

ПРО НАПІВДОСКОНАЛІ КІЛЬЦЯ З ЗАДАНИМИ ПРИЄДНАНИМИ ГРУПАМИ

О.Д. АРТЕМОВИЧ, Ю.Б. ІЩУК

O.D. Artemovych, Yu.B. Ishchuk. *On semiperfect rings with the prescribed adjoint groups* // Matematychni Studii, **6** (1996) P.23–32.

The semiperfect rings with the periodic (correspondently p -group, polycyclic, Černikov, simple) groups are characterized.

1. Вивченню спеціальних типів асоціативних кілець, приєднані групи яких належать до одного із відомих класів груп, присвячено багато робіт (див., наприклад, [1–10]).

В даній роботі охарактеризовано напівдосконалі кільця з періодичною (відповідно p -групою, поліциклічною, черніковською, простою) квазірегулярною групою.

Позначення:

$K \rtimes T$ – напівпрямий добуток груп K та T ;

p – просте число;

$GF(q)$ – скінченне поле порядку q , $q = p^n$ ($n \in \mathbb{N}$);

$M_m(q)$ – повне кільце матриць порядку m з елементами із поля $GF(q)$;

$GL_m(q)$ – повна лінійна група матриць порядку m з елементами із поля $GF(q)$;

R^+ – адитивна група кільця R ;

R° – приєднана (=квазі-регулярна) група кільця R ;

$\mathcal{U}(R)$ – група одиниць кільця R ;

$\mathcal{J}(R)$ – радикал Джекобсона кільця R ;

$1 + \mathcal{J}(R)$ – уніпотентна група кільця R ;

$\mathcal{F}(R)$ – періодична частина кільця R ;

$\text{char } R$ – характеристика кільця R ;

T^* – мультиплікативна група тіла T ;

$\pi(G)$ – множина всіх простих дільників порядків елементів періодичної групи G ;

$Z(G)$ – центр групи G ;

$Z(R)$ – центр кільця R ;

$C_G(a) = \{g \in G \mid ga = ag\}$ – централізатор елемента a в групі G ;

$C_R(a) = \{r \in R \mid ra = ar\}$ – централізатор елемента a в кільці R ;

$\mathbb{Z}_m$ – група (кільце) лишків за модулем m ;

Надалі будемо часто використовувати

Твердження 1.1. *Нехай R – кільце.*

1. *Якщо F – підкільце кільця R , то F° – підгрупа приєднаної групи R° .*
2. *Якщо I – ідеал кільця R , то I° – нормальна підгрупа приєднаної групи R° .*
3. *$(R/\mathcal{J}(R))^\circ \cong R^\circ/\mathcal{J}(R)^\circ$.*
4. *Якщо R – кільце з одиницею, то*
 - а) $R^\circ \cong \mathcal{U}(R)$;
 - б) $\mathcal{U}(1 + \mathcal{J}(R)) \cong \mathcal{J}(R)^\circ$;
 - в) $\mathcal{U}(R)/1 + \mathcal{J}(R) \cong \mathcal{U}(R/\mathcal{J}(R))$.

Нагадаємо також, що кільце R з одиницею називається *напівдосконалим*, якщо фактор-кільце $R/\mathcal{J}(R)$ класично-напівпросте, і ідемпотенти можна піднімати за модулем радикала Джекобсона $\mathcal{J}(R)$.

Решта позначень і фактів стандартні і їх можна знайти, наприклад, в [11–13].

2. Наступна лема впливає із [14] і [15].

Лема 2.1. *Для тіла T рівносильні такі твердження:*

- 1) T^* – періодична група;
- 2) T^* – локально скінченна група;
- 3) T^* – локально циклічна група;
- 4) T^* вкладається в фактор-групу $\mathbb{Q}/\mathbb{Z}$;
- 5) T^* – зліченна періодична абелева група;
- 6) T – поле простої характеристики p , алгебраїчне над простим підполем, і, як наслідок, T^* – p' -група;
- 7) $T^* \cong \sum_{r \in \pi}^\otimes T_r$, π – множина всіх простих чисел, T_r – підгрупа квазіциклічної r -групи $\mathbb{C}_{r^\infty}$, $T_p = 1$.

Поле T , яке задовольняє умови леми 2.1, називається *абсолютним*.

Лема 2.2. *Нехай R – радикальне кільце, породжене одним елементом. Якщо приєднана група R° періодична, то R – нільпотентне кільце.*

Доведення ведеться за тією ж схемою, як і в лемі 3 [16]. Для повноти викладу наведемо його.

