УДК 512.76

©2012 р. Ж.І. Довгей

Чернівецький національний університет імені Юрія Федьковича

НІЛЬПОТЕНТНІСТЬ ГРУПИ УНІТРИКУТНИХ АВТОМОРФІЗМІВ КІЛЬЦЯ МНОГОЧЛЕНІВ ВІД ДВОХ ЗМІННИХ НАД СКІНЧЕННИМ ПОЛЕМ

Доведено, що група унітрикутних автоморфізмів кільця многочленів $K[x,y]$ від двох змінних над скінченним полем є нільпотентною, наведено нижню оцінку для класу нільпотентності цієї групи, з якої випливає, що клас нільпотентності зростає з ростом числа елементів поля.

It is proved that the group of unitriangl automorphisms of the two variable polynomial ring over a finite field is nilpotent.

1. Вступ. Нехай K – фіксоване поле, $K[x,y]$ – кільце многочленів від змінних x,y над полем K, $G = AutK[x,y]$ – група автоморфізмів $K[x,y]$. Кожен автоморфізм кільця многочленів $K[x,y]$ однозначно визначається образами твірних елементів $x,y \in K[x,y]$:

$$x \mapsto a(x,y), y \mapsto b(x,y), \tag{1}$$

причому ці образи повинні бути такими многочленами з $K[x,y]$, щоб відображення кільця $K[x,y]$ в себе, яке задається відповідністю

$$f(x,y) \mapsto f(a(x,y), b(x,y)),$$

$f(x,y) \in K[x,y]$, продовжувалося до такої бієкції $K[x,y]$ в себе, що обернене відображення також поліноміальне.

Автоморфізм u, який визначає пара (1), діє на довільний многочлен $f(x,y) \in K[x,y]$ таким чином

$$u(f(x,y)) = f(a(x,y), b(x,y)).$$

Автоморфізм $\langle a(x,y), b(x,y)\rangle$ *трикутний*, якщо його перша компонента не залежить від змінної y. Для трикутних автоморфізмів функція $x \to a(x)$ має бути оборотною. З умови оборотності випливає, що в такому разі многочлен $a(x,y)$ повинен бути лінійним, тобто мати вигляд $\alpha x + \beta$. Враховуючи це, дістаємо, що многочлен $b(x,y)$ також повинен мати "трикутний" вигляд $\alpha y + f(x)$, де $\alpha \neq 0, f(x) \in K[x]$.

Отже, трикутний автоморфізм визначається перетвореннями вигляду

$$u(x) = ax + b, \quad u(y) = cy + d(x), \tag{2}$$

де a, b, $c \in K$, $a \neq 0$, $c \neq 0$, $d(x) \in K[x]$.

А тому, трикутні автоморфізми – це автоморфізми, що задаються парами вигляду

$$\langle \alpha_1 x + \beta_1, \alpha_2 y + f(x)\rangle,$$

де $\alpha_1, \beta_1, \alpha_2 \in K, \alpha_1 \cdot \alpha_2 \neq 0$, $f(x) \in K[x]$.

Трикутні автоморфізми (їх називають ще елементарними) утворюють підгрупу в групі всіх автоморфізмів $K[x,y]$, яку називають афінною групою Жонк'єра (інакше, групою елементарних перетворень) кільця $K[x,y]$ і позначають символом $J_2(K)$ (докладніше див.[1], [2]).

Група Жонк'єра $J_2(K)$ містить підгрупу унітрикутних автоморфізмів $UJ_2(K)$, тобто автоморфізмів вигляду (2), для яких $a = 1$, $c = 1$. Унітрикутне перетворення φ_u, задане рівностями

$$\varphi_u(x) = x + a, \quad \varphi_u(y) = y + b(x)$$

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

$$uv = [a_1 + a_2, b_1(x) + b_2(x + a_1)]. \tag{3}$$

А тому групу $UJ_2(K)$ можна ототожнити з групою найможливіших наборів вигляду

$[a, b(x)]$, $a \in K$, $b(x) \in K[x]$, з правилом множення, що задається рівністю (3). 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 [3], [4], [5] розпочато дослідження груп $J_2(K)$ і $UJ_2(K)$ над полями характеристики нуль, в роботі [6] – вивчення властивостей групи $UJ_2(K)$ над полями характеристики $p > 0$ та розвинуто теорію різницевих операторів в кільцях многочленів над такими полями.

