В данной лекции операцией на группе всегда будет умножение, кроме тех случаев, когда ей будет пятиконечная звезда или звезда Давида.

1 Как задавать группу?

Определение 1. Подгруппой группы G называется ее подмножество H, являющееся группой относительно операции в группе G. Обозначение: $H \leq G$.
Утверждение 1. Подмножество H группы G является подгруппой тогда и только тогда, когда оно замкнуто относительно операций умножения и взятия обратного, то есть $\forall a, b \in H$

1. $a \cdot b \in H$;
2. $a^{-1} \in H$.

Следствие 1. Пересечение любого набора подгрупп — подгруппа.
Задание группы порождающими. Во множестве ситуаций, рассматривая группу, нам хочется иметь какой-то ограниченный и удобный для работы набор элементов, через которые мы сможем выразить все остальные элементы группы.
Определение 2. Пусть M — произвольное подмножество в группе G. Рассмотрим пересечение всех подгрупп G, содержащих M: это подгруппа (*Следствие 1*), порожденная множеством M. (Ясно, что у одной и той же подгруппы могут быть различные порождающие множества).
Подгруппу, порожденную множеством M, будем обозначать $\langle M \rangle$. Если подгруппа, порожденная множеством M, совпадает со всей группой G, то M — порождающее множество для группы G.
Теорема 1. Если M — подмножество группы G, то $\langle M \rangle = \{a_1^{\epsilon_1} \cdot \dots \cdot a_s^{\epsilon_s} | a_i \in M, \epsilon_i = \pm 1, s = 1, 2, \dots\} = H$.
Доказательство. Подгруппа $\langle M \rangle$ содержит все $a_i \in M$, их произведения и обратные, а стало быть и все множество H; значит, $H \subset \langle M \rangle$. Но согласно *Утверждению 1* H — подгруппа, содержащая $\langle M \rangle$, значит, из определения подгруппы, порожденной множеством M, $\langle M \rangle \subset H$. Значит, $\langle M \rangle = H$.
Примеры: $\mathbb{Z}, \mathbb{Q}, S_n, \mathbb{Z}/n\mathbb{Z}$.
Соотношения. При задании подгруппы порождающими множествами мы должны учитывать, как именно устроено умножение элементов в этом порождающем множестве: может оказаться, что на перемножение некоторых элементов наложены определенные условия. Например: если a — элемент порождающего множества M, а a^{-1} — обратный к нему элемент, то выполняется условие $a \cdot a^{-1} = 1$. Могут возникнуть и какие-то другие условия на произведение элементов M, например, $a \cdot b \cdot c^{-1} \cdot a^{-1} \cdot d = d \cdot a^{-1}$; заметим сразу, что, домножая последовательно обе части уравнения слева на обратный к первому в правой части элемент, можно всегда записывать эти условия в виде "произведение каких-то элементов равно единице". Такие условия на умножение называются *соотношениями* в группе. Соотношения вида $a \cdot a^{-1} = 1$, выполняющиеся в любой группе, называют *тривиальными* соотношениями.
Примеры:

1. Абелева группа — это группа, в которой выполняются соотношения $\forall a, ba \cdot b \cdot a^{-1} \cdot b^{-1} = 1$, то есть, равносильно, $a \cdot b = b \cdot a$.
2. Циклическая группа $\mathbb{Z}/n\mathbb{Z}$ порядка n — это абелева группа, порожденная одним элементом a, с дополнительным соотношением $a^n = 1$. Как следствие, в этой группе для любого элемента b выполняется соотношение $b^n = 1$.

2 Эквивалентность

Определение 3, *в которое здесь можно не вдумываться.* Отношение эквивалентности между объектами — такое отношение " $\sim$ ", для которого выполняются три свойства:

1. $a \sim a$ (Рефлексивность);
2. Если $a \sim b$, то $b \sim a$ (Симметричность);
3. Если $a \sim b$ и $b \sim c$, то $a \sim c$ (Транзитивность).

Если для какого-то отношения $\sim$, заданного на произвольном множестве A, все эти три свойства выполняются, то $\sim$ называют *отношением эквивалентности* на этом множества, а элементы $a \sim b$ — эквивалентными. Говоря нестрого, отношение эквивалентности — это некоторое обобщение равенства двух элементов: элементы эквивалентны, когда они в каком-то смысле одинаковые, и поэтому они должны удовлетворять основным свойствам, которым удовлетворяют одинаковые объекты.
Примеры.

1. Равенство двух чисел является отношением эквивалентности; более того, равенство иных объектов (например, геометрических фигур) — отношение эквивалентности.
2. Сравнимость по фиксированному модулю (это тоже некоторое обобщение понятия равенства) $a \equiv b$ является отношением эквивалентности.
3. Отношение геометрического подобия является отношением эквивалентности; отношение $\parallel$ параллельности двух прямых или двух плоскостей является отношением эквивалентности.
4. Отношение «"(отношение строгого линейного порядка) на множестве рациональных чисел НЕ является отношением эквивалентности: оно тразитивно, но не рефлексивно (неверно, что $a < a$) и не симметрично.
5. Отношение "$\leq$"(отношение нестрогого линейного порядка) на множестве действительных чисел НЕ является отношением эквивалентности: действительно, оно рефлексивно и транзитивно, но не симметрично (из того, что $a \leq b$, не следует $b \leq a$).

