What I have learnt today

Author: 秦宇轩（Qin Yuxuan）

Last complied at 2025-07-05

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.

07-05: Compact theorem (by Ultraproduct)

- Ultraproduct: suppose $(A_i)_{i \in I}$ is a bunch of structure in language L, then we can construct a new structure $\mathcal{A}$ using them, provieded am ultrafilter $\mathcal{U}$ on I:

$$\mathcal{A} := \prod_{\mathcal{U}} A_i := \frac{\prod_{i \in I} A_i}{\underset{\mathcal{U}}{\sim}}.$$

- Los theorem: A formula is ture in an ultraproduct, if and only if this formula is ture in *many* smaller models which are used to made that ultraproduct. ("many" is defined by the ultrafilter.)
- Proof of Compact theorem: The model you want is the ultraproduct $\prod_{\mathcal{U}} A_i$ where $(A_i)_{i \in I}$, which is indexed by the set I of all finite sub-theory of given theory T, are models of $i \in I$ (by assumption these models must exist). To prove all formula φ in T are vaild in that ultraproduct, one consult for Los theorem. (The ultrafilter needed by Los theorem can just be solved out by your desire of "makeing $\mathcal{A}$ a model of T".)

A little interesting result: Suppose $\mathcal{U}_A$ is an ultrafilter generated by A on I (thus is priciple), then

$$\{\mathcal{U}_A \subset B : B \text{ ultrafilter on I}\} \simeq \{V : V \text{ ultrafilter on A}\}.$$

This can be used to prove every priciple ultrafilter is generated by a singleton, or equivalentlly, every non-principle ultrafilter must contain the Frechet filter as a subset.

Ref. Sets, Models and Proofs by Ieke Moerdijk and Jaap van Oosten.