Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

УДК 510.2:37.016:51

https://doi.org/10.52058/2786-4952-2026-4(62)-917-932

Матурін Юрій Петрович кандидат фізико-математичних наук, доцент, Дрогобицький державний педагогічний університет імені Івана Франка, м. Дрогобич, https://orcid.org/0000-0002-0544-1329

Хаць Руслан Васильович кандидат фізико-математичних наук, доцент, Дрогобицький державний педагогічний університет імені Івана Франка, м. Дрогобич, https://orcid.org/0000-0001-9905-5447

Комарницька Леся Іванівна кандидат фізико-математичних наук, доцент, Дрогобицький державний педагогічний університет імені Івана Франка, м. Дрогобич, https://orcid.org/0009-0001-0907-1038

МЕТОДИКА ВИВЧЕННЯ ЗАСТОСУВАНЬ ПОЛІВ ГАЛУА В КОМП'ЮТЕРНИХ НАУКАХ

Анотація. У статті розроблено, теоретично обґрунтовано та концептуалізовано цілісну інноваційну методичну модель вивчення застосувань скінченних полів Галуа в комп'ютерних науках для здобувачів другого (магістерського) рівня вищої освіти, які навчаються за освітньо-професійною програмою «Середня освіта (Математика, інформатика)». Актуальність дослідження зумовлена наявністю глибокої системної кризи у викладанні абстрактної алгебри, яка в освітній практиці майбутніх педагогів традиційно репрезентується переважно через суворо дедуктивний, аксіоматично замкнений і недостатньо пов'язаний із реальними прикладними задачами підхід. Наслідком цього є виникнення у магістрантів істотних когнітивних бар'єрів, що виявляються у фрагментарному сприйнятті математичного знання та у відсутності цілісного бачення взаємозв'язку між теорією груп, кілець і полів, з одного боку, та сучасними інформаційними технологіями, з іншого. Метою статті є подолання окресленого дидактичного розриву шляхом системної інтеграції математичної абстракції з понятєвим і алгоритмічним апаратом комп'ютерних наук крізь призму сучасної криптографії та теорії кодування.

Теоретико-методологічною основою запропонованої дидактичної парадигми визначено принцип «подвійного подання» (dual representation), згідно з яким кожне абстрактне математичне поняття (зокрема, група, кільце, поле, ізоморфізм) має вводитися паралельно зі своїм структурним, алгоритмічним або програмним відповідником у комп'ютерних науках (наприклад, абстрактний тип даних, інтерфейс, побітова операція, механізм обробки винятків). За такого підходу математичні аксіоми, зокрема асоціативність, дистрибутивність і

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

комутативність, інтерпретуються не лише як формальні логічні умови, а і як строгі програмні специфікації, що забезпечують коректність обчислень, підвищення їхньої ефективності та безпечне використання ресурсів пам'яті, зокрема запобігання критичним помилкам на кшталт переповнення буфера. Методологічним підґрунтям реалізації цього принципу виступає стратегія висхідного проєктування (bottom-up design), яка передбачає розгортання навчального процесу не від готових абстрактних конструкцій до їхніх застосувань, а навпаки − від постановки конкретної інженерної проблеми у сфері кібербезпеки, наприклад проблеми захисту даних від несанкціонованого доступу, до природної необхідності побудови відповідного математичного апарату, яким у цьому випадку постають скінченні поля.

У роботі докладно представлено дидактичний кейс побудови алгебраїчного розширення у вигляді фактор-кільця поліномів над базовим простим полем Галуа GF(2). Продемонстровано методику пояснення архітектури байта як полінома степеня не вище сьомого. Запропоновано послідовний дидактичний перехід від абстрактної характеристики поля до алгоритмічно значущої операції додавання без перенесення розряду (carry-less addition), яка в обчислювальному аспекті є тотожною логічній побітовій операції XOR. Окрему увагу приділено процедурі множення поліномів та необхідності їхньої модульної редукції за незвідним поліномом Рейндаля $m(x) = x^8 + x^4 + x^3 + x + 1$, що забезпечує збереження фіксованої розмірності блока даних. У контексті стандарту шифрування AES ґрунтовно проаналізовано застосування розширеного алгоритму Евкліда для знаходження мультиплікативного оберненого елемента, який становить математичне ядро нелінійних криптографічних перетворень, зокрема побудови S-блоків.

Найбільш інноваційним і методично вагомим складником запропонованої системи є адаптація криптографії на еліптичних кривих (Elliptic Curve Cryptography, ECC) до потреб педагогічної магістерської освіти. У відповідному розділі статті розкрито значний дидактичний потенціал еліптичних кривих як засобу візуалізації, інтерпретації та концептуальної матеріалізації абстрактних алгебраїчних груп.

Методика передбачає поетапний перехід від геометричної побудови операції додавання точок методом січної та дотичної на неперервній дійсній площині, заданій рівнянням Вейєрштрасса, до алгебраїзації цих операцій на дискретній ґратці скінченного поля F_p. Детально описано процес обґрунтування того факту, що множина точок еліптичної кривої утворює абелеву групу, що становить нетривіальний, концептуально насичений і педагогічно потужний приклад для магістрантів. Кульмінаційним елементом цього етапу є розгляд проблеми дискретного логарифмування на еліптичних кривих (ECDLP), опрацювання якої формує у здобувачів глибоке розуміння математичних засад блокчейн-технологій, сучасних асиметричних криптосистем і протоколів обміну ключами.

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

Обґрунтовано, що невід'ємним етапом повноцінного засвоєння навчального матеріалу має бути обов'язкова самостійна програмна реалізація досліджуваних алгебраїчних структур. У зв'язку з цим студентам пропонується здійснювати об'єктно-орієнтоване моделювання полів Галуа та еліптичних кривих засобами мови програмування Python або із використанням системи комп'ютерної алгебри SageMath. Такий підхід трансформує традиційний лекційний курс у формат інтерактивної дослідницької лабораторії, у межах якої математичні поняття постають не лише як предмет теоретичного вивчення, а і як об'єкти алгоритмічного конструювання та експериментальної перевірки. У підсумку зроблено висновок, що впровадження розробленої методики забезпечує принципову трансформацію теоретичних математичних знань магістрантів у практично значущий алгоритмічний інструментарій. Це безпосередньо впливає на формування їхньої фахової компетентності, створюючи передумови для того, щоб майбутні вчителі були здатні ефективно проєктувати інноваційні STEM-курси та інтегрувати вищу математику, програмування і сучасні цифрові технології у профільній середній освіті.

Ключові слова: скінченні поля Галуа, абстрактна алгебра, криптографія, криптографія на еліптичних кривих, комп'ютерні науки, математична освіта, магістерська підготовка.

Yuriy Maturin Candidate of Physical and Mathematical Sciences, Associate Professor, Drohobych Ivan Franko State Pedagogical University, Drohobych, https://orcid.org/0000-0002-0544-1329

Ruslan VKhats' Candidate of Physical and Mathematical Sciences, Associate Professor, Drohobych Ivan Franko State Pedagogical University, Drohobych, https://orcid.org/0000-0001-9905-5447

Lesia Komarnytska Candidate of Physical and Mathematical Sciences, Associate Professor, Drohobych Ivan Franko State Pedagogical University, Drohobych, https://orcid.org/0009-0001-0907-1038

METHODOLOGY FOR STUDYING APPLICATIONS OF GALOIS FIELDS IN COMPUTER SCIENCE

Abstract. This article presents the development, theoretical substantiation, and conceptual explication of a comprehensive and innovative methodological model for teaching the applications of finite Galois fields in computer science to master's students enrolled in the educational and professional program "Secondary Education (Mathematics, Informatics)." The relevance of the study is determined by a profound systemic crisis in the teaching of abstract algebra, which has traditionally been presented to prospective educators through an exclusively deductive and axiomatic

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

framework that remains largely detached from real-world applications and contemporary technological contexts. As a consequence, master's students encounter substantial cognitive barriers, as they frequently fail to perceive the intrinsic connections between the theory of rings, fields, and groups, on the one hand, and modern information technologies, on the other. The purpose of the article is to overcome this didactic discontinuity through the substantive integration of mathematical abstraction and computer science, interpreted through the conceptual and applied frameworks of modern cryptography and coding theory.

The proposed didactic paradigm is grounded in the principle of "dual representation," according to which every abstract mathematical concept (for example, group, ring, field, or isomorphism) should be introduced in parallel with its structural, algorithmic, or software-related analogue in computer science (for example, abstract data type, interface, bitwise operation, or exception handling mechanism). Within this framework, mathematical axioms such as associativity, distributivity, and commutativity are interpreted not merely as formal logical conditions, but also as rigorous programming specifications that ensure computational correctness, operational efficiency, and memory safety, including the prevention of critical failures such as buffer overflows. The methodological basis for implementing this principle is the bottom-up design strategy, which presupposes that the educational process should not begin with ready-made theoretical constructions, but rather with the formulation of an acute engineering problem in cybersecurity, such as the protection of data from unauthorized access, the solution of which naturally necessitates the construction of an appropriate mathematical apparatus, namely finite fields.

The article offers a detailed exposition of a didactic case involving the construction of an algebraic extension in the form of a quotient ring of polynomials over the base prime Galois field GF(2). It demonstrates a methodology for explaining the architecture of a byte as a polynomial of degree at most seven. The authors propose a didactic transition from the abstract characteristic of a field to the algorithmically meaningful operation of carry-less addition, which is computationally equivalent to the logical bitwise XOR function. Particular attention is devoted to the process of polynomial multiplication and to the necessity of modular reduction by the irreducible Rijndael polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$, which preserves the fixed dimensionality of the data block. Within the context of the AES encryption standard, the extended Euclidean algorithm for determining the multiplicative inverse is analyzed in depth, since it constitutes the mathematical core of nonlinear cryptographic transformations, in particular the construction of S-boxes.

The most innovative and pedagogically significant component of the proposed methodological system is the adaptation of Elliptic Curve Cryptography (ECC) to the needs of higher pedagogical education. This part of the article reveals the exceptional didactic potential of elliptic curves as an instrument for the visualization, interpretation, and conceptual materialization of abstract algebraic groups. The methodology presupposes a gradual transition from the geometric construction of point addition

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

through the tangent-and-chord method on the continuous real plane, as defined by the Weierstrass equation, to the algebraization of these operations on the discrete grid of a finite field F_p. The process of proving that the set of points on the curve forms an Abelian group is described in detail, thereby providing students with a nontrivial, conceptually rich, and mathematically powerful example. The culmination of this stage is the examination of the Elliptic Curve Discrete Logarithm Problem (ECDLP), the study of which fosters in master's students a profound understanding of the mathematical foundations of blockchain technologies and modern asymmetric key exchange protocols.

