ДИСКРЕТНАЯ МАТЕМАТИКА

ИУ3 - 5 семестр

Лекция 8. ТЕОРЕМА ЛАГРАНЖА (ПРОДОЛЖЕНИЕ). КОЛЬЦА, ТЕЛА, ПОЛЯ

Определение 8.1. Множества A и B называются **равномощными** ($|A| = |B|$), если существует взаимнооднозначное отображение (биекция) f множества A на множество B.

Теорема 1. Всякий левый смежный класс подгруппы H **равномощен** H.

◄ Для произвольного фиксированного $a \in G$ зададим отображение $\varphi_a\colon H \to aH$ следующим образом:

$$\varphi_a(h) = ah.$$

1. Отображение φ_a есть сюръекция, так как если $y \in aH$, то $y = ah$ для некоторого $h \in H$, откуда $y = \varphi_a(h)$.
2. φ_a — инъекция, поскольку из равенства $ah_1 = ah_2$ в силу законов сокращения в группе $\mathcal{G}$ следует $h_1 = h_2$.

Следовательно, φ_a — биекция и $|aH| = |H|$. ►

Определение 8.2. Порядком конечной группы называется количество элементов этой группы.

Теорема 2 (теорема Лагранжа). Порядок конечной группы делится на порядок любой ее подгруппы. (без доказательства)

Следствия теоремы Лагранжа.

Следствие 8.1. Любая группа простого порядка является циклической.

◄ Возьмем в группе, порядок которой есть простое число, какую-то ее циклическую подгруппу, образующий элемент которой отличен от единицы (нейтрального элемента) группы.
Тогда эта подгруппа содержит не менее двух элементов и ее порядок, согласно теореме Лагранжа, должен быть делителем порядка группы.
Поскольку порядок всей группы — простое число, а порядок подгруппы не меньше 2, то он совпадет с порядком всей группы.►

Рассмотрим моноид (группу) $(M, \cdot)$.

Подмоноид $(P, \cdot)$ (подгруппу) называют **тривиальным подмоноидом** (**тривиальной подгруппой**), если **носитель** содержит только единицу исходного моноида ($P = \{\mathbf{1}\}$) или совпадает с носителем исходного моноида (группы) ($P = M$).

Группу называют **неразложимой**, если она не имеет **нетривиальных подгрупп**.

Следствие 8.2. Конечная группа неразложима тогда и только тогда, когда она является циклической группой, порядок которой есть простое число.

◄ Пусть группа циклическая и ее порядок — простое число. Согласно теореме Лагранжа, каждая ее подгруппа имеет порядок, равный либо единице, либо порядку всей группы, следовательно, группа неразложима.
Обратно. Пусть конечная группа $\mathcal{G} = (G, \cdot, \mathbf{1})$ неразложима.
Покажем, что $|G|$ — простое число.
Выберем элемент $a \neq \mathbf{1}$.
Тогда циклическая подгруппа с образующим элементом a совпадает с $\mathcal{G}$.
Допустим, что $|G|$ — составное число, т.е.

$$\exists (k, l \in \mathbb{N}, k \neq 1, l \neq 1, k \neq |G|, l \neq |G|) \mid |G| = kl$$

Тогда циклическая подгруппа с образующим элементом $b = a^k$ не совпадает с $\mathcal{G}$, так как $b^l = a^{kl} = a^{|G|} = \mathbf{1}$ и в этой подгруппе не более l элементов, что противоречит неразложимости группы $\mathcal{G}$.
Следовательно, порядок группы $\mathcal{G}$ есть простое число. ►

Следствие 8.3. В конечной группе $\mathcal{G}$ для любого элемента $b \in G$ имеет место равенство $b^{|G|} = 1$.

