

ПРЕПОДАВАНИЕ АЛГЕБРЫ СТУДЕНТАМ ТЕХНИЧЕСКИХ ВУЗОВ

Зельвенский Игорь Григорьевич

Аннотация

В настоящее время алгебраические дисциплины занимают всё большее место в учебных планах технических вузов. Описана структура курса алгебры, читаемого на втором курсе факультета компьютерных технологий и информатики СПбГЭТУ (ЛЭТИ) и посвященного рассмотрению алгебраических систем — групп, колец, полей — и их связям с прикладными задачами и смежными разделами математики.

Ключевые слова: *прикладная алгебра в техническом вузе, подготовка специалистов по системам связи, компьютерной безопасности и криптографии.*

На факультете компьютерных технологий и информатики ЛЭТИ алгебра читается в течение 3-х семестров, назовем соответствующие части курса: «Алгебра I», «Алгебра II» и «Алгебра III». Части I и II являются традиционными для высшего технического образования и незначительно меняются от вуза к вузу, от факультета к факультету. «Алгебра I» включает в себя следующие темы: комплексные числа и рациональные (целые и дробные) функции над полем комплексных чисел, начала линейной алгебры (матрицы и системы линейных уравнений), элементы аналитической геометрии (курсы собственно аналитической геометрии остались лишь на математических факультетах университетов и педагогических вузов). Расхождения в программах «Алгебры I» касаются, главным образом, порядка при изучении перечисленных разделов. «Алгебра II» является стандартным курсом линейной алгебры, объем которого определяется конкретным вузом, и может в своем максимальном варианте заканчиваться тензорным исчислением. Примером удачного изложения этого курса может служить книга [1], рассчитанная на обучающихся по специальности «Прикладная математика». В ЛЭТИ «Алгебра II» включает в себя также описание поверхностей 2-го порядка, опирающееся на теорию билинейных и квадратичных форм.

Алгебра в ее современном понимании приобрела черты прикладной науки во 2-й половине XX в., появление электронно-вычислительных машин позволило обрабатывать большое количество дискретной информации. Возникла настоятельная необходимость в структурировании дискретных массивов, и вскоре алгебраические идеи и методы нашли широкое применение в таких областях, как теория автоматов и вычислительных машин, передача сообщений и шифрование, языки программирования.

Наиболее выразительным примером может служить появление блоковых кодов Боза–Чоудхури–Хоквингема в 1959–60 гг., позволяющих исправлять более одной ошибки в переданных сообщениях. При использовании соответствующих кодов необходимы вычисления в полях Галуа, являющихся конечными расширениями полей классов вычетов по простому модулю.

Базовые понятия из теории групп, колец и полей («Алгебра III») стали необходимы студентам инженерных вузов, особенно для таких специальностей как «Инфокоммуникационные технологии и системы связи», «Компьютерная безопасность», «Криптография».

Необходимо также отметить, что все студенты, изучающие разделы физики и химии, тесно связанные с понятием симметрии (кристаллографию, квантовую механику и др.), в обязательном порядке знакомятся и с основами теории групп, и с теорией представления групп — активно развивающимся разделом современной алгебры [2].

Обычно вузовский учебный курс, посвященный изучению алгебраических систем, называют «Прикладной алгеброй», что объясняется, по-видимому, желанием добавить главы, посвященные приложениям — теории кодирования, криптосистемам и др. Встречаются варианты наименований со словами «современная», «общая», «универсальная» и т. п., можно даже упомянуть название-оксюморон книги Лидла и Пильца «Прикладная абстрактная алгебра» [3], переведенной в Уральском федеральном университете и интересной подробным рассмотрением полугрупп и решеток. Основными же учебными пособиями на русском языке являются замечательная книга Биркгофа и Барти «Современная прикладная алгебра» [4], вышедшая в 1976 году в переводе Ю.И. Манина, и двухтомник Глухова, Елизарова и Нечаева «Алгебра» [5], в основу которого вошли лекции, читавшиеся в Институте криптографии, связи и информатики.

Структура курса «Алгебра III», который читается на ФКТИ ЛЭТИ, отражена на блок-схеме (рис. 1).

