УДК 512.552

**Кайдан Н.В., Щенсневич Ю.Ю.**

[1] *кандидат фізико-математичних наук, старший викладач кафедри алгебри, ДВНЗ «ДДПУ»*

[2] *студент 3 курсу фізико-математичного факультету, ДВНЗ «ДДПУ»*

e-mail: kaydannv@mail.ru

# СКІНЧЕННІ ЛАНЦЮГОВІ КІЛЬЦЯ

Розглядається поняття узагальненого кільця Галуа. Доведена теорема, яка показує аналогію між кільцями Галуа і полями Галуа.

**Ключові слова:** *скінченні кільця, кільця Галуа, ланцюгові кільця.*

## Вступ

Теорія кілець Галуа була розвинена в роботах [1], [5] і [9]. Пізніше, в [10] вивчалось застосування цих кілець в теорії кодування і криптографії [8] (псевдовипадкові послідовності, засновані на лінійних рекурентних послідовностях над кільцями Галуа). Розвиток теорії неасоціативних кілець Галуа є достатньо цікавим, головним чином з точки зору можливості нових застосувань в цих областях.

Кільце $A$ називається ланцюговим справа (зліва), якщо правий (лівий) регулярний модуль $A_A$ $({}_AA)$ є ланцюговим. Кільце називається ланцюговим, якщо воно ланцюгове справа і зліва.

Кільце $A$ називається напівланцюговим справа (зліва), якщо правий (лівий) регулярний модуль $A_A$ $({}_AA)$ є напівланцюговим. Кільце називається напівланцюговим, якщо воно напівланцюгове справа і зліва.

Модуль $M$ називається дистрибутивним, якщо всі його підмодулі $K, L, N$ $K \cap (L + N) = K \cap L + K \cap N$.

Отже, підмодуль та фактормодуль дистрибутивного модуля є дистрибутивними. Модуль називається напівдистрибутивним якщо він є прямою сумою дистрибутивних модулів.

Кільце $A$ називається напівдистрибутивним справа (зліва), якщо правий (лівий) регулярний модуль $A_A$ $({}_AA)$ є напівдистрибутивним. Напівдистрибутивне справа (зліва) кільце називається напівдистрибутивним.

Таким чином, кожний ланцюговий модуль є дистрибутивним модулем і кожний напівланцюговий модуль є напівдистрибутивним. [7]

**Теорема 1.** *Нехай $A$ – артінове слабопервинне напівдистрибутивне кільце, $R$ – його радикал Джекобсона.*

*Наступні умови рівносильні для кільця $A$*

(1) *кільце $A$ скінченне;*

(2) *факторкільце $A/R$ скінченне;*

(3) *існує локальний ідемпотент $e \in A$ кільця $A$ такий, що кільце $eAe$ скінченне.*

Отже, найбільш вивченими і найбільш важливими в теорії і застосуванні скінченних ланцюгових кілець є кільця Галуа.

## Про одну конструкцію в теорії кілець.

Основні відомості з теорії кілець містяться в [2]. Нехай $A$ — асоціативне кільце з $1 \neq 0$, $\sigma : A \to A$ автоморфізм кільця $A$. Розглянемо множину пар $(a, b)$, де $(a, b) \in A$ і задамо на цій множині додавання і множення за такими правилами:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1 a_2^{\sigma})$$

Це кільце будемо позначати через $H(A)$. Нехай $A$ – асоціативне кільце з $1 \neq 0$, тоді елемент $(0, 0)$ є нулем цього кільця, а одиницею цього кільця є елемент $(1, 0)$. Покажемо, що якщо $A$ — комутативне кільце і $\sigma$ тотожній автоморфізм, то кільце $H(A)$ — комутативне, тобто

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, a_1 b_2 + b_1 a_2)$$

$$(a_2, b_2)(a_1, b_1) = (a_2 a_1, a_2 b_2 + b_2 a_1)$$

Якщо $A$ – комутативне кільце, а $\sigma$ автоморфізм кільця $A$, який не є тотожнім, то кільце $H(A)$ некомутативне.

Нехай кільце $A$ буде полем. Розглянемо випадок, коли $A = K$, де $K$ є довільним полем і $\sigma : K \to K$ – автоморфізм цього поля. Нехай $(\alpha, \beta) \in H(K)$ довільний елемент кільця $H(K)$, $\quad \alpha, \beta \in K$.

