5. Ramification theory

Let $\mathcal{O}$ be an arbitrary integral domain (i.e. a commutative ring with the identity and without zero divisors), k its field of fractions.

Definition 5.1. Suppose I, J are $\mathcal{O}$-submodules in k. Then $I^{-1} \stackrel{\text{def}}{=} \{x \in k \text{ such that } xI \subset \mathcal{O}\}$, $\mathcal{O}(I) \stackrel{\text{def}}{=} \{x \in k \text{ such that } xI \subset I\}$, $I + J \stackrel{\text{def}}{=} \{x + y,\ x \in I,\ y \in J\}$, $IJ \stackrel{\text{def}}{=} \{\sum x_i y_i, \text{ a finite sum, } x_i \in I,\ y_i \in J\}$.

Definition-Theorem 5.2. Suppose $\mathfrak{p} \subset \mathcal{O}$ is a prime ideal. Consider the map $I \mapsto I \cap \mathcal{O}$: $\{\text{ideals of } \mathcal{O}_\mathfrak{p}\} \to (\text{ideals of } \mathcal{O})$. If I is prime then $I \cap \mathcal{O}$ is prime. If $I \neq \{0\}$ (resp. nontrivial) then $I \cap \mathcal{O} \neq \{0\}$ (resp. nontrivial). For any $\mathcal{O}$-submodule $J \subset k$ let $\phi_\mathfrak{p}(J) \,(\text{or } J_\mathfrak{p}) \stackrel{\text{def}}{=} J\mathcal{O}_\mathfrak{p}$. Then $(I \cap \mathcal{O})_\mathfrak{p} = I$.

Proof. Any $z \in \mathcal{O}_\mathfrak{p}$ is of the form $z = \dfrac{x}{y},\ y \notin \mathfrak{p}$ whence the Theorem ■

Notation. We use the abbreviation NICD ("Noetherian integrally closed domain") for a Noetherian integrally closed integral domain. In what follows $\mathcal{O}$ (or $\mathcal{O}_k$) will always be a NICD.

Theorem 5.3. Suppose $\mathfrak{p} \subset \mathcal{O}$ is a prime ideal. Then the local ring $\mathcal{O}_\mathfrak{p}$ is a NICD.

Proof. $\mathcal{O}_\mathfrak{p} \subset k$ hence it has no zero divisors. Also it contains 1 by definition. Suppose $I \subset \mathcal{O}_\mathfrak{p}$ is an ideal. The ideal $(I \cap \mathcal{O}) \subset \mathcal{O}$ is finitely generated as an $\mathcal{O}$-module. By the previous theorem the same set of generators generates I as an $\mathcal{O}_\mathfrak{p}$-module, hence $\mathcal{O}_\mathfrak{p}$ is Noetherian. Further, suppose $x \in k$ is integral over $\mathcal{O}_\mathfrak{p}$. This means that $x^m + \sum\limits_{i=0}^{m-1} a_i x^i = 0$ for some $\{a_i \in \mathcal{O}_\mathfrak{p}\}$. Let a be the product of the denominators of the a_i, then $a \notin \mathfrak{p}$. Clearly ax is integral over $\mathcal{O}$ hence $ax \in \mathcal{O}$. This implies $x \in \mathcal{O}_\mathfrak{p}$ therefore $\mathcal{O}_\mathfrak{p}$ is integrally closed ■

Definition 5.4. An $\mathcal{O}$-submodule $I \subset k$ is called a fractional ideal (f.i.) iff $I \neq \{0\}$ and $I^{-1} \neq \{0\}$.

Theorem 5.5. Suppose $I \subset k$ is an $\mathcal{O}$-submodule. Then I is a f.i. $\Leftrightarrow$ I is nonzero and finitely generated. If this is the case then I^{-1} is a f.i., $\mathcal{O}(I) = \mathcal{O}$. If I, J are f.i.'s then $I + J, IJ, I \cap J$ are also f.i.'s.

Proof. If I is a f.i. then by definition $\exists x \in k$ such that $xI \subset \mathcal{O}$. Then xI is an ideal in $\mathcal{O}$ thus is finitely generated therefore I also is. Conversely, if I is finitely generated then the product of the denominators of the generators is a nonzero element of I^{-1}. By definition any element of I is an element of $(I^{-1})^{-1}$ hence I^{-1} is a f.i. Now suppose $z \in \mathcal{O}(I)$. Choose nonzero elements $x \in I$ and $y \in I^{-1}$. Then $yxz \in yI \subset \mathcal{O}$. Therefore $xy \in (\mathcal{O}(I))^{-1} \Rightarrow (\mathcal{O}(I))^{-1} \neq \{0\}$. The ring $\mathcal{O}[z]$ is an $\mathcal{O}$-submodule of $\mathcal{O}(I)$ which implies $(\mathcal{O}(I))^{-1} \subset (\mathcal{O}[z])^{-1}$. Therefore the latter module is nonzero, so $\mathcal{O}[z]$ is a f.i. hence finitely generated. This means that z is integral over $\mathcal{O}$ thus $z \in \mathcal{O}$. The rest is clear ■

Definition 5.6. A NICD $\mathcal{O}$ i called a discretely valuated ring (d.v.r.) iff there exists exactly one nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}$.

