Теорема Лагранжа

Определение. Пусть M — некоторое множество. Если каждой упорядоченной паре элементов a и b множества M поставлен в соответствие определённый элемент $a * b$ этого же множества, то говорят, что на множестве M задана *бинарная операция* $*$.

1. Является ли бинарной операция

(a) скалярное произведение векторов на множестве всех векторов плоскости;

(b) расстояние между двумя точками на множестве всех точек плоскости;

(c) сложение на $\mathbb{N}$;

(d) вычитание на $\mathbb{N}$;

(e) вычитание на $\mathbb{Z}$;

(f) умножения на множестве a, b, c, где a, b, c — корни уравнения $x^3 - 1 = 0$?

Определение. *Группой* называется множество G с заданной на нем бинарной операцией $*$ если выполняются следующие условия:

1. ассоциативность: $(a * b) * c = a * (b * c)$ для любых элементов a, b, c из G;
2. в G имеется такой элемент e, что $a * e = e * a = a$ для любого a из G (этот элемент e называется *единичным*);
3. у каждого элемента a в G есть такой элемент a^{-1}, что $a * a^{-1} = a^{-1} * a = e$ (этот элемент называется *обратным* к элементу a).

2. Являются ли группами

(a) $\mathbb{N}$ с операцией сложения; **(b)** $\mathbb{N}$ с операцией умножения;

(c) $\mathbb{Z}$ с операцией сложения; **(d)** $\mathbb{Z}$ с операцией умножения;

(e) $\mathbb{Z}_m$ с операцией сложения по модулю;

(f) $\mathbb{Z}_m/\{0\}$ с операцией умножения по модулю;

(g) множество корней n-й степени из 1 с операцией умножения.

3. Доказать, что в любой группе существует единственный единичный элемент.

4. Доказать, что для любого элемента a группы существует единственный обратный элемент a^{-1}.

5. Доказать, что

(a) $e^{-1} = e$; **(b)** $(a^{-1})^{-1} = a$.

6. Доказать, что в произвольной группе $(ab)^{-1} = b^{-1}a^{-1}$.

Определение. *Порядком* элемента a группы G называют наименьшее натуральное число n такое, что $a^n = e$. Если такого n не существует, то говорят, что a — элемент бесконечного порядка.

7. Пусть элемент a имеет порядок n. Доказать, что все элементы $e, a, a_2, \ldots, a_{n-1}$ попарно различны.

Определение. Пусть $(G, *)$ — группа, H — подмножество G. Если H само является группой с операцией $*$, то его называют *подгруппой* группы G.

8. Пусть H — подгруппа группы G. Доказать, что

(a) единичные элементы в G и H совпадают;

(b) если a — элемент подгруппы H, то элементы, обратные к a в G и H совпадают.

9. Докажите, что пересечение нескольких подгрупп некоторой группы G также является подгруппой.

Определение. *Порядком* группы называется число ее элементов.

Теорема Лагранжа. Порядок подгруппы является делителем порядка группы.

Определение. Множество всех элементов группы G, получаемых умножением всех элементов подгрупп H на некоторый x из группы G $\{hx | x \in H\}$, называется *правым смежным классом* по H, порожденный элементом x.

10. **(a)** Докажите, что каждый элемент группы входит в некоторый правый смежный класс по подгруппе H.

(b) Пусть элемент y входит в правый смежный класс по H, порожденный элементом x. Доказать, что правые смежные классы по H, порожденные элементами x и y, совпадают.

(c) Пусть правые смежные классы, порожденные элементами x и y, содержат общий элемент. Доказать, что эти смежные классы совпадают.

(d) Докажите, что группа G разбивается на непересекающиеся правые смежные классы по H.

(e) Докажите теорему Лагранжа.

11. Докажите, что порядок любого элемента группы является делителем порядка группы.

12. **(a) Малая теорема Ферма.** Для любых взаимно простых a и p, где p — простое:

$$a^{p-1} \equiv_p 1.$$

(b) Теорема Эйлера. Для любых взаимно простых a и m:

$$a^{\varphi(m)} \equiv_m 1.$$