Знайдемо всі оборотні елементи. Нехай елемент $(\alpha_1, \beta_1)$ має правий обернений, тобто

$(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (\alpha_1 \alpha_2, \alpha_1 \beta_2 + \beta_1 \alpha_2^{\sigma}) = (1, 0)$;

$\alpha_1 \alpha_2 = 1; \quad \alpha_1 \beta_2 + \beta_1 \alpha_2^{\sigma} = 0;$

$\alpha_2 = \alpha_1^{-1}, \quad \alpha_1 \beta_2 + \beta_1 (\alpha_1^{-1})^{\sigma} = 0$

$\beta_2 = -\frac{\beta_1 (\alpha_1^{-1})^{\sigma}}{\alpha_1}$.

Оборотній елемент до елементу $(\alpha_1, \beta_1)$ буде $(\alpha_1^{-1}, -\frac{\beta_1 (\alpha_1^{-1})^{\sigma}}{\alpha_1})$, тобто він існує тоді і тільки тоді, коли $\alpha_1 \neq 0$.

$$(\alpha_1,\beta_1)(\alpha_1^{-1},-\frac{\beta_1(\alpha_1^{-1})^\sigma}{\alpha_1})=(1,-\frac{\alpha_1\beta_1(\alpha_1^{-1})^\sigma}{\alpha_1}+\beta_1(\alpha_1^{-1})^\sigma)=(1,0)$$

$$(\alpha_1^{-1},-\frac{\beta_1(\alpha_1^{-1})^\sigma}{\alpha_1})(\alpha_1,\beta_1)=(1,\alpha_1^{-1}\beta_1-\frac{\beta_1(\alpha_1^{-1})^\sigma}{\alpha_1}\alpha_1^\sigma)=(1,0)$$

Таким чином, елементи які є оборотніми мають першу ненульову координату і тільки вони. Значить, всі необоротні елементи мають першу координату нульову.

$R$ – двосторонній ідеал, який складається зі всіх необоротних елементів кільця $A$:

$$R=\{(0,0),(0,1),(0,x),(0,x+1)\}$$
$$(\alpha,\beta)R\subseteq R;\qquad R(\alpha,\beta)\subseteq R.$$

Елементи $(0,\beta)\in H(K)$ утворюють двосторонній ідеал $R$. Дійсно, $(\alpha_1,\beta_1)(0,\beta)=(0,\alpha_1\beta)$ і $(0,\beta)(\alpha_1,\beta_1)=(0,\beta\alpha_1^\sigma)$ утворюють двосторонній ідеал. Таким чином $R$ є радикалом кільця $H(K)$ і $R^2=0$, тобто для будь-яких $(0,\beta_1),(0,\beta_2)\in R$ маємо, що $(0,\beta_2),(0,\beta_2)=(0,0)$

Таким чином ми отримали, що $H(K)\supset R\supset 0$ є ланцюговим кільцем. [6]

## Кільця Галуа.

Кільцем Галуа називається скінченне комутативне кільце $R$ з одиницею $e$, в якому множина всіх дільників нуля має вид $p\cdot R$ для деякого простого числа $p$. [10]

**Позначення**: $R=GR(q^n,p^n)$ (іноді $R=GR(r,p^n)$ ) [9].

**Найпростіші приклади**: $GF(q)=GR(q,p),\quad \mathbb{Z}_{p^n}=GR(p^n,p^n)$.

**Теорема 2.** [*10*] *Нехай $R$ – кільце Галуа з множиною дільників нуля $\mathfrak{N}=pR$. Тоді виконуються наступні твердження:*
*$R^*$ - мультипликативна група (група оборотних елементів) кільця $R$, $R^*=R\setminus\mathfrak{N}$.*
*$\mathfrak{N}$ – єдиний максимальний ідеал кільця $R$, $R/\mathfrak{N}=GF(q)$,*
*$q=p^r,\quad r\in\mathbb{N}$.*
*Характеристика кільця $R$ має наступний вигляд: $charR=p^n,\quad n\in\mathbb{N}$.*
*Гратка всіх ідеалів кільця $R$ утворює ланцюг:*

$$R=\mathfrak{N}^0\supset\mathfrak{N}^1=pR\supset\ldots\supset\mathfrak{N}^{n-1}=p^{n-1}R\supset\mathfrak{N}^n=p^nR=0$$

*Для $t\in\overline{0,n}$ виконуються рівності: $|\mathfrak{N}^t|=q^{n-t}$, зокрема*

$$|R|=q^n,\quad |R^*|=q^{n-1}(q-1).$$

Для кільця Галуа $R$ характеристики $p^n$ поле $\overline{R} = R/pR$ називається полем лишків. Вочевидь, що природний епіморфізм кілець $R \to \overline{R}$ індукує епіморфізм кілець поліномів $R[x] \to \overline{R}[x] \cong R[x]/pR[x]$. Відображення полінома $A(x) = \sum a_i x^i \in R[x]$ при цьому епіморфізмі будемо позначати через $\overline{A}(x)$ : $\overline{A}(x) = \sum \overline{a}_i x^i \in \overline{R}[x]$. Унітарний поліном $F(x) \in R[x]$ називається поліномом Галуа над $R$, якщо $\overline{F}(x)$ – незведений поліном над полем $\overline{R}$. Вочевидь, що в $R[x]$ існує поліном Галуа будь-якого степеня.

