A BRIEF INTRODUCTION TO LOCAL FIELDS

TOM WESTON

The purpose of these notes is to give a survey of the basic Galois theory of local fields and number fields. We cover much of the same material as [2, Chapters 1 and 2], but hopefully somewhat more concretely. We omit almost all proofs, except for those having directly to do with Galois theory; for everything else, see [2].

1. The decomposition and inertia groups

Let L/K be an extension of number fields of degree n. We assume that L/K is Galois. Let $\mathfrak{p}$ be a fixed prime of $\mathcal{O}_K$ and let its ideal factorization in $\mathcal{O}_L$ be

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Recall that the Galois group $\mathrm{Gal}(L/K)$ acts on the set $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$, and this action is transitive. It follows that our factorization can actually be written as

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$$

and each $\mathfrak{P}_i$ has the same inertial degree f; we have $ref = n$.

When one has a group acting on a set, one often considers the subgroups stabilizing elements of the set; we will write these as

$$D(\mathfrak{P}_i/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\} \subseteq \mathrm{Gal}(L/K)$$

and call it the *decomposition group* of $\mathfrak{P}_i$. (Note that we are not asking that such σ fix $\mathfrak{P}_i$ pointwise; we are just asking that they send every element of $\mathfrak{P}_i$ to another element of $\mathfrak{P}_i$.)

It is easy to see how the decomposition groups of different $\mathfrak{P}_i$ are related: let $\mathfrak{P}_i$ and $\mathfrak{P}_j$ be two primes above $\mathfrak{p}$ and let $\sigma \in \mathrm{Gal}(L/K)$ be such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Then one checks immediately that

$$D(\mathfrak{P}_j/\mathfrak{p}) = \sigma D(\mathfrak{P}_i/\mathfrak{p})\sigma^{-1}.$$

That is, the decomposition groups are all conjugates of each other. Note also that since $\mathrm{Gal}(L/K)$ acts transitively and $D(\mathfrak{P}_i/\mathfrak{p})$ is the stabilizer of an element, we have

$$\#D(\mathfrak{P}_i/\mathfrak{p}) = \frac{n}{r} = ef.$$

Example 1. Let us fix now an example which we will use throughout the paper; it is an abelian extension, so it does not have quite all of the structure of the general case, but it should still illustrate our results. Consider the extension $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$, which is a Galois extension of degree 8. We will just write ζ for ζ_{15} from now on. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ can be identified with $(\mathbb{Z}/15\mathbb{Z})^*$, where $i \in (\mathbb{Z}/15\mathbb{Z})^*$ corresponds to the automorphism σ_i of $\mathbb{Q}(\zeta)$ characterized by $\sigma_i(\zeta) = \zeta^i$.

Let us also fix some specific primes to consider. Set

$$\begin{aligned}\mathfrak{p}_2 &= \big(2, \zeta^4 + \zeta + 1\big);\\ \mathfrak{p}_3 &= \big(3, \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1\big);\\ \mathfrak{p}_5 &= \big(5, \zeta^2 + \zeta + 1\big);\\ \mathfrak{p}_{31} &= \big(15, \zeta + 3\big).\end{aligned}$$

Each $\mathfrak{p}_p$ is a prime lying over p. We have the following values of r, e and f:

	r	e	f
$\mathfrak{p}_2$	2	1	4
$\mathfrak{p}_3$	1	2	4
$\mathfrak{p}_5$	1	4	2
$\mathfrak{p}_{31}$	8	1	1

Let us compute the decomposition groups of these primes. Three of these are quite easy: $D(\mathfrak{p}_3/3) = D(\mathfrak{p}_5/5) = \mathrm{Gal}(L/K)$ since in these cases there are no other primes above 3 and 5. Also, we have $D(\mathfrak{p}_{31}/31) = \{1\}$, since we know that it has order $ef = 1$.