◄ Если группа $\mathcal{G}$ циклическая и элемент b — ее образующий элемент, утверждение очевидно.
Если же элемент b является образующим элементом некоторой циклической подгруппы группы $\mathcal{G}$ порядка $k < |G|$, то в силу теоремы Лагранжа $|G| = kl$ для некоторого натурального l .
Отсюда получаем $b^{|G|} = b^{kl} = \left(b^k\right)^l = \mathbf{1}^l = \mathbf{1}$. ►

8.1. Кольца, тела, поля

Определение 8.3. Кольцом называют **алгебру**

$$\mathcal{R} = (R,\ +,\ \cdot,\ \mathbf{0},\ \mathbf{1}),$$

сигнатура которой состоит из двух бинарных и двух нульарных операций, причем для любых $a,\ b,\ c \in R$ выполняются равенства:

1) $a + (b + c) = (a + b) + c$;
2) $a + b = b + a$;
3) $a + \mathbf{0} = a$;
4) для каждого $a \in R$ существует элемент a', такой, что $a + a' = \mathbf{0}$;
5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
6) $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$;
7) $a \cdot (b + c) = a \cdot b + a \cdot c,\ (b + c) \cdot a = b \cdot a + c \cdot a$.

Операцию $+$ называют **сложением кольца**.
Операцию $\cdot$ — **умножением кольца**.
Элемент $\mathbf{0}$ — **нулем кольца**.
элемент $\mathbf{1}$ — **единицей кольца**.

Равенства 1–7, указанные в определении, называют **аксиомами кольца**.

Аксиомы кольца 1–4 означают, что алгебра $(R, +, \mathbf{0})$, сигнатура которой состоит только из операций сложения кольца $+$ и нуля кольца $\mathbf{0}$,является **абелевой группой**.

Эту группу называют **аддитивной группой кольца** $\mathcal{R}$

По сложению кольцо есть коммутативная (абелева) группа.

Аксиомы кольца 5 и 6 показывают, что алгебра $(R, \cdot, \mathbf{1})$, сигнатура которой включает только умножение кольца $\cdot$ и единицу кольца $\mathbf{1}$, есть моноид.

Этот моноид называют **мультипликативным моноидом кольца** $\mathcal{R}$

По умножению кольцо есть моноид.

Аксиома 7 устанавливает связь между сложением кольца и умножением кольца.

Операция умножения дистрибутивна относительно операции сложения.

Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями $\mathcal{R} = (R, +, \cdot, \mathbf{0}, \mathbf{1})$, такая, что:

1) алгебра $(R, +, \mathbf{0})$ — коммутативная группа;

2) алгебра $(R, \cdot, \mathbf{1})$ — моноид;

3) операция $\cdot$ (умножения кольца) дистрибутивна относительно операции $+$ (сложения кольца).

Определение 8.4. Кольцо называют **коммутативным**, если его операция умножения коммутативна.

Пример 8.1. **а.** Алгебра $(\mathbb{Z},\ +,\ \cdot,\ 0,\ 1)$ есть коммутативное кольцо. Отметим, что алгебра $(\mathbb{N},\ +,\ \cdot,\ 0,\ 1)$ кольцом не будет, поскольку $(\mathbb{N},\ +)$ — коммутативная полугруппа, но не группа.

б. Рассмотрим алгебру $\mathbb{Z}_k = (\{0,\ 1,\ \ldots,\ k-1\},\ \oplus_k,\ \odot_k,\ 0, 1)$ ($k \geq 1$) с операцией $\oplus_k$ сложения по модулю k и $\odot_k$ (умножения по модулю k).
Операция умножения по модулю k аналогична операции сложения по модулю k : $m \odot_k n$ равно остатку от деления на k числа $m \cdot n$.
Эта алгебра есть коммутативное кольцо, которое называют **кольцом вычетов по модулю** k .

в. Алгебра $(2^A,\ \triangle,\ \cap,\ \varnothing,\ A)$ — коммутативное кольцо. Это следует из свойств *пересечения* и *симметрической разности множеств*.

г. Множество всех квадратных матриц фиксированного порядка с операциями сложения и умножения матриц — некоммутативное кольцо.
Единицей этого кольца является единичная матрица, а нулем — нулевая.

Аксиомы кольца называют также **основными тождествами кольца**.

Тождество кольца — это равенство, справедливость которого сохраняется при подстановке вместо фигурирующих в нем переменных любых элементов кольца.