Theorem-Definition 5.7. Any d.v.r. $\mathcal{O}$ is a principal ideal ring. There exists a group isomorphism $\mathrm{v} : k^*/\mathcal{O}^* \xrightarrow{\sim} \mathbf{Z}$ such that $||x|| = s^{-\mathrm{v}(x)}$, $s > 1$ defines a discrete nonarchimedean absolute value on k, $\mathcal{O}$ and $\mathfrak{p}$ being, respectively, the valuation ring and the valuation ideal (cf. 2.3). For any f.i. $I \subset k$ $\mathrm{v}(I) \stackrel{\mathrm{def}}{=} \inf\limits_{a \in I} \mathrm{v}(a)$.

Proof. Step 1. First prove that $\mathfrak{p}^{-1} \neq \mathcal{O}$. Indeed, let I be a maximal element in the set of all ideals in $\mathcal{O}$ enjoying this property (ordered by inclusion). The set just defined is nonempty (it contains the zero ideal) and any linearly ordered subset has an upper bound (a chain of ideals in the Noetherian ring stabilizes) hence some I exists by the Zorn Lemma. We now will prove that I is a prime ideal therefore $I = \mathfrak{p}$ (since $\mathcal{O}^{-1} = \mathcal{O}$ I cannot be trivial). Indeed, suppose that $xy \in I$ while $x \in \mathcal{O} \diagdown I$ and $y \in \mathcal{O} \diagdown I$. By the definition of I there exists $z \notin \mathcal{O}$ such that $zI \subset \mathcal{O}$, in particular, $zxy \in \mathcal{O}$. This implies $zx \in ((y) + I)^{-1}$ hence $zx \in \mathcal{O}$ (otherwise I were not a maximal element). The last inclusion means that $z \in ((x) + I)^{-1}$ which again contradicts the assumption.
Step 2. Now prove that $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$. Indeed, $\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} \subset \mathcal{O}$. Since $\mathfrak{p}$ is the unique nonzero prime ideal it is maximal. By the Theorem 5.5 $\mathcal{O}(\mathfrak{p}) = \mathcal{O}$ while by the first step $\mathfrak{p}^{-1} \neq \mathcal{O}$, thus $\mathfrak{p}^{-1}\mathfrak{p} \neq \mathfrak{p}$ whence the statement.
Step 3. $\mathfrak{p}$ is a principal ideal. Indeed, by the second step $\mathfrak{p}^{-1} \subset \mathcal{O}(\bigcap\limits_{i=1}^{\infty} \mathfrak{p}^i)$ hence by the first step $\bigcap\limits_{i=1}^{\infty} \mathfrak{p}^i = (0)$. Therefore there exists π such that $\pi \in \mathfrak{p}$, $\pi \notin \mathfrak{p}^2$. Using step 2 one gets $(\pi)\mathfrak{p}^{-1} \subset \mathcal{O}$ while $(\pi)\mathfrak{p}^{-1} \not\subset \mathfrak{p}$. Since $\mathfrak{p}$ is the only maximal ideal this implies $(\pi)\mathfrak{p}^{-1} = \mathcal{O}$. Multiplying with $\mathfrak{p}$ leads to $(\pi) = \mathfrak{p}$.

Step 4. Since $\bigcap_{i=1}^{\infty}(\pi^i) = (0)$ one may for any $a \in \mathcal{O}\setminus\{0\}$ define $\mathrm{v}(a) \stackrel{\mathrm{def}}{=}$ (maximal i such that $\pi^i | a$). If $\mathrm{v}(a) = 0$ then the ideal (a) is not contained in $\mathfrak{p}$, but $\mathfrak{p}$ is the only maximal ideal thus $a \in \mathcal{O}^*$. Now it is easy to see that the function v extended to k^* with the formula v(numerator)-v(denominator) enjoys the properties announced in the formulation of the Theorem. For any f.i. I one may also define $\mathrm{v}(I) = \inf_{a\in I} \mathrm{v}(a)$. Since I is finitely generated $\mathrm{v}(I)$ is finite. If $I \subset \mathcal{O}$ then $\pi^{-\mathrm{v}(I)}I$ is an ideal containing an invertible element thus trivial. Therefore $I = (\pi^{\mathrm{v}(I)})$ which ends the proof ■

Definition-Theorem 5.8. A NICD $\mathcal{O}$ is called a Dedekind domain iff, equivalently,
1) Any nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}$ is maximal, or
2) For any nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}$ the local ring $\mathcal{O}_\mathfrak{p}$ is a d.v.r., or
3) For any f.i. $I \subset k$ $I^{-1}I = \mathcal{O}$.

Proof. 1) ⇒ 2) By the Theorem 5.3. $\mathcal{O}_\mathfrak{p}$ is a NICD. Suppose $I \subset \mathcal{O}_\mathfrak{p}$ is a nonzero prime ideal. By definition $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is the only maximal ideal in $\mathcal{O}_\mathfrak{p}$ thus $I \subset \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Therefore $I \cap \mathcal{O} \subset \mathfrak{p}\mathcal{O}_\mathfrak{p} \cap \mathcal{O} = \mathfrak{p}$. By the Theorem 5.2. $I = (I \cap \mathcal{O})\mathcal{O}_\mathfrak{p}$, $I \cap \mathcal{O}$ being a nonzero prime ideal in $\mathcal{O}$. By the assumption 1) $I \cap \mathcal{O} = \mathfrak{p}$ hence $I = \mathfrak{p}\mathcal{O}_\mathfrak{p}$ ■
2) ⇒ 3) Suppose $I \subset k$ is a f.i. Choose a prime ideal $\mathfrak{p} \subset \mathcal{O}$. By the assumption $\mathcal{O}_\mathfrak{p}$ is a d.v.r, k being its field of fractions, hence the function $\mathrm{v}_\mathfrak{p} : k^* \to \mathbf{Z}$ is defined. Let $\{a_1, \ldots, a_r\}$ be a set of generators of the $\mathcal{O}$-module I. Then $\mathrm{v}_\mathfrak{p}(I) = \mathrm{v}_\mathfrak{p}(a_i)$ for some i, one may suppose that $i = 1$ without loss of generality. Then $\forall i$ $a_1^{-1}a_i \in \mathcal{O}_\mathfrak{p}$. Let y be the product of the denominators of all $a_1^{-1}a_i$, then $y \notin \mathfrak{p}$. $\forall i$ $ya_1^{-1}a_i \in \mathcal{O}$ hence $ya_1^{-1} \in I^{-1}$ thus $y \in I^{-1}I$. Therefore $I^{-1}I \not\subset \mathfrak{p}$. Since this holds for an arbitrary $\mathfrak{p}$, $I^{-1}I = \mathcal{O}$ ■
3) ⇒ 1) Suppose $I \subset \mathcal{O}$ is a nonzero prime ideal which is contained in the maximal ideal $\mathfrak{p}$. Then $I\mathfrak{p}^{-1} \subset \mathcal{O}$. By the assumption $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$ thus $(I\mathfrak{p}^{-1})\mathfrak{p} = I$. SInce I is a prime ideal either $(I\mathfrak{p}^{-1}) \subset I$ or $\mathfrak{p} \subset I$. Multiplying the first formula with $I^{-1}\mathfrak{p}$ and using the assumption three times one gets the contradiction (namely $\mathcal{O} \subset \mathfrak{p}$) hence the second formula holds ■

Remark. The condition 3) is in fact very strong: it is easy to prove that if it holds in some integral domain the latter is a NICD hence a Dedekind domain.

Theorem-Definition 5.9. Suppose $\mathcal{O}$ is a Dedekind domain. Then the f.i.'s $I \subset k$ form a commutative group under multiplication (notation $\mathcal{F}(\mathcal{O})$) which is freely generated by the prime ideals $\mathfrak{p} \subset \mathcal{O}$. If $I \subset k$ is a f.i then $I = \prod_\mathfrak{p} \mathfrak{p}^{\mathrm{v}_\mathfrak{p}(I)}$ which is a finite product. $\forall \mathfrak{p}$ $I\mathcal{O}_\mathfrak{p} = (\mathfrak{p}\mathcal{O}_\mathfrak{p})^{\mathrm{v}_\mathfrak{p}(I)}$.

Proof. The group structure is clear after 5.7.3). Suppose $I \subset \mathcal{O}$ is a nontrivial nonzero ideal. Then $\exists \mathfrak{p}_1 \subset \mathcal{O}$ a maximal ideal such that $I \subset \mathfrak{p}_1$ thus $I\mathfrak{p}_1^{-1} \subset \mathcal{O}$. If $I\mathfrak{p}_1^{-1}$ is nontrivial then there exists another (maybe the same) maximal ideal $\mathfrak{p}_2$ such that $I\mathfrak{p}_1^{-1} \subset \mathfrak{p}_2$ thus $I\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \subset \mathcal{O}$ and so on. Since $\mathcal{O}$ is Noetherian the chain of ideals $I \subset I\mathfrak{p}_1^{-1} \subset I\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \subset \dots$ stabilizes hence one comes to the trivial ideal in finite number of steps. Therefore $\mathcal{F}(\mathcal{O})$ is generated by the prime ideals $\mathfrak{p}$. Now choose some $\mathfrak{p}$ and consider the map $\phi_{\mathfrak{p}} : \mathcal{F}(\mathcal{O}) \to \mathcal{F}(\mathcal{O}_{\mathfrak{p}}), \quad I \mapsto I_{\mathfrak{p}} = I\mathcal{O}_{\mathfrak{p}}$. This map is surjective by the Theorem 5.2 and it is a group homomorphism by the construction. If $\mathfrak{q} \neq \mathfrak{p}$ then $\mathfrak{q} \not\subset \mathfrak{p}$ by the first definition of a Dedekind domain hence the $\mathcal{O}_{\mathfrak{p}}$-ideal $\phi_{\mathfrak{p}}(\mathfrak{q})$ contains an invertible element. This implies $\phi_{\mathfrak{p}}(\mathfrak{q})$ is trivial therefore $\mathfrak{q} \in \ker(\phi_{\mathfrak{p}})$. The ring $\mathcal{O}_{\mathfrak{p}}$ is a d.v.r. hence by the Theorem 5.7 $\mathcal{F}(\mathcal{O}_{\mathfrak{p}})$ is an infinite cyclic group generated by the $\mathcal{O}_{\mathfrak{p}}$-ideal $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. Clearly $\phi_{\mathfrak{p}}$ maps the subgroup of $\mathcal{F}(\mathcal{O})$ generated by $\mathfrak{p}$ isomorphically on $\mathcal{F}(\mathcal{O}_{\mathfrak{p}})$. This ends the proof ■

Remark. Suppose $a \in k^*$. Then $\mathrm{v}_{\mathfrak{p}}(a) = \mathrm{v}_{\mathfrak{p}}(a\mathcal{O})$ hence $\mathrm{v}_{\mathfrak{p}}(a) = 0$ for all but a finite number of ideals $\mathfrak{p}$.

