Аксиомы арифметических действий

Определение 1. *Полем* (англ. *field*) называется множество F с операциями сложения "+" и умножения "·", удовлетворяющие следующим аксиомам.

1) Ассоциативность сложения $a + (b + c) = (a + b) + c$.
2) Существование *нуля* $0 \in F$, $a + 0 = 0 + a = 0$.
3) Вычитание. Для каждого a существует *противоположный элемент* $-a \in F$, такой что $a + (-a) = (-a) + a = 0$.
4) Коммутативность сложения $a + b = b + a$.
5) Билинейность умножения (дистрибутивность) $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$.
6) Ассоциативность умножения $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
7) Существование *единицы* $1 \in F$, $a \cdot 1 = 1 \cdot a = 1$.
8) Деление. Для каждого $a \neq 0$ существует *обратный элемент* $a^{-1} \in F$, такой что $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
9) Коммутативность умножения $a \cdot b = b \cdot a$.

В классическое определение часто входит предположение $1 \neq 0$. Случай $1 = 0$ соответствует полю из одного элемента, мы будем в дальнейшем называть его *нулевым.*

Упражнение 1 *Докажите из аксиом, что обратный и противоположный элементы единственны,* $0 \cdot a = 0$, $(-1) \cdot a = -a$.

Определение 2. Название множеств с операциями, для которых выполнена часть аксиом.

Русское название	Английское название	Аксиомы
кольцо	ring	1,2,3,4,5,6
кольцо с единицей	unitary ring	1,2,3,4,5,6,7
коммутативное кольцо	commutative ring	1,2,3,4,5,6,9
кольцо с делением, тело	division ring corps (фр.)	1,2,3,4,5,6,7,8
полукольцо	semi-ring	1,5,6

Название множеств с одной операцией (+) для которых выполнена часть аксиом.

Русское название	Английское название	Аксиомы
группа	group	1,2,3
коммутативная (абелева) группа	commutative (abelian) group	1,2,3,4
полугруппа	semi-group	1

Пример. Вещественные числа $\mathbb{R}$, комплексные числа $\mathbb{C}$, рациональные числа $\mathbb{Q}$ — поля.
Целые числа $\mathbb{Z}$, остатки $\mathbb{Z}/n\mathbb{Z}$ — коммутативные кольца с единицей (а $\mathbb{Z}/p\mathbb{Z}$ при простом p — поле).
Многочлены $K[x]$, где K — коммутативное кольцо — коммутативное кольцо.
Натуральные числа $\mathbb{N}$ — полукольцо.
Тропическое полукольцо — целые чсила со сложением $a \oplus b = \max(a, b)$, $a \otimes b = a + b$.
Элементы кольца K образуют коммутативную группу K^+ по сложению.
Ненулевые элементы тела/поля F образуют группу/коммутативную группу F^* по умножению.
Ряд примеров будет разбираться на семинарах.

Определение 3. *Отображение* полей/колец/групп (field/ring/group *homomorphism*) $\phi : F_1 \to F_2$ — отображение множеств, такое что $\phi(a + b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$ (второе — для колец и полей).

Упражнение 2 *Докажите, что для отображения полей выполнено* $\phi(0) = 0$, *а* $\phi(1) = 1$ *или* 0. *Как устроено отображение во втором случае?*

Определение 4. *Вложение/наложение/изоморфизм* полей/колец/групп — отображение полей/колец/групп, являющееся таковым на уровне множеств.

Предложение 1 *Всякое ненулевое отображение полей — вложение.*

Доказательство: Пусть ϕ — отображение полей. Если оно не вложение, найдутся $a \neq b$, такие что $\phi(a) = \phi(b)$. Тогда $\phi(a - b) = 0$, а значит

$$\phi(1) = \phi((a - b)^{-1}(a - b)) = \phi((a - b)^{-1})\phi(a - b) = 0,$$

откуда для всякого x $\phi(x) = \phi(x \cdot 1) = \phi(x)\phi(1) = 0$.

Определение 5. *Подполе/подкольцо/подгруппа (subring/subfield/subgroup)* $F_1 \subset F_2$ — подмножество, замкнутое относительно операций.

Определение 6. Поле называется *простым*, если оно не содержит нетривиальных (отличных от нулевого и самого поля) подполей.

Предложение 2 *Всякое ненулевое поле содержит ненулевое простое подполе.*

Доказательство: Требуемым является пересечение ненулевых подполей этого поля. Оно отлично от нуля, так как содержит единицу.

Предложение 3 *Поля* $\mathbb{Q}$ *и* $\mathbb{Z}/p\mathbb{Z}$ *являются простыми.*

Доказательство: Всякий элемент может быть выражен используя единицу и арифметические операции.

Литература к курсу

1) Э.Б.Винберг, Курс алгебры.
2) С.Ленг, Алгебра
3) Б.Л.Ван дер Варден, Алгебра
4) И.М.Гельфанд, Лекции по линейной алгебре
5) А.И.Кострикин, Ю.И.Манин, Линейная алгебра и геометрия
6) Wiki (лучше английская) и другие неизвестные источники — с осторожностью.