What I have learnt today

Author: 秦宇轩 (QIN Yuxuan)
Last compiled at 2025-08-25

Contents

2025 1
06-30: $F^\times$ is cyclic 1
07-05: Compact theorem (by Ultraproduct) 1
07-06: $\mathbb{C}$ is the ultraproduct of $\left(\overline{\mathbb{F}_p}\right)_{p \text{ prime}}$ 2
07-07: $\mathrm{Ran}_G G$ is a monad if it exists. Category admits arbitrary large limit must be a poset. 2
07-12: Adjoint Functor Theorem (and the free group functor) 2
07-14: Lefschetz principle and Ax-Grothendieck theorem 3
07-15: ACF_p is complete 4
07-30: Grp is cocomplete 4
08-23: Good use of Zorn's lemma 5
08-24: The codensity monad of Field $\hookrightarrow$ Ring 5
08-25: An algebra is amount to a functor 6

This is a diary-like note that recording what I have learnt that day, so I try to keep them short and readable instead of formal, but if furthur proofs or descriptions are needed then I would like to leave a pointer to my other notes.

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 $F_p[x]/(\pi(x))$, 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 $|G| \le \operatorname{ord} g$. 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 $|F^\times| \le \operatorname{ord} g$.

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

Ref. Finite **Field**. 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* (Section 2.5.1). 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 (and the free group functor)

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 an 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 $\mathbf{Grp}$ 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.

07-14: Lefschetz principle and Ax-Grothendieck theorem

Ax-Grothendieck theorem: For a bunch of polynomials $f_{i(t_1,\dots,t_n)} \in \mathbb{C}[t_1, \dots, t_n]$, if they are all injective viewed as a function $\mathbb{C}^n \to \mathbb{C}$, then the composed polynomial function $F(\boldsymbol{x}) := (f_1(\boldsymbol{x}), \dots, f_n(\boldsymbol{x})) : \mathbb{C}^n \to \mathbb{C}^n$ is automatically surjective (Note that when $n = 1$ Ax-Grothendieck theorem is just equivalent to the algebraic closeness of $\mathbb{C}$ and thus this theorem is a generalised version of algebraic closeness in some sense).

To prove it (from a model theory point of view), we need following theorems, for p prime or zero:

$\mathbf{ACF}_p$ is complete: Thus any algebraic closed field with same characteristic is elementary equivalent. (For proof see notes on 07-15)

Lefschetz principle: For $\mathbf{ACF}_p$ the theory of algebraic closed field with characteristic p and a $\mathcal{L}_{\mathrm{ring}}$-sentence φ, the following are equivalent:

1. For almost all primes p, $\mathbf{ACF}_p \vDash \varphi$;
2. For infinite many primes p, $\mathbf{ACF}_p \vDash \varphi$;
3. $\mathbf{ACF}_0 \vDash \varphi$;
4. $\mathbb{C} \vDash \varphi$;

proof.

- $1 \Rightarrow 2$: Obvious;
- $2 \Rightarrow 3$: Note that $\mathbf{ACF}_0 := \mathbf{ACF} \cup \{(\forall x, px \neq 0) : p \text{ prime}\}$, and every finite subtheory of $\mathbf{ACF}_0$ is satisfiable (the characteristic of a field is the *smallest* number p such that $\forall x, px = 0$) by the models of $\mathbf{ACF}_p$ for some big enough prime p;
- $3 \Rightarrow 1$: Now we play a trick: proof by contrapositive. So we are now trying to prove ($\neg(1)$ implies $\neg(3)$), by definition $\neg(1)$ means "For infinite many primes p, $\mathbf{ACF}_p \vDash \neg\varphi$", which impiles $\mathbf{ACF}_0 \vDash \neg\varphi$ by ($2 \Rightarrow 3$);
- $3 \Leftrightarrow 4$:
  - $3 \Rightarrow 4$: By definition;
  - $4 \Rightarrow 3$: Since $\mathbf{ACF}_0$ is complete.

The main idea of proving Ax theorem by Lefschetz property is that the theorem itself is just a $\mathcal{L}_{\mathrm{ring}}$-sentence φ, so to prove $\mathbb{C} \vDash \varphi$, by Lefschetz principle it suffices to prove $\mathbf{ACF}_p \vDash \varphi$ for infinite many primes p, furthur, by the completeness of $\mathbf{ACF}_p$ it is equivalent to prove $\overline{\mathbb{F}}_p = \bigcup_n \mathbb{F}_{p^{n!}} \vDash \varphi$ for infinite many primes p.

And when restricted to a finite field, injective always implies surjective, so F is surjective on all $\mathbb{F}_{p^{n!}}$ since it is global injective, and thus surjective on $\overline{\mathbb{F}}_p$. The sentence φ is actually true for all primes p and by Lefschetz principle we are done.

Thought. Lefschetz priciple is definitly useful: We can investigate "algebraic property" of any algebraic closed field by investigate $\mathbb{C}$, which can be studied by analytic methods.

