

$\iff \forall x(x \in A \cup B \rightarrow x \in \sim C \cup B)$	(子集定义)
$\iff \forall x((x \in A \vee x \in B) \rightarrow (\neg x \in C \vee x \in B))$	(集合并运算、绝对补运算定义)
$\iff \forall x(\neg(x \in A \vee x \in B) \vee (\neg x \in C \vee x \in B))$	(蕴涵等值式)
$\iff \forall x((\neg x \in A \wedge \neg x \in B) \vee (\neg x \in C \vee x \in B))$	(命题逻辑德·摩根律)
$\iff \forall x((\neg x \in A \vee \neg x \in C \vee x \in B) \wedge (\neg x \in B \vee \neg x \in C \vee x \in B))$	(命题逻辑分配律)
$\iff \forall x((\neg x \in A \vee \neg x \in C \vee x \in B) \wedge 1)$	(命题逻辑排中律、零律)
$\iff \forall x(\neg x \in A \vee \neg x \in C \vee x \in B)$	(命题逻辑同一律)
$\iff \forall x(\neg(x \in A \wedge x \in C) \vee x \in B)$	(命题逻辑德·摩根律)
$\iff \forall x((x \in A \wedge x \in C) \rightarrow x \in B)$	(蕴涵等值式)
$\iff \forall x((x \in A \cap C) \rightarrow x \in B)$	(集合交定义)
$\iff x \in A \cap C \subseteq B$	(子集定义)

下面证明 $*$, 即, 对任意集合 A, B , 有 $A \cap B = A \iff A \subseteq B$ 。

若 $A \cap B = A$, 则:

$\forall x,$

$x \in A$

$$\iff x \in A \cap B \quad (A \cap B = A)$$

$$\iff x \in A \wedge x \in B \quad (\text{集合交定义})$$

$$\implies x \in B \quad (\text{命题逻辑化简律})$$

从而有 $A \cap B = A \implies A \subseteq B$ 。

若 $A \subseteq B$, 则:

$\forall x,$

$x \in A$

$$\implies x \in B \quad (\text{子集定义})$$

$$\iff 1 \wedge x \in B \quad (\text{命题逻辑同一律})$$

$$\iff x \in A \wedge x \in B \quad (\text{前提})$$

$$\iff x \in A \cap B \quad (\text{集合交定义})$$

从而有 $A \subseteq B \implies A \cap B = A$ 。

综合得 $A \cap B = A \iff A \subseteq B$ 。

□

2.

$$(1) f(\mathbb{N} \times \{1\}) = \{n \cdot 1 \mid n \in \mathbb{N}\} = \mathbb{N}.$$

$$(2) f^{-1}(\{0\}) = \{\langle m, n \rangle \mid m, n \in \mathbb{N} \wedge mn = 0\} = \{\langle 0, n \rangle, \langle n, 0 \rangle \mid n \in \mathbb{N}\}.$$

(3) f 不是单射(例如 $f(\langle 1, 4 \rangle) = f(\langle 2, 2 \rangle) = 4$, 但 $\langle 1, 4 \rangle \neq \langle 2, 2 \rangle$), 从而也不是双射。

(4) f 是满射, 因为对任何 $n \in \mathbb{N}$, 有 $\langle n, 1 \rangle \in \mathbb{N} \times \mathbb{N}$, $f(\langle n, 1 \rangle) = n$ 。

3.

(1) 易知 $\text{Aut } G = \{\varphi_i \mid i = 1, 2, 3, 4\}$, 其中 $\varphi_i : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5 (i = 1, 2, 3, 4)$ 定义为 $\forall x \in \mathbb{Z}_5, \varphi_i(x) = ix \bmod 5$ 。

运算表如下: