Faculty of Mathematics and Mechanics
of Yerevan State University

Hakobyan Tigran

Symplectic space of formal modules

Speciality 01.01.06—"Algebra and number theory"

D I S S E R T A T I O N

For the degree of candidate
of physical and mathematical sciences

Scientific adviser:
doctor of phys.-math. sciences, professor
V. S. Atabekyan

Yerevan - 2018

Contents

Introduction

Let L/K be a finite Galois extension of fields with Galois group G. Then L can be regarded as a module over the group ring $K[G]$, where K acts by multiplication and G acts in a natural way. The normal basis theorem (See [1, Chapter 6, §13]) implies that this module is in fact cyclic, namely there is an isomorphism $L \cong K[G]$ of $K[G]$-modules. Similarly one may consider the $\mathbb{Z}[G]$-module L^*, but this time its structure is rather complicated and is not well studied even if the fields L and K are "good" enough.

Now suppose that K and L are finite extensions of $\mathbb{Q}_p$. Then the ring of integers $\mathcal{O}_L$ as well as all the fractional ideals $\mathfrak{p}_L^n, n \in \mathbb{Z}$ of the field L are $\mathcal{O}_K[G]$-modules and one might ask a question concerning their structure . In connection with this *S.V.Vostokov* proved in [2] that if L/K is an abelian p-extension with Galois group G and K does not contain a primitive p-th root of unity, then in the field L there exist ideals which are decomposable as $\mathcal{O}_K[G]$-modules if and only if the ramification index $e(L/K)$ divides the different $\mathfrak{D}_{L/K}$. In this respect see also [3].

The multiplicative case was studied in a series of articles [4–8]. We now want to focus on the result of *D.K.Faddeed*, published in [6]. He considered the case of cyclic p-extension L/K with Galois group $G = \langle\sigma\rangle$, such that K contains a primitive p-th root of unity ζ_p. It was proved that there is an isomorphism of $R = \mathbb{F}_p[G]$-modules

$$L^*/L^{*p} \cong \begin{cases} R^n \oplus R/(\sigma-1)^2, & \zeta_p \in N_{L/K}(L^*) \\ R^n \oplus R/(\sigma-1) \oplus R/(\sigma-1), & \text{otherwise} \end{cases}$$

Moreover, the author provided a canonical method for selecting the generating elements in a way that they satisfy certain requirements concerning Hasse's norm residue symbol.

In a similar way one may consider E/E^p as an R-module, where $E = 1 + \mathfrak{p}_L$ is the group of principal units in L. In the article [9] we considered this module in the case of a cyclic extension L/K of degree p. It turned out that its structure depends on several factors, including the ramification of the extension L/K. The proof of this result is provided in the first paragraph of the second chapter of the thesis. On the other hand it can be proved that E is a $\mathbb{Z}_p$-module, namely one can compute the expression u^α for any $u \in E$ and $\alpha \in \mathbb{Z}_p$. The structure of this module is completely studied in [10, Chapter 15]. In our case, when L is a finite extension of $\mathbb{Q}_p$, E decomposes into a direct sum

of a finite cyclic p-group and a free $\mathbb{Z}_p$-module of rank $[L:\mathbb{Q}_p]$. In contrast to this, if L is a local field of positive characteristic, then infinitely many generators are required and infinite products arise. Further, *Z.I.Borevich* studied E as a $\mathbb{Z}_p[G]$-module in the case of cyclic p-extensions L/K. Let $E_0 = 1 + \mathfrak{p}_K$ be the group of principal units in K, $\Gamma = N_{L/K}(E)$, $G = \langle\sigma\rangle$ and let $\zeta = \zeta_{p^s}, s \geq 1$ be a root of unity in E. In [7] the author proved that if the map $E_0/E_0^p \to E/E^p$, induced by the inclusion $E_0 \hookrightarrow E$ is injective and if $E_0 = \langle\zeta, \Gamma\rangle$, then the $\mathbb{Z}_p[G]$-module E decomposes into a direct sum of a finite cyclic p-group $\langle\zeta\rangle$ and a free $\mathbb{Z}_p[G]$-module of rank $[K:\mathbb{Q}_p]$.

We say that the field K is irregular, if it contains a primitive p-th root of unity. The irregularity degree of K is defined to be the maximal positive integer s for which K contains a primitive p^s-th root of unity. In this respect the following theorem concerning unramified extensions was proved in [7].

Theorem (Borevich, 1965) *If the extension L/K is unramified and the fields L and K have the same irregularity degree $s \geq 1$, then for the $\mathbb{Z}_p[G]$-module E there exist a system of generating elements $\theta_1, ..., \theta_{n-1}, \xi, \omega$ with the unique defining relation $\xi^{p^s} = \omega^{\sigma-1}$, where $n = [K:\mathbb{Q}_p]$.*

It should be noted that in the aforementioned work outside of consideration remained non cyclotomic extensions for which either the inertia degree and the ramification index are different from 1, or the irregularity degrees of L and K are different. The case of regular K is considered in the paper [8]. With the development of the theory of formal groups it became clear that the considered additive and multiplicative cases are special cases of a more general construction. Namely, let $M/L, L/K, K/\mathbb{Q}_p$ be finite extensions with M/L Galois. If F is a one dimensional formal group law over the ring $\mathcal{O}_K$ then one can introduce a new operation on the maximal ideal $\mathfrak{p}_M$ according to the rule $x \underset{F}{+} y = F(x,y)$. From the axioms of a formal group it follows that the structure obtained is in fact an abelian group. It is denoted by $F(\mathfrak{p}_M)$. Now the task is to study $F(\mathfrak{p}_M)$ as a $\mathrm{Gal}(M/L)$-module, more precisely as a $\mathrm{End}_{\mathcal{O}_K}(F)[\mathrm{Gal}(M/L)]$-module, where $\mathrm{End}_{\mathcal{O}_K}(F)$ is the ring of endomorphisms of the formal group F. If $F = \mathbb{G}_a, F(x,y) = x + y$ is the additive formal group, then $F(\mathfrak{p}_M)$ is simply the ideal $\mathfrak{p}_M$ and $\mathrm{End}_{\mathcal{O}_K}(F) = \mathcal{O}_K$. This is precisely the additive case we considered above. Similarly, if $K = \mathbb{Q}_p$ and $F = \mathbb{G}_m$ is the multiplicative formal group given by the law $F(x,y) = x+y+xy$, then $\mathrm{End}_{\mathcal{O}_K}(F) = \mathbb{Z}_p$ and $F(\mathfrak{p}_M) \cong E, x \mapsto 1+x$ as $\mathbb{Z}_p[\mathrm{Gal}(M/L]$-modules, where $E = 1+\mathfrak{p}_M$ is the group of principal units in M. This one is the multiplicative case we considered earlier. Moreover, if we want a particularly large endomorphism group, we arrive at the so-called Lubin-Tate formal groups F, in which case for any element $a \in \mathcal{O}_K$ there is an endomorphism $[a]_F$ of F, starting with ax and $\mathrm{End}_{\mathcal{O}_K}(F)$ can be

identified with the ring $\mathcal{O}_K$ via the correspondence $a \mapsto [a]_F$. In the case of Lubin-Tate formal groups each of the $\mathcal{O}_K$-submodules $F(s) = \ker[\pi^s]_F \subset F(\mathfrak{p}_{M^{\text{alg}}}), s \geq 1$ can be shown to be cyclic, which allows us to use the concept of the irregularity degree in complete analogy with the multiplicative case. Namely, we say that K has irregularity degree s, if K contains a generator of $F(s)$ and does not contain any generator of $F(s+1)$. A slight modification of Borevich's theorem was proved in the paper [11], where the authors studied the structure of $F(\mathfrak{p}_M)$ in the case of a Lubin-Tate formal group F. More precisely, they proved the following

Theorem (Vostokov-Nekrasov, 2014) *Suppose M/L is an unramified p-extension and F is a Lubin-Tate formal group for the prime element $\pi \in K$. Assume moreover that the fields M and L have the same irregularity degree, namely they contain a generator of $\ker[\pi^s]_F$ and do not contain a generator of $\ker[\pi^{s+1}]_F$ for some $s \geq 1$. Then for the $\mathcal{O}_K[G]$-module $F(\mathfrak{p}_M)$ there exists a system of generating elements $\theta_1, ..., \theta_{n-1}, \xi, \omega$ with the unique defining relation $[\pi^s]_F(\xi) = \omega^\sigma \underset{F}{-} \omega$, where $n = [L : K]$ and σ is a generating element of the Galois group $G = \text{Gal}(M/L)$.*

The key point of this work was the observation that the cohomology group $H^1(\text{Gal}(M/L), F(\mathfrak{p}_M))$ is trivial for unramified extensions M/L. In the paper [12] T.Honda introduced a new method of constructing formal groups which were later named in his honor. They appeared to be generalizations of Lubin-Tate formal groups due to the classification theorems of *O.V.Demchenko*, proved in [13]. Thanks to the tight connection between these two types of formal groups it became possible to generalize the results already proved for Lubin-Tate formal groups to the case of Honda formal groups. An example of such a generalization was the work [14] of Demchenko, where he deduced explicit formulas for the Hilbert symbol in the case of Honda formal groups. We assume that in addition to the fields K, L, M an intermediate field $\mathbb{Q}_p \subset K_0 \subset K$ is given such that the extension K/K_0 is unramified and let F be a Honda formal group relative to the extension K/K_0 and the prime $\pi \in K_0$ (See [12, §2]). In analogy with Lubin-Tate formal groups the submodule $F(s) \subset F(\mathfrak{p}_{M^{\text{alg}}})$ defined earlier is isomorphic to $(\mathcal{O}_{K_0}/\pi^s\mathcal{O}_{K_0})^h$ as a $\mathcal{O}_{K_0}$-module for each positive integer $s \geq 1$, where h is the height of F. Let $W_F = \bigcup_{s=1}^{\infty} F(s)$ and let $\text{Gal}(M/L) = \langle\sigma\rangle$. In the second paragraph of the second chapter of the thesis (See also [15]) we generalized the previous Theorem to the case of Honda formal groups in the following manner.

Theorem 2.2 *If the extension M/L is unramified and $W_F \cap F(\mathfrak{p}_L) = W_F \cap F(\mathfrak{p}_M) = F(s)$,*

for some $s \geq 1$, *then* $h \leq n = [L : K_0]$ *and for the* $\mathcal{O}_{K_0}[\mathrm{Gal}(M/L)]$*-module* $F(\mathfrak{p}_M)$ *there exist a system of generating elements* $\theta_j, \xi_i, \omega_i, 1 \leq j \leq n-h, 1 \leq i \leq h$ *with the only defining relations* $[\pi^s]_F(\xi_i) = \omega_i^\sigma \underset{F}{-} \omega_i, 1 \leq i \leq h$.

The thesis contains some of our results on arithmetic sequences, namely the sequences whose terms are integers. The well-known theorem of Schur [25, Part 8, Ex. 108] asserts that whenever P is a non-constant polynomial with integer coefficients, the corresponding sequence $P(1), P(2), ...$ can not be constructed using only finitely many prime numbers, that is one can find infinitely many primes, dividing at least one term of the sequence. We will call such a sequence distinguished. It turns out that the property of being distinguished is peculiar to all rather "slowly" growing sequences. In the paper [26] we proved the following

Theorem 3.1 *If* $A = (a_n)_{n=1}^{\infty}$ *is an increasing sequence of positive integers and if*

$$\liminf_{n\to\infty} \frac{\ln(\ln(a_n))}{\ln(n)} = 0$$

then A *is distinguished.*

This result was previously proved in [27] for almost injective sequences. Note that a sequence is called almost injective if there exists a constant $C > 0$ such that for any h there are at most C values of n for which $a_n = h$. We would like to stress that our result is independent of [27]. Our next result we would to mention is related to the Fermat sequence defined by the formula $a_n = 2^{2^n} + 1$ for all n. It is known [28, Chapter 1, Theorem 13] that any two distinct terms of this sequence are coprime. We where interested in whether the result would remain true if we replaced 1 with an odd number d. The research answered this question in the negative.

Theorem 3.3 *If* d *is any integer different from 1, then for any* $M > 0$ *there exist distinct positive integers* m *and* n *such that* $\gcd(2^{2^m} + d, 2^{2^n} + d) > M$.

The structure of the thesis. We found it important to include in the text all the necessary information concerning local fields, formal groups and G-modules to rid the reader of numerous searches of the corresponding results in the literature. Whenever the proof of a statement is omitted, the exact reference to the relevant place in the literature is given. All this material is the content of the first chapter. We also recommend the following books and articles to the interested reader: for local fields we refer to [16–18], [19, Chapter 2], for Lubin-Tate formal groups see [16, Chapter 4], [20, Chapter 3, §6], for Honda formal groups the best source is the article [12], see also [13, 14]. Regarding formal

groups in general see [21] and [22]. For G-modules and Galois cohomology we refer to [23, Chapter 4,5], [24] and [20, Chapter 1, §§3,4].

The second chapter is devoted to the investigation of G-modules defined in extensions of local fields. It is divided into two sections. In the first section for cyclic extensions of local fields L/K (finite extensions of $\mathbb{Q}_p$) the structure of the $\mathbb{F}_p[G]$-module E/E^p is examined in each of the seven possible cases (Theorem 2.1), where E is the group of principal units of L. The content of the second section is, by and large, the proof of Theorem 2.2 mentioned earlier.

The third chapter contains some of our results on arithmetic sequences. It is likewise divided into two sections. The first section is devoted to distinguished arithmetic sequences and contains proofs of Theorems 3.1, 3.2 and 3.3. The second section of Chapter 3 contains the proof of Theorem 3.4 concerning asymptotic estimates of the divisor function.

The main results of the thesis have been published in 3 scientific articles [9], [26] and [35] and in the preprint [15]. The obtained results were presented at the Research Seminar of Constructive Class Field Theory of St. Petersburg State University, 2016-2018 as well as were scheduled for presentation at the International Conference On Number Theory which took place in Palagna, Lithuania from 09 to 15 September, 2018.

CHAPTER 1

Basic concepts

1.1 Valuation theory

1.1.1 Normed fields

DEFINITION **1.1** *A normed field is a field k together with a function $\| \| : k \to \mathbb{R}$, called absolute value (norm), which satisfies the following conditions*

- $\|x\| \geq 0$ *and* $\|x\| = 0$ *iff* $x = 0$
- $\|x + y\| \leq \|x\| + \|y\|$
- $\|xy\| = \|x\| \cdot \|y\|$

The absolute value $\| \|$ is called non-archimedean iff the second condition is fulfilled in a stronger form

$$\|x + y\| \leq \max\{\|x\|, \|y\|\}.$$

Otherwise it is called archimedean.

DEFINITION **1.2** *A function $\nu : k \to \mathbb{R} \cup \{\infty\}$ on a field k is called a valuation iff*

1. $\nu(x) = \infty$ *iff* $x = 0$
2. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$
3. $\nu(xy) = \nu(x) + \nu(y)$

From these definitions one can immediately derive the following

PROPOSITION **1.1** *There is one to one correspondence between non-archimedean absolute values and valuations on the field k, given by $\| \| \mapsto -\log(\| \|)$.*

THEOREM **1.1** *An absolute value $\| \ \|$ on a field k is non-archimedean iff $\|n \cdot \mathbf{1}_k\| \leq 1$ for all $n \in \mathbb{Z}$, where $\mathbf{1}_k$ is the unity of k.*

Proof. It suffices to prove that $\|x\| \leq 1$ implies $\|1 + x\| \leq 1$. Indeed,

$$\|(1+x)^n\| = \left\| \sum_{k=0}^{n} \binom{n}{k} x^k \right\| \leq \sum_{k=0}^{n} \left\| \binom{n}{k} \right\| \|x\|^k \leq n+1.$$

Taking n-th roots and passing to the limit, we get the desired result. □

COROLLARY **1.1** *If k is a field of characteristic $p > 0$, then any absolute value on it is non-archimedean.*

Proof. In this case the prime subfield of k is the field $\mathbb{F}_p$ of p elements, so that $x^{p-1} = 1$ and thus $\|x\| = 1$ for any $x \in \mathbb{F}_p^*$. Therefore we can apply Theorem 1.1. □

From the proof of Corollary 1.1 we get

COROLLARY **1.2** *Any absolute value on a finite field k is trivial, i.e. $\|x\| = 1$ for any $x \in k^*$.*

In the sequel we will assume that $(k, \| \ \|)$ is a normed field and $\| \ \|$ is non-archimedean, if the opposite is not mentioned. What follows from Proposition 1.1, we can equivalently use valuations ν. If ν is the valuation corresponding to the absolute value $\| \ \|$, then

DEFINITION-THEOREM **1.1** *The set $\mathfrak{o} = \{x \in k | \nu(x) \geq 0\} = \{x \in k | \ \|x\| \leq 1\}$ is a subring of k, which is called the valuation ring of k. It is a local ring with maximal ideal $\mathfrak{p} = \{x \in k | v(x) > 0\} = \{x \in k | \ \|x\| < 1\}$, called the valuation ideal. Further, the set $U = \mathfrak{o} \setminus \mathfrak{p} = \{x \in k | \nu(x) = 0\} = \{x \in k | \ \|x\| = 1\}$ coincides with the group of invertible elements of $\mathfrak{o}$. The field $\mathrm{f} = \mathfrak{o}/\mathfrak{p}$ is called the residue field of k.*

Proof. Every element in $\mathfrak{o} \setminus \mathfrak{p}$ has valuation zero so that its inverse in k also has valuation zero and is thus in $\mathfrak{o}$, which means that it is invertible in the ring $\mathfrak{o}$. Hence $\mathfrak{o}$ is a local ring with maximal ideal $\mathfrak{p}$. Everything else is clear. □

Any normed field $(k, \| \ \|)$ is a metric space with respect to the metric $d(x, y) = \|x - y\|$ and turns into a topological field with respect to the topology induced by this metric, the collection $B_n = \{x \in k | \ \|x\| < 1/n\}$ is a basis of neighborhoods of 0.

Examples of normed fields

1. The usual absolute value is an archimedean absolute value on fields $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

2. Suppose p is a prime number. Each nonzero rational number r can be written uniquely in the form $r = p^n \frac{a}{b}$ where n, a, b are integers, $b > 0, \gcd(a, b) = 1$ and $p \nmid ab$. It can be shown that the function $\|\cdot\|_p : \mathbb{Q} \to \mathbb{R}$ defined by

$$\|r\|_p = \begin{cases} p^{-n}, & r \neq 0 \\ 0, & r = 0 \end{cases}$$

   is a non-archimedean absolute value, called the p-adic absolute value.

3. Suppose $\mathbb{F}$ is a field, $\mathbb{F}(t)$ is the field of rational functions and $p(t) \in \mathbb{F}[t]$ is a fixed irreducible polynomial. Similar to the previous case, any nonzero rational function $r(t)$ admits a representation $r(t) = p^n(t)\frac{a(t)}{b(t)}$ with uniquely determined integer n, where $p(t)$ does not divide $a(t)$ and $b(t)$. In complete analogy with the field of rational numbers, for given real number $c > 1$ the function $\|\cdot\|_p : \mathbb{F}(t) \to \mathbb{R}$ defined by

$$\|r\|_p = \begin{cases} c^{-n}, & r \neq 0 \\ 0, & r = 0 \end{cases}$$

   is a non-archimedean absolute value. In addition to these absolute values one can define a new one by the formula $\|r\|_\infty = c^{\deg p - \deg q}$, for any representation $r(t) = \frac{p(t)}{q(t)}$. Note that $\|\cdot\|_\infty$ is the compositum of $\|\cdot\|_T$ with the automorphism φ of $\mathbb{F}(t)$, given by $t \mapsto \frac{1}{t}$. More precisely, $\|r(t)\|_\infty = \|r\left(\frac{1}{t}\right)\|_T$.

We proceed with the following

DEFINITION **1.3** *Two absolute values* $\| \ \|_1$ *and* $\| \ \|_2$ *on a field* k *are called equivalent iff there is* $\alpha > 0$ *such that* $\|x\|_1 = \|x\|_2^\alpha$ *for all* $x \in k$.

THEOREM **1.2** *The absolute values* $\| \ \|_1$ *and* $\| \ \|_2$ *on a field* k *are equivalent iff they induce the same topology on* k.

Proof. The necessity follows from the fact that if $\|x\|_1 = \|x\|_2^\alpha$, then the open sets and thus the topologies defined by these absolute values do coincide. To prove the sufficiency observe that the

condition $\|x\| < 1$ is equivalent to the condition $x^n \to 0$, which is of topological nature. Therefore $\|x\|_1 < 1 \Leftrightarrow \|x\|_2 < 1$ and consequently $\|x\|_1 > 1 \Leftrightarrow \|x\|_2 > 1$. Let x and y satisfy $\|x\|_1 > 1$ and $\|y\|_1 > 1$. By what we mentioned above they also satisfy $\|x\|_2 > 1$ and $\|y\|_2 > 1$. By the same observation $\|x^m y^n\|_1 > 1 \Leftrightarrow \|x^m y^n\|_2 > 1$, so that $m\log(\|x\|_1) + n\log(\|y\|_1) > 0 \Leftrightarrow m\log(\|x\|_2) + n\log(\|y\|_2) > 0$. Since all the numbers $\log(\|x\|_i), \log(\|y\|_i)$ are positive, the latter equivalence means that $\frac{\log(\|x\|_1)}{\log(\|x\|_2)} = \frac{\log(\|y\|_1)}{\log(\|y\|_2)}$. Therefore there is a positive constant α for which the equality $\log(\|x\|_1) = \alpha\log(\|x\|_2)$ is valid for any x, satisfying $\|x\|_i > 1, i = 1, 2$. Since $\log(\|x^{-1}\|_i) = -\log(\|x\|_i)$, it holds for any $x \in k^*$. Exponentiation of the obtained equality yields the desired result. □

REMARK **1.1** *Simultaneously we have proved that the following conditions are equivalent*

- *The absolute values* $\|\ \|_1$ *and* $\|\ \|_2$ *induce the same topology on* k.
- *There exists* $\alpha > 0$ *such that* $\|x\|_1 = \|x\|_2^\alpha$ *for all* $x \in k$.
- *The conditions* $\|x\|_1 < 1$ *and* $\|x\|_2 < 1$ *are equivalent.*

From the proof of Theorem 1.2 it also follows that the aforementioned 3-rd condition can be weakened to the condition: $\|x\|_1 < 1 \Rightarrow \|x\|_2 < 1$. *Moreover, if the valuation* $\|\ \|_2$ *is non-trivial, we could equivalently use the implication* $\|x\|_1 < 1 \Rightarrow \|x\|_2 \leq 1$, *while for the trivial* $\|\ \|_2$ *the implication* $\|x\|_1 < 1 \Rightarrow \|x\|_2 \leq 1$ *is valid for any absolute value* $\|\ \|_1$ *and the latter is not equivalent to* $\|\ \|_2$, *unless it is trivial.*

COROLLARY **1.3** *An archimedean absolute value is never equivalent to a non-archimedean one.*

Proof. Indeed, due to Theorem 1.1, an absolute value is non-archimedean if and only if $\|n \cdot \mathbf{1}_k\| \leq 1$ for all $n \in \mathbb{Z}$. This condition does not depend on which of the equivalent valuations we consider. □

Suppose that we are given mutually nonequivalent non-trivial absolute values $\|\ \|_i, 1 \leq i \leq N$ on the field k. For each i we denote by k_i the topological space, whose underlying set is the underlying set of k and the topology is induced by $\|\ \|_i$. One can prove the following

THEOREM **1.3 (Artin-Waples, Approximation theorem)** *The image of the diagonal map* $k \to \prod_{1\leq i\leq N} k_i$ *is dense, where* $\prod_{1\leq i\leq N} k_i$ *is given the product topology.*

In other words, the theorem states that for any $\varepsilon > 0$ and elements $\alpha_i \in k, 1 \leq i \leq N$ there exists an element $\xi \in k$, such that $\|\xi - \alpha_i\|_i < \varepsilon$ for all i.

Proof. Observe that it is enough for each $1 \leq i \leq N$ to construct an element $\theta_i \in k$ for which $\|\theta_i\|_i > 1$ and $\|\theta_i\|_j < 1$ for each $j \neq i$. Indeed, in case these elements are constructed, the number

$$\xi = \sum_{1 \leq i \leq N} \frac{\theta_i^r}{1+\theta_i^r} \alpha_i$$

will satisfy the required conditions for sufficiently large positive integer r. We now prove the existence of $\theta = \theta_1$ by induction. For $N = 2$ the assertion follows from Remark 1.1. Suppose $N \geq 3$. By the induction hypothesis there exists an element $\phi \in k$ which satisfies the conditions $\|\phi\|_1 > 1$ and $\|\phi\|_i < 1$ for $2 \leq i \leq N-1$. Since $\| \ \|_1$ and $\| \ \|_N$ are not equivalent, then, according to Case $N = 2$ we conclude the existence of an element ψ for which $\|\psi\|_1 > 1$ and $\|\psi\|_N < 1$. To complete the proof we set

$$\theta = \begin{cases} \phi, & \|\phi\|_N < 1 \\ \phi^r \psi, & \|\phi\|_N = 1 \\ \phi^r \psi/(1+\phi^r), & \|\phi\|_N > 1 \end{cases}$$

for sufficiently large positive integer r. □

Note that for $k = \mathbb{Q}$, Theorem 1.3 , in a sence, is the Chinese remainder theorem. In the case of the field of rational numbers $\mathbb{Q}$ there is the usual absolute value and p-adic absolute value for each prime number p (see Example 2). It turns out that this is the full list of absolute values on $\mathbb{Q}$. More precisely there is an important

THEOREM **1.4 (Ostrowski, 1916)** *Each non-trivial absolute value on $\mathbb{Q}$ is equivalent to either the usual absolute value or a p-adic absolute value for certain prime number p.*

Proof. See [23, Chapter 2, Thm. 3.2] . □

Similarly, for the field of rational functions $\mathbb{F}(t)$ (see Example 3) there is a

THEOREM **1.5** *Each non-trivial absolute value on $\mathbb{F}(t)$, which is trivial on $\mathbb{F}$, is equivalent to either $\| \ \|_\infty$ or $\| \ \|_p$ for some irreducible polynomial $p(t) \in \mathbb{F}[t]$.*

From Corollary 1.2 and Theorem 1.4 we deduce

COROLLARY **1.4** *Each non-trivial absolute value on $\mathbb{F}_q(t)$ is equivalent to either $\| \ \|_\infty$ or $\| \ \|_p$ for some irreducible polynomial $p(t) \in \mathbb{F}_q[t]$, where $\mathbb{F}_q$ is the finite field of q elements.*

1.1.2 Complete fields, discrete valuations

DEFINITION **1.4** *A normed field k is called complete iff it is complete as a metric space with respect to the metric induced by the norm.*

DEFINITION **1.5** *Let k be a normed field, including the archimedean case. The field $\hat{k}$ is called the completion of k iff*

1. *$\hat{k}$ is complete*
2. *There is an isometric field embedding $k \hookrightarrow \hat{k}$ onto a dense subfield of $\hat{k}$*

Similar to metric spaces we have the following

THEOREM **1.6** *Any normed field k has a completion, which is unique up to an isometric isomorphism of fields over k.*

Proof. (Sketch) Consider the completion $\hat{k}$ of k in the sense of metric spaces. Recall that the elements of $\hat{k}$ are the equivalence classes of Cauchy sequences of elements from k. The addition and multiplication are defined on $\hat{k}$ in a natural way, endowing it with a ring structure. The role of 0 plays the equivalence class of null-sequences, i.e. the sequences tending to zero, similarly the role of 1 plays the equivalence class of the stationary sequence, consisting of ones. Any nonzero equivalence class is invertible in this ring, since any Cauchy sequence which is not equivalent to the zero sequence, is separated from zero and thus if we take the inverses of elements of this sequence, we get a new Cauchy sequence, the equivalence class of which is defined as the inverse of the equivalence class containing the initial sequence. Therefore $\hat{k}$ is a field, moreover if we take an equivalence class $\mathscr{C}$ and a Cauchy sequence $c = (c_n)_{n=1}^{\infty} \in \mathscr{C}$ then we can define $\|\mathscr{C}\|_{\hat{k}} = \lim_{n\to\infty} \|c_n\|_k$, which, as can be shown, exists and does not depend on the choice of the representative c. Passing to the limit we can show that $\| \ \|_{\hat{k}}$ is an absolute value on the field $\hat{k}$ and that the natural embedding of k into $\hat{k}$ is an isometry onto a dense subfield. If $\hat{k}_1$ and $\hat{k}_2$ are two completions of k, then they contain dense isometric copies of k. Extending this isometry, we get an isometric field isomorphism from $\hat{k}_1$ onto $\hat{k}_2$ over k. □

Examples

4. The field of rational numbers $\mathbb{Q}$ is not complete with respect to the usual absolute value. Its completion is the field of real numbers $\mathbb{R}$.