Введем операцию **вычитания** для кольца и докажем тождества для этой операции.

Это возможно потому, что аддитивная группа кольца коммутативна и в ней определена операция *вычитания*.

Теорема 3. В любом кольце выполняются следующие тождества:

1 $\mathbf{0} \cdot a = a \cdot \mathbf{0} = \mathbf{0}$;

2 $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$;

3 $(a - b) \cdot c = a \cdot c - b \cdot c$, $\quad c \cdot (a - b) = c \cdot a - c \cdot b$.

◄ Докажем тождество $\mathbf{0} \cdot a = \mathbf{0} \quad (1)$.

$$\forall\, a\ (a + \mathbf{0} \cdot a = \mathbf{1} \cdot a + \mathbf{0} \cdot a = (\mathbf{1} + \mathbf{0}) \cdot a = \mathbf{1} \cdot a = a).$$

В аддитивной группе кольца получили уравнение

$$a + \mathbf{0} \cdot a = a$$

относительно неизвестного элемента $\mathbf{0} \cdot a$.

В аддитивной группе любое уравнение вида $a + x = b$ имеет единственное решение $x = b - a$.

$\mathbf{0} \cdot a = a - a = \mathbf{0}$.

Тождество $a \cdot \mathbf{0} = \mathbf{0}$ доказывается аналогично.

Докажем тождество $-(a \cdot b) = a \cdot (-b)$ (2). Имеем

$$a \cdot (-b) + a \cdot b = a \cdot ((-b) + b) = a \cdot \mathbf{0} = \mathbf{0} \Rightarrow$$
$$\Rightarrow \; a \cdot (-b) = -(a \cdot b)$$

$(-a) \cdot b = -(a \cdot b)$ можно доказать точно так же.

Докажем тождества (3).
Рассмотрим $(a - b) \cdot c = a \cdot c - b \cdot c$.
С учетом доказанного выше имеем

$$a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b - a \cdot c,$$

т.е. тождество справедливо.
Тождество $c \cdot (a - b) = c \cdot a - c \cdot b$ доказывается аналогично. ▶

Следствие 8.4. В любом кольце справедливо тождество

$$(-\mathbf{1}) \cdot x = x \cdot (-\mathbf{1}) = -x.$$

◄ Указанное следствие вытекает из второго тождества теоремы 3 при $a = \mathbf{1}$ и $b = x$. ►

Первые два тождества в теореме выражают свойство, называемое **аннулирующим свойством нуля** в кольце.

Тождества (3) теоремы 3 выражает свойство дистрибутивности операции умножения кольца относительно операции вычитания.

В любом кольце производя вычисления , можно раскрывать скобки и менять знаки так же, как и при сложении, вычитании и умножении действительных чисел.

Определение 8.5. Ненулевые элементы a и b кольца $\mathcal{R}$ называют **делителями нуля**, если $a \cdot b = \mathbf{0}$ или $b \cdot a = \mathbf{0}$.

Пример 8.2. а. Кольцо вычетов по модулю k, если k — составное число. В этом случае произведение по модулю k любых m и n, дающих при обычном перемножении число, кратное k, будет равно нулю.
В кольце вычетов по модулю 6 элементы 2 и 3 являются делителями нуля, поскольку $2 \odot_6 3 = 0$.

б. Кольцо квадратных матриц фиксированного порядка (не меньшего двух). Например, для матриц второго порядка имеем

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

При отличных от нуля a и b приведенные матрицы являются делителями нуля.

По умножению кольцо является только моноидом, не группой.
Множество всех элементов кольца,в котором $\mathbf{0} \neq \mathbf{1}$, не может образовывать группы по умножению, так как нуль не может иметь обратного.
Если предположить, что такой элемент $\mathbf{0}'$ существует, то, с одной стороны, $\mathbf{0} \cdot \mathbf{0}' = \mathbf{0}' \cdot \mathbf{0} = \mathbf{1}$, а с другой — $\mathbf{0} \cdot \mathbf{0}' = \mathbf{0}' \cdot \mathbf{0} = \mathbf{0}$, откуда $\mathbf{0} = \mathbf{1}$.
Это противоречит условию $\mathbf{0} \neq \mathbf{1}$.

