初等数论, 群

请在 10 月 16 日课前提交纸质作业.

1. (10 分) (1) 求 $\gcd(10^6-1, 10^{15}-1)$.

   (2) 设自然数 $n, m \geq 1$，证明：$\gcd(2^m-1, 2^n-1) = 2^{\gcd(m,n)}-1$.

2. (10 分) 对实数 $x \in \mathbb{R}$，定义

$$\mu(x) = \inf\left\{\alpha \in \mathbb{R} : \left|x - \frac{p}{q}\right| \leq \frac{1}{q^\alpha} \text{ 仅有有限组互素整数解 } (p,q), q > 0\right\}.$$

   证明：对 $x \in \mathbb{Q}$，$\mu(x) = 1$.

   提示：首先证明 $\mu(x) \geq 1$，然后考虑 $|x - p/q| \leq 1/q^{1+\epsilon}$ 的解个数，进而证明 $\mu(x) < 1 + \epsilon$.

3. (5 分) 已知群 G 满足 $\forall g \in G, g^2 = e$. 证明 G 是阿贝尔群.

4. (10 分) 设 G 是一个有限阿贝尔群，证明以下命题

   (1) $\prod_{g\in G} g$ 的平方等于单位元 e.

   (2) 如果 G 中没有阶（order）为 2 的元素，或 G 中有超过一个阶为 2 的元素，那么 $\prod_{g\in G} g = e$.

   (3) 如果 G 中唯一的阶（order）为 2 的元素 y，那么 $\prod_{g\in G} g = y$.

   (4) (Wilson's theorem) 如果 p 是素数，$(p-1)! \equiv -1 \mod p$.

5. (10 分) 形如 $aba^{-1}b^{-1}$ 被称作 a, b 的换位子. 给定群 G, 定义它的换位子群（commutator subgroup）$G' = \langle aba^{-1}b^{-1} : a, b \in G\rangle$ 为所有换位子生成的群.

   (1) 证明：$G' \trianglelefteq G$.

   (2) 考虑 $N \trianglelefteq G$，证明：G/N 是 Abel 群当且仅当 $G' \leq N$.

   (3) 考虑 Sym(4)，即 $\{1,2,3,4\}$ 上的对称群，请给出一个序列：

$$S_4 = G^0 \triangleright G^1 \triangleright \cdots \triangleright G^n = \{1\},$$

   满足 G^i/G^{i+1}（$i = 0, \ldots, n-1$）是 Abel 群.

6. (5 分) 考虑集合 S 与 S 上的二元运算 $\cdot$. 如果 $\cdot$ 满足结合律, 那么 $(S, \cdot)$ 构成半群 (semigroup). 如果还存在单位元, 那么称作幺半群 (monid). 如果还存在逆元, 那么就是群.

   假设半群 $(S, \cdot)$ 额外满足

   - 对称性 $\forall a \forall b\ a \cdot b = b \cdot a$
   - 消去律 $\forall a \forall b \forall c\ a \cdot b = a \cdot c \to b = c$

   证明, 可以将 S 嵌入一个群 G 中. 也就是存在群 $(G, \star)$, 满足 $S \subseteq G$ 且 $\forall a \forall b\ a \cdot b = a \star b$.