

CLASS FIELD THEORY

WEEK 3

JAVIER FRESÁN

Recall from the introduction to the course that, given a complete discrete valued field K with finite residue field \mathbb{F}_q , the main theorem of local class field theory asserts the existence of a continuous group morphism

$$\rho_K: K^\times \longrightarrow \text{Gal}(K^{\text{ab}}/K),$$

such that: (1) for each finite abelian extension L/K , ρ_K induces an isomorphism

$$K^\times / N_{L/K}(L^\times) \xrightarrow{\sim} \text{Gal}(L/K);$$

and (2) it fits into a commutative diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{\rho_K} & \text{Gal}(K^{\text{ab}}/K) \\ \nu_K \downarrow & & \downarrow \\ \mathbb{Z} & \xrightarrow{\rho_{\mathbb{F}_q}} & \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q). \end{array}$$

Last week I explained the basics of infinite Galois theory, in particular, the structure of the above Galois groups. Recall that $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is the profinite completion $\widehat{\mathbb{Z}}$ of the integers and the map $\rho_{\mathbb{F}_q}$ sends 1 to the Frobenius automorphism $x \mapsto x^q$. Today and next week we will properly introduce local fields and study their Galois theory. One of the main results will be that there is a maximal unramified subextension $K \subseteq K^{\text{ur}} \subseteq K^{\text{ab}}$ whose Galois group is isomorphic to $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. This yields, by restriction, the right vertical map.

1. DISCRETE VALUATION RINGS

Recall that a *principal ideal domain* is a commutative ring A which is an integral domain (*i.e.* does not contain zero divisors) and has the property that every ideal is principal (*i.e.* can be generated by a single element).

Definition 1.1. A *discrete valuation ring* is a principal ideal domain A which has a unique non-zero¹ prime ideal \mathfrak{m} . A generator π of \mathfrak{m} is called a *uniformizer* and the field² $\kappa = A/\mathfrak{m}$ is called the *residue field* of A .

The group of invertible elements A^\times is equal to $A \setminus \mathfrak{m}$ (indeed, if $x \notin \mathfrak{m}$, the ideal (x) has to be the whole ring). It follows that, up to multiplication by an element of A^\times , the only

¹Recall that (0) is a prime ideal in an integral domain

²In a principal ideal domain A all non-zero prime ideals are maximal. Indeed, if (x) is a prime ideal and $(x) \subseteq (y)$ but $y \notin x$, then $x = ty$ implies $t = xz$ for some $z \in A$, hence $yz = 1$. But this shows that $(y) = A$.

irreducible³ element of the ring is π . Therefore, every non-zero element x of A can be written uniquely as $x = u\pi^n$ for an integer $n \geq 0$ and an invertible element $u \in A^\times$. The integer $v(x) = n$ does not depend on the choice of the uniformizer and is called the *valuation*⁴ of x . We extend v to A by setting $v(0) = +\infty$. Then the function $v: A \rightarrow \mathbb{Z}_{\geq 0} \cup \{+\infty\}$ satisfies

$$v(x+y) \geq \min(v(x), v(y)), \quad v(xy) = v(x) + v(y). \quad (1)$$

Let K be the fraction field of A . The valuation extends to K by setting

$$v(x/y) = v(x) - v(y),$$

which does not depend on the choice of representatives by (1). This yields a surjective group morphism $v: K^\times \rightarrow \mathbb{Z}$ such that

$$\begin{aligned} A &= \{x \in K \mid v(x) \geq 0\}, \\ \mathfrak{m} &= \{x \in K \mid v(x) > 0\}. \end{aligned}$$

Both points of view are thus equivalent.

Lemma 1.2. Let K be a field, together with a surjective map $v: K^\times \rightarrow \mathbb{Z}$ satisfying (1). Then $A = \{x \in K \mid v(x) \geq 0\}$ is a discrete valuation ring (called the *ring of integers* of K).

Proof. Let $\pi \in K^\times$ be an element such that $v(\pi) = 1$. Any $x \in K^\times$ can then be written as $x = u\pi^n$ with $n = v(x)$ and $v(u) = 0$. Let u^{-1} be the inverse of u in K . Then $v(u^{-1}) = 0$, hence u belongs to A^\times . This shows that all the non-zero ideals of A are of the form $\pi^n A$ for some $n \geq 0$. Therefore, A is a discrete valuation ring. \square

Example 1.3.