Рассмотрим множество всех ненулевых элементов кольца.
Если в кольце имеются **делители нуля**, то подмножество всех **ненулевых** элементов кольца не образует группы по умножению, это подмножество **не замкнуто** относительно операции умножения, т.е. существуют ненулевые элементы, произведение которых равно нулю.

Определение 8.6. Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют **телом**.

Определение 8.7. Коммутативное тело называют **полем**, а группу ненулевых элементов тела (поля) по умножению —**мультипликативной группой** этого **тела(поля)**.

Поле есть частный случай кольца, в котором операции обладают дополнительными свойствами.

Аксиомы поля

Поле есть алгебра $\mathcal{F} = (F, +, \cdot, \mathbf{0}, \mathbf{1})$, сигнатура которой состоит из двух бинарных и двух нульарных операций, причем справедливы тождества:

1) $a + (b + c) = (a + b) + c$;
2) $a + b = b + a$;
3) $a + \mathbf{0} = a$;
4) для каждого $a \in F$ существует элемент $-a$, такой, что $a + (-a) = \mathbf{0}$;
5) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
6) $a \cdot b = b \cdot a$;
7) $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$;
8) для каждого $a \in F$, отличного от $\mathbf{0}$, существует элемент a^{-1}, такой, что $a \cdot a^{-1} = \mathbf{1}$;
9) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Пример 8.3. **а.** Алгебра $(\mathbb{Q},\ ,+,\ \cdot,\ 0,\ 1)$ есть поле, называемое **полем рациональных чисел**.

б. Алгебры $(\mathbb{R},\ +,\ \cdot,\ 0,\ 1)$ и $(\mathbb{C},\ +,\ \cdot,\ 0,\ 1)$ есть поля, называемые **полями действительных** и **комплексных чисел** соответственно.

8.2. Области целостности

Областью целостности называют **коммутативное кольцо** без **делителей нуля**.

Так, кольцо целых чисел есть область целостности.

Утверждение 8.1. Если A — конечное множество и $f : A \to A$ — инъекция, то она является сюръекцией и следовательно биекцией

Теорема 4. Конечная область целостности является **полем**.

◄ Поле — это кольцо, умножение которого **коммутативно**, каждый ненулевой элемент a имеет **обратный элемент** относительно **умножения**.
Область целостности является **коммутативным** кольцом без делителей нуля.
Докажем, что для конечной области целостности любой ненулевой элемент обратим, т.е. $\forall\ (a \neq \mathbf{0}) \exists x$ (единственный) $\mid a \cdot x = \mathbf{1}$.
Фиксируем произвольный элемент $a \neq \mathbf{0}$.
Определим отображение f_a множества всех ненулевых элементов в себя по формуле $f_a(x) = a \cdot x$
($a \cdot x \neq \mathbf{0}$ в области целостности при $a \neq \mathbf{0}$ и $x \neq \mathbf{0}$).
Докажем, что отображение f_a — инъекция (каждый элемент из области значений имеет единственный прообраз).

$$a \cdot x = a \cdot y \ \Rightarrow\ a \cdot (x - y) = \mathbf{0} \Rightarrow$$
$$\Rightarrow x - y = \mathbf{0}\ (\text{т.к. делители нуля отсутствуют}) \Rightarrow\ x = y$$

Множество носитель по условию теоремы конечено,следовательно, f_a — биекция (утверждение 8.1).
Поэтому $\forall (y)\ \exists (\text{ единственный } x) \mid y = a \cdot x$.
В частности, при $y = \mathbf{1}$ равенство $a \cdot x = \mathbf{1}$ выполнено для некоторого однозначно определенного x , т.е. $x = a^{-1}$. ►

Следствия теоремы 4.

Следствие 8.5. Кольцо $\mathbb{Z}_p$ вычетов по модулю p является полем тогда и только тогда, когда p — простое число.