Now suppose K/k is a finite separable extension of degree n, $\mathcal{O}_K$ the integral closure of $\mathcal{O}$ in K.

Theorem 5.10. Suppose $\mathcal{O}$ is a Noetherian ring, M a finitely generated $\mathcal{O}$-module, $N \subset M$ an $\mathcal{O}$-submodule. Then N is finitely generated.

Proof. This is a generalisation of the Lemma to the Theorem 4.7. Since M is finitely generated there exists a surjective homomorphism $\phi : \mathcal{O}^m \to M$. Then $\phi^{-1}(N)$ is a submodule of $\mathcal{O}^m$ hence it is finitely generated by the Lemma just referred. Therefore $N = \phi(\phi^{-1}(N))$ is also finitely generated ■

Theorem 5.11. $\mathcal{O}_K$ is a NICD.

Proof. Clearly $\mathcal{O}_K$ contains 1 and has no zero divisors. Suppose $I \subset \mathcal{O}_K$ is an ideal. By the Theorem 4.7. $\mathcal{O}_K$ is a finitely generated $\mathcal{O}$-module hence by the previous theorem same is I. This of course implies I is finitely generated as an $\mathcal{O}_K$-module hence $\mathcal{O}_K$ is Noetherian. Now suppose that $x \in K$ is integral over $\mathcal{O}_K$. This means that the ring $\mathcal{O}_K[x]$ is finitely generated as an $\mathcal{O}_K$-module. Since $\mathcal{O}_K$ itself is a finitely generated $\mathcal{O}$-module this implies $\mathcal{O}_K[x]$ is a finitely generated $\mathcal{O}$-module. By the previous theorem same is $\mathcal{O}[x]$, hence x is integral over $\mathcal{O}$ thus by definition $x \in \mathcal{O}_K$, so $\mathcal{O}_K$ is integrally closed ■

Definition 5.12 (cf. 4.12). A finitely generated $\mathcal{O}$-submodule of K which contains a basis of the k-vector space K is called an $\mathcal{O}$-lattice in K.

Remark. If $n = 1$ then the concept of $\mathcal{O}$-lattice coincides with that of f.i.

Notation (cf. 5.2). Suppose N is an $\mathcal{O}$-submodule in K, $\mathfrak{p} \subset \mathcal{O}$ a prime ideal. Then $N_{\mathfrak{p}} \stackrel{\text{def}}{=} N\mathcal{O}_{\mathfrak{p}}$.

Theorem 5.13. Suppose $N \subset K$ is an $\mathcal{O}$-lattice, $\mathfrak{p} \subset \mathcal{O}$ a prime ideal.
1) If $\mathcal{O}$ is a principal ideal domain then N is a free $\mathcal{O}$-module of rank n.
2) If N is an $\mathcal{O}$-lattice then $N_{\mathfrak{p}}$ is a $\mathcal{O}_{\mathfrak{p}}$-lattice.

Proof. 1) By the Theorem 4.7. this holds for $\mathcal{O}_K$. Consider some basis of $\mathcal{O}_K$ and some set of generators of N. Let a be the product of the denominators of the coordinates of generators in that basis. Then $aN \subset \mathcal{O}_K$ hence aN is a free $\mathcal{O}$-module of rank $\leq n$ by the Lemma to the same theorem. Since aN contains a basis of K the rank equals n. $N \simeq aN$ as $\mathcal{O}$-modules ■
2) Clear ■

Remark. In general N (even $\mathcal{O}_K$ itself) needs not to be a free $\mathcal{O}$-module.

For the rest of this chapter $\mathcal{O}$ will be a Dedekind domain. The basic example is $\mathcal{O} = \mathbf{Z}$.

Theorem 5.14. Suppose $N \subset K$ is an arbitrary $\mathcal{O}$-submodule. Then $N = \bigcap_{\mathfrak{p}} N_{\mathfrak{p}}$.

Proof. $\subset$ clear; $\supset$ Suppose $x \in \bigcap_{\mathfrak{p}} N_{\mathfrak{p}}$. The set $I = \{a \in \mathcal{O} \text{ such that } ax \in N\}$ is an ideal in $\mathcal{O}$. Since $\forall \mathfrak{p}\ x \in N_{\mathfrak{p}}$ (i.e $x = \dfrac{y}{a},\ y \in N,\ a \notin \mathfrak{p}$) the ideal I contains elements outside arbitrary $\mathfrak{p}$. This implies I is trivial hence $1 \in I$ ■

Definition-Theorem 5.15. Index of the lattices. Suppose M and N are two $\mathcal{O}$-lattices in K. Then the index $(M : N)_{\mathcal{O}}$ is an $\mathcal{O}$-f.i. in k defined as follows:
1) If both M and N are free of rank n then $(M : N)_{\mathcal{O}} = (\det A)$, A being the matrix of coordinates of the elements of the basis of N with respect to the basis of M.
2) Generally, $(M : N)_{\mathcal{O}} \stackrel{\text{def}}{=} \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}((M_{\mathfrak{p}} : N_{\mathfrak{p}})_{\mathcal{O}_{\mathfrak{p}}})}$.