Зрозуміло, що кільце R – гомоморфний образ вільної радикальної $\mathbb{Z}$ -алгебри F , породженої одним елементом. Тоді $R \cong F/I$ для деякого ідеала I . Якщо через F' позначимо кільце, отримане приєднанням до F одиничного елемента 1 природним чином, то воно є підкільцем $\mathbb{Z}(x)$, породженим F та 1. Тоді I – також ідеал F' . Відображення $F/I \rightarrow F'/I$,

$$\frac{f}{1+g} + I \mapsto \left(1 - \frac{f}{1+g}\right) + I, \text{ де } f, g \in x\mathbb{Z}[x],$$

задає гомоморфізм приєднаної групи $(F/I)^\circ$ на мультиплікативну групу $G' = \{(1+f)/(1+g) + I | f, g \in x\mathbb{Z}[x]\}$. Тому G' – періодична група.

Нехай $g^* = x^n(\alpha_0 + \dots + \alpha_m x^m)$, де $\alpha_0 \neq 0, \alpha_m \neq 0$, – многочлен найменшого степеня в I . Якщо $m \geq 1$, то знайдеться таке ненульове комплексне число z , що $g^*(z) \equiv 0$. Оскільки g^* має найменший степінь в I , то z – корінь кожного многочлена із I .

Нехай H – підгрупа із G' , що складається із тих елементів G' , які можна записати у вигляді $(1 + f)/(1 + g) + I$, де $f(z) \neq -1$, $g(z) \neq -1$, і поставимо у відповідність кожному такому елементу із H ненульове комплексне число $(1 + f(z))/(1 + g(z))$. Ця відповідність задає гомоморфізм φ групи H в мультиплікативну групу комплексних чисел. Окрім того, H – періодична група.

Далі, $1 + \beta(\alpha + g^*/x^n) + I$, де β – довільне ціле число, є елементом із H , і відображається φ в комплексне число $1 + \beta\alpha_0$. Нехай M – образ H стосовно φ . Тоді M містить множину $\{1 + \beta\alpha_0 \mid \beta \in \mathbb{Z}\}$. Оскільки M – періодична група, то $\{1 + \beta\alpha_0 \mid \beta \in \mathbb{Z}\} = \{-1, 1\}$. Отримана суперечність показує, що поліном найменшого степеня в I має вигляд $\alpha_0 x^n$. Із таких поліномів найменшого степеня в I , наприклад, αx^N має мінімальне α . Якщо $\beta x^l \in I$ та $t = \max\{N, l\}$, то $\beta x^t \in I$ та $\alpha x^t \in I$. Використовуючи алгоритм Евкліда, отримаємо, що внаслідок мінімальності α число β ділить α . Доведемо, що $I \subseteq \alpha F$ від супротивного. Якщо $I \not\subseteq \alpha F$, то знайдеться такий многочлен $f = x^u(\beta_0 + \beta_1 x + \dots + \beta_v x^v) \in I$, де $\beta_0 \neq 0, \beta_v \neq 0$, що не всі його коефіцієнти діляться на α . Серед усіх таких многочленів виберемо той, в якого v – мінімальне, а серед них – з найменшим β_0 . Не зменшуючи загальності, можемо брати $u \geq N$. Знову використовуючи алгоритм Евкліда, легко перевірити, що β_0 ділить α , і тому $(\alpha/\beta_0)f - \alpha x^u \in I$. Внаслідок максимальності v всі коефіцієнти многочлена $(\alpha/\beta_0)f - \alpha x^u$ діляться на α . Отже, β_0 ділить кожний коефіцієнт β_j ($j = 1, \dots, v$) та $f = \beta_0 x^u(1 + g)$, де $g \in x\mathbb{Z}[x]$. Із $f \in I$ маємо, що $\beta_0 x^u = f/(1 + g) \in I$, і тому α ділить β_0 , який, в свою чергу, ділить кожний коефіцієнт многочлена f . Отримана суперечність показує, що $I \subseteq \alpha F$. Якщо $\alpha > 1$, то $I \subseteq pF$ для деякого простого p . Тоді F/pF – гомоморфний образ фактор-кільця F/I . Але F/pF ізоморфне вільній радикальній алгебрі з одним твірним над полем $GF(p)$, а за лемою 2 [16] $(F/pF)^\circ$ не є періодичною. Отже, $\alpha = 1$, I містить многочлен x^N , і тому F/I – нільпотентне кільце. Лему доведено.

Наслідок 2.3. Якщо R – радикальне кільце з періодичною групою R° , то R – ніль-кільце.

Лема 2.4. Нехай R – кільце з одиницею. Якщо його приєднана група R° – p -група, то радикал Джекобсона $\mathcal{J}(R)$ – ніль-ідеал і $\mathcal{J}(R) \subseteq \mathcal{F}(R)$.

Доведення. Справді, внаслідок леми 2.2 $\mathcal{J}(R)$ – ніль-ідеал, і за лемою 2.4 [17] $\mathcal{J}(R)^+$ – p -група.

