

## Роль алгебраической составляющей математических курсов в профессиональной подготовке студентов ИТ-специальностей

Подлевских Марина Николаевна

кандидат физико-математических наук, доцент, доцент кафедры прикладной математики и информатики,  
Вятский государственный университет. Россия, г. Киров. E-mail: podlevskih@vyatsu.ru

**Аннотация.** Важность математической подготовки в становлении ИТ-специалистов отражается в значительном объеме математических курсов, входящих в соответствующие образовательные программы. Одной из первоначальных методических задач выстраивания рабочей программы учебной дисциплины является обоснованный отбор учебного материала. Содержание учебных курсов должно соответствовать постоянно изменяющимся требованиям, предъявляемым сферой профессиональной деятельности, быть ориентированным на развитие личности будущего специалиста и обеспечивать его конкурентоспособность на рынке труда. В данной статье на основе опыта работы со студентами ИТ-направлений подготовки, используя некоторые результаты приложений алгебраических методов в современных исследованиях теоретической информатики, автор анализирует алгебраическую составляющую математических дисциплин, раскрывает ее значимость в профессиональной подготовке будущих специалистов. Полученные результаты могут быть использованы для конструирования математических курсов указанных направлений подготовки.

**Ключевые слова:** алгебра, теория чисел, теоретическая информатика, содержание учебных курсов, ИТ-специальности.

Программирование как наука базируется на классических математических дисциплинах, среди которых наиболее важную роль играют алгебра и математическая логика. Прикладные ИТ-специальности требуют серьезной подготовки в математическом моделировании соответствующей предметной области. Разнообразие направлений подготовки, связанных с ИТ-сферой и реализуемых в высшей школе, влечет за собой различные подходы к формированию учебных планов, рабочих программ и наполнению учебных курсов, при этом возможность создания и использования электронных учебных пособий и целых учебных курсов позволяет достаточно гибко варьировать предлагаемый учебный материал. В этой ситуации возникает проблема выделения базиса содержания математической подготовки, который необходим для формирования профессиональных компетенций ИТ-специалистов. Особое значение эта методическая задача приобретает сейчас, когда в РФ ожидается переход на новые стандарты высшего образования.

Обоснованием необходимости выделения алгебраической составляющей в математической подготовке ИТ-специалистов является широкое применение алгебраических методов при формализации различных предметных областей, включая информатику. Практическому программированию задачи из конкретной предметной области предшествует создание абстрактной модели, для построения которой необходимо владение в том числе алгебраической терминологией. Это позволяет ввести подходящие операции и отношения, с помощью которых строится модель, определять их свойства, имеющие алгебраическую природу, и впоследствии использовать эти свойства для анализа модели. Поэтому для студентов, изучающих информатику как основу выбранной специальности, «основным содержанием математической подготовки является овладение средствами исследования разнообразных математических объектов, их взаимосвязей и преобразований» [3, с. 31]. Такая формулировка указывает на важность генерализации знаний, одного из принципов фундаментальности образования, который подробно проанализирован в статье [9], где, в частности, утверждается, что «генерализация знаний позволяет обеспечить и лучшее понимание, поскольку порождает структуру, которая значительно теснее взаимодействует с новыми знаниями, чем отдельные факты» [9, с. 8]. Изучение разделов современной алгебры предоставляет возможность реализовать этот принцип при построении математических курсов посредством изучения алгебраических структур. Подробный методологический анализ этого алгебраического материала можно найти в пособии [1].

Фундаментальность понятий современной алгебры и их широкое использование в информатике и других областях математики позволяют создавать на основе алгебраических конструкций интегральные учебные курсы. Например, в статье [3] автор предлагает использовать многоосновные алгебры как «важный интегрирующий учебно-методический конструкт для программ и курсов разных видов и уровней» [6, с. 155].

