$. Для довільного елемента $a \in K$ згідно з лемою 2.3 многочлен $\Delta_1(ax^p)$ має степінь 0. Більше того,

$$\Delta_1(ax^p) = a(x+1)^p - ax^p = a,$$

а тому для перетворень $u = [0, ax^p] \in Q$, $v = [1, 0] \in UJ_2(K)$ маємо

$$(u, v) = [0, \Delta_1(ax^p)] = [0, a].$$

Звідси дістаємо, що довільне перетворення з центру $Z(UJ_2(K))$ міститься в $[Q, UJ_2(K)]$, тобто має місце потрібна рівність.

2) Задамо відображення φ: $UJ_2 \to G$, поклавши для довільного перетворення $u = [a, b(x)] \in UJ_2(K)$:

$$\varphi(u) = [a, \pi(b(x))].$$

Безпосередньо перевіряється, що відображення φ є гомоморфізмом $UJ_2(K)$ на групу G. Ядро цього гомоморфізму складається з перетворень вигляду $[0, b(x)]$, де $\pi(b(x)) = 0$. Остання рівність означає, що $b(x)$ є p-многочленом, тобто $[0, b(x)] \in Q$. Отже, $\mathrm{Ker}\varphi = Q$ і за теоремою про гомоморфізм дістаємо співвідношення

$$UJ_2(K)/Q \cong G.$$

Теорему доведено. □

5 Енгелева довжина групи $UJ_2(K)$

Кратний комутатор

$$e_k(x, y) = (x, {}_k y) = (x, \underbrace{y, \ldots, y}_{k})$$

називається енгелевим довжини k. Група називається енгелевою довжини k (див., напр., [10, с. 81]), якщо в ній виконується тотожність

$e_k(x, y) \equiv 1$, тобто для довільних елементів g, h цієї групи справджується рівність $e_k(g, h) = 1$. Найменше число k, для якого така тотожність в групі виконується, називається її енгелевою довжиною.

Теорема 5.1. *Для довільного поля K характеристики p група $UJ_2(K)$ є енгелевою довжини $\leq p + 1$.*

Доведення. Пересвідчимося, що в групі $UJ_2(K)$ виконується тотожність $(x, {}_{p+1}y) = e$. Для довільних елементів u, $v \in UJ_2(K)$ комутатор (u, v) є елементом вигляду $[0, f(x)]$, $f(x) \in K[x]$. Нехай $v = [-a, b(x)]$. Тоді для $k \geq 1$ маємо

$$(u, {}_{k+1}v) = ([0, f(x)], {}_k v).$$

Комутатор перетворень $[0, f(x)]$ і $[-a, b(x)]$ дорівнює $[0, \Delta_a f(x)]$. Ітеруючи процес побудови кратного комутатора згідно з лемою 4.2, дістанемо

$$([0, f(x)], {}_k v) = \Big[0, \sum_{i=0}^{k} C_k^i (-1)^i f(x + ia)\Big].$$

Нехай $k = p$. Тоді в полі K маємо:

$$C_p^i = 0 \text{ при } i = 1, 2, \ldots, p - 1; \quad C_p^0 = 1; \; C_p^p = 1.$$

Отже,

$$\sum_{i=0}^{p} C_p^i (-1)^i + (x + ia) = (-1)^0 f(x) + (-1)^p f(x + pa) = f(x) - f(x) = 0.$$

Таким чином,

$$([0, f(x)], {}_p v) = [0, 0],$$

а це й означає, що має місце рівність $(u, {}_{p+1}v) = e$. Оскільки u, v — довільні перетворення із $UJ_2(K)$, то в цій групі виконується тотожність $e_{p+1}(x, y) \equiv 1$, що й треба було довести.