Твердження 2.5. Для локального кільця рівносильні такі твердження:

- 1) приєднана група R° періодична;
- 2) $\text{char } R = p^k$ ($k \in \mathbb{N}$), $\mathcal{J}(R)$ – ніль-ідеал, $R/\mathcal{J}(R)$ – абсолютне поле;
- 3) $R^\circ = K \rtimes T$, K – p -група, T – локально циклічна p' -група.

Доведення. Імплікація 3) $\Rightarrow$ 1) очевидна.

1) $\Rightarrow$ 2). Якщо група R° періодична, то $R/\mathcal{J}(R)$ – поле з періодичною мультиплікативною групою, а отже, простої характеристики p . Але тоді за лемою 2.4 [18] періодична частина $\mathcal{F}(R)^+$ – p -група. Внаслідок леми 2.4 $R = \mathcal{F}(R)$ і за теоремою 2.4 [18] $\text{char } R = p^k$ для деякого додатного цілого k . Окрім того, за лемою 2.4 $\mathcal{J}(R)$ – ніль-ідеал, а за лемою 2.1 $R/\mathcal{J}(R)$ – абсолютне поле.

2) $\Rightarrow$ 3). Внаслідок леми 2.4 [17] $K = \mathcal{J}(R)^\circ$ – нормальна p -підгрупа групи R° . Оскільки $R/\mathcal{J}(R)$ – абсолютне поле, то

$$R/\mathcal{J}(R) = \bigcup_{i \in I} F_i -$$

(скінченне або нескінченно-зліченне) об'єднання вкладених одне в друге скінченних полів: $F_i \subseteq F_{i+1}$. Тоді

$$(R/\mathcal{J}(R))^* \cong \bigcup_{i \in I} F_i^*,$$

а отже,

$$R^\circ/\mathcal{J}(R)^\circ \cong \bigcup_{i \in I} D_i,$$

$D_i \cong F_i^*$, $D_i = \langle x_i \rangle$ – циклічна група, породжена елементом x_i ($i \in I$). Нехай a_i – який-небудь прообраз x_i в групі R° . Оскільки порядок елемента a_i дорівнює $m_i p^{s_i}$, де $s_i \in \mathbb{N}$, а числа m_i та p взаємно прості, і

$$u_i m_i + v_i p^{s_i} = 1$$

для деяких цілих чисел u_i, v_i , то $a_i = a_i^{u_i m_i} \cdot a_i^{v_i p^{s_i}}$. Прийmemo $b_i = a_i^{v_i p^{s_i}}$. Тоді $\langle b_i \rangle \cap K = 0$, $\langle b_i \rangle \leq \langle b_{i+1} \rangle$. Покладемо

$$B = \bigcup_{i \in I} \langle b_i \rangle.$$

Очевидно, B – локально-циклічна p' -група та $R^\circ = K \rtimes B$. Твердження доведено.

Наслідок 2.6. *Нехай R – кільце з одиницею і без дільників нуля. Якщо група одиниць $\mathcal{U}(R)$ періодична, то R – напівпросте (за Джекобсоном) кільце, причому $\text{char } R = 0$ або $\text{char } R \in \pi(\mathcal{U}(R))$.*

Теорема 2.7. *Нехай T – тіло. Тоді T^* – p -група, якщо і тільки якщо T – скінченне і ізоморфне одному із полів:*

- 1) $GF(2)$;
- 2) $GF(2^n)$, де $2^n - 1$ – просте число Мерсенна;
- 3) $GF(p)$, де $p = 2^{2^m} + 1$ – просте число Ферма;
- 4) $GF(9)$.

Доведення. Достатність очевидна.

Необхідність. Оскільки T^* – p -група, то характеристика T дорівнює q , $q \neq p$. За теоремою 1 [19, стор.314] T – поле.

Нехай P – просте підполе поля T . Тоді $|P^*| = q - 1 = p^s$ для деякого невід'ємного цілого s . Припустимо спочатку, що $q > 2$. Тоді $p = 2$, q – просте число Ферма. Якщо $T \neq P$, то знайдеться таке скінченне підполе D , що $P \subseteq D \subseteq T$ і $|D| = q^t$ для деякого цілого $t > 1$. Як наслідок, $|D^*| = q^t - 1 = 2^u$ для деякого цілого $u > s$. Якщо $t = 2m + 1$ для деякого цілого m , то 2 ділить $q^{2m} + \dots + q + 1$, а це неможливо. Отже, $t = 2m$. Тоді $q^t - 1 = (q^m + 1)(q^m - 1)$. Як і вище, доводиться, що m – парне число. Міркуючи аналогічно, отримуємо, що $t = 2^n$ для деякого цілого n . Тоді із рівності $q^{2^n} - 1 = 2^u$ випливає, що

$q - 1 = 2^v$, $q + 1 = 2^w$ для деяких цілих v , w , а отже, $q = 3$. Тепер легко довести, що $n = 1$, тобто $D = GF(9)$.