5. For each rational prime p, the field $\mathbb{Q}$ is not complete with respect to the p-adic absolute value $\| \ \|_p$ (see Example 2). In fact, it can be shown that the Cauchy sequence of rational numbers $r_n = \sum_{1\leq i\leq n} p^{i^2}$ does not converge to any rational number. The completion of $\mathbb{Q}$ with respect to the p-adic metric is called the field of p-adic numbers. It is denoted by $\mathbb{Q}_p$ and its elements are the formal expressions of the form $\alpha = \sum_{i\gg -\infty} a_i p^i$, where $a_i \in \{0, 1, ..., p-1\}$ for all i. Therefore the absolute value on $\mathbb{Q}_p$ is given by $\|\alpha\|_p = p^{-n}$, where n is the number of the first nonzero coefficient a_n. The elementary operations are performed in a natural way, extending the p-base arithmetic to infinite expressions. The ring of integers (see Definition-theorem 1.1) of $\mathbb{Q}_p$ is called the ring of p-adic integers and is denoted by $\mathbb{Z}_p$. It is the completion of the ring $\mathbb{Z}$ of ordinary integers with respect to the p-adic metric, induced from $\mathbb{Q}$. In its turn, the elements of $\mathbb{Z}_p$ are the expressions not containing negative terms, namely $\alpha = \sum_{i\geq 0} a_i p^i$. The valuation ideal is the ideal $p\mathbb{Z}_p$ of all p-adic integers, which are divisible by p and consists of the elements of the form $\alpha = \sum_{i\geq 1} a_i p^i$. The residue field is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.

6. If $\mathbb{F}$ is a field, then the field $\mathbb{F}(t)$ of rational functions is not complete with respect to the absolute value $\| \ \|_T$ (see Example 3), since the Cauchy sequence of rational functions $R_n(t) = \sum_{0\leq i\leq n} t^i$ is not convergent. One may check, that the completion of $\mathbb{F}(t)$ with respect to $\| \ \|_T$ is the field $\mathbb{F}((t))$ of Laurent series involving only finite number of negative powers. So the absolute value on $\mathbb{F}((t))$ is given by $\|\alpha(t)\|_T = c^{-n}$, where $\alpha(t) = \sum_{i\gg -\infty} a_i t^i$, n is the number of the first nonzero coefficient of α and $c > 1$ is the real number which was used when defining $\| \ \|_T$ on $\mathbb{F}(t)$. The valuation ring of $\mathbb{F}((t))$ is the ring $\mathbb{F}[[t]]$ of formal power series involving only non-negative powers, the valuation ideal is the ideal $t\mathbb{F}[[t]]$ of all formal power series involving only positive powers of the indeterminate t. The residue field is thus $\mathbb{F}[[t]]/(t) \cong \mathbb{F}$.

   Similarly, the completion of $\mathbb{F}(t)$ with respect to $\| \ \|_\infty$ (see Example 3) is the field $\mathbb{F}((1/t))$ of all Laurent power series containing finitely many positive powers. The absolute value on $\mathbb{F}((1/t))$ is given by $\|\alpha(t)\|_T = c^n$, where $\alpha(t) = \sum_{i\ll \infty} a_i t^i$, n is the number of the rightmost nonzero coefficient of α and $c > 1$ is the real number which was used when defining $\| \ \|_\infty$ on $\mathbb{F}(t)$. Furthermore, the valuation ring will be the ring $\mathbb{F}[[1/t]]$ of powers series without positive powers, the valuation ideal will be the ideal $(1/t)\mathbb{F}[[1/t]]$ and the residue field will be again $\mathbb{F}$.

In case of archimedean absolute values the situation is more or less clear due to the following

THEOREM **1.7 (Gelfand-Tornheim-Ostrowski)** *Any complete archimedean normed field $(k, \| \ \|)$ admits an isometric field isomorphism $\sigma : (k, \| \ \|) \to (\mathbb{R}, |\ |^c)$ or $(\mathbb{C}, |\ |^c)$ for uniquely determined $c \in (0, 1]$, where $|\ |$ is the standard absolute value on $\mathbb{R}$ (resp. $\mathbb{C}$). In particular, any archimedean normed field can be thought of as a subfield of the field of complex numbers the absolute value being equivalent to that induced by the usual absolute value on $\mathbb{C}$.*

Proof. See [19, Prop. 4.2] □

In non-archimedean case we have the following

PROPOSITION **1.2** *The normed field k is non-archimedean iff so is its completion $\hat{k}$. If this is the case then the corresponding absolute values have the same image as functions. Moreover, if we denote by $\hat{\mathcal{O}}$ and $\hat{\mathfrak{p}}$ the corresponding valuation ring and valuation ideal, then $\hat{\mathcal{O}}/\hat{\mathfrak{p}} = \mathcal{O}/\mathfrak{p}$.*

Proof. The first assertion follows from Theorem 1.1, while the second one is a direct consequence of the fact that whenever $\|y\| < \|x\|$ the equality $\|x + y\| = \|x\|$ holds. To prove the last assertion, observe that $\mathfrak{p} = \hat{\mathfrak{p}} \cap \mathcal{O}$, so that the inclusion $\mathcal{O} \hookrightarrow \hat{\mathcal{O}}$ induces a field embedding $\mathcal{O}/\mathfrak{p} \to \hat{\mathcal{O}}/\hat{\mathfrak{p}}$. The surjectivity of the latter follows from the construction of $\hat{k}$, namely for any $x \in \hat{\mathcal{O}}$, there exists an $y \in \mathcal{O}$ such that $\|x - y\| < 1$. □

We proceed with the definition of a normed vector space.

DEFINITION **1.6** *Let $(k, |\ |)$ be a normed field. A normed k-vector space is a pair $(V, \| \ \|)$ of a vector space V over k and a function $\| \ \| : V \to \mathbb{R}$, called norm, which satisfies the following conditions*

- $\|x\| \geq 0$ *and* $\|x\| = 0$ *iff* $x = 0$
- $\|x + y\| \leq \|x\| + \|y\|$
- $\|\lambda x\| = |\lambda| \cdot \|x\|$

for all $x, y \in V$ and $\lambda \in k$.

In what follows we shall need the following

LEMMA **1.1** *If k is complete, then any two norms $\| \ \|_1$ and $\| \ \|_2$ on a finite dimensional k-vector space V are equivalent, namely there exist positive constants C_1 and C_2 such that $\|x\|_1 \leq C_1\|x\|_2$ and*

$\|x\|_2 \leq C_2\|x\|_1$ *for all* $x \in V$. *Moreover, the vector space* V *is complete with respect to any norm on it.*

Proof. The last assertion is a direct consequence of the first one, so we focus on the former statement. Let us fix a basis $x_1, ..., x_N$ of V and define the norm $\| \ \|_0$ on V by the formula

$$\left\|\sum \lambda_n x_n\right\|_0 = \max_n |\lambda_n|.$$

It is enough to show that any norm $\| \ \|$ is equivalent to $\| \ \|_0$. First we note that

$$\left\|\sum \lambda_n x_n\right\| \leq \sum |\lambda_n| \cdot \|x_n\| \leq C_1 \left\|\sum \lambda_n x_n\right\|_0,$$

where $C_1 = \sum \|x_n\|$. Assume the contrary that there is no constant C_2 for which the inequality $\|x\|_0 \leq C_2\|x\|$ holds for any $x \in V$. Hence there exists a sequence $(v_i)_{i=1}^{\infty} \subset V$, $v_i = \sum_{1 \leq j \leq N} \lambda_{i,j} x_j$ of elements, for which $\|v_i\| < \frac{1}{i}\|v_i\|_0$ for all i. One has that there exist some index $1 \leq j_0 \leq N$ for which $\max_j \|\lambda_{i,j}\| = |\lambda_{i,j_0}\|$ for infinitely many indices i, so that we may assume without loss of generality that $j_0 = N$ and that $\lambda_{i,N} = 1$ for all i. Therefore $v_i \to 0$ and the sequence $\sum_{1 \leq j \leq N-1} \lambda_{i,j} x_j = v_i - x_n$ is a Cauchy sequence. The statement of the lemma is trivial for $N = 1$, suppose it is true for $N - 1$ dimensional spaces and observe that the sequence $(v_i - x_n)_{i=1}^{\infty}$ is in the $N - 1$ dimensional subspace of V generated by $x_1, ..., x_{N-1}$, so that by the induction hypothesis for each j the coordinate sequence $(\lambda_{i,j})_{i=1}^{\infty}$ is a Cauchy sequence in k. Now the completeness of k comes into play, showing that there are $\lambda_j^* \in k, 1 \leq j \leq N - 1$ for which $\lambda_{i,j} \to \lambda_j^*$ for each j. Passing to the limit in $v_i \to 0$ we get $\sum_{1 \leq j \leq N-1} \lambda_j^* x_j + x_N = 0$, which is a contradiction. Therefore such a constant C_2 with the required property exists and the induction step is complete, thus finishing the proof of the lemma. □

We find it necessary to introduce the following key lemma, which allows to factor polynomials over the valuation ring of a complete field.

LEMMA **1.2 (Hensel's)** *Let* $(k, \| \ \|)$ *be a non-archimedean complete normed field with valuation ring* $\mathfrak{o}$, *valuation ideal* $\mathfrak{p}$ *and residue field* $\mathrm{f} = \mathfrak{o}/\mathfrak{p}$. *Let* $f \in \mathfrak{o}[x]$,

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + ... + a_1 x + a_0$$

be a primitive polynomial, which means that the reduction $\bar{f}$ *of* f *modulo* $\mathfrak{p}$ *is nonzero, i.e.* $\max_{0 \leq i \leq m} \|a_i\| = 1$. *Assume moreover that* $\bar{f} = \mathfrak{g}\mathfrak{h}$, $\gcd(\mathfrak{g}, \mathfrak{h}) = 1$ *in* $\mathrm{f}[x]$. *Then there exist polynomials* $g, h \in \mathfrak{o}[x]$ *such that* $\bar{g} = \mathfrak{g}, \bar{h} = \mathfrak{h}$, $\deg(g) = \deg(\mathfrak{g})$ *and* $f = gh$.

We will not present the proof of this lemma here, since it is fairly long. If the reader is interested in the proof, we refer to [29, §144]. Instead we derive some crucial consequences on which the rest of the theory is founded.

COROLLARY **1.5** *Under the conditions of Lemma 1.2 if $\bar{f}$ has a simple root $a \in \mathrm{f}$, then there is a unique element $\alpha \in \mathfrak{o}$ such that $f(\alpha) = 0$ and $\bar{\alpha} = a$.*

Proof. It suffices to set $\mathfrak{g}(x) = x - a$ to complete the proof. □

COROLLARY **1.6** *If $(k, \| \ \|)$ is a non-archimedean complete normed field, $f(x) = \sum_{0 \le i \le n} a_i x^i \in k[x]$ is an irreducible polynomial of degree n, then $\max_{0 \le i \le n} \|a_i\| = \max\{\|a_0\|, \|a_n\|\}$. In particular, if f is monic, then $\|a_0\| \ \le 1$ implies $\|a_i\| \ \le 1$ for all i.*

Proof. For $n = 1$ the statement is true. Assume the contrary that $n > 1$ and $\max_{1 \le i \le n-1} \|a_i\| = \|a_j\| > \max\{\|a_0\|, \|a_n\|\}$. Since $\|a_j^{-1} a_0\| < 1, \|a_j^{-1} a_n\| < 1$ and $\|a_j^{-1} a_i\| \le 1$ for all $1 \le i \le n-1$ we get that for some $0 < t < n$ the reduction of the irreducible polynomial $a_j^{-1} f$ modulo $\mathfrak{p}$ is $X^t \mathfrak{h}$ for certain polynomial $\mathfrak{h}$ with $\mathfrak{h}(0) \neq 0$. This implication contradicts Hensel's lemma . □

We now introduce discrete valuations. In the following definition we prefer to use valuations rather than absolute values.

DEFINITION **1.7** *If ν is a valuation on the field k (See Definition 1.2), then the set $\Gamma = \nu(k^*)$ is a subgroup of $(\mathbb{R}, +)$, called the value group of ν. A valuation ν on the field k is called discrete iff Γ is discrete and regular iff $\Gamma = \mathbb{Z}$. If ν is discrete we will call k a discrete valuation field.*

All absolute values (valuations) mentioned in Examples 2,3,5,6 are examples of discrete valuations. Observe that each non-trivial discrete valuation becomes regular after multiplication by a suitable positive real constant, since each non-trivial discrete subgroup of $(\mathbb{R}, +)$ is generated by some $c > 0$.

DEFINITION-THEOREM **1.2** *A valuation ν on the field k is discrete iff the valuation ideal $\mathfrak{p}$ is principal. If this is the case, then the valuation ring $\mathfrak{o}$ is a discrete valuation ring, equivalently a local PID or a local Dedekind domain, with ideal group $I_k = \{\mathfrak{p}^n | n \in \mathbb{Z}\}$. If ν is regular then the elements $x \in k$ satisfying $\nu(x) = 1$ are all possible generators of $\mathfrak{p}$. Any such element is called a uniformizer and is denoted by π. The subgroups $\mathfrak{p}^n$ of $(k, +)$ form a basis of cl-open neighborhoods of 0, and k becomes a non-discrete totally disconnected topological field. Similarly the subgroups $U_0 = U, U_n = 1 + \mathfrak{p}^n, n \ge 1$*

of $(k^*, \cdot)$ *form a basis of cl-open neighborhoods of* $1 \in k^*$*, so that* k^* *becomes a non-discrete totally disconnected topological group. Moreover, there are isomorphisms of groups*

$$k^* \cong (\pi) \times U$$

$$U/U_1 \cong \mathrm{f}^*;\ [x] \mapsto x(\mathrm{mod}\ \mathfrak{p})$$

and

$$U_n/U_{n+1} \cong \mathrm{f}^+, n \geq 1;\ [1 + x\pi^n] \mapsto x(\mathrm{mod}\ \mathfrak{p}).$$

Proof. We will prove only the first assertion. To do this recall that a non-trivial subgroup of $(\mathbb{R}, +)$ is discrete if and only if it possesses a minimal positive element c. If the valuation ideal $\mathfrak{p}$ is principal then there surely exists an element with minimal positive valuation, in fact any generator of the valuation ideal will work. Conversely, if there is such an element λ, then each other element μ from the valuation ideal $\mathfrak{p}$ will satisfy $\nu(\mu) \geq \nu(\lambda)$ which is amount to saying that $\mu \in (\lambda)$ so that $\mathfrak{p} = (\lambda)$ is principal and we are done. Further, since the value group of ν is $\Gamma = \{nc | n \in \mathbb{Z}\}$, any nonzero ideal $\mathfrak{a} \subset \mathfrak{o}$ possesses an element of minimal positive valuation, say $\lambda_\mathfrak{a}$ with $\nu(\lambda_\mathfrak{a}) = n_\mathfrak{a} c$. Then in the same way we deduce that $\mathfrak{a} = (\lambda_\mathfrak{a}) = (\lambda^{n_\mathfrak{a}}) = \mathfrak{p}^{n_\mathfrak{a}}$, since $\lambda_\mathfrak{a}$ and $\lambda^{n_\mathfrak{a}}$ have the same valuation and therefore are associate. □

Suppose for each $m \in \mathbb{Z}$ an element $\pi_m \in k$ is fixed with $\nu(\pi_m) = m$. Let $R \subset \mathfrak{o}$ be a complete representative system of $\mathfrak{o}$ modulo $\mathfrak{p}$. Then one can prove the following

Proposition **1.3** *If* k *is a complete field with respect to a discrete regular valuation* ν *and* π *is a uniformizer, then any element* $x \in k$ *can be uniquely written as a Laurent series*

$$x = \sum_{m \gg -\infty} a_m \pi_m, a_m \in R.$$

Proof. Observe that $\mathfrak{o} = R + \mathfrak{p} = \{x + y | x \in R, y \in \mathfrak{p}\}$ and therefore $\mathfrak{p}^m = \pi_m \mathfrak{o} = \pi_m R + \mathfrak{p}^{m+1}$ for all $m \in \mathbb{Z}$. The completeness of k yields $\mathfrak{p}^m = \sum_{i \geq m} \pi_i R$ for all $m \in \mathbb{Z}$. Since $k = \bigcup_{m \in \mathbb{Z}} \mathfrak{p}^m$, we are done. Suppose $\sum_m a_m \pi_m = \sum_m b_m \pi_m$, where $a_m, b_m \in R$. If there exists m with $a_m \neq b_m$, then take the least such index m_0 and observe that $\nu\left(\sum_m (a_m - b_m)\pi_m\right) = m_0$. The attained contradiction completes the proof. □

1.1.3 Extensions of normed fields

In this section we will use the notation $(k, |\ |)$ for a normed field k equipped with an absolute value $|\ |$. Suppose K/k is an extension, we will assume that it is algebraic. Let $\|\ \|$ be a valuation on K. We will say that $\|\ \|$ is an extension of $|\ |$, if $\|x\| = |x|$ for all $x \in k$. A natural question arises: is it always possible to extend $|\ |$ to K. First we will consider the case when k is complete.

THEOREM **1.8** *If $(k, |\ |)$ is complete and K/k is any algebraic extension, then there is a unique extension of $|\ |$ to K. Moreover, if K/k is finite and $n = [K : k]$, then this extension can be given explicitly in the form $\|x\| = \sqrt[n]{\left|N_{K/k}(x)\right|}$. Moreover, $(K, \|\ \|)$ is a complete field.*

Proof. By a quick observation of the expression, mentioned in the statement of the theorem, one may reduce the proof to the case of finite extension K/k.

To prove the uniqueness, we recall that any absolute value $\|\ \|$ on K extending $|\ |$ turns it into a finite dimensional normed k-vector space. Using the completeness of $(k, |\ |)$ we get by Lemma 1.1 that $(K, \|\ \|)$ is complete and any two norms $\|\ \|_1$ and $\|\ \|_2$ on it are equivalent and hence are topologically equivalent. According to Theorem 1.2 one can write $\|\ \|_1 = \|\ \|_2^{\alpha}$ for some $\alpha > 0$. Since $\|\ \|_1$ and $\|\ \|_2$ coincide on k, we get that $\alpha = 1$ unless they are trivial. In the latter case, the trivial absolute on K extends $|\ |$ and therefore any other extension is trivial, being equivalent to the trivial absolute value.

For the existence we will try a good candidate $\|x\| = \sqrt[n]{\left|N_{K/k}(x)\right|}$ mentioned in the theorem, which turns out to be an extension of $|\ |$ and satisfies the conditions 1) and 3) of Definition 1.1. So it remains to check whether it satisfies 2). If $|\ |$ is archimedean, then by Theorem 1.7 $k = \mathbb{R}$ or $\mathbb{C}$ and $|\ |$ is equivalent to the standard absolute value, so that in either case $\|\ \|$ satisfies the condition 2). For the non-archimedean case it is enough to check that $\|\alpha\| \leq 1$ implies $\|\alpha - 1\| \leq 1$. Let us see what does this mean. If $f_\alpha(x) = x^m + \sum_{0 \leq i \leq n-1} a_i X^i$ is the minimal polynomial of α over k and $s = [K : k(\alpha)]$ then $N_{K/k}(\alpha) = (-1)^n a_0^s$ and $N_{K/k}(\alpha - 1) = (-1)^n (1 + \sum_{0 \leq i \leq n-1} a_i)^s$, so that the latter assertion is a direct consequence of Corollary 1.6. □

In general we proceed in the following way. If $\bar{k}$ denotes the completion of k and $\mathfrak{N}$ is the nil-radical of the ring $K \underset{k}{\otimes} \bar{k}$, then there is an isomorphism

$$\varphi : K \underset{k}{\otimes} \bar{k}/\mathfrak{N} \xrightarrow{\sim} \prod_{i=1}^{m} K_i$$

of $\bar{k}$-algebras for certain fields K_i, each of which is a finite extension of $\bar{k}$. Moreover, the number m is uniquely determined and the extensions K_i are unique in the sense that for any other such list $K_i', 1 \leq i \leq m$ of fields there exists a permutation $\sigma : \{1, 2, ..., m\} \to \{1, 2, ..., m\}$ and isomorphisms $\phi_i : K_i \xrightarrow{\sim} K'_{\sigma(i)}$ over $\bar{k}$. For more details we refer to [23, Chapter 2,§§9-11].

Since the fields K_i are finite extensions of the complete field $\bar{k}$, by Theorem 1.8 there exists a unique extension $\| \ \|_i$ of $| \ |$ to K_i and $(K_i, \| \ \|_i)$ is complete for each $1 \leq i \leq m$. Let $i : K \to K \underset{k}{\otimes} \bar{k}$ be the homomorphism $a \mapsto a \otimes 1$, $\pi : K \underset{k}{\otimes} \bar{k} \to K \underset{k}{\otimes} \bar{k}/\mathfrak{N}$ be the natural epimorphism and $\pi_i : \prod_{i=1}^m K_i \to K_i$ be the projections onto K_i for each $1 \leq i \leq m$. Then the maps $\psi_i = \pi_i \circ \varphi \circ \pi \circ i : K \to K_i, 1 \leq i \leq m$ are ring homomorphisms and are therefore injective so that K can be regarded as a subfield of K_i for all i. Since $K = K \underset{k}{\otimes} k$ is dense in $K \underset{k}{\otimes} \bar{k}$, the field $K \cong \psi_i(K)$ is a dense subfield of K_i, so that K_i is the completion of K with respect to the absolute value transplanted from K_i via ψ_i. Moreover, it turns out that these absolute values are pairwise distinct and constitute a complete list of extensions of the absolute value $| \ |$ to K.

If, in addition, $K = k(\alpha)$ for some $\alpha \in K$ with minimal polynomial $f \in k[x]$, then the composite map

$$K \underset{k}{\otimes} \bar{k} = \bar{k}[x]/(f) \to \prod_{i=1}^{m} \bar{k}[x]/(g_i) \xrightarrow{\sim} \prod_{i=1}^{m} \bar{k}(\alpha_i)$$

has kernel $(\prod_{1 \leq i \leq m} g_i(x))\bar{k}[x]/(f) = \mathfrak{N}\,(k[x]/(f))$, where $f = \prod_{1 \leq i \leq m} g_i^{e_i}$ is the factorization of f in $\bar{k}[x]$ and α_i is a root of g_i for each i. Moreover, $K_i = \bar{k}(\alpha_i)$ and $\psi_i : K \to K_i$ sends α to α_i. The number of distinct extensions of $| \ |$ to K is thus equal to m.

COROLLARY **1.7** *If K/k is a purely inseparable finite extension, then there is precisely one extension of $| \ |$ to K.*

Proof. Suppose $K = k(\alpha)$. The minimal polynomial of α has the form $X^{p^s} - a$ for some $a \in k$, which has only $m = 1$ irreducible factor as a polynomial in $L[x]$ for any extension L/k, in particular for $L = \bar{k}$. Therefore, according to what was said above the extension of $| \ |$ to K is unique . In general, K/k is a tower of such extensions, so that the conclusion remains true anyway. □

In what follows we will assume that K/k is an extension, not necessarily algebraic and the absolute value $\| \ \|$ on K extends the absolute value $| \ |$ of k. In this case we say that K/k is an extension of normed fields. Let $\Gamma', \mathfrak{o}', \mathfrak{p}', \mathrm{f}'$ and $\Gamma, \mathfrak{o}, \mathfrak{p}, \mathrm{f}$ denote the value group, valuation ring, valuation ideal and the residue field of K and k respectively. Note that $\Gamma = \{|x| : x \in k^*\}$ is a subgroup of

$\Gamma' = \{\|x\| : x \in K^*\}$ and f is a subfield of f′. One can define the numbers $e(K/k) = [\Gamma' : \Gamma] \leq +\infty$ and $f(K/k) = [\mathrm{f}' : \mathrm{f}] \leq +\infty$, which are called the *ramification index* and the *inertia degree* of the extension K/k respectively.

