NOTE: меня не было на первой лекции, поэтому материал разбросан и беден на доказательства

О чем теория

Группа – это множество G с бинарной операцией $\star$ (которую я буду опускать в написании):
1. $(ab)c = a(bc)$ – ассоциативность
2. $\exists e : ae = ea = a$ – нейтральный элемент
3. $\forall a : \exists a^{-1} : aa^{-1} = a^{-1}a = e$ – обратный элемент

Группа абелева, если:
1. $ab = ba$ – коммутативна

- Сколько нейтральных элементов? Один.
- Сколько обратных элементов? Один.

Порядок группы – $|G|$, порядок элемента группы – $\operatorname{ord} a = \min\{k \in \mathbb{N} \mid a^k = e\}$. А если такого k нет? Тогда порядок бесконечен.

Подгруппа

Критерий подгруппы H:
1. H замкнуто относительно $\star$
2. H замкнуто относительно взятия обратного

А если группа G конечна? Тогда 1-ого условия хватит. А еще, определение распространяется на операции над подгруппами ($HH = H, H^{-1} = H$).

Пусть H подгруппа G, тогда aH – левый смежный класс G по H, порожденный a.

Свойства:
1. Всякий левый класс порождается своим элементом: $y \in xH \Rightarrow yH = xH$
   - $\exists h : y = xh \Rightarrow yH = xhH = xH$ в силу замкнутости относительно умножения.
2. Любые 2 левых класса либо не пересекаются, либо совпадают
3. G – дизъюнктное объединение левых смежных классов
4. Мощности всех классов смежности совпадают

Для правого смежного класса аналогично.

Теорема Лагранжа. Порядок любой подгруппы конечной группы G является делителем ее порядка. (очевидно следует из 3-ого свойства смежных групп)

Подгруппа нормальна, если левостороннее разложение G по H совпадает с правосторонним.

Критерий нормальности.

$$H \lhd G \Leftrightarrow \forall x \in G : xH = Hx \Leftrightarrow x^{-1}Hx = xHx^{-1} = H$$

Например, $SL_n(F) \lhd GL_n(F)$ ($\det A = 1$ и $\det A \neq 0$).
- $\forall A, X : \det A = 1 \land \det X \neq 0 : \det(X^{-1}AX) = \det A = 1$

Пересечение нормальных подгрупп – нормально.

Другие группы

Симметрические группы:
- X – произвольное множество
- $S(X) = \{\text{все биекции на себя}\}$, если $X = \{1, ..., n\}$, то это S_n – симметрические группы
- id – identity, или в Java – `UnaryOperator.identity()` (это нейтральный элемент)

Циклические группы – это группы, образованные одним элементом. Они, очевидно, абелевы. Пример: $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}$.

А теперь дадим другое определение, но сначала скажем про подгруппу, порожденную подмножеством M:

$\langle M\rangle = \bigcap H : H$ подгруппа $G, M \subset H$ или $\langle M\rangle = \{m_1^{\varepsilon_1}...m_s^{\varepsilon_s} \mid m_i \in M, \varepsilon_i \in \{-1,1\}\}$. *Или* требует доказательства, которое мы опустим.

Итак, группа G циклическая, если $\exists a \in G : G = \langle a\rangle$. Всякая конечная циклическая группа изоморфна чему? А бесконечная? Смотреть примеры.

Преобразования

Гомоморфизм $\varphi : G_1 \to G_2$ (сохраняет групповую структуру):
- $\forall a, b \in G_1 : \varphi(a \star b) = \varphi(a) \cdot \varphi(b)$
- Ядро – прообраз e, внезапно, нормальная подгруппа G_1
- Образ – подгруппа G_2

Еще немного гомоморфных отображений:
1. биекция – изоморфизм
2. если $G_1 = G_2$, то это эндоморфизм, а изоморфизм – автоморфизм
3. еще есть эпиморфизм (всегда есть прообраз) и мономорфизм (прообразы равных равны)

Теорема Кэли. Всякая конечная группа G изоморфна подгруппе S_n.

Идея доказательства: определим

$$\varphi(a_i) = \begin{pmatrix} a_1 & ... & a_n \\ a_i a_1 & ... & a_i a_n \end{pmatrix}$$

где, как нетрудно понять, вторая строка – i-тая строка в матрице Кэли (еще это можно назвать сдвигом на элемент a_i). Свойства гомоморфизма проверяются, а изоморфизм из-за тривиальности ядра.

