Лекция 15

На прошлой лекции была доказана теорема Лагранжа.

Теорема 1 (Теорема Лагранжа). *Пусть G – конечная группа и H – ее подгруппа. Тогда*

$$|G| = |H| \cdot [G : H].$$

Сформулируем несколько следствий из нее. Начнем с очевидного следствия.

Следствие 1. *Пусть G – конечная группа и H – ее подгруппа. Тогда порядок G делится на порядок H.*

Определение 1. Группа G называется *циклической*, если существует элемент $g \in G$ такой, что G состоит из степеней элемента g с целым показателем. Говорят, что элемент g *порождает* G. Обозначается это так: $G = \langle g \rangle$.

Лемма 1. *Порядок циклической группы $\langle g \rangle$ равен порядку элемента g.*

Доказательство. Рассмотрим случай, когда $\mathrm{ord}(g) = \infty$. Тогда все элементы g^k, $k \in \mathbb{Z}$ различны. В самом деле если $g^k = g^l$ при $k > l$, то умножая это равенство на g^{-l}, получаем $g^{k-l} = e$. Это противоречит предположению $\mathrm{ord}(g) = \infty$.

Теперь рассмотрим случай $\mathrm{ord}(g) = n$. Докажем, что все элементы $e = g^0, g^1, \ldots, g^{n-1}$ различны. В самом деле, допустим, что $g^k = g^l$ при $n \geq k > l \geq 0$. Тогда, как и выше, $g^{k-l} = e$, причем $n > k - l > 0$, что противоречит $\mathrm{ord}(g) = n$. Теперь заметим, что любое целое число можно записать в виде $s = mn + r$, где $m \in \mathbb{Z}$, $0 \leq r \leq n - 1$. Тогда

$$g^s = g^{mn+r} = (g^n)^m g^r = e^m g^r = g^r.$$

Следовательно, все степени g, то есть все элементы $\langle g \rangle$ имеют вид g^r, где $0 \leq r \leq n - 1$. Так как эти элементы различны, в группе $\langle g \rangle$ ровно $n = \mathrm{ord}(g)$ элементов. □

Теперь мы можем доказать еще одно следствие из теоеремы Лагранжа.

Следствие 2. *Пусть g – элемент группы G. Тогда порядок группы G делится на порядок элемента g.*

Доказательство. Мы можем рассмотреть циклическую подгруппу $H = \langle g \rangle$, порожденную элементом g. Эта подгруппа группы G, состоящая из всех целых степеней элемента g (не утверждается, что они различны). Покажем, что это действительно подгруппа. Ясно, что это подмножество G. Это подмножество не пусто, так как $g^0 = e \in H$. Оно замкнуто относительно умножения, так как $g^k \cdot g^l = g^{k+l}$. Также подмножество H замкнуто относительно взятия обратного, так как $\left(g^k\right)^{-1} = g^{-k}$.

Итак, мы доказали, что H – подгруппа G. По следствию 1 порядок G делится на порядок H. По лемме 1, порядок H равен порядку g. В итоге получаем, что $|G|$ делится на $\mathrm{ord}(g)$. □

Непосредственно из следствия 2 следует еще одно.

Следствие 3. *Пусть g – элемент группы G. Тогда $g^{|G|} = e$.*

Доказательство. По следствию 2 выполнено $|G| = m \cdot \mathrm{ord}(g)$. Тогда

$$g^{|G|} = \left(g^{\mathrm{ord}(g)}\right)^m = e^m = e.$$

□

В качестве приложения теоремы Лагранжа докажем малую теорему Ферма.

Теорема 2 (Малая теорема Ферма). *Пусть p – простое число и пусть a – некоторое целое число, не делящееся на p. Тогда $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.*

Доказательство. Рассмотрим множество остатков $G = \{1, 2, \ldots, p-1\}$ по модулю p. Докажем, что G – группа относительно операции умножения. В самом деле, G – непустое множество. Оно замкнуто относительно умножения, так как если произведение двух чисел делится на p, то одно из них делится на p. К каждому ненулевому остатку по простому модулю есть обратный (ненулевой) остаток. Это должно быть известно из курса теории чисел. Доказывается это так: пусть m – число, не делящееся на p. Тогда НОД$(m, p) = 1$. Из алгоритма Евклида следует, что существуют целые числа u и v такие, что $um+vp=1$. Взяв остатки обоих частей по модулю p получаем $um \equiv 1 (\mathrm{mod}\ p)$. Итак, мы доказали, что G – группа. Так как $|G| = p-1$ по следствию 3 для любого ненулевого остатка $\overline{a}$ получаем

$$\overline{a}^{p-1} = 1.$$

Или в виде сравнения для целых чисел $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. □

Задача 1. Докажите аналогичным образом теорему Эйлера: пусть a – число взаимно простое с натуральным числом n, тогда $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$, где $\varphi(n)$ – это функция Эйлера, равная числу натуральных чисел взаимно простых с n меньших n.

Определение 2. Пусть R – непустое множество с двумя бинарными операциями $(x, y) \mapsto x + y$ и $(x, y) \mapsto xy$. Тогда R называется *кольцом*, если выполнены следующие аксиомы.