- (1) Let p be a prime number. The subring $\mathbb{Z}_{(p)}$ of \mathbb{Q} given by

$$\mathbb{Z}_{(p)} = \left\{ \frac{x}{y} \mid x, y \in \mathbb{Z}, p \text{ does not divide } y \right\}$$

is a discrete valuation ring with maximal ideal $p\mathbb{Z}_{(p)}$ consisting of those x/y such that p divides x . The residue field is \mathbb{F}_p and the field of fractions is \mathbb{Q} . The associated valuation $v_p: \mathbb{Q}^\times \rightarrow \mathbb{Z}$ is given by $v_p(x) = n$ if one writes $x = p^n a/b$ with a and b not divisible by p . It is called the *p-adic valuation*.

Remark 1.4. The ring $\mathbb{Z}_{(p)}$ is the localisation of \mathbb{Z} at the prime ideal p . More generally, the localisation of a Dedekind domain (*e.g.* the ring of integers of a number field) at a *non-zero* prime ideal is a discrete valuation ring.

- (2) Let p be a prime number. Recall that we have canonical projections

$$\mathbb{Z}/p \longleftarrow \mathbb{Z}/p^2 \longleftarrow \dots \mathbb{Z}/p^{n-1} \xleftarrow{\varphi_n} \mathbb{Z}/p^n \longleftarrow \dots \quad (2)$$

and one defines the ring of p-adic integers as the limit

$$\mathbb{Z}_p = \lim_n \mathbb{Z}/p^n \mathbb{Z},$$

³Recall that an *irreducible* element is a nonzero non-unit element which cannot be written as a product of two non-units.

⁴“Discrete” refers to the fact that v takes values in \mathbb{Z} .

which consists of sequences $(x_n)_n$ such that $x_n \in \mathbb{Z}/p^n$ and $\varphi_n(x_n) = x_{n-1}$. It is a discrete valuation ring with maximal ideal $p\mathbb{Z}_p$ and residue field \mathbb{F}_p . The invertible elements are those $(x_n)_n$ with $x_1 \neq 0$. The valuation is given by

$$v(x) = \begin{cases} 0 & x \in \mathbb{Z}_p^\times \\ n & \text{greatest integer such that } x_n = 0. \end{cases}$$

Note that, if $x_n = 0$, then $x_m = 0$ for all $m \leq n$ by the compatibility with the projections (2). The fraction field $\mathbb{Q}_p = \text{Frac}(\mathbb{Z}_p)$ is the field of *p-adic numbers*.

(3) Let k be a field. The ring of *formal power series*

$$k[[t]] = \left\{ f = \sum_{n=0}^{+\infty} a_n t^n \mid a_n \in k \right\}$$

is a discrete valuation ring with maximal ideal $t k[[t]]$ and residue field k . Its fraction field is the field $k((t))$ of *Laurent series*, that is,

$$k((t)) = \left\{ f = \sum_{n \geq n_0} a_n t^n \mid n_0 \in \mathbb{Z}, a_n \in k, a_{n_0} \neq 0 \right\}.$$

The valuation assigns to f as above the integer n_0 .

Remark 1.5. These examples show that K and the residue field κ can have different characteristics; it is called the *mixed* or *unequal* characteristic case. However, if K has characteristic $p > 0$, then κ has characteristic p as well, and if κ has characteristic zero, then K has characteristic zero. Here are the three possibilities:

	K	κ
char	0	0
char	p	p
char	0	p

2. COMPLETE DISCRETE VALUED FIELDS

2.1. From valuations to absolute values. Let K be a discrete valued field as before, $v: K^\times \rightarrow \mathbb{Z}$ the valuation and A the ring of integers. Let $0 < a < 1$ be a real number⁵. We define a map

$$|\cdot|: K \rightarrow \mathbb{R}_{\geq 0} \tag{3}$$

by setting $|0| = 0$ and, for all $x \in K^\times$,

$$|x| = a^{v(x)}.$$

It is immediate to verify that $|\cdot|$ satisfies the following three properties:

$$\begin{aligned} |x| = 0 &\iff x = 0 \\ |xy| &= |x||y|, \\ |x + y| &\leq \max(|x|, |y|). \end{aligned}$$

Therefore, the map (3) is a *non-archimedean* (or *ultrametric*) absolute value on K .