В даній роботі продовжується дослідження $UJ_2(K)$ в тому випадку, коли поле K є скінченним. Встановлено, що для довільного такого поля K група $UJ_2(K)$ є нільпотентною. За допомогою відомих результатів про клас нільпотентності вінцевих добутків елементарних абелевих p-груп наведено нижню оцінку для класу нільпотентності $UJ_2(K)$.

2. Нільпотентність групи $UJ_2(K)$ ***над скінченним полем.*** Нехай $K = F_q$ є скінченним полем, $q = p^m$, де p – деяке просте, а m – натуральне число. Група $UJ_2(F_q)$ є нескінченною, локально – скінченною групою показника p^2. Нехай $F_q^s[x]$ – підгрупа многочленів степеня $\leqslant s$ в $F_q[x]$ ($s = 0, 1, 2, \ldots$). Множина перетворень

$$U_q^s = \{[a, f(x)] | f(x) \in F_q^s[x]\}$$

є підгрупою групи $UJ_2(F_q)$, яка має порядок

$$|U_q^s| = q \cdot q^{s+1}.$$

А тому, підгрупа U_q^s нільпотентна $(s = 0, 1, 2, \ldots)$. Оскільки

$$UJ_2(F_q) = \bigcup_{i=0}^{\infty} U_q^s,$$

то група $UJ_2(F_q)$ є локально нільпотентною. Насправді, в цьому випадку можна сказати більше.

Нагадаємо, що різницевий оператор в кільці $K[x]$ визначається (див., напр. [6]) для елемента $a \in K$ як відображення $\Delta_a : K[x] \to K[x]$, яке задається рівністю

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

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

$$\Delta_a(\alpha f + \beta g) = \alpha \Delta_a f + \beta \Delta_a g.$$

Крім того, мають місце такі очевидні рівності:

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

(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 *ст.*$f(x)$ – степінь многочлена $f(x)$.

Наведемо таке допоміжне твердження.

Лема 1. Для довільних перетворень $u = [\alpha, f(x)]$ і $v = [\beta, g(x)]$ із групи $UJ_2(K)$ мають місце рівності

$$a) \quad u^{-1}vu =$$
$$= [\beta, -f(x - \alpha) + g(x - \alpha) + f(x - \alpha + \beta)];$$
$$b) (u, v) = u^{-1}v^{-1}uv =$$
$$= [0, -f(x - \alpha) - g(x - \alpha - \beta) +$$
$$+ f(x - \alpha - \beta) + g(x - \beta)].$$

Доведення див. [6].

Теорема 2. Для довільних p і m група $UJ_2(F_q), q = p^m$, є нільпотентною.

Доведення. Група $UJ_2(F_q)$ буде нільпотентною, якщо існує таке натуральне число c, що простий комутатор

$$(x_1, x_2, \ldots, x_c) \tag{4}$$

є тотожністю в цій групі. Згідно з лемою 1 комутатор довільних двох перетворень має вигляд $[0, f(x)]$, де $f(x) \in F_q[x]$. Комутатор цієї пари з довільною парою $[a, b(x)]$ має вигляд $[0, \Delta_a f(x)]$, тобто залежить лише від першої координати пари. А тому при $c \geqslant 3$ значення простого комутатора вигляду (4) на довільних перетвореннях $u_1, u_2, \ldots, u_s$ із $UJ_2(F_q)$ має вигляд

$$[0, \Delta_{a_1} \Delta_{a_2} \ldots \Delta_{a_{c-2}} f(x)],$$

де $f(x) \in F_q[x], a_1, a_2, \ldots, a_{c-2} \in F_q$. Оскільки символи операторів Δ_{a_i} у виразі $\Delta_{a_1}\Delta_{a_2}\ldots\Delta_{a_k}f(x)$ комутують, то їх можна перегрупувати так, щоб оператори з однаковими параметрами a_i стояли поряд. А тому цей вираз може бути переписаний у вигляді

$$\Delta_{a_{i_1}}^{r_1}\Delta_{a_{i_2}}^{r_2}\ldots\Delta_{a_{i_t}}^{r_t}f(x), \tag{5}$$