Многоосновные алгебраические системы используются как математические модели абстрактных типов данных, например, при решении проблемы автоматизации программирования задач, связанных с обработкой больших объемов информации в базах данных. Этот подход в теоретической информатике позволяет найти решение следующих практических задач: создание программного обеспечения, независимого от операционной среды; переработка программного обеспечения уровня взаимодействия с пользователем; описание процессов обработки данных, которые возможно оптимизировать. Идея использования алгебраических систем в управлении базами данных описана в статье [4]. Для понимания данного подхода к решению практических задач от специалистов требуется знание как минимум основ *абстрактной алгебры*.

Классическими математическими моделями, используемыми IT-специалистами в различных прикладных областях, являются линейные модели, изучением которых занимается *линейная алгебра*. Например, многие модели машинного обучения выражаются в матричном виде. Для обработки, преобразования данных и оценки таких моделей используются следующие понятия линейной алгебры и *теории векторных пространств*: обратная и транспонированная матрица; след, определитель, собственные значения и собственные векторы матрицы; размерность объекта или системы; векторы и их скалярное произведение, линейная зависимость и другие. Линейные модели, используемые в машинном обучении, можно найти в учебном пособии [8].

Для изучения основ теории кодирования, раздела теории информации, необходимо владеть методами *теории конечных полей*, которая является важной прикладной частью *теории алгебраических структур*. Теория конечных полей также использует *теорию многочленов*, тесно связанную с развитием классической алгебры.

В современных методах кодирования и шифрования успешно применяются понятия и методы алгебраической *теории чисел*. Например, для обмена данными, верификации источника программного обеспечения или отправителя данных используется алгоритм криптографии RSA, который является базовой частью HTTPS-протокола, широко используемого в РФ. Данный алгоритм основан на применении двух ключей: открытого и закрытого. Не обсуждая, как работает этот алгоритм, остановимся на процедуре получения этих ключей, что является математической задачей, состоящей из следующих этапов.

1. По отобранным случайнным образом двум простым числам и вычисляется функция Эйлера от произведения этих чисел:  $\varphi(pq) = \varphi(n)$ .

2. Выбирается число  $e$ , удовлетворяющее системе условий:  $e < \varphi(n)$  и  $\text{НОД}(e, \varphi(n)) = 1$ .

3. Находится число  $x$ , удовлетворяющее сравнению:  $ex \equiv 1 \pmod{\varphi(n)}$ .

4. Пары полученных чисел определяют ключи шифрования: – открытый ключ, – закрытый ключ.

Следовательно, для определения ключей шифрования в RSA необходимо знать следующие факты из теории чисел: простое число, взаимно-простые числа, наибольший общий делитель (НОД), функция Эйлера и ее свойства, отношение сравнимости по модулю. Кроме того, нужно уметь проводить генерацию простых чисел, вычислять функцию Эйлера, находить НОД пары чисел (алгоритм Евклида), решать сравнения с одной переменной, проводить вычисления, используя модульную арифметику, в том числе для процедуры шифровки и дешифровки информации. Знание основ теории чисел также дает понимание идеи, на которой основан данный алгоритм шифрования: сложность задач дискретного логарифмирования и факторизации произведения двух больших простых чисел. Подробное описание математической основы этой идеи шифрования можно найти в учебных пособиях по теории чисел, рекомендуемых для высшего образования, например [7].

Значимость изучения алгебраического материала, на наш взгляд, состоит в том, что на его основе создается база идей, применяемых при решении разнообразных прикладных задач, в том числе задач информатики. Это выявление структуры объекта относительно операций над этим объектом; понимание тождественности, изоморфности, гомоморфности объектов; арифметизация объекта; возможность описания объекта на основе различных систем оценок; получение новых объектов с помощью алгебраических методов, таких как подструктура или фактор-объект; выстраивание иерархии объектов; применение наиболее простых или наиболее адекватных поставленной задаче преобразований с объектами.

Например, изучение кольца классов вычетов не только дает пример факторизации кольца целых чисел, но и позволяет продемонстрировать возможность замены процедуры в общем виде бесконечного перебора на перебор конечный – ситуация, которая встречается во многих прикладных задачах. Знакомство с понятиями базиса и системы образующих в теории векторных пространств показывает, как бесконечное число объектов можно однозначно описать минимальным, возможно конечным и независимым друг от друга набором параметров, а возможность перехода к другому базису – это возможность изменения системы параметров или оценок, описывающих объект.

