# What I have learnt today

Author: 秦宇轩（Qin Yuxuan）
Last complied at 2025-06-30

## Contents

## 2025

### 06-30: $F^{\times}$ is cyclic

For finite field $F$, the multiplicative group $F^{\times}$ is cyclic. This result can be used to prove that every finite field is gained from a quotient like $\boldsymbol{F}_p[x]/(\pi(x))$, for some prime $p$ and monic irreducible $\pi(x)$.

**Main idea**: a group $G$ is cyclic iff there is an element $g$ such that $h = g^k$ for any other element $h$ and some $k$, so we must have $\operatorname{ord} g = |G|$. But by Lagrange theorem we alyways have $\operatorname{ord} g \mid |G|$ for any $g$ in $G$, so it suffices to prove $|G| \leq \operatorname{ord} g$. Thanks to the lemma below, we have $h^{\operatorname{ord} g} = 1$ for all $h$. So the polynomial $x^{\operatorname{ord} g} = 1$ has $|F^{\times}|$ roots, which implies $|F^{\times}| \leq \operatorname{ord} g$.

**Lemma**: In finite ablian group, the order of every element divides the maximal order. (It's fun to prove)

*Ref.* Finite Field by Conrad.