**Теорема 3.** [*10*] *Нехай $R$ – кільце Галуа характеристики $p^n$, яке складається з $q^n$ елементів, $F(x)$ – поліном Галуа над $R$ степеня $m$. Тоді кільце $S = R[x]/F(x)$, є кільцем Галуа с параметрами $charS = p^n, \quad |S| = q^{mn}$.*

В позначеннях теореми 3 можна вважати, що вихідне кільце Галуа $R$ з $q^n$ елементів є підкільце побудованого кільця Галуа $S$ з $q^{mn}$ елементів. Тоді будемо казати, що $S$ — розширення Галуа степеня $m$ кільця $R$.

**Наслідок 1.** *Для будь-якого кільця Галуа $R$ і будь-якого натурального $m$ існує розширення Галуа $S$ кільця $R$ степеня $m$.*

**Наслідок 2.** *Для будь-якого простого $p$ і $m, n \in \mathbb{N}$ існує кільце Галуа $S$ з $p^{mn}$ елементів характеристики $p^n$.*

**Лема 1.** *Нехай поліном $A(x) \in R[x]$ і елемент $\alpha \in S$ такі, що $\overline{A}(\overline{\alpha}) = \overline{0}$ і $\overline{A}'(\overline{\alpha}) \neq \overline{0}$. Тоді в кільце $S$ існує єдиний корінь $\beta$ полінома $A(x)$, такий, що $\overline{\beta} = \overline{\alpha}$.*

**Лема 2.** *Для будь-якого елемента $\alpha \in S$, якщо $\overline{S} = \overline{R}[\overline{\alpha}]$, то $S = R[\alpha]$ і*

$$S = \{A(\alpha) : A(x) \in R[x], \quad degA(x) < m\}. \tag{1}$$

Доведення лем представлено в [10].

Наступна теорема показує, що існує глибока аналогія між кільцями Галуа і полями Галуа.

**Теорема 4.** [*10*] *Нехай $S$ – розширення Галуа степеня $m$ кільця Галуа $R$ і $F(x)$ – поліном Галуа над $R$ степеня $k$. Тоді виконуються наступні твердження:*
*(а) Поліном $F(x)$ має корінь в $S$ в тому і лише в тому випадку, якщо $k|m$.*
*(б) Якщо $k|m$, то $F(x)$ має в $S$ рівно $k$ різних коренів $\alpha_1, ..., \alpha_k$, ці корні попарно не порівняні по модулю ідеалу $pS$ і $F(x) = (x - \alpha_1) \cdot ... \cdot (x - \alpha_k)$.*
*(в) Для будь-якого елементу $\alpha \in S$ рівність $S = R[\alpha]$ виконується тоді і тільки тоді, коли $\alpha$ – корінь поліному Галуа над $R$ степеня $m$.*

**Доведення.** (а) Поле $\overline{S} = S/pS$ розглянемо як розширення степеня $m$ поля $\overline{R} = R/pR$. Якщо $\alpha \in S$ і $F(\alpha) = 0$, то $\overline{F}(\overline{\alpha}) = \overline{0}$. Отже, $\overline{\alpha}$ – корінь в $\overline{S}$ незвідного полінома $\overline{F}(x) \in \overline{R}[x]$, і тому $k|m$. Зворотне твердження слідує з (б).

(б) Так як $\overline{F}(x)$ – незвідний поліном над полем $\overline{R}$ і $[\overline{S} : \overline{R}] = m$, то за умови $k|m$ поліном $\overline{F}(x)$ має в полі $\overline{S}$ рівно $k$ різних коренів: $a_1, ..., a_k$. Так як $\overline{F}'(a_s) \neq \overline{0}$ для $s \in \overline{1,k}$, то за лемою 1 в кільці $S$ існують корні $\alpha_1, ..., \alpha_k$, полінома $F(x)$, такі, що $\overline{\alpha}_s = a_s, \quad s \in \overline{1,k}$. Отже, ці корені попарно різні за модулем $pS$. Тому $F(x) = (x - \alpha_1) \cdot ... \cdot (x - \alpha_k)$ і в кільці $S$ поліном $F(x)$ не має інших коренів.