Proof. Since change of either basis multiplies A with an invertible matrix with entries from $\mathcal{O}$, the determinant is multiplied with an element of $\mathcal{O}^*$ thus not changing the index as defined in 1). In the general case let $\{x_i\}$ be a basis of the vector space K over k which is contained in M, $\{y_j\}$ same for N. Consider a set of generators of M. Since this is a finite set, for all $\mathfrak{p}$ but a finite number all the coordinates of its elements with respect to the basis $\{x_i\}$ are in $\mathcal{O}_\mathfrak{p}$, thus $\{x_i\}$ being an $\mathcal{O}_\mathfrak{p}$-basis of $M_\mathfrak{p}$. The same is true for $\{y_j\}$ and N. This implies for all $\mathfrak{p}$ but a finite number $(M_\mathfrak{p} : N_\mathfrak{p}) = (\det A)_\mathfrak{p}$, A being the matrix of the coordinates of the basis $\{y_j\}$ with respect to the basis $\{x_i\}$. Clearly for all $\mathfrak{p}$ but another (possibly greater) finite number this ideal is trivial hence the product in the definition 2) is finite ■

Theorem 5.16. 1) $(M : N)_\mathcal{O}(N : T)_\mathcal{O} = (M : T)_\mathcal{O}$.
2) $(M : M)_\mathcal{O} = \mathcal{O}$ (the trivial f.i.).
3) Suppose $N \subset M$. Then $(M : N)_\mathcal{O} \subset \mathcal{O}$, the equality holding iff $M = N$. If $\mathcal{O} = \mathbf{Z}$ then $(M : N)_\mathbf{Z}$ is generated by the usual index $(M : N)$.
4) If $l : K \to K$ is an invertible k-linear map then $(l(M) : l(N))_\mathcal{O} = (M : N)_\mathcal{O}$.

Proof. Immediate consequence of the definition and of the Theorem 5.9 ■

Definition 5.17 (cf. the proof of Theorem 4.7). Suppose $N \subset K$ is an $\mathcal{O}$-submodule. Then the dual module $D_\mathcal{O}(N) \stackrel{\text{def}}{=} \{y \in K \text{ such that } \forall x \in N\ Tr(xy) \in \mathcal{O}\}$.

Theorem 5.18. Suppose $N, M \subset K$ are $\mathcal{O}$-lattices. Then
1) If $N = \langle\{e_i\}\rangle$ is a free $\mathcal{O}$-module of rank n than $D_\mathcal{O}(N)$ is also free of rank n generated by the dual basis $\{f_j\}$.
2) $D_\mathcal{O}(N)$ is an $\mathcal{O}$-lattice.
3) $D_\mathcal{O}(D_\mathcal{O}(N)) = N$.
4) $(D_\mathcal{O}(N) : D_\mathcal{O}(M))_\mathcal{O} = (M : N)_\mathcal{O}$.
5) Suppose $\mathfrak{p} \subset \mathcal{O}$ is a prime ideal. Then $(D_\mathcal{O}(N))_\mathfrak{p} = D_{\mathcal{O}_\mathfrak{p}}(N_\mathfrak{p})$.

Proof. We start with the proof of 5). In fact both sides coincide with the set $\{y \in K$ such that $\forall x \in N\ Tr(xy) \in \mathcal{O}_\mathfrak{p}\}$. It looks natural to use the notation $D_{\mathcal{O}_\mathfrak{p}}(N)$ for this set besides N is not a $\mathcal{O}_\mathfrak{p}$-module. Since $N \subset N_\mathfrak{p}$, $D_{\mathcal{O}_\mathfrak{p}}(N_\mathfrak{p}) \subset D_{\mathcal{O}_\mathfrak{p}}(N)$. Since Tr is k-bilinear $D_{\mathcal{O}_\mathfrak{p}}(N) \subset D_{\mathcal{O}_\mathfrak{p}}(N_\mathfrak{p})$. For the same reason $(D_\mathcal{O}(N))_\mathfrak{p} \subset D_{\mathcal{O}_\mathfrak{p}}(N)$. Finally, to prove that $D_{\mathcal{O}_\mathfrak{p}}(N) \subset (D_\mathcal{O}(N))_\mathfrak{p}$ one should consider an arbitrary $y \in D_{\mathcal{O}_\mathfrak{p}}(N)$ and then multiply it with the product of the denominators of $Tr(yx_i)$, $\{x_i\}$ being a set of generators of the $\mathcal{O}$-module N, to obtain the element of $D_\mathcal{O}(N)$ ■

1) See problem 36 ■
2) Let $M = \langle\{e_i\}\rangle$, $\{e_i\}$ being some k-basis of K contained in N. Let a be the product of the denominators of the coordinates of some set of generators of the lattice N with respect to that basis. Then $aN \subset M$ hence $M \subset N \subset a^{-1}M$. This implies $D_{\mathcal{O}}(a^{-1}M) \subset D_{\mathcal{O}}(N) \subset D_{\mathcal{O}}(M)$, therefore $D_{\mathcal{O}}(N)$ is an $\mathcal{O}$-lattice by 1) and by the Theorem 5.10 ■
3) Clear for a free lattice, for the general case use 5) and the Theorem 5.14 ■
4) For a free lattice see Problem 41, for the general case use 5) and the Theorem 5.9 ■

Definition-Theorem 5.19. Suppose N is an $\mathcal{O}$-lattice in K. The $\mathcal{O}$ - f.i. in k $\mathfrak{d}_{\mathcal{O}}(N) \stackrel{\text{def}}{=} (D_{\mathcal{O}}(N) : N)_{\mathcal{O}}$ is called the discriminant of N. The notation $\mathfrak{d}_{K/k}$ is often used for the $\mathfrak{d}_{\mathcal{O}}(\mathcal{O}_K)$. The latter is an ideal in $\mathcal{O}$.

