# 4. Local Fields

**Definition 4.1.** Suppose $\mathcal{O}_1 \subset \mathcal{O}_2$ are Dedekind domains, $\mathfrak{p}_1 \subset \mathcal{O}_1$ and $\mathfrak{p}_2 \subset \mathcal{O}_2$ nonzero prime ideals such that $\mathfrak{p}_1 = \mathfrak{p}_2 \cap \mathcal{O}_1$.
1) Let $k_{\mathfrak{p}_1} = \mathcal{O}_1/\mathfrak{p}_1,\ k_{\mathfrak{p}_2} = \mathcal{O}_2/\mathfrak{p}_2$ be the residue fields. The inertia index or the residue class degree $f(\mathfrak{p}_2/\mathfrak{p}_1) \stackrel{\text{def}}{=} [k_{\mathfrak{p}_2} : k_{\mathfrak{p}_1}]$ ($f = \infty$ not excluded).
2) The ramification index $e(\mathfrak{p}_2/\mathfrak{p}_1) \stackrel{\text{def}}{=} \mathrm{v}_{\mathfrak{p}_2}(\mathfrak{p}_1\mathcal{O}_2)$ (clearly $e$ is finite).

**Theorem 4.2.** 1) Suppose $\mathcal{O}_1 \subset \mathcal{O}_2 \subset \mathcal{O}_3$ are three Dedekind domains, $\mathfrak{p}_i \subset \mathcal{O}_i$ such that the condition above holds for both extensions. Then $f(\mathfrak{p}_3/\mathfrak{p}_1) = f(\mathfrak{p}_3/\mathfrak{p}_2)f(\mathfrak{p}_2/\mathfrak{p}_1)$ if at least two of three are finite.
2) The same is true for $e$.
3) Suppose $\mathcal{O}_1 = \mathcal{O}_\mathfrak{p}$ is a d.v.r, $\mathcal{O}_2 = \widehat{\mathcal{O}}_\mathfrak{p}$ its completion. Then $f(\mathfrak{p}\widehat{\mathcal{O}}_\mathfrak{p}/\mathfrak{p}) = e(\mathfrak{p}\widehat{\mathcal{O}}_\mathfrak{p}/\mathfrak{p}) = 1$.

*Proof.* Hometask ■

From now on we always suppose $\mathcal{O}$ is a **complete d.v.r**, $\mathfrak{p}$ its maximal ideal, $k$ its field of fractions, $K/k$ a finite separable extension of degree $n$, $\mathcal{O}_K$ its valuation ring (recall that the $\mathfrak{p}$-adic absolute value on $k$ extends to $K$ in a unique way), $\mathfrak{P} \subset \mathcal{O}_K$ a unique maximal ideal, $k_\mathfrak{p}$ and $K_\mathfrak{P}$ corresponding residue fields. We also suppose that the extension $K_\mathfrak{P}/k_\mathfrak{p}$ is separable (this is not a direct consequence of $K/k$ being separable but still is fulfilled in the arithmetic case in which the residue fields are finite).

We will sometimes use the notation $e$ or $e_{K/k}$ instead of $e(\mathfrak{P}/\mathfrak{p})$, same for $f$.

**Theorem 4.3.** 1) $\forall x \in K\ \ \mathrm{v}_\mathfrak{P}(N(x)) = n\mathrm{v}_\mathfrak{P}(x)$.
2) The unique extension of the absolute value $||x||_\mathfrak{p} = s^{-\mathrm{v}_\mathfrak{p}(x)}$ from $k$ to $K$ is given by the formula $||x|| \stackrel{\text{def}}{=} ||N(x)||^{\frac{1}{n}}$.

*Proof.* 1) If $K/k$ is Galois then the action of the Galois group $G$ preserves the absolute value (cf. Theorem 3.33) hence $\forall g \in G\ \ \mathrm{v}_\mathfrak{P}(g(x)) = \mathrm{v}_\mathfrak{P}(x)$ whence the statement. If $K/k$ is not Galois then choose a Galois extension $L/k$ such that $K \subset L$. Let $\mathfrak{Q} \subset \mathcal{O}_L$ be the maximal ideal. Then $\forall g \in \mathrm{Gal}\,(L/k)\ \ \mathrm{v}_\mathfrak{Q}(g(x)) = \mathrm{v}_\mathfrak{Q}(x)$. Since $N_{K/k}(x)$ is the product of some $n$ of these $g(x)$, $\mathrm{v}_\mathfrak{Q}(N_{K/k}(x)) = n\mathrm{v}_\mathfrak{Q}(x)$ hence this also holds for $\mathrm{v}_\mathfrak{P}$ ■
2) First suppose $x \in k$. Since $N(x) = x^n$ the formula holds. By the definition $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^e$ thus $\mathrm{v}_\mathfrak{P}(x) = e\mathrm{v}_\mathfrak{p}(x)$, therefore for $x \in k$ $||x|| = s^{-\frac{1}{e}\mathrm{v}_\mathfrak{P}(x)}$. The extension of the absolute value to $K$ is unique hence the same formula should hold for $x \in K$. Now use 1) ■