(1) для любых $x, y, z \in R$ выполнено $(x + y) + z = x + (y + z)$;
(2) существует $0 \in R$ такой, что $\forall x \in R$ выполнено $0 + x = x + 0 = x$;
(3) для каждого $r \in R$ существует $-r \in R$ такой, что $r + (-r) = (-r) + r = 0$;
(4) для любых $x, y \in R$ выполнено $x + y = y + x$;
(5) для любых $x, y, z \in R$ выполнено $(x + y)z = xz + yz$;
(6) для любых $x, y, z \in R$ выполнено $z(x + y) = zx + zy$.

Если из контекста не понятно, какие операции имеются в виду, то используют обозначение $(R, +, \cdot)$

- Говорят, что кольцо R *ассоциативно*, если для любых $x, y, z \in R$ выполнено $(xy)z = x(yz)$.
- Говорят, что кольцо R – это *кольцо с единицей*, если существует элемент $e \neq 0$ такой, что $\forall r \in R$ выполено $er = re = r$.
- Говорят, что ассоциативное кольцо с единицей R является *телом*, если $\forall r \neq 0$ существует r^{-1} такое, что $rr^{-1} = r^{-1}r = e$.
- Говорят, что кольцо R *коммутативно*, если для любых $x, y \in R$ выполнено $xy = yx$.

Определение 3. *Поле* – это коммутативное тело, то есть ассоциативное коммутативное кольцо с единицей, у которого каждый ненулевой элемент обратим.

Таким образом, поле – это непустое множество F с операциями сложения и умножения, в котором выполнены следующие аксиомы.

(1) для любых $x, y, z \in F$ выполнено $(x + y) + z = x + (y + z)$;
(2) существует $0 \in F$ такой, что $\forall x \in R$ выполнено $0 + x = x + 0 = x$;
(3) для каждого $r \in F$ существует $-r \in R$ такой, что $r + (-r) = (-r) + r = 0$;
(4) для любых $x, y \in F$ выполнено $x + y = y + x$;
(5) для любых $x, y, z \in F$ выполнено $(x + y)z = xz + yz$;
(6) для любых $x, y, z \in F$ выполнено $z(x + y) = zx + zy$;
(7) для любых $x, y, z \in F$ выполнено $(xy)z = x(yz)$;
(8) существует элемент $e \neq 0$ такой, что $\forall x \in F$ выполено $ex = xe = x$;
(9) для любых $x, y \in F$ выполнено $xy = yx$;
(10) $\forall x \neq 0$ из F существует x^{-1} такое, что $xx^{-1} = x^{-1}x = e$.

Объясним, почему мы требуем обратимости только от ненулевых элементов. Допустим, что в нашем кольце существует элемент 0^{-1}. Тогда

$$e = 0^{-1}0 = 0^{-1}(0 + 0) = 0^{-1}0 + 0^{-1}0 = e + e.$$

Прибавляя $-e$ к обеим частям, получаем $e = 0$. Теперь для любого элемента $r \in R$ выполнено

$$r = re = r0 = r(0 + 0) = r0 + r0 = re + re = r + r.$$

Прибавляя $-r$ к обеим частям, получаем $r = 0$. Таким образом, наше кольцо состояло бы только из одного элемента $e = 0$. Чтобы исключить этот случай, мы требуем, чтобы 0 и e были различны.

Лемма 2. *Простейшие свойства.*

- *Ноль в кольце единственный.*
- *Противоположный элемент к каждому элементу единственный.*
- *Единица в кольце, если она есть, единственная.*
- *Обратный к данному элементу в кольце с единицей, если он есть, единственный.*

- *Для любого* $x \in R$ *выполнено* $x0 = 0x = 0$. *Докажем одно из равенств:*
$$x0 = x(0+0) = x0 + x0.$$
Прибавим к каждой части $-(x0)$, *получим* $0 = x0$.
- *Пусть* R *– ассоциативное кольцо с единицей. Множество обратимых элементов* $R^{\times}$ *с операцией умножения образует группу. Докажем это. Множество* $R^{\times}$ *непусто, так как содержит единицу и замкнуто относительно умножения, так как произведение двух обратимых элементов – обратимый элемент:* $(ab)^{-1} = b^{-1}a^{-1}$. *Ассоциативность умножения следует из того, что кольцо* R *ассоциативно. Единица, как мы уже сказали, лежит в* $R^{\times}$. *Обратный элемент к каждому элементу из* $R^{\times}$ *существует и тоже попадает в* $R^{\times}$, *так как* $\left(a^{-1}\right)^{-1} = a$.