Включение алгебраического материала в математические курсы имеет и методологическое значение: знакомство с различными алгебраическими структурами дает современное представление о содержании математики как науки. Изучение различных алгоритмов решения алгебраических задач, применяемых в теоретической информатике, а также их обоснование формирует алгоритмическую культуру обучающихся. Задачи, имеющие известный алгоритм решения, можно решать с помощью систем компьютерной математики. Их использование в процессе обучения позволяет освободить время для более глубокого изучения материала, а также дает возможность разнообразить предлагаемый учебный материал, включая в него задания творческого характера, что формирует более конкурентоспособного специалиста.

Итак, изучение основ современной алгебры и теории чисел позволяет решать важные задачи в профессиональной подготовке IT-специалистов, что необходимо учитывать при разработке образовательных программ и учебных планов соответствующих направлений подготовки. Объем статьи не позволяет привести большее число примеров, но можно сделать вывод, что к алгебраической составляющей математической подготовки IT-специалистов следует как минимум отнести: линейную алгебру, включающую теорию векторных пространств; отдельные разделы теории чисел; теорию алгебраических и порядковых структур; теорию многочленов.

Отметим, что в зависимости от реализуемой образовательной программы и уровня подготовки студентов данное содержание можно оформить в виде отдельного курса алгебры и теории чисел или распределить по разным учебным математическим дисциплинам. Как математическую основу элементы алгебры и теории чисел можно включать в содержание специальных профессионально ориентированных учебных курсов, таких как, например, теория автоматов, теория кодирования. Отдельные темы, имеющие прикладное значение, могут стать основой факультативов или частью самостоятельной работы для подготовки к специальным курсам, например [2, 5]. В качестве примера приведем также курс математики, разработанный преподавателями кафедры прикладной математики и информатики ВятГУ [10].

### Список литературы

1. Вечтомов Е. М. Основные математические структуры. Киров : Радуга-ПРЕСС, 2013. 292 с.
2. Вычисления в конечных полях : учеб.-метод. пособие / Ш. Т. Ишмухаметов, Р. Г. Рубцова. Казань : Казанский ун-т, 2019. 23 с.
3. Гейн А. Г. Фундаментальное математическое образование и подготовка IT-аналитиков // Образовательные технологии. 2018. № 1. С. 28–33.
4. Емельченков Е. П., Левин Н. А., Мунерман В. И. Алгебраический подход к оптимизации разработки и эксплуатации систем управления базами данных // Системы и средства информатики : сб. ст. М., 2009. Т. 19, № 2. С. 114–137.
5. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел : учеб. пособие. Казань : Казанский федеральный университет, 2011. 190 с.
6. Многоосновные алгебры как интегрирующий конструкт при комплексном изложении учебных курсов в области естественных наук и когнитивных методов / И. В. Степура // Наука и образование: опыт, проблемы, перспективы развития : сб. ст. по материалам междунар. науч.-практ. конф. Красноярск, 2021. Т. 2, ч. 2. С. 151–156.
7. Нестеренко Ю. В. Теория чисел : учеб. для студ. высш. учеб. завед. М. : Академия, 2008. 272 с.
8. Практический курс классического машинного обучения с использованием моделей математического программирования : учеб.-метод. пособие / П. Ф. Чернавин, Н. П. Чернавин, Ф. П. Чернавин. Екатеринбург : Издво Урал. ун-та, 2023. 124 с.
9. Гестов В. А. Фундаментальность образования: современные подходы // Педагогика. 2006. № 4. С. 3–9.
10. Курс математики. URL: <https://e.vyatsu.ru/course/view.php?id=5504>.