**Theorem 4.4.** $f$ is finite, $ef = n$

*Proof.* Consider the ascending series of subspaces of the the $k_\mathfrak{p}$-vector space $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ : $(0) \subset \mathfrak{P}^{e-1}/\mathfrak{p}\mathcal{O}_K \subset \mathfrak{P}^{e-2}/\mathfrak{p}\mathcal{O}_K \subset \cdots \subset \mathfrak{P}/\mathfrak{p}\mathcal{O}_K \subset \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. All the quotient spaces $\mathfrak{P}^{i-1}/\mathfrak{P}^i$, $1 \leq i \leq e$ are isomorphic, the successive isomorphism being defined by multiplication with some generator of the ideal $\mathfrak{P}$. The very first quotient space is $\mathcal{O}_K/\mathfrak{P} = K_\mathfrak{P}$ thus its $k_\mathfrak{p}$-dimension equals $f$. On the other hand, $\mathcal{O}_K$ is a free $\mathcal{O}$-module of rank $n$ hence $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ is an $(\mathcal{O}/\mathfrak{p} = k_\mathfrak{p})$-module of rank $n$. Thus $n = ef$ and, by the way, $f$ is finite ■

*Remark.* In the general Dedekind domain case $n = \sum e_i f_i$ where $e_i = e(\mathfrak{P}_i/\mathfrak{p})$, $f_i = f(\mathfrak{P}_i/\mathfrak{p})$.

**Notation.** From now on we will use the bar symbol to denote residues modulo $\mathfrak{P}$ of elements in $\mathcal{O}_K$ or in its suitable quotients (resp. residues modulo $\mathfrak{p}$ of elements in $\mathcal{O}$ or its qoutients). No algebraic closures will appear up to the end thus mix-up looks improbable.

**Theorem 4.5.** Suppose $x \in \mathcal{O}_K$. Then
1) $\overline{Tr_{K/k}(x)} = e\, Tr_{K_\mathfrak{P}/k_\mathfrak{p}}(\overline{x})$.
2) $\overline{N_{K/k}(x)} = (N_{K_\mathfrak{P}/k_\mathfrak{p}}(\overline{x}))^e$.

*Proof.* 1)-2) Denote $\bullet x$ the operator of multiplication with $x$. By definition, $Tr_{K/k}(x) = Tr(\bullet x$ acting on the free $\mathcal{O}$-module $\mathcal{O}_K)$. Since $\mathfrak{p}\mathcal{O}_K \subset \mathfrak{P}$, $\overline{Tr_{K/k}(x)} = Tr(\bullet x$ acting on the $k_\mathfrak{p}$-algebra $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$. The subspaces $\mathfrak{P}^i/\mathfrak{p}\mathcal{O}_K$ introduced in the previous theorem are $\mathcal{O}_K$-submodules hence $\overline{Tr_{K/k}(x)} = \sum_{i=1}^{e} Tr(\bullet x$ acting on the quotient space $\mathfrak{P}^{i-1}/\mathfrak{P}^i) = e\, Tr(\bullet x$ acting on $\mathcal{O}_K/\mathfrak{P}) = e\, Tr_{K_\mathfrak{P}/k_\mathfrak{p}}(\overline{x})$ which ends the proof for the trace. The proof for the norm is the same ■

**Theorem 4.6.** $\mathrm{v}_\mathfrak{P}(\mathfrak{D}_{K/k}) \geq e - 1$.

*Proof.* $\dim_{k_\mathfrak{p}} \mathfrak{P}/\mathfrak{p}\mathcal{O}_K = (e-1)f$ while $\dim_{k_\mathfrak{p}} \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = ef = n$. Thus in $\mathcal{O}_K$ there exists an $\mathcal{O}$-basis $\{x_i, 1 \leq i \leq n\}$ such that for $1 \leq i \leq (e-1)f$ $x_i \in \mathfrak{P}$. Therefore for $1 \leq i \leq (e-1)f$, $j$ arbitrary $x_i x_j \in \mathfrak{P}$ hence by the previous theorem $\overline{Tr_{K/k}(x_i x_j)} = e\, Tr_{K_\mathfrak{P}/k_\mathfrak{p}}(\overline{x_i x_j}) = 0$. This implies the first $(e-1)f$ rows of the Gram matrix $Tr(x_i x_j)$ have all the entries in $\mathfrak{p}$ hence $\mathrm{v}_\mathfrak{p}(\mathfrak{d}_{K/k}) \geq (e-1)f \Rightarrow \mathrm{v}_\mathfrak{P}(\mathfrak{D}_{K/k}) = \dfrac{1}{n}\mathrm{v}_\mathfrak{P}(N_{/k}(\mathfrak{D}_{K/k})) =$

$\frac{1}{n}\mathrm{v}_{\mathfrak{P}}(\mathfrak{d}_{K/k}) = \frac{e}{n}\mathrm{v}_{\mathfrak{p}}(\mathfrak{d}_{K/k}) \geq \frac{e(e-1)f}{n} = e-1$ (by the theorems 3.39, 4.3 and 4.4) ■

**Definition 4.7.** The extension $K/k$ is called
1) unramified iff $e = 1$,
2) tamely ramified iff $\mathrm{char}(k_{\mathfrak{p}}) \nmid e$,
3) totally ramified iff $f = 1$.