This leaves the case of $D(\mathfrak{p}_2/2)$. We know that this group has order $ef = 4$. To compute the group explicitly, we use the fact that $\mathfrak{p}_2$ is the kernel of the map

$$\mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/\mathfrak{p}_2 \cong \mathbb{F}_2[x]/(x^4 + x + 1)$$

sending ζ to x. Since

$$\sigma_i\big(2, \zeta^4 + \zeta + 1\big) = \big(2, \sigma_i(\zeta^4 + \zeta + 1)\big) = \big(2, \zeta^{4i} + \zeta^i + 1\big)$$

we see that σ will lie in $D(\mathfrak{p}_2/2)$ if and only if $\zeta^{4i} + \zeta^i + 1$ is in the kernel of the above map. This in turn will occur if and only if $x^4 + x + 1$ divides $x^{4i} + x^i + 1$ in $\mathbb{F}_2[x]$. From here one can easily check the possibilities, and it turns out that

$$D(\mathfrak{p}_2/2) = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8\}.$$

The most interesting thing about the decomposition group is its relationship to the Galois theory of the residue field. Specifically, fix one of the $\mathfrak{P} = \mathfrak{P}_i$ lying over $\mathfrak{p}$. Let σ be an element of $D(\mathfrak{P}/\mathfrak{p})$. Since $\sigma(\mathfrak{P}) = \mathfrak{P}$, it induces an automorphism of the residue field $\mathcal{O}_L/\mathfrak{P}$. This automorphism certainly fixes $\mathcal{O}_K/\mathfrak{p}$, so we have obtained a map

$$D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$$

which is easily checked to be a homomorphism. In fact, it is also surjective; we will prove this fact later in our discussion of local fields.

Let us define the *inertia group* of $\mathfrak{P}$ by

$$I(\mathfrak{P}/\mathfrak{p}) = \ker\big(D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})\big)$$

thus $I(\mathfrak{P}/\mathfrak{p})$ is a normal subgroup of $D(\mathfrak{P}/\mathfrak{p})$ and there is an isomorphism (using the surjectivity mentioned above)

$$D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}).$$

Somewhat more explicitly, we see from the definition that

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}/\mathfrak{p}) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \text{ for all } \alpha \in \mathcal{O}_L\}.$$

Note also that as with decomposition groups, if $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are two primes lying over $\mathfrak{p}$ with $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$, then

$$I(\mathfrak{P}_j/\mathfrak{p}) = \sigma I(\mathfrak{P}_i/\mathfrak{p})\sigma^{-1}.$$

The inertia group is related to our usual notion of inertia in the following simple way. Recall that $D(\mathfrak{P}/\mathfrak{p})$ has order $n/r = ef$. We also know that $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p})$ has order f, by definition. It follows that $I(\mathfrak{P}/\mathfrak{p})$ has order e. In particular, $I(\mathfrak{P}/\mathfrak{p})$ is trivial if and only if $\mathfrak{P}/\mathfrak{p}$ is unramified in L/K.

Example 2. The proposition shows that the inertia groups of $\mathfrak{p}_2$ and $\mathfrak{p}_{31}$ are both trivial. The group $I(\mathfrak{p}_3/3)$ has order 2; to compute it we note that σ_i will induce the identity on the residue field

$$\mathbb{Z}[\zeta]/\mathfrak{p}_3 \cong \mathbb{F}_3[x]/(x^4 + x^3 + x^2 + x + 1)$$

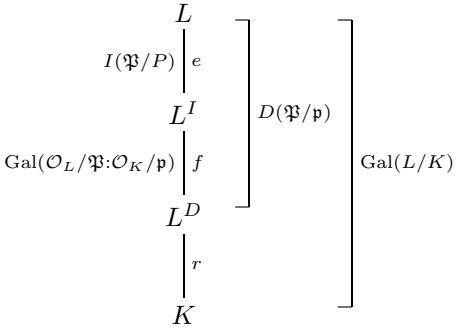
if and only if $\sigma_i(\zeta) \cong \zeta \pmod{\mathfrak{p}_3}$. Under the above isomorphism, this is the same as $\sigma_i(x) = x^i$ being congruent to x modulo $x^4 + x^3 + x^2 + x + 1$. This occurs if and only if $x^4 + x^3 + x^2 + x + 1$ divides $x^i - x$, which is an easy condition to check. One finds that

