Лекция 8. Нормальные подгруппы. Факторгруппы.

#вшпи #дискретная_математика #теория

Автор конспекта: Гридчин Михаил

Теорема Лагранжа

На прошлой лекции было доказано, что левые (правые) смежные классы не пересекаются или совпадают.

Теорема (Лагранжа). Количество элементов в группе делится на количество элементов в подгруппе. Записывается:

$$\boxed{|G| = (G : H)|H|}$$

Где $(G : H)$ - индекс подгруппы H.

$\square$
Докажем для левых смежных классов, для правых доказательство аналогично.

ШАГ 1. Докажем сначала, что количество элементов в $|gH| = |H|$. То есть, другими словами $\forall h_1, h_2 \in H, h_1 \neq h_2 \implies g \circ h_1 \neq g \circ h_2$. Действительно, если это не так и выполнено $g \circ h_1 = g \circ h_2$, то умножим обе части на $g^{-1} \in G$ слева. Получим:

$$g^{-1} \circ (g \circ h_1) = g^{-1} \circ (g \circ h_2)$$

$$e \circ h_1 = e \circ h_2$$

$$h_1 = h_2$$

Противоречие, значит, количество элементов в $|gH|$ действительно равно количеству элементов в $|H|$.

ШАГ 2. Докажем, что $\forall g \in G \implies g \in gH$. Действительно, поскольку H - подгруппа, то $e \in H$. Но тогда $g \circ e = g \in gH$.

ШАГ 3. Смежные классы не пересекаются или совпадают. Тогда группа G разбита на непересекающиеся подмножества $aH, bH, \ldots$, в каждом из которых ровно по $|H|$ элементов. Также каждый элемент G принадлежит какому-то смежному классу. Значит, количество элементов в G делится на количество элементов в H. Получили требуемое. А индекс подгруппы H - это количество различных смежных классов (левых)
$\blacksquare$

Def. *Правый смежный класс по подгруппе H группы G с представителем $g \in G$*:

$$Hg := \{h \circ g \mid h \in H\}$$

Нормальные подгруппы

Def. Подгруппа $H < G$ называется *нормальной* (и обозначается $H \lhd G$), если $\forall g \in G \implies gH = Hg$.

Размышления. $gH = Hg \iff \{g \circ h \mid h \in H\} = \{h \circ g \mid h \in H\}$. Умножим на g^{-1} справа. Но тогда получим:

$$gHg^{-1} = H$$

Тогда можно ввести эквивалентное определение нормальной подгруппы.

Def (эквивалентное определение нормальной подгруппы).

$$H \lhd G \iff \forall g \in G, \forall h \in H \implies g \circ h \circ g^{-1} \in H$$

Теорема: Приведённые определения эквивалентны.
□
$1 \Rightarrow 2$: $H \lhd G \implies gH = Hg \implies \forall h_1 \in H \exists h_2 \in H : g \circ h_1 = h_2 \circ g \implies g \circ h_1 \circ g^{-1} = h_2 \in H$.
$1 \Leftarrow 2$: $\forall g \in G, \forall h \in H \implies g \circ h \circ g^{-1} \in H$. Тогда рассмотрим $gHg^{-1} = \{g \circ h \circ g^{-1} \mid h \in H\}$. Но это множество содержит столько же элементов, сколько и H. Почему меньше быть не может? Смотрите первый шаг доказательства теоремы Лагранжа. Тогда поскольку также все элементы $g \circ h \circ g^{-1} \in H \forall h \in H \forall g \in G$, то выполнено $gHg^{-1} = H$. Умножим на g справа, получим $gH = Hg$, это и требовалось показать.
■

Факторгруппы

"Нормальные подгруппы - это достаточно ценная вещь. С её помощью мы можем делать так называемые факторгруппы. Пусть есть множество каких-то объектов, которые вместе с операцией образуют группу. Элементов в ней может быть достаточно много, но иногда для наших прикладных целей столько элементов рассматривать не надо. Надо рассматривать какие-то более группы. Факторизация - это возможность объединять некоторые группы в подмножества и делать групповую операцию над укрупнёнными подгруппами".

Def. Пусть $H \lhd G$. Рассмотрим смежные классы. Для определённости левые по H. Введём операцию $(aH) * (bH) := (a \circ b)H, a \in G, b \in G$. То есть это операция на множестве смежных классов, которая двум смежным классам сопоставляет третий.

Утверждение + Def. Множество смежных классов относительно данной операции образует группу (называемую *факторгруппой группы G по нормальной подгруппе H и обозначаемую G/H*).

$\square$

ШАГ 1. Докажем ассоциативность $(*)$.

$$\forall a, b, c \in G \implies \begin{cases} ((aH) * (bH)) * (cH) = ((a \circ b)H) * (cH) = ((a \circ b) \circ c)H = (a \circ b \circ c)H \\ (aH) * ((bH) * (cH)) = (aH) * ((b \circ c)H) = (a \circ (b \circ c))H = (a \circ b \circ c)H \end{cases}$$

Получили требуемое.