Определение 4. Фиксируем какое-то конкретное отношение эквивалентности на множестве X. Классом эквивалентности элемента a называется множество всех элементов, эквивалентных a, обозначение: $[a] = \{x \in X | x \sim a\}$.
Класс эквивалентности можно тоже рассматривать как элемент некоторого множества (множества классов эквивалентности элементов X). Более того: если на множестве X определена операция " $\cdot$ ", сохраняющая эквивалентность элементов (то есть: если $a \sim b$ и $x \sim y$, то $a \cdot b \sim x \cdot y$), можно определить согласованную с ней операцию и на множестве классов эквивалентности.

3 О свободной группе

Важный пример 1. Рассмотрим множество слов из букв конечного алфавита $\{a_1, a_2, \ldots, a_m, a_1^{-1}, a_2^{-1}, \ldots, a_m^{-1}\}$ (то есть множество из элементов вида $a_{i_1}^{k_1} \ldots a_{i_s}^{k_s}$, где k_j — целые числа, обозначающие количество подряд идущих одинаковых элементов) и такое отношение эквивалентности: слова называются эквивалентными, если их можно перевести друг в друга последовательным добавлением или удалением кусков вида $x^k x^{-k}$ или $x^{-k} x^k$.
Введем следующую операцию умножения на словах: если u и v — два слова, то их произведение $u \cdot v = uv$ — слово, полученное приписыванием слова v справа к слову u (такая операция называется операцией *конкатенации*. Несложно проверить, что такая операция сохраняет эквивалентность элементов из *важного примера 1*: если мы могли добавить и

удалить несколько тривиальных кусков из частей слов, чтобы они стали разные, мы сможем сделать то же самое и в случае, когда они приписаны друг к другу. Значит, теперь мы можем в качестве нашего множества (чтобы у нас не было различных "одинаковых то есть эквивалентных, элементов) брать множество классов эквивалентности слов (и производить с ними те же операции, что и с самими словами). Чтобы не вводить громоздких обозначений, писать мы все равно будем сами слова (и обычно в несократимой записи — то есть без тривиальных кусков вида $x^k x^{-k}$).

Упражнение. Доказать, что у любого слова существует ровно одна несократимая запись, то есть запись без участков вида $x^k x^{-k}$, которые можно удалять.

Несложно понять, что в группе с порождающими $a_1, a_2, \ldots, a_m$ любой элемент может быть записан как слово над соответствующим алфавитом (возможно, не единственным способом); и если в группе нет никаких соотношений, кроме тривиальных, его можно записать единственным образом в виде несократимого слова (иначе говоря — единственным образом сопоставить ему класс эквивалентности его слов, ведь мы выяснили, что классу эквивалентности однозначно сопоставляется несократимое слово). Мы готовы ввести

Определение 5. Свободная группа — это порожденная некоторым множеством M группа, между порождающими которой нет никаких соотношений, кроме тривиальных.

Теорема 2. Для любого множества порождающих $M = \{a_i | i \in I\}$ существует свободная группа, порожденная этим множеством; она состоит из всевозможных несократимых слов над этим алфавитом (или, что то же самое, из классов эквивалентности таких слов, определенных выше) с операцией "склеивания"(конкатенации).

Доказательство. Нейтральным элементом группы является пустое слово (класс эквивалентности любого тривиального слова, например, $[aa^{-1}]$; обратным к слову $a_{i_1}^{k_1} \ldots a_{i_s}^{k_s}$ будет слово $a_{i_s}^{-k_s} \ldots a_{i_1}^{-k_1}$. Осталось проверить, что все аксиомы группы выполняются.

Упражнение. Свободные группы с двумя и более порождающими некоммутативны.

Важный пример 2. Пусть на элементах алфавита $\{a_1, a_2, \ldots, a_m, a_1^{-1}, a_2^{-1}, \ldots, a_m^{-1}\}$ задан некий набор соотношений (возможно, не только тривиальных), то есть набор равенств между некоторыми словами. Введем на словах из *важного примера 1* новое отношение эквивалентности: мы считаем слова эквивалентными, если можно заменой в одном из слов некоторых кусков на равные (в соответствии с соотношениями) превратить его во второе. Аналогично с *важным примером 1*, на классах эквивалентности таких слов можно определить операцию "склеивания а затем и доказать, что они образуют группу.

Определение 6. Пусть ψ — множество соотношений на множестве M. Группой, порожденной порождающим множеством M и множеством порождающих соотношений ψ, называется группа $\langle M|\psi\rangle$ классов эквивалентностей слов (построенных по порождающим соотношениям ψ) с операцией конкатенации.

В частности, тривиальные соотношения ψ порождают свободную группу.

4 Гомоморфизмы

Мы не будем подробно изучать отображения между группами, а лишь кратко напомним основные определения.