DEFINITION **1.8** *The extension K/k of normed fields is called unramified if $e(K/k) = 1$ and is called totally ramified if $f(K/k) = 1$.*

It can be seen that if $(L, \| \|^*)$ further extends $(K, \| \|)$, then $e(L/k) = e(L/K)e(K/k)$ and $f(L/k) = f(L/K)f(K/k)$. Hence the extension L/k is unramified (resp. totally ramified) if and only if so are the extensions K/k and L/K. From now on we will assume that the absolute value $| \, |$ is discrete. In this respect one can prove the following

PROPOSITION **1.4** *If K/k is a finite extension, then $\| \|$ is discrete and the inequality $e(K/k)f(K/k) \leq [K : k]$ holds.*

Proof. Suppose $s \leq e(K/k)$ and the elements $x_1, ..., x_s \in K$ are chosen in a way that the elements $\|x_i\| \in \Gamma', 1 \leq i \leq s$ are different modulo Γ. If $\sum_{i=1}^{s} c_i x_i = 0$ for some $c_1, ..., c_s \in k$, then $\max_{1 \leq i \leq s} \|c_i x_i\| = 0$, since all $\|c_i x_i\|$ are different. Therefore all the numbers c_i are equal to 0, so that $x_1, ..., x_s$ are linearly independent over k and $s \leq [K : k]$. Since s was arbitrary, we conclude that $e = e(K/k) \leq [K : k]$ which shows that $\Gamma' \subset \Gamma^{1/e}$ is a discrete group. Therefore the absolute value $\| \|$ is discrete. Further, we choose elements $y_1, ..., y_r \in \mathfrak{o}'$, such that their residue classes $\bar{y_1}, ..., \bar{y_r} \in \mathrm{f}'$ are linearly independent over f. Let $\pi \in K$ be an element for which $\|\pi\| = c < 1$ is the largest possible element of Γ', in other words π is a uniformizer with respect to the normalized valuation ν corresponding to the absolute value $\| \|$ (See Def-thm.1.2). We claim that the elements $\pi^i y_j, 0 \leq i \leq e-1, 1 \leq j \leq r$ are linearly independent over k. Assume the contrary that the relation

$$\sum_{i,j} c_{i,j} \pi^i y_j = \sum_{i=0}^{e-1} \left(\sum_{j=1}^{r} c_{i,j} y_j \right) \pi^i = 0 \qquad (*)$$

holds for some elements $c_{i,j} \in k$ not all of which are zero. Multiplying this relation by a suitable power π^m we may assume that the elements $c_{i,j}\pi^m$ are integral while not all of them are divisible by π. According to the choice of the elements $y_1, ..., y_r$ at least for one index i_0, $0 \leq i_0 \leq e-1$ the coefficient $\sum_{j=1}^{r} c_{i_0,j} y_j$ of π^{i_0} is nonzero. By what was said at the beginning of the proof, the latter assertion contradicts $(*)$, since $\|\pi^i\| = c^i, 0 \leq i \leq e-1$ are distinct modulo Γ. In the long run we get that $er \leq [K : k]$ and therefore $e(K/k)f(K/k) \leq [K : k]$, since $r \leq f(K/k)$ was arbitrary. □

Note that $e(\bar{k}/k) = f(\bar{k}/k) = 1$ by Proposition 1.2, but

$$[\bar{k} : k] \neq 1 = e(\bar{k}/k)f(\bar{k}/k)$$

whenever k fails to be complete. In case k is complete the situation changes due to the following

PROPOSITION **1.5** *If k is a complete discrete valuation field and K/k is an extension, then it is finite if and only if both numbers $e(K/k)$ and $f(K/k)$ are finite. If this is the case then $e(K/k)f(K/k) = [K : k]$.*

Proof. The necessity follows from Proposition 1.4. To prove the sufficiency we may assume that K is complete, since passing to the completion does not change either the numbers $e(K/k)$ and $f(K/k)$ nor the value group Γ' (See Proposition 1.2). Since $e = e(K/k)$ is finite, the subgroup Γ' is discrete, so that $\| \ \|$ is discrete. Note that in the course of the proof of Proposition 1.4 we constructed a linearly independent set $\pi'^i y_j \in K, 0 \leq i \leq e-1, 1 \leq j \leq r$ over k, where π' is a uniformizer of K and we may assume $r = f = f(K/k)$. Therefore we only need to show that it is in fact a k-basis. Indeed, let R be a complete representative system of $\mathfrak{o}$ modulo $\mathfrak{p}$. Then the system $R' = \left\{\sum_{i=1}^{f} a_i y_i : a_i \in R\right\}$ can be shown to be a complete representative system of $\mathfrak{o}'$ modulo $\mathfrak{p}'$. Let us fix a uniformizer $\pi \in k$. If ν is the normalized valuation corresponding to the absolute value $\| \ \|$, then $\nu(\pi) = e$ and $\nu(\pi') = 1$. For each integer n we divide n by e with reminder and write $n = em + i$ for uniquely determined integers m and $0 \leq i \leq e-1$. Therefore $\nu(\pi_n) = i + em = n$ if we set $\pi_n = \pi'^i \pi^m$ for all $n \in \mathbb{Z}$. According to Proposition 1.3 any $x \in K$ has a unique representation

$$x = \sum_{n \gg -\infty} a_n \pi_n = \sum_{m \gg -\infty, 0 \leq i < e} \left(\sum_{1 \leq j \leq f} c_{i,j,m} y_j \right) \pi'^i \pi^m = \sum_{i,j} c_{i,j} \pi'^i y_j,$$

where $c_{i,j} = \sum_{m \gg -\infty} c_{i,j,m} \pi^m \in \mathfrak{o}, c_{i,j,m} \in R$ and $a_n \in R'$. Note that we additionally proved that the system $\pi'^i y_j \in K, 0 \leq i \leq e-1, 1 \leq j \leq f$ is a free $\mathfrak{o}$-basis of $\mathfrak{o}'$. In the long run we get $[K : k] \leq [\bar{K} : k] = ef$ and therefore $ef \leq [K : k] \leq [\bar{K} : k] = ef$ by Proposition 1.4, so that $K = \bar{K}$ is complete and $[K : k] = ef$. □

1.1.4 Local fields

DEFINITION **1.9** *A normed field $(k, |\ |)$ with a non-trivial absolute value $|\ |$ is called a local field if it is a local compact topological field in the topology induced by $|\ |$.*

REMARK **1.2** *In case the absolute value is archimedean, by Theorem 1.7 one may assume that k is a dense subfield of either $\mathbb{R}$ or $\mathbb{C}$, the absolute value being equivalent to the usual one. Hence local compact archimedean fields can be identified with either $\mathbb{R}$ or $\mathbb{C}$ with the absolute value $|\ |^c$ for some $c > 0$.*

In what follows, by a local field we mean a non-archimedean local field, unless otherwise specified.

PROPOSITION **1.6** *For a non-archimedean normed field $(k, |\ |)$ with non-trivial absolute value $|\ |$ the following statements are equivalent*

1. *k is a local field.*
2. *The valuation ring $\mathfrak{o}$ is compact.*
3. *The absolute value $|\ |$ is discrete, k is complete and the residue field $\mathrm{f} = \mathfrak{o}/\mathfrak{p}$ is finite.*

Proof. 1)⇔2) Observe that if U is an open neighborhood of 0 for which $\overline{U}$ is compact, then for sufficiently large N the ball $B_N = \{x \in k : |x| < 1/N\}$ is contained in $\overline{U}$ and is therefore compact since it is closed at the same time. We choose an element $a \in k$ with $|a| > N$ and observe that $\mathfrak{o} \subset aB_N$ is compact, being a closed subset. The reverse inclusion is clear, since $\mathfrak{o}$ is both closed and open at the same time.
2)⇒3) If $\mathfrak{o}$ is compact, then $\mathfrak{p}$ is compact as well as a closed subset. Therefore the open cover $S_N = \{x \in k : |x| < 1 - 1/N\}, N > 1$ of $\mathfrak{p}$ must admit a finite sub-cover, so that $\mathfrak{p} = S_N$ for sufficiently large N, whence the discreteness of $|\ |$. Being a compact metric space, $\mathfrak{o}$ is complete and totally bounded, in particular for $\varepsilon = 1$ there is a finite ε-net for $\mathfrak{o}$, which is equivalent to saying that the residue field $\mathrm{f} = \mathfrak{o}/\mathfrak{p}$ is finite. To prove that k is complete observe that for any Cauchy sequence $(x_n)_{n\geq 1}$ either $x_n \to 0$ or $|x_n|$ is eventually constant so that for some m and N one has $x_n \in \mathfrak{p}^m, n \geq N$. Since $\mathfrak{p}^m$ is compact for any $m \in \mathbb{Z}$, the sequence $(x_n)_{n\geq N}$ must converge in it.
3)⇒2) Since $|\ |$ is discrete, the prime ideal $\mathfrak{p}$ is principal and therefore $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong \mathfrak{o}/\mathfrak{p}$ as $\mathfrak{o}$-modules for all $i \geq 1$. Hence for all $i \geq 1$, the quotient ring $\mathfrak{o}/\mathfrak{p}^i$ is finite, which amounts to saying that $\mathfrak{o}$ possesses a finite ε-net for any $\varepsilon > 0$ and is thus totally bounded metric space. On the other hand it is complete and is therefore compact. □

Observe that if k is a local field then its characteristic is either zero or equals the characteristic

of its residue field. Indeed, there is a ring homomorphism $\mathfrak{o} \to \mathfrak{o}/\mathfrak{p} = \mathrm{f}$, and therefore char(f) must divide char(k). We will treat each case separately but first we need the following

LEMMA **1.3** *In a local field k the equation $x^q = x$ has exactly q solutions, where $q = |\mathrm{f}|$ is the cardinality of the residue field* f *of k.*

Proof. Note that the polynomial $x^q - x$ has q different roots in f, namely all the elements of f. Corollary 1.5 of Hensel's lemma 1.2 allows us to uniquely lift all these roots to the ring $\mathfrak{o}$, so that we end up with q different roots of $x^q - x$ in $\mathfrak{o}$. Moreover, observe that the nonzero elements of them constitute a group μ_{q-1} of order $q-1$, which is cyclic being a finite subgroup of k^*. Since these elements project onto different elements of the residue field, we thus have found a complete representative system modulo $\mathfrak{p}$, closed with respect to multiplication. □

COROLLARY **1.8 (Teichmuller's decomposition)** *For a local field k there is an isomorphism of groups $k^* = \langle\pi\rangle \times \mu_{q-1} \times U_k^{(1)}$, where π is any prime element, μ_{q-1} is the subgroup of $q-1$-th roots of unity in $\mathfrak{o}_k$ and $U_k^{(1)} = 1 + \mathfrak{p}_k$ is the group of principal units.*

Proof. It is immediate that $k^* = \langle\pi\rangle \times U_k$. On the other hand the projection $\pi : \mathfrak{o}_k \to \mathrm{f}_k$ induces a homomorphism $\varphi : U_k \to \mathrm{f}_k^*$. From Lemma 1.3 it follows that there is a homomorphism $j : \mathrm{f}_k^* \to U_k$ such that $\varphi \circ j = \mathrm{Id}$. Hence $U_k = \ker\varphi \times \mathrm{Im}j = U_k^{(1)} \times \mu_{q-1}$. □

We are now ready to classify non-archimedean local fields. For each prime number p the fields $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ are local fields, so that their finite extensions are also local. It turns out that the converse is also true.

THEOREM **1.9** *Each local field k is a finite extension of either $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$, depending on whether char$(k) = 0$ or p. In any case the equality $p =$ char(*f*) is valid.*

Proof. If $\mathrm{char}(k) = 0$, k must contain $\mathbb{Q}$. Suppose $p = \mathrm{char}(\mathrm{f})$, then $p \cdot 1_k \in \mathfrak{p}$, so that the restriction of the absolute value $|\ |$ of k to $\mathbb{Q}$ is non-archimedean, satisfying $|p| < 1$. By Ostrowski's theorem 1.4 it is therefore equivalent to the p-adic absolute value $|\ |_p$ (See Examples 2,5). Since k is complete, it must contain the completion of $\mathbb{Q}$ with respect to $|\ |_p$, namely $\mathbb{Q}_p$ (See Example 5). We now focus on the extension $k/\mathbb{Q}_p$. Since both fields are discrete, their value groups Γ' and Γ are discrete, hence the ramification index $e = e(k/\mathbb{Q}_p) = [\Gamma' : \Gamma]$ is finite. On the other hand, since the residue field f is

finite, the inertia degree $f = f(k/\mathbb{Q}_p) = [\mathrm{f} : \mathbb{F}_p]$ must also be finite. Now Proposition 1.5 comes into play, showing that $[k : \mathbb{Q}_p]$ is finite.

Assume now that $\mathrm{char}(k) = \mathrm{char}(\mathrm{f}) = p > 0$. Let $q = p^f$ be the cardinality of the residue field f. Since we are working over a field of positive characteristic, the map $x \mapsto x^q$ is an endomorphism, so that the set $R = \{x \in k | x^q = x\}$ is a subfield of k, consisting of q elements (See Lemma 1.3). Let us fix a uniformizer $\pi \in k$. It follows from Proposition 1.3 that each element of k can be uniquely expressed in the form

$$\sum_{n \gg -\infty} a_n \pi^n, a_n \in R.$$

Moreover, since R is a field, the operations of summation and multiplication on these elements are carried out in exactly the same way as in the field $\mathbb{F}_q((t))$. Therefore the map $\varphi : k \to \mathbb{F}_q((t))$ which maps π to T and leaves the subfield $\mathbb{F}_q$ fixed, yields an isomorphism of these fields. It remains to note that $\mathbb{F}_q((t))$ is a finite extension of $\mathbb{F}_p((t))$ of degree f. □

Extensions of local fields.

Suppose $(k, |\ |)$ is a local field and K/k is a finite extension of fields. By Theorem 1.8 the absolute value $|\ |$ has a unique extension $\|\ \|$ to K and $(K, \|\ \|)$ is a complete field. From Propositions 1.4 and 1.5 it follows that $\|\ \|$ is discrete, both numbers $e(K/k)$ and $f(K/k)$ are finite and $[K : k] = e(K/k)f(K/k)$. Since $f(K/k) = [\mathrm{f}' : \mathrm{f}]$ is finite and the residue field f of k is finite, the residue field f′ of K is also finite. Collecting everything together we get, according to Proposition 1.6 that $(K, \|\ \|)$ is a local field. In the sequel by an extension of local fields we mean the aforementioned construction. It turns out that one can give a fairly clear overview of all finite unramified extensions of a given local field k.

THEOREM **1.10** *Let k be a local field with the residue field $\mathrm{f} \cong \mathbb{F}_q$. Then for each positive integer $n \geq 1$ there exists an unramified extension k' of k of degree n and k' is unique up to an isomorphism over k. The field k' is a splitting field of the polynomial $X^{q^n} - X$ over k and it is a cyclic extension of degree n. Let f' be the residue field of the local field k'. Then each element $\sigma \in Gal(k'/k)$ induces an automorphism σ' of f'/f and the map $\sigma \mapsto \sigma'$ induces an isomorphism*

$$\psi : Gal(k'/k) \xrightarrow{\sim} Gal(\mathrm{f}'/\mathrm{f}).$$

Proof. Existence. Let $n \geq 1$ be a fixed positive integer. Since f is a finite field, there exists a monic irreducible polynomial $g \in \mathrm{f}[x]$ of degree n. Let $P \in \mathfrak{o}[x]$ be a monic polynomial of degree n, which

lifts g, namely $\bar{P} = g$. Suppose w is a root of P, $k' = k(w)$ and $\mathfrak{o}', \mathfrak{p}', \mathrm{f}'$ denote the valuation ring, valuation ideal and the residue field of the local field k' respectively. Since P is monic, then $w \in \mathfrak{o}'$ and $g(\bar{w}) = 0$, which implies that $[\mathrm{f}(\bar{w}) : \mathrm{f}] = n$. Therefore

$$n = [\mathrm{f}(\bar{w}) : \mathrm{f}] \leq [\mathrm{f}' : \mathrm{f}] \leq [k' : k] \leq n$$

so that $[k' : k] = [\mathrm{f}' : \mathrm{f}] = n$ and the extension k'/k is unramified of degree n.

Uniqueness. Suppose k'/k is an arbitrary finite extension of local fields and $\mu_{q'-1} = \{x \in k' : x^{q'} = x\}$, where $q' = q^f = |\mathrm{f}'|, q = |\mathrm{f}|, f = f(k'/k)$ (See Lemma 1.3). Let $k_0 = k(\mu_{q'-1})$ be the intermediate field obtained by adjoining all the elements of $\mu_{q'-1}$ to k and let $\mathfrak{o}_0, \mathfrak{p}_0, \mathrm{f}_0$ denote the valuation ring, valuation ideal and the residue field of k_0. We claim that k_0/k is a cyclic unramified extension of degree $f = f(k'/k)$. Indeed, k_0 is a splitting field of the separable polynomial $P(x) = x^{q'} - x$ over k and is therefore a Galois extension. Further, each automorphism $\sigma \in \mathrm{Gal}(k_0/k)$ induces automorphisms of the ring $\mathfrak{o}_0$ and the ideal $\mathfrak{p}_0$ and hence of the residue field $\mathrm{f}_0 = \mathfrak{o}_0/\mathfrak{p}_0$, so that there is a natural homomorphism $\psi : \mathrm{Gal}(k_0/k) \to \mathrm{Gal}(\mathrm{f}_0/\mathrm{f}), \sigma \mapsto \sigma'$. Moreover, if $\sigma' = 1$, then σ leaves the elements of $\mu_{q'-1}$ fixed and is therefore trivial, since the elements of $\mu_{q'-1}$ constitute a complete residue system of $\mathfrak{o}_0$ modulo $\mathfrak{p}_0$. Hence the homomorphism ψ is injective and $[k_0 : k] \leq [\mathrm{f}_0 : \mathrm{f}] = f(k_0/k)$, from which we obtain that $[k_0 : k] = f(k_0/k)$, k_0/k is unramified and $\mathrm{Gal}(k_0/k) \cong \mathrm{Gal}(\mathrm{f}_0/\mathrm{f})$ is a cyclic group of order $f(k_0/k)$. On the other hand $[\mathrm{f}_0 : \mathrm{f}] = [\mathrm{f}' : \mathrm{f}]$ since the q' elements of $\mu_{q'-1}$ are distinct modulo $\mathfrak{p}_0$. The latter conclusion means exactly that $f(k_0/k) = f(k'/k)$. Assume now that k'/k is an unramified extension of degree n. Then $f(k'/k) = [k' : k] = n$ and thus $k_0 = k'$, namely k' is a splitting field of the polynomial $P(x) = x^{q^n} - x$ over k, which is determined up to an isomorphism over k, whence the uniqueness. □

REMARK **1.3** *The field k_0 constructed above is called the inertia field of the extension k'/k. It turns out to be the maximal unramified subfield of the extension k'/k. Indeed, let $k \subset k'' \subset k'$ be a subfield such that k''/k is unramified. From the proof of Theorem 1.10 we already know that k'' is the splitting field of the polynomial $X^{q''} - X$ over k, where $q'' = q^{f''}$ is the cardinality of the residue field of k'' and $f'' = f(k''/k)$ is the inertia degree. Since $f'' = f(k''/k)|f(k'/k) = f(k_0/k) = f_0$, it follows that $X^{q''} - X | X^{q^{f_0}} - X$ and therefore $k'' \subset k_0$, since k_0 is the splitting of $X^{q^{f_0}} - X$ over k.*

REMARK **1.4** *The element* $\mathrm{Frob}(k'/k) \in \mathrm{Gal}(k'/k)$ *corresponding via ψ to the Frobenius automorphism $\omega \to \omega^q$ of* $\mathrm{Gal}(\mathrm{f}'/\mathrm{f})$ *is called the Frobenius automorphism of the unramified extension k'/k. It is*

uniquely determined by the condition $\mathrm{Frob}(k'/k)(a) \equiv a^q (mod\ \mathfrak{p}')$, *for all* $a \in \mathfrak{o}'$.

We now switch to totally ramified extensions. Recall that the extension K/k of normed fields is called totally ramified if $f(K/k) = 1$. Let k be a local field, $\mathfrak{o}, \mathfrak{p}$ and f be the valuation ring valuation ideal and the residue field of k respectively.

DEFINITION **1.10** *The polynomial* $P(x) = \sum_{i=0}^{n} a_i x^i \in \mathfrak{o}[x]$ *is called an Eisensteinian if* $a_n \notin \mathfrak{p}, a_i \in \mathfrak{p}, 0 \leq i \leq n-1$ *and* $a_0 \notin \mathfrak{p}^2$.

LEMMA **1.4** *Any Eisensteinian* P *is an irreducible polynomial in* $k[x]$.

Proof. Since $\mathfrak{o}$ is a PID and thus a UFD, Gauss's lemma is applicable and it suffices to show that P cannot be written as a product of two non-constant polynomials in the ring $\mathfrak{o}[x]$. Assume the contrary that the relation $P = gh$ holds for some non-constant polynomials $g, h \in \mathfrak{o}[x]$. Modulo $\mathfrak{p}$ this gives $\bar{a_n} X^n = \bar{g}\bar{h}$ in the ring f$[x]$, so that $\bar{g} = ax^t$ and $\bar{h} = bx^s$ for some $s, t > 0, s + t = n$ and $a, b \in \mathrm{f}^*$. Therefore $g(0), h(0) \in \mathfrak{p}$ and $P(0) \in \mathfrak{p}^2$, which contradicts Definition 1.10. □

THEOREM **1.11** *If* k *is a local field and* $P \in \mathfrak{o}[x]$ *is an Eisensteinian of degree* n*, then adjoining a root of* P *to* k *yields a totally ramified extension of degree* n *in which the adjoined element is a uniformizer. Conversely, if* k'/k *is a totally ramified extension of degree* n *and* $\Pi \in k'$ *is a prime element (uniformizer), then the minimal polynomial of* Π *is an Eisensteinian of degree* n *and* $k' = k(\Pi)$.

Proof. Let α be a root of P and $k' = k(\alpha)$. Since P is irreducible in $k[x]$, the extension k'/k has degree n. If $|\ |$ and $\|\ \|$denote the corresponding absolute values of k and k' then according to Theorem 1.8 $\|\alpha\| = |N_{k'/k}(\alpha)|^{1/n}$. Since P is an Eisensteinian, $N_{k'/k}(\alpha) = P(0)$ is a prime element of k and therefore $\|\alpha\| = c^{1/n}$, where $c < 1$ is the generator of the value group Γ of $|\ |$. If Γ' denotes the corresponding value group of $\|\ \|$, then it becomes clear that $e(k'/k) = [\Gamma' : \Gamma] \geq n$ and that α is a prime element of k', as well as $f(k'/k) = 1$ according to the equality $e(k'/k)f(k'/k) = n$.
Conversely, let $P(x) = \sum_{i=0}^{m-1} a_i x^i + x^m \in k[x]$ be the minimal polynomial of the prime element $\Pi \in k'$. Then again by Theorem 1.8 we obtain $c'^m = |N_{k'/k}(\Pi)|^{m/n} = \left|a_0^{n/m}\right|^{m/n} = |a_0| \in \Gamma$, where $c' < 1$ is the generator of the group Γ'. Since $f(k'/k) = 1$ then $[\Gamma' : \Gamma] = e(k'/k) = n$ and therefore $m = n$. Hence $|a_0| = c'^n = c$, showing that $a_0 \in \mathfrak{p} \setminus \mathfrak{p}^2$ is a prime element. Since $|a_0| < 1$ we get by Corollary 1.6 that $P \in \mathfrak{o}[x]$. If there is some index $0 \leq i \leq n-1$ such that $a_i \notin \mathfrak{p}$ then the reduction $\bar{P}$ of P

modulo $\mathfrak{p}$ can be written as $\bar{P} = x^t h$ for some $0 < t < n$ and a polynomial $h \in \mathfrak{f}[x]$ with $h(0) \neq 0$. This conclusion contradicts Hensel's Lemma 1.2, so that all $a_i \in \mathfrak{p}, 0 \leq i \leq n-1$ and P is an Eisensteinian. □

Galois extensions.

Assume that K/k is a finite Galois extension of local fields with Galois group $G = G(K/k)$. For $s \geq -1$ define $G_s = G_s(K/k) = \{g \in G : |x^g - x| \leq c^{s+1} \text{ for all } x \in \mathcal{O}_K\}$, where $c < 1$ is the generator of the value group Γ_K of K and $\mathcal{O}_K$ is the valuation ring of K. By a quick observation we may convince ourselves that $G_s \trianglelefteq G$ for all $s \geq -1$. Note that there is a natural homomorphism $\psi : G \to \mathrm{Gal}(\mathfrak{f}_K/\mathfrak{f}_k)$ (See Theorem 1.10), where $\mathfrak{f}_K$ and $\mathfrak{f}_k$ denote the corresponding residue fields. On the one hand one has $\ker(\psi) = \{g \in G : |x^g - x| < 1 \text{ for all } x \in \mathcal{O}_K\} = G_0$. On the other hand, if k_0 denotes the inertia field of the extension K/k (See Remark 1.3), then as was proved in Theorem 1.10, $k_0 = k(\mu_{q_K-1})$, where $\mu_{q_K-1} = \{x \in K : x^{q_K} = x\}$ is a complete residue system modulo $\mathfrak{p}_K$ and therefore $\ker(\psi)$ coincides with the subgroup of G, leaving k_0 fixed. In other words we have proved that $G_0 = \mathrm{Gal}(K/k_0)$. Furthermore, we have the induced monomorphism $\bar{\psi} : \mathrm{Gal}(k_0/k) \to \mathrm{Gal}(\mathfrak{f}_K/\mathfrak{f}_k)$ which is an isomorphism, since both groups have order $f = f(K/k)$. This observation proves the surjectivity of ψ. Moreover, one can prove the following

THEOREM **1.12** *If π_K is a fixed prime element of K then for all integers $n \geq 0$ the map*

$$G_n/G_{n+1} \to U_K^{(n)}/U_K^{(n+1)}, \sigma \mapsto \frac{\sigma(\pi_K)}{\pi_K}$$

is an injective homomorphism, which is independent of the prime element π_K. Here $U_K^{(n)}$ denotes the n-th group of principal units of K, i.e. $U_K^{(0)} = \mathcal{O}_K^*$ and $U_K^{(n)} = 1 + \mathfrak{p}_K^n$, for $n \geq 1$.