$$I(\mathfrak{p}_3/3) = \{\sigma_1, \sigma_{11}\}.$$

The computation for $I(\mathfrak{p}_5/5)$ is similar; one finds this time that

$$I(\mathfrak{p}_5/5) = \{\sigma_1, \sigma_4, \sigma_7, \sigma_{13}\}.$$

To give a slightly more intuitive explanation of these groups, let us now suppose for simplicity that $\mathrm{Gal}(L/K)$ is abelian. Define the *inertia field* L^I of $\mathfrak{P}/\mathfrak{p}$ to be the fixed field of $I(\mathfrak{P}/\mathfrak{p})$ and the *decomposition field* L^D of $\mathfrak{P}/\mathfrak{p}$ to be the fixed field of $D(\mathfrak{P}/\mathfrak{p})$. We have a diagram



One can show (see [1, Chapter 4]) that in the extension L^D/K, $\mathfrak{p}$ splits completely into

$$\mathfrak{p}\mathcal{O}_{L^D} = \mathfrak{P}_1^D \cdots \mathfrak{P}_r^D,$$

where each $\mathfrak{P}_i^D$ has inertial degree 1. Next, in L^I/L^D, each $\mathfrak{P}_i^D$ remains inert; that is, $\mathfrak{P}_i^I = \mathfrak{P}_i^D\mathcal{O}_{L^D}$ is still prime, and it has inertial degree f. Lastly, each prime $\mathfrak{P}_i^I$ is totally ramified in L/L^I, so that $\mathfrak{P}_i^I\mathcal{O}_L = \mathfrak{P}_i^e$. Thus the decomposition and inertia groups somehow separate out the different sorts of behavior of primes in the extension L/K.

2. Local fields

We would like to obtain a Galois theoretic interpretation of the entire decomposition group $D(\mathfrak{P}/\mathfrak{p})$, rather than just its quotient $D(\mathfrak{P}/\mathfrak{p})/I(\mathfrak{P}/\mathfrak{p})$. To do this we will introduce the notion of a local field, which is of fundamental importance in algebraic number theory. Our construction will be extremely brief; for the details, see [3] and the bibliography there.

Before explaining how to associate local fields to number fields, we will give the abstract definition of local fields. Fix a rational prime p. We begin with the ring $\mathbb{Z}_p$ of p-adic integers. One can define $\mathbb{Z}_p$ topologically as the completion of $\mathbb{Z}$ with respect to the p-adic metric; we give an algebraic definition instead:

$$\mathbb{Z}_p = \varprojlim_{n\to\infty} \mathbb{Z}/p^n\mathbb{Z}.$$

Recall that an element a of such an inverse limit can be represented as an infinite sequence

$$a = (a_1, a_2, \ldots)$$

with $a_i \in \mathbb{Z}$ and $a_i \equiv a_{i+1} \pmod{p^i}$ for all i. We have a natural injection of $\mathbb{Z}$ into $\mathbb{Z}_p$ given by sending $a \in \mathbb{Z}$ to the sequence

$$(a, a, a, \ldots).$$

However, $\mathbb{Z}_p$ contains many other elements. Intuitively, elements of $\mathbb{Z}_p$ are supposed to have information "modulo arbitrarily high powers of p."