It is argued that an indispensable stage in the full mastery of the material is the compulsory independent software implementation of the algebraic structures under consideration. In this regard, students are encouraged to carry out object-oriented modeling of Galois fields and elliptic curves by means of the Python programming language or through the use of Computer Algebra Systems (CAS), in particular SageMath. Such an approach transforms the lecture-based course into an interactive research laboratory in which mathematical concepts appear not merely as objects of theoretical reflection, but also as entities subject to algorithmic construction and experimental verification. It is ultimately concluded that the implementation of the developed methodology ensures a fundamental transformation of the theoretical mathematical knowledge of master's students into a practically significant algorithmic toolkit. This directly contributes to the formation of their professional competence, enabling future teachers to design innovative STEM-oriented courses effectively and to integrate higher mathematics, programming, and contemporary digital technologies into specialized secondary education.

Keywords: Galois fields, abstract algebra, cryptography, elliptic curves, computer science, mathematics education, master's degree.

Постановка проблеми. Модернізація вітчизняної математичної освіти об'єктивно потребує системного подолання наявного розриву між фундаментальними теоретичними засадами сучасної математики та їх прикладною реалізацією у сфері інформаційних технологій. Для здобувачів другого (магістерського) рівня вищої освіти, які готуються до професійної діяльності як викладачі математики та інформатики, курс абстрактної алгебри нерідко становить суттєву дидактичну проблему, оскільки у традиційній освітній практиці він здебільшого репрезентується ізольовано від задач і методів Computer Science. Водночас саме скінченні алгебраїчні структури, передусім поля Галуа $GF(p^n)$, становлять математичне підґрунтя сучасної криптографії, алгоритмів виявлення та виправлення помилок, а також ключових механізмів кібербезпеки. Відсутність концептуально цілісної та методично вивіреної системи навчання, яка б інтегрувала строгий аксіоматичний апарат теорії кілець і полів із їх алгоритмічною та програмною реалізацією, зокрема в криптографічних системах на еліптичних кривих, істотно знижує рівень фахової

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

підготовки майбутніх педагогів-дослідників і обмежує їхню готовність до міждисциплінарної професійної діяльності.

Аналіз останніх досліджень і публікацій. Сучасні світові тенденції у сфері математичної дидактики засвідчують виразне зміщення теоретико-методологічних акцентів у бік конструктивних, алгоритмічних та обчислювально орієнтованих підходів до навчання [1]. У працях зарубіжних дослідників, зокрема, N. Koblitz [2], W. Stallings [3], W. Gao і M. Li [4] та інших, підкреслюється необхідність переосмислення й реконструкції традиційного курсу алгебри на основі концепції «обчислювальних просторів», що відкриває можливості для органічного поєднання абстрактного математичного мислення з практиками алгоритмізації та комп'ютерного моделювання. Упровадження систем комп'ютерної алгебри, таких як SageMath і GAP, а також включення елементів сучасної криптографії в освітній процес дедалі частіше розглядаються як потужний дидактичний чинник, що виконує функцію ефективного педагогічного інструмента і суттєво підвищує мотивацію студентів до вивчення дискретної математики, абстрактної алгебри та суміжних розділів теоретичної інформатики. Водночас в українській педагогічній і методичній літературі проблема адаптації теорії полів Галуа та криптографії на еліптичних кривих до потреб підготовки здобувачів вищої освіти за предметною спеціальністю А4.04 «Середня освіта (Математика)» і дотепер залишається недостатньо розробленою та фрагментарно висвітленою.

Мета статті полягає у розробленні та теоретичному обґрунтуванні цілісної методичної системи навчання застосувань полів Галуа в комп'ютерних науках, зокрема, в задачах сучасної криптографії, шифрування та геометрії еліптичних кривих, для здобувачів другого (магістерського) рівня вищої освіти освітньо-професійної програми «Середня освіта (Математика, інформатика)», спрямованої на послідовне формування їхніх математичної, алгоритмічної та професійно-методичної компетентностей.

Виклад основного матеріалу.

1. Концептуальні засади методики. Традиційна побудова курсу абстрактної алгебри, що історично сформувалася в руслі класичної університетської математичної освіти, переважно ґрунтується на суворо дедуктивному способі викладу навчального матеріалу. Такий підхід передбачає послідовний рух від максимально абстрактних конструкцій до їх конкретизації: від теоретико-множинних передумов до введення бінарних операцій, формулювання загальних аксіом, зокрема асоціативності, дистрибутивності, існування нейтрального та оберненого елементів, побудови понять напівгрупи, групи, кільця і лише на завершальному етапі − до вивчення полів. Для здобувачів другого (магістерського) рівня вищої освіти за предметною спеціальністю А4.04 «Середня освіта (Математика)» такий рівень початкової абстракції нерідко стає суттєвим когнітивним бар'єром. Унаслідок цього абстрактна алгебра сприймається ними як відокремлена, самодостатня теоретична дисципліна, слабко пов'язана з

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

другою складовою їхньої фахової підготовки − інформатикою. Усвідомлюючи наявність цієї дидактичної проблеми, ми вважаємо за доцільне принципово змінити методологічний вектор викладання, поклавши в його основу інтегративний підхід, який органічно поєднує аксіоматичну строгість математичного мислення з алгоритмічною конструктивністю сучасних комп'ютерних наук.

