1 Группы

1.1 Общие понятия и примеры

Группа – это множество с одной ассоциативной обратимой бинарной операцией.

Если операция коммутативна, то группа называется абелевой.

- Бесконечные группы:
  - Бесконечные абелевы группы
    - $(Z,+)$; $(Q,+)$; $(R,+)$; $(C,+)$
    - $(Q^* = Q\backslash\{0\},\cdot)$; $(R^*,\cdot)$; $(C^*,\cdot)$
  - Бесконечные неабелевы группы
    - $(GL(n) = \{A : det\ A \neq 0\},\cdot)$
    - $(SL(n) = \{A : det\ A = \pm 1\},\cdot)$
    - $(SL_+(n) = \{A : det\ A = 1\},\cdot)$
    - $(O(n) = \{A : A \cdot A^T = E\},\cdot)$; $O(n) \subset SL(n)$ (почему?)
    - $(SO(n) = \{A : A \in O(n),\ det\ A = 1\},\cdot)$
- Конечные группы:
  - Конечные абелевы группы
    - $(Z/nZ = Z_n,+)$
    - $((Z/pZ)^* = Z_p^*,\cdot);\ p -$ простое число (доказать!)
  - Конечные неабелевы группы
    - $(S_n,\cdot) -$ группа перестановок n элементов

Число $|G|$ элементов конечной группы G называется порядком группы.

Минимальное положительное число n, такое что $a^n = e\ -$ называется порядком элемента $a \in G$

$|S_n| = n!$

Любая конечная группа порядка n может быть вложена в группу S_n

Два способа задания конечной группы:

1. Таблица умножения (сложения)
2. Образующие и соотношения

Пусть G – группа и $S \subset G$. Тогда множество:

$$< S > = \{s_1 \cdot \ldots \cdot s_k \ : \ s_i \in S \text{ или } s_i^{-1} \in S\}$$

является (почему?) подгруппой и называется подгруппой, порожденной S, а S называется порождающим множеством для $< S >$

2 Циклические группы

Если все элементы группы являются степенями одного элемента, то группа называется циклической, а соответствующий элемент – образующей. Циклическая группа – абелева. Все циклические группы одного порядка изоморфны. Количество различных образующих циклической группы порядка n равно $\varphi(n)$, где φ – функция Эйлера ($\varphi(n)$ – количество чисел меньших n и взаимно простых с n).

3 Некоторые свойства групп

Пусть p – простое число, делящее порядок группы

1. Любая группа G порядка n может быть реализована как подгруппа в S_n (теорема Кэли)
2. Порядок подгруппы делит порядок группы (теорема Лагранжа)
3. Порядок элемента делит порядок группы (2 $\Rightarrow$ 3)
4. В группе существует элемент (подгруппа) порядка p
5. Если $|G| = p^n \cdot m$ и $(p^n, m) = 1$, то существует подгруппа порядка p^n (силовская подгруппа)
6. Существует единственная (с точностью до изоморфизма) группа простого порядка – циклическая