

NIS2312-1 Spring 2021-2022

信息安全的数学基础 (1)

Assignment 1

2022 年 2 月 17 日

Problem 1

设集合 $S = \{(a, b) | a, b \in \mathbf{Z}, b \neq 0\}$, 在集合 S 中, 规定关系“ \sim ”:

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

证明: “ \sim ” 是 S 的一个等价关系.

Problem 2

试分别给出满足下列条件的关系:

1. 有对称性、传递性, 但无反身性;
2. 有对称性、反身性, 但无传递性;
3. 有反身性、传递性, 但无对称性;

Problem 3

设 a, b, m 是正整数, 如果 $\gcd(a, m) = 1$, 试证明: $\gcd(ab, m) = \gcd(b, m)$.

Problem 4

给出乘法群 \mathbf{Z}_{13}^* 中每个元素的逆元素.

Problem 5

令 G 是实数对 $(a, b), a \neq 0$ 的集合, 在 G 上定义 $(a, b) \star (c, d) = (ac, ad + b)$. 证明: G 关于 \star 构成群.

Problem 6

设 $G = \{x \in \mathbf{R} \mid 0 \leq x < 1\}$ 且 $x \star y$ 是 $x + y$ 的小数部分. 证明: G 关于 \star 构成阿贝尔群.

Problem 7

设 G 是一个群, 证明: $(gh)^{-1} = h^{-1}g^{-1}, \forall h, g \in G$.

Problem 8

证明: 一个有限群是阿贝尔群当且仅当它的群表是对称矩阵.