Коммутатор и коммутант

Коммутатор элементов x, y – произведение $[x, y] = xyx^{-1}y^{-1}$, пару свойств:
1. $xy = [x, y]yx$
2. x, y коммутируют $\Leftrightarrow [x, y] = e$
3. $[x, y]^{-1} = [y, x]$

Если $\varphi : G \to A$ – гомоморфизм в абелеву группу, то $\varphi[x, y] = [\varphi(x), \varphi(y)] = e$.

Коммутант (производная подгруппы) – $[G, G] = \langle [x, y] \mid x, y \in G\rangle$. С ними связано много интересного, отметим следующее
- $\varphi : G \to H$ – гомоморфизм, тогда $\varphi(G')$ подгруппа H' (уважает производные подгруппы)
- эпиморфизм сохраняет производные подгруппы

Абеленизацией группы G называется ее факторгруппа по коммутанту – $G^{ab} = G/[G, G]$

Забегая наперед, абеленизация свободной группы F_n *превращает* ее в свободную абелеву группу $\mathbb{Z}^n$.

Свободная группа

Давайте предъявим строковую интуицию: множество $S = \{a, b, c\}, T = S \cup S^{-1} = \{a^{-1}, b^{-1}, c^{-1}, a, b, c\}$. А так же *пустая* строка ε и операция конкатенации. Предъявим так же и редукцию (понятно, что она делает).

Тогда свободной группой F_S является группа редуцированных строк над S с операцией конкатенации:
- все свободные группы, порожденные равномощными множествами, изоморфны (ее ранг – мощность пораждающего множества)
- любая подгруппа свободной группы свободна
- коммутант свободной группы конечного ранга имеет бесконечный ранг. Например, коммутант порождённой двумя элементами свободной группы $F(a, b)$ – это свободная группа коммутаторов $[a^n, b^m]$

Для любой группы G и любого отображения множеств $f : S \to G$ существует единственный гомоморфизм групп $\varphi : F_S \to G$, для которого следующая диаграмма коммутативна:

$$\begin{tikzcd}
S \arrow[r] \arrow[d, "f"] & F_S \arrow[dl, dashed, "\varphi"] \\
G &
\end{tikzcd}$$

Таким образом, существует взаимно однозначное соответствие между множествами отображений $S \to G$ и гомоморфизмов $F_S \to G$.

Дополнительно

Группы Бернсайда

Давайте вспомним циклические группы. Если допустить m образующих элементов и такое число n, что $\forall a \in G : a^n = e$, то полученный класс групп называется группой Бернсайда и обозначается как $B(m, n)$

Чем они интересны? А тем, (во-первых) что это нерешенная проблема – точно знаем, что есть и конечные, и бесконечные группы, но ничего не знаем, например, про $B(2, 5)$.

А что еще знаем? $\forall m : B(m, 3), B(m, 4), B(m, 6)$ конечны. В качестве упражнения можно поизучать $B(2, 2)$, на чем небольшое комбинаторное отступление заканчивается.

Копредставление группы

Очень неформально – это запись вида $G = \langle S \mid R \rangle$, где S – множество образующих (как в свободных группах), а R – множество уравнений, которые определяют, как образующие взаимодействуют друг с другом

1. $\mathbb{Z}_n = \langle a \mid a^n = e \rangle$
2. группа диэдра D_n (группа симметрий правильного n-угольника)
   - $D_n = \langle r, s \mid r^n = e, s^2 = e, srs = r^{-1} \rangle$, где r, s – поворот на $\frac{2\pi}{n}$ и отражение

Точные последовательности

Это последовательности алгебраических объектов G_i с последовательностью гомоморфизмов, такие что образ φ_{i-1} совпадает с ядром φ_i

- точные последовательности вида $0 \to A \to B \to C \to 0$ – короткие (что можно сказать об имеющихся здесь гомоморфизмах?)
- длинная – точная с бесконечным числом объектов

Например,

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{f} \mathbb{Z}_6 \xrightarrow{g} \mathbb{Z}_3 \longrightarrow 0$$

- тривиальный гомоморфизм переводит 0 в образ 0 – ядро f
- $f = 3x$ переводит $\mathbb{Z}_2$ в образ $\{0, 3\}$, что является ядром $g = x \bmod 3$
- очевидно

А еще можно заметить, что композиция $g \circ f$ – тривиальна. Более подробно об этом рассказывается на курсе гомологий.