Number Theory With A View Toward Algebraic Geometry

Koji Sunami

October 10, 2022

Contents

1 Intro

1.1 Preface

This is a script for GSS talk on Oct 11 2022.

My initial motivation for this project is to study the background of étale topology for my own field of study, but I found there are beautiful relationships among variety of subjects in mathematics: number theory, algebraic geometry, algebraic topology, sheaf theory etc and I want to share my experience.

From my project, I thought it is especially fascinating that in étale topology, fundamental group and Galois theory are connected, étale cohomology treats cohomology of finite abelian group, that are isomorphic to sheaf cohomology of Zariski topology, which is moreover Picard group in a specific sense. Also, it is indispensable in algebraic geometry that étale topology fixes the problems of fiber product in Zariski topology, and preservation of exactness by the functor of sections. Also, by étale topology, we can prove Weil conjecture, which is our temporary goal for today's talk. From my talk, I hope everybody will feel from my talk that étale topology is quite common to our daily life.

The oraganization of my script is as follows: Section 1 is review of preliminary stuffs, but it must be read.

Section 2 is about an algorithm of finding roots of polynomial of general degree with henselian ring, which is namely, in polynomial of global field $f(X) \in \mathbb{Q}[X]$, the polynomial $f(X)$ is not neccessarily factorizable by roots of unity, but if we use infinite abelian Galois extensions, the polynomial will be solvable. The idea of henselian is a little classical notion, but it is an inducing problem toward étale topology. In fact, in algebraic geometry, local ring in Zariski topology corresponds to its strict henselization in étale topology, so this argument is unconscious way of argument without specific definition of étaleness. Note that in fact, The idea of extending notion of local ring by Henselian ring in 1950s' Algebraic geometry inspired Grothendieck to introduce Grothendieck topology.

Section 3 is an introduction of étale topology from various points of view. Just briefly, what is étale topology? There are variety of definitions: from general topology, discrete valuation ring, Grothendieck topology. Each of them says, local isomorphismness, unramified flat morphism, treating category as topological space.

In Section 4, I will introduce the relationship between étale topology and Galois theory. Étale topological version of the fundamental group $\pi_1(X, x)$ is given by the analogy of automorphism of universal covering space, and it is actually equal to some Galois group. Finally, the notion will reach to a formalism to Galois category.

In Section 5, I claim statement of Weil conjecture, introducing some relevant notions such as Lefschetz theory. Also, there are diversity of Lefschetz theory in itself, and some of them are not still solved today.

In Section 6, I will briefly mention class field theory, and in Section 7, I will tell my future.

1.2 Reviewing Commutative Algebra

Definition 1.2.1 *(Local Ring)*
Let R be a ring. R is a local ring if it has a unique maximal ideal $m \subset R$.

Definition 1.2.2 *(Localization Of Ring)*
Let R be a ring, let S be a multiplicative subgroup $S \subset R$. We define localization of R as

$$\begin{aligned} R &\to S^{-1}R \\ 1 &\mapsto \frac{1}{1} \end{aligned} \tag{1}$$

where addition and multiplication are defined as $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, and $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$. In particular, for some prime ideal $p \subset R$, we can let $S = R \subset p$ to define $S^{-1}R$.

Definition 1.2.3 *(Discrete Valuation Ring)*
Let R be a ring. R is Discrete Valution Ring if it is principal domain and it is a local ring.

Definition 1.2.4 *(Dedekind Domain)*
Let A be a ring. All non proper ideals are written by some product of prime ideals, as for $I \subset A$, $I = \prod_i p_i^{e_i}$ for some $e_i \in \mathbb{N}$.

Proposition 1.2.1 *(Dedekind Domain)*
Localization of Dedekind rings by a prime ideal is a DVR.

Definition 1.2.5 *(Integrally Closed Domain)*
Let R be a domain. R is integrally closed domain if for polynomial $f(x) \in R[X]$, their roots exist in its field of fraction.

Proposition 1.2.2 *(ICD and DVR)*
Let R be an integral closed domain, and let $\mathfrak{p}$ be a minimal prime ideal. Then the localization $R_{\mathfrak{p}}$ is a discrete valuation ring. The intersection of the local ring $\bigcap R_{\mathfrak{p}}$ is R itself.

Definition 1.2.6 *(Krull Dimension)*
Let R be a commutative ring. The set of all the prime ideals contained in R creates an ordered lattice structure by inclusion relations as $\mathfrak{p}_1 \subset ... \subset \mathfrak{p}_{n-1} \subset \mathfrak{p}_n \subset R$ for some $n \in \mathbb{N}$, where $\mathfrak{p}_n$ is called a maximal ideal and $\mathfrak{p}_1$ is called a minimal ideal. The length of resolution $n \in \mathbb{N}$ is called Krull Dimension.

1.3 Reviewing Galois Theory And Field

Definition 1.3.1 *(Finite Galois theory)*
For any field K, an field extension is a field L defined by $L = K[X]/(f(X))$ for some polynomial $f(X) \in K[X]$, and particularly Galois extension is field extension which is separable and normal.

Field extension is separable if the polynomial $f(X)$ does not have a multiplicity of roots. Also, field extension is normal if L splits over K, mean that all roots of $f(X)$ is contained in L. But why do we call it "normal"? For a field extension L/K, let there be an intermediate extension E/K. We call it Galois if the corresponding group is the normal subgroup $Gal(E/K) \trianglelefteq Gal(L/K)$.

If L is a Galois extension of K, then we define Galois group as $Gal(L/K) = Aut_K(L)$. If Galois extension is finite, then Galois extension and its Galois group has a 1-to-1 correspondence.

Definition 1.3.2 *(Infinite Galois theory)*
Let L be a field extension of K then we have TFAE:

1. *$L = \bigcup_i L_i$ where L_i/K is a finite Galois extension.*
2. *L is the splitting field over K of a set of separable polynomials in $K[X]$.*
3. *$L^{Aut(L/K)} = K$*
4. *L/K is both separable and normal.*

If we satisify the above condition, we call L is a Galois extension of K. Particularly if the Galois group $Gal(L/K)$ is an infinite group, then the extension if infinite Galois extension.

Example 1.3.1 *(Infinite Galois extension)*

1. *$L = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, ...)$*
   Then the corresponding group is $Gal(L/\mathbb{Q}) = \prod_i \mathbb{Z}/2\mathbb{Z}$.
2. *$L = \mathbb{Q}(\zeta_{p^\infty}) = \bigcup \mathbb{Q}(\zeta_{p^n}) = \bigcup L_i$,*
   so $Gal(L/\mathbb{Q}) = \bigcup Gal(L_i/\mathbb{Q}) = \lim \mathbb{Z}/p^i\mathbb{Z}$.
3. *$Gal(\mathbb{F}_p^{sep}/\mathbb{F}_p)$ for some finite field $\mathbb{F}_p$.*
   The Galois group is isomorphic to $\hat{\mathbb{Z}} \cong \prod \mathbb{Z}_n$ where $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ is cyclic abelian group. We call the Galois extension to the separable closure is called absolute Galois group.
4. *$Gal(\mathbb{Q}^{sep}/\mathbb{Q})$ in a similar way, but the group structure is still unknown. However, according to Shafarevich's conjecture, it is a believe to be profinite group.*

Definition 1.3.3 *(Profinite Group)*
All Finite/Infinite Galois Group is a topological space, which is profinite group. Profinite group is compact Hausdorff and totally disconnected topological space, and its name "profinite group" comes from projective limit of finite groups.

Proposition 1.3.1 *(Topology of Galois Group)*

1. *All infinite Galois group is countable as a set, so its base is at most second countable.*
2. *For all infinite Galois group, all finite sets are closed.*
3. *From the previous claim, all infinite Galois group is locally connected.*

Definition 1.3.4 *(Galois Representation)*

$$\rho : G_{\mathbb{Q}} \to GL_n(F)$$

is called Galois Representation of dimension n, which is is a linear map where $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is an absolute Galois group, and F is any topological field. Topological field is an ordinary field where each inverse, multiplication, addition operations are continuous.

Particularly if F is an (finite) extension of $\mathbb{Q}_l$, we call ρ an l-adic Galois representation.