Proof. Since $\mathcal{O}_K \subset D_{\mathcal{O}}(\mathcal{O}_K)$ the Theorem 5.16 3) ends the proof ■

Theorem 5.20. Suppose $N, M \subset K$ are $\mathcal{O}$-lattices. Then
1) If $N = \langle\{e_i\}\rangle$ is a free $\mathcal{O}$-module then $\mathfrak{d}_{\mathcal{O}}(N) = (\det Tr(e_i e_j))$.
2) $\mathfrak{d}_{\mathcal{O}}(N) = \mathfrak{d}_{\mathcal{O}}(M)(M : N)^2_{\mathcal{O}}$.
3) Suppose $N \subset M$. Then $\mathfrak{d}_{\mathcal{O}}(N) \subset \mathfrak{d}_{\mathcal{O}}(M)$, the equality holding iff $M = N$.
4) $\mathfrak{d}_{\mathcal{O}}(N) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{v}_{\mathfrak{p}}(\mathfrak{d}_{\mathcal{O}_{\mathfrak{p}}}(N_{\mathfrak{p}}))}$.

Proof. 1) See Problem 42 ■
2) An easy consequence of the theorems 5.16 1) and 5.18 4) ■
3) This is a consequence of 2) and the Theorem 5.16 3) ■
4) Use the definition of the index and the Theorem 5.18 5) ■

Remark. If N is a free $\mathcal{O}$-module the formula from 1) defines the element $\Delta_{\mathcal{O}}(N) \in k^*/(\mathcal{O}^*)^2$ generating $\mathfrak{d}_{\mathcal{O}}(N)$. If $\mathcal{O} = \mathbf{Z}$ the notation $\Delta(N)$ (resp. Δ_K for $N = \mathcal{O}_K$) is used. Since $(\mathbf{Z}^*)^2 = \{1\}$ $\Delta(N)$ (resp. Δ_K) is an element of $\mathbf{Q}$ (resp. of $\mathbf{Z}$).

Definition 5.21. The prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ lies over the prime ideal $\mathfrak{p} \subset \mathcal{O}$ (notation $\mathfrak{P} \,|\, \mathfrak{p}$) iff $\mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$.

Theorem 5.22. 1) $\mathcal{O}_K$ is a Dedekind domain.
2) Suppose $\mathfrak{p} \subset \mathcal{O}$ is a prime ideal. Then $(\mathcal{O}_K)_{\mathfrak{p}}$ is the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in K.
3) For any prime ideal $\mathfrak{p} \subset \mathcal{O}$ there exists a prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ (not necessary unique) such that $\mathfrak{P} \,|\, \mathfrak{p}$. Conversely, for any nonzero prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ $\mathfrak{P} \cap \mathcal{O} \neq (0)$.

Proof. 1) By the Theorem 5.11 $\mathcal{O}_K$ is a NICD. Suppose $\mathfrak{P} \subset \mathcal{O}_K$ is a nonzero prime ideal. Let $0 \neq x \in \mathfrak{P}$. Then the minimal polynomial $P_{x,k}(T)$ is monic with coefficients in $\mathcal{O}$. Since $P_x(x) = 0$ its free term is an element of $\mathfrak{p} \stackrel{\text{def}}{=} \mathfrak{P} \cap \mathcal{O}$. Since P_x is irreducible over k, $\mathfrak{p}$ is nonzero. The intersection of the prime ideal with a subring is clearly prime, thus $\mathfrak{p}$ is prime and therefore maximal. This implies $k_\mathfrak{p} \stackrel{\text{def}}{=} \mathcal{O}/\mathfrak{p}$ is a field. Consider the quotient ring $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. Since $\mathcal{O}_K$ is a $\mathcal{O}$-module of finite rank this ring is a $k_\mathfrak{p}$-algebra of finite dimension, $\mathfrak{P}/\mathfrak{p}\mathcal{O}_K$ being a prime ideal in it, thus $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/(\mathfrak{P}/\mathfrak{p}\mathcal{O}_K)$ is a finite-dimensional $k_\mathfrak{p}$-algebra without zero divisors. Problem 43 implies it is a field. The identity map $\mathcal{O}_K \to \mathcal{O}_K$ defines a surjective ring homomorphism $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{P}$ with the kernel $\mathfrak{P}/\mathfrak{p}\mathcal{O}_K$, hence $(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)/(\mathfrak{P}/\mathfrak{p}\mathcal{O}_K) \simeq \mathcal{O}_K/\mathfrak{P}$. This means that $\mathcal{O}_K/\mathfrak{P}$ is a field hence $\mathfrak{P}$ is a maximal ideal ■

2) $x \in (\mathcal{O}_K)_\mathfrak{p}$ means that $x = \dfrac{y}{a},\ y \in \mathcal{O}_K,\ a \in \mathcal{O},\ a \notin \mathfrak{p}$. Since $y \in \mathcal{O}_K,\ \ y^m + \sum\limits_{i=0}^{m-1} a_i y^i = 0$ for some $\{a_i \in \mathcal{O}\}$ therefore $x^m + \sum\limits_{i=0}^{m-1} \dfrac{a_i}{a^{m-i}} x^i = 0$ hence x is integral over $\mathcal{O}_\mathfrak{p}$. Conversely, suppose x is integral over $\mathcal{O}_\mathfrak{p}$. Then $x^m + \sum\limits_{i=0}^{m-1} \dfrac{a_i}{b_i} x^i = 0$ $(\forall i \ \ b_i \notin \mathfrak{p})$. It is easy to check that $x \prod\limits_{i=0}^{m-1} b_i$ is integral over $\mathcal{O}$ ■