There is another description of $\mathbb{Z}_p$ which is somewhat more concrete. Let $a = (a_1, a_2, \ldots)$ be an element of $\mathbb{Z}_p$ and note that there is some unique $b_0 \in \{0, 1, \ldots, p-1\}$ such that $a_1 \equiv b_0 \pmod{p}$; in fact, this implies that $a_i \equiv b_0 \pmod{p}$ for all i. Thus

$$a - b_0 = (a_1 - b_0, a_2 - b_0, \ldots)$$

(where we regard the b_0 on the left as an element of the image of $\mathbb{Z}$ in $\mathbb{Z}_p$) is divisible by p; that is, we can write

$$a - b_0 = p(a_1', a_2', \ldots)$$

for some $a_i' \in \mathbb{Z}$. Repeating this process for $a' = (a_1', a_2', \ldots)$ yields a $b_1 \in \{0, 1, \ldots, p-1\}$ such that $a' - b_1$ is divisible by p, and thus such that

$$a - b_0 - pb_1$$

is divisible by p^2. Continuing in this way, we can write

$$a = \sum_{i=0}^{\infty} b_i p^i$$

with each $b_i \in \{0, 1, \ldots, p-1\}$. That is, a can be written as a sort of "power series" in p with coefficients in $\{0, 1, \ldots, p-1\}$. Note that this fits with our description of $\mathbb{Z}_p$ as containing information modulo arbitrarily high powers of p: cutting off the power series expression after the p^{i-1} term yields the image a_i of the element in $\mathbb{Z}/p^i\mathbb{Z}$.

The ring $\mathbb{Z}_p$, although somewhat confusing, is very convenient algebraically. It is what is called a *discrete valuation ring*; that is, it is a Dedekind domain with only one non-zero prime ideal. In this case, that non-zero prime ideal is simply generated by p. Unique factorization of ideals now implies that every ideal of $\mathbb{Z}_p$

is generated by p^n for some n. Note that the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is just the finite field $\mathbb{F}_p$.

We define $\mathbb{Q}_p$ to be the field of fractions of $\mathbb{Z}_p$. In fact, we can obtain $\mathbb{Q}_p$ from $\mathbb{Z}_p$ just by inverting the single element p; that is, $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. It follows that any element of $\mathbb{Q}_p$ can be written as

$$\sum_{i>>0}^{\infty} b_i p^i$$

where $b_i \in \{0, 1, \ldots, p-1\}$ and the sum has only finitely many negative terms. Note that $\mathbb{Q}_p$ has characteristic 0.

A *local field* (for this fixed p) is simply a finite extension of $\mathbb{Q}_p$; as always, such extensions can be obtained simply by adjoining roots of polynomials in $\mathbb{Q}_p[x]$. Given such a field K, we define its ring of integers $\mathcal{O}_K$ to be the integral closure of $\mathbb{Z}_p$ in K. It can be shown to also be a discrete valuation ring. (The proof that $\mathcal{O}_K$ is a Dedekind domain is basically the same as the proof for rings of integers of number fields; that it has only one non-zero prime ideals follows from results on topological vector spaces.) If $\mathfrak{p}$ is its unique non-zero prime ideal, we must have $\mathfrak{p} \cap \mathbb{Z}_p = p\mathbb{Z}_p$; in particular, $\mathfrak{p}$ contains p. It follows that the *residue field* $\mathcal{O}_K/\mathfrak{p}$ of $\mathcal{O}_K$ is a finite field of characteristic p.

3. Galois theory of finite fields

Before we begin to investigate the Galois theory of local fields, it will be useful to recall the basic Galois theory of finite fields. Let ℓ/k be an extension of finite fields of characteristic p and let q be the cardinality of k; it is a power of p. This extension if automatically Galois; let n be the degree. Then $\mathrm{Gal}(\ell/k)$ is cyclic of order n, with a canonical generator φ given by

$$\varphi(\alpha) = \alpha^q$$

for all $\alpha \in \ell$. (The easiest way to see this is to note that ℓ can be characterized as the solutions of $x^{q^n} - x$, which shows that φ^n will be the first power of φ which is trivial; since the Galois group has order n, this implies that φ is a generator.) φ is called the *Frobenius automorphism*. Note in particular that if $\alpha \in \ell$, then its conjugates are all just powers of α.