Proposition 1.3.2 *(Character Formula)*
Define the cyclotomic character of l as χ_l
$\chi_l : G_{\mathbb{Q}} \twoheadrightarrow Gal(\mathbb{Q}(\mu_{l^\infty}/\mathbb{Q})) \cong \mathbb{Z}_l^\times$

$$G_{\mathbb{Q}} \twoheadrightarrow \mathbb{Z}_l^\times \hookrightarrow \mathbb{Q}_l^\times = GL_1(\mathbb{Q}_l)$$

Definition 1.3.5 *(Ramification)*
Let p be any prime number, and $\mathfrak{p}$ be a prime ideal lying on some field extension K. Then, we have a morphism
$D_{\mathfrak{p}} \to Gal(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$

where $D_{\mathfrak{p}} = \{\sigma \in Gal(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}$ and $\mathbb{F}_{\mathfrak{p}} = O_K/\mathfrak{p}$ is the residue field at $\mathfrak{p}$. If the kernel of the morphism is trivial, theni σ_p generates $D_{\mathfrak{p}}$, and K is unramified at p. Furthermore, this idea can be naturally extended to the absolute extensions.

The morphism $D_p \to Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$

Example 1.3.2 *(l-adic Cyclotomic Character)*
Consider a natural morphism induces a character χ_l
$G_{\mathbb{Q}} \twoheadrightarrow Gal(\mathbb{Q}(\mu_{l^\infty})/\mathbb{Q}) = limGal(\mathbb{Q}(\mu_{l^n})/\mathbb{Q})$

Then, $G_{\mathbb{Q}} \twoheadrightarrow \mathbb{Z}_l^{\times} \hookrightarrow \mathbb{Q}_l^{\times}$

and each extension $\mathbb{Q}(\mu_l^n)/\mathbb{Q}$ *is unramified at all* $p \neq l$.

The notion might be generalized to Galois category.

Proposition 1.3.3 *(Cardinality of Field)*

1. *Cardinality of* $\mathbb{Q}$ *is* $\aleph_0$.
2. *Cardinality of* $\mathbb{F}_p$ *is* p*, which is finite.*
3. *Let* k *be a field. If* k *is a finite field, the cardinality of algebraic closure* $card(\bar{k}) = \aleph_0$
4. *If* k *is a field of countable elements, then the cardinality of algebraic closure* $card(\bar{k}) = \aleph_0$

1.4 Reviewing Algebraic Geometry

Remark 1.4.1 *(Open Sets In Euclidean Topology)*
For an Euclidean space $\mathbb{R}^n$ *for some* $n \in \mathbb{N}$*, topological basis is an open ball* B_ϵ*. The open ball is always* n*-dimensional. Considering from that fact, Zariski topology related each geometry to a closed subset, since they don't have to be* n*-dimensional. For example, maximal ideal is related to a closed point, but if it would be open, it is quite weird.*

Definition 1.4.1 *(Algebraic Variety & Scheme)*
For affine variety, let R *be a noetherian ring. Affine variety is a subset of an algebraic set* $\mathbb{A}^n$ *such that where* $Spec(R)$ *the spectrum of prime ideal of* R *corresponds to the closed subset of the corresponding affine variety. Mainly, Affine variety satisfies:*

1. *If two ideals* $I\_1 \subset I_2$*, then the corresponding closed geometries* $V(I_1) \supset V(I_2)$ *have reverse inclusion.*
2. *If an ideal* $I = \bigcap \mathfrak{q}_i$ *is the primary decomposition, where* $\mathfrak{q}_i$ *is* $\mathfrak{p}_i$*-primary, then* $V(I)$ *is an union* $V(I) = \bigcup V(\mathfrak{p}_i)$.
3. *SpecmR is set of all closed points of* R.

For general definition of abstract variety and scheme, more to be added.

Definition 1.4.2 *(Section)*
In Zariski topology, we define section as:
$\mathscr{O}_{X,x} = \lim \Gamma(U, \mathscr{O}_X)$
In Étale topology, we define section as:
$\mathscr{O}_{X,\bar{x}} = \lim \Gamma(U, \mathscr{O}_U)$

Definition 1.4.3 *(Generic Points, Closed Points, And Irreducible Varierty)*
Let X be a scheme. A generic point is a point $x \in X$ where for some irreducible subscheme $U \subset X$, closure of the point generates the subscheme U as $\{\bar{x}\} = U$.

For example, $\mathbb{R}[X]$ be an algebraic variety, and a prime ideal $(x^2+1) \subset \mathbb{R}[X]$ corresponds to an irreducible variety. Let $Specm(\mathbb{R}[X])$ be a set of maximal ideals of $\mathbb{R}[X]$, and this is equivalent to the set of all closed points, since each prime ideal corresponds to a closed subset of the variety particularly a maximal ideals to a point.

Definition 1.4.4 *(Base Of Scheme)*
For a morphism $f : X \to Y$ be a morphism of schemes, and we consider Y as a base scheme of X.

Since category of scheme allows fiber product, we may induce a morphism $X \times_Y Z \to Z$ for some scheme Z, and this morphism has a base Z. This is called change of base*.*

Definition 1.4.5 *(Weil Divisor)*
Let X be regular in codimension one, namely, every local ring $\mathscr{O}_X$ of X of dimension one is regular. If X is moreover noetherian integral separated scheme, then we can define a prime divisor, which is a closed integral subscheme $Y \subset X$ of codimension one.

Let Set be a category of all prime divisors of X and let Ab be a category of abelian groups. Consider a functor $Free : Set \to Ab$ such that for $\{Y_i\} \in Ob(Set)$ and $\{Y_i\} \mapsto \{\Sigma n_i[Y_i]\}$, and the domain is free abelian group denoted $DivX$.

Weil divisor Y is an element of the free abelian group $DivX$.

Remark 1.4.2 *(What is the meaning of Weil Divisor After All?)*
Recall an affine variety has 1-to-1 correspondence between closed algebraic sets and prime divisors. Also, each prime divisor has an inverse inclusion relationships. If we take $\mathfrak{p}_1$, $\mathfrak{p}_2$ be prime ideals as $\mathfrak{p}_1 \subset \mathfrak{p}_2$, then the corresponding varieties are containing one another but in an opposite way $V(\mathfrak{p}_2) \subset V(\mathfrak{p}_1)$.

For example, maximal ideals $\mathfrak{m} \subset R$ correspond to a point, and by Nullstellensatz, the minimal prime ideals represents irreducible proper subvariety of X, namely a subvariety of codimension 1. Furthermore, the localization of minimal prime ideal $S^{-1}R$ where $S = R - \mathfrak{p}$ is a discreate valuation ring, quite number theoretical. Also, intersection of all the minimal ideals of noetherian ring R is nilradical, so it's identical to (0) ideal through Nullstellensatz.

Proposition 1.4.1 *(Weil-Divisor Sequence)*
$0 \to A^\times \to K^\times \to \bigotimes_{ht(\mathfrak{p})=1} \mathbb{Z} \to 0$

$0 \mapsto a \mapsto ord_{\mathfrak{p}}(a)$
for $A = \{a \in K | ord_{\mathfrak{p}}(a) \geqq 0 \ all \ \mathfrak{p}\}$
for $A_{\mathfrak{p}} = \{a \in K | ord_{\mathfrak{p}}(a) \geqq 0\}$
for $A^{\times} = \{a \in K | ord_{\mathfrak{p}}(a) = 0 \ all \ \mathfrak{p}\}$

Similarly, for any open subscheme $U \subset X$,
$0 \to \mathscr{O}_X^{\times} \to \Gamma(U, K^{\times}) \to Div(U) \to 0$
is a left exact, and it is short exact sequence if X *is regular.*

Definition 1.4.6 *(Ramification In Algebraic Geometry)*
Let $f : X \to Y$ *be a morphism of schemes. The support of quasi-coherent sheaf* $\Omega_{X/Y}$ *is called the ramificatio of locus of* f *and the image of the ramification locus,* $f(Supp(\Omega_{X/Y}))$ *is called the branch locus of* f. *If* $\Omega_{X/Y} = 0$, *we say that* f*is formally unramified, and if* f *is also of locally finite presentation we say* f *is unramified.*

1.5 Reviewing Local Field And Global Field

Definition 1.5.1 *(Global And Local Field)*
The formal definition of global field is a field which is either

1. *a field of finite extension of* $\mathbb{Q}$.
2. *The function field of an algebraic curve over a finite field. Or equivalently, finite extension of* $F_q(T)$, *the field of rational functions, called global function field.*

The formal definition of local field is a field if it is complete with respect to the topology induced by a discrete valuation ν, *and residue field* k *is finite, and it is either*

1. *Archimedian local fields:* $\mathbb{R}$ *and* $\mathbb{C}$.
2. *Non-archimedian local fields of characteristic* 0*: finite extension of* $\mathbb{Q}_p$.
3. *Non-archimedian local fields of characteristic* p*: field of Laurent series* $\mathbb{F}_{p^n}((T))$

In fact, p-adic number is characteristic 0 *because* $\mathbb{Z}_p \cong \mathbb{Z}[[t]]/(t-p)$.

