2025/9/9

验证讲义中定义的$\mathbb{F}_p$上的加法和乘法运算良定, 并且使$\mathbb{F}_p$构成域.

Proof: Let $+ : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p, \bar{x} + \bar{y} \mapsto \overline{x+y}$, and $\cdot : \mathbb{F}_p^{\cdot} \times \mathbb{F}_p^{\cdot} \to \mathbb{F}_p^*, \bar{x} \cdot \bar{y} \mapsto \overline{xy}$. For any $\bar{x} = \bar{u}$ and $\bar{y} = \bar{v}$, $x + y \equiv u + v \pmod p$ and $xy \equiv uv \pmod p$, hence $+, \cdot$ are well-defined.
Obviously $+, \cdot$ are both associative and communicative, (since so is addition and multiplication on $\mathbb{Z}$), and $\bar{0} + \bar{x} = \bar{x}$, $\bar{1} \cdot \bar{x} = \bar{x}$, $\overline{-x} + \bar{x} = \bar{0}$. The existence of multiplicative inverse comes from Bezout's theorem: for any $x \in \mathbb{Z}$ such that $\bar{x} \neq \bar{0}$, there exists $u, v \in \mathbb{Z}$ such that $xu + vp = 1$, i.e. $\bar{x} \cdot \bar{u} = \bar{1}$.
For any $x, y, z \in \mathbb{Z}$, $\bar{x} \cdot (\bar{y} + \bar{z}) = \bar{x} \cdot \overline{y+z} = \overline{x(y+z)} = \overline{xy} + \overline{xz}$.
Hence $(\mathbb{F}_p, +, \cdot)$ forms a (finite) field.