Пример 1.
- $(\mathbb{R}^3, +, [,])$ *– не ассоциативное кольцо (умножение – векторное произведение).*
- $(\mathrm{Mat}_{nn}(\mathbb{R}), +, \cdot)$, $(\mathrm{Mat}_{nn}(\mathbb{Q}), +, \cdot)$ *– не коммутативные ассоциативные кольца с единицей.*
- $(\mathbb{Z}, +, \cdot)$ *– коммутатвиное ассоциативное кольцо с единицей.*
- $(2\mathbb{Z}, +, \cdot)$ *– коммутатвиное ассоциативное кольцо.*
- $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ *– поля.*

Определение 4. Если $a, b \in R$, $a \neq 0$, $b \neq 0$ и $ab = 0$, то a называется *левым делителем нуля*, а b – *правым делителем нуля*. Совокупность левых и правых делителей нуля называется множеством *делителей нуля*.

Пример 2.
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Лемма 3. *В кольце с единицей делитель нуля не может быть обратим.*

Доказательство. Пусть $ab = 0$ и пусть, например, a – обратимый элемент. Тогда
$$0 = a^{-1}0 = a^{-1}ab = b.$$
□

Определение 5. Элемент $x \neq 0 \in R$ называется *нильпотентом* (нильпотентным элементом), если существует $n \in \mathbb{N}$ такое, что $x^n = 0$.

Пример 3.
$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Лемма 4. *Нильпотентный элемент является делителем нуля.*

Доказательство. Если n наименьшее со свойством $x^n = 0$, то $x \cdot x^{n-1} = 0$ – делители нуля. □

Определение 6 (Кольцо вычетов)**.** Пусть m – натуральное число. Рассмотрим множество остатков при делении целых чисел на m. Это множество $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$. Определим сложение и умножение на $\mathbb{Z}_m$ следующим образом. Чтобы сложить два элемента из $\mathbb{Z}_m$ мы складываем их как целые числа, а затем берем остаток. Чтобы умножить два элемента из $\mathbb{Z}_m$ мы умножаем их как целые числа, а затем берем остаток. Получится ассоциативное коммутативное кольцо с единицей.

Теорема 3. *Кольцо* $\mathbb{Z}_m$ *является полем тогда и только тогда, когда* m *простое.*

Доказательство. Если $m = kl$, то $\overline{k} \cdot \overline{l} = \overline{0}$ – делители нуля, то есть не обратимы.

Пусть m простое и $\overline{x} \neq 0$. Рассмотрим $\overline{x0}, \overline{x1}, \overline{x2}, \dots, \overline{x(m-1)}$ Они все различны. Действительно, если $\overline{xi} = \overline{xj}$, то $x(i-j)$ делится на m, что не возможно. Значит, среди этих элементов есть $\overline{1}$, то есть $\overline{x}$ обратим. □

Задача 2. При каких n в кольце $\mathbb{Z}_n$ есть нильпотенты?

Определение 7. Пусть F – поле. *Характеристика* $\mathrm{char}\, F$ поля F равна наименьшему натуральному k такому, что сумма k единиц равна нулю, если такое натуральное k существует. Если же такого натурального k не существует, то говорят, что характеристика F равна нулю.

Пример 4. $\operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{Q} = 0$;
$\operatorname{char}\mathbb{Z}_p = p$.

Теорема 4. *Характеристика поля либо равна нулю, либо является простым числом.*

Доказательство. Допустим, что $\operatorname{char} F = mn$. Тогда

$$\underset{mn}{1 + 1 + \ldots + 1} = \underset{m}{(1 + 1 + \ldots + 1)}\underset{n}{(1 + 1 + \ldots + 1)}$$

Так как в поле нет делителей нуля, один из множителей равен нулю. $\square$

Лемма 5. *Пусть F – поле характеристики p. Если сложить элемент $a \in F$ с собой pk раз, то получится ноль.*

Доказательство. $pka = (1 + 1 + \ldots + 1)ka = 0ka = 0$. $\square$

Теорема 5. *Пусть F – поле характеристики p. Тогда для $a, b \in F$ выполнено $(a + b)^p = a^p + b^p$.*

Доказательство. По формуле бинома Ньютона

$$(a + b)^p = \sum_{i=0}^{p} C_p^i a^i b^{p-i} = a^p + \sum_{i=1}^{p-1} C_p^i a^i b^{p-i} + b^p.$$

При этом $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p при $i \in \{1, 2, \ldots, p-1\}$. Таким образом, в поле F все слагаемые, кроме крайних равны нулю. То есть $(a + b)^p = a^p + b^p$. $\square$

Следствие 4. *Пусть F – поле характеристики p. Тогда для $a_1, \ldots, a_m \in F$ выполнено $(a_1 + \ldots + a_m)^p = a_1^p + \ldots + a_m^p$.*

В качестве следствия получим еще одно доказательство малой теоремы Ферма. Для удобства сформулируем ее несколько иначе (легко видеть, что это эквивалентная формулировка).

Теорема 6 (Малая теорема Ферма)**.** *Пусть p – простое число. Для любого целого числа n выполнено $n^p \equiv n (\operatorname{mod} p)$.*

Доказательство. Утверждение теоремы равносильно тому, что в кольце $\mathbb{Z}_p$ выполнено $\overline{n}^p = \overline{n}$. Это следует из следующей цепочки равенств.

$$\overline{n}^p = (\overline{1} + \ldots + \overline{1})^p = (\overline{1} + \ldots + \overline{1}) = \overline{n}.$$

$\square$