⁵If the residue field is finite, with q elements, the standard choice will be $a = q^{-1}$.

Remark 2.1. The ring of integers of K is given by the elements with $|x| \leq 1$. That this is indeed a ring uses the fact that the absolute value is non-archimedean (the set of real numbers with usual absolute value ≤ 1 is obviously not a subring of \mathbb{R}).

To the absolute value is attached the topology corresponding to the distance

$$d(x, y) = |x - y|,$$

and different choices of a give equivalent topologies. It is a *totally disconnected* topological space, meaning that its connected components are exactly the singletons.

2.2. Complete fields. Recall that $(K, |\cdot|)$ is said to be *complete* if all Cauchy sequences⁶ $(a_n)_n$ converge to an element a of K , *i.e.* $\lim_{n \rightarrow +\infty} |a_n - a| = 0$.

Example 2.2.

- (1) The field \mathbb{Q} , together with the absolute value $|\cdot|_p$ obtained from the p -adic valuation is *not* complete. For instance, one can show that

$$x_n = \sum_{j=0}^n p^{j^2}$$

is a Cauchy sequence which does *not* converge to a rational number (do the exercise!).

- (2) The field of Laurent series $k((t))$ is always complete.

Starting from a non-complete field K , there is a standard procedure to obtain a complete one called *completion*. Namely, one considers the set R of all Cauchy sequences in K . Together with termwise addition and multiplication, it is a ring. Null-sequences (*i.e.* those $(a_n)_n$ with the property that, for all $\varepsilon > 0$, there exists N such that $|a_n| < \varepsilon$ for all $n \geq N$) form a maximal ideal \mathfrak{m} . Then one defines the completion to be the quotient

$$\widehat{K} = R/\mathfrak{m}.$$

The absolute value extends from K to \widehat{K} by the rule

$$|(a_n)| = \lim_{n \rightarrow +\infty} |a_n|.$$

The limit exists because $|a_n|$ is a Cauchy sequence of real numbers. The field \widehat{K} is complete for this absolute value and there is an injective map $K \hookrightarrow \widehat{K}$ sending a to the constant Cauchy sequence (a, a, \dots) .

Example 2.3. The completion of $(\mathbb{Q}, |\cdot|_p)$ is the field \mathbb{Q}_p of p -adic numbers. Since $\mathbb{Q} \neq \mathbb{Q}_p$, this is an alternative way to show that \mathbb{Q} is not complete.

The following proposition will be proved in the exercise session this week:


Proposition 2.4. A discrete valued field K is locally compact (*i.e.* every point has a compact neighborhood) if and only if it is complete and the residue field is finite.

When the assumptions are satisfied, the ring of integers $A = \{x \in K \mid |x| \leq 1\}$ is compact. It is then a Hausdorff, compact and totally disconnected group, hence a profinite group (see Week 2). For example, $\mathbb{Z}_p = \lim_n \mathbb{Z}/p^n$ and $k[[t]] = \lim_n k[t]/t^n$.

⁶This means that, for all $\varepsilon > 0$, there exists an integer N such that $|a_n - a_m| < \varepsilon$ for all $m, n \geq N$.

2.3. Local fields. We have now all the ingredients for the main definition:

Definition 2.5. A *local field* is a complete discrete valuation field with finite residue field.

 This is not the definition from Week 1 (locally compact field for a non-trivial absolute value), which also allows \mathbb{R} and \mathbb{C} to be local fields. Since their class field theory is kind of trivial, we will not lose anything in adopting this more restrictive definition. Many parts of the theory also work under the assumption that the residue field is perfect.

Example 2.6. \mathbb{Q}_p and $\mathbb{F}_q((t))$ are examples of local fields. By Theorem 3.1 below, any finite extension K/\mathbb{Q}_p is a local field as well (these are called *p-adic fields*). We will see that these are actually all local fields.