□

Приклад 1. *Нехай $K = Z_2$ — поле лишків за модулем 2. Оберненим до перетворення $[0, f(x)] \in UJ_2(Z_2)$ буде воно саме, а оберненим* *до перетворення* $[1, f(x)]$ *— перетворення* $[1, f(x+1)]$. *А тому, комутатор* (u, v) *перетворень вигляду* $u = [0, f(x)]$ *і* $v = [1, g(x)]$ *дорівнює* $[0, f(x+1)+f(x)]$, *а для перетворень вигляду* $u = [1, f(x)]$, $v = [1, g(x)]$ *маємо* $(u, v) = [0, f(x+1)+f(x)+g(x+1)+g(x)]$. *Якщо перетворення* $w \in UJ_2(K)$ *має вигляд* $[0, h(x)]$, *то* $(u, v, w) = e$, *а якщо воно має вигляд* $[1, h(x)]$, *то*

$$((u, v), w) = [0, f(x+1+1) + f(x+1) + g(x+1+1) + g(x+1)+$$

$$+f(x+1) + f(x) + g(x+1) + g(x)] = [0, 0].$$

Таким чином, в групі $UJ_2(Z_2)$ виконується тотожність $(x, y, z) \equiv 1$, тобто вона є нільпотентною класу 2. А тому, ця група буде також енгелевою довжини 2, тобто оцінка енгелевої довжини, встановлена в теоремі 5.1, в цьому випадку не є точною.

[1] *van der Essen A.* Polynomial Automorphisms and the Jacobian Conjecture. — Basel: Bickhausen Verlag, 2000. — 329 p.

[2] *Mikhalev A.A., Shpilrain V., Yu J.-T.* Combinatorial Methods. Free groups, Polynomical and Free Algebras. — New-York etc.: Springer, 2004. — 314 p.

[3] *van der Kulk W.* On polynomial rings in two variables. // Niew. Archief voor Wiskunde. — 1953. — **1**, №3. — P. 33–41.

[4] *Shafarevich J.R.* On some infinite-dimensional groups. // Rend. Math. Appl. — 1966. — **25**. — P. 208–212.

[5] *Lami S.* Une preuve geometrique du theoreme de Jung. // L'Enseignement Mathematique. — 2002. — **48**. — P. 291–315.

[6] *Довгей Ж., Сущанський В.* Будова групи унітрикутних автоморфізмів кільця многочленів від двох змінних над полем характеристики нуль. // Математичний вісник НТШ. — 2010. — **6**. — С. 84–95.

[7] *Довгей Ж.* Вербальні підгрупи групи трикутних автоморфізмів кільця многочленів від двох змінних над полем характеристики 0 // Вісник Київського університету імені Тараса Шевченка. Сер. фіз.-мат. н. — 2011. — **4.** — С. 18–26.

[8] *Довгей Ж., Сумарюк М.* Вільні піднапівгрупи у групі автоморфізмів кільця многочленів від двох змінних над числовими полями // Карпатські мат. публ. — 2011. — **3**, №2. — С. 64–70.

[9] *Кострикин А.И.* Введение в алгебру. Часть 3. — Москва: Физматгиз, 2004. — 271 с.

[10] *Lennox J.C., Robinson D.J.S.* The Theory of Infinite Soluble Groups. — Oxford: Oxford Sci. Publ., 2004. — 342 p.

UNITRIANGLE AUTOMORPHISMS OF THE TWO VARIABLE POLYNOMIAL RING OVER A FIELD OF CHARACTERISTIC $P > 0$

Zhanna DOVGHEI[1], *Vitaliy SUSHCHANSKYY*[2]

[1] Yuriy Fed'kovych Chernivtsi National University,
2 Kotsyubynskyi Str., Chernivtsi 58012, Ukraine
[2] Institute of Mathematics, Silesian University of Technology
44-100 Gliwice, Poland

e-mail: *janacucureac@mail.ru, Vitaliy.Sushchanskyy@polsl.pl*

A basic properties of the unitriangle automorphism group of the two variable polynomial ring over a field of characteristic $p > 0$ are investigated. We characterize the $p > 0$-power werbal subgroup, found its width and we estimate the Engel length of the unitriangle automorphism group.