Definition 1.5.2 *(p-adic Number)*
For each prime number $p \in \mathbb{Z}$, *p-adic number is a ring, as a set of elements that can be written by the series* $r = \Sigma_{n=-k}^{\infty} a_n p^{-n}$.

Alternatively, p-adic number is an inverse limit of finite abelian group $lim_p(\mathbb{Z}/p^n\mathbb{Z})$. *Inverse limit on a small category is a product of sequences of objects* $\{A_i\}$ *where* $A_i \in Ob(C)$, $i \in I$, *which is quotioned by an equivalence class, and it is formally written as* $lim_i(A_i) = \prod_i A_i / \sim$.

Also, p-adic field is $\mathbb{Q}_p$, *which is a field of fraction of* $\mathbb{Z}_p$.

Proposition 1.5.1 *(p-adic Topology)*

1. $\mathbb{Q} = \bigcap_p \mathbb{Q}_p$
2. $\bar{\mathbb{Q}} \subset \bigcup_p \mathbb{Q}_p$
3. $\bar{\mathbb{Q}_p} \neq \mathbb{Q}_p$
4. *Each p-adic field $\mathbb{Q}_p$ is Hausdorff.*
5. *Each p-adic field $\mathbb{Q}_p$ is complete.*
6. *cardinality of p-adic field $card(\mathbb{Q}_p)$ is $\aleph_0$*
7. *p-adic integer $\mathbb{Z}_p$ is homeomorphic to Cantor set. Also, Cantor set is compact because it is closed and bounded.*

Note that the union of $\mathbb{Q}_p$ contains algebraic closure of $\mathbb{Q}$, but each of them is not algebraic closure of itself.

Also, p-adic field $\mathbb{Q}_p$ is a complete metric space. First of all, Considered that the cardinality if $\aleph_0$, its topology is paracompact, and paracompact Hausdorff is a normal space, which is enough to say metrizable (Urysohn's metrizability theorem).

Proposition 1.5.2 *(p-adic Manifold)*
p-adic field $\mathbb{Q}_p$ is totally disconnected Hausdorff space whose topological dimension is 0. By these properties, $\mathbb{Q}_p$ can also be considered as a 0-dimensional manifold, since this is Hausdorff and disconnectedness means that each point is open. Furthermore, in fact, p-adic field $\mathbb{Q}_p$ is an infinite Galois group $\mathbb{Q}_p = \bigcup_n \mathbb{Q}(\zeta^{p^n})$, and if that is considered, $\mathbb{Q}_p$ is a Lie group.

Now this notion can extended to K-analytic manifold where K is some p-adic field, by adding some conditions that each open neighborhood is homeomorphic to K^n-vector space.

From now, we will introduce Adele ring.

Definition 1.5.3 *(Haar measure)*
Haar measure is namely a measure defined over a group.

Let G be a locally compact Hausdorff topological group, and let $\mu : G \to \mathbb{R}_{\geqq 0}$ be a measure. μ is Haar measure if it satisfies the following properties:

1. *$\mu(S) = \mu(gS)$ for Borel sets $S \subset G$, $g \in G$.*
2. *$\mu(S) = \mu(Sg)$ for Borel sets $S \subset G$, $g \in G$.*

3. $\mu(K) < \infty$ *for a compact set* $K \subset G$.

4. $\mu(G) = 1$

5. $\mu(S) = inf\{\mu(U) : S \subset U, U \text{ open}\}$ *(outer regular)*

6. $\mu(S) = sup\{\mu(U) : K \subset U, K \text{ compact}\}$ *(inner regular)*

For example, for Euclidean space is trivially an additive group $(\mathbb{R}, +)$*, and this case, haar measure is Lebesgue measure.*

Remark 1.5.1 *(Ostrowski)*
In fact, the only complete metric space over $\mathbb{Q}$ *is* $\mathbb{R}$ *or* $\mathbb{C}$ *if archimedean absolute value is defined, or p-adic fields if non-archimedian absolute value is defined (Ostrowski).*

Definition 1.5.4 *(Valuation Ring)*
An integral domain R *is a valuation ring if for all* $x \in F$ *of fraction of field* F*,* x *or* x^{-1} *is contained in* R*. That says,* $R \subset F$*. This valuation ring* R *is, in fact, a local ring, and every ideal of* R *is totally orderd by inclusion.*

The valuation of R *is a map* $\nu : F \to \Gamma \bigcup \{\infty\}$ *where for* $x \in R$*,* $\nu(x) \geqq 0$*, and* Γ *is an abelian group.*

Definition 1.5.5 *(Adele Ring)*
Let K *be a global field, and* $\mathbb{A}_K$ *be an adel ring if* $\mathbb{A}_K = \prod_\nu (K_\nu, O_\nu)$ *where* ν *is all the possible valuations.*

Particularly, if $K = \mathbb{Q}$*, by Ostrowski's theorem, all the valuation rings are real field* $\mathbb{R}$ *or p-adic integers* $\mathbb{Z}_p$*. Namely,* $\mathbb{A}_K = \mathbb{R} \times \prod_p (\mathbb{Q}_p, \mathbb{Z}_p)$.

2 Polynomial And Henselization

In this section, we will see number theoretical viewpoint of the solution of polynomial $f(x) \in \mathbb{Q}[X]$ by using a local field $\mathbb{F}_p[X]$ for some prime p and Hensel's lemma. In fact, the solution of polynomial always exists in p-adic completion $\mathbb{Q}_p$ for some prime p.

What kind of techniques are used to solve polynomial?

Algorithm	Theory
Newton's method	Liouville's theorem
Hypergeometric function	Lefschetz Fix point theorem
Hensel's lemma	Winding number
Roots of unity	Bezout's theorem
etc	Galois theory

2.1 Hensel's Lemma and Factorization Of Polynomial

Hensel's lemma is an algorithm of polynomial factorization, because it claims that by certain conditions, a polynomial factorizable in a local field is also factorizable in the global field. Generally speaking, factorization of polynomial in global field is complicated especially for higher degree, and I suppose a different solution.

Proposition 2.1.1 *(Krull's Intersection Theorem)*
Let R be a Noetherian commutative local ring and $\mathfrak{m} \subset R$ be the maximal ideal. Then, $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0)$

Proposition 2.1.2 *(Hensel's lemma)*
Let R be a local ring and $h \in R[X]$ be a polynomial where h is $h = \alpha_0 X^n + ... + \alpha_{n-1}X + \alpha_n$ where $\alpha_0 \notin \mathfrak{m}$ for some arbitrary maximal ideal $\mathfrak{m}$, and if h is locally factorizable by some other polynomials $f, g \in R[X]$ modulo $\mathfrak{m}$ as $h = \alpha_0 fg(mod\mathfrak{m})$, then the equality can be lifted as follows:

$$h = \alpha_0 f_k g_k (mod\mathfrak{m}^k)$$

$$f_k \equiv f, \quad g_k \equiv g(mod\mathfrak{m})$$

and f_k and g_k are unique modulo $\mathfrak{m}^k$ for all $k \in \mathbb{N}$. Here recall that since R is a local ring, so by Krull's intersection theorem, at most countable times of operations induce the equality of $h = fg$ where $f = lim_{n\to\infty} f_k$ and $g = lim_{n\to\infty} g_k$.

Proposition 2.1.3 *(Factorization Algorithm Over Finite Field)*
Let $f(X) \in \mathbb{F}[X]$ be a polynomial over a finite field $\mathbb{F}$. Then, $f(X)$ may be factorized to the product of linear formulae by the following algorithms:

1. *Berlekamp's algorithm*
2. *Cantor-Zassenhaus algorithm*
3. *Eisenstein's Criterion*
4. *Hasse principle*

Proposition 2.1.4 *(Eisenstein's Criterion)*
Let $f(X) \in \mathbb{Z}[X]$ be a polynomial of integer coefficients as $f(X) = a_n X^n + ... + a_1 X + a_0$. If we chooes arbitrary prime p such that a_0 is divisible by p but not p^2, a_i is divisible by p for $1 \leq i \leq n-1$ and a_n is not divisible by p, then the polynomial is not divisible.

This irreducibility criterion may be generalized to the case of rational polynomials, That says, if a rational polynomial $f(X)$ is irreducible if we multiply

some constant $a \in \mathbb{Z}$ such that $af(X) \in \mathbb{Z}[X]$, and we apply Gauss lemma, which claims primitive element in $\mathbb{Z}[X]$ is irreducible in $\mathbb{Q}[X]$.

