AN APPROACH TO LOCAL FIELD PROBLEMS

HEJING SHI

Abstract. The ultimate goal of number theory is essentially solving Diophantine equations on $\mathbb{Q}$. However, the problems are usually too hard if we do not think out of $\mathbb{Q}$. One of the main principle in number theory is to solve the equation in each local field, and then figure out when and how the local fields solution may implies a result in global field.

A natural question rising in this process is : Why is local field nice? What are the useful tools that we can use to solve local field problems?

In this talk, I will give out three concrete examples to illustrate this central but simple idea: local field is decent and we do have powerful tools. The first example is about totally ramifies extension(which is some of my experiments with Michael Barz), the second example is about elliptic curve where we are trying to estimate the number of torsion points, and the third one is about Galois representation where we give a brief sketch of the proof of Fermat's Last Theorem.

Contents

1. Definition

We will first define the objects that we are interested in today.

Not assuming everybody familiar with definition of local fields, we will give a very brief but vague definition here. For more precise definition and why "local field" is called this way, one can refer to any textbook in Algebraic Geometry.

Convention 1.1. Here, the local fields that we will discuss is just the finite extension of $\mathbb{Q}_p$.(since it has characteristic 0, every extension of $\mathbb{Q}_p$ is separable).

1.1. Local number field.

Definition 1.1. discrete valuation

A discrete valuation $\nu : F \to \mathbb{Z} \bigcup \{\infty\}$ that satisfies the following properties:

- $\nu(xy) = \nu(x) + \nu(y)$
- $\nu(0) = \infty$
- $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$

Remark 1.2. (1) The simplest example is $\mathrm{ord}_p(\cdot)$.

(2) The discrete valuation can determine a topology in the local field K by taking

$$V_n = \{x \in K | \nu(x-a) \geq n\}$$

as a fundamental system of neighborhoods for each point $a \in K$. This topology coincides with the one that is defined by the metric

$$d_{\nu,c}(x,y) = c^{\nu(x-y)} \quad (x \neq y)$$

where $0 < c < 1$ is a fixed real number.

Definition 1.3. local number field

Local field is just complete discrete valuation field with finite residue field.

(another interpretation) A local number field is a finite-dimensional extension K of $\mathbb{Q}_p$, for some prime number p. One also says that K is a **p-adic field**.

Next, we offer two ways to understand what is "complete". For convenience, the local number field we take here is just $\mathbb{Q}_p$.

Recall in the world of real numbers, a sequence of rational numbers may converge to a number which is not a rational number, as the following example shows:

$$1.4, 1.41, 1.414, 1.4142, ... \to \sqrt{2} \notin \mathbb{Q}$$

That implies the world of rational numbers is an incomplete world where sequences such as the one above may not have a limit even if it "should converge", which specifically refers to it being a Cauchy sequence(for a rigorous definition, one can refer to any textbook in Analysis). And if a field K is **completed**, it means the Cauchy sequences over K converges to some element in K.

Thus, $\mathbb{Q}_p$ is nothing but adding the "limit" of Cauchy sequences(in p-adic valuation/distance sense) over $\mathbb{Q}$ into $\mathbb{Q}$.

One thing that helps to understand completion/completed and distinguish $\mathbb{R}$ and $\mathbb{Q}$ is that For any $x \in \mathbb{Q}_p$,

$$x = \sum_{n=m}^{+\infty} a_n p^n$$

.

And for $x \in \mathbb{R}$

$$x = \sum_{-\infty}^{n=m} a_n p^n$$

Note that their intersection is just $\mathbb{Q}$.

For further discussion, we give out some necessary definition related to local field.

Definition 1.4. The set

$$\mathcal{O}_F = \{x \in F : \nu(x) \geq 0\}$$

is called **ring of integers**.

We usually write

$$\mathfrak{p} = \{x \in F : \nu(x) \geq 1\}$$

Remark 1.5. The intuition for ring of integers is: integers with one prime!(this is also why it is called local, because no other prime is useful here)

The following proposition explains why local fields are decent and comparatively easy to deal with.

Proposition 1.6. *Let F be a field with a discrete valuation ν.*

1. *$\mathcal{O}_F$ is a ring. The group of units consists those elements having zero valuation.*
2. *$\mathfrak{p}$ is its unique maximal ideal(and also prime ideal)*
3. *There exists $\pi \in \mathcal{O}_F$ such that $\mathfrak{p} = (\pi)$, and then all ideals of $\mathcal{O}_F$ are of the form (π^n) for some $n \in \mathbb{N}$. In particular, $\mathcal{O}_F$ is PID.*
4. *Every non-element $x \in \mathcal{O}_F$ can be written uniquely as $x = \pi^n u$ where u is a unit.*

Definition 1.7. The field

$$\mathbb{F} = \mathcal{O}_F/\mathfrak{p}$$

is called residue field of F.

Remark 1.8. The fact that the residue field is a finite field makes the problem about it so simple.(Because every extension of it is cyclic, generated by Frobenius map).