Концептуальним ядром запропонованої методики є впровадження принципу «подвійного подання» (dual representation) кожної математичної структури. Зміст цього принципу полягає в тому, що жодне абстрактне алгебраїчне поняття не повинно вводитися без одночасного виявлення його чіткого інформаційного, структурного або алгоритмічного відповідника. Магістрант має усвідомити, що алгебраїчна система є не лише множиною з визначеними на ній операціями, а й може бути інтерпретована як абстрактний тип даних (Abstract Data Type, ADT) у термінах сучасного програмування. За такого підходу математичні аксіоми постають як програмні специфікації або інтерфейси, що забезпечують коректну, безпечну та передбачувану поведінку алгоритмів, тоді як теореми функціонують як інваріанти, на основі яких стає можливою оптимізація обчислювальних процесів.

Зазначена синергія між математикою та комп'ютерними науками виявляється на всіх рівнях абстрагування. Так, замкненість алгебраїчної операції може бути дидактично інтерпретована як гарантія відсутності критичних помилок типу buffer overflow під час роботи з типами даних, що репрезентують машинне слово фіксованої довжини. Асоціативність доцільно демонструвати як фундаментальну властивість, яка забезпечує можливість безпечного розпаралелювання обчислень (parallel computing) без втрати коректності підсумкового результату. Існування оберненого елемента розглядається як базова умова побудови зворотних криптографічних перетворень, тобто надійного дешифрування. У такий спосіб математична абстракція перестає постати як самодостатня теоретична мета й набуває в очах здобувача статусу функціонального інструмента проєктування стійких та ефективних інформаційних систем.

На противагу традиційному дедуктивному викладові нами пропонується використання стратегії висхідного проєктування (bottom-up design). Такий дидактичний прийом певною мірою відтворює природну логіку наукового пошуку та інженерного конструювання. Замість того щоб спочатку подавати готовий математичний апарат, а вже потім добирати до нього приклади застосування, викладач свідомо створює ситуацію когнітивного дисонансу через постановку конкретної прикладної проблеми з галузі комп'ютерних наук. Студентам пропонується розв'язати реальну задачу, для якої традиційна арифметика дійсних або цілих чисел виявляється принципово неадекватною.

Як приклад такої тригерної задачі розглядається проблема забезпечення цілісності та конфіденційності даних під час їх передавання каналами зв'язку. Формулюється технічне завдання: побудувати алгоритм шифрування одного блока даних, тобто байта, який одночасно задовольняв би вимоги повної

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

оборотності, відсутності похибок округлення та збереження фіксованого обсягу пам'яті, а саме 8 бітів на вході і 8 бітів на виході. У процесі аналізу магістранти переконуються, що неперервна множина дійсних чисел R не є придатною для такого завдання через проблеми машинної точності та необхідність оперувати потенційно нескінченними ресурсами пам'яті. Водночас звичайне кільце цілих чисел Z або арифметика за модулем складеного числа також не задовольняють поставленим вимогам, оскільки в подібних структурах існують дільники нуля і не кожний елемент має мультиплікативний обернений, що алгоритмічно унеможливлює побудову однозначного дешифрування. Саме цей етап − усвідомлення недостатності класичного математичного інструментарію − становить найбільш продуктивний дидактичний момент для введення теорії Галуа.

Конструктивний метод у цьому контексті передбачає безпосередню побудову числових множин [5] і операцій над ними на основі вже засвоєних математичних ідей. Спираючись на цей підхід, із яким магістранти попередньо ознайомилися в курсі математичного аналізу під час розширення множини раціональних чисел до множини дійсних, зокрема, через перерізи Дедекінда [5], ми пропонуємо їм самостійно «сконструювати» алгебраїчне середовище, яке відповідало б інженерним вимогам сучасної кібербезпеки. Байт даних у межах такого підходу інтерпретується не просто як число, а як поліном степеня не вище сьомого над простим полем Галуа GF(2). Операція побітового додавання, тобто XOR, природно виводиться як додавання поліномів, у якому виконується співвідношення 1 + 1 = 0, що автоматично розв'язує проблему збереження фіксованої розрядності. Натомість операція множення потребує введення незвідного полінома, який виконує функцію своєрідного «модуля» для забезпечення сталої розмірності масиву даних. За такого конструктивного розгортання навчального матеріалу означення фактор-кільця поліномів $F_2[x]/<m(x)>$ втрачає надмірну теоретизованість і сприймається здобувачами як елегантне математично точне інженерне розв'язання складної алгоритмічної проблеми. Більше того, це формує розуміння того, що вибір конкретного незвідного полінома у криптографічному стандарті AES не є випадковим, а є математично детермінованим кроком, спрямованим на досягнення максимальної дифузії.

Ще однією принципово важливою складовою запропонованих концептуальних засад є обов'язкова програмна реалізація досліджуваних алгебраїчних структур. Принцип «подвійного подання» передбачає, що доведення теоретичних тверджень має супроводжуватися створенням відповідного алгоритмічного коду. Використовуючи сучасні мови програмування, зокрема Python, або системи комп'ютерної алгебри (Computer Algebra Systems, CAS), наприклад SageMath, магістранти конструюють власні класи та модулі, які імітують поведінку елементів скінченних полів. Самостійна програмна реалізація розширеного алгоритму Евкліда для поліномів з метою знаходження

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

мультиплікативного оберненого елемента виконує подвійну функцію: з одного боку, вона слугує засобом глибокого математичного осмислення відповідної теорії, а з іншого − формує практичні навички проєктування й реалізації ефективних алгоритмів.