Moreover, the notion of Eisenstein's criterion might be generalized to any polynomial rings of coefficient ring is integral domain. Let $f(X) \in R[X]$ be a polynomial where R is an integral domain as $f(X) = a_n X^n + ... + a_1 X + a_0$ where $a_i \in R$, and for some $Q \subset R[X]$ be a prime ideal. If a_n is not divisible by Q, a_i is divisible by Q for $0 \leq i \leq n-1$ and a_0 is not divisible by Q^2, then the polynomial $f(X)$ is irreducible. Particularly, for example, for polynomial rings of p-adic integers such as $\mathbb{Z}_p[X]$, consider that $\mathbb{Z}_p$ is an integral domain, and $p\mathbb{Z}_p$ is its prime ideal, we can apply Eisenstein criterion for it.

Example 2.1.1 *(case of p-adic integer)*
Let's consider the factorization of $f(X) = X^6 - 2$ where $f(X) \in \mathbb{Q}[X]$. First of all, we will find some prime p such that $f(X)$ is factorized to the product of linear functions, and in fact, it does always exist!. After doing this, we can apply Hensel's lemma to find a p-adic integers for the roots of polynomial.

If $p = 2$, then the natural map $\mathbb{Q}[X] \to \mathbb{F}_2[X]$ induces $f(\bar{X}) = X^6 - \bar{2} \in \mathbb{F}_2[X]$, and it can be factored into $f(\bar{X}) = X^6 - \bar{2} = X^6$, but by Eisenstein's criterion, $f(\bar{X})$ is irreducible in $\mathbb{Z}_2[X]$.

If $p = 7$, the given polynomial will be $f(\bar{X}) = X^6 - \bar{2} \in \mathbb{F}_7[X]$, and $f(\bar{X}) = X^6 - \bar{2} = X^6 - \bar{16} = (X^3 - \bar{4})(X^3 + \bar{4})$, and it is irreducible.

If $p = 727$, the given polynomial will be $f(\bar{X}) = X^6 - \bar{2} \in \mathbb{F}_7 27[X]$, and $f(\bar{X}) = X^6 - \bar{2} = (X - \bar{3})(X - \bar{116})(X - \bar{119})(X - \bar{608})(X - \bar{611})(X - \bar{724})$, and hence the factorization is done.

Definition 2.1.1 *(Henselization of ring)*
Henselian ring is a ring that satisfies Hensel's lemma. This Henselian ring can be induced by any local ring A. We define $A \to A^h$ be a henselization of A if for any Henselian ring B and homomorphism $f : A \to B$ factors through A^h as $A \to A^h \to B$.

Particularly for all $x \in X$, each local ring of scheme $\mathscr{O}_{X,x}$ has a henselization of ring $\mathscr{O}_{X,\bar{x}}$, where the latter ring is the stalk of structure sheaf in étale topology, and $\bar{x}$ is a geometric point $\bar{x} : Spec(\Omega) \to X$, and $\mathscr{O}_{X,\bar{x}}$ is defined as $\mathscr{O}_{X,\bar{x}} = \lim \Gamma(U, \mathscr{O}_U)$.

Example 2.1.2 *(Examples of Henselian Rings)*
Complete Hausdorff local rings are Henselian. For example, p-adic integer $\mathbb{Z}_p$, $k[[x]]$ are henselian where $k = \bar{k}$ or $k = \mathbb{R}$, complete Hausdorff local ring. More generally, Nagata claims the henselization of integrally closed integrity domains.

On the other hand, not all discrete valuation rings are Henselian, but complete discrete valuation ring is Henselian.

Remark 2.1.1 *(t-adic Completion Is Not Metrizable)*
t-adic completion of a polynomial $k[t]$ where $\bar{k}$ is $k[[t]]$, and this is Henselian and local ring. It is not a metric space because the cardinality of the formal series $k[[t]]$ is $\aleph_1$ while its topology is totally disconnected, so it might not be paracompact.

Proposition 2.1.5 *(One-Variable Fundamental Theorem of Algebra)*
We might know already at least one proof of fundamental theorem of algebra, but this is a different version.

All polynomials $f(X) \in \mathbb{Q}[X]$ are factorizable by some local field $\mathbb{Z}_p$ where p is a prime, and it's lifted by Hensel's lemma.

Proposition 2.1.6 *(Multi-Variable Fundamental Theorem of Algebra)*
Topologically, in multi-variable case, there is no differences in what we have to do: In fact, the zero points are intersection of the zero hyperplane and the given polynomial, and for some situations, they are isolated points. Here I will abbreviate the rigorous proof, but there is a multi-variable version of fundamental theorem of algebra. The method is that there exists a multi-variable version of henselization of a multivariable polynomial ring, and we apply this to the multi-variable version of Bézout's theorem.

Remark 2.1.2 *(Conjecture: Multi-Variable Fundamental Theorem of Algebra)*
Consider the fundamental theorem of algebra exists in $\mathbb{C}[X]$, and it is contained in its henselization $\mathbb{C}[[t]]$. Then, an arbitrary polynomial $f(X, Y) \in \mathbb{C}[X][Y]$ is contained in $\mathbb{C}[[X]][Y]$, and the Hensel's lemma should be applied.

2.2 Relation to Algebraic Geometry

In algebraic geometry, local ring is one of our interests, and we could see it from commutative algebra perspective. In abstract algebra, local ring is a ring of unique maximal ideal, but in geometry, some doubts if local ring really represents the local information of geometry,

Example 2.2.1 *(Connection to Grothendieck topology)*
Grothendieck topology is an analogy of topology defined over categories. An example of Grothendieck topology is, Zariski topology, Nisnevich topology, étale topology, fppf topology, and fpqc topology, finer by its order. If the topology is finer, then it has more information but it is difficult to compute.

Althogh it is little more minor than étale topology, Nisnevich topology is considered to be the topology of the henselization of local rings. , and if the henselization is strict, then it makes étale topology, and we call Henselization is strict if residue field is separably closed. separate extension is def by separable polynomial f(x). Nevertheless, Nisnevich topology is used in the modern age of research, which are for example, The Nisnevich Motive Of An Algebraic Stack *(Choudhury, Deshmukh, Hogadi), and* Descent Properties Of Equivariant

K-Theory *(Christian Serpé).*

Another case is fpqc, which is one of topology in Grothendieck Topology, and it is used to categorical quotient in the scheme theory.

Example 2.2.2 *(Maclaurin expansion)*
Completion of coordinate ring $\mathbb{C}[X,Y]$ at origin $\mathfrak{m} = (X)$ has a formal power series $\mathbb{C}[[X]]$, which is a local ring, which is also Henselian. This is used to describe Maclaurin expansion at the point origin.

Also, if we consider number theory, then DVR might be an interest.

Example 2.2.3 *(Algebraic Curve and Local Ring)*
given an algebraic curve, a local ring at a smooth point p is principal, so it is discrete valuation ring. Discrete valuation ring A has a unique prime ideal, and the krull dimension is 1*.*

3 Étaleness

In a word, in algebraic geometry, étale topology is an expansion of Zariski topology, and it often makes us easy to treat several mathematical objects: fiber products, quotient of scheme, moduli space, DVR for number theory, or defining topology on finite field as an analogy to Euclidean topology. Also, in sheaf cohomology in Zariski, not all exact sequence of sheaves preserves the exactness by functor of global section if the sheaf is not flasque, but sheaf cohomology induced by étaleness might fix this problem.

In this section, we will see the scheme theoretic construction of étale topology, étale morphism, and étale cohomology, but first of all, I will introduce the naive definition of étaleness in topological space.

Definition 3.0.1 *(Étale map)*
Étale map is a map which is locally homeomorphic.

Example 3.0.1 *(Étale map – polynomial)*
For a map $f : \mathbb{C} \to \mathbb{C}$, let the map be $f(z) = z^n$ for some natural number $n \in \mathbb{N}$, then f is an étale map.

Example 3.0.2 *(Étale map – covering space)*
Let f be a continuous map $f : \mathbb{R} \to S^1$ which is surjective. Then $\mathbb{R}$ is a covering space of S^1, and the preimage of some $U \subset S^1$ is union of open subsets of $\mathbb{R}$, where each of them is homeomorphic to U. Then f is an étale map.

3.1 Grothendieck Topology

To be added.

3.2 Sheaf Cohomology

In general, in geometry, sheaf is an idea that relates topology and sets, and this is used to describe the geometrical structure of sets. For example, for scheme X, there is a naturally defined structure sheaf $\mathscr{O}_X$. Sheaf cohomology is, by definition, a cohomology induced from a sequence of sheaves to a sequence of their sections.

