Группы. Словарик.

Предупреждение. Этот текст НЕ является записью лекции! Здесь лишь собраны наиболее употребительные определения и теоремы, а также приведены несколько упражнений на понимание определений.

Доказательства многих теорем из курса (а также многих других!) можно изучить по книгам:

- С. Ленг. Алгебра. М., 1968.
- Б. Л. ван дер Варден. Алгебра. М., 1976. (См. также первое издание: Б. Л. ван-дер-Варден. Современная алгебра. М.–Л., 1947.)

Определение 1. Множество натуральных чисел $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Обозначения. Множество целых чисел обозначается $\mathbb{Z}$. Множество рациональных чисел обозначается $\mathbb{Q}$. Множество действительных чисел обозначается $\mathbb{R}$. Множество комплексных чисел обозначается $\mathbb{C}$.

Определение 2. *n-арная операция* на множестве M — это отображение $o\colon \underbrace{M \times M \times \ldots \times M}_{n \text{ сомножителей}} \to M$.

Определение 3. Множество M с бинарной операцией $a, b \mapsto a \circ b$ и выделенным элементом e называется *моноидом*, если:

1) Для любых $a, b, c \in M$ верно равенство $(a \circ b) \circ c = a \circ (b \circ c)$.
2) Для любого $a \in M$ верны равенства $a \circ a = e \circ a = a$.

В этом случае e называют *нейтральным элементом*, или *единицей*. Первое свойство называется *ассоциативностью* бинарной операции. Если для любых $a, b \in G$ верно равенство $a \circ b = b \circ a$, то моноид называется *коммутативным*, или *абелевым*.

(По аналогии с числами бинарную операцию часто называют умножением, и точку между сомножителями пропускают. Если неясно, какая бинарная операция имеется в виду, пишут $(M, \circ)$.)

Пример 1. Все отображения данного множества в себя образуют моноид относительно операции композиции. Также моноидами являются $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$.

Определение 4. Множество G с бинарной операцией $a, b \mapsto a \circ b$, унарной операцией $a \mapsto a^{-1}$ и выделенным элементом e называется *группой*, если:

1) Для любых $a, b, c \in G$ верно равенство $(a \circ b) \circ c = a \circ (b \circ c)$.
2) Для любого $a \in G$ верны равенства $a \circ a^{-1} = a^{-1} \circ a = e$.
3) Для любого $a \in G$ верны равенства $a \circ a = e \circ a = a$.

Названия здесь такие же как и для моноида: e называют *нейтральным элементом*, или *единицей*. Первое свойство называется *ассоциативностью* бинарной операции. Если для любых $a, b \in G$ верно равенство $a \circ b = b \circ a$, то группа называется *коммутативной*, или *абелевой*. Элемент a^{-1} называется *обратным* к элементу a.

Пример 2. Остатки по модулю N с операцией сложения образуют группу, которая обозначается $\mathbb{Z}/N\mathbb{Z}$. (Более научно: рассмотрим множество, каждый элемент которого есть множество целых чисел вида $a + Nk, k \in \mathbb{Z}$, для некоторого $a \in \mathbb{Z}$. На этом множестве можно ввести структуру группы (проделайте это!).) Также являются группами $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\{\pm 1\}, \cdot)$. Перестановки n элементов (взаимно однозначные отображения n-элементного множества в себя) образуют группу относительно операции композиции. Эта группа обозначается по-разному: S_n, Σ_n, $\mathfrak{S}_n$.

Определение 5. Отображение групп $\varphi\colon G \to H$ называется *гомоморфизмом*, если для любых $a, b \in G$ верно равенство $\varphi(ab) = \varphi(a)\varphi(b)$.

Упражнение 1. Докажите, что в этом случае для любого $a \in G$ верно равенство $\varphi(a^{-1}) = \varphi(a)^{-1}$. (Или, что эквивалентно, $\varphi(e_G) = e_H$, где e_G и e_H — единицы в группах G и H соответственно.)

Пример 3. Отображение, сопоставляющее перестановке её чётность, является гомоморфизмом в группу $\mathbb{Z}/2\mathbb{Z}$. (См. соответствующую задачу в листке.) Вложение $(\mathbb{Z}, +) \to (\mathbb{Q}, +)$ является гомоморфизмом. Для любого целого числа N отображение $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto Na$, является гомоморфизмом. Отображение $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, $a \mapsto a \bmod N$, является гомоморфизмом.

