Алгебра, первый семестр

Е. Ю. Смирнов

Аннотация. Записки лекций по алгебре для первого курса факультета математики ВШЭ, осень 2015/16 учебного года

1. Первая лекция, 1 сентября 2015 г.

1.1. **Поля.**

Определение 1.1. Множество $\mathbb{K}$ называется *полем*, если на нём заданы две бинарные операции — *сложение* и *умножение*, т.е. отображения $+\colon \mathbb{K}\times\mathbb{K}\to\mathbb{K}$ и $\cdot\colon \mathbb{K}\times\mathbb{K}\to\mathbb{K}$, удовлетворяющие следующим аксиомам:

- **(A1):** $a+b=b+a$ для любых $a,b\in\mathbb{K}$ (коммутативность сложения);
- **(A2):** $(a+b)+c=a+(b+c)$ для любых $a,b,c\in\mathbb{K}$ (ассоциативность сложения);
- **(A3):** существует такой элемент $0\in\mathbb{K}$, называемый *нулём*, для которого $a+0=a$ для любого $a\in\mathbb{K}$ (существование нуля);
- **(A4):** для любого $a\in\mathbb{K}$ найдётся такой элемент $-a\in\mathbb{K}$, для которого $a+(-a)=0$ (существование противоположного элемента);
- **(M1):** $a\cdot b=b\cdot a$ для любых $a,b\in\mathbb{K}$ (коммутативность умножения);
- **(M2):** $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ для любых $a,b,c\in\mathbb{K}$ (ассоциативность умножения);
- **(M3):** существует такой элемент $1\in\mathbb{K}$, называемый *единицей* и отличный от 0, для которого $a\cdot 1=a$ для любого $a\in\mathbb{K}$ (существование единицы);
- **(M4):** для любого $a\in\mathbb{K}$, не равного 0, найдётся такой элемент $a^{-1}\in\mathbb{K}$, для которого $a\cdot(a^{-1})=1$ (существование обратного элемента);
- **(D):** $(a+b)\cdot c=a\cdot c+b\cdot c$ для любых $a,b,c\in\mathbb{K}$.

Вы используете эти записки на свой страх и риск. Никто не гарантирует, что их текст полностью соответствует содержанию лекций. Тем более не гарантируется отсутствие в этом тексте ошибок. Впрочем, о найденных ошибках лучше сообщать автору.

Неформально говоря, поле — это множество, элементы которого можно складывать, умножать, вычитать и делить, и для этих операций выполняются все привычные нам свойства.

Пример 1.2. Множества *рациональных чисел* $\mathbb{Q}$ и *действительных*[1] *чисел* $\mathbb{R}$ являются полями (для $\mathbb{Q}$ проверьте все аксиомы самостоятельно, для $\mathbb{R}$ это будет частью определения).

Упражнение 1.3. Рассмотрим множество $\mathbb{F}_2 = \{0, 1\}$ и определим на нем операции сложения и умножения так: $0 + 1 = 1 \cdot 1 = 0$, а все остальные суммы и произведения равны 0. Докажите, что полученное множество с такими операциями является полем.

Упражнение 1.4. Постройте поле из: **а)** 3; **б)** 5; **в*)** 4 элементов.

Выведем из аксиом поля несколько следствий.

Предложение 1.5. *Во всяком поле* $\mathbb{K}$

(1) *нуль (т.е. элемент, определенный аксиомой* (A3)*) единственен;*
(2) *единица единственна;*
(3) *для любого элемента* $a \in \mathbb{K}$ *противоположный к нему элемент* $(-a)$ *определен однозначно;*
(4) *для любого ненулевого элемента* $a \in \mathbb{K}$ *обратный к нему элемент* a^{-1} *определен однозначно;*
(5) $0 \cdot a = 0$ *для любого* $a \in \mathbb{K}$*;*
(6) $(-1) \cdot a = -a$ *для любого* $a \in \mathbb{K}$*;*
(7) *если* $a \cdot b = 0$*, то либо* $a = 0$*, либо* $b = 0$*.*

Доказательство. 1. Пусть в поле существует два нуля: 0_1 и 0_2, удовлетворяющих аксиоме (A3). Рассмотрим их сумму $0_1 + 0_2$. Согласно аксиоме (A3), имеем $0_1 + 0_2 = 0_1$ (т.к. 0_2 — нуль). Но, с другой стороны, $0_1 + 0_2 = 0_2 + 0_1 = 0_2$ (в последнем переходе мы использовали тот факт, что 0_1 — тоже нуль). Значит, $0_1 = 0_2$.