Тепер припустимо, що $q = 2$ і $T \neq P$. Тоді, як і вище, знайдеться таке скінченне підполе D , що $P \subseteq D \subseteq T$ і $|D| = 2^z$ ($z > 1$). Звідси $2^z - 1 = p^l$ для деякого додатного цілого l . Якщо $l = 1$, то $2^z - 1$ – просте число Мерсенна. Тому нехай $l \geq 2$. Якщо $l = 2k$ – парне число, то $2^z - 1 = p^{2k} - 1 = (p^k - 1)(p^k + 1)$, а отже, 2 ділить $2^{z-1} - 1$, а це неможливо. Якщо ж $l = 2k + 1$ – непарне число, то $2^z = p^{2k+1} + 1 = (p + 1)(p^{2k} - p^{2k-1} + \dots - p + 1)$, а це також неможливо. Теорему доведено.

Теорема 2.8. *Нехай R – напівдосконале кільце.*

- 1) Тоді R° – 2-група, якщо і тільки якщо R належить до одного з типів:
 - а) $R = T_1 \oplus \dots \oplus T_m$ ($m \in \mathbb{N}$) – пряма сума полів, кожне з яких ізоморфне $GF(2)$, або $GF(p)$, де p – просте число Ферма, або $GF(9)$;
 - б) $R/\mathcal{J}(R) \cong GF(2) \oplus \dots \oplus GF(2)$, $\text{char } R = 2^k$ ($k \in \mathbb{N}$), $\mathcal{J}(R)$ – ніль-ідеал.
- 2) Тоді R° – p -група ($p > 2$), якщо і тільки якщо $R = T_1 \oplus \dots \oplus T_m$ ($m \in \mathbb{N}$) – пряма сума полів, кожне з яких ізоморфне $GF(2)$ або $GF(2^n)$, де $(2^n - 1)$ – просте число Мерсенна.

Доведення. Достатність очевидна.

Необхідність. Припустимо, що $R = M_n(T)$ – кільце квадратних матриць порядку n над тілом T . Оскільки R° – p -група, то T^* також p -група, і за теоремою 2.7 T ізоморфне одному із полів: $GF(2)$, $GF(2^n)$, $GF(p)$, $GF(9)$, де $2^n - 1$ – просте число Мерсенна, p – просте число Ферма. Легко показати, що $R = T$.

Якщо тепер R – напівдосконале кільце, то $(R/\mathcal{J}(R))^\circ$ – p' -група, а тому

$$R/\mathcal{J}(R) \cong GF(2) \oplus \dots \oplus GF(2)$$

або $\mathcal{J}(R) = 0$. Звідси внаслідок теореми 2.7 легко випливає твердження теореми.

Твердження 2.9. *Для напівдосконалого кільця R рівносильні такі твердження:*

- 1) R° – періодична група;
- 2) $R/\mathcal{J}(R) = M_{n_1}(T_1) \oplus \dots \oplus M_{n_s}(T_s)$, T_i – абсолютне поле характеристики p_i ($i = 1, \dots, s$), $\mathcal{J}(R)$ – ніль-ідеал, R^+ – періодична група скінченної експоненти.

Доведення. 2) $\Rightarrow$ 1) очевидно.

1) $\Rightarrow$ 2). Оскільки $R/\mathcal{J}(R) = \sum_{i=1}^s \oplus M_{n_i}(T_i)$ ($s \in \mathbb{N}$) та T_i^* ізоморфно вкладається в $GL_{n_i}(T_i)$, то T_i – абсолютне поле характеристики p_i ($i = 1, \dots, s$). Окрім того, в R знайдеться деяка система ненульових попарно ортогональних ідемпотентів $e_1, \dots, e_s$, для яких $e_1 + \dots + e_s = 1$ (див. [11]). Покладемо

$$R_{ij} = e_i R e_j \quad (1 \leq i, j \leq n).$$

Тоді $R^+ = \sum_{i,j} \oplus R_{ij}$, R_{ii} – локальне кільце з періодичною приєднаною групою R_{ii}° , а тому $\text{char } R_{ii} = p_i^{k_i}$ ($k_i \in \mathbb{N}$) і, як наслідок, R^+ – періодична група скінченної експоненти. Теорему доведено.