4. Galois theory of local fields

Let L/K be a finite Galois extension of local fields; we mean by this (among other things) that L and K are both extensions of the same $\mathbb{Q}_p$. As is always the case, these extensions are just the splitting fields of polynomials in $K[x]$. We should note, however, that our intuition from $\mathbb{Q}$ is often incorrect in this setting and local fields often contain elements which we would not have expected; for example, we will see later that $\mathbb{Q}_{31}(\zeta_{15}) = \mathbb{Q}_{31}$.

Let $\mathcal{O}_L$ and $\mathcal{O}_K$ be the rings of integers of L and K respectively, and let $\mathfrak{P}$ and $\mathfrak{p}$ be the unique non-zero primes of these rings. For any $\sigma \in \mathrm{Gal}(L/K)$, we must have $\sigma(\mathfrak{P}) = \mathfrak{P}$, since σ must send $\mathfrak{P}$ to some other prime ideal, and there aren't any others. Thus σ induces an automorphism of the residue field $\ell = \mathcal{O}_L/\mathfrak{P}$ which clearly fixes $k = \mathcal{O}_K/\mathfrak{p}$; we now get a homomorphism

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(\ell/k).$$

We claim that this homomorphism is surjective. To see this, choose a primitive element a for ℓ/k. Since a is a primitive element, its characteristic polynomial equals its minimal polynomial. It follows that it is just given by

$$f(x) = \prod_{s \in \mathrm{Gal}(\ell/k)} \big(x - s(a)\big) \in k[x].$$

Now, choose any $\alpha \in \mathcal{O}_L$ which maps to a under the map $\mathcal{O}_L \twoheadrightarrow \ell$. Let $S \subseteq \mathrm{Gal}(L/K)$ be some subset of the Galois group such that each conjugate of α appears exactly once among the $\sigma(\alpha)$ for $\sigma \in S$. Then the minimal polynomial for α in $K[x]$ (in fact, in $\mathcal{O}_K[x]$) is just

$$g(x) = \prod_{\sigma \in S} \big(x - \sigma(\alpha)\big).$$

Now, consider the image $\bar{g}(x)$ of $g(x)$ in $k[x]$. Since α is a root of $g(x)$, a is a root of $\bar{g}(x)$; thus $f(x)$, being the minimal polynomial of a, divides $\bar{g}(x)$ in $k[x]$. In particular, for each $s \in \mathrm{Gal}(\ell/k)$, $s(a)$ is a root of $\bar{g}(x)$. In other words, for each such s there exists $\sigma \in \mathrm{Gal}(L/K)$ such that

$$\sigma(\alpha) \equiv s(a) \pmod{\mathfrak{P}}.$$

But since a is a primitive element for ℓ/k, $s : \ell \to \ell$ is determined entirely by $s(a)$. In particular, we see that σ induces s on ℓ, so s is the image of σ under our map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\ell/k)$. Since this is true for every such s, this shows that this map is surjective.

We now define the inertia subgroup $I(L/K)$ of $\mathrm{Gal}(L/K)$ to be the kernel of this map. Thus $I(L/K)$ is a normal subgroup of $\mathrm{Gal}(L/K)$ which we can also write as

$$I(L/K) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\alpha) \equiv \alpha \text{ for all } \alpha \in \mathcal{O}_L\}.$$

We also have a canonical isomorphism

$$\mathrm{Gal}(\ell/k) \cong \mathrm{Gal}(L/K)/I(L/K).$$

We will say that L/K is *unramified* if $I(L/K) = \{1\}$; this occurs if and only if

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k).$$

Note that in this situation $\mathrm{Gal}(L/K)$ is cyclic of degree $n = [L : K]$ (since $\mathrm{Gal}(\ell/k)$ is) and we obtain a canonical generator φ which corresponds to the Frobenius automorphism of ℓ/k. By abuse of language we will also call this the Frobenius automorphism of L/K; it is characterized by

$$\varphi(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}}$$

for all $\alpha \in \mathcal{O}_L$.

It is a fundamental fact that for every extension ℓ of k, there is a unique *unramified* extension L of K with residue field ℓ. Since for each positive integer n, k has a unique extension of degree n, this also implies that for each positive integer n, K has a unique unramified extension of degree n.