Унаслідок цього лекційний курс трансформується в інтерактивну цифрову лабораторію, у межах якої абстрактні об'єкти можна не лише теоретично описувати, а й генерувати, тестувати щодо швидкодії криптографічних примітивів та емпірично перевіряти на відповідність базовим алгебраїчним аксіомам.

Зрештою, окреслений підхід безпосередньо орієнтований на формування професійно-методичної компетентності майбутнього викладача-дослідника. Магістр, який на концептуально глибокому рівні усвідомив абстрактну алгебру як універсальну мову проєктування інформаційних систем, отримує можливість продуктивно застосовувати ці знання у своїй подальшій педагогічній діяльності. Такий фахівець набуває унікальної здатності методично адаптувати складний математичний матеріал для учнів профільних ІТ-класів, студентів коледжів та інших категорій здобувачів освіти, а також розробляти інтегровані STEM-курси, у межах яких поняття подільності, простих чисел, конгруенцій та алгебраїчних структур вивчаються в процесі створення школярами власних утиліт для шифрування даних або генерації кодів виправлення помилок Ріда–Соломона. Отже, парадигма подвійного подання в поєднанні зі стратегією висхідного проєктування не лише підвищує рівень фахової підготовки магістрантів, а й забезпечує їх сучасним інноваційним дидактичним інструментарієм, який повною мірою відповідає інтелектуальним і технологічним викликам цифрової епохи.

2. Дидактичний кейс: арифметика GF(256) та стандарт AES. Фундаментальним етапом запропонованої методики є вивчення будови байта не лише як базової одиниці зберігання інформації, а передусім як елемента алгебраїчного розширення поля. Такий ракурс принципово змінює науково-методичний світогляд здобувачів освіти: замість суто утилітарного сприйняття байта як набору нулів і одиниць, призначеного виключно для машинної обробки, майбутнім учителям відкривається його глибока структурна та алгебраїчна природа. Байт інтерпретується як поліном степеня не вище сьомого, коефіцієнти якого належать простому базовому полю Галуа GF(2), тобто можуть набувати лише двох можливих значень − 0 або 1. Саме такий підхід уможливлює встановлення строгого ізоморфізму між множиною всіх 256 можливих станів байта F_2^8 та відповідним фактор-кільцем поліномів. Наприклад, класичний двійковий рядок 01010111_2, який у шістнадцятковій системі числення записується як 57_{16}, дістає математично строгу інтерпретацію у вигляді многочлена:

$f(x) = 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 1 \cdot x^1 + 1 \cdot x^0 = x^6 + x^4 + x^2 + x + 1.$

Завдяки такому поданню будь-яка послідовність бітів набуває статусу

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

повноцінного алгебраїчного об'єкта, до якого можуть бути застосовані концептуальні засоби й методи класичної теорії кілець та полів.

Методичний акцент першого рівня складності, тобто рівня адитивної структури, зосереджується на тому, що поле GF(2) має характеристику 2, а отже, для кожного елемента $a \in GF(2)$ виконується тотожність $a + a = 0$. Дидактичне значення цього факту є винятково високим. У ході аудиторної роботи магістранти самостійно приходять до висновку, що додавання поліномів над таким полем відбувається без перенесення розряду (carry-less addition). У термінах комп'ютерної архітектури ця операція виявляється обчислювально тотожною швидкій апаратній побітовій логічній операції «виключне АБО» (XOR, що позначається символом XOR). Водночас операція віднімання стає повністю тотожною додаванню, унаслідок чого зникає потреба в окремому апаратному або програмному розмежуванні цих двох арифметичних дій. У такий спосіб студент безпосередньо спостерігає, як абстрактна алгебраїчна властивість трансформується в елегантне інженерне рішення, яке забезпечує економію процесорного часу та зменшує апаратну складність мікроелектронних систем.

Перехід до мультиплікативної структури, тобто до множення елементів, формує другий рівень складності й водночас становить кульмінаційний момент цього дидактичного кейсу. Множення двох поліномів степеня 7 за правилами класичної алгебри неминуче приводить до утворення полінома степеня аж до 14. З інформатичного погляду це означає вихід за межі 8-бітного регістру, тобто виникнення ситуації byte overflow, що є принципово неприпустимим для алгоритмів блочного шифрування, які вимагають строгої інваріантності розміру блока даних. Саме на цьому етапі викладач вводить поняття модульної редукції за незвідним поліномом, проводячи чітку й методично продуктивну аналогію з роллю простих чисел в арифметиці Z_p. Для стандарту Advanced Encryption Standard (AES), реалізованого алгоритмом Рейндаля (Rijndael), жорстко зафіксовано поліном восьмого степеня: $m(x) = x^8 + x^4 + x^3 + x + 1$. Цей поліном є незвідним над GF(2), тобто не розкладається на множники нижчих степенів, що гарантує відсутність дільників нуля і, відповідно, перетворює кільце поліномів на повноцінне скінченне поле $GF(2^8)$. Будь-який результат множення, степінь якого є більшим або дорівнює 8, ділиться на m(x) з остачею, і саме ця остача розглядається як остаточний результат відповідної операції.