**Theorem 4.8.** $K/k$ is unramified $\Leftrightarrow \mathfrak{d}_{K/k} = \mathcal{O}$.

*Proof.* $\Leftarrow \mathfrak{d}_{K/k} = \mathcal{O} \Leftrightarrow \mathfrak{D}_{K/k} = \mathcal{O}_K \Rightarrow e = 1$ by the Theorem 4.6 ■
$\Rightarrow e = 1 \Rightarrow \mathfrak{p}\mathcal{O}_K = \mathfrak{P} \Rightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = K_{\mathfrak{P}}$. Hence if $\{x_i\}$ is an $\mathcal{O}$-basis in $\mathcal{O}_K$ then $\{\overline{x_i}\}$ is a $k_{\mathfrak{p}}$-basis in $K_{\mathfrak{P}}$. Since $e = 1$, by the Theorem 4.5 $\overline{\det Tr(x_i x_j)} = \det Tr(\overline{x_i}\overline{x_j}) \neq 0$, therefore $\mathfrak{d}_{K/k} \not\subset \mathfrak{p}$ ■

**Theorem 4.9.** $K/k$ is tamely ramified $\Leftrightarrow Tr_{K/k}(\mathcal{O}_K) = \mathcal{O} \Leftrightarrow \mathrm{v}_{\mathfrak{P}}(\mathfrak{D}_{K/k}) = e-1$.

*Proof.* Since the map $Tr : K_{\mathfrak{P}} \to k_{\mathfrak{p}}$ is nonzero, the first equality is a direct consequence of the Theorem 4.5. Further, by the hometask, $D_{\mathcal{O}}(\mathcal{O}_K) \cap k = (Tr_{K/k}(\mathcal{O}_K))^{-1}$. For any $\mathcal{O}_K$-f.i $I \subset K$ $I \cap k = \{x \in k \text{ such that } e\mathrm{v}_{\mathfrak{p}}(x) \geq \mathrm{v}_{\mathfrak{P}}(I)\}$. Therefore $Tr_{K/k}(\mathcal{O}_K) = \mathcal{O} \Leftrightarrow$ $-e < \mathrm{v}_{\mathfrak{P}}((\mathfrak{D}_{K/k})^{-1}) \leq 0$. Theorem 4.6 now ends the proof of the second equality ■

**Definition-Theorem 4.10.** A separable polynomial $P(T) = T^n + \sum_{i=0}^{n-1} a_i T^i \in \mathcal{O}[T]$ is called an Eisenstein polynomial iff all $a_i \in \mathfrak{p}$ and $\mathrm{v}_{\mathfrak{p}}(a_0) = 1$. Then $P(T)$ is irreducible.

*Proof.* Suppose $P = P_1 P_2$ in $k[T]$. Then by the Gauss lemma both $P_1$ and $P_2$ lie in $\mathcal{O}[T]$. Taking residues mod $\mathfrak{p}$ one gets $\overline{P_1}\overline{P_2} = T^n$ hence $\overline{P_1} = T^{n_1}$, $\overline{P_2} = T^{n_2}$. Therefore free terms of $P_1$ and of $P_2$ are both contained in $\mathfrak{p}$ which contradicts the definition ■

**Theorem 4.11** (totally ramified extensions).
1) Suppose $K = k_P$, $P \in \mathcal{O}[T]$ is an Eisenstein polynomial. Then $K/k$ is totally ramified. If $\Pi \in K$, $P(\Pi) = 0$ then $\mathrm{v}_{\mathfrak{P}}(\Pi) = 1$.
2) Suppose $K/k$ is totally ramified, $\Pi \in \mathcal{O}_K, \mathrm{v}_{\mathfrak{P}}(\Pi) = 1$. Then $P_{\Pi}$ is an Eisenstein polynomial, $K = k(\Pi)$, $\mathcal{O}_K = \mathcal{O}[\Pi]$.

*Proof.* 1) By definition, $N_{K/k}(\Pi) = \pm a_0$. By the Theorem 4.3 $\mathrm{v}_{\mathfrak{P}}(\Pi) = \frac{1}{n}\mathrm{v}_{\mathfrak{P}}(a_0) = \frac{e}{n}\mathrm{v}_{\mathfrak{p}}(a_0) = \frac{e}{n}$. Since $e \leq n$, $n = e$ and $\mathrm{v}_{\mathfrak{P}}(\Pi) = 1$ ■

