Введение в теорию полей

Листок 1

Поля: определения, примеры, основные свойства.

Определение 1. Множество G с операцией $*$ называется *группой*, если выполняются следующие свойства:

1) $\forall x, y, z \in G\ (x * y) * z = x * (y * z)$ (ассоциативность);

2) $\exists e \in G \forall x \in G\ e * x = x * e = x$ (элемент e называется *единицей* группы G);

3) $\forall x \in G \exists y \in G\ x * y = y * x = e$ (элемент y называется *обратным* для x и обозначается через x^{-1}).

Если в группе G дополнительно выполняется свойство *коммутативности*

$$\forall x, y \in G\ x * y = y * x,$$

то G называется *абелевой группой*.

Знак $*$ часто опускается, результат применения операции $*$ к элементам x и y записывается через xy.

В случае абелевой группы операцию в группе чаще всего называют *сложением* (обозначение: $+$), такую запись называют *аддитивной*.

Задача 1. Приведите примеры абелевых и неабелевых групп.

Определение 2. Подмножество H группы G называется *подгруппой*, если

$$\forall x, y \in H\ xy \in H \wedge x^{-1} \in H.$$

Определение 3. Пусть H — подгруппа группы G, $g \in G$. Тогда *правым* (*левым*) *смежным классом элемента g по подгруппе H* называется множество

$$gH = \{gh \mid h \in H\} \quad (Hg = \{hg \mid h \in H\}).$$

Задача 2. Пусть G — группа, H — ее подгруппа, $g_1, g_2 \in G$. Тогда либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \emptyset$.

Задача 3 (теорема Лагранжа). Если G — конечная группа, H — ее подгруппа, то количество правых (левых) смежных классов G по H равно $G : H$ (это количество называется *индексом* подгруппы H в группе G). Как следствие, порядок подгруппы всегда делит порядок группы.

Определение 4. *Порядком* элемента g группы G называется минимальное натуральное число $n > 0$ такое, что $g^n = e$. Если такого числа не существуют, то говорят, что порядок элемента g бесконечен.

Задача 4. В конечной группе порядок любого элемента делит порядок группы.

Определение 5. Множество $\mathbb{F}$ с двумя бинарными операциями $+$ (сложение) и $\cdot$ (умножение) называется *полем*, если относительно сложения множество $(\mathbb{F}, +)$ является абелевой группой (нейтральный элемент в этой группе обозначается через 0 и называется нулем), относительно умножения множество $\mathbb{F}^* = (\mathbb{F} \setminus 0, \cdot)$ является абелевой группой (нейтральный элемент в $\mathbb{F}^*$ обозначается через 1), а также выполняется аксиома *дистрибутивности*

$$\forall x, y, z \in \mathbb{F}\ x \cdot (y + z) = xy + xz.$$

Задача 5. Выведите из аксиом поля следующее свойство:

$$\forall x \in \mathbb{F}\ 0 \cdot x = 0.$$

Задача 6. Выведите из аксиом поля следующее свойство:

$$\forall x, y \in \mathbb{F}\ xy = 0 \Rightarrow x = 0 \vee y = 0.$$

Задача 7. Какие из перечисленных ниже множеств с операциями являются полями:

а) множество $\mathbb{Z}$ (целые числа с операциями сложения и умножения);

б) множество $n\mathbb{Z}$, $n > 1$ (все целые числа, кратные n, с операциями сложения и умножения) ;

в) множества $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (рациональные, действительные и комплексные числа, соответственно, с операциями сложения и умножения

г) множество рациональных чисел, в несократимой записи которых знаменатели делят фиксированное число $n \in \mathbb{N}$;

д) множество рациональных чисел, в несократимой записи которых знаменатели не делятся на фиксированное простое число p;

е) множество рациональных чисел, в несократимой записи которых знаменатели являются степенями фиксированного простого числа p;

ж) множество вещественных чисел вида $x + y\sqrt{2}$, где $x, y \in \mathbb{Q}$;

з) множество вещественных чисел вида $x + y\sqrt[3]{2}$, где $x, y \in \mathbb{Q}$;

и) множество вещественных чисел вида $x + y\sqrt[3]{2} + z\sqrt[3]{4}$, где $x, y, z \in \mathbb{Q}$;

к) множество комплексных чисел вида $x + yi$, где $x, y \in \mathbb{Z}$;

л) множество комплексных чисел вида $x + yi$, где $x, y \in \mathbb{Q}$?

