L08

Tuesday, August 9, 2022 9:45 AM

Q: Given any (target) order, say $q=3$ or $q=15$, can we construct the "finite field of order q"?

Q: If so, how to describe / construct the $+$, and $\cdot$ operations?

Q: Is the construction unique?

Ans: If a construction is possible, then all other constructions are identical in terms of isomorphism

Proof omitted.

Q: What are the set of $\{q\}$ for which construction exists?

Ans: Any $q = p^m$ where p is a prime number and $m \geq 1$ is an integer a prime number and m is an integer. Proof omitted.

---

* Construction of a finite field.

* Simplest Case: $q = p$ is a prime number

$$GF(p) = \{0, 1, 2, \cdots, p-1\}$$

$$a \cdot b = \mathrm{mod}(a \boxed{\cdot} b, p)$$

$$a + b = \mathrm{mod}(a \boxed{+} b, p)$$

Exercise: prove $GF(q)$ is a field.

Two different ways of representing $GF(p)$

* Method #1: By the "addition" interpretation

$GF(q) = \{0, 1, 2, \cdots, p-1\}$ just as we discussed before.