де $a_{i_1}, a_{i_2}, \ldots, a_{i_t}$ є попарно різними елементами із F_q. При цьому якщо один з елементів a_{i_l} $(1 \leqslant l \leqslant t)$ дорівнює нулю, або один з показників r_l більший або рівний p, то многочлен, який визначається цим виразом дорівнює нулю. Виберемо число k так, щоб виконувалась нерівність

$$(p^m - 1)(p - 1) > k$$

тоді для виразу (5) має місце нерівність

$$r_1 + r_2 + \ldots + r_t > (p^m - 1)(p - 1).$$

Число t не може перевищувати кількість ненульових елементів поля, тобто $t \leq p^m - 1$. А тому принаймні одне з чисел r_l $(1 \leqslant l \leqslant t)$ мусить бути не меншим ніж p. Таким чином, для таких значень k при довільному многочленові $f(x) \in F_q[x]$ і довільних елементів $a_1, a_2, \ldots, a_k \in F_q$ має місце рівність

$$\Delta_{a_1}\Delta_{a_2}\ldots\Delta_{a_k}f(x) \equiv 0.$$

А це й означає, що для довільних перетворень $u_1, u_2, \ldots, u_k \in UJ_2(F_q)$ виконується рівність

$$(u_1, u_2, \ldots, u_k) = e,$$

тобто простий комутатор $(x_1, x_2, \ldots, x_k)$ є тотожністю в $UJ_2(F_q)$. Теорему доведено.

Для того, щоб оцінити знизу клас нільпотентності групи $UJ_2(F_q)$ розглянемо гомоморфізм цієї групи на вінцевий добуток двох елементарних абелевих груп порядку p^m. Вінцевий добуток $W(m,p) = C_p^m \quad wr \quad C_p^m$ двох елементарних абелевих p-груп рангу m можна розглядати таким чином. Ототожнимо групу C_p^m з адитивною групою поля F_q. Елементами вінцевого добутку $W(m,p)$ є пари $[a, f]$, де $a \in C_p^m$ і f – довільне відображення із C_p^m в C_p^m, а правило множення задається рівністю

$$[a_1, f_1][a_2, f_2] = [a_1 + a_2, f_1 + f_2^{a_1}],$$

де f^a– відображення із C_p^m в C_p^m, визначене рівністю

$$f^a(x) = f(x + a), x \in C_p^m.$$

При ототожненні групи C_p^m з адитивною групою поля F_q кожне відображення $f : C_p^m \to C_p^m$ ототожнюється з відображенням $F_q \to F_q$ поля F_q в себе.

Лема 3. Кожна скрізь визначена функція $f : F_q \to F_q$ задається деяким многочленом. Два многочлена f_1 і f_2 із $F_q[x]$ завдають одну й ту ж функцію тоді й лише тоді, коли

$$f_1(x) \equiv f_2(x) mod(x^q - x). \tag{6}$$

Доведення. Функція f визначена своєю (скінченною) таблицею значень

0	a_1	$\ldots$	a_{q-1}
$f(0)$	$f(a_1)$	$\ldots$	$f(a_{q-1})$

де $a_1, a_2, \ldots, a_{q-1}$ – ненульові елементи поля F_q, а тому однозначно задається інтерполяційним многочленом у формі Лагранжа, який обчислюється за цією таблицею (див.[7], стор. 158). Оскільки мультиплікативна група F_q^* має порядок $q-1$, то для довільного елемента $a \in F_q^*$ виконується умова $a^{q-1} = 1$, звідки дістаємо $a^q - a = 0$. Отже, многочлен $x^q - x$ в будь-якій точці $x \in F_q$ набуває значення 0, тобто завдає тотожно рівну нулю функцію. Таку ж властивість має кожен многочлен, що кратний $x^q - x$, і навпаки, кожен многочлен, який завдає тотожно рівну нулю функцію, ділиться на $x^q - x$. А це й означає, що має місце конгруенція (6). Лему доведено.

Лема 4. Вінцевий добуток

$$W(p,m) = C_p^m \quad wr \quad C_p^m$$

є нільпотентною групою класу $m(p-1)+1$.
Доведення див. [8].

Нехай $C(G)$ – клас нільпотентності групи G.

Теорема 5. Для довільних p і m клас нільпотентності групи $UJ_2(F_q)$ задовольняє нерівність

$$c(UJ_2(F_q)) \geqslant m(p-1) + 1. \tag{7}$$

Доведення. Нехай $Fun(F_q)$ – множина скрізь визначених функцій над полем F_q, тобто $|Fun(F_q)| = q^q$. Задамо відображення $\gamma : F_q[x] \to Fun(F_q)$, поклавши для довільного многочлена $f(x) \in F_q[x]$, що $\gamma(f(x))$ – це функція, яка визначена цим многочленом над F_q. Очевидно, виконуються співвідношення:

$$a) \quad \gamma(f(x) + g(x)) = \gamma(f(x)) + \gamma(g(x)),$$

$f(x), g(x) \in F_q[x]$;

$$b) \quad \gamma(f(x + a)) = (\gamma f)(x + a),$$

$f(x) \in F_q[x], a \in F_q$.

Користуючись цим, задамо відображення π із $UJ_2(F_q)$ у вінцевий добуток $W(p, m)$, поклавши для кожного перетворення $[a, f]$ із $UJ_2(F_q)$: $\pi([a, f]) = [a, \gamma(f)]$. Пересвідчимося, що відображення π є епіморфізмом. Якщо f пробігає $F_q[x]$, то $\gamma(f)$ пробігає $FunF_q$, а тому π є сюр'єктивним. Покажемо, що воно має властивість гомоморфності. Нехай $[a_1, f_1]$ і $[a_2, f_2]$ – довільні два перетворення із $UJ_2(F_q)$. Маємо

$$\begin{gathered}
\pi([a_1, f_1] \cdot [a_2, f_2]) = \\
= \pi([a_1 + a_2, f_1(x) + f_2(x + a)]) = \\
= [a_1 + a_2, \gamma(f_1(x) + f_2(x + a))] = \\
= [a_1 + a_2, \gamma(f_1(x)) + \gamma(f_2(x + a))] = \\
= [a_1 + a_2, \gamma(f_1(x)) + (\gamma f_2)(x + a)] = \\
= [a_1, \gamma(f_1(x))][a_2, \gamma(f_2(x))] = \\
= \pi([a_1, f_1])\pi([a_2, f_2]).
\end{gathered}$$

Отже, відображення π є гомоморфізмом.

Таким чином, вінцевий добуток $W(p, m)$ є гомоморфним образом групи $UJ_2(F_q)$. А тому для класу нільпотентності цих груп маємо нерівність

$$c(UJ_2(F_q)) \geqslant c(W(p, m)).$$

Тепер нерівність (7) випливає з леми 4 і теорему доведено.

Таким чином, із зростанням числа m клас нільпотентності груп $UJ_2(F_q), q = p^m$, строго зростає.

СПИСОК ЛІТЕРАТУРИ

1. *Arno van der Essen.* Polynomial Automorphisms and the Jacobian Conjecture / Arno van der Essen // Basel: Bickhausen Verlag. – 2000. – 329 p.

2. *Alexander A. Mikhalev.* Combinatorial Methods. Free groups, Polynomical and Free Algebras/ Alexander A. Mikhalev, Vladimir Shpilrain, Jee-Tai Yu.// New-York etc.: Springer. – 2004. – 314 p.

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

4. *Довгей Ж.І.* Вербальні підгрупи групи трикутних автоморфізмів кільця многочленів від двох змінних над полем характеристики 0 / Ж.І. Довгей// Вісник Київського університету імені Тараса Шевченка. Серія фізико-математичні науки. – 2011. – Вип.4. – С. 18-26.

5. *Довгей Ж.І.* Вільні піднапівгрупи у групі автоморфізмів кільця многочленів від двох змінних над числовими полями / Ж.І. Довгей, М.І. Сумарюк // Карпатські математичні публікації. – 2011. – **3**, N2. – С. 64 - 70.

6. *Довгей Ж.І.* Унітрикутні автоморфізми кільця многочленів від двох змінних над полем характеристики $p > 0$ / Ж.І. Довгей, В.І. Сущанський // Математичний вісник НТШ. – 2012. – **Т. 9**. – С. 108-123.

7. *Курош А.Г.* Курс высшей алгебры. / А.Г. Курош // Москва: Наука. – 1971. – 432 с.

8. *Сущанський В.И.* Сплетения элементарных абелевых групп / В.И. Сущанський // Мат. заметки. – 1972. – **11**. – С. 61-72.