Proof. Suppose $n \geq 0$ is fixed. One can check readily that the map $\varphi_n : G_n \to U_K^{(n)}/U_K^{(n+1)}$, induced by the map $\sigma \mapsto \frac{\sigma(\pi_K)}{\pi_K}$ is a well defined group homomorphism. Indeed, if π'_K is another prime element, then $\pi'_K = \pi_K u$ for some unit u and $\frac{\sigma(\pi'_K)}{\pi'_K} = \frac{\sigma(\pi_K)}{\pi_K}\frac{\sigma(u)}{u}$. Since $\frac{\sigma(u)}{u} = 1 + \frac{\sigma(u)-u}{u} \in U_K^{(n+1)}$ for $\sigma \in G_n$, we obtain that the class $\frac{\sigma(\pi_K)}{\pi_K}$ modulo $U_K^{(n+1)}$ is independent of the choice of π_K. Moreover, if $\tau \in G_n$ is another element, then for $u = \frac{\tau(\pi_K)}{\pi_K}$ one has

$$\frac{\sigma\tau(\pi_K)}{\pi_K} = \frac{\sigma(\tau(\pi_K))}{\tau(\pi_K)}\frac{\tau(\pi_K)}{\pi_K} = \frac{\sigma(\pi_K)}{\pi_K}\frac{\tau(\pi_K)}{\pi_K}\frac{\sigma(u)}{u} \equiv \frac{\sigma(\pi_K)}{\pi_K}\frac{\tau(\pi_K)}{\pi_K} \left(\mathrm{mod}\ U_K^{(n+1)}\right),$$

showing that φ_n is a homomorphism. It remains to prove the injectivity of φ_n. To do this we observe that $G_n(K/k) = G_n(K/k_0)$ for $n \geq 0$, which allows us to assume that the extension K/k is totally

ramified. According to Theorem 1.11, $K = k(\pi_K)$, from which by simple observations we obtain that $\mathcal{O}_K = \mathcal{O}_k[\pi_K]$. Now suppose that $\frac{\sigma(\pi_K)}{\pi_K} \in U_K^{(n+1)}$. Then $\sigma(\pi_K) - \pi_K \in \mathfrak{p}_K^{n+2}$ and therefore $\sigma(a) - a \in \mathfrak{p}_K^{n+2}$ for all $a \in \mathcal{O}_K$, since each such a is expressible as a polynomial in π_K with coefficients from $\mathcal{O}_k$. This proves the injectivity of φ_n. □

Since for $n \geq 1$ the group $U_K^{(n)}/U_K^{(n+1)} \cong \mathrm{f}_K^+$ is an elementary abelian p-group, then by Theorem 1.12, each $G_n/G_{n+1}, n \geq 1$ is an elementary abelian p-group. Besides that for

$$c^n < \max_{\sigma \in G, \sigma \neq 1} \{|\pi_K^\sigma - \pi_K|\}$$

the group G_n is trivial, hence all $G_n, n \geq 1$ are p-groups. Furthermore, the group G_0/G_1 is cyclic of order coprime to p, as a subgroup of the cyclic group $U_K^{(0)}/U_K^{(1)} \cong \mathrm{f}_K^*$ of order $q_K - 1$ (See Def-thm. 1.2). Note that since G_1 is a normal p-subgroup of G_0 of index coprime to p, it is precisely the Sylow p-subgroup of G_0. On the other hand

$$G/G_0 \cong \mathrm{Gal}(\mathrm{f}_K/\mathrm{f}_k) \cong \mathbb{Z}/f\mathbb{Z}$$

for $f = f(K/k)$ as was proved earlier. Collecting everything together we get that G is a solvable group. More precisely we proved the following

COROLLARY **1.9** *Any finite Galois extension of a local field has a solvable Galois group.*

1.2 Formal groups

1.2.1 Invariant differential and formal logarithm

From now on R is assumed to be a commutative ring with unity.

DEFINITION **1.11** *A one dimensional formal group law (or formal group) over R is a power series $F = F(x, y) \in R[[x, y]]$ satisfying the following conditions*

1. $F(x, 0) = x, F(0, y) = y$
2. $F(F(x, y), z) = F(x, F(y, z))$

The formal group is called commutative if in addition the condition $F(x, y) = F(y, x)$ is satisfied. To indicate that F is a formal group defined over a ring R we will use the notation F/R.

REMARK **1.5** *It can be proved that the first condition can be replaced with the condition* $F(x,y) \equiv x+y(\text{mod } \deg 2)$.

Example 1. The *additive* formal group $\mathbb{G}_a$ given by $\mathbb{G}_a(x,y) = x+y$.

Example 2. The *multiplicative* formal group $\mathbb{G}_m$ given by $\mathbb{G}_m(x,y) = x+y+xy$.

Example 3. For each $c \in R$ one can define a formal group F_c according to the rule

$$F_c(x,y) = x+y+cxy.$$

It turns out that these formal groups constitute a complete list of formal groups, whose underlying formal group law is a polynomial. Inspired by this fact they are called *polynomial formal groups.*

LEMMA **1.5** *If* F *is a formal group, then there exists a unique power series* $i(x) \in R[[x]]$ *which satisfies* $F(x,i(x)) = 0$.

Proof. We inductively construct a sequence of polynomials $i_n(x) \in R[x], n \geq 1$ such that $i_{n+1}(x) \equiv i_n(x)(\text{mod } x^{n+1})$ and $F(x,i_n(x)) \equiv 0(\text{mod } x^{n+1})$ for all n. We set $i_1(x) = x$ and suppose that $i_n(x)$ has already been constructed, so that $F(x,i_n(x)) \equiv c_n x^{n+1}(\text{mod } x^{n+2})$. We claim that $i_{n+1}(x) = i_n(x) - c_n x^{n+1}$ is the only possible candidate. Indeed, since $F(x,0) = x$ and $F(0,y) = y$, then $F(x,y) = x+y+\sum_{i,j\geq 1} c_{i,j}x^i y^j$ and therefore

$$F(x,i_{n+1}(x)) \equiv F(x,i_n(x)) - c_n x^{n+1} \equiv 0(\text{mod } x^{n+2}).$$

It remains to set $i(x) = \lim\limits_{n\to\infty} i_n(x) \in R[[x]]$ to complete the proof. The uniqueness follows from the above constructions. □

We recall that for a power series $h \in R[[x]]$ with $h(0) = 0$ there exists an inverse series with respect to composition if and only if its first coefficient is invertible.

DEFINITION-THEOREM **1.3** *A homomorphism of formal groups* $F, G/R$ *is a power series* $h \in R[[x]]$ *without constant term, satisfying the relation* $h(F(x,y)) = G(f(x),f(y))$. *An invertible homomorphism is called an isomorphism. If* G *is commutative, then the set of all homomorphisms* $\text{Hom}_R(F,G)$ *from* F *to* G *is an abelian group with respect to the operation* $f \underset{G}{+} g = G(f,g)$. *The additive 0 is the identical zero power series and the additive inverse of* f *is the power series* $G(f, f\circ i)$, *where* i

is the unique series mentioned in Lemma 1.5. Moreover, the abelian group $\mathrm{End}_R(G) := \mathrm{Hom}_R(G, G)$ *becomes a ring if we introduce a new operation of multiplication by setting* $f * g = f \circ g$*, where the latter is the usual composition of series.*

Proof. An easy check. □

An expression of the form $\omega = P(t)dt$ for $P \in R[[t]]$ is called an invariant differential of a formal group F/R if it satisfies the invariance condition $\omega \circ F(t, s) = \omega$, or equivalently the condition $P(F(t, s))F_x(t, s) = P(t)$. An invariant differential ω is called normalized if $P(0) = 1$. One can prove the following

LEMMA **1.6** *For any formal group* F *there exists a unique normalized invariant differential which can be explicitly given in the form* $\omega_F = F_x^{-1}(0, t)dt$*. Any other invariant differential* ω *is a multiple of the normalized one, namely* $\omega = a\omega_F$ *for an appropriate* $a \in R$*.*

Proof. See [30, Chapter 4, Prop. 4.2]. □

DEFINITION **1.12** *Let* R *be a ring of characteristic zero,* F/R *be a formal group,* $A = R \otimes \mathbb{Q}$ *and*

$$\omega_F(t) = (1 + c_1 t + c_2 t^2 + ...)dt \in R[[t]]$$

be the normalized invariant differential of F*. The formal logarithm* $\log_F$ *of* F *is defined to be the power series*

$$\log_F(t) = \int \omega(t)dt = t + \frac{c_1}{2}t^2 + ... \in A[[t]]$$

The formal exponential of F/R *is the unique power series* $\exp_F(t) \in A[[t]]$ *satisfying*

$$\exp_F \circ \log_F(t) = \log_F \circ \exp_F(t) = t$$

Example 4. For the additive formal group $F = \mathbb{G}_a$ the normalized invariant differential, the formal logarithm and the formal exponential are $\omega_F(t) = dt$ and $\log_F(t) = t$ and $\exp_F(t) = t$ respectively, while for the multiplicative formal group $F = \mathbb{G}_m$ one has $\omega_F(t) = \frac{1}{1+t}dt$,
$\log_F(t) = t - \frac{t^2}{2} + \frac{t^3}{3} - ... = \log(1 + t)$ and $\exp_F(t) = t + \frac{t^2}{2!} + \frac{t^3}{3!} + ... = e^t - 1$.

PROPOSITION **1.7** *If* F/R *is a formal group, then the identity*

$$\log_F(F(x, y)) = \log_F(x) + \log_F(y)$$

holds in the ring $A[[x,y]]$. *The power series* $\log_F$ *sets up an isomorphism* $F \cong \mathbb{G}_a$ *of formal groups over the ring* A.

Proof. Integrating the identity $\omega(F(t,s)) = \omega(t)$ with respect to t yields $\log_F(F(t,s)) = \log_F(t) + f(s)$ for some constant of integration $f \in A[[x]]$. Substituting $t = 0$ we get $f(s) = \log_F(s)$. Therefore $\log_F$ is a homomorphism from F to $\mathbb{G}_a$. It is in fact an isomorphism, being an invertible power series in $A[[x]]$. □

If R is torsion free as an abelian group, or equivalently if the natural map $R \to A$ given by $r \mapsto r \otimes 1$ is an injective ring homomorphism, then one treats the identity

$$F(x,y) = (\log_F)^{-1}(\log_F(x) + \log_F(y))$$

as an equality of power series in $R[[x,y]]$ thereby deducing that F is commutative. In this respect we have the following

THEOREM **1.13** *There exist non-commutative formal groups over the ring* R *if and only if there is a nonzero* $a \in R$ *and integers* $m, n \geq 1$ *such that* $na = a^m = 0$.

Proof. See [21, Therem 6.1] □

Counterexample. Suppose $R = \mathbb{F}_p[t]/(t^p)$ and $F(x,y) = x + y + \bar{t}xy^p$. Then F/R is a formal group, but as can be seen it is not commutative. The reason is that $p\bar{t} = \bar{t}^p = 0$ in the ring R.

Formal groups are widely used to produce abstract groups in the following sense. Suppose we are given a local field K of characteristic zero with valuation ring $\mathfrak{o}_K$ and maximal ideal $\mathfrak{p}_K$. If $F/\mathfrak{o}_K$ is a commutative formal group, then for any elements $a, b \in \mathfrak{p}_K$, the series $F(a,b)$ converges to an element of $\mathfrak{p}_K$ so that one can define a new binary operation on $\mathfrak{p}_K$ by declaring $a \underset{F}{+} b = F(a,b)$. Now the axioms of a formal group guarantee that the structure thus obtained is an abelian group, which we will denote by $F(\mathfrak{p}_K)$ in what follows. If we treat the formal logarithm $\log_F$ as a power series with coefficients from the field K, then the following theorem holds

THEOREM **1.14** *The power series* $\log_F$ *induces a homomorphism* $\log_F : F(\mathfrak{p}_K) \to K^+$. *Moreover, for* $m > \frac{e}{p-1}$ *it maps the subgroup* $F(\mathfrak{p}_K^m)$ *isomorphically onto the subgroup* $\mathfrak{p}_K^m$ *of* K, *where* $e = e(K/\mathbb{Q}_p)$ *is the absolute ramification degree and* $p = \mathrm{char}(\mathrm{f}_K)$ *is the characteristic of the residue field of* K.

Proof. (Sketch) Since $\log_F(x) = \sum_{n\geq 1} \frac{a_n}{n} x^n$ for certain elements $a_n \in \mathfrak{o}_K, n \geq 1$, the series $\log_F(\alpha)$ converges to an element of K for each $\alpha \in \mathfrak{p}_K$. Indeed, if ν_K denotes the normalized valuation of K, then for any $\alpha \in \mathfrak{p}_K$,

$$\nu_K\left(\frac{a_n}{n}\alpha^n\right) \geq n\nu_K(\alpha) - \nu_K(n) \geq n - \log_p(n) \to \infty,$$

whence the convergence of the required series. Furthermore, Proposition 1.7 shows that the map $\log_F : F(\mathfrak{p}_K) \to K, \alpha \mapsto \log_F(\alpha)$ is in fact a homomorphism of groups. The proof of the second assertion is a little bit tricky and requires some work to do. This time we choose a rather small neighborhood $\mathfrak{p}_K^m$ of 0 on which the power series $\exp_F$ converges. Luckily, this is always possible to do since the denominators of $\exp_F$ grow not too fast. In fact, it can be proved that $\exp_F(x) = \sum_{n\geq 1} \frac{b_n}{n!} x^n$, for some $b_n \in \mathfrak{o}_K, n \geq 1$. Using the famous inequality $\nu_p(n!) = \sum_{k\geq 1} \left[\frac{n}{p^k}\right] \leq \frac{n-1}{p-1}$ we get

$$\nu_K\left(\frac{a_n}{n!}\alpha^n\right) \geq n\nu_K(\alpha) - e\nu_p(n!) \geq \nu_K(\alpha) + (n-1)\nu_K(\alpha) - e\frac{n-1}{p-1} =$$

$$= \nu_K(\alpha) + (n-1)\left(\nu_K(\alpha) - \frac{e}{p-1}\right) \geq m + (n-1)\left(m - \frac{e}{p-1}\right),$$

for $\alpha \in \mathfrak{p}_K^m$. Therefore for $m > \frac{e}{p-1}$ and $\alpha \in \mathfrak{p}_K^m$ the series $\exp_F(a)$ converges to an element of $\mathfrak{p}_K^m$, so that $\exp_F : \mathfrak{p}_K^m \to F(\mathfrak{p}_K^m)$ and $\log_F : F(\mathfrak{p}_K^m) \to \mathfrak{p}_K^m$ are mutually inverse homomorphisms and thereby isomorphisms. □

1.2.2 Lubin-Tate formal groups.

Let K be a local field, π be a fixed prime element in it and q be the cardinality of the residue field. Consider the set $\mathscr{E}_\pi$ of power series $e \in \mathcal{O}_K[[X]]$, satisfying the conditions

1. $e(X) \equiv \pi X (\text{mod deg } 2)$
2. $e(X) \equiv X^q (\text{mod } \pi)$

THEOREM **1.15** *For each $e \in \mathscr{E}_\pi$ there is a unique formal group $F = F_e \in \mathcal{O}_K[[X, Y]]$, for which e is an endomorphism. Moreover there is an injective ring homomorphism $\mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_K}(F)$, $a \mapsto [a]_F(X)$ such that $[a]_F(X) \equiv aX (mod\ deg\ 2)$ for each $a \in \mathcal{O}_K$ and $[\pi]_F = e$. Besides, it turns out that for any two power series e and e' in $\mathscr{E}_\pi$ the corresponding formal groups F_e and $F_{e'}$ are isomorphic.*

Proof. See [20, Chapter 3, §6, Thm. 6.7]. □

The formal groups $F = F_e$ mentioned in the theorem are called Lubin-Tate formal groups. Since for all $e \in \mathscr{E}_\pi$ they are isomorphic, one may speak of the Lubin-Tate formal group corresponding to the given prime π. Lubin-Tate formal groups play a crucial role in class field theory and are used to describe the maximal abelian extension of a given local field K. Namely, suppose K^{alg} is a fixed algebraic closure of K and K^{ab} is the compositum of all finite abelian subextensions of K^{alg}/K. Let $F/\mathcal{O}_K$ be the Lubin-Tate formal group for the prime element $\pi \in K$. For each $n \geq 1$ we introduce a field $K_{\pi,n} = K(F(n))$, called the field of π^n-division points, where $F(n) = \{x \in \mathfrak{p}_{K^{\text{alg}}} : [\pi]_F^n(x) = 0\}$. It turns out that all the extensions $K_{\pi,n}/K$ are totally ramified Galois extensions with Galois group $G(K_{\pi,n}/K) \cong U_K/U_K^{(n)}$. Furthermore, let K^{nr} be the maximal unramified subextension of K^{alg}/K, namely K^{nr} is the compositum of all finite unramified extensions of K. Since all finite unramified extensions are cyclic (See Theorem 1.10), the extension K^{nr} is abelian. Moreover, it turns out that

$$K^{\text{ab}} = K^{\text{nr}} K_\pi,$$

where $K_\pi = \bigcup_{n=1}^{\infty} K_{\pi,n}$

Example 5. Let p be a rational prime number. The multiplicative formal group $\mathbb{G}_m$ defined earlier is the Lubin-Tate formal group over the ring $\mathbb{Z}_p$ of p-adic integers corresponding to the prime $p \in \mathbb{Z}_p$. Indeed, it can be verified that the power series $e(X) = (1+X)^p - 1$ belongs to $\mathscr{E}_p$ defined previously and is an endomorphism of $\mathbb{G}_m$ at the same time. The conclusion follows according to Theorem 1.15.

1.2.3 Honda formal groups.

Suppose K is a discrete valuation field of characteristic 0, possessing an automorphism φ which satisfies the condition $a^\varphi \equiv a^q (\text{mod } \pi)$ [1] for all $a \in \mathcal{O}_K$, where π is a fixed prime element of K and q is a power of the characteristic of the residue field, which is assumed to be positive. Consider the non commutative ring $\mathcal{O}_{K,\varphi}[[T]]$ of power series in which the multiplication is carried out according to the rules $T^i T^j = T^{i+j}$ and $Ta = a^\varphi T$ for all $i, j \geq 0$, $a \in \mathcal{O}_K$. One can prove that $\mathcal{O}_{K,\varphi}[[T]]$ is a division ring. Let $K[[x]]_0$ be the ideal of all polynomials in $K[[x]]$ vanishing at 0. For each $u \in \mathcal{O}_{K,\varphi}[[T]], u(T) = \sum_{i\geq 0} a_i T^i$ and $f \in K[[X]]_0$ we define the power series $u * f \in K[[X]]_0$ according to the rule

$$u * f = \sum_i a_i f^{\varphi^i}\left(X^{q^i}\right).$$

[1] In particular if k is a finite extension of $\mathbb{Q}_p$, then any unramified extension K/k (finite or infinite) will satisfy the condition with $\varphi = \text{Frob}(K/k)$ (See Remark 1.4) and $q = |\mathfrak{f}_k|$, the cardinality of the residue field of k.

An element $u \in \mathcal{O}_{K,\varphi}[[T]]$ is called special iff it starts with π.

THEOREM **1.16** *If $f \in K[[X]]_0$ is an invertible power series and $u * f \equiv 0 (mod\ \pi)$ for some special element u, then the formal group defined by the rule $F_f(X,Y) = f^{-1}(f(X) + f(Y))$ has all its coefficients in the ring $\mathcal{O}_K$. Moreover, if $g \in K[[X]]_0$ is another such element with $u * g \equiv 0 (mod\ \pi)$, then the power series $\theta = g^{-1} \circ f$ belongs to $\mathcal{O}_K[[X]]$ and sets up an isomorphism $\theta : F_f \to F_g$. For each special element u there is a canonical formal group F_u associated with u, namely the one which arises from $h = (u^{-1}\pi) * X$, where u^{-1} is the inverse of u in $K_\varphi[[T]]$.*

For the proof of this theorem we refer to [12, §2, Thm.2]. The formal group F_f constructed above is called Honda formal group. Observe that $f = f'(0)\log_{F_f}$ and $F_f = F_{\log_F}$. We say that the Honda formal group F is of type u if u is a special element and $u * \log_F \equiv 0 (\text{mod } \pi)$. It turns out that if $v * \log_F \equiv 0 (\text{mod } \pi)$ for some $v \in \mathcal{O}_{K,\varphi}[[T]]$, then there exists an element $t \in \mathcal{O}_{K,\varphi}[[T]]$ such that $v = tu$ and therefore all types of F constitute a class of left associate elements in the ring $\mathcal{O}_{K,\varphi}[[T]]$. In case K is complete one can deduce using the Weierstrass preparation lemma for the ring $\mathcal{O}_{K,\varphi}[[T]]$ that among all types of a Honda formal group there exists a unique canonical type $\tilde{u}$ of the form $\tilde{u} = \pi - \sum_{i=1}^{h} a_i T^i$, where $a_1, ..., a_{h-1}$ are divisible by π and a_h is a unit. The number $h \leq +\infty$ is called the height of the Honda formal group F and it is infinite if and only if $\log_F \in \mathcal{O}_K[[X]]$ or equivalently if $F \approx \mathbb{G}_a$ [2]. In what follows h is assumed to be finite.

THEOREM **1.17** *For any invertible power series $f, g \in K[[X]]_0$ one has $\text{Hom}_{\mathcal{O}_K}(F_f, G_g) = \{g^{-1}(cf) : c \in \mathcal{O}_K,\ \exists t\ s.t.\ vc = tu\}$. Moreover, if K is complete and u, v are canonical, then $\text{Hom}_{\mathcal{O}_K}(F_f, G_g) = \{g^{-1}(cf) : c \in \mathcal{O}_K\ s.t.\ vc = cu\}$. In particular, Honda formal groups $F, G/\mathcal{O}_K$ are strongly isomorphic if and only if their canonical types coincide.*

Proof. See Theorem 3 and Proposition 3.6 in [12]. □

Honda formal groups form a fairly wide class due to the following

THEOREM **1.18** *Let K be a discrete valuation field of characteristic zero, whose residue field has positive characteristic p. Assume that the valuation of K is unramified [3], that is p is a prime element*

[2] The notation $F \approx G$ for formal groups means that they are strongly isomorphic, that is there exists an isomorphism $\theta : F \to G$ such that $\theta'(0) = 1$

[3] In particular any unramified extension of $\mathbb{Q}_p$ will work

of $\mathcal{O}_K$. *Then for each formal group* $F/\mathcal{O}_K$ *there exists a special element* $u = u_F \in \mathcal{O}_{K,\varphi}[[T]]$ *such that* $u * \log_F \equiv 0 (\text{mod } p)$, *that is* F *is a Honda formal group of type* u.

Proof. See [12, §3, Thm.4]. □

Suppose k is a local field of characteristic zero and K/k is a finite unramified extension with Frobenius automorphism $\varphi = \text{Frob}(K/k)$. Let π be a prime element of k. Theorem 1.15 shows that a Lubin-Tate formal group is recovered by a single endomorphism, satisfying certain conditions. It turns out that something similar is valid in the case of Honda formal groups. In these respect it is important to note O.V.Demchenko's classification theorems (See [13]).

THEOREM **1.19** *For given Honda formal group* F *of canonical type* $\tilde{u} = \pi - \sum_{i=1}^{h} a_i T^i \in \mathcal{O}_{K,\varphi}[[T]]$ *there exists a Honda formal group* $\mathscr{A}F$ *and a distinguished homomorphism* $f_F \in \text{Hom}_{\mathcal{O}_K}(F, \mathscr{A}F)$ *such that* $f_F(x) \equiv \pi x (\text{mod } \deg 2)$ *and* $f_F(X) \equiv x^{q^h} (\text{mod } \pi)$.

THEOREM **1.20** *Suppose* $\tilde{u} = \pi - \sum_{i=1}^{h} a_i T^i \mathcal{O}_{K,\varphi}[[T]]$ *is a canonical element and* $f \in \mathcal{O}_K[[x]]$ *is a power series satisfying the conditions* $f(x) \equiv \pi x (\text{mod } \deg 2)$ *and* $f(X) \equiv x^{q^h} (\text{mod } \pi)$. *Then there exists a unique Honda formal group* F *of type* $\tilde{u}$ *such that* $f = f_F$ *is the distinguished homomorphism from* F *to* $\mathscr{A}F$.

We would like to conclude this section by the following

REMARK **1.6** *If we let* $\tilde{u} = \pi - T$, *then the corresponding Honda formal group mentioned in Theorem 1.20 will be precisely the Lubin-Tate formal group* F *corresponding to the prime* π. *Moreover,* $\mathscr{A}F = F$ *and* $f_F = [\pi]_F \in \text{End}_{\mathcal{O}_K}(F)$ *in this case.*

1.3 G-modules

Let G be an abstract group.

DEFINITION **1.13** *A* G*-module is an abelian group* A *together with a homomorphism* $\rho : G \to \text{Aut}(A)$.

From now on for each $g \in G$ and $a \in A$ we will use the notation ga instead of $\rho(g)(a)$.

Example 1. Any abelian group A is automatically a G-module, if we let the group G act on A trivially, namely if ρ is the trivial homomorphism.

Example 2. Suppose L/K is a Galois extension of fields with Galois group G. Then both abelian groups L^* and L^+ are G-modules, the action of G on them being given in a natural way.

DEFINITION **1.14** *A subset B of the G-module A is called a G-submodule, if B is a subgroup of A and $g \cdot b \in B$ for all $g \in G$ and $b \in B$. Ones B is a G-submodule of A, it is possible to define the quotient G-module A/B naturally by declaring $g[a] = [ga]$. If A and B are G-modules, then the map $f : A \to B$ is called a G-homomorphism if f is a group homomorphism and preserves the action of G, that is $f(ga) = gf(a)$ for all $g \in G$ and $a \in A$.*

An attentive reader should immediately spot that the notion of a G-module is in fact the same as the notion of the usual module over the group ring $\mathbb{Z}[G]$, namely the corresponding categories could be identified. We will denote this category by **G-Mod**. To each G module one can canonically attach an abelian group A^G called the fixed module , which is the set of all points in A, fixed by the whole group G. Namely,

$$A^G = \{a \in A | ga = a \text{ for all } g \in G\}$$

It turns out that the correspondence $A \to A^G$ is a left exact functor **G-Mod** $\to$ **Ab**. The right adjoint functors of this functor exist and unique up to canonical equivalence (See [23, Chapter 4, Thm.1.1]). They are called the cohomology group functors of A and are denoted by $H^n, n = 1, 2....$ More precisely, each short exact sequence of G-modules

$$0 \to A \to B \to C \to 0$$

induces a long exact sequence of abelian groups

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to ...$$

The cohomology group $H^1(G, A)$ can be defined more explicitly.

DEFINITION **1.15** *Let $Z^1(G, A)$ be the subgroup of functions $f : G \to A$, satisfying the condition $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$ and let $B^1(G, A)$ be the subgroup of functions $f_a : G \to A, a \in A$ such that $f_a(\sigma) = \sigma a - a$ for all $\sigma \in G$.*

It can be proved that $H^1(G, A) = Z^1(G, A)/B^1(G, A)$ (See [20, Chapter1, Prop. 3.1]). For further purposes we will also need the groups $H^i(G, A)$ for $i = 0, -1$. Assume that G is a finite group.

DEFINITION **1.16** *Let A be a G-module. For each $a \in A$ define the norm of a by $N_G(a) = \sum_{\sigma \in G} \sigma a$. Then the set $N_G(A) = \{N_G(a) | a \in A\}$ is a subgroup of A^G, the quotient group $A^G/N_G(A)$ is called the norm residue group and is denoted by $H^0(G, A)$. Further, let ${}_{N_G}A = \{a \in A | N_G(a) = 0\}$ and let $I_G(A)$ be the subgroup of ${}_{N_G}A$ generated by all elements of the form $\sigma a - a$. The group ${}_{N_G}A/I_G(A)$ is denoted by $H^{-1}(G, A)$.*

One can prove the following

PROPOSITION **1.8** *If G is a finite cyclic group then for any G-module A there is an isomorphism $H^1(G, A) \cong H^{-1}(G, A)$.*

Proof. Let us fix a generator σ of G and let $n = |G|$. For any $f \in Z^1(G, A)$ the element $f(\sigma)$ sits in ${}_{N_G}A$, since

$$N_G(f(\sigma)) = \sum_{\tau \in G} \tau(f(\sigma)) = \sum_{\tau \in G} (f(\tau\sigma) - f(\tau)) = \sum_{\tau \in G} f(\tau\sigma) - \sum_{\tau \in G} f(\tau) = 0.$$

Moreover, for each $a \in {}_{N_G}A$ the function $f : G \to A$ defined by the rule

$$f(\sigma^k) = \sum_{i=0}^{k-1} \sigma^i a, 1 \leq k \leq n$$

belongs to $Z^1(G, A)$. Therefore the map $\varphi : Z^1(G, A) \to {}_{N_G}A, f \mapsto f(\sigma)$ is a surjective group homomorphism. On the other hand $f(\sigma) \in I_G(A)$ means that $f(\sigma) = \sigma a - a$ for some a which is equivalent to saying that $f = f_a$. Therefore $f \in B^1(G, A) \Leftrightarrow \varphi(f) \in I_G(A)$ and the induced homomorphism $\bar{\varphi} : H^1(G, A) \to H^{-1}(G, A)$ is an isomorphism. □

THEOREM **1.21 (Hilbert-Noether)** *If L/K is a Galois extension (finite or infinite) with Galois group G, then $H^1(G, L^*) = 1$.*

Proof. Let $\mathscr{E}$ be the set of all finite Galois subextensions of L/K. Then

$$H^1(G(L/K), L^*) = \varinjlim_{F/K \in \mathscr{E}} H^1(G(F/K), F^*),$$

and we are reduced to the case of a finite extension. Let $f \in Z^1(G, L^*)$. We need to show that there exists some $\alpha \in L^*$ such that $f(\tau) = \frac{\tau(\alpha)}{\alpha}$ for all $\tau \in G$. Indeed, since all $f(\sigma) \in L^*$ are nonzero and the automorphisms $\sigma \in G$ are linearly independent over L (Artin's theorem on the independence of characters), there exists some $a \in L^*$ such that

$$\sum_{\sigma \in G} f(\sigma)\sigma(a) = \beta \neq 0.$$

Thereby for any $\tau \in G$,

$$\tau(\beta) = \sum_{\sigma \in G} \tau(f(\sigma))\tau(\sigma(a)) = f(\tau)^{-1} \sum_{\sigma \in G} f(\tau\sigma)(\tau\sigma)(a) = f(\tau)^{-1}\beta.$$

If we put $\alpha = \beta^{-1}$, then we obtain $f(\tau) = \frac{\tau(\alpha)}{\alpha}$ for any $\tau \in G$, as desired. □

A direct consequence of this theorem is the following

THEOREM **1.22 (Hilbert, 90)** *Let L/K be a finite cyclic extension and let σ be a generator of $G = \mathrm{Gal}(L/K)$. If $N_{L/K}(\alpha) = 1$ for some $\alpha \in L^*$, then $\alpha = \frac{\sigma(\beta)}{\beta}$ for an appropriate $\beta \in L^*$.*

Proof. According to Proposition 1.8 and Theorem 1.22 one has $H^{-1}(G, L^*) \cong H^1(G, A) = 1$, so that ${}_{N_G}L^* = I_G(L^*)$ and we are done. □

CHAPTER 2

Galois modules in extensions of local fields

2.1 The reduced group of principal units as Galois module

Let p be a rational prime number, k be a finite extension of $\mathbb{Q}_p$ of degree n containing a primitive p-th root of unity ζ_p and let K/k be a cyclic extension of degree $L = p^m$ for some positive integer m. Let us fix a generator σ of the Galois group $G = \mathrm{Gal}(K/k)$. We denote by Γ and γ the norm group of the extension K/k and k_1/k respectively, where k_1 is the unique subfield of K of degree p over k. Observe that the group K^*/K^{*p} can be regarded as a multiplicatively written $\mathbb{F}_p$-vector space. In the article [6] the following theorem is proved

Theorem (Faddeev, 1959) *In the group K^* there is an almost normal basis modulo K^{*p} of the form*

$$\{A_1, A_1^{\sigma}, ..., A_1^{\sigma^{L-1}}, A_2, A_2^{\sigma}, ..., A_2^{\sigma^{L-1}}, ..., A_n, A_n^{\sigma}, ..., A_n^{\sigma^{L-1}}, A_0, b\}$$

with the following cases

Case 1 *($\zeta_p \notin \Gamma$) : $b \in k^* \setminus \gamma$ is any element and $A_0 \in K^*$ is any element satisfying $\frac{\sigma(A_0)}{A_0} \in bK^{*p}$.*

Case 2 *($\zeta_p \in \Gamma$) : $b \in k^* \setminus \gamma$ is any element and $A_0 \in K^*$ is an element, satisfying $\frac{\sigma(A_0)}{A_0} = B_0^p$, where $B_0 \in K^*$ satisfies $N_{K/k}(B_0) = \zeta_p$.*

Let $R = \mathbb{F}_p[G]$ denote the group ring over G. Note that from the results of the theorem follows the isomorphism of R-modules $K^*/K^{*p} \cong R^n \oplus R/(\sigma - 1)^2$ in the first case and $K^*/K^{*p} \cong R^n \oplus R/(\sigma - 1) \oplus R/(\sigma - 1)$ in the second case. The idea of the proof is as follows.

The linear operator $v = \sigma - 1 \in R$ satisfies the conditions $v^L = \sigma^L - 1 = 0, v^{L-1} \neq 0$, so that it is nilpotent of degree L. Hence the whole space K^*/K^{*p} decomposes into a direct sum of cyclic v-invariant subspaces. Moreover, each of these subspaces is an R-module, isomorphic to $R/(\sigma - 1)^k$, where k is the dimension of the corresponding subspace. What remains is to calculate the number g_k of cyclic subspaces of each dimension k. In this respect recall that the number of subspaces of maximal dimension L is equal to $\dim(\mathrm{Im}\ v^{L-1})$ while the total number of subspaces is $\dim(\ker v)$. In [6] these

two numbers were calculated in each case separately, leading us to the following result

$$(g_L, g_{L-1}, ..., g_1) = \begin{cases} (n, 0, ..., 1, 0), & \text{if } \zeta_p \notin \Gamma \\ (n, 0, ..., 0, 2), & \text{if } \zeta_p \in \Gamma \end{cases}$$

which already proves the theorem. On the other hand it is not difficult to prove that

$$(g_L, g_{L-1}, ..., g_1) = (n, 0, ..., 0, 1), \text{ if } \zeta_p \notin K.$$

Observe that in exactly the same way $v = \sigma - 1$ can be regarded as a linear operator on the space $V = U_1'/U_1'^p$, where $U_1' = 1 + \mathfrak{p}_K$ is the group of principal units in K^*. In complete analogy with the previous case, we want to study the structure of V as an R-module. Likewise for each k we introduce the number l_k, namely the number of k-dimensional cyclic subspaces in a decomposition of V into a direct sum of cyclic v-invariant subspaces.

DEFINITION **2.1** *For each positive integer $t \geq 1$ we define $G_t = \{x \in K^* : x^{v^t} \in K^{*p}\}$ and $W_t = \{x \in U_1' : x^{v^t} \in U_1'^p\}$.*

The numbers l_i are related to the numbers g_i as the following proposition shows

PROPOSITION **2.1** *$(g_L, g_{L-1}, ..., g_1) \succcurlyeq (l_L, l_{L-1}, ..., l_1)$, that is $\sum_{j \geq t} g_j \geq \sum_{j \geq t} l_j$ for all $t \geq 1$.*

Proof. Observe that $W_t = G_t \cap U_1'$ for all $t \geq 1$. Indeed, if $x \in U_1'$ and $x^{v^t} = \alpha^p$, then $\alpha^p \in U_1'$ and therefore $\alpha \in U_1'$. Hence the inclusions $W_t \hookrightarrow G_t$ induce monomorphisms $W_t/W_{t-1} \to G_t/G_{t-1}$, so that

$$\dim_{\mathbb{F}_p}(W_t/W_{t-1}) \leq \dim_{\mathbb{F}_p}(G_t/G_{t-1}) \text{ for all } t \geq 1.$$

It remains only to note that

$$\dim_{\mathbb{F}_p}(W_t/W_{t-1}) = \sum_{j \geq t} l_j \quad \text{and} \quad \dim_{\mathbb{F}_p}(G_t/G_{t-1}) = \sum_{j \geq t} g_j.$$

□

In what follows the extension K/k is assumed to be cyclic of degree $L = p$. The equality $[K : k] = e(K/k)f(K/k)$ mentioned in Proposition 1.5 implies that the extension K/k is either unramified or totally ramified. Let $R_k = \{x \in k : x^{q_k - 1} = 1\}$ and $R_K = \{x \in K : x^{q_K - 1} = 1\}$, where q_k and q_K are the cardinalities of corresponding residue fields respectively. If $\Pi \in K$ is a uniformizer, then according

to Corollary 1.8 for any $\alpha \in K^*$ we will write $\alpha = \Pi^{v_\Pi(\alpha)}\eta_\alpha u_\alpha$, for uniquely determined elements $\eta_\alpha \in R_K$ and $u_\alpha \in U_1'$. From now on we will study the numbers l_i, depending on the extension K/k. For convenience we denote $W := W_1$ and $N := N_{K/k}$, the norm map of the extension K/k.

2.1.1 The group W

Note that if $\zeta_p \in K$, then $\zeta_p = \alpha_0^{\sigma-1}$ for some $\alpha_0 \in K^*$ by Theorem 1.22. Furthermore, if $\zeta_p = N(\alpha_1) \in \Gamma$ then $N(\alpha_1^p) = 1$, so that $\alpha_1^p = \beta_0^{\sigma-1}$ for some $\beta_0 \in K^*$. We first study the group G_1, since

$$W = W_1 = G_1 \cap U_1'.$$

The following lemma is due to D.K.Faddeev [6].

LEMMA **2.1**

$$G_1 = \begin{cases} k^*K^{*p}, & \zeta_p \notin \Gamma \\ \langle\beta_0\rangle k^*K^{*p}, & \zeta_p \in \Gamma \end{cases}$$

Proof. First suppose $\zeta_p \notin \Gamma$ and $x \in G_1$, which means that $x^{\sigma-1} = \alpha^p$ for some $\alpha \in K^*$. Taking norms, we get $N^p(\alpha) = 1$, which gives $N(\alpha) = 1$ and therefore $\alpha = y^{\sigma-1}$ for some $y \in K^*$, showing that $x^{\sigma-1} = (y^p)^{\sigma-1}$ and consequently $x \in k^*K^{*p}$. The opposite inclusion is clear.
On the other hand, if $\zeta_p \in \Gamma$, then from $N^p(\alpha) = 1$ we infer that $N(\alpha) = \zeta_p^t$ for some t. Therefore $N(\alpha\alpha_1^{-t}) = 1$, which implies that $\alpha = \alpha_1^t y^{\sigma-1}$ for some $y \in K^*$. Hence

$$x^{\sigma-1} = \alpha^p = (\alpha_1^t y^{\sigma-1})^p = (\alpha_1^p)^t (y^p)^{\sigma-1} =$$

$$= (\beta_0^{\sigma-1})^t (y^p)^{\sigma-1}) = (\beta_0^t y^p)^{\sigma-1},$$

which yields $x \in \langle\beta_0\rangle k^*K^{*p}$. As $\beta_0^{\sigma-1} = \alpha_1^p \in K^{*p}$, we deduce that $\beta_0 \in G_1$, and thereby the opposite inclusion $\langle\beta_0\rangle k^*K^{*p} \subset G_1$ is also proved. □

We now select any uniformizers $\pi \in k$ and $\Pi \in K$, and define

$$\lambda_{\pi,\Pi} = \begin{cases} 1, & K/k \text{ is unramified} \\ u_{\pi\Pi^{-p}}, & K/k \text{ is totally ramified} \end{cases}$$

Observe that the class

$$\lambda_{\pi,\Pi} (\text{mod } U_1 U_1'^p)$$

is independent of the choice of uniformizers π and Π, where U_1 is the group of principal units in k^*. In other words, if we choose other uniformizers $\pi_1 \in k$ and $\Pi_1 \in K$, then

$$\lambda_{\pi_1,\Pi_1} \in \langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p.$$

Indeed, if K/k is unramified then

$$\lambda_{\pi_1,\Pi_1} = \lambda_{\pi,\Pi} = 1$$

by definition. On the other hand, if K/k is totally ramified, then $\pi\Pi^{-p}$ and $\pi_1\Pi_1^{-p}$ differ by a factor of the form $\mu\mu_1^p$ for some units $\mu \in k$ and $\mu_1 \in K$. Therefore

$$\lambda_{\pi_1,\Pi_1}\lambda_{\pi,\Pi}^{-1} = u_{\mu\mu_1^p} = u_\mu u_{\mu_1}^p \in U_1 U_1'^p,$$

as claimed.

If $\zeta_p \in \Gamma$, then as we have shown, $\beta_0^{\sigma-1} = \alpha_1^p$. Suppose $\beta_0 = \Pi^l u_{\beta_0}\eta_{\beta_0}$, where l is an integer, $u_{\beta_0} \in U_1'$ and $\eta_{\beta_0} \in R_K$. Dividing by an appropriate power of π, we may assume that $0 \le l < p$. If $l = 0$, then

$$u_{\alpha_1}^p \eta_{\alpha_1}^p = \alpha_1^p = \beta_0^{\sigma-1} = u_{\beta_0}^{\sigma-1}\eta_{\beta_0}^{\sigma-1},$$

implying that $u_{\beta_0}^{\sigma-1} = u_{\alpha_1}^p$, by the uniqueness of Teichmuller's decomposition. Furthermore, assume that

$$s = \begin{cases} 1, & l = 0 \\ 0, & l \neq 0 \end{cases}$$

Lemma **2.2**

$$W = \begin{cases} \langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p, & \zeta_p \notin \Gamma \\ \langle \lambda_{\pi,\Pi} \rangle \langle u_{\beta_0}^s \rangle U_1 U_1'^p, & \zeta_p \in \Gamma \end{cases}$$

Moreover, $u_{\beta_0} \notin \langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p$.

Proof. First we assume that $\zeta_p \notin \Gamma$. In this case

$$W = G_1 \cap U_1' = k^* K^{*p} \cap U_1',$$

by Lemma 2.1. Suppose $x = ay^p \in U_1'$, for some $a \in k^*$ and $y \in K^*$.

If K/k is unramified, we may assume $\Pi = \pi$ and write $a = \pi^m b$, $y = \pi^r z$ for some integers m, r and units $b \in k, z \in K$. Since $x \in U_1'$, then $m = -rp$, and therefore $x = bz^p$. Hence

$$x = u_{bz^p} \in U_1 U_1'^p.$$

Suppose now that K/k is totally ramified and write $a = \pi^m b, y = \Pi^r z$ for some integers m, r and units $b \in k, z \in K$. The condition $v_\Pi(x) = 0$ implies that $m = -r$, but this time we get $x = (\pi\Pi^{-p})^m b z^p$, which yields

$$x = \lambda_{\pi,\Pi}^m u_b u_z^p \in \langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p.$$

On the other hand

$$\lambda_{\pi,\Pi}^{\sigma-1} = (\Pi^{1-\sigma})^p \in U_1'^p,$$

as $\Pi^{1-\sigma} \in U_1'$ for totally ramified extensions. Therefore $\lambda_{\pi,\Pi} \in W$, which together with the fact $U_1 U_1'^p \in W$ proves the opposite inclusion $\langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p \subset G_1$.

If $\zeta_p \in \Gamma$, then by Lemma 2.1, $G_1 = \langle \beta_0 \rangle k^* K^{*p}$ and therefore

$$W = \langle \beta_0 \rangle k^* K^{*p} \cap U_1',$$

and by the same method we applied in case $\zeta_p \notin \Gamma$, one can show that in both the unramified and totally ramified cases the inclusions

$$\langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p \subset W \subset \langle u_{\beta_0} \rangle \langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p$$

hold. Suppose that $x = a\beta_0^t y^p \in W$ for some $a \in k^*$ and $y \in K^*$, then one has the relation

$$tl = v_\Pi(\beta_0^t) = v_\Pi(x a^{-1} y^{-p}) \vdots p.$$

If $l \neq 0$, then $p \mid t$, hence $G_1 \cap U_1' \subset k^* K^{*p}$ and

$$W = G_1 \cap U_1' \subset k^* K^{*p} \cap U_1' = \langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p,$$

as we have already proved. On the other hand, if $l = 0$, then according to the paragraph before Lemma 2.2, $u_{\beta_0}^{\sigma-1} = u_{\alpha_1}^p$, implying that $u_{\beta_0} \in W$ and

$$W = \langle u_{\beta_0} \rangle \langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p.$$

Let us prove that $u_{\beta_0} \notin \langle \lambda_{\pi,\Pi} \rangle U_1 U_1'^p$.

Assume the contrary that $u_{\beta_0} = \lambda_{\pi,\Pi}^m a y^p$, for some $a \in k^*$ and $y \in K^*$, then

$$u_{\alpha_1}^p = u_{\beta_0}^{\sigma-1} = \begin{cases} (y^{\sigma-1})^p, & K/k \text{ is unramified} \\ ((\Pi^{-m} y)^{\sigma-1})^p, & K/k \text{ is totally ramified} \end{cases}$$

which means that $u_{\alpha_1} = \zeta_p^\nu z^{\sigma-1}$, and therefore $N(u_{\alpha_1}) = 1$. As a result we obtain the relation

$$\zeta_p = N(\alpha_1) = N(u_{\alpha_1}) N(\eta_{\alpha_1}) = N(\eta_{\alpha_1}) \in R_K,$$

which, of course, is incorrect. □

2.1.2 The numbers e_1 and l_p

We define $\Gamma_0 = N_{K/k}(U_1') \subset U_1$. Recall that if $\zeta_p \in K$, then $\zeta_p = \alpha_0^{\sigma-1}$ for some $\alpha_0 \in K^*$ and dividing by a power of π, we may assume that $0 \leq v_\Pi(\alpha_0) < p$. For simplicity we define

$$\delta = \begin{cases} 0, & v_\Pi(\alpha_0) \neq 0 \\ 1, & v_\Pi(\alpha_0) = 0 \end{cases}$$

LEMMA **2.3**

$$U_1 \cap U_1'^p = \Gamma_0 \cap U_1'^p = \begin{cases} U_1^p, & \zeta_p \notin K \\ U_1^p \langle u_{\alpha_0}^{p\delta} \rangle, & \zeta_p \in K \end{cases}$$

Proof. Suppose $x = y^p$, for some $x \in U_1$, and $y \in U_1'$, so that $(\sigma(y))^p = y^p$.

If $\zeta_p \notin K$, then $\sigma(y) = y$, hence $y \in k \cap U_1' = U_1$ and consequently $x = y^p \in U_1^p$, showing that $U_1 \cap U_1'^p = U_1^p$. On the other hand, if $\zeta_p \in K$, then $\sigma(y) = \zeta_p^t y$ for some t, which implies that $y = a\alpha_0^t$, for some $a \in k$.

If $\delta = 0$ i.e. $v_\Pi(\alpha_0) \neq 0$, then K/k is totally ramified, so that

$$t v_\Pi(\alpha_0) = -v_\Pi(a) \vdots p,$$

showing that

$$p | t, \sigma(y) = y, \text{ and therefore } U_1 \cap U_1'^p = U_1^p,$$

as in case $\zeta_p \notin K$.

If $\delta = 1$ i.e. $v_\Pi(\alpha_0) = 0$, then $\alpha_0 = \eta_{\alpha_0} u_{\alpha_0}$, where $\eta_{\alpha_0} \in R_K$ and $u_{\alpha_0} \in U_1'$. As we have shown before, $y = a\alpha_0^t$, for some $a \in k$, and therefore $y = u_{a\alpha_0^t} = u_a u_{\alpha_0}^t$, which yields

$$x = y^p = u_{\alpha_0}^{pt} u_a^p \in \langle u_{\alpha_0}^p \rangle U_1^p,$$

as claimed. On the other hand, the condition $\sigma(\alpha_0) = \zeta_p \alpha_0$ implies that $\sigma(u_{\alpha_0}) = \zeta_p u_{\alpha_0}$, showing that $u_{\alpha_0}^p \in U_1 \cap U_1'^p$.

Noting that $U_1^p \subset \Gamma_0 \cap U_1'^p \subset U_1 \cap U_1'^p$ and that $u_{\alpha_0}^p = N(u_{\alpha_0})$ (when $v_\Pi(\alpha_0) = 0$), we infer that in both cases considered above, the equality $\Gamma_0 \cap U_1'^p = U_1 \cap U_1'^p$ holds. The lemma is proved. □

LEMMA **2.4** *Suppose K/k is a totally ramified extension. If $\zeta_p \notin K$, then $\lambda_{\pi,\Pi} \notin U_1 U_1'^p$. Otherwise, the following three conditions are equivalent.*

1. $\lambda_{\pi,\Pi} \in U_1 U_1'^p$.

2. *There exist uniformizers* $\pi_0 \in k$ *and* $\Pi_0 \in K$ *such that* $\pi_0 = \Pi_0^p$.

3. $v_\Pi(\alpha_0) \neq 0$.

Proof. First we consider the case $\zeta_p \notin K$. Assume the contrary that $\lambda_{\pi,\Pi} = ay^p$ for some $a \in U_1$ and $y \in U_1'$. Then

$$(\Pi^{1-\sigma})^p = \lambda_{\pi,\Pi}^{\sigma-1} = (y^{\sigma-1})^p,$$

implying that $\Pi^{1-\sigma} = y^{\sigma-1}$, or equivalently, that $\Pi y \in k$, which is a contradiction, as $v_\Pi(\Pi y) = 1$.
Suppose now that $\zeta_p \in K$. In order to prove the lemma, it is enough to prove the following implications.
2) $\Rightarrow$ 1) If such uniformizers π_0 and Π_0 do exist, then $\lambda_{\pi_0,\Pi_0} = 1 \in U_1 U_1'^p$. It remains to recall that the condition $\lambda_{\pi,\Pi} \in U_1 U_1'^p$ is independent of the choice of uniformizers π and Π.
1) $\Rightarrow$ 2) If $\lambda_{\pi,\Pi} = ay^p$ for some uniformizers π, Π and elements $a \in U_1, y \in U_1'$, then

$$\pi\Pi^{-p} = ay^p \eta_{\pi\Pi^{-p}} = ay^p \eta^p,$$

for some $\eta \in R_K$, as the order of the cyclic group R_K is $q-1$, which is coprime to p and therefore each element from R_K is a p-th power. If we denote $\pi_0 = \pi a^{-1}$ and $\Pi_0 = \Pi y \eta$, then we get $\pi_0 = \Pi_0^p$, as claimed.
2) $\Leftrightarrow$ 3) If $\pi_0 = \Pi_0^p$, then $\Pi_0^{\sigma-1} = \zeta_p^t$, for some $0 < t < p$. Hence $\zeta_p = (\Pi_0^l)^{\sigma-1}$, where $0 < l < p$ is the inverse of t modulo p. Therefore $v_\Pi(\alpha_0) = l$, as $0 \leq v_\Pi(\alpha_0) < p$, showing that $v_\Pi(\alpha_0) \neq 0$.
Recall that if $\zeta_p \in k$, then any cyclic extension of k of order p has the form $K = k(\sqrt[p]{a})$ for some $a \in k^*$. Moreover, a can be chosen either as a uniformizer, or a principal unit.
Suppose there are no uniformizers π_0 and Π_0, such that $\pi_0 = \Pi_0^p$. Then we can choose $a \in U_1$ and conclude that $\beta = \sqrt[p]{a} \in U_1'$. Therefore $\zeta_p = (\beta^l)^{\sigma-1}$ for some $0 < l < p$, showing that $v_\Pi(\alpha_0) = 0$, as $v_\Pi(\beta^l) = 0$. □

To prove the following lemma we need the asserion provided below .

$$\dim_{\mathbb{F}_p} U_1/U_1^p = \begin{cases} [k:\mathbb{Q}_p], & \zeta_p \notin k \\ [k:\mathbb{Q}_p]+1, & \zeta_p \in k \end{cases}$$

For the proof we refer the reader to [10, Chapter 15, §5].

LEMMA **2.5**

$$e_1 = \begin{cases} n, & \zeta_p \notin K,\ K/k \text{ is unramified} \\ n+1, & \zeta_p \in K,\ K/k \text{ is unramified} \\ n+1, & \zeta_p \notin \Gamma,\ K/k \text{ is totally ramified} \\ n+1+s, & \zeta_p \in \Gamma,\ K/k \text{ is totally ramified} \end{cases}$$

Proof. First we note that

$$e_1 = \dim_{\mathbb{F}_p}(W/U_1'^p) = \dim_{\mathbb{F}_p}(W/U_1U_1'^p) + \dim_{\mathbb{F}_p}(U_1U_1'^p/U_1'^p).$$

It will be convenient to denote $e_1' = \dim_{\mathbb{F}_p}(W/U_1U_1'^p)$ and $e_1'' = \dim_{\mathbb{F}_p}(U_1U_1'^p/U_1'^p)$.

