Лекции курса «Алгебра», лекторы И. В. Аржанцев и Р. С. Авдеев
ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2014/2015 учебный год

Лекция 10

Конечные поля. Простое подполе и порядок конечного поля. Автоморфизм Фробениуса. Теорема существования и единственности для конечных полей. Поле из четырех элементов. Цикличность мультипликативной группы. Неприводимые многочлены над конечным полем. Подполя конечного поля.

В этой лекции будем использовать следующее обозначение: $K^\times = K \setminus \{0\}$ — мультипликативная группа поля K.

Пусть K — конечное поле. Тогда его характеристика отлична от нуля и потому равна некоторому простому числу p. Значит, K содержит поле $\mathbb{Z}_p$ в качестве простого подполя.

Теорема 1. *Число элементов конечного поля равно p^n для некоторого простого p и натурального n.*

Доказательство. Пусть K — конечное поле характеристики p, и пусть размерность K над простым подполем $\mathbb{Z}_p$ равна n. Выберем в K базис $e_1, \ldots, e_n$ над $\mathbb{Z}_p$. Тогда каждый элемент из K однозначно представляется в виде $\alpha_1 e_1 + \ldots + \alpha_n e_n$, где $\alpha_1, \ldots, \alpha_n$ пробегают $\mathbb{Z}_p$. Следовательно, в K ровно p^n элементов. □

Пусть K — произвольное поле характеристики $p > 0$. Рассмотрим отображение
$$\varphi\colon K \to K, \quad a \mapsto a^p.$$
Покажем, что φ — гомоморфизм. Для любых $a, b \in K$ по формуле бинома Ньютона имеем
$$(a+b)^p = a^p + C_p^1 a^{p-1} b + C_p^2 a^{p-2} b^2 + \ldots + C_p^{p-1} a b^{p-1} + b^p.$$
Так как p — простое число, то все биномиальные коэффициенты C_p^i при $1 \leqslant i \leqslant p-1$ делятся на p. Это значит, что в нашем поле характеристики p все эти коэффициенты обнуляются, в результате чего получаем $(a+b)^p = a^p + b^p$. Ясно, что $(ab)^p = a^p b^p$, так что φ — гомоморфизм. Ядро любого гомоморфизма колец является идеалом, поэтому $\operatorname{Ker}\varphi$ — идеал в K. Но в поле нет собственных идеалов, поэтому $\operatorname{Ker}\varphi = \{0\}$, откуда φ инъективен.

Если поле K конечно, то инъективное отображение из K в K автоматически биективно. В этой ситуации φ называется *автоморфизмом Фробениуса* поля K.

Замечание 1. Пусть K — произвольное поле и ψ — произвольный автоморфизм (т. е. изоморфизм на себя) поля K. Легко видеть, что множество неподвижных точек $K^\psi = \{a \in K \mid \psi(a) = a\}$ является подполем в K.

Прежде чем перейти к следующей теореме, обсудим понятие формальной производной многочлена. Пусть $K[x]$ — кольцо многочленов над произвольным полем K. Формальной производной называется отображение $K[x] \to K[x]$, которое каждому многочлену $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ сопоставляет многочлен $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + a_1$. Из определения следует, что это отображение линейно. Легко проверить, что для любых $f, g \in K[x]$ справедливо привычное нам равенство $(fg)' = f'g + fg'$ (в силу дистрибутивности умножения проверка этого равенства сводится к случаю, когда f, g — одночлены). В частности, $(f(x)^m)' = m f(x)^{m-1}$ для любых $f(x) \in K[x]$ и $m \in \mathbb{N}$.

Теорема 2. *Для всякого простого числа p и натурального числа n существует единственное* (*с точностью до изоморфизма*) *поле из p^n элементов.*

Доказательство. Положим $q = p^n$ для краткости.

Единственность. Пусть поле K содержит q элементов. Тогда мультипликативная группа $K^\times$ имеет порядок $q-1$. По следствию 3 из теоремы Лагранжа мы имеем $a^{q-1} = 1$ для всех $a \in K \setminus \{0\}$, откуда $a^q - a = 0$ для всех $a \in K$. Это значит, что все элементы поля K являются корнями многочлена $x^q - x \in \mathbb{Z}_p[x]$. Отсюда следует, что K является полем разложения многочлена $x^q - x$ над $\mathbb{Z}_p$. Из теоремы о полях разложения, формулировавшейся на прошлой лекции, следует, что поле K единственно с точностью до изоморфизма.

Существование. Пусть K — поле разложения многочлена $f(x) = x^q - x \in \mathbb{Z}_p[x]$. Тогда имеем $f'(x) = q x^{q-1} - 1 = -1$ ($q x^{q-1}$ обнуляется, так как q делится на p, а p — характеристика поля $\mathbb{Z}_p$). Покажем, что многочлен $f(x)$ не имеет кратных корней в K. Действительно, если α — корень кратности $m \geqslant 2$, то $f(x) = (x-\alpha)^m g(x)$ для некоторого многочлена $g(x) \in \mathbb{Z}_p[x]$. Но тогда $f'(x) = m(x-\alpha)^{m-1} g(x) + (x-\alpha)^m g'(x)$, откуда видно, что $f'(x)$ делится на $(x-\alpha)$. Но последнее невозможно, ибо $f'(x) = -1$ — многочлен нулевой степени. Итак, многочлен $f(x)$ имеет ровно q различных корней в поле K. Заметим, что эти корни — в точности неподвижные точки автоморфизма $\varphi^n = \underbrace{\varphi \circ \ldots \circ \varphi}_{n}$, где φ — автоморфизм Фробениуса.