3) The second statement has already been proved in 1). Now start with the prime ideal $\mathfrak{p} \subset \mathcal{O}$. Consider the ideal $\mathfrak{p}\mathcal{O}_K \subset \mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_K \neq \mathcal{O}_K$ (otherwise $\mathcal{O}_K = \mathfrak{p}^{-1}\mathcal{O}_K \Rightarrow \mathfrak{p}^{-1} \subset \mathcal{O}_K \Rightarrow \mathfrak{p}^{-1} \subset \mathcal{O}$ which contradicts the properties of the Dedekind domain).This implies there exists a maximal ideal $\mathfrak{P} \subset \mathcal{O}_K$ such that $\mathfrak{p}\mathcal{O}_K \subset \mathfrak{P} \Rightarrow \mathfrak{P}$ lies over $\mathfrak{p}$ ■

Theorem-Definition 5.23. $D_\mathcal{O}(\mathcal{O}_K)$ is an $\mathcal{O}_K$-f.i. in K containing $\mathcal{O}_K$. The different (notation $\mathfrak{D}$ or $\mathfrak{D}_{K/k}$) is an ideal in $\mathcal{O}_K$ defined by the formula $\mathfrak{D} \stackrel{\text{def}}{=} (D_\mathcal{O}(\mathcal{O}_K))^{-1}$.

Proof. Use the Theorem 5.18 2) and the definition of the dual lattice ■

Theorem 5.24. Suppose $x \in \mathcal{O}_K$ is a primitive element (i.e. $K = k(x)$), $P_x \in \mathcal{O}[T]$ its minimal polynomial. Then
1) $\mathcal{O}[x]$ is an $\mathcal{O}$-lattice in K.
2) $D_\mathcal{O}(\mathcal{O}[x]) = (P'(x))^{-1}\mathcal{O}[x]$.
3) $\mathfrak{d}_\mathcal{O}(\mathcal{O}[x]) = (N_{K/k}(P'_x(x))) = (\Delta_{P_x})$.
4) $\mathcal{O}_K = \mathcal{O}[x] \Leftrightarrow \mathfrak{D}_{K/k} = (P'_x(x))$.

Proof. 1) Clear since x is integral over $\mathcal{O}$ and primitive ■

2) Suppose $P_x[T] = T^n + \sum\limits_{i=0}^{n-1} a_i T^i, \quad a_i \in \mathcal{O}; \quad \dfrac{P_x[T]}{T-x} = T^{n-1} + \sum\limits_{j=0}^{n-2} b_j T^j, \quad b_i \in K$. Then the two $\mathcal{O}$-lattices $\langle 1, x, \ldots, x^{n-1} \rangle$ and $\langle b_0, b_1, \ldots, b_{n-2}, 1 \rangle$ coincide. Indeed, the system of equations $\{a_0 = -b_0 x; \ a_i = b_{i-1} - x b_i \text{ for } 1 \leq i \leq n-2, \quad a_{n-1} = b_{n-2} - x\}$ provides us with a linear expression of the elements b_j via x^i and vice versa with coefficients in $\mathcal{O}$ (namely, $b_j = \sum\limits_{i=j+1}^{n-1} a_i x^{i-1-j} + x^{n-1-j}, \quad x^i$ may be reconstructed from these expressions one by one). Now it is possible to calculate the dual basis for $\langle b_0, b_1, \ldots, b_{n-2}, b_{n-1} = 1 \rangle$. Consider the set of polynomials $\{P_r(T) \in \overline{k}[T], \ 0 \leq r \leq n-1\}$, $P_r(T) \stackrel{\text{def}}{=} \sum\limits_{\sigma \in \Sigma_{K/k}^{\overline{k}/k}} \left(\dfrac{P_x(T)}{T - \sigma(x)} \right) \dfrac{\sigma(x)^r}{P_x'(\sigma(x))} - T^r$. Since P_x is separable it has no common roots with its derivative, hence the definition is correct (neither denominator equals zero). By the construction each P_r has at least n different roots (namely, all $\sigma(x)$) being of the degree $\leq n-1$, therefore $\forall r, \ 0 \leq r \leq n-1, P_r = 0$. On the other hand the direct calculation leads to $P_r = \sum\limits_{j=0}^{n-1} Tr \left(\dfrac{x^r}{P_x'(x)} b_j \right) T^j - T^r$, hence $Tr \left(\dfrac{x^i}{P_x'(x)} b_j \right) = \delta_{ij}$. This means that the dual lattice to one generated by b^j (hence to one generated by x^i) has the basis $\{ \dfrac{x^i}{P_x'(x)}, \ 0 \leq i \leq n-1 \}$ ■

3) and 4) Now these become direct consequences of the definitions of the norm (resp. of the different) ■

What remains is divided in two parts.

First, we prove that the decomposition of a prime ideal of $\mathcal{O}$ to the product of prime ideals in $\mathcal{O}_K$, the different and the discriminant may be calculated "locally" in terms of the finite extensions of complete fields of p-adic type.

Second, we study what happens to the prime ideal $\mathfrak{p} \subset \mathcal{O}$ in the finite extension $\mathcal{O}_K/\mathcal{O}$, $\mathcal{O}$ being a complete d.v.r.