◄ Пусть $\mathbb{Z}_p$ является полем. Покажем, что p — простое число.
Предположим — p составное.
Тогда найдутся такие k и l, $0 < k \leq p-1; 0 < l \leq p-1$, что $p = k \cdot l \Rightarrow$ $k \cdot l = 0 \,(\mathrm{mod\ p}) \Rightarrow$ k и l — делители нуля в кольце $\mathbb{Z}_p$.
Следовательно, $\mathbb{Z}_p$ — не поле.
Число p не может быть составным.

Пусть p — простое число.
Предположим, что $m \cdot n = 0 \,(\mathrm{mod\ p})$, т.е. элементы m и n кольца $\mathbb{Z}_p$ будут делителями нуля (кольцо не область целостности).
p — простое число и $(m \cdot n = 0 \,(\mathrm{mod\ p})) \Rightarrow$
$(\ (m = 0 \,(\mathrm{mod\ p})) \vee (n = 0 \,(\mathrm{mod\ p}))\ )$
Т.к. $((0 \leq m \leq p-1) \wedge (0 \leq n \leq p-1)) \Rightarrow (m = 0) \vee (n = 0)$.
Следовательно, при простом p делителей нуля нет.
Кольцо $\mathbb{Z}_p$ является конечной областью целостности и по теореме 4 — полем. ►

ДОПОЛНИТЕЛЬНЫЙ МАТЕРИАЛ.
Доказательство теоремы Лагранжа.
Подгруппоид тривиальный.
Подгруппоид собственный.
Малая теорема Ферма

Теорема Лагранжа Порядок конечной группы делится на порядок любой ее подгруппы.

◄ Во введенном выше отношении эквивалентности $\sim_H$ классом эквивалентности элемента a является множество aH (левый смежный класс подгруппы H по элементу a).
Согласно теореме 5 из лекции 5, все левые смежные классы образуют разбиение множества G на подмножества, равномощные в силу теоремы 1 подгруппе H .
Так как группа $\mathcal{G}$ конечна, то число элементов разбиения конечно. Обозначив это число через k , заключаем, что $|G| = k|H|$. Следовательно, порядок группы $|G|$ делится на порядок группы $|H|$. ►

Напомним, что теорема 5 из лекции 5 имеет следующую формулировку:
бинарное отношение $\sim_H$ есть эквивалентность на G, причем класс эквивалентности произвольного элемента $a \in G$ совпадает с левым смежным классом aH .

Подмоноид, **носитель** которого содержит только единицу исходного моноида ($P = \{\mathbf{1}\}$), а также подмоноид, носитель которого совпадает с носителем исходного моноида ($P = M$), называют **тривиальным подмоноидом** (в частности, **тривиальной подгруппой**).

Подмоноид, не являющийся тривиальным, называют **нетривиальным подмоноидом** (в частности, **нетривиальной подгруппой**).

Подгруппоид (подполугруппу, подмоноид, подгруппу) $(G, *)$ называют **собственным подгруппоидом** (**подполугруппой**, **подмоноидом**, **подгруппой**) группоида (полугруппы, моноида, группы) $(K, *)$, если его носитель G есть *собственное подмножество* множества K .

С помощью теоремы Лагранжа (точнее, следствия 8.3) можно доказать, что если целое число n не делится на простое число p, то $n^{p-1}-1$ делится на p. В теории чисел это утверждение известно как **малая теорема Ферма**. Действительно, пусть $n = rp + k$, где r — целое, а $0 < k < p$ (остаток от деления n на p). Тогда ясно, что $n^{p-1} = k^{p-1} \,(\mathrm{mod\ p})$ (достаточно разложить $(rp+k)^{p-1}$ по формуле *бинома Ньютона*). Рассмотрим группу $\mathbb{Z}_p^*$ (*мультипликативную группу вычетов по модулю* p) и в этой группе элемент k. Порядок группы $\mathbb{Z}_p^* = p-1$. Если $k = 1$, то

$$n^{p-1} - 1 = (1^{p-1} - 1) \,(\mathrm{mod\ p}) = 0 \,(\mathrm{mod\ p})$$

и утверждение очевидно. Согласно следствию 8.3, в группе $\mathbb{Z}_p^*$ справедливо равенство $k^{p-1} = 1$, т.е. $k^{p-1} = 1 \,(\mathrm{mod\ p})$, и, следовательно, $k^{p-1} - 1 = 0 \,(\mathrm{mod\ p})$, т.е. число k^{p-1} равно 1 по модулю p. Поэтому $n^{p-1} = k^{p-1} = 1 \,(\mathrm{mod\ p})$.