The structure of ramified extensions is considerably more complicated. We can, however, at least use some of our knowledge of the unramified case. Define K^{ur} to be the fixed field of $I(L/K)$ in L. By Galois theory we have

$$\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \mathrm{Gal}(L/K)/I(L/K) \cong \mathrm{Gal}(\ell/k).$$

In fact, one sees easily that K^{ur}/K is unramified and that K^{ur} has residue field ℓ; thus K^{ur} is the unique unramified extension of K with residue field ℓ. The extension

L/K^{ur} has Galois group $I(L/K)$ and is *totally ramified*; it is much more complicated in general (although with more effort one can still obtain a lot of information in the case that p does not divide $\#I(L/K)$.)

5. Construction of local fields

We have yet to give any real examples of local fields. Their fundamental importance comes from the fact that they arise naturally from number fields.

Let K be a number field and let $\mathfrak{p}$ a prime of $\mathcal{O}_K$. We will define the completion of $\mathcal{O}_K$ at $\mathfrak{p}$ analogously to the way we defined $\mathbb{Z}_p$ and $\mathbb{Q}_p$. We define

$$\mathcal{O}_{K,\mathfrak{p}} = \varprojlim_{n\to\infty} \mathcal{O}_K/\mathfrak{p}^n;$$

thus elements of $\mathcal{O}_{K,\mathfrak{p}}$ can be represented as infinite sequences

$$(a_1, a_2, \ldots)$$

with each a_i in $\mathcal{O}_K$ and $a_i \equiv a_{i+1} \pmod{\mathfrak{p}^i}$. We obtain a natural injection $\mathcal{O}_K \hookrightarrow \mathcal{O}_{K,\mathfrak{p}}$ by sending $a \in \mathcal{O}_K$ to $(a, a, a, \ldots) \in \mathcal{O}_{K,\mathfrak{p}}$.

$\mathcal{O}_{K,\mathfrak{p}}$ turns out to be a discrete valuation ring, and its unique non-zero prime ideal is simply the extended ideal $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$. One also shows that the injection $\mathcal{O}_K \hookrightarrow \mathcal{O}_{K,\mathfrak{p}}$ induces an isomorphism

$$\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$$

of residue fields. It is a basic fact that any discrete valuation ring is a principal ideal domain; in fact, any element $\pi \in \mathfrak{p} - \mathfrak{p}^2$ will be a generator of $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$, and unique factorization of ideals now shows that every ideal has the form (π^n) for some n. A generator of $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ is called a *uniformizer*.

We can describe $\mathcal{O}_{K,\mathfrak{p}}$ in an analogous way to our power series description of $\mathbb{Z}_p$. Specifically, let $c_1, \ldots, c_k$ be any elements of $\mathcal{O}_K$ such that each element of $\mathcal{O}_K/\mathfrak{p}$ is the image of exactly one c_i. Proceeding as with $\mathbb{Z}_p$, we find that we can write any $a = (a_1, a_2, \ldots) \in \mathcal{O}_{K,\mathfrak{p}}$ as

$$a = \sum_{i=0}^{\infty} b_i \pi^i$$

where each b_i is equal to one of the c_j and π is any (fixed) uniformizer.

We define the field $K_{\mathfrak{p}}$ to be the field of fractions of $\mathcal{O}_{K,\mathfrak{p}}$; it can be obtained simply by inverting a uniformizer π. Note that it contains K since $\mathcal{O}_{K,\mathfrak{p}}$ contains $\mathcal{O}_K$.