2) Since $f = 1$ the residue field $K_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$ coincides with $k_{\mathfrak{p}} = \mathcal{O}/\mathfrak{p}$. Choose a full system of representatives of residues $T \subset \mathcal{O}$ (for example, if $k = \mathbf{Q}_p$ then the union of zero and the Teichmüller elements (cf. Theorem 1.19) fits), then $\#T = \#k_{\mathfrak{p}}$. For $-\infty \leq r \leq \infty$ choose elements $\Pi_r \in K$ such that $\mathrm{v}_{\mathfrak{P}}(\Pi_r) = r$. Then for any $x \in K$ there exists a unique representation $x = \sum_{r=-\infty}^{\infty} t_r \Pi_r$ where $t_r \in T$, the sum being finite to the left while possibly infinite to the right. The proof is evident, using the induction by $\mathrm{v}_{\mathfrak{P}}(x)$. Let $\pi \in \mathcal{O}$ be some generator of $\mathfrak{p}$. One may now choose the elements $\Pi_r = \pi^{\alpha(r)}\Pi^{\beta(r)}$ such that $\forall r\ \alpha(r) \in \mathbf{Z},\ \beta(r) \in \mathbf{Z},\ 0 \leq \beta(r) \leq e-1$. The sum above becomes a polynomial in $\Pi$ of degree at most $e-1$ with coefficients in $\mathcal{O}$. Therefore $K = k(\Pi)$ and $\mathcal{O}_K = \mathcal{O}[\Pi]$. Since $\Pi \in \mathcal{O}_K,\ \ P_\Pi$ is monic, since $K = k(\Pi),\ \ \deg(P_\Pi) = n = e$. If $a_0$ is the free term of $P_\Pi$ then $a_0 = \pm N_{K/k}(\Pi)$ hence by the assumption and by the Theorem 4.3 $\mathrm{v}_{\mathfrak{p}}(a_0) = 1$. Finally, $\overline{P_\Pi}$ is a characteristic polynomial of the endomorphism $\bullet\Pi$ of the $n$-dimensional $k_{\mathfrak{p}}$-vector space $V = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ which is nilpotent of period $e = n$, hence the chain of subspaces $\{V_r = \ker(\bullet\Pi^r), 1 \leq r \leq n\}$ increases strictly. Choosing a basis $\{y_r\}$ such that $y_r \in V_r,\ y_r \notin V_{r-1}$ one may see that $\overline{P_\Pi} = T^n$ which ends the proof ■

**Theorem 4.12** (unramified extensions).
1) Suppose $K = k_P,\ \ P \in \mathcal{O}[T]$ is monic of degree $n$, such that $\overline{P} \in k_{\mathfrak{p}}[T]$ is irreducible and separable. Then $K/k$ is unramified and $K_{\mathfrak{P}} = (k_{\mathfrak{p}})_{\overline{P}}$.
2) Suppose $K/k$ is unramified. Then $\exists x \in \mathcal{O}_K$ such that $K_{\mathfrak{P}} = k_{\mathfrak{p}}(\overline{x})$. If this is the case then $K = k(x),\ \mathcal{O}_K = \mathcal{O}[x],\ \ \overline{P_x} \in k_{\mathfrak{p}}[T]$ is irreducible and separable.

*Proof.* 1) $[K : k] = n = [(k_{\mathfrak{p}})_{\overline{P}} : k_{\mathfrak{p}}] \leq [K_{\mathfrak{P}} : k_{\mathfrak{p}}] = f \leq n$. This implies $f = n$ and $K_{\mathfrak{P}} = (k_{\mathfrak{p}})_{\overline{P}}$ ■
2) Since $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is separable, $\exists \overline{x} \in K_{\mathfrak{P}}$ such that $K_{\mathfrak{P}} = k_{\mathfrak{p}}(\overline{x})$. Choose $x \in \mathcal{O}_K$ such that $x \equiv \overline{x} \mod \mathfrak{P}$. Then $[K_{\mathfrak{P}} : k_{\mathfrak{p}}] = \deg(P_{\overline{x}}) \leq \deg(\overline{P_x}) = \deg(P_x) \leq [K : k]$. Since by the assumption $[K : k] = [K_{\mathfrak{P}} : k_{\mathfrak{p}}]$, this implies $\overline{P_x} = P_{\overline{x}}$, therefore $P_x$ is irreducible and separable of degree $n = [K : k]$, thus $K = k(x)$. Consider the set $\{x^i,\ 0 \leq i \leq n-1\}$. Since $e = 1$, by the Theorem 4.5 $\det Tr(\overline{x^{i+j}}) = \overline{\det Tr(x^{i+j})}$. Since $\{\overline{x^i}\}$ is a $k_{\mathfrak{p}}$-basis in $K_{\mathfrak{P}}$ the left side is nonzero, hence so is the right side, which implies $\det Tr(x^{i+j})$ is invertible in $\mathcal{O}$. Thus $\mathfrak{d}_{\mathcal{O}}(\mathcal{O}[x]) = \mathcal{O}$, therefore by the theorems 4.8 and 3.25. 3) $\mathcal{O}[x] = \mathcal{O}_K$ ■

**Definition-Theorem 4.13** (reduction of homomorphisms).
Suppose $K/k$ and $K'/k$ are finite separable extensions, $\sigma : K/k \to K'/k$ a homomorphism. Then the map $\sigma_{\mathfrak{p}} : \mathcal{O}_K/\mathfrak{P} \to \mathcal{O}_{K'}/\mathfrak{P}'$ defined as $\sigma_{\mathfrak{p}}(x \mod \mathfrak{P}) \stackrel{\mathrm{def}}{=} \sigma(x) \mod \mathfrak{P}'$ is a correctly defined homomorphism of extensions $K_{\mathfrak{P}}/k_{\mathfrak{p}} \to K'_{\mathfrak{P}'}/k_{\mathfrak{p}}$.

*Proof.* Clearly $\sigma(\mathcal{O}_K) \subset \mathcal{O}'_K$ (both are integral closures of $\mathcal{O}$). Using the Theorem 3.27 for the extension $K'/K$ one may conclude that $\sigma(\mathfrak{P})$ is nontrivial, hence $\sigma(\mathfrak{P}) \subset \mathfrak{P}'$. Therefore $\sigma(x) \mod \mathfrak{P}'$ depends only on the residue of $x \mod \mathfrak{P}$ ■

*Remark.* Clearly reduction commutes with the composition of homomorphisms, thus the reduction of an isomorphism is an isomorphism.