З метою уникнення надмірного формалізму та подолання алгоритмічного відчуження магістрантам пропонується докладно розглянути концепцію множення на базовий елемент x, яка в контексті AES реалізується через функцію xtime. З аналітичного погляду множення довільного полінома b(x) на x є еквівалентним зсуву всіх бітів байта на одну позицію вліво (left shift). Якщо старший біт початкового байта дорівнює 0, операція на цьому завершується. Якщо ж старший біт дорівнює 1, такий зсув породжує біт, що «виходить» за межі байта, тобто відповідає члену x^8. Відповідно до структури поля, необхідно виконати редукцію результату, замінивши x^8 на $x^4 + x^3 + x + 1$, що в програмній

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

реалізації зводиться до застосування операції XOR з константою 11011_2, або, у шістнадцятковому записі, $1B_{16}$. Саме такий мікрорівневий аналіз наочно демонструє майбутнім учителям, чому складні алгебраїчні обчислення, покладені в основу криптографії, можуть виконуватися з надзвичайно високою швидкістю навіть на малопотужних пристроях, вбудованих системах або смарт-картах.

Третім, найбільш абстрактним за своїм змістом етапом є вивчення операції знаходження мультиплікативного оберненого елемента, яка є критично необхідною для побудови S-блоків (Substitution boxes) у стандарті AES. Магістранти мають усвідомити глибинне криптографічне підґрунтя цієї конструкції: лінійні операції, зокрема XOR, відносно легко піддаються криптоаналітичному дослідженню. Саме тому для забезпечення криптографічної стійкості шифру К. Шеннон сформулював принцип конфузії, або плутанини, який вимагає застосування нелінійних перетворень. У межах алгебри полів Галуа однією з найнадійніших нелінійних операцій є інверсія, тобто відображення вигляду $x \to x^{-1} \pmod{m(x)}$. Оскільки $GF(2^8)$ є полем, для кожного ненульового елемента гарантовано існує єдиний мультиплікативно обернений елемент. Для його знаходження здобувачам пропонується вивчити й реалізувати поліноміальний варіант розширеного алгоритму Евкліда.

З метою остаточного закріплення набутих знань і переведення їх із пасивно-рецептивного рівня на активний діяльнісний рівень доцільно організувати лабораторну роботу з моделювання відповідних алгебраїчних структур. Магістрантам пропонується самостійно реалізувати об’єктно-орієнтовану модель поля $GF(2^8)$ мовою програмування Python. Використовуючи механізм перевантаження магічних методів (Dunder methods), таких як __add__, __mul__, __invert__, студенти проєктують клас GaloisFieldElement. Написання програмного коду для множення в полі змушує здобувача власноруч реалізувати побітові зсуви та процедуру редукції за модулем $1B_{16}$, тоді як створення функції для знаходження оберненого елемента вимагає глибокого розуміння розширеного алгоритму Евкліда на рівні циклічних структур, покажчиків, умов переходу та загальної логіки обчислювального процесу.

Розглянутий дидактичний кейс має виразний синергетичний ефект. Він фактично руйнує усталений стереотип про абстрактну алгебру як про дисципліну, відірвану від реальних технічних застосувань. Коли магістрант власноруч створює програмний код, який реалізує аксіоми кільця для поліномів, а згодом переконується, що саме цей код лежить в основі побудови криптографічно стійкого S-блока стандарту AES, за допомогою якого щосекунди здійснюється шифрування величезної кількості банківських транзакцій у глобальному цифровому середовищі, відбувається справжнє професійне усвідомлення значущості математичної теорії. У свідомості здобувача формується міцний інтелектуальний зв’язок між теорією кілець, поліморфізмом у програмуванні та апаратною логікою сучасних мікропроцесорних систем. Як

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

наслідок, майбутній педагог набуває здатності оперувати поняттями вищої математики як гнучким інструментом проєктування, що в подальшій професійній діяльності дасть йому змогу вільно конструювати авторські міждисциплінарні STEM-курси, у яких математична строгість органічно поєднується з інженерною прагматикою та цифровою технологічністю.

3. Еліптичні криві над полями Галуа як засіб візуалізації груп. Найбільш інноваційним і дидактично змістовним складником пропонованої методики є введення елементів криптографії на еліптичних кривих (Elliptic Curve Cryptography, ECC). У традиційному курсі вищої алгебри теорія груп найчастіше ілюструється відносно простими числовими прикладами, зокрема адитивними групами цілих чисел, мультиплікативними групами матриць або групами симетрій геометричних фігур. Водночас саме еліптичні криві над скінченними полями надають унікальну можливість продемонструвати магістрантам нетривіальний, концептуально глибокий і водночас візуально інтуїтивний приклад абстрактної алгебраїчної структури, яка становить один із фундаментів сучасних систем кіберзахисту. Цей розділ має винятково високий педагогічний потенціал, оскільки дає змогу візуалізувати абстрактні поняття теорії груп за допомогою геометричних образів, алгебраїчних співвідношень і алгоритмічних перетворень.

У межах відповідного навчального модуля розглядається класичне рівняння Вейєрштрасса над простим полем Галуа F_p, де $p > 3$ − просте число:

$$y^2 \equiv x^3 + ax + b \pmod{p}.$$

Принципово важливою дидактичною умовою є введення поняття дискримінанта еліптичної кривої. Викладач має спеціально акцентувати увагу на вимозі відсутності кратних коренів, тобто особливих точок, точок самоперетину або загострення, що в математичному вираженні задається умовою:

$$\Delta = -16(4a^3 + 27b^2) \not\equiv 0 \pmod{p}.$$

Методика вивчення цього змістового блоку для магістрів предметної спеціальності А4.04 «Середня освіта (Математика)» структурована у вигляді трьох послідовних, взаємопов’язаних і концептуально цілісних етапів:

• Геометрична інтерпретація операції та дидактичний перехід до дискретності.