Определение 7. Пусть даны две группы $(G, \star)$ и $(H, \bigstar)$. Отображение $\varphi : G \longrightarrow H$ называется *гомоморфизмом групп*, если для любых a, b из G $\varphi(a \star b) = \varphi(a) \bigstar \varphi(b)$.

Упражнение. Доказать: образ единицы в группе G при гомоморфизме — единица в группе H.

Упражнение. Доказать: образ группы G при гомоморфизме — подгруппа в группе H.

Определение 8. *Изоморфизмом групп* называется взаимно-однозначный гомоморфизм.

Упражнение. Доказать: гомоморфизм является изоморфизмом тогда и только тогда, когда у него существует обратный.
Упражнение. Доказать: любые две свободные группы с одинаковым количеством порождающих изоморфны, то есть между ними можно построить отображение φ, являющееся изоморфизмом.
Определение 9. *Эндоморфизмом* группы G называется ее гомоморфизм в саму группу G, то есть такой гомоморфизм (из определения 7), в котором группы G и H совпадают.
Автоморфизмом группы G называется ее изоморфизм в саму группу G.
Важное упражнение. Пусть $M = \{a_1, \ldots, a_m\}$ — порождающее множество группы G и на элементах множества M задано отображение φ: $M \longrightarrow G$. Доказать, что φ продолжается до эндоморфизма группы G (то есть что существует эндоморфизм $\psi : G \longrightarrow G$, который элементы множества M переводит туда же, куда и φ.

5 Подгруппы, выдерживающие гомоморфизмы

Определение 10. Подгруппа $H \leq G$ *выдерживает эндоморфизм (автоморфизм)* φ группы G, если $\varphi(H) < H$.
Определение 11. Подгруппа H группы G называется *характеристической*, если она выдерживает все автоморфзимы группы G.
Подгруппа H группы G называется *вполне характеристической*, если она выдерживает все эндоморфзимы группы G.
Пусть V — некоторое множество слов $\{x_{i_1}, \ldots, x_{i_s}\}$ над некоторым алфавитом X. Множество $V(G)$ зададим так: оно состоит из всевозможных слов, полученных из слов множества V в результате подстановки вместо каждого из x_i какого-то элемента множества G.
Определение 12. Подгруппа $V(G)$ группы G называется *вербальной* подгруппой группы G, построенной по множеству слов V.
Упражнение. Проверить, что $V(G)$ — действительно подмножество в G и подгруппа в G.
Утверждение 2. Вербальная подгруппа является вполне характеристической.
Доказательство. Пусть φ — эндоморфизм группы G. Все элементы подгруппы $V(G)$ имеют вид $u = v(g_1, \ldots, g_m)$ для каких-то $g_i \in G$ и $v \in V$. Тогда $\varphi(u) = v(\varphi(g_1), \ldots, \varphi(g_m)) = v(h_1, \ldots, h_m)$ при некоторых $\varphi(g_i) = h_i \in G$, а такие элементы по определению лежат в $V(G)$. $V(G)$ сохраняется при любое эндоморфизме группы G, а значит является вполне характеристической подгруппой G.
Упражнение. Доказать: вербальная подгруппа вербальной подгруппы вербальна во всей группе.
Теорема. Если группа G свободная, то её вербальные подгруппы — это в точности вполне характеристические подгруппы.
Доказательство. Докажем, что все вполне характеристические подгруппы вербальны:
$M = \{a_1, \ldots, a_m\}$ — какая-то система порождающих свободной группы G, H — ее вполне характеристическая подгруппа. Рассмотрим множество V, состоящее из всех слов $v(x_1, \ldots, x_m)$, для которых $v(a_1, \ldots, a_m) \in G$: такое слово можно построить по каждому элементу группы G, просто заменив порождающие a_i на буквы x_i. При подстановке в V вместо букв порождающих из M мы заведомо получим все слова из H, значит, $H \subset V(G)$. Обратно, пусть $v \in V$; докажем, что $v(g_1, \ldots, g_m) \in H$:
$v \in V$, поэтому $v(a_1, \ldots, a_m) \in H$. Построим отображение $\varphi : a_i \longrightarrow g_i$. Из *важного упражнения* φ можно продолжить до эндомоморфизма ψ группы G, при котором, в частности, $v(a_1, \ldots, a_m) \longrightarrow v(g_1, \ldots, g_m)$. Но подгруппа H — вполне характеристическая, и она выдерживает эндоморфизмы G; в частности, $v(g_1, \ldots, g_m) \in H$.
То, что все вербальные подгруппы являются вполне харакретистическими, в общем случае доказано в утверждении 2.

6 Где про это почитать

1. М. И. Каргаполов, Ю. И. Мерзляков: Основы теории групп — гл. 1, 2, 5;
2. А. Г. Курош: Теория групп — гл. 1, 2, 4, 5;
3. Lectures on Topics In The Theory of Infinite Groups By B.H. Neumann — Chapter 2, 4, 5;
4. Что-то близкое и много полезного можно найти в лекциях спецкурса А. А. Клячко и О. В. Куликовой "Теория Групп": они выложены на сайте спецкурса, http://halgebra.math.msu.su/staff/klyachko/sk.htm