If $\zeta_p \notin \Gamma$ then by Lemma 2.2 and Lemma 2.4 we get $W = \langle\lambda_{\pi,\Pi}\rangle U_1U_1'^p$ and

$$e_1' = \begin{cases} 0, & K/k \text{ is unramified} \\ 1, & \zeta_p \notin K,\ K/k \text{ is totally ramified} \\ \delta, & \zeta_p \in K,\ K/k \text{ is totally ramified} \end{cases}$$

If $\zeta_p \in \Gamma$ then again according to Lemma 2.2 and Lemma 2.4 we get $W = \langle\lambda_{\pi,\Pi}\rangle\langle u_{\beta_0}^s\rangle U_1U_1'^p$ and

$$e_1' = \begin{cases} 1, & K/k \text{ is unramified} \\ \delta+s, & K/k \text{ is totally ramified} \end{cases}$$

Recall that for unramified extensions K/k, $\zeta_p \in \Gamma$ if and only if $\zeta_p \in K$. Therefore, combining the cases $\zeta_p \notin \Gamma$ and $\zeta_p \in \Gamma$, we get

$$e_1' = \begin{cases} 0, & \zeta_p \notin K,\ K/k \text{ is unramified} \\ 1, & \zeta_p \in K,\ K/k \text{ is unramified} \\ 1, & \zeta_p \notin K,\ K/k \text{ is totally ramified} \\ \delta, & \zeta_p \in K \setminus \Gamma,\ K/k \text{ is totally ramified} \\ \delta+s, & \zeta_p \in \Gamma,\ K/k \text{ is totally ramified} \end{cases}$$

On the other hand Lemma 2.3 together with the paragraph before the formulation of Lemma 2.5 implies

$$e_1'' = \begin{cases} n, & \zeta_p \notin K \\ n+1-\delta, & \zeta_p \in K \end{cases}$$

To finish the proof it remains to recall that

$$e_1 = e_1' + e_1''.$$

□

Finally we calculate l_p in the following

LEMMA **2.6**

$$l_p = \begin{cases} n, & K/k \text{ is unramified} \\ n-1, & \zeta_p \notin K,\ K/k \text{ is totally ramified} \\ n-\delta, & \zeta_p \in K,\ K/k \text{ is totally ramified} \end{cases}$$

Proof. Observe that

$$l_p = \dim_{\mathbb{F}_p}(\mathrm{Im}(\sigma-1)^{p-1}) = \dim_{\mathbb{F}_p}(\Gamma_0 U_1'^p/U_1'^p) = \dim_{\mathbb{F}_p}(\Gamma_0/\Gamma_0 \cap U_1'^p)$$

If K/k is unramified then $\Gamma_0 = U_1$ and by Lemma 2.3

$$l_p = \begin{cases} n, & \zeta_p \notin K \\ n+1-\delta, & \zeta_p \in K \end{cases}$$

which gives $l_p = n$, since $\delta = 1$ in this case.

On the other hand, if K/k is totally ramified then $[U_1 : \Gamma_0] = p$, which together with Lemma 2.3 yields

$$l_p = \begin{cases} n-1, & \zeta_p \notin K \\ n-\delta, & \zeta_p \in K \end{cases}$$

and we are done. □

2.1.3 Proof of Theorem 2.1

1. If $\zeta_p \notin K$ then we know that $(g_p, g_{p-1}, ..., g_1) = (n, ..., 1)$. Lemma 2.5 and 2.6 imply that if K/k is unramified, then $e_1 = l_p = n$, while if K/k is totally ramified then $e_1 = n+1$ and $l_p = n-1$. Recall that $\dim_{\mathbb{F}_p}(V) = np$, which shows that in the unramified case $(l_p, l_{p-1}, ..., l_1) = (n, 0, ..., 0)$,

while in the totally ramified case $(l_p, l_{p-1}, ..., l_1) = (n-1, ..1, ..1, ..)$, where $1'$s are at positions a and b with $a+b=p$. Proposition 2.1 shows that

$$(n, 0, ..., 1) = (g_p, g_{p-1}, ..., g_1) \succcurlyeq (l_p, l_{p-1}, ..., l_1) = (n-1, ..1, ..1, ..),$$

which means that if $a < b$ then $a = 1$ and therefore $b = p-1$, showing that $(l_p, l_{p-1}, ..., l_1) = (n-1, 1, ..., 1)$.

2. If $\zeta_p \in K \setminus \Gamma$, then K/k is a totally ramified extension and therefore $e_1 = n+1, l_p = n-\delta$, by Lemma 2.5 and Lemma 2.6. On the other hand, $(g_p, g_{p-1}, ..., g_1) = (n, ..., 1, 0)$ and $\dim_{\mathbb{F}_p}(V) = np+1$. Hence, if $\delta = 0$, then $(l_p, l_{p-1}, ..., l_1) = (n, ..., 1)$, while if $\delta = 1$, then $(l_p, l_{p-1}, ..., l_1) = (n-1, ..1, .., 1, ..)$, where $1'$s are at positions a and b with $a \leq b,\ a+b = p+1$, which shows that $a > 1$ as $b < p$. Using Proposition 2.1 we obtain

$$(n, ..., 1, 0) \succcurlyeq (n-1, ..1, ..1, ..)$$

and therefore $a = 2, b = p-1$, implying that $(l_p, l_{p-1}, ..., l_1) = (n-1, 1, ..., 1, 0)$.

3. Consider the last case $\zeta_p \in \Gamma$. Then one has $(g_p, g_{p-1}, ..., g_1) = (n, ..., 2)$ and $\dim_{\mathbb{F}_p}(V) = np+1$. Lemma 2.5 and Lemma 2.6 again imply that if K/k is unramified, then $e_1 = n+1, l_p = n$, while if K/k is totally ramified, then $e_1 = n+1+s$ and $l_p = n-\delta$. Hence, if K/k is unramified, then $(l_p, l_{p-1}, ..., l_1) = (n, ..., 1)$.

   Suppose K/k is totally ramified. If $\delta = 0$, then again $(l_p, l_{p-1}, ..., l_1) = (n, ..., 1)$, as $l_p = n-\delta = n$, which simultaneously shows that $s = 0$. Assume now that $\delta = 1$. If $s = 0$, then by Proposition 2.1, we would have a relation

$$(n, ..., 2) \succcurlyeq (n-1, ..1, ..1, ..)$$

with two 1's at places a and b with $a \leq b,\ a+b = p+1$, implying that $a = 1$ and $b = p$, which is a contradiction, as $b < p$. Therefore $s = 1$ and we get a relation

$$(n, ...2) \succcurlyeq (n-1, ..1, ..1, ..1, ..),$$

where 1's are at some positions a, b, c with $a \leq b \leq c,\ a+b+c = p+1$, which yields $a = b = 1$ and $c = p-1$, showing that $(l_p, l_{p-1}, ..., l_1) = (n-1, 1, ..., 2)$.

Thus everything proven can be incorporated within the following table in the form of a theorem. Here u denotes a principal unit in k.

THEOREM **2.1**

	The extension K/k	R*-module* V
1.	$\zeta_p \notin k$, *unramified*	R^n
2.	$\zeta_p \notin k$, *totally ramified*	$R^{n-1} \oplus R/(\sigma-1)^{p-1} \oplus R/(\sigma-1)$
3.	$K = k(\sqrt[p]{u}), \zeta_p \in k \setminus \Gamma$	$R^n \oplus R/(\sigma-1)$
4.	$K = k(\sqrt[p]{\pi}), \zeta_p \in k \setminus \Gamma$	$R^{n-1} \oplus R/(\sigma-1)^{p-1} \oplus R/(\sigma-1)^2$
5.	$\zeta_p \in \Gamma$, *unramified*	$R^n \oplus R/(\sigma-1)$
6.	$K = k(\sqrt[p]{u}), \zeta_p \in \Gamma$, *totally ramified*	$R^n \oplus R/(\sigma-1)$
7.	$K = k(\sqrt[p]{\pi}), \zeta_p \in \Gamma$, *totally ramified*	$R^{n-1} \oplus R/(\sigma-1)^{p-1} \oplus R/(\sigma-1) \oplus R/(\sigma-1)$

It can be proved that in all cases any $\mathbb{F}_p$-basis of V modulo $\ker((\sigma-1)^{p-1})$ can serve as an R-basis of the corresponding free part. Moreover, it is not hard to show that in cases 3 and 6 the additional generator α can be chosen as any element from the set $U_1 \setminus \Gamma_0$, while in case 5 one may choose $\alpha = u_{\beta_0}$ (see Section 2.1.1).

2.2 Honda formal group as Galois module

Let p be a rational prime, $K/\mathbb{Q}_p, L/K, M/L$ be a tower of finite extensions of local fields, M/L be a Galois extension with Galois group G and F be a one dimensional formal group law over the ring $\mathcal{O}_K$. The operation $x \underset{F}{+} y = F(x,y)$ sets a new structure of abelian group on the maximal ideal $\mathfrak{p}_M$ of the ring $\mathcal{O}_M$ which we will denote by $F(\mathfrak{p}_M)$. Taking into account the natural action of the group G on $F(\mathfrak{p}_M)$, one may consider it as an $\mathrm{End}_{\mathcal{O}_K}(F)[G]$-module, in which the multiplication by scalars from $\mathrm{End}_{\mathcal{O}_K}(F)$ is performed by the rule $f * x = f(x)$. We refer the reader to Section 1.2 as well as to [23, Chapter 6, §3], [20, Chapter 3, §6], [16, Chapter 4] and [30, Chapter 4] for more details concerning formal groups and the group $F(\mathfrak{p}_M)$.

If F is a Lubin-Tate formal group law, then there is an injection $\mathcal{O}_K \hookrightarrow \mathrm{End}_{\mathcal{O}_K}(F)$ (see Theorem 1.15 and [23, Chapter 6, Prop. 3.3]), which enables us to regard $F(\mathfrak{p}_M)$ as an $\mathcal{O}_K[G]$-module. The structure of this module in case of multiplicative formal group $F = G_m$ and $K = \mathbb{Q}_p$ is studied in sufficient detail in [4,5,7]. The starting point of the current study is the following theorem of Borevich in [7].

Theorem (Borevich, 1965) *Suppose M/L is an unramified p-extension and $K = \mathbb{Q}_p$. If the fields*

M and L have the same irregularity degree [1] *then for the $\mathcal{O}_K[G]$-module U_M there exists a system of generating elements $\theta_1, ..., \theta_{n-1}, \xi, \omega$ with the unique defining relation $\xi^{p^s} = \omega^{\sigma-1}$, where $n = [L : \mathbb{Q}_p]$ and σ is a generating element of the Galois group $G = \mathrm{Gal}(M/L)$.*

It may seem that the group of principal units E_M has nothing to do with formal groups, but in fact it is easy to show that for the multiplicative formal group $F = G_m$ there is an isomorphism $F(\mathfrak{p}_M) \cong E_M, x \mapsto 1 + x$ of $\mathbb{Z}_p[G]$-modules.

The next stop in the course of investigations was the joint work of S.V.Vostokov and I.I.Nekrasov [11], where they generalized the aforementioned theorem to the case of Lubin-Tate formal groups (See Subsection 1.2.2 for details concerning Lubin-Tate formal groups). More precisely, they managed to prove the following

Theorem (Vostokov-Nekrasov, 2014) *Suppose M/L is an unramified p-extension and F is a Lubin-Tate formal group for the prime element $\pi \in K$. Assume moreover that the fields M and L have the same irregularity degree, namely they contain a generator of $\ker[\pi^s]_F$ and do not contain a generator of $\ker[\pi^{s+1}]_F$ for some $s \geq 1$* [2]*. Then for the $\mathcal{O}_K[G]$-module $F(\mathfrak{p}_M)$ there exists a system of generating elements $\theta_1, ..., \theta_{n-1}, \xi, \omega$ with the unique defining relation $[\pi^s]_F(\xi) = \omega^\sigma \underset{F}{-} \omega$, where $n = [L : K]$ and σ is a generating element of the Galois group $G = \mathrm{Gal}(M/L)$.*

The key point in this work was the proof of the triviality of the cohomology groups $H^i(G(M/L), F(\mathfrak{p}_M)), i = 0, -1$ (See Definition 1.15) for unramified extensions M/L. In its turn, our work is devoted to the generalization of the last result to the case of Honda formal groups. Namely, let $K_0/\mathbb{Q}_p$ be a finite extension such that K/K_0 is unramified, $\pi \in K_0$ be a uniformizer, F be a Honda formal group over $\mathcal{O}_K$ relative to the extension K/K_0 of type $u \in \mathcal{O}_{K,\varphi}[[T]]$. We refer the reader to Subsection 1.2.3 as well as to [12, §§2,3] and [13, 14] for more information concerning Honda formal groups. Suppose K^{alg} is a fixed algebraic closure of the field K, $\mathfrak{p}_{K^{\mathrm{alg}}}$ is the valuation ideal, i.e. the set of all points in K^{alg} with positive valuation. Define $W_F^n = \ker[\pi^n]_F \subset F(\mathfrak{p}_{K^{\mathrm{alg}}})$ to be the π^n-torsion submodule. More precisely, let $W_F^n = \{x \in \mathfrak{p}_{K^{\mathrm{alg}}} | [\pi^n]_F(x) = 0\}$, where $[\pi^n]_F \in \mathrm{End}_{\mathcal{O}_K}(F)$, and let $W_F = \bigcup_{n=1}^{\infty} W_F^n$.
It is known (See Theorem 1.17 and [12, §2, Thm. 3]) that there is a ring embedding $\mathcal{O}_{K_0} \hookrightarrow \mathrm{End}_{\mathcal{O}_K}(F)$,

[1] This means that the field L contains a p^s-th primitive root of unity, while M does not contain a primitive p^{s+1}-th root of unity for some $s \geq 1$

[2] In fact, $\ker[\pi^s]_F$ is a cyclic $\mathcal{O}_K$-module, whenever F is a Lubin-Tate formal group (See [20, Chapter 3, Prop. 7.2])

which allows as to regard $F(\mathfrak{p}_M)$ as an $\mathcal{O}_{K_0}[G]$-module. In this section, using generators and defining relations we describe the structure of this module in the case of unramified p-extension M/L, provided that $W_F \cap F(\mathfrak{p}_L) = W_F \cap F(\mathfrak{p}_M) = W_F^s$, for certain $s \geq 1$ (See [15]). According to Theorem 1.10 any finite unramified extension of a local field is a cyclic extension, so that G is a cyclic p-group.

We agree in the following notation

$n-$the degree of the field L over K_0;

$h-$the height of the type $u = \pi + \sum_{i\geq 1} a_i T^i$ of the formal goup F, i.e. the minimal h, for which a_h is invertible.

$f-$the logarithm of F;

$p^m-$the order of the group $G = \mathrm{Gal}(M/L)$;

$\sigma-$a generating element of G;

$\zeta_i, 1 \leq i \leq h-$a fixed basis of the $\mathcal{O}_{K_0}/\pi^s\mathcal{O}_{K_0}$-module W_F^s;

$k_0, l-$the residue fields of K_0 and L respectively;

$q-$the order of k_0;

$x \underset{F}{+} y := F(x, y)$;

$\sum\limits_{F;i=1}^{k} x_i := x_1 \underset{F}{+} x_2 \underset{F}{+} ... \underset{F}{+} x_k.$

2.2.1 Auxiliary lemmas

LEMMA **2.7** *The $\mathcal{O}_{K_0}$-module W_F^n is isomorphic to $(\mathcal{O}_{K_0}/\pi^n\mathcal{O}_{K_0})^h$.*

Proof. See [14, Prop. 1]. □

LEMMA **2.8** *In the case of an unramified extension M/L, the groups $H^i(G, F(\mathfrak{p}_M))$ are trivial for $i = 0, -1$.*

LEMMA **2.9** *If the elements $x_1, x_2, ..., x_k$ from $F(\mathfrak{p}_M)$ are such that the system $\{N_{F(\mathfrak{p}_M)}(x_i), 1 \leq i \leq k\}$ [3] is linearly independent in the k_0-vector space $F(\mathfrak{p}_M)/[\pi]_F(F(\mathfrak{p}_M)$, then so is the system $\{x_i^{\sigma^j}, 1 \leq i \leq k, 0 \leq j \leq p^m - 1\}$.*

LEMMA **2.10** *If the elements $x_1, x_2, ..., x_k$ from $F(\mathfrak{p}_M)$ generate the k_0-vector space $F(\mathfrak{p}_M)/[\pi]_F(F(\mathfrak{p}_M)$, then they generate $F(\mathfrak{p}_M)$ as an $\mathcal{O}_{K_0}$-module.*

[3] Here $N_{F(\mathfrak{p}_M)}$ is the G-module norm, see Definition 1.16.

The proofs of lemmas 2.8-2.10 can be found in the article [11], as well as in [7, §3].

LEMMA **2.11** *The natural linear map*

$$\varphi : F(\mathfrak{p}_L)/[\pi]_F(F(\mathfrak{p}_L)) \to F(\mathfrak{p}_M)/[\pi]_F(F(\mathfrak{p}_M))$$

of k_0-vector spaces, induced by inclusion, has kernel of dimension h.

Proof. Consider the elements $\eta_i = [\pi^{s-1}]_F\zeta_i, 1 \le i \le h$. They form a basis of W_F^1 as an $\mathcal{O}_{K_0}/\pi\mathcal{O}_{K_0}$-module. Since $N_{F(\mathfrak{p}_M)}\eta_i = [p^m]_F\eta_i = 0$, then by Lemma 2.8 we get that $\eta_i = t_i^\sigma \underset{F}{-} t_i$ for some elements $t_i \in F(\mathfrak{p}_M)$. Suppose that $x \in F(\mathfrak{p}_L)$ and $x = [\pi]_F(y)$ for some $y \in F(\mathfrak{p}_M)$. Then $[\pi]_F(y^\sigma \underset{F}{-} y) = x^\sigma \underset{F}{-} x = 0$, from which it follows that

$$y^\sigma \underset{F}{-} y = \sum_{F;i=1}^{h} [a_i]_F(\eta_i) = \sum_{F;i=1}^{h} \left(([a_i]_F(t_i))^\sigma \underset{F}{-} [a_i]_F(t_i) \right),$$

for certain elements $a_i \in \mathcal{O}_{K_0}$, uniquely determined modulo π. The last relationship indicates the existence of $z \in F(\mathfrak{p}_L)$, for which $y = \sum\limits_{F;i=1}^{h} [a_i]_F(t_i) \underset{F}{+} z$. Therefore,

$$x = [\pi]_F(y) = \sum_{F;i=1}^{h} [a_i]_F([\pi]_F(t_i)) \underset{F}{+} [\pi]_F(z).$$

Hence the elements $[\pi]_F(t_i), 1 \le i \le h$ constitute a basis of $\ker\varphi$. The lemma is proved. □

LEMMA **2.12** *The dimension of the k_0-vector space $F(\mathfrak{p}_L)/[\pi]_F(F(\mathfrak{p}_L))$ is equal to $n + h$.*

Proof. According to Theorem 1.14 for $i > \frac{e(L/\mathbb{Q}_p)}{p-1}$ there is an isomorphism of groups $f : F(\mathfrak{p}_L^i) \xrightarrow{\sim} \mathfrak{p}_L^i$, which is in fact an isomorphism of $\mathcal{O}_{K_0}$-modules due to the relation $f \circ [a]_F = af$ which holds for all $a \in \mathcal{O}_{K_0}$. Consequently, $F(\mathfrak{p}_L^i)$ is a free $\mathcal{O}_{K_0}$- module of rank n. From the exactness of sequences of $\mathcal{O}_{K_0}$-modules:

$$0 \to F(\mathfrak{p}_L^{i+1}) \to F(\mathfrak{p}_L^i) \to l \to 0,\ i \ge 1$$

it follows that $F(\mathfrak{p}_L^i)$ is an $\mathcal{O}_{K_0}$-submodule of finite index in $F(\mathfrak{p}_L)$. Therefore $F(\mathfrak{p}_L)$ is a finitely generated $\mathcal{O}_{K_0}$-module of rank n. The theory of finitely generated modules over a PID yields $F(\mathfrak{p}_L) = T \oplus A$, where T is the torsion submodule, which in our case coincides with W_F^s, while A is a free $\mathcal{O}_{K_0}$-module of rank n. In the long run we get

$$|F(\mathfrak{p}_L)/[\pi]_F(F(\mathfrak{p}_L))| = |T/[\pi]_F T| \cdot |A/[\pi]_F A| = q^h \cdot q^n = q^{n+h},$$

completing the proof of the lemma. □

REMARK **2.1** *Likewise we get that* $\dim_{k_0}(F(\mathfrak{p}_M)/[\pi]_F(F(\mathfrak{p}_M))) = np^m + h$.

REMARK **2.2** *Since* $F(\mathfrak{p}_M)$ *is a finitely generated* $\mathcal{O}_{K_0}$*- module, then by Nakayama's lemma we obtain a new proof of the assertion of Lemma 2.10.*

LEMMA **2.13** *The elements* $\zeta_i, 1 \le i \le h$ *are linearly independent modulo* $\ker\varphi$.

Proof. Suppose the relation $\sum_{F;i=1}^{h} [a_i]_F\zeta_i = [\pi]_F(y)$ holds for some $a_i \in \mathcal{O}_{K_0}, y \in F(\mathfrak{p}_M)$. Applying the endomorphism $[\pi^s]_F$, we get that $[\pi^{s+1}]_F(y) = 0$, which gives $[\pi^s]_F(y) = 0$. The latter means that $\sum_{F;i=1}^{h} [\pi^{s-1}a_i]_F\zeta_i = 0$, which is equivalent to the condition $a_i \vdots \pi, 1 \le i \le h$. The lemma is proved. □

COROLLARY **2.1** $h \le n$

Proof. In view of the lemmas proved, it follows that the maximal number of linearly independent vectors modulo $\ker\varphi$ in $F(\mathfrak{m}_L)/[\pi]_F(F(\mathfrak{p}_L))$ is equal to

$$\dim \mathrm{Im}\varphi = \dim_{k_0}(F(\mathfrak{p}_L)/[\pi]_F(F(\mathfrak{p}_L))) - \dim\ker\varphi = (n+h) - h = n.$$

By Lemma 2.13 we already have h linearly independent vectors modulo $\ker\varphi$, from which the desired result follows. □

2.2.2 Proof of Theorem 2.2

THEOREM **2.2** *If the extension* M/L *is unramified and* $W_F \cap F(\mathfrak{p}_L) = W_F \cap F(\mathfrak{p}_M) = W_F^s$*, for some* $s \ge 1$*, then* $h \le n$ *and for the* $\mathcal{O}_{K_0}[G]$*-module* $F(\mathfrak{p}_M)$ *there exist a system of generating elements* $\theta_j, \xi_i, \omega_i, 1 \le j \le n-h, 1 \le i \le h$ *with the only defining relations* $[\pi^s]_F(\xi_i) = \omega_i^\sigma \underset{F}{-} \omega_i, 1 \le i \le h$.