Ref. Model Theory Lectures by Prof. Piotr Kowalski at Nesin Mathematics Village in Turkey. Availabe on 哔哩哔哩 and Youtube.

07-15: $\mathbf{ACF}_p$ is complete

To prove it we need a lemma: Any extension of an *algebraic closed* field is actually an elementary extension of the base field (This is not trivial since there may be non-algebraic extensions, of course for algebraic extensions they actually must be isomorphic so everything is fine). All following numberings of theorems and corollaries are from 李文威《代数学方法卷一》.

proof of lemma. By assumption we have an extension $E \hookrightarrow F$ where E is algebraic closed, which implies F is also algebraic closed due to the property of algebraic closed fields.

To produce something elementary equivalent to an given object, the immediately idea is Lowenheim-Skolem theorem: choose a large enough cardinal κ and we obtain two fields E' and F' with both cardinal κ and elementary equivalent to E and F, respectively. So for any $\mathcal{L}_{\text{ring}} \cup E$-sentence φ, we have $E \underset{E}{\equiv} E'$, and since $F \underset{F}{\equiv} F'$ and F is an extension of E we have also $F \underset{E}{\equiv} F'$.

The last part of this proof is, as you have guessed, to show that $E' \underset{E}{\equiv} F'$, but thanks to algebraists, there are several theorems in field theory ensure that these two fields are actually E-isomorphic! Details: By (推论 8.8.7) we only need to show that transcedence degrees of these two extensions are equal $\text{trdeg}_E E' = \text{trdeg}_E F'$, let us denote the transcedence basis of E' and F' over the base field E as T_1 and T_2 respectively. By (命题 8.1.13) we have $|E(T_1)| = |E'| = \kappa$ and $|E(T_2)| = |F'| = \kappa$. So $|T_1| = |T_2| = \kappa$, that is the transcedence degrees are equal. So we are done.

Of course the E-isomorphism between E' and F' preserves truth of $\mathcal{L}_{\text{ring}} \cup E$-sentences, so $E' \underset{E}{\equiv} F'$, since the elementary equivalent is a equivalence relation, finally $E \underset{E}{\equiv} F$.

Note that for any two fields $X \vDash \mathbf{ACF}_p$ and $Y \vDash \mathbf{ACF}_p$, we can consider them as extensions of $\overline{\mathbb{F}}_p$ which is algebraic closed, so by the lemma X and Y are all elementary equivalent to $\overline{\mathbb{F}}_p$, thus they are elementary equivalent.

Every two models of $\mathbf{ACF}_p$ are elementary equivalent, this implies $\mathbf{ACF}_p$ itself is indeed complete.

Remark. There is another "more model-theoretic" proof based on Vaught's test, which claim that if a theory has only infinite models and is κ-categorical for an infinite cardinal κ, then it is complete. (Indeed $\mathbf{ACF}_p$ is κ-categorical for any uncountable κ). This method do not need the cute lemma in our proof.

07-30: Grp is cocomplete

That's another application of the famous Adjoint Functor Theorem.

It is well known that for any small category J and X, the colimit functor $\text{colim}_J : [J, X] \to X$ is the **left adjoint** of the constant functor $\Delta : X \to [J, X]$, and thus we are only need to apply the Adjoint Functor Theorem to $\Delta : \mathbf{Grp} \to [J, \mathbf{Grp}]$.

- Show that the domain of Δ is **complete**: This is an elementary construction.

- Show that there exists a solution class: For $X : J \to \mathbf{Grp}$, define $\lambda := |\coprod_{j \in J} X_j$, obviously the are only “a few” groups whose size is smaller than λ and all those groups form a **set** $\{G_k\}$, of course module isomorphism.
  - Now we claim that $\{G_k\}$ is a solution class: Indeed, for any other morphism $\varphi \in (X \downarrow \Delta)$, i.e. any natural transformation $\varphi : X \to \Delta_H$ where H is a group, the size of the subgroup generated by $\bigcup \varphi_j(X_j)$ is smaller than λ and thus this subgroup is isomorphic to G_k for some k, and thus we obtain a bunch of inclusions $X_j \hookrightarrow G_k$, and since φ is a natural transformation these inclusions form a natural transformation $X \Rightarrow \Delta_{G_k}$. Since the group H is arbitrary, we are done.

By the Adjoint Functor Theorem, Δ has a left adjoint, which is definitly isomorphic to the colimit functor based on J.

Ref. *Abstract nonsense proof of the cocompleteness of the category of groups.* Math Stack Exchange. Accessed at 2025-07-30.

08-23: Good use of Zorn’s lemma

Here is an interesting proposition about any non-separable metric space (X, d): For every non-countable subset $U \subset X$ and any real number $\theta > 0$, there exists $x, y \in U$ such that $x \neq y$ and $d(x, y) \geq \theta$.

proof. Of course we need consider the opposite: suppose all non-countable subsets do not satisfy the property, or in a other way, all subsets admit that property are countable. Now we need to construct a countable dense subset.

