



Лекция 2

Структура группы

Содержание лекции:

В настоящей лекции мы кратко рассмотрим основы теории групп, введем связанные объекты и понятия, которые будут необходимы в дальнейшем и в целом играют очень важную роль в приложениях. Лекция носит ознакомительный характер.

Ключевые слова:

Группа, коммутативная группа, гомоморфизм групп, изоморфизм, автоморфизм, ядро гомоморфизма, образ гомоморфизма, вложение, подгруппа, отношение эквивалентности, правый (левый) смежный класс, нормальная подгруппа, фактор-группа, канонический гомоморфизм, теорема об изоморфизме.

Авторы курса:

Трифанов А.И.

Ссылка на ресурсы:

mathdep.ifmo.ru/geolin

2.1 Определение. Примеры

Непустое множество G называется **группой**, если на нем задан закон композиции $G \times G \rightarrow G$, так что $(x, y) \mapsto xy$ и имеют место следующие три свойства:

G1. Ассоциативность закона:

$$\forall x, y, z \in G \quad (xy)z = x(yz).$$

G2. Существует нейтральный элемент:

$$\exists e \in G : \quad \forall x \in G \quad xe = x = ex.$$

G3. Существует обратный элемент:

$$\forall x \in G \quad \exists x^{-1} : \quad xx^{-1} = e = x^{-1}x.$$

Пример 2.1. На практике группы чаще всего встречаются в виде *групп преобразований* каких-то объектов:

- группа D_3 симметрий правильного треугольника;
- симметрическая группа S_n перестановок;
- группа Рубика - группа внутренних вращений кубика Рубика;

Коммутативной или **абелевой** называется такая группа, любые два элемента которой *коммутируют*:

$$\forall x, y \in G \quad xy = yx.$$

Пример 2.2. Примеры коммутативных групп:

1. Аддитивная группа целых чисел \mathbb{Z}^+ ;
2. Мультипликативная группа вещественных чисел $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$;
3. Группа углов (точек единичной окружности) - группа вещественных чисел \mathbb{R}^+ по модулю $2\pi\mathbb{Z}$. Групповая операция \oplus определяется следующим образом:

$$\begin{cases} x \oplus y = x + y, & x + y < 2\pi \\ x \oplus y = x + y - 2\pi, & x + y \geq 2\pi \end{cases}$$

4. Булева группа множества X - множество 2^X всех подмножеств множества X вместе с операцией симметрической разности Δ ;
5. Группа размерностей физических величин;

2.2 Гомоморфизмы групп

Гомоморфизмом групп G и G' называется отображение $\sigma : G \rightarrow G'$, обладающее следующими свойствами:

$$\forall x, y \in G \quad \sigma(xy) = \sigma(x)\sigma(y), \quad \sigma(e) = e'.$$

Nota bene Множество гомоморфизмов из группы G в группу G' принято обозначать $\text{Hom}(G, G')$. Гомоморфизмы из G в G называются эндоморфизмами и их множество обозначается $\text{End}(G) \triangleq \text{Hom}(G, G)$.

Лемма 2.1. Пусть $\sigma \in \text{Hom}(G, G')$, тогда

$$\forall x \in G \quad \sigma(x^{-1}) = \sigma(x)^{-1}.$$

Гомоморфизм σ называется **изоморфизмом**, если

$$\exists \chi \in \text{Hom}(G', G) : \quad \chi \circ \sigma = \text{id}_G, \quad \sigma \circ \chi = \text{id}_{G'}.$$

Nota bene Подмножество отображений в $\text{Hom}(G, G')$, являющихся изоморфизмами, принято обозначать $\text{Iso}(G, G')$. В случае $\text{Iso}(G, G)$ обычно пишут $\text{Aut}(G)$ и соответствующие отображения называют **автоморфизмами**.

Пример 2.3. Множество $\text{Aut}(G)$ вместе с операцией композиции и тождественным отображением id_G является группой (автоморфизмов группы G).