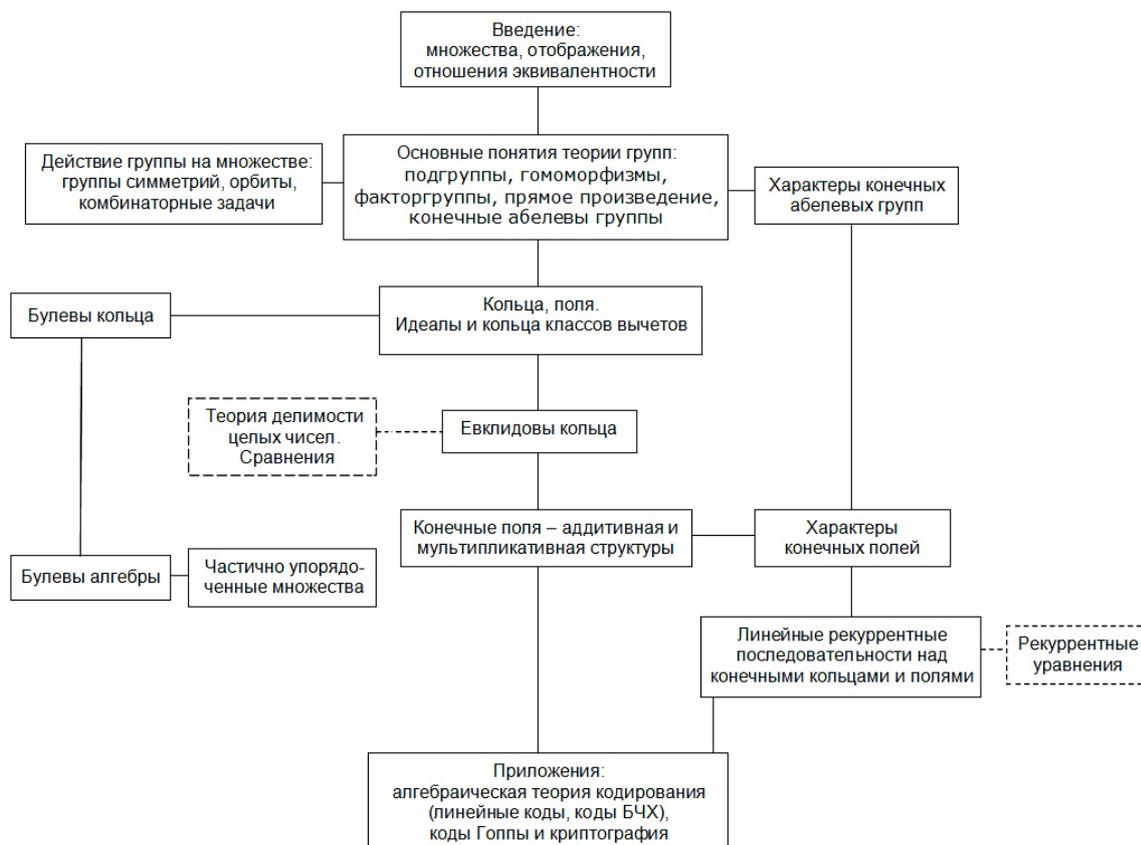


Рис. 1

Комментарии к блок-схеме:

Основная часть «Алгебры III» через элементы теории групп (главным образом, абелевых), через элементы теории коммутативных колец (главным образом, евклидовых) выводит обучающихся к построению полей Галуа, к выработке навыков вычислений в этих полях. В зависимости от целей курса и отведенных на него часов излагаются дополнительные темы:

- группы симметрий и лемма Бернсайда;
- группы характеров абелевых групп и конечных полей;
- линейные рекуррентные последовательности и их приложения к сверточным кодам;
- булевы кольца и алгебры;
- частично упорядоченные множества и решетки.

Два блока (элементарная теория чисел и рекуррентные уравнения) выделены штриховыми линиями — это темы, тесно связанные с рассматриваемым материалом и традиционно освещаемые в курсе дискретной математики, при необходимости их можно было бы излагать и в курсе алгебры.

Список литературы

1. Шикин Е.В. Линейные пространства и отображения. М.: Изд-во МГУ, 1987.
2. Эллиот Дж., Добер П. Симметрия в физике. Т. I-II. М.: Мир, 1983.
3. Лидл Р., Пильц Г. Прикладная абстрактная алгебра. Екатеринбург: Изд-во УрГУ, 1996. [Перевод 1-го английского издания 1984 г., 2-е издание, исправленное и расширенное, вышло в 1998 г.]
4. Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976. [1-е английское издание вышло в 1970 г. В Санкт-Петербурге русский перевод переиздали в 2005 г. в издательстве «Лань».]
5. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра. Т. I-II. М.: Гелиос АРВ, 2003.

TEACHING ALGEBRA TO STUDENTS OF TECHNICAL COLLEGES

Zelvensky I. G.

Abstract

Today algebraic academic disciplines take an important place in the syllabus of higher technical school. The report describes the structure of an algebra course taught at the LETI School of Computer Science and Technology. This course is devoted to the studying of algebraic systems such as groups, rings and fields and their connections both with applied problems and with adjacent areas of mathematics.

Keywords: *applied algebra in higher technical education, teaching of the communication systems students, computer security, cryptography.*



Наши авторы, 2015.

Our authors, 2015.

Зельвенский Игорь Григорьевич,
кандидат физико-математических наук,
доцент, доцент кафедры высшей
математики №2 СПбГЭТУ «ЛЭТИ»,
i.zelvensky@gmail.com