Proof. From the triviality of the group $H^0(G, F(\mathfrak{p}_M))$ it follows the existence of elements $\xi_i \in F(\mathfrak{p}_M), 1 \le i \le h$, such that $N_{F(\mathfrak{p}_M)}(\xi_i) = \zeta_i$. Since $N_{F(\mathfrak{p}_M)}([\pi^s]_F(\xi_i)) = [\pi^s]_F(\zeta_i) = 0$ and the group $H^{-1}(G, F(\mathfrak{p}_M))$ is trivial, there exist elements $\omega_i \in F(\mathfrak{p}_M), 1 \le i \le h$, satisfying the relations $[\pi^s]_F\xi_i = \omega_i^\sigma \underset{F}{-} \omega_i$. In view of Corollary 2.1, the system $\zeta_i, 1 \le i \le h$ can be supplemented to a basis modulo $\ker\varphi$ via elements $\varepsilon_j \in F(\mathfrak{m}_L), 1 \le j \le n-h$. For $1 \le j \le n-h$ we select elements $\theta_j \in F(\mathfrak{p}_M)$, so that $N_{F(\mathfrak{p}_M)}(\theta_j) = \varepsilon_j$ for all j and we prove that the system

$$\mathscr{E} = \{\omega_i, \xi_i^{\sigma^k}, \theta_j^{\sigma^k} | 1 \le i \le h, 1 \le j \le n-h, 0 \le k \le p^m - 1\}$$

is linearly independent modulo $[\pi]_F(F(\mathfrak{p}_M))$. Assume the contrary that there exist elements $a_i, a_{i,k}, b_{j,k} \in \mathcal{O}_{K_0}$ and $\beta \in F(\mathfrak{p}_M)$ such that

$$\sum_{F;i}[a_i]_F\omega_i \underset{F}{+} \sum_{F;i,k}[a_{i,k}]_F(\xi_i^{\sigma^k}) \underset{F}{+} \sum_{F;j,k}[b_{j,k}]_F(\theta_j^{\sigma^k}) \underset{F}{+} [\pi]_F(\beta) = 0.$$

We apply $\sigma - 1$ to both parts of the latter relation and use the relations $[\pi^s]_F\xi_i = \omega_i^\sigma \underset{F}{-} \omega_i, 1 \le i \le h$ to deduce the equality

$$\sum_{F;i,k}[a_{i,k} - a_{i,k-1}]_F(\xi_i^{\sigma^k}) \underset{F}{+} \sum_{F;j,k}[b_{j,k} - b_{j,k-1}]_F(\theta_j^{\sigma^k}) \underset{F}{+} \sum_{F;i}[a_i]_F[\pi^s]_F\xi_i \underset{F}{+} [\pi]_F(\beta^\sigma \underset{F}{-} \beta) = 0.$$

From lemmas 2.9 and 2.13 it follows that the system

$$\mathscr{E}_0 = \{\xi_i^{\sigma^k}, \theta_j^{\sigma^k} | 1 \le i \le h, 1 \le j \le n-h, 0 \le k \le p^m - 1\}$$

is linearly independent modulo $[\pi]_F(F(\mathfrak{p}_M))$, so that $a_{i,k} (\mathrm{mod}\ \pi)$ and $b_{j,k} (\mathrm{mod}\ \pi)$ are independent of k. Therefore, without loss of generality we may assume that

$$\sum_{F;i}[a_i]_F[\pi^s]_F\xi_i \underset{F}{+} [\pi]_F(\beta^\sigma \underset{F}{-} \beta) = 0,$$

changing if needed β. From the obtained follows the existence of $b_i \in \mathcal{O}_{K_0}, 1 \le i \le h$ such that

$$\sum_{F;i}[a_i\pi^{s-1}]_F(\xi_i) \underset{F}{+} \beta^\sigma \underset{F}{-} \beta = \sum_{F;i}[b_i]_F\eta_i$$

Taking norms $N_{F(\mathfrak{p}_M)}$, the obtained relation leads to the equality $\sum_{F;i}[a_i\pi^{s-1}]_F(\zeta_i) = 0$ which implies that $a_i \vdots \pi, 1 \le i \le h$. From the linear independence of the system $\mathscr{E}_0$ it follows that $a_{i,k} \vdots \pi$ and $b_{j,k} \vdots \pi$ for all i, j and k. This completes the proof of the linear independence of the system $\mathscr{E}$. The number of vectors in it is $np^m + h = \dim_{k_0}(F(\mathfrak{p}_M)/[\pi]_F(F(\mathfrak{p}_M)))$, so that they generate the space $F(\mathfrak{p}_M)/[\pi]_F(F(\mathfrak{p}_M))$. From lemma 2.10 it follows that they generate $F(\mathfrak{p}_M)$ as an $\mathcal{O}_{K_0}$-module, and consequently the elements $\theta_j, \xi_i, \omega_i, 1 \le j \le n-h, 1 \le i \le h$ generate $F(\mathfrak{p}_M)$ as an $\mathcal{O}_{K_0}[G]$-module. It remains only to prove the assertion concerning defining relations. Let us further agree to write multiplication by elements of the ring $\mathcal{O}_{K_0}[G]$ through exponentiation. Suppose that the relation

$$\sum_{F;i}\xi_i^{\alpha_i} \underset{F}{+} \sum_{F;i}\omega_i^{\beta_i} \underset{F}{+} \sum_{F;j}\theta_j^{\delta_j} = 0,$$

holds for some elements $\alpha_i, \beta_i, \delta_j \in \mathcal{O}_{K_0}[G]$. Our goal is to prove the existence of elements $\gamma_i \in \mathcal{O}_{K_0}[G]$ for which $\alpha_i = \pi^s\gamma_i, \beta_i = (1-\sigma)\gamma_i$ and $\delta_j = 0$. Indeed, let $\beta_i = b_i + (1-\sigma)\gamma_i$ for certain

elements $b_i \in \mathcal{O}_{K_0}$ and $\gamma_i \in \mathcal{O}_{K_0}[G]$. Taking into account the relations $[\pi^s]_F\xi_i = \omega_i^\sigma \underset{F}{-} \omega_i$ for $1 \leq i \leq h$ we get

$$\sum_{F;i} \omega_i^{b_i} \underset{F}{+} \sum_{F;i} \xi_i^{\alpha_i'} \underset{F}{+} \sum_{F;j} \theta_j^{\delta_j} = 0,$$

where $\alpha_i' = \alpha_i - \pi^s\gamma_i$. Factoring the latter relation modulo $[\pi]_F(F(\mathfrak{p}_M))$ and recalling that the system $\mathscr{E}$ is a basis modulo $[\pi]_F(F(\mathfrak{p}_M))$, we find that there exist elements $b_i^{(1)}, \beta_i', \delta_j^{(1)} \in \mathcal{O}_{K_0}[G]$ such that $b_i = \pi b_i^{(1)}, \alpha_i' = \pi\beta_i', \delta_j = \pi\delta_j^{(1)}$. Therefore, for some elements $a_i \in \mathcal{O}_{K_0}$ we must have the equality

$$\sum_{F;i} \omega_i^{b_i^{(1)}} \underset{F}{+} \sum_{F;i} \xi_i^{\beta_i' - a_i\sum_k \sigma^k} \underset{F}{+} \sum_{F;j} \theta_j^{\delta_j^{(1)}} = 0,$$

due to the fact that $\zeta_i = N_{F(\mathfrak{p}_M)}(\xi_i) = \xi_i^{\sum_k \sigma^k}$. For the same reasons, all $b_i^{(1)}$ and $\delta_j^{(1)}$ are divisible by π. By induction we construct sequences $(b_i^{(\nu)})_{\nu\geq 0}$ and $(\delta_j^{(\nu)})_{\nu\geq 0}$ satisfying the conditions $b_i^{(0)} = b_i, \delta_j^{(0)} = \delta_j, b_i^{(\nu)} = \pi b_i^{(\nu+1)}$ and $\delta_j^{(\nu)} = \pi\delta_j^{(\nu+1)}$ for all $\nu \geq 0, 1 \leq i \leq h, 1 \leq j \leq n-h$, from which it follows that $b_i = 0$ for all i and $\delta_j = 0$ for all j. There remains only the relation $\sum_{F;i} \xi_i^{\alpha_i'} = 0$. Let now $\alpha_i' = \sum_k a_{i,k}\sigma^k$, where $a_{i,k} \in \mathcal{O}_{K_0}$ for all i, k. The factorization modulo $[\pi]_F(F(\mathfrak{p}_M))$ yields $a_{i,k} = \pi b_{i,k}$. Further, we obtain that

$$\sum_{F;i} \xi_i^{\sum_k b_{i,k}\sigma^k} = \sum_{F;i} [\lambda_i]_F(\zeta_i) = \sum_{F;i} \xi_i^{\lambda_i\sum_k \sigma^k},$$

for some elements $\lambda_i \in \mathcal{O}_{K_0}$. Consequently $b_{i,k} (\mathrm{mod}\pi)$ is the same for all k, and so on. In the end we get that $a_{i,k} = a_i$ and that $\sum_{F;i}[a_i]_F(\zeta_i) = 0$, i.e. $a_i = \pi^s t_i$ for certain $t_i \in \mathcal{O}_{K_0}$ and therefore

$$\alpha_i - \pi^s\gamma_i = \alpha_i' = \pi^s t_i \sum_k \sigma^k.$$

If we denote $\gamma_i' = \gamma_i + t_i\sum_k \sigma^k$, then we will have $\alpha_i = \pi^s\gamma_i'$ and $\beta_i = (1-\sigma)\gamma_i = (1-\sigma)\gamma_i'$, thus completing the proof of the theorem . □

CHAPTER 3

Properties of arithmetic sequences

3.1 Distinguished sequences

It is known that for any non-constant polynomial P with integer coefficients there exist infinitely many primes, dividing at least one term of the sequence $(P(n))_{n=1}^{\infty}$ [25, Part 8, Ex. 108]. In this respect we are interested if there is a general phenomenon behind this fact. It turns out that the answer is positive and somehow depends on the rate of growth of the given sequence . To be more precise we give the definition of distinguished sequences of positive integers.

DEFINITION **3.1** *We say that a sequence $(n_k)_{k=1}^{\infty}$ of positive integers is distinguished, if there are infinitely many primes dividing at least one term of the sequence.*

To formulate our results we need one more

DEFINITION **3.2** *Suppose $S = \{p_1, p_2, ..., p_n\}$ is a finite set consisting of prime numbers. We define $\hat{S} = \{{p_1}^{k_1}{p_2}^{k_2} \cdot ... \cdot {p_n}^{k_n} | k_1, k_2, ..., k_n \in \mathbb{Z}_+\}$ and arrange the set $\hat{S}$ in increasing order to get the sequence $(n_k(S))_{k=1}^{\infty}$.*

In this section we prove the following theorems.

THEOREM **3.1** $\lim\limits_{k\to\infty} \dfrac{\ln(\ln(n_k(S)))}{\ln(k)} = \dfrac{1}{n}$.

THEOREM **3.2** *Suppose $(n_k)_{k=1}^{\infty}$ and $(m_k)_{k=1}^{\infty}$ are sequences of positive integers. Then the sequence $(n_k)_{k=1}^{\infty}$ is distinguished, provided that the following conditions hold.*

1. $\lim\limits_{k\to\infty} n_k = \infty$
2. $\gcd(n_k, n_{k+l}) < m_l$ *for all positive integers k and l*

We also deal with sequences of the form $a_n = 2^{2^n} + d$, where $d \in \mathbb{Z}$. Recall that a Fermat number is a positive integer of the form $F_n = 2^{2^n} + 1$ for some nonnegative integer n. It is well known that $\gcd(F_k, F_l) = 1$, whenever $k \neq l$. For the proof we refer to [28, Chapter 1, Thm. 13]. In this way a natural question arises. Whether this result is true for sequences $a_n = 2^{2^n} + d$ for odd integers d? In this respect we prove a theorem, which gives a negative answer to this question.

THEOREM **3.3** *For any integer $d \neq 1$ and positive integer m there exist distinct elements a_k and a_l in the sequence $a_n = 2^{2^n} + d$ such that $\gcd(a_k, a_l) > m$.*

3.1.1 Proof of Theorem 3.1

Suppose we have positive numbers $w_1, w_2, ..., w_n > 0$.

DEFINITION **3.3** *For any $W > 0$ we define*

$$N(W; w_1, w_2, ..., w_n) = \left| \left\{ (k_1, k_2, ..., k_n) \in (\mathbb{Z}_+)^n | \sum_{i=1}^{n} k_i w_i \leq W \right\} \right|.$$

LEMMA **3.1** $$\frac{W^n}{n! \prod_{i=1}^n w_i} \leq N(W; w_1, w_2, ..., w_n) \leq \frac{(W + \sum_{i=1}^n w_i)^n}{n! \prod_{i=1}^n w_i}.$$

Proof. Consider the lattice Λ in $\mathbb{R}^n$, spanned over the basis $\{w_1 e_1, ..., w_n e_n\}$, where $\{e_1, ..., e_n\}$ is the standard basis of $\mathbb{R}^n$. Define

$$\Pi_r = \{(x_1, x_2, ..., x_n) \in (\mathbb{R}_+)^n | \sum_{i=1}^{n} x_i \leq r\} \subset \mathbb{R}^n$$

for any $r > 0$. Then $N(W; w_1, w_2, ..., w_n) = |\Lambda \cap \Pi_W|$ is the number of lattice points in the simplex Π_W.

Now for any point $x = (x_1, x_2, ..., x_n) \in \Lambda \cap \Pi$ (i.e. for any solution) construct an open parallelotope $\Pi_x = \{(t_1, ..., t_n) | |t_i - x_i| < w_i/2, i = 1, 2, ..., n\} \subset \mathbb{R}^n$ with a center at that point. Note that
$\Pi_x \cap \Pi_y = \emptyset, \mathbb{V}(\Pi_x) = \prod_{i=1}^{n} w_i$ for all $x, y \in \Lambda \cap \Pi_W,\ x \neq y$,
where $\mathbb{V}$ stands for the volume.
Set $\Delta = \sum_{i=1}^{n} w_i, v = (w_1/2, ..., w_n/2) \in \mathbb{R}^n$ and $\Pi_{r,v} = \{x - v | x \in \Pi_r\}$ (the shift of Π_r by vector v).
Note that $\Pi_W \subset \bigcup_{x \in \Lambda \cap \Pi_W} \Pi_x \subset \Pi_{W+\Delta, v}$.
Comparing volumes yields $\frac{W^n}{n!} \leq N(W; w_1, w_2, ..., w_n) \prod_{i=1}^{n} w_i \leq \frac{(W + \sum_{i=1}^n w_i)^n}{n!}$. It remains only to divide all the parts of the inequality by $\prod_{i=1}^{n} w_i$. □

One can find additional information concerning Lemma 3.1 in [31].

DEFINITION **3.4** *For any positive integer l we set $t_l = |\{k|n_k(S) \leq l\}|$.*

Observe that due to Definition 2

$$t_l = \left|\left\{(k_1, k_2, ..., k_n) \in (\mathbb{Z}_+)^n | \prod_{i=1}^{n} p_i^{k_i} \leq l\right\}\right| =$$

$$= \left|\left\{(k_1, k_2, ..., k_n) \in (\mathbb{Z}_+)^n | \sum_{i=1}^{n} \ln(p_i)k_i \leq \ln(l)\right\}\right| =$$

$$= N(\ln(l); \ln(p_1), \ln(p_2), ..., \ln(p_n)).$$

As a consequence of Lemma 3.1 we get that there exist constants $c_1 > 0$ and $c_2 > 0$ such that $c_1 W^n < N(W; w_1, w_2, ..., w_n) < c_2 W^n$ for all $W > \ln(2)$. Therefore, for some constants $a > 0$ and $b > 0$ the inequality

$$a(\ln(l))^n < N(\ln(l); \ln(p_1), \ln(p_2), ..., \ln(p_n)) < b(\ln(l))^n$$

holds for all $l \geq 2$. Substituting $l = n_k(S)$ for $k = 2, 3, ...$, we obtain

$$a(\ln(n_k(S)))^n < t_{n_k(S)} < b(\ln(n_k(S)))^n$$

and, therefore $\ln(a) + n\ln(\ln(n_k(S))) < \ln(t_{n_k(S)}) < \ln(b) + n\ln(\ln(n_k(S)))$. Using that $(n_k(S))_{k=1}^{\infty}$ is an increasing sequence, we conclude that $t_{n_k(S)} = k$ for all k. As a result

$$\ln(a) + n\ln(\ln(n_k(S))) < \ln(k) < \ln(b) + n\ln(\ln(n_k(S)))$$

for all $k \geq 2$ and so

$$\limsup_{k\to\infty} \frac{\ln(\ln(n_k(S)))}{\ln(k)} \leq 1/n \leq \liminf_{k\to\infty} \frac{\ln(\ln(n_k(S)))}{\ln(k)},$$

which shows that $\lim_{k\to\infty} \frac{\ln(\ln(n_k(S)))}{\ln(k)} = \frac{1}{n}$. □

COROLLARY **3.1** *If $(n_k)_{k=1}^{\infty}$ is an increasing sequence of positive integers and $\liminf_{k\to\infty} \frac{\ln(\ln(n_k))}{\ln(k)} = 0$, then it is distinguished.*

REMARK **3.1** *A close result was previously proved in [27]. The result was formulated for almost injective sequences, i.e. for the sequences $(n_k)_{k=1}^{\infty}$ of positive integers for which there exists a constant C such that $|\{k|n_k = m\}| \leq C$ for all positive integers m. The concept of almost injective sequences was inspired by non-constant polynomials P, since they attain any value at most $C = \deg(P)$ times. Our result is independent of [27].*

Proof. Suppose the opposite is true. This means that there is a finite set S of prime numbers such that $(n_k)_{k=1}^{\infty}$ is a subsequence of $(n_k(S))_{k=1}^{\infty}$. Hence

$$\liminf_{k\to\infty} \frac{\ln(\ln(n_k))}{\ln(k)} \geq \liminf_{k\to\infty} \frac{\ln(\ln(n_k(S)))}{\ln(k)} = \frac{1}{|S|} > 0,$$

which is a contradiction. □

COROLLARY **3.2** *For any non-constant polynomial P with integer coefficients the sequence $(P(n))_{n=1}^{\infty}$ is distinguished.*

Proof. The sequence $(P(n))_{n=1}^{\infty}$ is eventually increasing and $\lim_{n\to\infty} \frac{\ln(\ln(P(n)))}{\ln(n)} = 0$, so that it remains to use Corollary 3.1. □

We would also like to give a purely number theoretic proof of this fact.

Proof. Suppose that the finite set $S = \{p_1, p_2, ..., p_n\}$ contains all possible prime factors of all numbers $P(n)$, $n \in \mathbb{N}$, where P is the given polynomial. For $j \in \{1, 2, .., n\}$ we define $k_j = \min_{n\in\mathbb{N}} \nu_{p_j}(P(n))$. Suppose also that $k_j = \nu_{p_j}(P(s_j))$ for each $j \in \{1, 2, .., n\}$. By the Chinese Remainder Theorem, there is a positive integer n such that $n \equiv s_j(\mod {p_j}^{k_j+1})$ for all $j \in \{1, 2..., n\}$. From this it follows that $P(n) \equiv P(s_j)(\mod {p_j}^{k_j+1})$ for all $j \in \{1, 2..., n\}$. Consequently, $P(n)$ is not divisible by ${p_j}^{k_j+1}$ for all $j \in \{1, 2..., n\}$. Hence, $P\Big(n + s\prod_{j=1}^{n} {p_j}^{k_j+1}\Big)$ is not divisible by ${p_j}^{k_j+1}$ for all $j \in \{1, 2..., n\}$ and $s \in \mathbb{N}$. As a result we obtain $P\Big(n + s\prod_{j=1}^{n} {p_j}^{k_j+1}\Big) \leq \prod_{j=1}^{n} {p_j}^{k_j}$ for all $s \in \mathbb{N}$. The latter assertion contradicts the fact that P is a non constant polynomial. □

3.1.2 Proof of Theorem 3.2

Assume the contrary that the sequence $(n_k)_{k=1}^{\infty}$ is not distinguished. Then there is a finite set $S = \{p_1, p_2, ..., p_s\}$, consisting of prime numbers such that any term of the sequence $(n_k)_{k=1}^{\infty}$ is a product of some elements (not necessarily distinct) from the set S. As the sequence $(n_k)_{k=1}^{\infty}$ tends to infinity, it is unbounded, so there is at least one prime $p \in S$ such that the sequence $(\nu_p(n_k))_{k=1}^{\infty}$ is unbounded, where $\nu_p(m) = \max\{k | m \vdots p^k\}$ for any integer m and prime p. WLOG we may assume that the set of all such primes $p \in S$ is $\{p_1, p_2, ..., p_l\}$, for some $1 \leq l \leq s$.

DEFINITION **3.5** *For any $1 \leq t \leq l$ and $M \in \mathbb{N}$ we define*

$$A_t(M) \triangleq \{k | \nu_{p_t}(n_k) > M\} = (s_{M,t,j})_{j=1}^{\infty}$$

and

$$L \triangleq \max\{\nu_{p_j}(n_k) | l+1 \le j \le s,\ k \in \mathbb{N}\} < \infty,$$

if $l < s$.

COROLLARY **3.3** *For each* $M \in \mathbb{N}$, *one has that* $\mathbb{N} = \bigcup_{t=1}^{l} A_t(M) \cup A_M$ *for the set*

$$A_M = \{k | \nu_{p_t}(n_k) \le M,\ t = 1, 2, ..., l\}.$$

It is finite, since $|A_M| \le \left| \left\{ k | n_k \le \prod_{i=1}^{l} p_i^M \cdot \prod_{j=l+1}^{s} p_j^L \right\} \right|$, *where the latter product* $T = \prod_{j=l+1}^{s} p_j^L$ *is assumed to be 1 if* $l = s$.

LEMMA **3.2** *For sufficiently large* M *the inequality* $s_{M,t,j+1} - s_{M,t,j} > l$ *holds for all* $t \in \{1, 2, ..., l\}$ *and* $j \in \mathbb{N}$.

Proof. We choose M large enough to satisfy $2^M > m_l$. Using that $p_t^M | n_{s_{M,t,j+1}}$ and $p_t^M | n_{s_{M,t,j}}$ we deduce that $m_{(s_{M,t,j+1} - s_{M,t,j})} > \gcd(n_{s_{M,t,j+1}}, n_{s_{M,t,j}}) \ge {p_t}^M \ge 2^M > m_l$. Without loss of generality, we may assume that the sequence $\left(m_t\right)_{t=1}^{\infty}$ is increasing, which yields the inequality $s_{M,t,j+1} - s_{M,t,j} > l$, thereby proving the lemma. □

Consequently for all $t \in \{1, 2, ..., l\}$, $N \in \mathbb{N}$, and sufficiently large M,

$$|A_t(M) \cap \{1, 2, ..., N\}| \le \left[\frac{N}{l+1}\right] + 1,$$

where $[x]$ stands for the integer part of $x \in \mathbb{R}$. Therefore, for a fixed sufficiently large M

$$|A_M| \ge |\{1, 2, ..., N\} \setminus \bigcup_{t=1}^{l} A_t(M)| \ge$$

$$\ge N - \sum_{t=1}^{l} |A_t(M) \cap \{1, 2, ..., N\}| \ge N - l\left(\left[\frac{N}{l+1}\right] + 1\right) \ge \frac{N}{l+1} - l$$

for each positive integer N. From this inequality we infer that A_M is infinite, which is contrary to Corollary 3.3. The Proof of Theorem 2 is complete. □

3.1.3 Proof of Theorem 3.3

Suppose that there is an integer $d \neq 1$ and a positive integer m such that $\gcd(a_k, a_l) \leq m$ for all distinct elements a_k and a_l of this sequence. It follows that if for some positive integer ν and distinct positive integers k and l, $p^\nu | a_k$ and $p^\nu | a_l$, then $p^\nu \leq \gcd(a_k, a_l) \leq m$. Consequently for each prime p the sequence $(\nu_p(a_n))_{n=1}^\infty$ is bounded. Let us prove some auxiliary lemmas.

LEMMA **3.3** *If positive integers n and k are given, which satisfy $\nu_2(k) < n$, then there is a positive integer $l > n$ such that $(2^l - 2^n) \vdots k$.*

Proof. Let $k = 2^a b$, where $a = \nu_2(k) < n$ and b be an odd number. Since

$$b | 2^{\phi(b)} - 1$$

(ϕ is the Euler's totient function), we get that $(2^{n+\phi(b)} - 2^n) \vdots 2^n b \vdots 2^a b = k$. We now set $l = n + \phi(b)$. The Lemma is proved. □

LEMMA **3.4** *If for some prime $p > m$ and positive integer n the relation $p | a_n$ holds, then $p \equiv 1 (mod\ 2^n)$.*

Proof. Suppose $p \not\equiv 1 (\mathrm{mod}\ 2^n)$. Then by Lemma 3.3 there is some positive integer $l > n$, such that $(2^l - 2^n) \vdots (p-1)$. Consequently,
$a_l - a_n = 2^{2^l} - 2^{2^n} = 2^{2^n}(2^{2^l - 2^n} - 1) \vdots 2^{2^n}(2^{p-1} - 1) = 2^{2^n - 1}(2^p - 2) \vdots p$
by Fermat's little theorem. Since $p | a_n$, we thus get that $p | a_l$, and so

$$p \leq \gcd(a_n, a_l) \leq m,$$

which contradicts the conditions of the Lemma. □

LEMMA **3.5** *$|d|$ is a power of 2.*

Proof. Let $a_n = 2^{k_n} b_n c_n$ for any positive integer n, where the prime divisors of b_n are precisely the odd prime divisors of a_n, which are less or equal to m. If there is no such prime, we set $b_n = 1$. From Lemma 3.4 it follows that $c_n \equiv 1 (\mathrm{mod}\ 2^n)$ and so $a_n \equiv 2^{k_n} b_n (\mathrm{mod}\ 2^n)$. On the other hand, $a_n = 2^{2^n} + d \equiv d (\mathrm{mod}\ 2^n)$, hence $2^{k_n} b_n \equiv d (\mathrm{mod}\ 2^n)$. As the number of primes not exceeding m is finite, and the sequence $(\nu_p(a_n))_{n=1}^\infty$ is bounded for each prime p, there exists some positive integer

M such that $2^{k_n}b_n \leq M$ for all $n \in \mathbb{N}$. In the long run we get $2^{k_n}b_n = d$ for all sufficiently large n (in particular $d \neq 0$, which was clear). From this we infer that

$$2^{2^n} + d = a_n = 2^{k_n}b_nc_n = dc_n \vdots d$$

and, therefore, $d|2^{2^n}$ for all sufficiently large $n \in \mathbb{N}$. □

LEMMA **3.6** *For any sufficiently large positive integer n there is a positive integer $l_n > n$ such that $a_{l_n} \vdots a_n$.*

Proof. For $d = -1$ one has that $a_{n+1} = 2^{2^{n+1}} - 1 \vdots 2^{2^n} - 1 = a_n$ and we are done. Suppose now $d \neq \pm 1$. In accordance with Lemma 3.5, $d = \pm 2^k$ for some positive integer k. Let us choose a positive integer $n > \nu_2(k)$, then $\nu_2(2^n - k) = \nu_2(k)$. Choose $l_n > n$ from Lemma 3.3, then $(2^{l_n} - 2^n) \vdots (2^n - k)$, and thereby $(2^{l_n} - k) \vdots (2^n - k)$. Since $\nu_2(2^{l_n} - k) = \nu_2(k) = \nu_2(2^n - k)$, the quotient $\dfrac{2^{l_n} - k}{2^n - k}$ is an odd integer, which means that

$$(2^{2^{l_n} - k} \pm 1) \vdots (2^{2^n - k} \pm 1).$$

Multiplying by 2^k, we obtain $a_{l_n} \vdots a_n$, depending on whether $d = 2^k$ or $d = -2^k$. □

One can infer from Lemma 3.6, that $a_n = \gcd(a_n, a_{l_n}) \leq m$ for $n > \nu_2(k)$, which is a contradiction. □

3.2 Some analytic estimates for the divisor τ-function

The function $\tau(n)$ defined as the number of positive divisors of the given positive integer n has many investigated asymptotic properties and some of them are presented below.

1. For any $\varepsilon > 0$, $\tau(n) = o(n^{\varepsilon})$.

2. For given $\varepsilon > 0$ there exist infinitely many positive integers n such that $\tau(n) > 2^{(1-\varepsilon)(\ln n)/(\ln(\ln n))}$. Moreover, $\tau(n) < 2^{(1+\varepsilon)(\ln n)/\ln(\ln n)}$ holds for sufficiently large n (Vigert, 1907).

3. Let $D(x) = \sum_{n \leq x} \tau(n)$ be the summatory function of τ. Dirichlet proved the asymptotic equality

$$D(x) = x \ln x + (2\gamma - 1)x + O(x^{1/2}),$$

where γ is the Euler's constant. Dirichlet's divisor problem consists of determining the smallest α for which the error term is $O(n^{\alpha+\epsilon})$ for any $\varepsilon > 0$. G.Voronoi has showed that $\alpha \leq 1/3$, while

Hardy and Gauss proved that the error term is not $O(x^{1/4})$, and therefore $\alpha \geq 1/4$. It is conjectured that $\alpha = 1/4$.

For (1)–(3) we refer to [28, Chapter 6, §3].

4. It is worth mentioning the result in [32] concerning Karatsuba's problem on determining the asymptotic behavior of the sum
$$S_a(x) = \sum_{n \leq x} \frac{\tau(n)}{\tau(n+a)}$$
stated in 2004 which was estimated by M. A. Korolev in 2010.

5. In [33], the average behavior of the function $\tau_k(n)$ is studied, where for each positive integer n, $\tau_k(n)$ is defined as the number of solutions of the equation $m_1 m_2 ... m_k = n$ in positive integers $m_1, m_2, ..., m_k$.