Ядром гомоморфизма $\sigma \in \text{Hom}(G, G')$ называется множество

$$\ker \sigma = \{g \in G : \sigma(g) = e'\}.$$

Лемма 2.2. Ядро $\ker \sigma$ является группой.

Лемма 2.3. Гомоморфизм $\sigma \in \text{Hom}(G, G')$ ядро которого тривиально инъективен.

Образом гомоморфизма $\sigma \in \text{Hom}(G, G')$ называется подмножество G' , такое что

$$\text{Im } \sigma = \{g' \in G' : \exists g \in G, \quad \sigma(g) = g'\}.$$

Лемма 2.4. Образ $\text{Im } \sigma$ является группой.

Вложением называется гомоморфизм $\sigma \in \text{Hom}(G, G')$, обладающий следующим свойством

$$G \simeq \text{Im } \sigma \subset G'.$$

2.3 Подгруппы

|| Подгруппой H группы G называется подмножество G , имеющее структуру группы, индуцированной групповым законом G .

Nota bene Подгруппа $\{e\}$ называется *тривиальной подгруппой*, G как подгруппа самой себя называется *несобственной*, остальные подгруппы G называются *собственными подгруппами*.

Пример 2.4. Пусть $\sigma \in \text{hom}(G, G')$, тогда $\ker \sigma \leq G$ и $\text{Im } \sigma \leq G'$.

Nota bene Напомним, что отношением эквивалентности на произвольном множестве называется отношение, удовлетворяющее свойствам:

- рефлексивность: $\forall x \in M \quad x \sim x$;
- симметричность: $\forall x, y \in M \quad x \sim y \Rightarrow y \sim x$;
- транзитивность: $\forall x, y, z \in M \quad x \sim y, \quad y \sim z \Rightarrow x \sim z$.

Отношение эквивалентности разбивает множество M на непересекающиеся подмножества (классы эквивалентности). Множество классов эквивалентности по заданному отношению, называется фактор-множеством множества M по отношению \sim и обозначается M/\sim .

Лемма 2.5. Пусть G - группа и $H \leq G$. Тогда отношением эквивалентности является

$$x \sim y \Rightarrow xy^{-1} \in H.$$

►

Проверим свойства:

- $x \sim x : \quad xx^{-1} = e \in H$;
- $x \sim y \Rightarrow xy^{-1} = (yx^{-1})^{-1} \in H \Rightarrow yx^{-1} \in H \Rightarrow y \sim x$.
- $x \sim y, \quad y \sim z \Rightarrow xy^{-1}, yz^{-1} \in H \Rightarrow xy^{-1}yz^{-1} = xz^{-1} \in H \Rightarrow x \sim z$.

◄

Nota bene Из того, что $xy^{-1} \in H$ получаем

$$x \in Hy = \{hy : h \in H\} \Rightarrow \exists h_x \in H : h_x y = x.$$

|| Множество Hy называется **правым смежным классом** G по подгруппе H .

Лемма 2.6. Смежные классы, Hx и Hu , имеющие хотя бы один общий элемент, совпадают.



Пусть $z \in Hx$ и $z \in Hu$, тогда существуют $u, v \in H$, такие что $z = ux = vy$ и мы имеем:

$$ux = vy \Rightarrow x = u^{-1} \cdot v \cdot y, \quad u^{-1}v \in H$$

и тогда

$$Hx = Hu^{-1}vy = Hy.$$



Nota bene Смежные классы, соответствующие различным элементам $x \in G$ не пересекаются.

Nota bene Так как существует только один правый смежный класс, которому принадлежит элемент $x \in G$ целесообразно выбрать данный элемент представителем этого класса и записывать $[x]_R$. В зависимости от ситуации мы будем использовать как мультипликативную, так и аддитивную (для абелевых групп) форму записи для правых смежных классов:

$$[x]_R = Hx, \quad [x]_R = H + x.$$

Nota bene Аналогично правым смежным классам, могут быть определены **левые смежные классы** группы G по подгруппе H :

$$[x]_L = xH, \quad [x]_L = x + H.$$

|| Подгруппа H группы G называется **нормальной**, если

$$\forall x \in G \quad xH = Hx.$$

Nota bene Если H - нормальная подгруппа в G , то обычно пишут $H \triangleleft G$.