ШАГ 2. Докажем существование нейтрального элемента. Докажем, что $eH = H$ - искомый нейтральный элемент. Действительно,

$$\forall a \in G \implies (aH) * (eH) = (a \circ e)H = (e \circ a)H = (eH) * (aH)$$

Теперь докажем единственность нейтрального элемента. Доказательство от противного. Пусть существуют nH и eH - нейтральные элементы относительно операции $(*)$. Заметим, что e - нейтральный элемент относительно операции $(\circ)$, а n - нет. Тогда:

$$(nH) * (eH) = (eH) = (nH)$$

Первое равенство из того, что nH - нейтральный, второе равенство из того, что eH - нейтральный. Получили, что $eH = nH$. Противоречие. Значит, нейтральный элемент единственный. Получили требуемое.

ШАГ 3. Докажем существование обратного элемента. Действительно,
$\forall a \in G \implies (aH) * (a^{-1}H) = (a^{-1}H) * (aH) = eH = H$.
Единственность доказывается аналогично шагу 2.

Значит, множество смежных классов относительно введённой операции $(*)$ образует группу.
$\blacksquare$

Вопрос. Зачем нам нужна была нормальность подгруппы, если мы её нигде не использовали? Ответ: мы воспользовались нормальностью подгруппы H в тот момент, когда ввели операцию $(*)$. Оказывается, что её можно определить для нормальной подгруппы и нельзя для ненормальной. Действительно, корректности (независимости от представителя) должно быть выполнено:

$$\begin{cases} \forall a_1 \in aH \implies a_1H = aH \\ \forall b_1 \in bH \implies b_1H = bH \end{cases}$$

$\square$
$(a_1H) * (b_1H) = (a_1 \circ b_1)H$. Покажем, что $(a_1 \circ b_1)H = (a \circ b)H$. Для этого нам достаточно найти хотя бы один общий элемент, чтобы они были равны (поскольку смежные классы не пересекаются или совпадают). Покажем, что $(a_1 \circ b_1) \in (a \circ b)H$. Действительно,

$$\begin{aligned} &a_1 \in aH \implies \exists h_a \in H : a_1 = a \circ h_a \\ &b_1 \in bH \implies \exists h_b \in H : b_1 = b \circ h_b \\ &a_1 \circ b_1 = a \circ \boxed{h_a \circ b} \circ h_b \end{aligned}$$

Но у нас нет коммутативности, чтобы поменять h_a и b местами, чтобы получить требуемое. В этот момент нам и приходит на помощь нормальность подгруппы. Мы знаем, что

$$bH = Hb \implies \forall h \in H \exists \tilde{h} \in H : h \circ b = b \circ \tilde{h}$$

Но тогда и для $\boxed{h_a \circ b}$ найдётся такой элемент $\tilde{h}_a : b \circ \tilde{h}_a = h_a \circ b$. Итого получаем:

$$a_1 \circ b_1 = a \circ b \circ \underbrace{\tilde{h}_a \circ h_b}_{=:\tilde{h} \in H} = a \circ b \circ \tilde{h}$$

Но так как $\tilde{h} \in H$, то и $(a_1 \circ b_1) \in (a \circ b)H$.
■

Вопрос. Сколько элементов в факторгруппе? Ответ: индекс H. Действительно, вся факторгруппа состоит из всех смежных классов, количество которых равно индексу H.

Гомоморфизм групп

Из прошлой лекции *гомоморфизм* - это такое отображение $\varphi : G(M, (\circ)) \to G'(M', (*))$, что $\forall a, b \in G \implies \varphi(a \circ b) = \varphi(a) * \varphi(b)$.
Уже доказанные свойства:

- $\varphi(e) = e'$
- $\varphi(a^{-1}) = (\varphi(a))^{-1}$. Следствие: $\varphi(a^m) = (\varphi(a))^m$
- порядок элемента $\varphi(a)$ является делителем порядка элемента a.

Def. *Образ гомоморфизма* - $\mathrm{Im}\varphi = \varphi(G) = \{\varphi(a) \mid a \in G\}$.
Теорема. Образ гомоморфизма - это подгруппа G'.
□
Из определения $Im\varphi \subseteq G'$. Применим *критерий подгруппы* для доказательства, что это подгруппа. Рассмотрим произвольные элементы $c, d \in Im\varphi$. По определению образа $\exists a, b \in G : \varphi(a) = c, \varphi(b) = d$. Рассмотрим $(c * d^{-1})$:

$$c * d^{-1} = \varphi(a) * \varphi(b^{-1}) = \varphi(a \circ b^{-1}) \in Im\varphi$$