The thing to note here is that: not only is it simple, but it can provide us very important information as well.

Theorem 1.9. *(Hensel's lemma) Let F be a field that is complete with respect to a discrete valuation ν. Let $f \in \mathcal{O}_F[X]$ be a polynomial such that there is a factorization in residue field :$\overline{f} = f_1 f_2$ with $f_i \in \mathbb{F}[X]$ relatively prime. Then there is a factorization $f = gh$ with $g, h \in \mathcal{O}_F[X]$ satisfying $\overline{g} = f_1$ $\overline{h} = f_2$ with* $\deg(g) = \deg(\overline{g})$

Remark 1.10. This indicates that an extension of residue field can be lifted to the extension of local field. But that gives out a requirement for the extension of local field. That is, the irreducible polynomial associated to the extension must not be reducible in residue field. If it is, then this reduction will lose information.

Thus, we give out the following definition.

Definition 1.11. Let F be local number field. K/F be finite extension.
K/F is called **unramified extension** if $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(\mathbb{K}/\mathbb{F})$.
K/F is called **totally ramified extension** if $\mathrm{Gal}(K/F) \cong \{1\}$

The reason why we tend to turn problems in $\mathbb{Q}$ into local field problems is that: local field has more decent structure. We know that field extensions are usually quite complicated. But in local world, all the extensions can be divided into two part: unramified extension and totally ramified extension.

Proposition 1.12. *Let K/F be an extension of p-adic fields. Then there exists a unique intermediate field K_0, with $F \subset K_0 \subset K$, called the inertia subfield of K/F, with the following property:*
For any field with $F \subset L \subset K$, the extension L/F is unramimified $\Leftrightarrow L \subset K_0$.
This is equivalent to say, K/K_0 totally ramified and K_0/F unramified.

Since the unramified extension are totally determined by the extension of residue field, one can even know the explicit extension given the extension degree.

However, residue field can help with totally ramified case as well. And we give out a naive but concrete example as following.

2. A concrete but naive example

Claim 2.1. For any $d \in \mathbb{N}$, $\exists L/\mathbb{Q}_p$ totally ramified such that

- $[L : \mathbb{Q}_p] = d$
- $X^p - 1 = 0$ has no solution in L

We first consider following special case. Assume that $e = p - 1$, we claim that one of the following field must have a=0

- $\mathbb{Q}_p(p^{\frac{1}{p-1}})$
- $\mathbb{Q}_p((up)^{\frac{1}{p-1}})$, where u satisfies the following conditions
  $u \in \mathbb{Q}_p$ and that $\mathrm{ord}_p(u) = 0$
  $u^{\frac{1}{p-1}} \notin \mathbb{Q}_p(p^{\frac{1}{p-1}})$

Firstly, the above two field extensions are totally ramified with ramification index $e = p - 1$. However, they are not isomorphic. Because if so, then it will contradict with the condition that $u^{\frac{1}{p-1}} \notin \mathbb{Q}_p(p^{\frac{1}{p-1}})$.

That means, the cyclotomic extension $\mathbb{Q}_p(\zeta_p)$ can only(and will) be isomorphic to one of them. Thus one of them must have $a = 0$.

Next, we show the existence of such u in second construction. To see that $u^{\frac{1}{p-1}} \notin \mathbb{Q}_p(p^{\frac{1}{p-1}})$, we only need to show that the equation

$$X^{p-1} = u$$

does not have solution in $\mathbb{Q}_p(p^{\frac{1}{p-1}})$.

This is where residue field comes to play.

Since $X^{p-1} = 1$ for every $X \in \mathbb{F}_p$, thus we know that we only need to take $u \in \mathbb{Q}_p$ s.t. $u \neq 1$ in $\mathbb{F}_p$. Thus we know that this kind of u always exists.

Similarly, we can also assume that $e = n \cdot (p-1)$ and the reasoning is totally the same as above.

Remark 2.1. I would like to highlight that so far this is not a trivial result(I guess). I have been thinking about using group theory to solve this problem. But by the explicit formula of unramified extension, it occurs to me that totally ramified extension(although might not be unique), may not be able to have arbitrary Galois group as we expected. Thus, the fail to the generalized group theory problem does not mean it impossible to solve the problem concerned.

2.1. A little bit background.

Why is this important, you might wonder. This is actually a problem that I have noticed while reading and has been working on since.

Theorem 2.2. *The topological group $K^\times$, with the topology induced from the valuation on the p-adic field F, is topologically isomorphic to*

$$\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$$

where $d = [K : \mathbb{Q}_p]$, the residue field $\mathbb{K}$ has q elements, and $a \geq 0$ is some integer. Moreover, under the following identification:

- *$K^\times \to \mathbb{Z}$ correspond to the projection to the first factor is ν, the normalized valuation*
- *$0 \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$ corresponds to $\mathcal{O}_K^\times$*
- *$0 \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times$ corresponds to the roots of unity contained in K*

For unramified extension L, one can know that there is no p-torsion in L. That indicates all the p-torsion comes from the totally ramified sub-field. Different from unramified extension, there can be many totally ramified extension up to isomorphic sense, thus it is natural to ask the bound of the number of p-torsion.