6. Connections with Galois theory of number fields

Now let L/K be a Galois extension of number fields and let $\mathfrak{P}$ and $\mathfrak{p}$ be primes as in the first section. We claim that there is a natural injection

$$\mathcal{O}_{K,\mathfrak{p}} \hookrightarrow \mathcal{O}_{L,\mathfrak{P}}.$$

The proof of this is a tiny bit messy. Basically, one lets $\mathfrak{P}^e$ be the exact power of $\mathfrak{P}$ dividing $\mathfrak{p}\mathcal{O}_L$, and one shows that for any i we have $\mathfrak{P}^{ie} \cap \mathcal{O}_K = \mathfrak{p}^i$. We therefore obtain natural maps

$$\mathcal{O}_K/\mathfrak{p}^i \hookrightarrow \mathcal{O}_L/\mathfrak{P}^{ie};$$

from here one uses general properties of inverse limits to conclude that there is indeed an injection $\mathcal{O}_{K,\mathfrak{p}} \hookrightarrow \mathcal{O}_{L,\mathfrak{P}}$.

From this injection we see also that $K_\mathfrak{p} \hookrightarrow L_\mathfrak{P}$; thus $L_\mathfrak{P}$ is an extension of $K_\mathfrak{p}$. In fact, one can show that $L_\mathfrak{P}/K_\mathfrak{p}$ is a Galois extension; we will return a bit later to this issue, but for now let us just assume it. It is also not difficult to show that if $L = K(\alpha)$ with α a root of $f(x) \in K[x]$, then $L_\mathfrak{P} = K_\mathfrak{p}(\alpha')$, where α' is some root of $f(x)$ in $L_\mathfrak{P}$; however, $f(x)$ need not still be irreducible in $K_\mathfrak{p}[x]$.

Note that we can apply these results in particular in the case $K = \mathbb{Q}$ and $\mathfrak{p} = (p)$; we conclude that each $L_\mathfrak{P}$ and $K_\mathfrak{p}$ is an extension of $\mathbb{Q}_p$, where $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$. In particular, we are now in the situation studied previously. (Although to be completely honest we should acknowledge that we have not yet showed that $L_\mathfrak{P}/K_\mathfrak{p}$ is a finite extension; we will do this in a moment.)

Let us determine the Galois group $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. Given any $\sigma \in \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$, we can restrict σ to L to obtain an automorphism of L which fixes K, since $K \subseteq K_\mathfrak{p}$. That is, we obtain a map

$$\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$$

which is easily seen to be a homomorphism. Furthermore, since we must have $\sigma(\mathfrak{P}\mathcal{O}_{L,\mathfrak{P}}) = \mathfrak{P}\mathcal{O}_{L,\mathfrak{P}}$, as it is the only prime of $L_\mathfrak{P}$, we see that the image of this map must lie in the decomposition group $D(\mathfrak{P}/\mathfrak{p})$.

On the other hand, given $\sigma \in \mathrm{Gal}(L/K)$ lying in $D(\mathfrak{P}/\mathfrak{p})$, note that $\sigma(\mathfrak{P}^i) = \mathfrak{P}^i$ for all i. Thus σ yields automorphisms of each residue ring $\mathcal{O}_L/\mathfrak{P}^i$, and therefore an automorphism of $\mathcal{O}_{L,\mathfrak{P}}$, given by

$$\sigma\big((a_1, a_2, \ldots)\big) = \big(\sigma(a_1), \sigma(a_2), \ldots\big)$$

for $(a_1, a_2, \ldots) \in \mathcal{O}_{L,\mathfrak{P}}$. Thus we have another homomorphism

$$D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}).$$

It is clear from the definitions that the composition

$$D(\mathfrak{P}/\mathfrak{p}) \to \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$$

is just the natural injection of $D(\mathfrak{P}/\mathfrak{p})$ into $\mathrm{Gal}(L/K)$. It follows from all of this that the map

$$\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$$

is an injection, with image $D(\mathfrak{P}/\mathfrak{p})$. In particular,

$$\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \cong D(\mathfrak{P}/\mathfrak{p}),$$

so we have obtained our desired Galois theoretic interpretation of $D(\mathfrak{P}/\mathfrak{p})$.

Note that this also shows that $L_\mathfrak{P}/K_\mathfrak{p}$ is a finite extension. In fact, the easiest way to show that it is Galois is to show independently that it has degree ef and then to use the above isomorphism.