3. Нехай H – група, V – $\mathbb{Z}H$ -модуль, $v_1, \dots, v_m$ – елементи із V , W – підмодуль модуля V . Тоді W називається *коротким H -модулем* з базою $\{v_1, \dots, v_m\}$, якщо знайдеться додатне ціле число k таке, що будь-який елемент $w \in W$ можна записати у вигляді

$$w = \sum_{i=1}^s (v_i) \gamma_i,$$

де $\gamma_i = \epsilon_{i1} h_{i1} + \dots + \epsilon_{ik_i} h_{ik_i}$, $\epsilon_{ij} \in \{-1, 1\}$, $h_{ij} \in H$, $k_i \leq k$ для всіх i, j (див. [20]).

Лема 3.1 ([20, лема 1]). *Нехай K – кільце без дільників нуля і H – скінченно породжена підгрупа групи $\mathcal{U}(K)$. Якщо K – короткий H -модуль з базою $\{1\}$, то K має скінченну характеристику.*

Наслідок 3.2. *Якщо мультиплікативна група T^* тіла T скінченно породжена, то T має просту характеристику.*

Доведення. Справдї, оскільки T^* скінченно породжена, то T – короткий T^* -модуль з базою $\{1\}$, і за лемою 3.1 характеристика тіла T – просте число.

Лема 3.3. *Для тіла T наступні умови рівносильні:*

- 1) мультиплікативна група T^* періодична і скінченно породжена;
- 2) T – скінченне поле;
- 3) T^* – циклічна група;
- 4) T^* – черніковська група.

Доведення леми нескладне і ми його опускаємо.

Лема 3.4. *Нехай R – локальне кільце. Якщо його приєднана група R° поліциклічна, то R – скінченне кільце характеристики p^m ($m \in \mathbb{N}$).*

Доведення. Оскільки приєднана група R° поліциклічна, то R – нетерове кільце. З огляду на теорему В [17] радикал Джекобсона $\mathcal{J}(R)$ – ніль-ідеал, а за наслідком [11, стор.115] $\mathcal{J}(R)$ також нільпотентний.

Далі, мультиплікативна група поля $R/\mathcal{J}(R)$ скінченно породжена, а тому $R/\mathcal{J}(R) \cong GF(p^n)$ для деяких простого p і додатного цілого n . Внаслідок леми 2.3 [18] $\mathcal{F}(R)^+$ – p -група.

Нехай r – який-небудь оборотний елемент кільця R . Тоді $pr \in \mathcal{J}(R)$, а отже, $(pr)^s = 0$ для деякого додатного цілого s . Звідси $r^s \in \mathcal{F}(R)$. Оскільки елемент r^s оборотний, то $\mathcal{F}(R) = R$. За лемою 2.4 [17] $\mathcal{J}(R)^\circ$ – p -група, і з огляду на поліциклічність підгрупа $\mathcal{J}(R)^\circ$ скінченна. Отже, R – скінченне кільце. Лему доведено.

Твердження 3.5. *Для локального кільця R наступні твердження рівносильні:*

- 1) R° – поліциклічна група;
- 2) R° задовольняє умову максимальності для абелевих підгруп;
- 3) R° задовольняє умову максимальності для підгруп;
- 4) R° – черніковська група;
- 5) R – скінченне кільце характеристики p^k , $R/\mathcal{J}(R) \cong GF(p^n)$ ($k, n \in \mathbb{N}$);
- 6) $R^\circ = K \rtimes T$, K – скінченна p -група, T – циклічна група порядку $p^n - 1$ ($n \in \mathbb{N}$);

Доведення. Імплікація $1) \Rightarrow 5)$ доведена в лемі 3.4.

$4) \Rightarrow 5)$. Оскільки група $(R/\mathcal{J}(R))^*$ також черніковська, то за лемою 3.3 вона скінченна, а отже, $R/\mathcal{J}(R) \cong GF(p^n)$ для деяких простого p та додатного цілого n . За твердженням 2.5 $\text{char } R = p^k$ для деякого додатного цілого k . Окрім того, кільце R артінове зліва і справа, і внаслідок леми 3 [4] R – скінченне кільце.

$5) \Rightarrow 6)$. Враховуючи лему 2.4 [17] $\mathcal{J}(R)^\circ$ – скінченна p -група, і за теоремою Шура $R^\circ = \mathcal{J}(R)^\circ \rtimes B$, де $B \cong \mathbb{Z}_{p^{n-1}}$.

Доведення інших імплікацій нескладне. Твердження доведено.

Теорема 3.6. *Для напівдосконалого кільця R рівносильні такі твердження:*

- 1) R° – поліциклічна група;
- 2) R – скінченне кільце, $R/\mathcal{J}(R) = D_1 \oplus \dots \oplus D_m$ – пряма сума кілець, кожне з яких ізоморфне одному із наступних кілець:
 - a) $GF(p^n)$ ($n \in \mathbb{N}$);
 - б) $M_2(2)$;
 - в) $M_2(3)$;
- 3) $R^\circ = A \rtimes B$, A – скінченна нільпотентна група, $B = B_1 \times \dots \times B_m$ – прямий добуток скінченних груп, кожна з яких ізоморфна одній із наступних груп:
 - a) $\mathbb{Z}_{p^{n-1}}$ ($n \in \mathbb{N}$);
 - б) $GL_2(2)$;
 - в) $GL_2(3)$;

Доведення. Імплікації $2) \Rightarrow 3)$, $3) \Rightarrow 1)$ очевидні.