Следовательно, $\mathrm{Im}\varphi < G'$ по критерию подгруппы.
■

Def. *Ядро гомоморфизма* - $\mathrm{Ker}\varphi = \{g \mid g \in G, \varphi(g) = e'\}$.
Теорема. Ядро гомоморфизма - это подгруппа G.
□
Из определения $\mathrm{Ker}\varphi \subseteq G$. Применим *критерий подгруппы* для доказательства, что это подгруппа. Возьмём произвольные $a, b \in \mathrm{Ker}\varphi$. Тогда:

$$\varphi(a \circ b^{-1}) = \varphi(a) * \varphi(b) = e' * (e')^{-1} = e' \implies a \circ b^{-1} \in Ker\varphi$$

Следовательно, $\mathrm{Ker}\varphi < G$ по критерию подгруппы.
■

Теорема. $Ker\varphi \triangleleft G$.
□
Рассмотрим произвольный элемент $g \in G$. Рассмотрим $g\mathrm{Ker}\varphi$. Поскольку $\mathrm{Ker}\varphi < G$, то $|g\mathrm{Ker}\varphi| = |(\mathrm{Ker}\varphi)g| = |\mathrm{Ker}\varphi|$. Рассмотрим произвольное $\boxed{t \in g\mathrm{Ker}\varphi}$. Для него $\exists h \in \mathrm{Ker}\varphi : t = g \circ h$. Рассмотрим $g \circ h \circ g^{-1}$. Для него выполнено $\varphi(g \circ h \circ g^{-1}) = \varphi(g) * \varphi(h) * \varphi(g^{-1})$. Заметим, что $\varphi(h) = e'$, так как $h \in \mathrm{Ker}\varphi$. Тогда $\varphi(g \circ h \circ g^{-1}) = e' \implies (g \circ h \circ g^{-1}) \in \mathrm{Ker}\varphi \implies \underbrace{g \circ h}_{=t} \in (\mathrm{Ker}\varphi)g \implies \boxed{t \in (\mathrm{Ker}\varphi)g}$. Но t и g были выбраны произвольно. Тогда по определению нормальной подгруппы $\mathrm{Ker}\varphi \triangleleft G$.
■

Факторгруппа по ядру гомоморфизма

Рассмотрим $G/\mathrm{Ker}\varphi$ (факторгруппа G по подгруппе $\mathrm{Ker}\varphi$).

Утверждение. Два элемента группы G содержатся в одном смежном классе по $\mathrm{Ker}\varphi \iff$ их образы совпадают. То есть $a, b \in g\mathrm{Ker}\varphi \iff \varphi(a) = \varphi(b)$. То есть между элементами $\mathrm{Im}\varphi$ и смежными классами биекция $\varphi(g) \iff g\mathrm{Ker}\varphi$.
□
$\Rightarrow$
Рассмотрим произвольные $a, b \in g\mathrm{Ker}\varphi \implies \exists h_a, h_b \in \mathrm{Ker}\varphi : a = g \circ h_a, b = g \circ h_b$.
Рассмотрим $\varphi(a) = \varphi(g \circ h_a) = \varphi(g) * \underbrace{\varphi(h_a)}_{=e'} = \varphi(g)$. Аналогично, $\varphi(b) = \varphi(g)$. Тогда $\varphi(a) = \varphi(b)$.
$\Leftarrow$
Пусть $\varphi(a) = \varphi(b) \implies \varphi(a \circ b^{-1}) = \varphi(a) * (\varphi(b))^{-1} = e' \implies (a \circ b^{-1}) \in \mathrm{Ker}\varphi$. Тогда поскольку $a = (a \circ b^{-1}) \circ b \in (\mathrm{Ker}\varphi)b = b(\mathrm{Ker}\varphi)$. А также $a \in a\mathrm{Ker}\varphi$. А значит смежные классы совпадают, поскольку имеют общий элемент.
■

Теорема. $\mathrm{Im}\varphi \cong G/\mathrm{Ker}\varphi$ (гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма).
□
В предыдущем утверждении мы доказали биекцию между $\mathrm{Im}\varphi$ и $G/\mathrm{Ker}\varphi(\times)$
$f : \varphi(g) \iff g\mathrm{Ker}\varphi$.

$$f(\varphi(g)) = g\mathrm{Ker}\varphi$$

$$f(\varphi(a) * \varphi(b)) = f(\varphi(a \circ b)) = (a \circ b)\mathrm{Ker}\varphi$$

$$f(\varphi(a)) \times f(\varphi(b)) = a\mathrm{Ker}\varphi \times b\mathrm{Ker}\varphi = (a \circ b)\mathrm{Ker}\varphi$$

Следовательно, $f(\varphi(a) * \varphi(b)) = f(\varphi(a)) \times f(\varphi(b))$. Значит, f - гомоморфизм. Но f - биекция. Следовательно, f - изоморфизм.

■