**Theorem 4.14**. Suppose $K/k$ is unramified, $K'/k$ any finite separable extension. Then the natural map $\Sigma_{K/k}^{K'/k} \to \Sigma_{K_\mathfrak{P}/k_\mathfrak{p}}^{K'_{\mathfrak{P}'}/k_\mathfrak{p}}$ is a one-to-one correspondence. If $K_\mathfrak{P}/k_\mathfrak{p} \simeq K'_\mathfrak{P}/k_\mathfrak{p}$ and $K'/k$ is unramified then $K/k \simeq K'/k$.

*Proof.* Choose $x \in \mathcal{O}_K$ such that $k(x) = K$ and $k_\mathfrak{p}(\overline{x}) = K_\mathfrak{P}$. Suppose $\gamma \in \Sigma_{K_\mathfrak{P}/k_\mathfrak{p}}^{K'_{\mathfrak{P}'}/k_\mathfrak{p}}$. Let $\overline{y} = \gamma(\overline{x})$. Clearly $P_{\overline{x}}(\overline{y}) = 0$, hence by the Hensel's Lemma 1.20 there exists a unique $y \in \mathcal{O}_{K'}$ such that $P_x(y) = 0$ and $y \mod \mathfrak{P}' = \overline{y}$. Define $\sigma$ by the formula $\sigma(x) = y$, then $\sigma_\mathfrak{p} = \gamma$ and such $\sigma$ is unique. The residue field of $\sigma(K)$ coincides with $\gamma(K_\mathfrak{P})$ by the construction, so it coincides with $K'_{\mathfrak{P}'}$ if $\gamma$ is an isomorphism. If in addition $K'/k$ is unramified then $[K' : k] = [K'_{\mathfrak{P}'} : k_\mathfrak{p}] = [\gamma(K_\mathfrak{P}) : k_\mathfrak{p}] \leq [\sigma(K) : k]$ hence $K' = \sigma(K)$ ■

**Theorem 4.15** (maximal unramified subextension).
1) There exists a unique subfield $k \subset K_0 \subset K$ which is unramified and contains any other unrumified subfield. Any subfield $k \subset K_1 \subset K_0$ is unramified. $(K_0)_{\mathfrak{P}_0} = K_\mathfrak{P}$.
2) If $K/k$ is normal, same is $K_0/k$. Suppose $G = \mathrm{Gal}\,(K/k)$. Then $K_0/k$ corresponds to the subgroup $G_0 \subset G$ defined as $G_0 \stackrel{\text{def}}{=} \{g \in G \text{ such that } \forall x \in \mathcal{O}_K \ \ \mathrm{v}_\mathfrak{P}(g(x) - x) > 0\}$.
*Proof.* 1) Choose $\overline{x} \in K_\mathfrak{P}$ which generates $K_\mathfrak{P}/k_\mathfrak{p}$. Let $P(T) \in \mathcal{O}[T]$ be a monic polynomial such that $\overline{P} = P_{\overline{x}}$. By the Theorem 4.12 $k_P/k$ is unramified and its field of residues coincides with $K_\mathfrak{P}$. By the previous theorem there exists an inclusion $k_P/k \to K/k$, let $K_0$ be its image. By construction $K_0/k$ is unramified and $(K_0)_{\mathfrak{P}_0} = K_\mathfrak{P}$. Any subextension of an unramified extension (in particular, of $K_0/k$) is unramified by the Theorem 4.2.
Suppose now that $k \subset K_1 \subset K$, $K_1/k$ unramified. Let $j_0 : K_0/k \to K/k$ and $j_1 : K_1/k \to K/k$ be corresponding inclusions. Since $(j_0)_\mathfrak{p}$ is an isomorphism, $(j_0)_\mathfrak{p}^{-1} \circ (j_1)_\mathfrak{p} : (K_1)_{\mathfrak{P}_1} \to (K_0)_{\mathfrak{P}_0}$ is defined. By the previous theorem there exists a unique $\psi : K_1/k \to K_0/k$ such that $\psi_\mathfrak{p} = (j_0)_\mathfrak{p}^{-1} \circ (j_1)_\mathfrak{p} \Leftrightarrow (j_0)_\mathfrak{p} \circ \psi_\mathfrak{p} = (j_1)_\mathfrak{p}$. Applying the same theorem to the pair $(K_1/k, K/k)$ one gets $j_0 \circ \psi = j_1$, thus $K_1 \subset K_0$ ■

2) Suppose $K/k$ is normal. Since $\forall g \in G \quad g(K_0)$ is unramified by the Theorem 3.33, $K_0$ is normal by 1) above. Suppose $Q \in k_{\mathfrak{p}}[T]$ is an irreducible polynomial having a root in $K_{\mathfrak{P}}$. Since $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is separable $Q$ is separable, hence there exists an irreducible separable polynomial $P \in k[T]$ such that $\overline{P} = Q$. By the Hensel's Lemma $P$ has a root in $K$ hence decomposes totally in $K$. Therefore $Q$ decomposes totally in $K_{\mathfrak{P}}$, thus $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is normal. Consider the homomorphism $G \to \mathrm{Gal}\,(K_0/k) \to \mathrm{Gal}\,(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ sending $g$ to $g_{\mathfrak{p}}$. By the definition, $G_0 = \ker(G \to \mathrm{Gal}\,(K_{\mathfrak{P}}/k_{\mathfrak{p}}))$. The second arrow above is an isomorphism by the Theorem 4.14, hence $G_0 = \ker(G \to \mathrm{Gal}\,(K_0/k))$ ■

*Remark.* The group $G_0$ is called the inertia group. In fact there exists a decreasing chain of subgroups $G \supset G_0 \supset G_1 \supset \ldots$ which are called ramification groups. For example, $G_1$ corresponds to the subfield $K_1 \subset K$ which contains all the tamely ramified subfields.