$1) \Rightarrow 2)$. Оскільки підгрупа $\mathcal{J}(R)^\circ$ також поліциклічна, то ідеал $\mathcal{J}(R)$ нільпотентний і скінченний. Окрім того, внаслідок [21, част.IV], якщо група одиниць $GL_n(T)$ кільця $M_n(T)$ поліциклічна, то воно ізоморфне або $GF(p^n)$ ($n \in \mathbb{N}$), або $M_2(2)$, або $M_2(3)$. Теорему доведено.

Наслідок 3.7. *Нехай R – напівдосконале кільце. Тоді приєднана група R° черніковська, якщо і тільки якщо R – скінченне кільце.*

Доведення. Достатність очевидна.

Необхідність. Зрозуміло, що

$$R/\mathcal{J}(R) = \sum_{i=1}^k \oplus M_{n_i}(T_i),$$

T_i – скінченне поле характеристики p_i ($i = 1, \dots, k$). Окрім того, R – артінове кільце, і з огляду на лему 3[4] R – скінченне кільце. Наслідок доведено.

Якщо адитивна група R^+ кільця R є p -групою, то R називається p -кілцем.

Оскільки напівдосконале кільце з циклічною приєднаною групою скінченне, то внаслідок теореми 5 [2] отримуємо

Наслідок 3.8. *Будь-яке напівдосконале кільце R з циклічною приєднаною групою R° скінченне і є прямою сумою p -кілець за різними простими p , кожне з яких ізоморфне одному із наступних кілець:*

- 1) $GF(p^n)$ ($n \in \mathbb{N}$);
- 2) $\mathbb{Z}_q$, $q = p^n$ ($n \in \mathbb{N}$);

- 3) $\mathbb{Z}_4$;
- 4) $\mathbb{Z}_p[x]/(x^2)$;
- 5) $\mathbb{Z}_2[x]/(x^3)$;
- 6) $\mathbb{Z}_4[x]/(2x, x^2 - 2)$;
- 7) $\left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \mid x, y, z \in GF(2) \right\}$.

Зауваження 3.9. Нехай $F = GF(p^n)$, σ – автоморфізм Фробеніуса поля F , $F[x, \sigma]$ – кільце косих многочленів таке, що $xa = \sigma(a)x$ для будь-якого $a \in F$. Тоді $R = F[x, \sigma]/(x^2)$ – локальне кільце з поліциклічною приєднаною групою, яка не є надрозв'язною.

Лема 3.10. Нехай R – локальне кільце з надрозв'язною групою одиниць $\mathcal{U}(R)$. Тоді $R/\mathcal{J}(R) \cong GF(p^n)$ ($n \in \mathbb{N}$).

- а) Якщо A – нормальна підгрупа групи $\mathcal{U}(R)$ порядку p , то $A \leq Z(\mathcal{U}(R))$.
- б) Якщо $p = 2$, то $\mathcal{U}(R)$ – нільпотентна група і $\mathcal{J}(R)$ – нільпотентний ідеал.
- в) Якщо $p \neq 2$, $n = 1$, то $\mathcal{U}(R)$ – нільпотентна група і $\mathcal{J}(R)$ – нільпотентний ідеал.

Доведення. За твердженням 3.5 $R/\mathcal{J}(R) \cong GF(p^n)$, $\text{char } R = p^k$, де $n, k \in \mathbb{N}$.

Нехай $1 + a$ – елемент порядку p із $1 + \mathcal{J}(R)$, який породжує нормальну підгрупу A в $\mathcal{U}(R)$. Тоді

$$\left| \mathcal{U}(R) / C_{\mathcal{U}(R)}(1 + a) \right| \leq p - 1. \quad (*)$$

Якщо $p = 2$, то із співвідношення (*) внаслідок теореми 10.5.2 [12] випливає, що $\mathcal{U}(R)$ – нільпотентна група. Тоді за наслідком 2 [16] радикал Джекобсона $\mathcal{J}(R)$ нільпотентний.