На першому етапі навчання магістрантам пропонується дослідити еліптичну криву над полем дійсних чисел R. За допомогою систем динамічної математики, зокрема GeoGebra або Desmos, майбутні вчителі візуалізують відповідну криву та відтворюють геометричне правило додавання двох точок P і Q − метод січної і дотичної. У процесі цієї роботи вони наочно переконуються, що пряма, проведена через дві точки кривої, неодмінно перетинає її ще в одній, третій точці, а відображення цієї третьої точки відносно осі абсцис і визначає результат операції додавання.

Справжній когнітивний прорив відбувається тоді, коли викладач здійснює перенесення цієї неперервної геометричної моделі на дискретну ґратку точок

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

скінченного поля F_p. Графік кривої втрачає неперервний характер і візуально постає як розсіяна система точок, що набуває вигляду своєрідної «псевдовипадкової хмари» в квадраті $[0, p-1] \times [0, p-1]$. Проте майбутнім учителям демонструється принципово важливий математичний факт: алгебраїчні формули додавання, виведені на основі геометричних міркувань для дійсних чисел, зберігають свою чинність і в умовах модульної арифметики. Для обчислення координат суми $R(x_3, y_3) = P(x_1, y_1) + Q(x_2, y_2)$ магістранти застосовують формули:

$$\lambda \equiv (y_2 - y_1)(x_2 - x_1)^{-1} \pmod p,$$
$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod p,$$
$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod p.$$

Методичний акцент при цьому робиться на тому, що операція ділення, представлена через множник $(x_2 - x_1)^{-1}$, у полі F_p фактично зводиться до знаходження мультиплікативного оберненого елемента за допомогою розширеного алгоритму Евкліда. Це створює потужний міждисциплінарний зв'язок із теорією чисел і водночас поглиблює розуміння студентами природи модульних обчислень.

Поряд із базовим правилом додавання двох різних точок, критично важливою дидактичною складовою є розгляд випадку подвоєння точки, тобто ситуації, коли $P = Q$. З геометричного погляду на неперервній площині це відповідає проведенню дотичної до еліптичної кривої в точці $P(x_1, y_1)$. Оскільки в дискретному просторі поля F_p класичне геометричне поняття дотичної втрачає свій первісний наочний зміст, викладач має продемонструвати концептуальний перехід за допомогою методів алгебраїчної геометрії. Кутовий коефіцієнт λ у цьому випадку знаходиться через неявне диференціювання формальної похідної від рівняння Вейєрштрасса і обчислюється за формулою:

$$\lambda \equiv (3x_1^2 + a)(2y_1)^{-1} \pmod p,$$

за умови, що $y_1 \not\equiv 0 \pmod p$ (інакше дотична стає вертикальною, і результатом подвоєння є нескінченно віддалена точка, нейтральний елемент: $P + P = O$). Координати результуючої точки $R(x_3, y_3) = 2P$ обчислюються за тими самими базовими формулами для x_3 та y_3. Введення цієї формули є не лише вимогою математичної повноти, а й суворою алгоритмічною необхідністю, адже саме математична операція подвоєння становить обчислювальний фундамент алгоритму скалярного множення Double-and-Add, який магістранти програмно реалізовуватимуть на наступному етапі вивчення.

• Алгебраїчна структура та комп'ютерно підтримуване доведення властивостей абелевої групи.

На другому етапі студенти доводять, що множина точок еліптичної кривої разом зі спеціальною нескінченно віддаленою точкою O утворює абелеву групу. Точка O вводиться як нейтральний елемент, тобто як аналог нуля відносно операції додавання, а обернений до точки елемент визначається геометрично просто: $-P = (x_P, -y_P \pmod p)$. Особливу педагогічну цінність має аналіз аксіоми

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

асоціативності: (P + Q) + R = P + (Q + R). Аналітичне доведення цієї властивості вручну є вкрай громіздким і технічно складним, тому викладач використовує саме цей момент для продуктивної інтеграції інформатичного компонента у вивчення вищої алгебри. Магістрантам пропонується написати скрипт мовою Python або використати систему комп'ютерної алгебри SageMath для символьної чи чисельної перевірки асоціативності. Завдяки цьому студенти отримують нетривіальний і водночас методично надзвичайно цінний приклад групи, елементами якої є не окремі числа, а впорядковані пари координат, тоді як комп'ютер постає не лише як засіб ілюстрування, а як повноцінний інструмент математичного дослідження, експерименту та перевірки гіпотез.

• **Проблема дискретного логарифмування на еліптичних кривих (ECDLP) та її зв'язок із комп'ютерними науками.**

Завершальний етап присвячено переходу від чисто математичного аналізу до прикладної криптографії. На цьому рівні вводиться поняття скалярного множення точки на ціле число k:

$$k \cdot P = P + P + ... + P \text{ (k разів)}.$$

Здобувачам освіти демонструється алгоритм подвоєння та додавання (Double-and-Add), який дає змогу обчислювати $k \cdot P$ за логарифмічний час O(log k). У методичному плані принципово важливо показати, що цей алгоритм безпосередньо спирається на двійкове подання числа k, а отже, актуалізує вже наявні в студентів знання з інформатики, дискретної математики та архітектури обчислень.