В самом деле, для элемента $a \in K$ равенство $a^q - a = 0$ выполнено тогда и только тогда, когда $a^{p^n} = a$, т.е. $\varphi^n(a) = a$. Значит, корни многочлена $x^q - x$ образуют подполе в K, которое по определению поля разложения совпадает с K. Следовательно, в поле K ровно q элементов. □

Конечные поля еще называют *полями Галуа*. Поле из q элементов обозначают $\mathbb{F}_q$. Например, $\mathbb{F}_p \cong \mathbb{Z}_p$.

Пример 1. Построим явно поле из четырёх элементов. Многочлен $x^2 + x + 1$ неприводим над $\mathbb{Z}_2$. Значит, факторкольцо $\mathbb{Z}_2[x]/(x^2 + x + 1)$ является полем и его элементы — это классы $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}$ (запись $\overline{a}$ означает класс элемента a в факторкольце $\mathbb{Z}_2[x]/(x^2 + x + 1)$). Например, произведение $\overline{x} \cdot \overline{x+1}$ — это класс элемента $x^2 + x$, который равен $\overline{1}$.

Предложение 1. *Мультипликативная группа конечного поля $\mathbb{F}_q$ является циклической.*

Доказательство. Заметим, что $\mathbb{F}_q^{\times}$ — конечная абелева группа, и обозначим через m её экспоненту (см. конец лекции 4). Предположим, что группа $\mathbb{F}_q^{\times}$ не является циклической. Тогда $m < q - 1$ по следствию 2 лекции 4. По определению экспоненты это значит, что $a^m = 1$ для всех $a \in \mathbb{F}_q^{\times}$. Но тогда многочлен $x^m - 1$ имеет в поле $\mathbb{F}_q$ больше корней, чем его степень, — противоречие. □

Теорема 3. *Конечное поле $\mathbb{F}_q$, где $q = p^n$, можно реализовать в виде $\mathbb{Z}_p[x]/(h(x))$, где $h(x)$ — неприводимый многочлен степени n над $\mathbb{Z}_p$. В частности, для всякого $n \in \mathbb{N}$ в кольце $\mathbb{Z}_p[x]$ есть неприводимый многочлен степени n.*

Доказательство. Пусть α — порождающий элемент группы $\mathbb{F}_q^{\times}$. Тогда минимальное подполе $\mathbb{Z}_p(\alpha)$ поля $\mathbb{F}_q$, содержащее α, совпадает с $\mathbb{F}_q$. Значит, поле $\mathbb{F}_q$ изоморфно полю $\mathbb{Z}_p[x]/(h(x))$, где $h(x)$ — минимальный многочлен элемента α над $\mathbb{Z}_p$. Из результатов прошлой лекции следует, что многочлен $h(x)$ неприводим. Поскольку степень расширения $[\mathbb{F}_q : \mathbb{Z}_p]$ равна n, этот многочлен имеет степень n. □

Теорема 4. *Всякое подполе поля $\mathbb{F}_q$, где $q = p^n$, изоморфно $\mathbb{F}_{p^m}$, где m — делитель числа n. Обратно, для каждого делителя m числа n в поле $\mathbb{F}_q$ существует ровно одно подполе из p^m элементов.*

Доказательство. Пусть F — подполе поля $\mathbb{F}_q$. По определению простого подполя имеем $F \supset \mathbb{Z}_p$, откуда $\operatorname{char} F = p$. Тогда теорема 1 нам сообщает, что $|F| = p^m$ для некоторого $m \in \mathbb{N}$. По теореме 2 имеем $F \cong \mathbb{F}_{p^m}$. Обозначим через s степень (конечного) расширения $F \subset \mathbb{F}_q$. Рассуждая так же, как в доказательстве теоремы 1, мы получим $p^n = (p^m)^s$, откуда $p^n = p^{ms}$ и m делит n.

Пусть теперь m — делитель числа n, т.е. $n = ms$ для некоторого $s \in \mathbb{N}$. Рассмотрим многочлены $f(x) = x^{p^n} - x$ и $g(x) = x^{p^m} - x$ над $\mathbb{Z}_p$. Заметим, что для элемента $a \in \mathbb{F}_q$ равенства $a^{p^m} = a$ следует

$$a^{p^n} = a^{p^{ms}} = a^{(p^m)^s} = (\ldots((a^{p^m})^{p^m})^{p^m} \ldots)^{p^m} \text{ (s раз возвели в степень p^m)} = a.$$

Поэтому каждый корень многочлена $g(x)$ является и корнем многочлена $f(x)$. Отсюда поле разложения многочлена $f(x)$ лежит в поле разложения многочлена $g(x)$. Значит, $\mathbb{F}_{p^m}$ содержится в $\mathbb{F}_{p^n}$.

Наконец, все элементы подполя из p^m элементов неподвижны при автоморфизме $\psi = \underbrace{\varphi \circ \ldots \circ \varphi}_{m} \colon x \mapsto x^{p^m}$ (φ — автоморфизм Фробениуса). Поскольку число корней многочлена $x^{p^m} - x$ в поле $\mathbb{F}_q$ не превосходит p^m, множество элементов данного подполя совпадает с множеством неподвижных точек автоморфизма ψ. Значит, такое подполе единственно. □

Список литературы

[1] Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 9, § 5)
[2] А. И. Кострикин. Введение в алгебру. Основные структуры алгебры. М.: Наука. Физматлит, 2000 (глава 5, § 2)
[3] Сборник задач по алгебре под редакцией А. И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 14, § 68)
[4] Р. Лидл и Г. Нидеррайтер. Конечные поля (2 тома). М.: Мир, 1988 (главы 2–3)