(в) Нехай $\alpha \in S$ і $\alpha$ – корінь поліному Галуа $G(x) \in R[x]$ степеня $m$. Тоді $\overline{\alpha}$ – корінь в $\overline{S}$ незвідного поліному $\overline{G}(x) \in \overline{R}[x]$ степеня $m = [\overline{S} : \overline{R}]$, і тому $\overline{S} = \overline{R}[\overline{\alpha}]$. Рівність $S = R[\alpha]$ випливає з леми 2 і виконується рівність 1. Це означає, що елемент $\alpha^m$ виглядає наступним чином: $\alpha^m = A(\alpha)$, де $A(x) \in R[x], \quad degA(x) < m$. Тоді $\alpha$ – корінь унітарного полінома $G(x) = x^m - A(x)$ степеня $m$. $G(x)$ – поліном Галуа, так як $\overline{G}(x)$ незвідний над $\overline{R}$, оскільки $\overline{\alpha}$ – його корінь в $\overline{S}$ і $[\overline{S} : \overline{R}] = m$. □

**Наслідок 3.** *Якщо $S$ – кільце Галуа характеристики $p^n$, яке складається з $p^{mn}$ елементів, тоді $S \cong \mathbb{Z}_{p^n}[x]/F(x)$, де $F(x)$ – довільний поліном Галуа степеня $m$ над $\mathbb{Z}_{p^n}$.*

**Наслідок 4.** *Два кільця Галуа ізоморфні тоді і тільки тоді, коли їх потужності і характеристики рівні.*

Наслідки 3 і 4 виводяться з теореми 4 таким самим чином, яким доводяться аналогічні теореми для полів Галуа, якщо відмітити, що в кільці Галуа $S$, з наслідку 3, підкільце $S_0$, яке породжене одиницею, є кільце Галуа, ізоморфне $\mathbb{Z}_{p^n}$, та $S$ – розширення Галуа кільця $S_0$ степеня $m$.

Наслідок 4 робить коректним позначення $S = GR(q^n, p^n)$ для кільця Галуа $S$ з $q^n$ елементів, яке має характеристику $p^n$. Зокрема, $GF(p^r) = GR(p^r, p), \quad \mathbb{Z}_{p^n} = GR(p^n, p^n)$.

## Висновки

Скінченні кільця є дуже важливою і цікавою алгебраїчною структурою. Найбільш вивченими і найбільш важливими в теорії і застосуванні скінченних ланцюгових кілець є кільця Галуа. Кільце Галуа, як і поле Галуа, визначається однозначно, з точність до ізоморфізму, кількістю елементів та характеристикою. Для доведення цього факту та опису будови кілець Галуа використовується метод редукції до полів Галуа. Нами було наведено доведення теореми, яка показує аналогію між кільцями Галуа і полями Галуа.

## Література


1. *Janusz G.J.* Separable algebras over commutative rings /G.J. Janusz// Trans. Amer. Math. Soc. (1996) 122, — 1996. — P. 461–478.
2. *Hazewinkel M.* Algebras, rings and modules / M. Hazewinkel, N. Gubareni and V. Kirichenko//Vol. 1. Mathematics and its Applications, 575. Kluwer Academic Publishers, Dordrecht, — 2004. — xii+380 pp.
3. *Krull W.* Algebraische Theorie der Ringe II / W. Krull //Math. Ann. (1924) 91,— 1924. — P. 1–46.
4. *McDonald B. R.* Finite rings with identity / B.R. McDonald // Wiley, New York, — 1974. — 429 p.
5. *Raghavendran R.* Finite associative rings / R. Raghavendran // Compos. Math. — Vol. 21, №2. — 1969. — P. 195–219.
6. *Кайдан Н.В.* Про одну конструкцію в теорії кілець /Н.В.Кайдан, О.В.Ніколаєва // Тринадцята міжнародна наукова конференція імені академіка М. Кравчука, Київ: Матеріали конф. Т. 1. — К.: НТУУ «КПІ» — 2010. — С. 184.
7. *Кайдан Н.В.* Про слабопервинні скінченні кільця /Н.В. Кайдан// Вісник Київського університету, випуск №3, 2008. Серія: фізико-математичні науки. — К.: — 2008. — — С. 266.
8. *Нечаев А.А.* Линейные рекуррентные последовательности над кольцом Галуа /А.А. Нечаев, А.С. Кузьмин// Алгебра и логика — Т.34, №2, — 1995. — С. 1–17.
9. *Нечаев А.А.* Конечные кольца главных идеалов /А.А. Нечаев// Матем. сб. (1973) 91, №3. — 1973. — С. 350–366.
10. *Нечаев А.А.* Код Кердока в циклической форме /А.А. Нечаев// Дискретная математика (1989) 1, №4. — 1989. — С. 123–139.