Next we discuss some elements of $p$-adic calculus. In what follows the bar sign means the algebraic closure.

**Definition 4.16**. The field $\mathbf{C}_p$ (or the Tate field).

The function $\mathrm{v}_p$ extends in a unique way from $\mathbf{Q}_p^*$ to $\overline{\mathbf{Q}_p}^*$ with the formula $\mathrm{v}_p(x) \stackrel{\mathrm{def}}{=} \frac{1}{\deg x}\mathrm{v}_p(N_{\mathbf{Q}_p(x)/\mathbf{Q}_p}(x))$ with values in $\mathbf{Q}$ and defines (after one chooses $1 < s \in \mathbf{R}$) a nonarchimedean (indiscrete) absolute value $||x|| \stackrel{\mathrm{def}}{=} s^{-\mathrm{v}_p(x)}$ on the field $\overline{\mathbf{Q}_p}$. $\mathbf{C}_p$ (the Tate field) is the completion of the field $\overline{\mathbf{Q}_p}$ with respect to the absolute value defined above.

**Theorem 4.17**.The field $\mathbf{C}_p$ contains some elements which are transcendental over $\mathbf{Q}_p$.

*Proof.* Search $x$ in the form $x = \sum\limits_{i=0}^{\infty} \zeta_i p^i$ where $\zeta_0 = 1$ and all the $\zeta_i$ are roots of unity of degrees not divisible by $p$ with the additional property that $\forall\, i\ \zeta_i \in \mathbf{Q}_p(\zeta_{i+1})$. Such an element in fact is contained in the completion of the maximal unramified subfield $\mathbf{Q}_p^{nr} \subset \overline{\mathbf{Q}_p}$. Let $x_n = \sum\limits_{i=0}^{n} \zeta_i p^i$. Then $\mathrm{v}_p(x - x_n) = n + 1$. Let $k_n = \mathbf{Q}_p(\zeta_{n-1})$. Suppose $x$ is algebraic over $\mathbf{Q}_p$. Let $K_n$ - be a finite Galois extension of $k_n$ which contains $\zeta_n$ (hence also $x_n$) and $x$. Define $G_n = \mathrm{Gal}\,(K_n/k_n)$. Suppose $\sigma,\ \tau \in G_n$ act differently on $\zeta_n$, so that $\sigma(\zeta_n) \neq \tau(\zeta_n)$. Then $\mathrm{v}_p(\sigma(x_n) - \tau(x_n)) = \mathrm{v}_p(\sigma(\zeta_n) - \tau(\zeta_n)) + n = n$ as different roots of unity have different residues modulo the maximal ideal in $\mathcal{O}_{\mathbf{Q}_p^{nr}}$ (recall that this ideal is generated by $p$ and the residues themselves take values in $\overline{\mathbf{F}_p}$). At the same time $\mathrm{v}_p(\sigma(x) - \sigma(x_n)) = \mathrm{v}_p(x - x_n) = n + 1$ and the same is true for $\tau$. Since

$\sigma(x)-\tau(x)=(\sigma(x_n)-\tau(x_n))+(\sigma(x)-\sigma(x_n))-(\tau(x)-\tau(x_n))$ one concludes by using Theorem 1.4 that $\mathrm{v}_p(\sigma(x)-\tau(x))=n$ thus $\sigma(x)\neq\tau(x)$.
If $x$ is algebraic over $\mathbf{Q}_p$ of degree $d$, then it is algebraic over $k_n$ of degree no more than $d$ hence there exist no more than $d$ conjugates to $x$ over $k_n$. Now choose the sequence $\zeta_i$ making the degree of $\zeta_i$ over the field $\mathbf{Q}_p(\zeta_{i-1})$ tend to infinity. The order of the group $G_n$ (thus the number of conjugates to $x$) then also tends to infinity which leads to a contradiction ■

**Theorem 4.18** (Krasner's lemma).
Suppose $k$ is a field complete with respect to a non-archimedean absolute value $||\ ||$, the latter could thus be uniquely extended to the algebraic extensions. Suppose $P\in k[T]$ is a monic separable polynomial with the roots $\alpha=\alpha_1,\alpha_2,\dots\alpha_n\ \in\ k^{\mathrm{sep}}$. Suppose $\beta\in k^{\mathrm{sep}}$ and $\forall i\geq 2\ \ ||\alpha-\beta||<||\alpha-\alpha_i||$. Then $\alpha\in k(\beta)$.
*Proof.* If $\alpha'$ is conjugate to $\alpha$ over $k(\beta)$ (i.e. $\exists\sigma\in\sum_{\overline{k}/k(\beta)}^{\overline{k}/k(\beta)}$ such that $\sigma(\alpha)=\alpha'$) then $||\alpha-\beta||=||\alpha'-\beta||$ (the absolute values of conjugate elements coincide since the absolute value extends in a unique way). Since $\alpha$ and $\alpha'$ both are roots of $P$, one may apply the strict triangle inequality to the formula $\alpha-\alpha'=(\alpha-\beta)-(\alpha'-\beta)$ the result contradicting to the assumption of the theorem ■
The particular case of the theorem ($\beta\in k$ while $P=P_{\alpha,k}$) proves that no $\alpha$ which is algebraic over $k$ may admit rational approximation more close to $\alpha$ than some of its conjugates.