The usefulness of these results is that they allow us to examine the Galois group "one prime at a time", and the Galois theory of local fields is much easier than that of number fields. As an important example, let us suppose that $\mathfrak{p}$ is unramified. Then $I(\mathfrak{P}/\mathfrak{p})$ is trivial, so we have an injection

$$\mathrm{Gal}(\ell/k) \cong \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \cong D(\mathfrak{P}/\mathfrak{p}) \hookrightarrow \mathrm{Gal}(L/K),$$

where ℓ and k are the appropriate residue fields. In particular, we can interpret the canonical Frobenius generator $\varphi_\mathfrak{P}$ of $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ as an element of $\mathrm{Gal}(L/K)$; it is characterized by

$$\varphi_\mathfrak{P}(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}}$$

for all α in $\mathcal{O}_L$. Such elements turn out to be extremely important in the study of number fields, especially in the case that $\mathrm{Gal}(L/K)$ is abelian.

7. Examples

Let us return to our $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$ situation in order to give some "concrete" examples of local fields. Let us begin with the prime $\mathfrak{p}_2$. We have $e = 1$ and $f = 4$, so the local field extension $\mathbb{Q}(\zeta)_{\mathfrak{p}_2}/\mathbb{Q}_2$ is an unramified Galois extension of degree 4. Since $\mathbb{Q}(\zeta)_{\mathfrak{p}_2}$ is just $\mathbb{Q}_2(\zeta)$, we see that the unique unramified extension of $\mathbb{Q}_2$ of degree 4 is just $\mathbb{Q}_2(\zeta_{15})$. However, there are many quite different looking ways to write this field. For example, a similar argument shows that $\mathbb{Q}_2(\zeta_5)$ is also an unramified extension of $\mathbb{Q}_2$ of degree 4, and thus equals $\mathbb{Q}_2(\zeta_{15})$. In particular, we seem to have picked up a third root of unity "for free".

Next consider $\mathfrak{p}_3$, which has $e = 2$ and $f = 4$. Here we find that the local field $\mathbb{Q}(\zeta)_{\mathfrak{p}_3} = \mathbb{Q}_3(\zeta)$ is a Galois extension of $\mathbb{Q}_3$ of degree 8, with an inertia group of order 2. There is a not whole lot else we can say about it at the moment. Similarly, $\mathbb{Q}_5(\zeta)$ is a Galois extension of $\mathbb{Q}_5$ of degree 8, with inertia group of order 4.

Lastly, we consider $\mathfrak{p}_{31}$. Here we find that $\mathbb{Q}_{31}(\zeta)$ has degree 1 over $\mathbb{Q}_{31}$; that is, $\zeta_{15} \in \mathbb{Q}_{31}$. More generally, one can use the fact that a prime p splits completely in $\mathbb{Q}(\zeta_m)$ if and only if $p \equiv 1 \pmod{m}$ to show that $\mathbb{Q}_p$ contains the $(p-1)^{\text{st}}$ roots of unity. In general, the cyclotomic polynomial $\Phi_m(x)$ need not be irreducible over $\mathbb{Q}_p$; in fact, one can determine how it factors based on how p factors in $\mathbb{Q}(\zeta_m)$.

As a final example, let us consider extensions $\mathbb{Q}_p(\sqrt{2})$. We know from our general theory that this extension will be trivial if and only if p splits completely in $\mathbb{Q}(\sqrt{2})$; this in turn happens if and only if $x^2 - 2$ has distinct roots modulo p. In other words, $\sqrt{2} \in \mathbb{Q}_p$ if and only if $\sqrt{2} \in \mathbb{F}_p$, at least for $p \neq 2$. This is a first instance of Hensel's lemma, which says (roughly) that a polynomial has roots in $\mathbb{Q}_p$ if and only if it has roots in $\mathbb{F}_p$.

References

[1] Daniel Marcus, *Number Fields*. Springer-Verlag, New York, 1977.
[2] Jean-Pierre Serre, *Local Fields*. Springer-Verlag, New York, 1979.
[3] Tom Weston, *The idelic approach to number theory*.