Головна концептуальна ідея, яку повинен засвоїти магістрант, полягає в асиметричному характері цієї операції. Пряма задача, тобто обчислення $Q = k \cdot P$ за заданими k та P, розв'язується ефективно. Натомість обернена задача − відновити множник k за відомими точками P та Q − для класичних комп'ютерів не має ефективного поліноміального алгоритму розв'язання. Саме ця задача дістала назву проблеми дискретного логарифмування на еліптичних кривих (Elliptic Curve Discrete Logarithm Problem, ECDLP). Викладач має пояснити, що саме відсутність для еліптичних кривих субекспоненційних алгоритмів розв'язування цієї задачі, на відміну від ситуації з RSA, де застосовується метод решета числового поля, забезпечує можливість використання значно коротших ключів за збереження того самого рівня криптографічної стійкості. Наприклад, 256-бітний ключ ECC забезпечує приблизно той самий рівень захисту, що й 3072-бітний ключ RSA. Саме це становить одну з теоретичних основ сучасної асиметричної криптографії, яка лежить в основі блокчейн-технологій (зокрема стандарту secp256k1), захищених протоколів зв'язку TLS/SSL та алгоритмів цифрового підпису, таких як ECDSA.

Залучення еліптичних кривих до змісту навчального курсу має виразний синергетичний ефект. Воно дає змогу майбутнім учителям побачити внутрішню логіку й концептуальну красу інтеграції вищої алгебри, зокрема теорії груп і полів Галуа, аналітичної геометрії, представленої кривими третього порядку, та

Журнал «Перспективи та інновації науки»
№4(62) 2026
ISSN 2786-4952 Online

комп'ютерних наук, які охоплюють алгоритмічну складність, криптографічні протоколи та обчислювальні моделі. Унаслідок такого підходу здобувач освіти перестає бути пасивним ретранслятором готових формул і перетворюється на компетентного фахівця, здатного осмислено розуміти, методично адаптувати та професійно викладати математичні основи найсучасніших інформаційних технологій цифрового суспільства.

Висновки. Запропонована методика вивчення полів Галуа засвідчує свою високу дидактичну ефективність у процесі підготовки магістрів за предметною спеціальністю А4.04 «Середня освіта (Математика)». Перенесення акценту з суто абстрактного опрацювання теоретичних конструкцій на їхню конструктивну, алгоритмічну та програмно орієнтовану реалізацію, зокрема в межах арифметики поля GF(256) та криптографії на еліптичних кривих, дає змогу здобувачам вищої освіти осмислити математику не лише як систему формальних знань, а як фундаментальний концептуальний і алгоритмічний код сучасних цифрових технологій. Такий підхід забезпечує формування фахівця нового типу, здатного не лише до глибокого розуміння математичних основ інформаційних процесів, а й до проєктування та реалізації сучасних міждисциплінарних STEM-курсів у профільній середній школі та закладах фахової передвищої освіти.

Література:

1. Андрійчук В.І., Комарницький М.Я., Іщук Ю.Б. Вступ до дискретної математики. Львів: Видавничий центр ЛНУ ім. І. Франка, 2003. 254 с.

2. Koblitz, N. A Course in Number Theory and Cryptography. Springer-Verlag, 1994.

3. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson, 2017.

4. Gao, W., Li, M. A Computational-Space-Oriented Reconstruction of Abstract Algebra Teaching in Foundations of Information Security Mathematics. *International Journal of Computer Science and Information Technology*, 8(3), 2026, 73-81. doi:https://doi.org/10.62051/ijcsit.v8n3.08

5. Хаць Р.В., Комарницька Л.І., Матурін Ю.П. Аксіоматичний та конструктивний підходи до побудови теорій числових множин. Перспективи та інновації науки (Серія "Педагогіка"), 2(60), 2026, 1572-1585. doi:https://doi.org/10.52058/2786-4952-2026-2(60)-1572-1585

References:

1. Andriichuk, V.I., Komarnytskyi, M.Ya., & Ishchuk, Yu.B. (2003). Vstup do dyskretnoi matematyky [Introduction to discrete mathematics]. Lviv: Vydavnychyi tsentr LNU im. I. Franka [in Ukrainian].

2. Koblitz, N. (1994). A Course in Number Theory and Cryptography. Springer-Verlag.

3. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

4. Gao, W., & Li, M. (2026). A Computational-Space-Oriented Reconstruction of Abstract Algebra Teaching in Foundations of Information Security Mathematics. International Journal of Computer Science and Information Technology, 8(3), 73-81. doi:https://doi.org/10.62051/ijcsit.v8n3.08

5. Khats, R.V., Komarnytska, L.I., & Maturin, Yu.P. (2026). Aksiomatychnyi ta konstruktyvnyi pidkhody do pobudovy teorii chyslovykh mnozhyn. Perspektyvy ta innovatsii nauky

Журнал «Перспективи та інновації науки»
№4(62) 2026

ISSN 2786-4952 Online

(Seriia "Pedahohika"), 2(60), 1572-1585 [in Ukrainian]. doi:https://doi.org/10.52058/2786-4952-2026-2(60)-1572-1585

Дата першого надходження статті до видання: 03.04.2026
Дата прийняття статті до друку після рецензування: 17.04.2026