**Theorem 4.19**. $\mathbf{C}_p$ is algebraically closed.
*Proof.* Suppose $\alpha\in\overline{\mathbf{C}_p}$, the roots of $P\stackrel{\mathrm{def}}{=}P_{\alpha,\mathbf{C}_p}$ being $\alpha=\alpha_1,\alpha_2,\dots\alpha_n\ \in\ \overline{\mathbf{C}_p}$. WLOG one may suppose that $\alpha$ is integral over $\mathcal{O}_{\mathbf{C}_p}$ (otherwise multiply $\alpha$ with a suitable constant) hence $P\in\mathcal{O}_{\mathbf{C}_p}[T]$. Choose a monic polynomial $Q\in\mathcal{O}_{\overline{\mathbf{Q}_p}}[T]$ which enjoys the property $\mathrm{v}_p(Q-P)>n\ \max\limits_{i\geq 2}\mathrm{v}_p(\alpha-\alpha_i)$ where $\mathrm{v}_p(\text{a polynomial})\stackrel{\mathrm{def}}{=}\min\mathrm{v}_p(\text{coefficients})$. Suppose $\{\beta_i\}$ are the roots of $Q$. Then $\sum\limits_i\mathrm{v}_p(\alpha-\beta_i)=\mathrm{v}_p(Q(\alpha))=\mathrm{v}_p(Q(\alpha)-P(\alpha))\geq\mathrm{v}_p(Q-P))>n\ \max\limits_{i\geq 2}\mathrm{v}_p(\alpha-\alpha_i)$. Therefore $\exists i$ such that $\mathrm{v}_p(\alpha-\beta_i)>\max\limits_{i\geq 2}\mathrm{v}_p(\alpha-\alpha_i)$ Using the Krasner lemma one concludes that $\alpha\in\mathbf{C}_p(\beta_i)=\mathbf{C}_p$. ■

**Definition-Theorem 4.20**. For a power series $F(T)=\sum\limits_{i=0}^{\infty}a_iT^i\in\mathbf{C}_p[[T]]$ define $\mathrm{v}_p(F)\stackrel{\mathrm{def}}{=}\liminf\frac{\mathrm{v}_p(a_i)}{i}$. ($\mathrm{v}_p(F)$ may be finite or equal to either $+\infty$ or $-\infty$). Then $F(x)$ converges if $\mathrm{v}_p(x)>-\mathrm{v}_p(F)$ and defines a continuous function. If $\mathrm{v}_p(x)<-\mathrm{v}_p(F)$ then $F(x)$ does not converge.

*Proof.* Since the absolute value is nonarchimedean one may apply Theorem 1.11. The power series $F(x)$ converges iff $\lim\limits_{i\to\infty}(\mathrm{v}_p(a_i)+i\mathrm{v}_p(x))=\infty$. This means that $\forall\, C>0\,\exists i(C)$ such that for $i>i(C)$ $\frac{\mathrm{v}_p(a_i)}{i}+\mathrm{v}_p(x)>\frac{C}{i}$ which is the same as (using the definition of $\mathrm{v}_p(F)$) for $i>i(C)$ $\frac{\mathrm{v}_p(a_i)}{i}-\liminf\frac{\mathrm{v}_p(a_i)}{i}+\mathrm{v}_p(F)+\mathrm{v}_p(x)>\frac{C}{i}$. Clearly the last inequality holds provided $\mathrm{v}_p(F)+\mathrm{v}_p(x)$ is a positive constant and cannot hold if that constant is negative. This proves the statement concerning convergence. For the proof of conitinuity see hometask ■

**Definition 4.21**. The Newton polygon $N(F)$ of a power series $F(T)=1+\sum\limits_{i=1}^{\infty}a_iT^i\in 1+T\mathbf{C}_p[[T]]$ is a lower convex hull of the points $(i,\mathrm{v}_p(a_i))$ on the plane. The Newton polygon may coincide with the lower half of the vertical axis. If this is not the case then the strictly increasing sequence of slopes $\lambda_j(F)$ of the segments is defined; the length of the projection of the corresponding segment onto the horisontal axis is called the length of that slope.
If the power series $F(T)$ is a polynomial of degree $n$ then its Newton polygon ends in the point $(n,\mathrm{v}_p(a_n))$. If the power series is not a poliynomial while the sequence of slopes is finite then the maximal slope has infinite length.