Определение 6. *Ядро* гомоморфизма есть множество элементов $g \in G$, для которых $\varphi(g) = e_H$. (Ядро гомоморфизма φ обозначается $\operatorname{Ker}\varphi$.) *Образ* гомоморфизма φ есть множество элементов группы H вида $\varphi(g)$, $g \in G$. (Образ гомоморфизма φ обозначается $\operatorname{Im}\varphi$.)

Упражнение 2. Ядро и образ любого гомоморфизма — подгруппы в соответствующих группах.

Определение 7. Гомоморфизм групп называется *изоморфизмом*, если он является биекцией. (Обозначение: $G \simeq H$.)

Определение 8. Изоморфизм $\varphi\colon G \simeq G$ называется *автоморфизмом*.

Упражнение 3. Пусть дан элемент g группы G. Проверьте, что отображение $\varphi_g\colon G \to G$, $\varphi_g(h) = ghg^{-1}$, является автоморфизмом группы G. Такие автоморфизмы называются *внутренними*.

Определение 9. Подмножество группы называется подгруппой, если оно замкнуто относительно умножения и взятия обратного элемента. Подгруппа H группы G называется *нормальной*, если она сохраняется (как множество) всеми внутренними автоморфизмами группы G: для любых $g \in G, h \in H \;\; ghg^{-1} \in H$.

Упражнение 4. Ядро гомоморфизма в любую группу является нормальной подгруппой. Подгруппа абелевой группы нормальна.

Определение 10. Пусть G — группа, H — её подгруппа. Определим отношение эквивалентности на группе G: $g_1 \sim g_2$, если $g_1 = hg_2$ для некоторого $h \in H$. Классы эквивалентности (класс эквивалентности элемента g — это множество $\{g_1 \mid g_1 \sim g\}$) называются *правыми смежными классами* группы G по подгруппе H. Аналогично определяются *левые смежные классы.* Соответствующие разбиения группы на классы называются *левым и правым разложением* по подгруппе H.

Упражнение 5. Число элементов в каждом смежном классе равно числу элементов в группе. Любые два смежных класса либо не пересекаются, либо совпадают (это общее свойство классов эквивалентности).

Определение 11. *Порядком* (конечной) группы называется число элементов этой группы.

Теорема 1. Пусть G — конечная группа, H — её подгруппа. Тогда порядок подгруппы H является делителем порядка группы G. (Кстати, целое число $\frac{\#G}{\#H}$ называется *индексом* H в G.)

Упражнение 6. Пусть дан элемент a некоторой группы и целое число k. Дайте определение элемента a^k.

Определение 12. Группа G называется *циклической*, если она порождена одним элементом,т. е. существует $a \in G$, такое что для каждого

$b \in G$ существует $k \in \mathbb{Z} \colon b = a^k$.

Пример 4. Группы $\mathbb{Z}$ и $\mathbb{Z}/N\mathbb{Z}$ — циклические.

Определение 13. Целое положительное число k называется *порядком* элемента a, если $a^k = e$, и это наименьшее целое положительное число с таким свойством.

Теорема 2. Порядок любого элемента группы является делителем порядка группы. (Доказательство: рассмотрите циклическую подгруппу, порождённую этим элементом.)

Упражнение 7. Подгруппа является нормальной тогда и только тогда, когда левое разложение по ней совпадает с правым.

На смежных классах по нормальной подгруппе есть структура группы: для того, чтобы перемножить два смежных класса, надо выбрать по представителю, перемножить их и рассмотреть смежный класс, содержащий их произведение.

Упражнение 8. Проверьте, что этим задаётся структура группы (в частности, определите обратный элемент и единицу).

Определение 14. Построенная группа называется *факторгруппой* группы G по подгруппе H и обозначается G/H.

Пример 5. Обозначение $\mathbb{Z}/N\mathbb{Z}$ не напрасно: эта группа действительно является факторгруппой группы целых чисел по подгруппе чисел, которые делятся на N.

Теорема 3. Пусть $\varphi \colon G \to H$ — гомоморфизм групп. Тогда имеет место изоморфизм $\operatorname{Im}\varphi \simeq G/\operatorname{Ker}\varphi$. («Гомоморфный образ группы // Каноническим морфизмом // Изоморфен факторгруппе // По ядру гомоморфизма.»)