For $\mu > 0$ consider the sequence

$$T_n(\mu) = (\tau(n))^{-1} \max_{1 \leq t \leq [n^{1/\mu}]} \{\tau(n+t)\}, \ n = 1, 2, ...$$

and define

$$\theta = \inf\{\lambda > 0 | D(x) = x \ln x + (2\gamma - 1)x + O(x^{\lambda})\},$$

where $D(x) = \sum_{n \leq x} \tau(n)$ is the summatory function of τ. Assume that $(n_k)_{k=1}^{\infty}$ is a sequence of positive integers such that $n_k = {p_k}^{j_k}$, where p_k is prime and $j_k \in \mathbb{N}$ for all positive integers k. In this section we prove the following theorem.

THEOREM **3.4** ***a)*** *If $\mu > 0$, then $T_{n_k}(\mu) \to \infty$, as $j_k \to \infty$;* ***b)*** *If $1 \leq \mu < \theta^{-1}$, then $T_{n_k}(\mu) \to \infty$, as $n_k \to \infty$.*

Note that if Theorem 3.4 holds for some $\mu_0 > 0$ then it holds for any $0 < \mu < \mu_0$. Hence one may assume that $\mu > 1$ is a fixed integer.

DEFINITION **3.6** *For any positive integer n and prime number p we define* $\nu_p(n) = \max\{k \geq 0 | n \vdots p^k\}$ *and* $\Delta(n) = \sum_{p|n} \nu_p(n)$.

It is immediate that $\Delta(mn) = \Delta(m) + \Delta(n)$, $\Delta(n^k) = k\Delta(n)$, for any positive integers m, n, k. Observe that for any integer $0 \leq s < \mu m$ and prime number p

$$\tau(p^{\mu m} + p^s) = (s+1)\tau(p^{\mu m - s} + 1).$$

We start with the following

PROPOSITION **3.1** *If $n = 2^t a$, where a is odd, then $\tau(p^n + 1) \geq \tau(a) \geq \Delta(a)$.*

Proof. Indeed, if $a \vdots b$ then $(p^n + 1) \vdots (p^{2^t b} + 1)$, hence the left part of the inequality holds. On the other hand, the right part of the inequality follows from

$$\tau(a) = \prod_{p|a}(1 + \nu_p(a)) > \sum_{p|a} \nu_p(a) = \Delta(a),$$

where p ranges through the set of prime divisors of a. □

The following lemma enables us to estimate $\Delta(m!)$ from above.

LEMMA **3.7** *The inequality $\Delta(m!) < 2m \ln(\ln m)$ holds for sufficiently large positive integer m.*

Proof. Using the famous identity $\nu_p(n!) = \sum_{s=1}^{\infty} [np^{-s}]$ (henceforth $[x]$ stands for the integer part of $x \in \mathbb{R}$) and the asymptotic equality

$$\sum_{\{p \leq x | p \text{ is prime}\}} p^{-1} = \ln(\ln x) + O(1) \text{ (see [34], Exercise 3.1.8)}$$

we get

$$\Delta(m!) = \sum_{p \leq m} \nu_p(m!) = \sum_{p \leq m} \sum_{s=1}^{\infty} \left[mp^{-s}\right] < \sum_{p \leq m} \frac{m}{p-1} =$$

$$= m \left(\sum_{p \leq m} p^{-1} + \sum_{p \leq m} \frac{1}{p(p-1)} \right) < m \left(\sum_{p \leq m} p^{-1} + h \right) < 2m \ln(\ln m)$$

for sufficiently large positive integer m, where $h = \sum_p (p(p-1))^{-1}$. The lemma is proved. □

DEFINITION **3.7** *We define $A(m) = \sum_{s=1}^{m} (s+1)\Delta(\mu m - s)$ and $A'(m) = \prod_{s=1}^{m} (\mu m - s)^{s+1}$.*

Observe that

$$A'(m) = \prod_{s=1}^{m} (\mu m - s)^{s+1} = \frac{(\mu m - 1)!}{((\mu - 1)m - 1)!} \prod_{s=1}^{m} \frac{(\mu m - s)!}{((\mu - 1)m - 1)!}$$

and

$$A(m) = \Delta(A'(m)) = B(m) + C(m),$$

where

$$B(m) = \Delta\left(\frac{(\mu m - 1)!}{((\mu - 1)m - 1)!} \right) \quad \text{and} \quad C(m) = \Delta\left(\prod_{s=1}^{m} \frac{(\mu m - s)!}{((\mu - 1)m - 1)!} \right).$$

LEMMA **3.8** *The inequality $A(m) > (1/4)m^2 \ln(\ln m)$ holds for sufficiently large positive integer m.*

Proof. Recall that $A(m) = B(m) + C(m)$ and

$$B(m) = O(m \ln(\ln m)) = o(m^2 \ln(\ln m))$$

by Lemma 3.7. On the other hand

$$C(m) = \sum_{l=(\mu-1)m}^{\mu m-1} \sum_{p \le \mu m-1} \left(\sum_{s=1}^{\infty} \left[\frac{l}{p^s} \right] - \sum_{s=1}^{\infty} \left[\frac{(\mu-1)m-1}{p^s} \right] \right) \ge$$

$$\ge \sum_{l=(\mu-1)m}^{\mu m-1} \sum_{p \le \mu m-1} \left(\sum_{s=1}^{\infty} \left[\frac{l-(\mu-1)m+1}{p^s} \right] \right),$$

which together with the inequality

$$\sum_{s=1}^{\infty} \left[\frac{n}{p^s} \right] > \sum_{s=1}^{[\log_p n]} \frac{n}{p^s} - [\log_p n] \ge \frac{n-1}{p-1} - \log_p(np)$$

yields

$$C(m) \ge \sum_{p \le \mu m-1} \left(\sum_{k=1}^{m-1} \frac{k}{p-1} - \log_p \left(\prod_{k=2}^{m} kp \right) \right) = X(m) - Y(m) - Z(m),$$

where for $x > 0$, $\pi(x)$ is the number of primes not exceeding x,

$$X(m) = \frac{m(m-1)}{2} \sum_{p \le \mu m-1} \frac{1}{p-1}, \quad Y(m) = (m-1)\pi(\mu m - 1),$$

$$\text{and } Z(m) = \sum_{p \le \mu m-1} \log_p(m!).$$

Using the asymptotic equality

$$\sum_{\{p \le x | p \text{ is prime}\}} p^{-1} = \ln(\ln x) + O(1)$$

we infer that

$$X(m) = \frac{m(m-1)}{2} \sum_{p \le \mu m-1} (p-1)^{-1} > \frac{m(m-1)}{2} \sum_{p \le \mu m-1} p^{-1} =$$

$$= \frac{m(m-1)}{2} (\ln(\ln(\mu m - 1)) + O(1)) > \frac{1}{3} m^2 \ln(\ln m)$$

for sufficiently large m. Furthermore,

$$Y(m) = (m-1)\pi(\mu m - 1) \le (m-1)(\mu m - 1) = o(m^2 \ln(\ln m))$$

and

$$Z(m) = \sum_{p \le \mu m - 1} \log_p(m!) = \ln(m!) \sum_{p \le \mu m - 1} \frac{1}{\ln p} \le$$

$$\le \ln(m!) \left((\ln(2))^{-1} + \int_2^{\mu m - 1} \frac{dt}{\ln(t)} \right) = O(m \ln m) O\left(m (\ln m)^{-1} \right) = o(m^2 \ln(\ln m)),$$

due to Stirling's asymptotic formula for $\ln(m!)$ and Prime Number Theorem, which states that the functions

$$\pi(x), \frac{x}{\ln x} \text{ and } Li(x) = \int_2^x \frac{dt}{\ln t}$$

are asymptotically equivalent at infinity (see [28, Chapter 11]).

In the long run

$$A(m) = B(m) + C(m) \ge X(m) + o(m^2 \ln(\ln m)) >$$

$$> \frac{1}{3} m^2 \ln(\ln m) + o(m^2 \ln(\ln m)) > \frac{1}{4} m^2 \ln(\ln m)$$

for sufficiently large positive integer m. The lemma is proved. □

REMARK **3.2** *From the proof of Lemma 3.8 it is evident that the constant* $1/4$ *can be made arbitrary close to* $1/2$.

We proceed with the following definition.

DEFINITION **3.8** *For arbitrary positive integer* $m > 1$ *and positive real number* $\beta > 0$ *we define*

$$I_\beta(m) = \sum_{\{1 \le s \le m | \nu_2(\mu m - s) > \beta \ln(\ln m)\}} (s+1) \Delta(\mu m - s).$$

LEMMA **3.9** *For every* $\beta > 0$, $I_\beta(m) = o(m^2 \ln(\ln m))$.

Proof. If $1 \le s \le m$ and $\mu m - s = 2^l a$, for some odd a and $l > \beta \ln(\ln m)$, then $a < L_\beta(m) = \mu m 2^{-\beta \ln(\ln m)}$. Observe that $(\mu - 1)m \le \mu m - s \le \mu m - 1$, which implies that for fixed a there is at most one value of l such that $(\mu - 1)m \le a 2^l \le \mu m - 1$. Consequently, there are at most $L^*_\beta(m) \le L_\beta(m)$ summands with $\nu_2(\mu m - s) > \beta \ln(\ln m)$. Let us number them, say $s_1, s_2, \ldots, s_{L^*_\beta(m)}$ and write $\mu m - s_j = 2^{l_j} a_j$, where a_j is odd and $l_j > \beta \ln(\ln m)$ for every $j \in \{1, 2, \ldots, L^*_\beta(m)\}$. Observe that

$$I_\beta(m) = \sum_{j=1}^{L^*_\beta(m)} (s_j + 1) \Delta(\mu m - s_j) = I_{1,\beta}(m) + I_{2,\beta}(m),$$

where

$$I_{1,\beta}(m) = \sum_{j=1}^{L^*_\beta(m)} (s_j+1)l_j \text{ and } I_{2,\beta}(m) = \sum_{j=1}^{L^*(m)} (s_j+1)\Delta(a_j).$$

To estimate $I_{1,\beta}(m)$ we denote

$$T_{m,\beta} = \{[\beta \ln(\ln m)]+1, [\beta \ln(\ln m)]+2, \ldots, [\log_2(\mu m)]\}$$

for sufficiently large m. It is clear that $l_j \in T_{m,\beta}$ for every $j \in \{1,2,\ldots,L^*_\beta(m)\}$.

We fix some $t \in T_{m,\beta}$ and consider those s for which $\mu m - s = 2^t a$, where a is odd. Notice that a takes values from a progression with difference $d=2$, so that $2^t a$ takes values from a progression with difference $d = 2^{t+1}$. Hence the inequality

$$S(m,d) = \sum_{\{\nu_2(\mu m - s)=t\}} (\mu m - s) \le \sum_{l=1}^{k+1} ((\mu-1)m + ld)$$

holds where k is the unique integer satisfying $kd \le m < (k+1)d$, i.e. $k = [m/d]$. Therefore

$$S(m,d) \le (k+1)(\mu-1)m + \frac{k(k+1)}{2}d + (k+1)d \le$$

$$\le (\mu-1)\frac{m^2}{d} + (\mu-1)m + \frac{m}{2}\left(\frac{m}{d}+1\right) + \left(\frac{m}{d}+1\right)d =$$

$$\le \left(\mu - \frac{1}{2}\right)\frac{m^2}{d} + \left(\mu+\frac{3}{2}\right)m,$$

which yields

$$\sum_{l_j=t} s_j l_j \le t\left(\left(\mu-\frac{1}{2}\right)\frac{m^2}{2^{t+1}} + \left(\mu+\frac{3}{2}\right)m\right)$$

for all $t \in T_{m,\beta}$. Thereby

$$I_{1,\beta}(m) = \sum_{j=1}^{L^*_\beta(m)} s_j l_j + \sum_{j=1}^{L^*_\beta(m)} l_j = \sum_{t\in T_{m,\beta}} \sum_{l_j=t} s_j l_j + \sum_{j=1}^{L^*_\beta(m)} l_j \le$$

$$\le \sum_{t\in T_{m,\beta}} t\left(\left(\mu-\frac{1}{2}\right)\frac{m^2}{2^{t+1}} + \left(\mu+\frac{3}{2}\right)m\right) + L_\beta(m)\log_2(\mu m) \le$$

$$\le \left(\mu-\frac{1}{2}\right)m^2 \sum_{t\in T_{m,\beta}} \frac{t}{2^{t+1}} + \left(\mu+\frac{3}{2}\right)m \sum_{t\in T_{m,\beta}} t + \mu m \log_2(\mu m) \le$$

$$\le \left(\mu-\frac{1}{2}\right)m^2\theta_m + \left(\mu+\frac{3}{2}\right)m\log_2^2(\mu m) + \mu m \log_2(\mu m) = o(m^2 \ln(\ln m)),$$

since $\theta_m = \sum_{t\in T_{m,\beta}} t2^{-(t+1)} \to 0$.

In order to estimate $I_{2,\beta}(m)$ observe that

$$I_{2,\beta}(m) = \sum_{j=1}^{L^*_\beta(m)} (s_j+1)\Delta(a_j) \le \sum_{j=1}^{L^*_\beta(m)} (m+1)\Delta(a_j) \le$$

$$\le (m+1) \sum_{j=1}^{[L_\beta(m)]} \Delta(j) \le 2(m+1)L_\beta(m)\ln(\ln L_\beta(m))$$

by Lemma 1 and the inequality $a_j \le [L_\beta(m)]$ for all $j \in \{1,2,\dots,L^*_\beta(m)\}$, therefore in accordance with the equality $L_\beta(m) = \mu m 2^{-\beta\ln(\ln m)}$ we get

$$I_{2,\beta}(m) \le Cm^2\ln(\ln m)2^{-\beta\ln(\ln m)} = o(m^2\ln(\ln m)).$$

In the long run we end up with the asymptotic equality

$$I_\beta(m) = I_{1,\beta}(m) + I_{2,\beta}(m) = o(m^2\ln(\ln m)),$$

which terminates the proof of the lemma. □

COROLLARY **3.4** *For sufficiently large positive integer m it is always possible to select an $s_0 \in \{1,2,\dots,m\}$ such that*

$$\nu_2(\mu m - s_0) \le \frac{1}{16}\ln(\ln m) \quad \textit{and} \quad (s_0+1)\Delta(\mu m - s_0) \ge \frac{1}{4}m\ln(\ln m).$$

Proof. Define $I^*_{1/16}(m) = A(m) - I_{1/16}(m)$. According to Remark 3.2 and Lemma 3.9, the inequality $I^*_{1/16}(m) \ge (1/4)m^2\ln(\ln m)$ holds for sufficiently large m. We choose an s_0, satisfying $\nu_2(\mu m - s_0) \le \frac{1}{16}\ln(\ln m)$, which maximizes the expression $(s_0+1)\Delta(\mu m - s_0)$ and deduce that

$$(s_0+1)\Delta(\mu m - s_0) \ge \frac{I^*_{1/16}(m)}{m} \ge \frac{1}{4}m\ln(\ln(m)).$$

□

3.2.1 Proof of Theorem 3.4

a) We choose sufficiently large positive integer m and an s_0 satisfying the conditions of Corollary 3.4. In other words, suppose $\mu m - s_0 = 2^t a$, where a is odd, $1 \le t \le (1/16)\ln(\ln m)$ and $(s_0+1)\Delta(\mu m - s_0) \ge (1/4)m\ln(\ln m)$. Hence

$$\Delta(\mu m - s_0) \ge \frac{1}{4}\frac{m\ln(\ln m)}{s_0+1} \ge \frac{m}{4(m+1)}\ln(\ln m) \ge \frac{1}{8}\ln(\ln m) \ge 2t,$$

implying that

$$\frac{\Delta(a)}{\Delta(\mu m - s_0)} = 1 - \frac{t}{\Delta(\mu m - s_0)} \geq \frac{1}{2}.$$

Therefore

$$\tau(p^{\mu m} + p^{s_0}) = (s_0 + 1)\tau(p^{2^t a} + 1) \geq (s_0 + 1)\Delta(a)$$
$$\geq \frac{1}{4} m \ln(\ln m) \frac{\Delta(a)}{\Delta(\mu m - s_0)} \geq \frac{1}{8} m \ln(\ln m),$$

where we used the inequality $\tau(p^{2^t a} + 1) \geq \Delta(a)$, which is true by Proposition 3.1. On the other hand from the proofs of Lemma 3.8 and Lemma 3.9 it is clear that we may assume $s_0 > 2\mu$. Therefore for any integer r, $0 \leq r \leq \mu - 1$,

$$\tau(p^{\mu m - r} + p^{s_0 - r}) = \frac{s_0 - r + 1}{s_0 + 1} \tau(p^{\mu m} + p^{s_0}) \geq$$
$$\geq \frac{1}{2} \tau(p^{\mu m} + p^{s_0}) \geq \frac{1}{16} m \ln(\ln m).$$

Observe that $\mu(s_0 - r) \leq \mu m - \mu r < \mu m - r$, which shows that if $n_k = p_k^{j_k}$, where p_k is prime and j_k is a positive integer for each k, then

$$T_{n_k}(\mu) \geq \frac{[j_k/\mu] \ln(\ln[j_k/\mu])}{16(j_k + 1)} \to \infty, \text{ when } j_k \to \infty, \text{ as desired. } \square$$

b)

LEMMA **3.10** *If $1 \leq \mu < \theta^{-1}$, then there exists a constant $c > 0$ such that $T_n(\mu) > c(\tau(n))^{-1} \ln n$ for all positive integers n.*

Proof. Fix any ε, satisfying $0 < \varepsilon < \mu^{-1} - \theta$ and apply the formula

$$\sum_{k=1}^{n} \tau(k) = n \ln n + (2\gamma - 1)n + O(n^{\theta + \varepsilon})$$

to get

$$\sum_{k=n+1}^{n + \lceil n^{1/\mu} \rceil} \tau(k) = n^{1/\mu} \ln n + O(n^{1/\mu}) + O(n^{\theta+\varepsilon}) = n^{1/\mu} \ln n + O(n^{1/\mu}).$$

Therefore there exists a constant $c > 0$ such that the inequality

$$\max_{1 \leq t \leq \lceil n^{-1/\mu} \rceil} \{\tau(n + t)\} \geq n^{-1/\mu} \sum_{k=n+1}^{n + \lceil n^{1/\mu} \rceil} \tau(k) = \frac{n^{1/\mu} \ln n + O(n^{1/\mu})}{n^{1/\mu}} > c \ln n,$$

holds for any positive integer n, which yields

$$T_n(\mu) = (\tau(n))^{-1} \max_{1 \leq t \leq \lceil n^{1/\mu} \rceil} \{\tau(n + t)\} > c(\tau(n))^{-1} \ln n$$

for all positive integers n. The lemma is proved. $\square$

Suppose $(n_k)_{k=1}^{\infty}$ is a sequence of positive integers such that $n_k = {p_k}^{j_k}$, where p_k is prime, j_k is a positive integer for each $k \in N$ and $n_k \to \infty$ as $k \to \infty$. Assume $E > 0$ is an arbitrary number. According to Theorem 3.4 a) there is an $A > 0$ such that $j_k > A$ implies $T_{n_k}(\mu) > E$. Lemma 3.10 shows that

$$T_{n_k}(\mu) > c\frac{\ln n_k}{\tau(n_k)} = c\frac{j_k \ln p_k}{j_k + 1} \geq \frac{1}{2} c \ln p_k.$$

So there is some $B > 0$ such that $p_k > B$ implies $T_{n_k}(\mu) > E$.

The condition $n_k \to \infty$ shows that there are only finitely many positive integers k, such that $j_k \leq A$ and $p_k \leq B$. Hence there exists a positive integer $k = k(E)$ such that $T_{n_k}(\mu) > E$ for any positive integer $k > k(E)$.

Since E was arbitrary, we conclude that $T_{n_k}(\mu) \to \infty$ as $k \to \infty$. The theorem is proved. □

In this respect the following conjecture was stated in [35]

CONJECTURE **3.1** $\lim_{n\to\infty} T_n(\mu) = \infty$ *for any* $\mu > 0$.

Conclusion

Summarizing what has been said, it can be noted that the following main results were obtained in the thesis.

1. The structure of the $\mathbb{F}_p[\mathrm{Gal}(K/k)]$-module $V = E/E^p$ was studied in the case of cyclic extensions K/k of local fields of prime degree p, where E is the group of principal units in K.

2. Generating elements and defining relations for the $\mathcal{O}_{K_0}[\mathrm{Gal}(M/L)]$-module $F(\mathfrak{p}_M)$ were found in the case of unramified cyclic p-extensions M/L of local fields and Honda formal groups $F/\mathcal{O}_K$ relative to the unramified extension K/K_0.

3. It was proved that a sequence $A = (a_n)_{n=1}^{\infty}$ of positive integers is distinguished as soon as it satisfies one of the conditions listed below

   - $\liminf\limits_{n\to\infty} \dfrac{\ln(\ln(a_n))}{\ln(n)} = 0$ and A is increasing.
   - $\lim\limits_{n\to\infty} a_n = \infty$ and there is a sequence $(b_n)_{n=1}^{\infty}$ such that $\gcd(a_k, a_{k+l}) < b_l$ for all k and l.

4. It was proved that if d is any integer different from 1, then for any $M > 0$ there exist distinct positive integers m and n such that $\gcd(2^{2^m} + d, 2^{2^n} + d) > M$.

5. It was proved that if $A = (n_k)_{k=1}^{\infty}$ is a sequence of positive integers each term of which is a power of a prime, namely $n_k = p_k^{m_k}$, where p_k is prime for all k, then

   - If $\mu > 0$, then $T_{n_k}(\mu) \to \infty$, as $m_k \to \infty$.
   - If $1 \le \mu < \theta^{-1}$, then $T_{n_k}(\mu) \to \infty$, as $n_k \to \infty$.

   where

   $$T_n(\mu) = (\tau(n))^{-1} \max_{1\le t\le \left[n^{1/\mu}\right]} \{\tau(n+t)\},\ n = 1, 2, ...,$$

   $$\theta = \inf\{\lambda > 0 | D(x) = x\ln x + (2\gamma - 1)x + O(x^{\lambda})\}$$

   and $D(x) = \sum_{n\le x} \tau(n)$ is the summatory function of τ.

Bibliography

[1] Serge Lang, *Algebra* (Springer, 2002).

[2] С. В. Востоков, *Идеалы абелева p-расширения локального поля как модули Галуа*, Зап. научн. сем. ЛОМИ, **57**(1976), 64–84.

[3] З. И. Боревич, С. В. Востоков, *Кольцо целых элементов расширения простой степени локального поля как модуль Галуа*, Зап. научн. сем. ЛОМИ, 31(1973), 24–37.

[4] K. Iwasawa, *On Galois groups of local fields.* Trans. Amer. Soc **80**, No.2 (1955), 448-469.

[5] K. Iwasawa, *On local cyclotomic fields.* J. Math. Soc. Japan **12**, No.1 (1960), 16-21.

[6] Д. К. Фаддеев, *К строению приведенной мультипликативной группы циклического расширения локального поля*, Изв. АН СССР. Сер. матем., **24**:2 (1960), 145–152.

[7] З. И. Боревич, *О мультипликативной группе циклических p- расширений локального поля.* Тр. МИАН СССР **80** (1965), 16-29.

[8] З. И. Боревич, *Мультипликативная группа регулярного поля с циклической группой операторов*, Изв. АН СССР. Сер. матем., **28**:3 (1964).

[9] T. Hakobyan, *On the reduced group of principal units in cyclic extensions of local fields*, Зап. научн. сем. ПОМИ, **455**(2017), 14–24.

[10] H. Hasse, *Number theory*, Springer, 1980.

[11] С. В. Востоков, И. И. Некрасов, *Формальный модуль Любина–Тейта в циклическом неразветвленном p-расширении как модуль Галуа.* Зап. научн. сем. ПОМИ, **430**, (2014), 61–66.

[12] Honda, Taira. *On the theory of commutative formal groups.* J. Math. Soc. Japan **22** (1970), No. 2, 213-246.

[13] О. В. Демченко, *Новое в отношениях формальных групп Любина–Тэйта и формальных групп Хонды*, Алгебра и анализ, **10**:5 (1998), 77–84.

[14] О. В. Демченко, *Формальные группы Хонды: арифметика группы точек.* Алгебра и анализ, **12**:1 (2000), 132–149.

[15] T. Hakobyan, S.Vostokov, *Honda formal group as Galois module in unramified extensions of local fields.*Preprint, arXiv:1810.01695, 2018.

[16] K. Iwasawa, *Local class field theory*, Oxford University Press, 1986.

[17] Jean-Pierre Serre, *Local fields* (Springer, 1979).

[18] S. V. Vostokov, I. B. Fesenko, *Local fields and their extensions*, American Mathematical Society, 1993.

[19] J. Neukirch, *Algebraic number theory*, Springer, 1999.

[20] J. Neukirch, *Class field theory*, Springer-Verlag, 1986.

[21] Michiel Hazewinkel, *Formal groups and applications*, Academic Press, New-York, 1978.

[22] A. Frohlich, *Formal groups* (Springer, 1968).

[23] Алгебраическая теория чисел, под редакцией Дж. Касселса и А. Фрелиха, М.: Мир, 1969.

[24] Jean-Pierre Serre, *Galois cohomology* (Springer, 1997).

[25] Polya G., Szego G., *Problems and Theorems in Analysis* p I, II. 1978, M.: Nauka.

[26] T. L. Hakobyan, *On the P_1 property of sequences of positive integers*, Уч. записки ЕГУ, сер. Физика и Математика, 2016, no. **2**, 22–27.

[27] Elsholtz Ch., *Prime divisors of thin sequences*, The American Mathematical Monthly, **119**:4 (2012), 331-333.

[28] K. Chandrasekharan, *Introduction to analytic number theory* (Springer, 1968).

[29] Б.Л.Ван-дер-Варден, *Алгебра*, М.: Мир,1976.-648с.

[30] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[31] Manfred W. P.,*A Remark on an Inequality for the Number of Lattice Points in a Simplex,* SIAM Journal on Applied Mathematics, **20**:4 (1971), 638-641.

[32] M. A. Korolev, *On Karatsuba's Problem Concerning the Divisor Function* $\tau(n)$, Monatsh. Math **168** (3-4), 403–441 (2012).

[33] A. A. Karatsuba, *Uniform approximation of the remainder term in the Dirichlet divisor problem,* Math. USSR-Izv. **6** (3), 467–475 (1972).

[34] E. Ram Murty, *Problems in analytical number theory* (Springer, 1998).

[35] T.Hakobyan, S.Vostokov, *On an asymptotic property of divisor* τ*-function,* Lobachevskii J Math (2018) **39**:1, 77-83.