Sheaf is, need less to say, can be defined on any topologies. For example, Zariski topology is a naturally defined topology by the structure sheaf of some ring space, and the sheaf cohomology is defined. However, its computation is the problem since for the short exact sequence of sheaves $0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{H} \to 0$, the induced sequence of sections $0 \to \mathscr{F}(U) \to \mathscr{G}(U) \to \mathscr{H}(U) \to 0$ is not in general exact if $\mathscr{F}$ is not flasque.

Definition 3.2.1 *(Flasque)*
For every inclusion of open sets $V \subset U$, $\mathscr{F}(U) \to \mathscr{F}(V)$ is surjective.

Also, for example, in analytic topology, sheaf cohomology might be efficiently computed by $\check{C}$ech cohomology, and in analytic topology, paracompactness might be the criteria.

Proposition 3.2.1 *(Paracompactness)*
A topological space X is paracompact, if and only if X is second countable, or if and only if it has a locally finite open refinement.

If a topological space X is Hausdorff(T2) and paracompact, then X is a normal(T4) space. For example, CW complex(or triangulable space) is paracompact.

In normal space, Cech cohomology and sheaf cohomology are equal.

Definition 3.2.2 *(Categorical Presheaf)*
Let X be a presite. Presite is any object which has an corresponding category C_X. Presheaf is a functor from category to a category of sets $F : C_X \to Set$ and this naturally defines a category of presheaves $PSh(X, Set) = Fun({C_X}^{op}, Set)$.

In particular, in Hartshorne's definition, presheaf is a functor $F : Top \to Ab$ from category of topological spaces to category of abelian groups with restriction maps preserves orders. In this case, category of presheaves is an abelian category, and it induces homology.

Definition 3.2.3 *(Categorical Sheaf)*
Let $Sh(X, Set) \subset Psh(X, Set)$ is a full subcategory of presheaves. Suppose for all local isomorphism $A \to U \in C_{\hat{X}}$, $\mathscr{F}(U) \to \mathscr{F}(A)$ is an isomorphism where $\mathscr{F} \in Sh(X, Set)$, then we call $Sh(X, Set)$ as a sheaf.

Particularly, in Hartshorne, we have defined a specific sheaf for Zariski topology.

Definition 3.2.4 *(Sheaf Cohomology)*
Let $(X, \mathscr{O}_X)$ be a ringed space. Then the category $\mathscr{M}(X)$ of sheaves of $\mathscr{O}_X$-modules has enough injectives. Thus, any sheaf $F \in \mathscr{M}(X)$ has an injective resolution.

Let $(X, \mathscr{O}_X)$ be a ringed space. Then any injective $\mathscr{O}_X$-module is flasque, which means that any short exact sequence of sheaves functorially preserves exactness.
If $0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{H} \to 0$
is exact, then the sections of sheaves
$0 \to \mathscr{F}(U) \to \mathscr{G}(U) \to \mathscr{H}(U) \to 0$
is exact.

Definition 3.2.5 *(Zariski Sheaf and Étale Sheaf)*
Sheaf on Hartshorne's definition is one thing. Let there be a cohomology of presheaf $0 \to F(U) \to \prod_i F(U_i) \to \prod_{i,j} F(U_{ij}) \to ...$
$f \mapsto f|_{U_i}$
$f_{U_i} \mapsto f_{U_i}|_{U_i \cap U_j} - f_{U_j}|_{U_i \cap U_j}$
where $U \subset X$ is any open subset, and $\{U_i\}_{i \in I}$ is an open cover of U, and we denote $U_{ij} = U_i|_{U_j} - U_j|_{U_i}$. If the sequence is exact, then we call this presheaf as sheaf with respect to Zariski topology.

Also, sheaf of étale topology may be similarly defined. Let there be a cohomology of presheaf $0 \to F(U) \to \prod_i F(U_i) \to \prod_{i,j} F(U_{ij}) \to ...$
$f \mapsto f|_{U_i}$
$f_{U_i} \mapsto f_{U_i}|_{U_i \cap U_j} - f_{U_j}|_{U_i \cap U_j}$
where $U \subset X$ is any open subset, and $\{U_i\}_{i \in I}$ is an open cover of U, and we denote $U_{ij} = U_i \times_U U_j$. If the sequence is exact, then we call this presheaf as sheaf with respect to étale topology.

3.3 Étale morphism

In this section, we will define étale morphism. Étale morphism is an unramified morphism, which is also a flat morphism.

Definition 3.3.1 *(Ramification of Ring of integers)*
Let K and L be fields of extension of $\mathbb{Q}$, and O_K and O_L be the corresponding ring of integers, and if $K \subset L$, then we have a natural morphism $O_K \to O_L$. Then for prime $\mathfrak{p} \in O_K$, pO_L is any ideal of O_L, but since O_L is Dedekind domain, the ideal can be factored by some product $\mathfrak{p}O_L = \prod_i \mathfrak{p}_i^{e_i}$. We call $\mathfrak{p}$ is unramified if for all i, $e_i = 1$, and ramified if $e_i > 1$ for some i.

For definiting a ramification of local field, we use extensions of p-adic numbers.

Definition 3.3.2 *(Unramified Morphism of Local Ring)*
Let A and B be local rings, and let $f : A \to B$ be a homomorphism of rings. We say that f is unramified if $f(m_A)B = m_B$ and residue fields B/m_B is a finite separate extension of A/m_A.

Remark 3.3.1 *(Completion)*
$f : A \to B$ is an unramified morphism if and only if the completion $\hat{f} : \hat{A} \to \hat{B}$ is unramified.

Example 3.3.1 *(Unramified morphism of DVR)*
For example if A and B are DVR and $f : A \to B$ is a ring homomorphism, and if $f(m_A)B \subsetneqq m_B$, then the morphism $f : A \to B$ is ramified. Because B is a DVR, principality says Krull dimension is 1, and since it is local ring, there is only one maximal ideal, meaning that there is only one prime ideal exists in B (so does A). If $f(m_A)B$ is a properly contained ideal in m_B, then it needs to be a primary ideal, contradiction to the unramifiedness.

Definition 3.3.3 *(Unramified Morphism of Scheme)*
Let $f : X \to Y$ is a morphism of schemes. f is unramified at $x \in X$ if the induced morphism $f^* : \mathscr{O}_{Y,y} \to \mathscr{O}_{X,x}$ is unramified for $y = f(x)$. Particularly, if $f : X \to Y$ is unramified if it is unramified at all $x \in X$.

Next, I will speak flatness of morphism, one of étaleness property of morphism.

Definition 3.3.4 *(flatness of commutative algebra)*
A module N over a ring A is said to be flat if the functor $F : M \to M \otimes_A N$ is exact. If the functor is faithful, then the morphism is faithfully flat.

Also, a morphism of ring $f : A \to B$ is flat if the induced functor $F : M \to M \otimes_A B$ is exact.

Definition 3.3.5 *(flatness of scheme)*
A scheme morphism $f : X \to Y$ is flat at $x \in X$ if the induced morphism $f^* : O_{Y,y} \to O_{X,x}$. If $f : X \to Y$ is flat if it is flat at all $x \in X$.

Remark 3.3.2 *(fpqc topology)*
The notion of fpqc topology appears when we define the quotient map of Zariski topological space. Fpqc is a further generalization of étale topology.

Definition 3.3.6 *(Étale morphism)*
If the morphism $f : X \to Y$ is unramified morphism, and it is also flat, then $f : X \to Y$ is an étale morphism.

Proposition 3.3.1 *(Properties of Étale morphism)*
Let $\phi : Y \to X$ is an étale morphism.

1. *For all $y \in Y$, $\mathscr{O}_{Y,y}$ and $\mathscr{O}_{X,x}$ have the same Krull dimension.*

2. *The morphism ϕ is quasi-finite.*

3. *The morphism ϕ is open.*

4. *If X is reduced, then so also is Y.*

5. *If X is normal, then so also is Y.*

6. *If X is regular, then so also is Y.*

3.4 Étale cohomology

As noted earlier, étale cohomology is a sheaf cohomology that preserves exactness on the long exact sequence of presheaves:

$0 \to F(U) \to \prod_i F(U_i) \to \prod_{i,j} F(U_{ij}) \to ...$ where $U \subset X$ is any open subset, and $\{U_i\}_{i \in I}$ is an open cover of U, and we denote $U_{ij} = U_i \times_U U_j$. If the sequence is exact, then we call this presheaf as sheaf with respect to étale topology.

For this section, I will finally define Étale site.

Definition 3.4.1 *(Étale Site)*
Étale topology is a Grothendieck topology. Let X be a fixed scheme. Category of all étale morphisms of any scheme to X is denoted $Et(X)$. Étale presheaf is a contravariant functor from a category $Et(X)$ to Sets.