Нехай надалі $p \neq 2$. Тоді із (*) випливає, що $1 + \mathcal{J}(R) \leq C_{\mathcal{U}(R)}(1 + a)$, а отже, $\mathcal{J}(R) \subseteq C_R(a)$. Оскільки $1 + \mathcal{J}(R) \leq \mathcal{U}(C_R(a))$, то $\mathcal{U}(C_R(a))$ – нормальна підгрупа групи одиниць $\mathcal{U}(R)$. Далі, оскільки $C_{\mathcal{U}(R)}(1 + a) \leq \mathcal{U}(C_R(a))$, то $|\mathcal{U}(R)/\mathcal{U}(C_R(a))| = d$, де d – деякий дільник числа $p - 1$. Тоді внаслідок ізоморфізму

$$\left(\mathcal{U}(R) / 1 + \mathcal{J}(R) \right) / \left(\mathcal{U}(C_R(a)) / 1 + \mathcal{J}(R) \right) \cong \mathcal{U}(R) / \mathcal{U}(C_R(a))$$

отримуємо, що

$$\left| \mathcal{U}(C_R(a) / \mathcal{J}(R)) \right| = \left| \mathcal{U}(C_R(a)) / 1 + \mathcal{J}(R) \right| = \frac{p^n - 1}{d}.$$

Оскільки $C_R(a)/\mathcal{J}(R)$ – підполе поля $R/\mathcal{J}(R)$, то $C_R(a)/\mathcal{J}(R) \cong GF(p^m)$, де m ділить n . Отже, $(p^n - 1)/d = p^m - 1$ і, як наслідок, $d = 1$ та $A \leq Z(\mathcal{U}(R))$.

Нарештї, припустимо, що $n = 1$. Нехай V – підкільце кільця R , породжене його одиницею. Тоді $V \subseteq Z(R)$ і $R = \mathcal{J}(R) + V$. Візьмемо який-небудь елемент $a \in \mathcal{U}(R)$. Тоді $a = j + z$ для деяких $j \in \mathcal{J}(R)$, $z \in Z(R)$. Оскільки $a \in \mathcal{J}(R)$, то $z \in \mathcal{J}(R)$, а отже, z – оборотний елемент, і тому $a = (1 + z^{-1}j)z \in (1 + \mathcal{J}(R))\mathcal{U}(Z(R))$. Таким чином, $\mathcal{U}(R) = (1 + \mathcal{J}(R))\mathcal{U}(Z(R))$ – нільпотентна група. Лему доведено.

4. Нагадаємо, що неединична група, яка володіє лише тривіальними нормальними підгрупами, називається *простою*.

Лема 4.1. Для локального кільця R приєднана група R° проста, якщо і тільки якщо R ізоморфне одному із кілець:

- а) $GF(3)$;
- б) $GF(2^s)$, де $(2^s - 1)$ – просте число Мерсенна;
- в) $\mathbb{Z}_4$.

Доведення. Достатність очевидна.

Необхідність. Оскільки $\mathcal{J}(R)^\circ$ – нормальна підгрупа R° , то $\mathcal{J}(R) = 0$ (а отже, R – поле) або $\mathcal{J}(R)^\circ = R^\circ$ (а отже, $R/\mathcal{J}(R) \cong GF(2)$).

Нехай R – поле. Тоді R^* – циклічна група простого порядку q і $|R| = q + 1 = p^s$ для деяких простого p і додатного цілого s . Якщо $q = 2$, то $s = 1$ і $R \cong GF(3)$. Якщо ж $q > 2$, то $q + 1$ – парне число, а тому $p = 2$, $q = 2^s - 1$ – просте число Мерсенна і $R \cong GF(2^s)$.

Тепер припустимо, що $\mathcal{J}(R) \neq 0$. Легко довести, що $R = \mathcal{F}(R)$, і за лемою 2.4 [18] $\text{char } R = 2^k$ ($k \in \mathbb{N}$). Оскільки $\mathcal{J}(R)$ – мінімальний ідеал кільця R , то зважаючи на твердження 1 [11, стор.103] $\mathcal{J}(R)^2 = 0$. Окрім того, $\mathcal{J}(R)^\circ$ – абелева група експоненти 2 і $|R| \leq 4$. Звідси $R \cong \mathbb{Z}_4$. Лему доведено.

Теорема 4.2. Для напівдосконалого кільця R рівносильні такі твердження:

- 1) R° – проста група;
- 2) група R° ізоморфна $\mathbb{Z}_2$ або $\mathbb{Z}_p$, де $p = 2^s - 1$ – просте число Мерсенна;
- 3) R ізоморфне одному із наступних кілець:
 - а) $GF(3)$;
 - б) $GF(2^s)$, де $2^s - 1$ – просте число Мерсенна;
 - в) $GF(3) \oplus GF(2) \oplus \dots \oplus GF(2)$;
 - г) $GF(2^s) \oplus GF(2) \oplus \dots \oplus GF(2)$, де $2^s - 1$ – просте число Мерсенна;
 - д) $\mathbb{Z}_4$;
 - е) $\mathbb{Z}_4 \oplus GF(2) \oplus \dots \oplus GF(2)$.