## The role of the algebraic component of mathematical courses in the professional training of students of IT specialties

Podlevskikh Marina Nikolaevna

PhD in Physical and Mathematical Sciences, associate professor, associate professor of the Department of Applied Mathematics and Computer Science, Vyatka State University, Russia, Kirov. E-mail: podlevskikh@vyatsu.ru

**Abstract.** The importance of mathematical training in the development of IT specialists is reflected in the significant volume of mathematical courses included in the relevant educational programs. One of the initial methodological tasks of building a work program for an academic discipline is the reasonable selection of educational material. The content of the training courses should meet the constantly changing requirements of the field of professional activity, be focused on the personal development of the future specialist and ensure his competitiveness in the labor market. Based on the experience of working with students of IT fields of study, using some results of applications of algebraic

methods in modern research of theoretical computer science, this article analyzes the algebraic component of mathematical disciplines and reveals its importance in the professional training of future specialists. The results obtained can be used to design mathematical courses in these areas of study.

**Keywords:** algebra, number theory, theoretical computer science, the content of the training course, IT qualifications.

### **References**

1. Vechtomov E. M. *Osnovnye matematicheskie struktury* [Basic Mathematical Structures]. Kirov, Raduga-PRESS. 2013. 292 p.
2. *Vychisleniya v konechnykh polyah : ucheb.-metod. posobie* [Computations in a finite fields : educational and methodological guide] / Sh. T. Ishmukhametov, R. G. Rubtsova. Kazan, Kazan Federal University. 2019. 23 p.
3. Gein A. G. *Fundamental'noe matematicheskoe obrazovanie i podgotovka IT-analitikov* [Fundamental Mathematical Education and Training of IT Analysts] // *Obrazovatel'nye tekhnologii* – Educational Technologies. 2018., No. 1. Pp. 28–33.
4. Emelchenkov E. P., Levin N. A., Munerman V. I. *Algebraicheskij podhod k optimizaci i razrabotki i ekspluatacii sistem upravleniya bazami dannyh* [Algebraic Approach to Optimizing the Development and Operation of Database Management Systems, Systems and Means of Information] // *Sistemy i sredstva informatiki : sb. st.* – Computer science systems and tools: collection of articles. M., 2009. Vol. 19. No. 2. Pp. 114–137.
5. Ishmukhametov Sh. T. *Metody faktorizacii natural'nyh chisel : ucheb. posobie* [Methods of Factoring Natural Numbers : a tutorial]. Kazan, Kazan Federal University. 2011. 190 p.
6. *Mnogoosnovnye algebry kak integriruyushchij konstrukt pri kompleksnom izlozenii uchebnyh kursov v oblasti estestvennyh nauk i kognitivnyh metodov* [Multigroup algebras as an integrating construct in the complex presentation of training courses in the field of natural sciences and cognitive methods] / I. V. Stepura // *Nauka i obrazovanie: opyt, problemy, perspektivy razvitiya : sb. st. po materialam mezhdunar. nauch.-prakt. Konf* – Science and Education: Experience, Problems, and Prospects of Development: Collection of Articles based on the materials of the International Scientific and Practical Conference. Krasnoyarsk, 2021. Vol. 2. Part 2. Pp. 151–156.
7. Nesterenko Yu. V. *Teoriya chisel : ucheb. dlya stud. vyssh. ucheb. zaved.* [Number Theory : textbook for university students]. M., Academy. 2008. 272 p.
8. *Prakticheskij kurs klassicheskogo mashinnogo obucheniya s ispol'zovaniem modelej matematicheskogo programmirovaniya : ucheb.-metod. posobie* [Practical course of classical machine learning using mathematical programming models : educational and methodological guide] / P. F. Chernavin, N. P. Chernavin, F. P. Chernavin. Yekaterinburg, Ural University Publ. 2023. 124 p.
9. Testov V. A. *Fundamental'nost' obrazovaniya: sovremennye podhody* [Fundamentality of Education: Modern Approaches] // *Pedagogika* – Pedagogy. 2006. No. 4. Pp. 3–9.
10. *Kurs matematiki* [Mathematics course]. Available at: <https://e.vyatsu.ru/course/view.php?id=5504>.

Поступила в редакцию: 18.06.2025

Принята к публикации: 02.07.2025