What I have learnt today

Author: 秦宇轩（Qin Yuxuan）

Last complied at 2025-07-12

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 $\mathrm{ord}\ g = |G|$. But by Lagrange theorem we alyways have $\mathrm{ord}\ g \mid |G|$ for any g in G, so it suffices to prove $|G| \leq \mathrm{ord}\ g$. Thanks to the lemma below, we have $h^{\mathrm{ord}\ g} = 1$ for all h. So the polynomial $x^{\mathrm{ord}\ g} = 1$ has $|F^\times|$ roots, which implies $|F^\times| \leq \mathrm{ord}\ g$.

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:

$$\mathcal{A} := \prod_{\mathcal{U}} A_i := \left(\prod_{i\in I} A_i\right) / \underset{\mathcal{U}}{\sim}\ .$$

- 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 in $\mathcal{P}(I)$ i.e., by a single subset of I, or equivalentlly, every non-principle ultrafilter must contain the Frechet filter (consists of precisely all "cofinite" subsets of I) as a subset.

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

07-06: $\mathbb{C}$ is the ultraproduct of $\left(\overline{\mathbb{F}_p}\right)_{p \text{ prime}}$

Do not know why yet. Can not even ensure the correctness, but I think...

07-07: $\mathrm{Ran}_G G$ is a monad if it exists. Category admits arbitrary large limit must be a poset.

This is the construction of socalled **codensity** monad of an arbitrary functor $G : A \to B$, and the monadness can be proved in a clever way:

Define a category r_G whose:
- Objects: $(X : B \to B, x : XG \Rightarrow G)$, i.e., right extensions of G;
- Morphisms between (X, x) and (Y, y): Natural transformations $\eta : X \Rightarrow Y$ which campatible with x and y.

And $(r_G, \mathrm{id}_B, \circ)$ is a (strict) monoidal category.

Then we find: $\mathrm{Ran}_G G$ is the terminal object in r_G! So by common abstract nonsense argument, it has an unique monoid structure.

Ref.
- *CODENSITY AND THE ULTRAFILTER MONAD* (Section 5). Tom Leinster.
- complete small category, Theorem 2.1. ncatlab.

07-12: Adjoint Functor Theorem

In this section we fix a Grothendieck universe $\mathbb{U}$ and all "complete" are intepreted as "$\mathbb{U}$-small complete".

Adjoint Functor Theorem: For $G : \mathcal{A} \to \mathcal{X}$ a continuous functor with complete domain $\mathcal{A}$, it has a *left adjoint* $F : \mathcal{X} \to \mathcal{A}$ if and only if the nutorious solution set condition is satisfied: For all $x \in \mathcal{X}$ there is a bunch of objects $a_i^x \in \mathcal{A}$ indexed by a small set such that there are a bunch of morphisms $\eta_i^x : x \to Ga_i^x$ which form a initial class in the comma category $(x \downarrow G)$.

The solution set condition is just a combinition of two *small* facts:
1. For a *small complete* category with *small* hom-sets, a initial class produce the initial object (tricky);
2. The unit of a adjunction $\eta : \mathrm{Id}_{\mathcal{X}} \Rightarrow GF$ is made up of initial objects of comma categories $(x \downarrow G)$ for all $x \in \mathcal{X}$ (ordinary observation).

The solution set condition is just the result of applying fact 1 to fact 2. And, as your expectation, $Fx := a_x$.

I have a sense that this solution set condition is just a rephrasement of $\mathrm{Ran}_G \mathrm{Id}_A$ is a absolute right Kan extension.

Application: We now show the existence of free group functor: By the Adjoint Functor Theorem and the well known fact that **Grp** is complete, we just need to construct an initial class for each set $S \in \mathbf{Set}$. In the following proof, $U : \mathbf{Grp} \to \mathbf{Set}$ is the forgetful functor, we want its right adjoint.

For an arbitrary morphism $g : S \to UH$ where S is a set and H a group, good candidates of the solution set are those subgroups generated by $\mathrm{im}\ g$, note that the elements of $\langle \mathrm{im}\ g \rangle$ are all of the form $g(s_1)^\alpha g(s_2)^\alpha \cdots g(s_n)^\alpha$ where $\alpha = \pm 1$ and s_i are not necessarily diffferent, i.e. every element of this generated subgroup is always a finite composition of elements in $\mathrm{im}\ g$, so the cardinality of $\langle \mathrm{im}\ g \rangle$ is bounded by $|S| + \aleph_0$, for any g, for any H.

Furthur more, the number of group structures on $|S| + \aleph_0$ is also bounded (by simple estimation). So, by the Axiom of Choice, we choose a group from each isomorphic class of those group structures and gather these representations up and obtain the solution set.

Finally, we get the free group functor.

Ref. *Category Theory for Working Mathematicians* (Chapter V, Section 6). Mac Lane.