While the lower bound is sharp and solved completely, the upper bound remains unknown and I have been doing several experiments on it.

3. Some serious applications

3.1. **Elliptic Curve.** Next, I will introduce an important problem on elliptic curve and illustrate how important it is to consider reduction.

Definition 3.1. Here, one can take elliptic curve as some algebraic curve defined by $E : y^2 = x^3 + Ax + B$ with "good" pair (A, B)

A famous and fundamental result of elliptic curve is

Theorem 3.2. *Mordell-Weil K an arbitrary number field.*

$$E(K) \cong E(K)_{tor} \oplus \mathbb{Z}^r$$

A very natural follow-up question would be: How do we know about the size of torsion?

The fact is: if we consider good reduction(did not quote because this name is real), this can simplify our problem based on the following two facts.

Lemma 3.3.

$$E(\mathbb{Q})_{tor} \hookrightarrow E(\mathbb{F}_p) \quad if\ p \nmid 4A^3 + 27B^2$$

About elliptic curve over finite field, we have the classical result as following:

Lemma 3.4. *Hasse*

$$\#E(\mathbb{F}_p) = p + 1 - a_p$$

where a_p is some constant such that $|a_p| \leq 2\sqrt{p}$

Here we give out a reason why the above two lemmas are useful. Given a concrete elliptic curve, we can compute the torsion explicitly.

Example 3.5. consider $y^2 = x^3 - 2$ which is an elliptic curve over $\mathbb{Q}$, it can be computed that the discriminant of the curve is 108.

A direct proof shows that:

$$\#E(\mathbb{F}_5) = 6$$
$$\#E(\mathbb{F}_7) = 7$$

Since $\#E(\mathbb{Q}_{tor})|\#E(\mathbb{F}_p)$, thus we know that $\#E(\mathbb{Q}_{tor}) = 1$

Actually for $\mathbb{Q}$, the structure of $E(\mathbb{Q})$ is now explicit owing to the work by Barry Mazur.

Theorem 3.6. *Mazur $E(\mathbb{Q})_{tor}$ is one of the following*

- $\mathbb{Z}/N\mathbb{Z}$ *for* $1 \leq N \leq 10$ *or* $N = 12$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *for* $1 \leq N \leq 4$

and actually each group occurs for some curve $E/\mathbb{Q}$

However, for general number field, the structure of torsion remains unknown. But there is following conjecture

Conjecture 3.7. *$|E(K)| \leq C_K$, where C_K is some constant depending only on the number field K.*

3.2. **Galois Representation.** I have also been learning some Galois representation this summer, and this area is another strong proof that reduction(or residual representation) provides essential information.

Notation 3.8. $G_K := \mathrm{Gal}(\overline{K}/K)$ which is the absolute Galois group.

One fundamental problem in number theory is to understand subgroups of this absolute Galois group(up to conjugation). That leads to the study of Galois representation $\rho : G_K \to GL_N(A)$ where such A is a complete noetherian local ring with finite residue field k.

Analogue to the discussion above, we have so called **residual representation** defined as below

$$\overline{\rho} : G_K \to GL_N(A) \to GL_N(k)$$

It seems like we are cutting out lots of information again, but with some restrictions on the residual representation, it can be lifted to the original representation we want(this process is called **deformation**) and gives out the classification.

One of the key theorem is as following:

Proposition 3.9. *Suppose $\overline{\rho} : G_K \to GL_N(k)$ is absolutely irreducible, then there exists a "universal coefficient ring" $R = R(\overline{\rho})$ with residue field k and a "universal deformation" of $\overline{\rho}$ to R*

$$\rho^{univ} : G_K \to GL_N(R)$$

satisfying that:

Given arbitrary coefficient-ring A with residue field k

$$\begin{array}{ccccc} G_{K,S} & \xrightarrow{\rho^{univ}} & GL_N(R) & \longrightarrow & GL_N(k) \\ & \searrow^{\rho} & \downarrow{\scriptstyle \exists 1} & & \Vert \\ & & GL_N(A) & \longrightarrow & GL_N(k) \end{array}$$

the above diagram commutes.

Actually, irreducibility is not the only restriction that we can impose on the residual representation. Combination with other restriction such as ramification and flatness gives out a contradiction of non-trivial solution to Fermat's equation, which leads to the proof of Fermat's Last Theorem.

The landscape is as follows:

Non-trivial solution of Fermat's equation

$\longrightarrow$ residual representation$\overline{\rho}$ with a bunch of restrictions

$\longrightarrow$ restrictions on modular forms(some functions) associated with $\overline{\rho}$. But because modular forms itself contains many strict restrictions, and those restrictions contradict with each other.