Proposition 3.4.1 *(Comparison Theorem)*
Let X be a variety over complex field, $X(\mathbb{C})$ be the same set but acuquired standard topology from $\mathbb{C}$. If we let Λ be a finite set, we have an isomorphic relationship between étale cohomology and analytic cohomology, and the formula below describes the relationship between number theory and algebraic topology.

$H^r(X_{et}, \Lambda) \to H^r(X(\mathbb{C}), \Lambda)$ is naturally isomorphic.
Especially if $\Lambda = \mathbb{Z}/l^n\mathbb{Z}$, take an inverse limit by all the natural numbers $n \in \mathbb{N}$, and we will get homology group of p-adic integer. Also, since inverse limit lim is a functor, and since the lim functor commutes with the homology group, it naturally preserves the equality as:

$H^r(X_{et}, \mathbb{Z}_p) \to H^r(X(\mathbb{C}), \mathbb{Z}_p)$

Futhermore, if we apply tensor product $- \bigotimes_{\mathbb{Z}_l} \mathbb{Q}_l$ on both sides

$H^r(X_{et}, \mathbb{Q}_p) \to H^r(X(\mathbb{C}), \mathbb{Q}_p)$.

Proposition 3.4.2 *(Čech cohomology and Zariski sheaf)*
If given scheme X is noetherian separated, and if $\mathscr{F}$ is quasi-coherent, then Cech cohomology is isomorphic to sheaf cohomology as $\check{H}^p(\mathfrak{A}, \mathscr{F}) \cong H^p(X, \mathscr{F})$.

Proposition 3.4.3 *(Correspondence of Etale and Zariski Cohomology)*
$H^p(X_{et}, \mathscr{F}|_{et}) \cong H^p(X, \mathscr{F})$.

Particularly if $\mathscr{F}$ is the stucture sheaf, then

$H^p(X_{et}, \mathbb{G}_m) \cong H^p(X, \mathscr{O}_X)$.

Notice that if $p = 1$, then we can describe étale cohomology group by the Picard group $Pic(X)$

$H^1(X_{et}, \mathbb{G}_m) \cong H^1(X, \mathscr{O}_X) = Pic(X)$

Definition 3.4.2 *(Kummer Sequence)*
Kummer sequence is a sequence

$0 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 0$
$z \mapsto z^n$

where μ_n is a group of n-th root of unity (so it is a finite group!), $\mathbb{G}_m$ is a multiplicative group over an etale site. Also, there is additive version of Kummer Sequence, which is called Artin Schreier sequence:

$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_a \to \mathbb{G}_a \to 0$
$t \mapsto t^p - t$

Proposition 3.4.4 $H^1(X_{et}, \mathbb{G}_m) = H^1(X_{zar}, \mathscr{O}_X{}^{\times}) = Pic(X)$

where $\mathbb{G}_m$ is any multiplicative group.
As a result, $H^r(X_{et}, \mathbb{G}_m) = \Gamma(X, \mathscr{O}_X^{\times})r = 0$
$Pic(X)r = 1$
$0r > 1$

Proposition 3.4.5 *The cohomology groups $H^r(X_{et}, g_*\mathbb{G}_{j,n})$ and $H^r(X_{et}, Div_X)$ are zero for all $r > 0$.*

Proposition 3.4.6 $H^r(X_{et}, \mathscr{F}) \cong H^r(Spec(\mathscr{O}^h_{X,x}), \mathscr{F})$
where $\mathscr{O}^h_{X,x}$ is a henselization of $\mathscr{O}_{X,x}$.

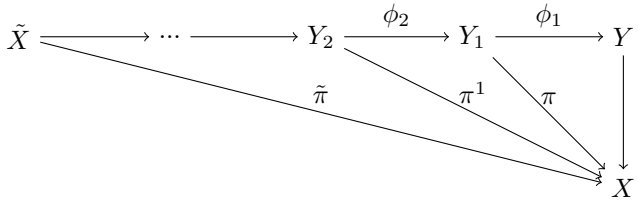
4 Étale Topology And Galois Theory

4.1 Étale Fundamenatal Group

Definition 4.1.1 *(Analytic Covering Space)*
Let X be a connected topological space, and let $\pi : Y \to X$ is a covering is π is continuous and surjective, and for all point $x \in X$, preimage of open neighborhood $U \ni x$ is disjoint union of open sets where each open set is homeomorphic

to U.

Now let $\pi : Y \to X$ and $\pi' : Y' \to X$ be two covering of X, and we let $\phi : (Y, \pi) \to (Y', \pi')$ be a transformation of covering, where $\pi = \pi' \circ \phi$. Now let $Cov(X)$ be a category of covering spaces where each object is a cover (Y, π), Then by the universal property, we have an initial object of covering $(\tilde{X}, \tilde{\pi})$ up to isomorphism. Here for an automorphism $Aut_X(\tilde{X})$, the natural morphism $Aut_X(\tilde{X}) \to \pi_1(\tilde{X}, x)$ is in fact isomorphism, or we might define ordinary fundamental group in this way.



Note that this universal covering space $\tilde{X}$ is simply connected (why?).

Definition 4.1.2 *(Étale Covering Space)*
We will consider the étale version of covering space and its fundamental group.

In étale space, we have a covering map $f : Y \to X$ in a similar way, and $\bar{x}$ be a geometric point. We let a morphism of covering maps $\phi : (Y, \pi) \to (Y', \pi')$ for some arbitrary covers. However, étale topology in general, there is no universal covering exists, so we construct étale fundamental group in a different way from the ordinary definition. We consider an arbitrary sequence of cover $... \to Y_i \to Y_{i+1} \to ...$, and for each i, we have an automorphism $Aut(Y_i)$, and we let $Aut(\tilde{X}) =_{def} \lim Aut_X(Y_i)$, as étale fundamental group, so we denote $\pi_1(X, \bar{x}) = Aut(\tilde{X})$.

Example 4.1.1 *(Étale Fundamental Group of Étale covering)*
For example, $\pi : \mathbb{A}_1 \setminus \{0\} \to \mathbb{A}_1 \setminus \{0\} : t \mapsto t^n$ is an étale map, and it is a covering space. Now we cosider all the possible étale covering of $\mathbb{A}_1 \setminus \{0\}$, and naturally we have a sequence where the final object is $(\mathbb{A} \setminus \{0\}, \pi)$. Then,
$\pi(\mathbb{A} \setminus \{0\}) = Aut_{\mathbb{A}\setminus\{0\}}(\tilde{X}) = \lim Aut_{\mathbb{A}\setminus\{0\}}(X_i)$.
In fact, $\pi(\mathbb{A} \setminus \{0\}) = \hat{\mathbb{Z}}$ where $\hat{\mathbb{Z}}$ is a completion of $\mu_n(k)$.

Example 4.1.2 *(Étale Fundamental Group of Algebraic Variety)*
Let X be an connected normal variety, and let $k(X)$ be a field of rational functions on X. Let L be a union of all finite separable extensions K of $k(X)$, then the étale fundamental group is Galois group as $\pi_1(X, \bar{x}) = Gal(L/k(X))$, and it

has a Krull topology structure.

Note that this makes a natural short exact sequence
$1 \to \pi_1(X_{k^{sep}}, \bar{x}) \to \pi_1(X, \bar{x}) \to Gal(k^{sep}/k) \to 1.$

Also similar thing is called "the most interesting things in mathematics" if you agree on that.
$1 \to \pi_1(X_{\mathbb{Q}^{al}}, \bar{x}) \to \pi_1(X, \bar{x}) \to Gal(\mathbb{Q}^{al}/\mathbb{Q}) \to 1.$

4.2 Galois Covering

Definition 4.2.1 *(Galois Covering)*
Let $\phi : Y \to X$ be a morphism, and G be a finite group. The right action of G is $Y \times G \to Y \times_X Y$, but from categorical view, it is equivalent to say $\alpha : G \to Aut_X(Y)$ where $\alpha(gh) = \alpha(h) \circ \alpha(g)$ is contravariant. If $Y \to X$ is called Galois covering of X with group G if the morphism $Y \times G \to Y \times_X Y : (y, g) \mapsto (y, yg)$ is an isomorphism. Here $Y \times G$ is an ordinary product which is a coproduct of disjoint union $Y \times G = \coprod_g Y_g$ where Y_g is isomorphism to Y for all g.

$\phi : Y \to X$ is surjective, finite, and étale of degree equal to the order of G, and in this case, $Aut_X(Y)$ will be a Galois group.

