0.1 Group

10. Given a monoid G, b is the inverse of an element a in G iff the equations below hold:

$$aba = a \qquad ab^2a = 1 \tag{1}$$

proof. It is clear that a is a bijective if you view an element of the monoid as a function.

Therefore there exists the inverse of a. Then $ba = 1$ holds.We have

$$ab \cdot ba = ab \cdot 1 = 1$$

which indicates $ab = 1$ as well. □

11. Let G be a finite group, and $|G| = n$. $a_1, a_2, \ldots, a_n$ are n random elements in G, which does not necessarily differ pairwise. Proof that exists p, q suit that $1 \leq p \leq q \leq n$ s.t.

$$a_p a_{p+1} \ldots a_q = 1$$

proof. Consider $b_j = \prod_{i=1}^{j} a_i, j = 1, \ldots, n$. Either b_js differ pairwise, or there exists j_1, j_2 s.t. $b_{j_1} = b_{j_2}$ □

12. Proof that $x^2 = 1$ has even number of roots in a group of n order.

证明. 考虑一个等价关系: $x \sim y \iff x = y \text{ or } y = x^{-1}$. 可以证明出 2 阶群元的个数只有奇数个. □

13. G 是 n 阶有限群, S 是 G 的子集, 若 $|S| > n/2$ 则 $\forall g \in G(\exists a, b \in S(g = ab))$

证明. 可以证明 $|S| > n/2 \to 1 \in S$, 之后用得到. 随后使用反证法, 设存在 $g \in G$, 不存在 $a, b \in S$ 使得 $ab = g$.

如果说 $g \in S$ 则和 $1 \in S$ 矛盾.

如果说 $g \notin S$, 那么下面命题成立

$$c \in S \to gc^{-1} \notin S$$

这足够说明 $|S| \leq n/2$ 了. $\square$

18. 证明 $(\mathbb{Q}, +)$ 和 $(\mathbb{Q}^+, *)$ 不同构, 而 $(\mathbb{R}, +)$ 和 $(\mathbb{R}^+, *)$ 同构.

证明. 设同构存在, 记为 $\varphi : (\mathbb{Q}, +) \to (\mathbb{Q}^+, *)$. 存在 x s.t. $\varphi(x) = 2$. 此时, $x = x/2 + x/2$, 那么 $\varphi(x) = \varphi(x/2 + x/2) = \varphi(x/2) * \varphi(x/2) = 2$, 可是有理数之中并不存在 y s.t. $y * y = 2$. $\square$

19. G 是有限群. $\alpha \in \mathrm{Aut}(G)$ 除了幺元之外没有不动点, 即, $\alpha(x) = x \implies x = 1$, 证明 G 是奇数阶的阿贝尔群.

证明. 考虑 $x \sim y \iff x = \alpha(y)$ or $x = y$. 能够证明 $|G|$ 是奇数.

其次, 我们需要证明 $\alpha(x) = x^{-1}$. 该条件等价于对于任意的 $g \in G, \exists h \in G$ s.t. $g = h^{-1}\varphi(h)$.

$$g = h^{-1}\varphi(h) \qquad \varphi(g) = \varphi(h)^{-1}h = g^{-1}$$

随后, 为了证明 $\forall g \in G, \exists h \in G(g = h^{-1}\varphi(h))$ 成立, 我们需要证明 $\sigma\colon G \to G, k \mapsto k^{-1}\varphi(k)$ 是一个满射. $\square$