By Zorn’s lemma, we obtain a sequence of sets $\{S_n\}_{n \in \mathbb{N}}$ such that for all $x, y \in S_n$, we have $d(x, y) \geq \frac{1}{n}$ (for simplicity we name this property as “$\frac{1}{n}$-sparse”) and S_n is a maximal subset with this property (Indeed, any chain consists of $\frac{1}{n}$-sparse subsets has a greatest element: the union of elements of the chain). And we claim that $S := \cup_{n \in \mathbb{N}} S_n$ is a dense countable subset.

- It is countable: because S_n is countable for all n;
- S_n is dense: For any $x \in X$ and any real number $r > 0$, there exists n such that $\frac{1}{n} < r$, we claim that the open ball $B(x, r) \cap S_n$ is not empty. If not, then we have $d(x, s) \geq r > \frac{1}{n}$, thus $S_n \cup \{x\}$ is again a $\frac{1}{n}$-sparse subset, contradict with the maximality of S_n. Since x and r are arbitrary, S is indeed dense.

Ref. Lectures and Exercises on Functional Analysis, Chapter 2, Exercise 2. A. Ya. Helemskii.

08-24: The codensity monad of $\mathbf{Field} \hookrightarrow \mathbf{Ring}$

I saw this result in Prof. Leinster’s paper (see reference below). And I think there is something more deep behind this theorem, maybe related to commutative algebra or something but I don’t know (yet).

So let’s state it: the codensity monad T of $\mathbf{Field} \hookrightarrow \mathbf{Ring}$ is

$$T(R) = \prod_{p \in \operatorname{Spec}(R)} \operatorname{Frac}(R/p)$$

where $\operatorname{Frac}(R/p)$ stands for the localization of R with respect to a multiplicative subset p, and $R \in \mathbf{Ring}$.

proof. Prof. Leinster claim that $T(R)$ is the limit of $R/\mathbf{Field} \hookrightarrow \mathbf{Field} \hookrightarrow \mathbf{Ring}$. And by considering the connected components (That is, the zigzag classes in a category) of $R/\mathbf{Field}$, we are only need to construct a morphism from $T(R)$ to each connected component since those components do nothing to each others anyway, and then assembly those morphisms together.

If two field $R \to k_1$ and $R \to k_2$ are in the same connected component of category $R/\mathbf{Field}$, then of course they share the same characteristic since they can communicate with each other, and furthur

$\ker(R \to k_1)$ is a prime ideal of R. Because the morphism between k_1 and k_2 is injective the kernels of $R \to k_i$ are the same. So we can classify the connected components by $\mathrm{Spec}(R)$.

And we are lucky: the initial object in each connected component exists: $R \twoheadrightarrow R/p \hookrightarrow \mathrm{Frac}(R/p)$ by the universal property of field of fractions, so the limit of those initial objects is exactly $T(R)$. Since those initial objects are in diffferent connected components, the limit of them is exactly the product of them, i.e., $T(R) = \prod_{p \in \mathrm{Spec}(R)} \mathrm{Frac}(R/p)$.

Thought. To compute a limit of a functor based on a category B, we can first classify the connected components of B, and compute the limit of each connected component and finally the product of those limits are what we need. Same argument also applies to co-limits, of course.

Ref. *CODENSITY AND THE ULTRAFILTER MONAD*, Example 5.1. Tom Leinster.

08-25: An algebra is amount to a functor

Suppose $T : \mathcal{A} \to \mathcal{A}$ is a monad and we want to find a T-algebra structure on an object $a \in \mathcal{A}$, under some mild assumptions of the completeness of $\mathcal{A}$, we can consider the monad morphisms between T and the endomorphism monad of a, i.e. $\mathbf{End}_a$, and that's exactly what we need to do, in theory.

More precisely, we have a natural isomorphism:

$$\mathbf{CAT}/\mathcal{A}(a : \mathbb{1} \to \mathcal{A}, U^T : \mathcal{A}^T \to \mathcal{A}) \simeq \mathbf{Mnd}(T, \mathbf{End}_a),$$

where U^T is the forget functor from the Eilenberg-Moore category $\mathcal{A}^T$ to $\mathcal{A}$, and $\mathbf{End}_a$ is the codensity monad of $a : \mathbb{1} \to \mathcal{A}$ which choose a.

Admit this result, we can immediately see that if there is a monad morphism between T and $\mathbf{End}_a$, then there must be a morphism g such that

$$\begin{tikzcd}
\mathbb{1} \arrow[rr, "g"] \arrow[dr, "a"'] & & \mathcal{A}^T \arrow[dl, "U^T"] \\
& \mathcal{A} &
\end{tikzcd}$$

commutes.

So there exists $f : Tx \to x$ in $\mathcal{A}^S$ such that $U^T(f) = a$, where by definition $U^T(f) = x$. So we obtain a T-algebra structure on a.

Thought. Wow, interesting! But I need to find some applications (if they exist)...

Ref. *CODENSITY AND THE ULTRAFILTER MONAD*, Proposition 6.2, Example 6.3. Tom Leinster.