Definition 4.2.2 *(Base Change Of Scheme)*
For a morphism $f : X \to Y$ be a morphism of schemes, and we consider Y as a base scheme of X. Here let Z be any scheme, and we can naturally deduce another morphism $g : X \times_Y Z \to Z$, where $X \times_Y Z$ is a scheme whose base scheme is Z, and we call this operation as a base change of X.

$$\begin{array}{ccc} X \times_Y Z & \longrightarrow & Z \\ \downarrow & & \downarrow \\ X & \xrightarrow{f} & Y \end{array}$$

Proposition 4.2.1 *(Criterion of Étaleness in Scheme)*
Let $f : X \to Y$ be a morphism of schemes. Then f is étale if we assume

1. *f is locally of finite type.*
2. *X and Y are irreducible.*
3. *Y is normal.*
4. *f is dominant.*
5. *There is a surjective morphism $g : Z \to Y$ of schemes such that the base change of f by g is unramified.*

Then f is étale.

Proposition 4.2.2 *(Base Change Under Galois Cover)*
Let $f : X \to Y$ be a finite morphism between quasi-projective varieties where Y is smooth. Let $Z \to Y$ be a Galois cover for some scheme Z, and if the base change $Z \times_Y X \to Z$ is a finite étale cover, then f is also étale.

4.3 Galois Category

Definition 4.3.1 *(Galois Category)*
Let C be a category, and $F : C \to FinSet$ be a functor.

C has all finite limits and colimits.

F is exact and conservative.

For any morphism in C, $f : A \to C$, there is an object B and $g : A \to B$ and $h : B \to C$ such that $f = h \circ g$.

Definition 4.3.2 *(Galois Category with a view toward Tannakian Category)*
To be added.

Definition 4.3.3 *(Hopf-Galois Extension)*
To be added.

4.4 Future

In *Weil And Grothendieck Approaches To Adelic Points*, Conrad introduces adel ring is used to study adelic point of algebraic geometry.

Proposition 4.4.1 *(Algebraic Cycle And Chern Classes)*
To be added.

Proposition 4.4.2 *(Künneth Formula)*
To be added.

Proposition 4.4.3 *(Poincare Duality)*
To be added.

5 Weil Conjecture

Finally, we've come to Weil conjecture! Some people care Weil conjecture, and in my knowledge for example, Weil conjecture is used to calculate the Tamagawa numbers of all semisimple algebraic groups.

Definition 5.0.1 *(Tamagawa Number)*
For a semisimple algebraic group G defined over a global field k, Tamagawa number is a haar measure of quotient $G(A)/G(k)$, where $A = A(k)$ is an adele ring of a number field k.

Also, Deligne's proof of Weil conjecture is used to prove *hard Lefschetz theorem over finite fields*, *Ramanujan-Petersson conjecture*, *estimates for exponential sums* , and *Künneth type standard conjecture over finite fields*, and there are all interesting.

In this section, I will introduce the statement of Weil conjecture and Lefschetz pencil, main component to prove Weil conjecture.

5.1 Weil Conjecture

Let k be a field $k = \mathbb{F}_q$ for some prime q, and let X be a scheme of finite type over k. Let $\overline{X} = X \times_k \overline{k}$ be the corresponding scheme. Let k_r be a field $k = \mathbb{F}_{q^r}$

Let X_0 be a non-singular projective variety over $\mathbb{F}_q$. Let N_m be a number of points on X_0 with coordinates in $\mathbb{F}_{q^m}$.

We define zeta function to be $Z(X_0, t) = e^{(\Sigma_{m \geqq 1} N_m \frac{t^m}{m})} \in \mathbb{Q}[[t]]$

Weil conjecture could be said as an analogy of Riemann hypothesis, by defining finite version of Riemann zeta function over a finite field $\mathbb{F}_p$.

Proposition 5.1.1 *(Order of Galois Extension of Finite Field)*
A field of order q^r exists for all prime p and natural number $r \in \mathbb{N}$. In fact, order of any finite Galois extension over $\mathbb{F}_q$ is $\mathbb{F}_{q^r}$.

For example, F_9 exists because $F_3[i]$ is order 9, because it has basis $\{1, i\}$, and since coefficient would be arbitrary, there are $9 = 3^2$ different way of choosing c_1 and c_2 from $x = c_1 * 1 + c_2 * i$. Namely, the order of $F_3[i]$ is 9. In general, for a field $\mathbb{F}_q$ of arbitrary prime order, we may have a arbitrary degree of Separable Galois extensions, that says its order is q^r.

Example 5.1.1 *(one-dimensional projective space)*
For a one-dimensional projective space $\mathbb{P}^1$, the space has $q^r + 1$ points over $\mathbb{F}_{q^r}$. Thus,
$Z(\mathbb{P}^1, t) = e^{(\Sigma_{r \geqq 1}(q^r + 1)\frac{t^r}{r})}$,
which is easy to find a series $Z(\mathbb{P}^1, t) = \frac{1}{(1-t)(1-qt)}$

Proposition 5.1.2 *(Weil Conjecture)*

1. *Rationality. $Z(t)$ is a rational function of t, i.e., a quotinet of polynomials with rational coefficients.*

2. *Functional equation. Let E be the self-intersection number of the diagonal Δ of $X \times X$. Then $Z(t)$ satisfies a functional equation, namely $Z(\frac{1}{q^n t}) = \pm q^{nE/2} t^E Z(t)$*

3. *Analogue of the RIemann hypothesis. It is possible to write $Z(t) = \frac{P_1(t)P_3(t)...P_{2n-1}(t)}{P_0(t)P_2(t)...P_{2n}(t)}$ where $P_0(t) = 1 - t$ and $P_{2n}(t) = 1 - q^n t$ and for each $1 \leq i \leq n-1$, $P_i(t)$ is a polynomial with integer coefficients, and can be written as $P_i(t) =$*

$\prod(1-\alpha_{ij}t)$ *where* $|\alpha_{ij}| = q^{i/2}$ *is an algebraic integer, and this determines each* $P_i(t)$ *uniquely.*

4. *Betti numbers. Assuming 1.3, we can define i-th Betti number* $B_i = B_i(X)$ *to be the degree of the polynomial* $P_i(t)$*. Then we have* $E = \Sigma(-1)^i B_i$*. Furthermore, suppose tht* X *is objtained from a variety* Y *defined over an algebraic number ring* R*, by reduction modulo a prime ideal* $\mathfrak{p}$ *of* R*. Then* $B_i(X)$ *is equal to the i-th Betti number of the topological space* $Y_h = (Y \times_{\mathbb{R}} \mathbb{C})_h$ *i.e.,* $B_i(X)$ *is the rank of the ordinary cohomology group* $H_i(Y_h, \mathbb{Z})$*.*

Example 5.1.2 *(one-dimensional projective space)*
If $X = \mathbb{P}^1$*, the invariant* D *of* $\mathbb{P}^1$ *is* 2*, and one verifies immediately the functional equation which says in this case* $Z(\frac{1}{qt}) = qt^2 Z(t)$*.*

5.2 Lefschetz Fix Point Theorem

Proposition 5.2.1 *(Classical Lefschetz Fix Point Theorem)*
For a continuous morphism $f : X \to X$ *with analytic topological space* X *which is compact (and orientable) and triangulable space, and let* $L(f)$ *be a Lefschetz number defined as* $L(f) = I(\Delta, graph(f))$ *where* $\Delta : X \to X \times X$ *is a diagonal morphism, and* $graph(f) : X \to X \times X : x \mapsto (x, f(x))$ *is a morphism of graph.* I *is called an intersection number, which is a sum of orientation number. Orientation number is given by* $\{\pm 1\}$ *because this is the orientation, and this is why* X *needs to be oriented.*

For a morphism $f : X \to Y$ *where* $Z \subset Y$ *is transversal to* f*,* $f^{-1}(Z)$ *is* 0*-dimensional pre-image. Based on that fact, We define intersection number* $I(f, Z)$ *as a sum of orientation number for each point of* $f^{-1}(Z)$*. Particulaly, if* f *is identity, and* $X \subset Y$*, then the intersection number is denoted by* $I(X, Z)$*.*

If $L(f) \neq 0$*, then it has a fix point.*

Proposition 5.2.2 *(More Classical Lefschetz Fix Point Theorem)*
More formally, Lefschetz number can be defined by singular homology group of rational coefficients:

$$\Lambda_f = \Sigma(-1)^k tr(f_* | H_k(X, \mathbb{Q})),$$

where the induced sequence of singular homology group is bounded, so we have finite times of summation. The induced map $f_* : C_k(X) \to C_k(X)$ *is a linear map of the singular chain complexes* $C_k(X)$*, The* tr *map is an ordinary matrix trace of the linear map* f_**, and if* $\Lambda(f) \neq 0$*, then it has a fix point.*

Proposition 5.2.3 *(Étale Lefschetz Fix Point Theorem)*
Let X *be a variety defined over a finite field* k *with* q *elements, and let* $\overline{X}$ *be a base change of* X *by the algebraic closure* $\bar{k}$ *of* k*. Let* F_q *be a Frobenius automorphism of* $\overline{X}$ *such that* $F_q : x_1, ..., x_n \mapsto x_1^q, ..., x_n^q$*. Thus the fixed points of* F_q

are exactly the points of X with coordinates in k, and the set of such points are denoted by $X(k)$. By this context, we have Lefschetz number as the cardinality of the finite set $X(k)$ as:

$$\#X(k) = \Sigma(-1)^i tr(F_q^* | H_c^i(\overline{X}, \mathbb{Q}_l))$$

and this formula involves the trace of Frobenius on the étale cohomology, with compact supports, of $\overline{X}$ with values in the field of l-adic numbers, where l is co-prime to q.