Задача 8. Докажите, что множество остатков от деления целых чисел на фиксированное натуральное число n с операциями сложения и умножения остатков по модулю n (обозначение: $\mathbb{Z}_n$) является полем тогда и только тогда, когда число n — простое.

Определение 6. В поле $\mathbb{F}$ наименьшее натуральное число n, для которого $\underbrace{1 + \cdots + 1}_{n} = 0$, называется *характеристикой поля* $\mathbb{F}$ (обозначение: $\operatorname{char}\mathbb{F}$). Если такого натурального n не существует, то говорят, что характеристика поля $\mathbb{F}$ равна 0.

Задача 9. Докажите, что если у поля характеристика не равна нулю, то она является простым числом.

Определение 7. Подмножество $\mathbb{L} \subseteq \mathbb{F}$ поля $\mathbb{F}$ называется его *подполем*, если оно является полем относительно тех же операций сложения и умножения, что и $\mathbb{F}$.

Задача 10. Докажите, что если поле $\mathbb{F}$ имеет характеристику 0, то в него естественно вложено подполе $\mathbb{Q}$ рациональных чисел. Если поле $\mathbb{F}$ имеет характеристику p, то в него естественно вложено подполе $\mathbb{Z}_p$.

Определение 8. Отображение

$$\varphi : \mathbb{F}_1 \to \mathbb{F}_2$$

из поля $\mathbb{F}_1$ в поле $\mathbb{F}_2$ называется *гомоморфизмом* полей, если

1) $\forall x, y \in \mathbb{F}_1 \ \varphi(x + y) = \varphi(x) + \varphi(y)$;

2) $\forall x, y \in \mathbb{F}_1 \ \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

Взаимно однозначное отображение, являющееся гомоморфизмом, называется *изоморфизмом* полей.

Задача 11. Докажите, что

а) композиция изоморфизмов — изоморфизм;

б) отображение, обратное к изоморфизму, является изоморфизмом.

Задача 12. Докажите, что гомоморфизм между двумя полями всегда либо является нулевым (все элементы первого поля отображаются в ноль второго поля), либо инъективен (является вложением).

Определение 9. Два поля называются *изоморфными*, если между ними существует изоморфизм.

Задача 13. Найдите все, с точностью до изоморфизма, поля из двух, трех, четырех элементов.

Задача 14. Существует ли поле из 6 элементов?

Задача 15. Докажите, что конечное поле может содержать только p^n элементов, где p — простое, n — натуральное число.

Задача 16. Существует ли бесконечное поле положительной характеристики?

Задача 17. Докажите, что поле из p^2 элементов, где p — простое число, имеет единственное собственное подполе.

Задача 18. Существует ли поле, строго содержащее поле комплексных чисел?

Задача 19 *. Может ли поле быть изоморфно своему собственному подполю?

Определение 10. *Автоморфизмом* поля $\mathbb{F}$ называется его изоморфизм на себя.

Задача 20. Найдите все автоморфизмы полей а) $\mathbb{Z}_p$, б) $\mathbb{Q}$, в) $\mathbb{Q}[\sqrt{2}]$, г) $\mathbb{R}$.

Задача 21. Докажите, что если поле $\mathbb{F}$ характеристики p конечно, то отображение $x \mapsto x^p$ является его автоморфизмом.

Задача 22. Какие из уравнений а) $x^2 = 5$; б) $x^7 = 7$; в) $x^3 = a$ имеют решение в поле $\mathbb{Z}_{11}$?