Informally speaking, in order to costruct the Newton polygone one turns the lower vertical semiaxis anti-clockwise. When it meets the point $(i,\mathrm{v}_p(a_i))$ one drives in a nail and supports the semiaxis with a hinge. If the semiaxis meets several points at the same time one drives in a nail choosing the last (righthand direction) point. The procedure stops if the semiaxis meets infinite number of points at the same time or else if the successive turns are blocked with the infinite number of points, the directions to which from the last nail tend to the direction from next-to-the-last nail to the last one (even if the semiaxis does not meet these points).

**Theorem 4.22**. $\mathrm{v}_p(F)=\sup\lambda_j(F)$. Suppose $\mathrm{v}_p(x)=-\mathrm{v}_p(F)$. The power series $F(x)$ converges iff the list of slopes of the Newton polygon $N(F)$ is finiite and the vertical distance between the points $(i,\mathrm{v}_p(a_i))$ and the infinite segment of $N(F)$ tends to infinity.

*Proof.* The maximal slope $\lambda_{\max}(F)$ (if it is finite) coincides with $\mathrm{v}_p(F)=\liminf\frac{\mathrm{v}_p(a_i)}{i}$ by the definition of $N(F)$. The affine equation of the infinite segment of $N(F)$ looks like $c+\lambda_{\max}i$ while the vertical distance mentioned in the formulation of the theorem equals $a(i)-c-\lambda_{\max}i$. If $\mathrm{v}_p(x)=-\mathrm{v}_p(F)$ then $\mathrm{v}_p(a_ix^i)$ differs from the said distance by a constant so that they both either do tend or do not tend to infinity simultaneously ■

**Theorem 4.23**. Suppose $k \subset \mathbf{C}_p$ is a subfield complete with respect to the absolute value, $F(T) \in 1+Tk[T]$ a polynomial. Then $F(T) = \prod F_{\lambda_j(F)}$, $F_{\lambda_j(F)} \in k[T]$, $\deg F_{\lambda_j(F)} = l_j(F)$ and for each root $\alpha \in \mathbf{C}_p$ of the polynomial $F_{\lambda_j(F)}$ one has $\mathrm{v}_p(\alpha) = -\lambda_j(F)$.

*Proof.* Suppose $F(T) = 1 + \sum\limits_{s=1}^{n} a_s T^s = \prod\limits_{i-1}^{n}(1 - \frac{T}{\alpha_i})$, define $\lambda_i \stackrel{\text{def}}{=} -\mathrm{v}_p(\alpha_i)$. Let the roots be ordered so that $\lambda_1 \leq \cdots \leq \lambda_n$ (this means that the absoute value of the roots does not decrease). Suppose that $\lambda_1 = \cdots = \lambda_r < \lambda_{r+1}$. Since the coefficients of $F(T)$ are elementary symmetric functions on $\alpha_i^{-1}$ one concludes that $\mathrm{v}_p(a_i) \geq i\lambda_1$ (for any $i \geq 1$), $\mathrm{v}_p(a_r) = r\lambda_1$(as the term $\alpha_1^{-1} \ldots \alpha_r^{-1}$ dominates all the other terms of $a_r$) and $\mathrm{v}_p(a_{r+1}) > (r+1)\lambda_1$. This means that the first segment of $N(F)$ connects the points $(0,0)$ and $(r, \mathrm{v}_p(a_r))$. These calculations could be repeated for each successive collection of equal $\lambda_i$ hence the statement of the theorem. Since the function $\mathrm{v}_p$ is Galois-invariant, the polynomials $F_{\lambda_j(F)}$ have coefficients in $k$ ■

**Theorem 4.24** (Weierstrass theorem, $\mathbf{C}_p$ - version).
1) Suppose $F(T) \in 1 + T\mathbf{C}_p[[T]]$ is a power series such that $F(x)$ converges for all $x$ such that $\mathrm{v}_p(x) \geq -\lambda$. Define $n(\lambda, F) \stackrel{\text{def}}{=} \sum\limits_{\lambda_j(F) \leq \lambda} l_j(F)$ (if the sum contains the length of the maximal slope which is infinite then make an agreement that the corresponding segment ends in the last point $(i, \mathrm{v}_p(a_i))$ lying on it).
Then $\exists! H(T) \in 1 + T\mathbf{C}_p[T]$, $\deg H = n(\lambda, F)$ and $G(T) \in 1 + T\mathbf{C}_p[[T]]$ such that $F(T) = H(T)G(T)$ where $G(x)$ converges to some nonezero element of $\mathbf{C}_p$ for all $x$ $|\mathrm{v}_p(x) \geq -\lambda$. The Newton polygon $N(H(T))$ coincides with the part of the Newton polygon $N(F(T))$ situated between the points $(0,0)$ and $(n(\lambda, F), \mathrm{v}_p(a_{n(\lambda,F)}))$.
2) Suppose $F(T) \in 1 + T\mathbf{C}_p[[T]]$ converges for all $x \in \mathbf{C}_p$. Let $\{\alpha_k, 1 \leq k \leq \infty\}$ be the list of zeros of the function $F(x)$ ordered by decreasing $\mathrm{v}_p(\alpha_k)$. Then $\forall r \#(k \,|\mathrm{v}_p(\alpha_k) \geq r) < \infty$ and the infinite product $\prod\limits_{k=1}^{\infty}(1 - \alpha_k^{-1}x)$ converges to $F(x)$ for all $x \in \mathbf{C}_p$.

*Proof.* Hometask.