2. Доказывается аналогично 1.

3. Пусть имеются два элемента $-a_1$ и $-a_2$, каждый из которых даёт нуль в сумме с a. Тогда $-a_1 = -a_1 + 0 = -a_1 + (a + (-a_2)) = (-a_1 + a) + (-a_2) = 0 + (-a_2) = -a_2$.

4. Доказывается аналогично 3.

5. Пусть $0 \cdot a = b$. Тогда $b + a = 0 \cdot a + a = 0 \cdot a + 1 \cdot a = (0+1) \cdot a = 1 \cdot a = a$. Значит, a и $b + a$ равны (иначе говоря, это один и тот же элемент поля). Поэтому равны элементы $a + (-a)$ и $b + a + (-a)$. Значит, $0 = b$, что и требовалось.

6. Нужно проверить, что $(-1) \cdot a + a = 0$. Действительно, $(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = ((-1) + 1) \cdot a = 0 \cdot a = 0$ (в предпоследнем

[1]Мы считаем, что у читателя есть представление о действительных числах из школьного курса; строгая конструкция поля действительных чисел будет приведена в курсе математического анализа.

равенстве мы воспользовались только что доказанным свойством 5).

7. Предположим, что $a \neq 0$. Тогда к a существует обратный элемент a^{-1}. Тогда $b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$. Значит, $b = 0$. □

1.2. **Пример расширения полей:** $\mathbb{Q}[\sqrt{2}]$**.** Рассмотрим поле $\mathbb{Q}$. Уравнение $x^2 = 2$ в нём неразрешимо: действительно, если бы существовало такое рациональное число $x = p/q$, что $x^2 = 2$, то выполнялось бы равенство $p^2 = 2q^2$, что противоречит основной теореме арифметики (простой множитель 2 входит в нечетной степени в правую часть равенства и в чётной — в левую). Добавим к полю $\mathbb{Q}$ элемент $\sqrt{2}$ (то есть элемент, равный в квадрате 2), «принудительно»: рассмотрим множество

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},$$

операции на котором заданы по правилу

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2};$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}.$$

(можно просто рассматривать запись $a + b\sqrt{2}$ как пару рациональных чисел (a, b); на множестве таких пар сложение и умножение вводится указанным выше образом).

Такие числа образуют поле; легко проверить, что в нём действительно выполняются все необходимые аксиомы. Единственная аксиома, проверка которой нетривиальна — это существование обратного. Проделаем эту проверку:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} =$$
$$= \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

(Контрольный вопрос: почему знаменатель всегда отличен от нуля?)

Упражнение 1.6. Постройте поле $\mathbb{Q}[\sqrt[3]{2}]$, и проверьте аксиому существования обратного элемента.

1.3. **Комплексные числа.** Рассмотрим поле $\mathbb{R}$. Как известно, в нём нет решения уравнения $x^2 = -1$. Попробуем точно так же добавить его к $\mathbb{R}$ «принудительно». Обозначим через i элемент, квадрат которого будем считать равным -1, и рассмотрим множество

$$\mathbb{C} = \mathbb{R}[i] = \{a + bi \mid a, b \in \mathbb{R}\}.$$

Сложение в нем определим покомпонентно, умножение — исходя из равенства $i^2 = -1$:

$$(a+bi)+(c+di) = (a+c)+(b+d)i; \qquad (a+bi)(c+di) = (ac-bd)+(bc+ad)i.$$

Аксиомы поля проверяются без труда. Проверим, что к каждому ненулевому элементу из $\mathbb{C}$ будет существовать обратный:

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i.$$

Упражнение 1.7. Проверьте, что квадратное уравнение x^2+px+q с коэффициентами из $\mathbb{C}$ имеет в $\mathbb{C}$ два решения (возможно, совпадающих), которые находятся по известной формуле $x = \frac{-p\pm\sqrt{p^2-4q}}{2}$.

Пример 1.8. Приведенная проверка существования обратного не является тавтологией. Так, если добавить к $\mathbb{R}$ вместо i элемент j, квадрат которого равняется $j^2 = 1$, то полученное множество $\mathbb{R}[j]$ уже не будет полем. Например, элемент $1+j$ необратим. Действительно, если $(1+j)^{-1} = a+bj$, то $(1+j)(a+bj) = (a+b)+(a+b)j$, что не может равняться 1.

Упражнение 1.9. Опишите все обратимые элементы в $\mathbb{R}[j]$.

E-mail address: `esmirnov@hse.ru`