Малая теорема Ферма дает возможность доказывать утверждения о делимости очень больших чисел. Например, из нее следует, что при $p = 97$ число 97 является делителем $n^{96} - 1$ для любого n, не делящегося на 97. Подобного рода заключения важны при разработке алгоритмов защиты информации.

Кроме того, используя малую теорему Ферма, можно вычислять в *полях вычетов* по *модулю* p (p — простое число) элементы, обратные к заданным относительно умножения. Действительно, если $a \in \mathbb{Z}_p$, то, так как $a^{p-1} = 1$, умножая последнее равенство на a^{-1}, получим $a^{p-2} = a^{-1}$. Таким образом, для того чтобы вычислить элемент, обратный к a по умножению, достаточно возвести его в степень $p - 2$ или, что равносильно, в степень, равную остатку от деления числа $p - 2$ на порядок циклической подгруппы группы $\mathbb{Z}_p^*$, порожденной элементом a.

Пример 8.4. Рассмотрим, как вычислить элемент, обратный к a по умножению в поле $\mathbb{Z}_{17}$. Согласно полученному выше результату, для вычисления обратного к a элемента нужно найти $a^{17-2} = a^{15}$. Однако объем вычислений можно сократить, если порядок циклической подгруппы, порожденной элементом a, меньше порядка группы.

Порядок группы $\mathbb{Z}_{17}^*$ равен 16, следовательно, порядок циклической подгруппы, порожденной элементом a, может составлять, согласно теореме Лагранжа, 2, 4, 8, 16 (т.е. быть каким-то из делителей числа 16). Поэтому при поиске обратного элемента достаточно проверить следующие степени a (кроме 15-й): 1 (остаток от деления 15 на 2), 3 (остаток от деления 15 на 4) и 7 (остаток от деления 15 на 8).

Найдем элемент, обратный к 2. Очевидно, что $2^{-1} \neq 2$, так как $2 \odot_{17} 2 = 4 \neq 1$. Далее получим $2^3 = 4 \odot_{17} 2 = 8$. Поскольку $2 \odot_{17} 8 = 16 \neq 1$, то $2^3 = 8$ также не является обратным к 2. Вычислим $2^7 = 2^3 \odot_{17} 2^3 \odot_{17} 2 = 8 \odot_{17} 8 \odot_{17} 2 = 9$. Поскольку $9 \odot_{17} 2 = 1$, в итоге получаем $2^{-1} = 9$.

Найдем элемент, обратный к 14. Так как $14 \odot_{17} 14 = 9$, то $14^{-1} \neq 14$. Вычисляем $14^3 = 14 \odot_{17} 9 = 7$, но $14 \odot_{17} 7 = 13$, т.е. $14^3 \neq 14^{-1}$. Далее,

$$14^7 = 14^3 \odot_{17} 14^4 = 7 \odot_{17} 13 = 6,$$
$$14 \odot_{17} 6 = 16 = -1.$$

Мы видим, что и $14^7 \neq 14^{-1}$. Следовательно, остается вычислить $14^{-1} = 14^{15}$. Однако в этом случае вычисления можно сократить, заметив, что $14 \odot_{17} 14^7 = 14 \odot_{17} 6 = -1$. Из последнего равенства получим

$$1 = 14 \odot_{17} (-6) = 14 \odot_{17} 11,$$

откуда $14^{-1} = 11$.
Отметим, что $14^{16} = 1$, т.е. порядок циклической подгруппы, порожденной элементом 14, совпадает с порядком всей группы $\mathbb{Z}_{17}^*$, и, следовательно, эта группа является циклической, порожденной элементом 14 (хотя и не только им).