3. EXTENSIONS

Throughout, K denotes a complete discrete valued field, v the valuation, A the ring of integers and κ the residue field. If L/K is a finite extension, we let B denote the integral closure of A in L , that is, the set of elements of L which are integral⁷ over A .

Theorem 3.1. Let L/K be a finite extension of degree n .

- (a) B is a discrete valuation ring. It is a free A -module of rank n .
- (b) Let \mathfrak{p}_B be the unique non-zero prime ideal of B . Write $\mathfrak{p}_A B = \mathfrak{p}_B^e$ for some $e \geq 1$ and let f be the degree of the extension B/\mathfrak{p}_B of κ . Then $ef = n$.
- (c) The field L is complete for the topology induced by B . There is a unique discrete valuation w of L which induces on K the same topology as v . Explicitly,

$$w(x) = \frac{1}{f}v(N_{L/K}(x)),$$

where $N_{L/K}$ is the norm of the extension (defined, for each $x \in L$, as the determinant of the K -linear map $L \rightarrow L$ “multiplication by x ”).

This will be proved next time.

Definition 3.2. The integer e is called the *ramification index* and f is called the *inertia degree*. An extension L/K is said to be

- *unramified* if $e = 1$ and B/\mathfrak{p}_B is a separable field extension of κ ,
- *totally ramified* if $f = 1$,
- *tamely ramified* if the characteristic of κ does not divide e .

One sees in particular that unramified extensions are tamely ramified. Many examples will be given in the exercise sessions.

Remark 3.3. If $x \in K^\times$, then $w(x) = \frac{1}{f}v(x^n) = \frac{n}{f}v(x) = ev(x)$, so the valuation w only extends v if L/K is unramified. This is why the theorem says “induces the same topology” rather than “extends the valuation”. In general, we cannot have an extension of v with integral values.

⁷Recall that $x \in L$ is integral over A if it satisfies an equation of the form $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ with $a_i \in A$.

3.1. Unramified extensions. The composite of two unramified extensions is again unramified, hence the following definition makes sense:

Definition 3.4. The union K^{ur} of all unramified extensions of K inside a fixed separable closure K^s of K is called the *maximal unramified extension* of K .

Theorem 3.5. Let K be a complete discrete valued field with ring of integers A and residue field κ . For each finite separable extension l/κ , there exists a unique extension L/K whose associated residue field extension is l/κ . Moreover, $[L:K] = [l:\kappa]$ and L/K is Galois if and only if l/κ is Galois. If this is the case, $\text{Gal}(L/K) \simeq \text{Gal}(l/\kappa)$.

Corollary 3.6. The maximal unramified extension K^{ur} is a Galois extension of K with Galois group $\text{Gal}(K^{\text{ur}}/K) \simeq \text{Gal}(\kappa^s/\kappa)$.

Remark 3.7. The field K^{ur} has a valuation extending v , but it may not be complete. The example of the field of Laurent series will be discussed in the exercises.

Example 3.8. Let K be a local field. Then κ is finite, so for each $n \geq 0$, there is a unique degree n extension of κ . Correspondingly, the theorem affirms that K has a unique unramified extension of degree n . Therefore,

$$\text{Gal}(K^{\text{ur}}/K) \simeq \text{Gal}(\bar{\kappa}/\kappa) \simeq \widehat{\mathbb{Z}}.$$

The image of $x \mapsto x^q$ is called the Frobenius of K^{ur} . Now, observe that all unramified extensions of K are abelian, since $\text{Gal}(L/K) \simeq \text{Gal}(l/\kappa) = \mathbb{Z}/n$. It follows that $K^{\text{ur}} \subseteq K^{\text{ab}}$. By restriction one gets the map $\text{Gal}(K^{\text{ab}}/K) \rightarrow \text{Gal}(\bar{\kappa}/\kappa)$ in the diagram of the main theorem of local class field theory.

REFERENCES

ETH ZÜRICH, D-MATH, RÄMISTRASSE 101, CH-8092 ZÜRICH, SWITZERLAND

E-mail address: javier.fresan@math.ethz.ch