5.3 Lefschetz Pencil

The remaining part of proof is that "F acts rationally on $H^{n+1}(X, \mathbb{Q}_l)$ and its eigenvalues α satisfy $q^{n/2} < |\alpha| < q^{n/2+1}$".

Here I will briefly introduce key idea for proving Weil conjecture, which is Lelfschetz pencil.

Definition 5.3.1 *(Lefschetz Pencil)*
Hyperplane is a form $H = \Sigma a_i T_i$ in projective space $\mathbb{P}^m$. The set of all hyperplanes generates the dual projective space $\check{\mathbb{P}}^m$, and a line D in $\check{\mathbb{P}}^m$ is called Lefschetz pencil of hyperplanes in $\mathbb{P}^m$.

For a projective space $\mathbb{P}^m$, let H_0 and H_∞ be two distinct hyperplanes (subvariety) in D, and we let $A = H_0 \cap H_\infty$ be a Lefschetz pencil, which is a linear subvariety of codimension 2. In general, any Lefschetz pencil is written by the linear combination $\alpha H_0 + \beta H_\infty = \bigcap_{t \in D} H_t$ with $(\alpha : \beta) \in \mathbb{P}(k)$.

Definition 5.3.2 *(Lefschetz Pencil)*
A line D in $\check{\mathbb{P}}^m$ is said to be Lefschetz pencil for $X \subset \mathbb{P}^m$ if

1. *The axis A of the pencil $(H_t)_{t \in D}$ cuts X transversally.*
2. *The hyperplane sections $X_t = X \bigcap H_t$ of X are nonsingular for all t in some open dense subset U of D.*
3. *for $t \notin U$, X_t has only a single singularity, and the singularity is an ordinary double point.*

For any situations, Lefschetz pencil does exist.

Proposition 5.3.1 *(Lefschetz Pencil)*
Let $D = (H_t)$ be a Lefschetz pencil for X with axis $A = \bigcap H_t$. Then, there exists a variety X^* and maps

$$X \leftarrow X^* \rightarrow^\pi D$$

1. *the map $X^* \to X$ is the blowing up of X along $A \bigcap X$.*

2. *the fibre of $X^* \to D$ over t is $X_t = X \bigcap H_t$.*

Moreover, π is proper, flat, and has a section.

Definition 5.3.3 *(Cohomology of Lefschetz Pencil)*
To be added.

6 Class Field Theory

In number theory, class field theory is an idea that connects global fields to local fields

Proposition 6.0.1 *(Artin Reciprocity Law)*
Artin reciprocity law is an area of class field theory.

Let L/K be a Galios extension of global fields and C_L stand for the idéle class group of L. Artin reciprociry law claims that there is a canonical isomorphism of global symbol map:

$$\theta : C_K/N_{L/K}(C_L) \to Gal(L/K)^{ab}.$$

where $Gal(L/K)^{ab}$ is an abelianization. Abelianization of a group G is a quotient by its commutator $G^{ab} = G/[G,G]$, which is an abelian group. On the other hand, we have canonical isomorphism of local symbol map:

$$\theta_\nu : K_\nu^\times/N_{L_\nu/K_\nu}(L_\nu^\times) \to G^{ab}.$$

Proposition 6.0.2 *(Serre Duality Theorem)*
If X is a smooth curve, there is an alternative version of proof of Serre duality theorem with adele ring.

Let X be a smooth curve over the complex numbers, one can define an adele of function $\mathbb{C}(X)$, which is a global field, exactly as the finite field case. The Serre duality on X is:

$$H^1(X, \mathscr{L}) \cong H^0(X, \Omega_X \bigotimes \mathscr{L}^{-1}).$$

It may be deduced from an adele ring $\mathbb{A}_{\mathbb{C}(X)}$. Here $\mathscr{L}$ is a line bundle on X.

7 Future

From the arguments above, I have realized that there are many topics of number theory that can be seen in a language of algebraic geometry, and even if I will not do any research in number theory, I consider it might not be a waste of

time, and it might be helpful to current my speciality, which is algebraic geometry. Lastly, I want to introduce my future interests in number theory, though I cannot promise to finish all of them.

There are many things to do for number theory which connect to algebraic geometry. For example, algebraic cycle in étale cohomology theory makes Tate conjecture, and it is an arithmetic analogy of Hodge conjecture. Also, though in the last chapter, I didn't finish my satisfactory level, there is a future prospective to my study project. Adel ring might be used to study class field theory, which has a further generalization to anabelian geometry, and if we study anabelian geometry and p-adic Teichmüller theory and p-adic Hodge theory, these theories might be generalized to interuniversal teichmüller theory (link). Also, representation of algebraic groups over local fields and adels, automorphism form might be related to Galois group and algebraic number theory, which is Langlands program. The theory of Lefschetz Pencil may be applied to study Picard-Lefschetz theory for Fukaya category (link).

Another of my speciality is Lie algebra, which is one of my qual topics. Lie algebra might have some relations with number theory. For example, Metaplectic representation is a representation of finite dimensional Lie algebra, and its Weyl group action studies a harmonic analysis of Hecke algebra (link). Unramified representation of Lie algebra is used to study local Satake isomorphism for Langlands program. Satake isomorphism identifies the Hecke algebra of a reductive group over a local field with a ring of invariants of the Weyl group, which is number theoretical, but there is also an geometric version (link). Also, for the case of infinite dimensional Lie algebra, monstrous moonshine conjecture is proved by infinite dimensional generalized Kac-Moody algebra acting on the monster group, and it is used to study the fourier coefficients of j-invariant as a modular elliptic function (link).

Number theory might also be used in analysis. For example, they might be p-adic analysis, p-adic integral, and fractal geometry, Ergodic theory, but these idea can be applied to Alain Connes' non-commutative geometry, and since I am geometer myself, that should be an interesting topic if it is algebraic or not (link).

References

[1] Alfonso, Lombardi (2018), *Local Bézout Theorem for Henselian rings* https://arxiv.org/abs/1512.04306

[2] Behrend (2012), *Introduction to Algebraic Stacks*, https://secure.math.ubc.ca/ behrend/math615A/stacksintro.pdf

[3] Bhatt, *The Étale Topology* http://www-personal.umich.edu/ bhattb/math/etalestcksproj.pdf

[4] B. Conrad (2011), *Weil And Grothendieck Approaches To Adelic Points*< https://math.stanford.edu/ conrad/papers/adelictop.pdf

K. Conrad, *A Multivariable Hensel's Lemma* https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf

[5] Choudhury, Deshmukh, Hogadi(2020), *The Nisnevich Motive Of An Algebraic Stack*, https://arxiv.org/abs/2012.13304

[6] Christian Serpé (2010), *Descent Properties Of Equivariant K-Theory* https://arxiv.org/abs/1002.2565

[7] Guillemin, Pollack (1974), *Differential Topology*

[8] J.S. Milne(2013), *Lectures on Étale Cohomology*, https://www.jmilne.org/math/CourseNotes/LEC.pdf

[9] Kashiwara, Schapira (2005), *Categories and Sheaves* https://www.maths.ed.ac.uk/ v1ranick/papers/kashiwara2.pdf

[10] Keith Conrad (2020), *Infinite Galois Theory* https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf

[11] Marks, *Galois representations*, https://people.math.harvard.edu/ smarks/mod-forms-tutorial/mf-notes/galois-reps.pdf

[12] Robin Hartshorne (1977) *Algebraic Geometry*,

[13] Summers (2020), *Galois and Tannakian Categories* https://nedsummers.com/wp-content/uploads/2020/04/GaloisTannakianCategoriesNScorrect.pdf

[14] Wikipedia