Nota bene Нормальной является любая подгруппа абелевой группы.

Nota bene В случае нормальной подгруппы имеем

$$\forall x \in G \quad [x]_R = [x]_L = \bar{x}.$$

Лемма 2.7. Пусть $\sigma \in \text{hom}(G, G')$, тогда $\ker \sigma \triangleleft G$.



Пусть $H = \ker \sigma$, тогда

$$e' = \sigma(x \cdot x^{-1}) = \sigma(x)\sigma(H)\sigma(x^{-1}) = \sigma(x \cdot H \cdot x^{-1}) \Rightarrow x \cdot H \cdot x^{-1} \subset H.$$

Замена $x \leftrightarrow x^{-1}$ дает

$$H \subset x \cdot H \cdot x^{-1} \Rightarrow H = x \cdot H \cdot x^{-1}$$



Лемма 2.8. Пусть $H \triangleleft G$, тогда G/H имеет структуру группы.



Для доказательства достаточно проверить групповые аксиомы:

1. Пусть $\bar{x}, \bar{y}, \bar{z} \in G/H$, тогда $(\bar{x}\bar{y})\bar{z} = \bar{x}(\bar{y}\bar{z})$:

$$(\bar{x}\bar{y})\bar{z} = (xH \cdot yH) \cdot zH = (xy)H \cdot zH = (xy)zH = x(yz)H = \bar{x}(\bar{y}\bar{z}).$$

2. H - нейтральный элемент G/H :

$$xH \cdot H = xH.$$

3. $x^{-1}H$ - обратный элемент к xH :

$$x^{-1}H \cdot xH = x^{-1}xH = eH = H.$$



|| Группа G/H называется **фактор-группой** группы G по нормальной подгруппе H

Теорема 2.1. Пусть $H \triangleleft G$, тогда существует такой гомоморфизм φ (называемый каноническим), что $\ker \varphi = H$.



Рассмотрим отображение

$$\varphi : G \rightarrow G/H, \quad \varphi(x) = xH,$$

и прямой проверкой убеждаемся, что

$$\varphi \in \text{hom}(G, G/H), \quad \ker \varphi = H.$$



Теорема 2.2. (Об изоморфизме) Пусть $\sigma : G \rightarrow G'$ - гомоморфизм групп, тогда

$$G/\ker \sigma \simeq \text{Im } \sigma.$$



Зададим отображение $\bar{\sigma} : G/\ker \sigma \rightarrow \text{Im } \sigma$

$$\bar{\sigma}(\bar{x}) = \sigma(x),$$

и покажем, что оно определено корректно. Именно, пусть $\bar{x} = \bar{y}$, тогда

$$\bar{\sigma}(\bar{y}) = \sigma(y) = \sigma(xx^{-1}y) = \sigma(x)\sigma(x^{-1}y) = \sigma(x)e = \sigma(x) = \bar{\sigma}(\bar{x}).$$

Далее, $\bar{\sigma}$ - гомоморфизм:

$$\bar{\sigma}(\bar{x}\bar{y}) = \sigma(xy) = \sigma(x)\sigma(y) = \bar{\sigma}(\bar{x})\bar{\sigma}(\bar{y}).$$

Тривиально проверяется, что $\text{Im } \bar{\sigma} = \text{Im } \sigma$, и остается прямой проверкой убедиться, что ядро $\bar{\sigma}$ тривиально:

$$\bar{z} \in \ker \bar{\sigma} \Rightarrow \sigma(z) = \bar{\sigma}(\bar{z}) = e \Rightarrow z \in \ker \sigma \Rightarrow \bar{z} = \bar{e}.$$

Таким образом, мы показали, что $\bar{\sigma}$ - изоморфизм.

