Finite fields

TODO: ref to Hua and Peter's notes

Definition 0.1. *field* $+, \cdot$

Lemma 0.2. *all non-zero elts have the same + order.*

Proof. exercise □

Definition 0.3. *characteristic, prime subfield*

Lemma 0.4. $|F| = p^d$

Proof. F is a vector space over F_0. □

Lemma 0.5. $F^\times$ *is cyclic.*

Proposition 0.6. $\forall$ *prime* p *and* $d \in \mathbb{N}_+$, $\exists_1 F$ *of order* p^d, *denoted as* $\mathbb{F}_{p^d}$.

Lemma 0.7. $\mathrm{Aut}(\mathbb{F}_{p^d}) \cong \mathbb{Z}_d$.