Доведення. 1) $\Rightarrow$ 3). Оскільки R° – проста група, то $\mathcal{J}(R) = 0$ або $\mathcal{J}(R)^\circ = R^\circ$.

Нехай $K = M_n(T)$. Якщо K° – проста група, то легко перевірити, що $n = 1$ і K – поле. Припустимо, що $\mathcal{J}(R) = 0$. Тоді R – класично-напівпросте кільце, а тому $R = T_1 \oplus \dots \oplus T_k$ – скінченна пряма сума полів і, як наслідок, R – кільце одного із типів а)–г).

Якщо ж $\mathcal{J}(R)^\circ = R^\circ$, то $\mathcal{J}(R)$ – мінімальний ідеал кільця R і внаслідок твердження 1 [11, стор.103] $\mathcal{J}(R)^2 = 0$. Оскільки $(R/\mathcal{J}(R))^\circ = 0$, то

$$R/\mathcal{J}(R) \cong GF(2) \oplus \dots \oplus GF(2).$$

З огляду на це, легко отримати, що R^+ – 2-група. Окрім того, $\mathcal{J}(R)^\circ \cong \mathcal{J}(R)^+$ – абелева група порядку 2, а тому R – кільце типу д) або г).

Імплікації 3) $\Rightarrow$ 2), 2) $\Rightarrow$ 1) майже очевидні. Теорему доведено.

ЛІТЕРАТУРА

1. Eldridge K.E., Fisher I. *D.C.C. rings with a cyclic group of units* // Duke Math. J. 1967. V.34, P.243–248.
2. Fisher I., Eldridge K.E. *Artinian rings with cyclic quasi-regular groups* // Duke Math. J. 1969. V.36, № 1. P.43–47.
3. Bateman J.M., Goleman D.B. *Group algebras with nilpotent unit groups* // Proc. Amer. Math. Soc. 1968. V.19, P.448–449.

4. Eldridge K.E. *On ring structures determined by groups* // Proc. Amer. Math. Soc. 1969. V.23, №3. P.472–477.
5. Bateman J.M. *On the solvability of unit groups of group algebras* // Trans. Amer. Math. Soc. 1971. V.157, P.73–86.
6. Хрипта И.И. *О нильпотентности мультипликативной группы группового кольца* // Матем. заметки. 1972. Т.11, №2. С.191–200.
7. Fisher J.L., Parmenter M.M., Sehgal S.K. *Group rings with solvable, n -Engel unit groups* // Proc. Amer. Math. Soc. 1976. V.59, №2. P.195–200.
8. Бовди А.А., Хрипта И.И. *Групповые алгебры периодических групп с разрешимой мультипликативной группой* // Матем. заметки. 1977. Т.22, №3. С.421–432.
9. Groza G. *Artinian rings having a nilpotent group of units* // J. Algebra. 1989. V.121, №2. P.253–262.
10. Artemovych O., Ishchuk Yu. *On the local rings having a periodic group of units* // Всеукраїнська наукова конференція "Розробка та застосування математичних методів в науково-технічних дослідженнях", присвячена 70-річчю від дня народження професора П.С. Казімірського. Львів, 1995. С.51.
11. Ламбек И. Кольца и модули. – М.: Мир, 1971. 277с.
12. Холл М. Теория групп. – М.: Изд. иностр. лит., 1962. 468с.
13. Черников С.Н. Группы с заданными свойствами системы подгрупп. – М.: Наука, 1980. 384с.
14. Faudree R.J. *Locally finite and solvable subgroups of fields* // Proc. Amer. Math. Soc. 1969. V.22, P.407–417.
15. Tilman S.J. *The multiplicative group of absolutely algebraic fields in characteristic p* // Proc. Amer. Math. Soc. 1969. V.23, P.601–604.
16. Watters J.F. *On the adjoint group of a radical ring* // J. London Math. Soc. 1968. V.43, P.725–729.
17. Amberg B., Dickenshied O. *On the adjoint group of a radical ring* // Canad. Math. Bull. 1995. V.38, №3. P.262–270.
18. Feigelstock S. *The additive groups of local ring* // Ark. Math. 1980. V.18, №1. P.49–51.
19. Джекобсон Н. Строение колец. – М.: Изд. иностр. лит., 1961. 392с.
20. Rhemtulla A., Sidki S. *Factorizable infinite solvable groups* // J. Algebra. 1989. V.122, №2. P.397–409.
21. Артин Е. Геометрическая алгебра. – М.: Наука, 1969. 284с.

Механіко-математичний факультет, Львівський університет,
вул. Університетська 1, 290602 Україна

Надійшло 10.01.96.