Theorem 5.25. Suppose K/k is a finite extension of the fields, $||\ ||: K \to \mathbf{R}_{\geq 0}$ an absolute value such that its restriction to k makes k a complete metric space. Then the topology of the metric space K coincides with the topology of the coordinate space k^n. In particular, the absolute value $||\ ||$, if exists, is defined by its restriction to k.

Remark. In the proof we suppose that k is locally compact and $||\ ||_k$ is nontrivial (thus covering the arithmetic case). The statement of the Theorem is still true in the general case, the proof being more technical.

Proof. Choose a basis $\{e_i,\ 1 \leq i \leq n\}$ of the k-vector space K. By definition, the length of the vector in the coordinate space metric is given by the formula $||\sum a_i e_i||_0 \stackrel{\text{def}}{=} \max_i(||a_i||)$. To prove the first statement it suffices to find two real constants $c_1, c_2 > 0$ such that $\forall x \in K\ \ ||x|| \leq c_1||x||_0$ and $\forall x \in K\ \ ||x||_0 \leq c_2||x||$. Clearly one may choose $c_1 := \sum_i ||e_i||$, then the first inequality holds by the triangle inequality for the absolute value function $||\ ||$. In particular, the function $||x||$ is continuous in the coordinate space topology. Consider the set $T_1 \stackrel{\text{def}}{=} \{x \in K \text{ such that } ||x||_0 = 1\}$. Then T_1 is a closed subset of the unit ball in $B_1^n \subset k^n$ where B_1 is the unit ball in k. Since k is locally compact there exists some ball in k which is compact. Moving the center to 0 and multiplying with some big $c \in k$ (which exists since $||\ ||_k$ is nontrivial) one gets a compact set containing B_1. Hence B_1, B_1^n and T_1 are all compact. Therefore the continuous function $||\ ||$ achieves its lower bound on T_1, namely, $\exists x_1 \in T_1$ such that $||x_1|| = \inf_{x \in T_1} ||x||$. Since $0 \notin T_1$, $||x_1|| > 0$. Now choose $c_2 := (||x_1||)^{-1}$, then the second inequality holds. To prove the second statement suppose that $||\ ||_1$ and $||\ ||_2$ are two absolute value functions on K such that their restrictions to k coincide. Then the coordinate space topology on k^n is the same in both cases, hence by the first statement of the Theorem $||\ ||_1$ and $||\ ||_2$ define the same topology on K. By the Theorem 2.9 they are equivalent ($||\ ||_1 = ||\ ||_2^t$). Since the restrictions to k coincide by the assumption, the two absolute values are in fact the same ■

Remark. The condition that $(k,\ ||\ ||)$ is a complete metric space is essential.

Recall the agreed notations and introduce some more. $\mathcal{O}$ is a Dedekind domain, k its field of fractions, $\mathfrak{p} \subset \mathcal{O}$ some nonzero prime ideal, $\mathcal{O}_\mathfrak{p}$ the corresponding local ring. Let $\widehat{k_\mathfrak{p}}$ be the completion of the field k with respect to the absolute value $||\ ||_\mathfrak{p}$ (which is defined by the function $\mathrm{v}_\mathfrak{p}$), $\widehat{\mathcal{O}}_\mathfrak{p}$ being the topological closure of $\mathcal{O}_\mathfrak{p}$ in $\widehat{k_\mathfrak{p}}$. K/k is a finite separable extension of degree n, $\mathcal{O}_K$ the integral closure of $\mathcal{O}$ in K ("ring of integers"). By the Theorem 5.22 $\mathcal{O}_K$ is a Dedekind domain.

As in the "Geometry of numbers" consider the tensor product $K \otimes_k \widehat{k_\mathfrak{p}}$. By the Theorem 3.52 there exists a $\widehat{k_\mathfrak{p}}$-algebra isomorphism $K \otimes_k \widehat{k_\mathfrak{p}} \simeq \oplus K_i$ where $K_i/\widehat{k_\mathfrak{p}}$ are finite separable extensions of degrees n_i such that $\sum n_i = n$. The collection of isomorphism classes of extensions $K_i/\widehat{k_\mathfrak{p}}$ is uniquely defined. If one chooses a k-basis in K and a $\widehat{k_\mathfrak{p}}$-basis in each K_i then both sides become topological coordinate spaces over $\widehat{k_\mathfrak{p}}$, the topology not depending on the choice and the isomorphism above becoming a homeomorphism.

In what follows we identify both sides of the isomorphism above with an n-dimensional $\widehat{k_\mathfrak{p}}$-algebra $\mathbf{V}_\mathfrak{p}$ endowed with the topology of coordinate space and carrying both structures (those of the tensor product and of the direct sum). The field K will be identified with its canonical image in $\mathbf{V}_\mathfrak{p}$ which is a subring ($x \mapsto x \otimes 1$ in the standard construction of the tensor product), π_i will denote canonical projections $\mathbf{V}_\mathfrak{p} \to K_i$.

Theorem 5.26. 1) The three sets below are in the one-to-one correspondence:
1) Different prime ideals $\mathfrak{P}_i \subset \mathcal{O}_K$ lying over $\mathfrak{p} \subset \mathcal{O}$,
2) Different absolute value functions $||\ || : K \to \mathbf{R}_{\geq 0}$ extending the $\mathfrak{p}$-adic absolute value,
3) Components K_i of the direct sum $\mathbf{V}_\mathfrak{p} = \oplus K_i$.

Proof. 1) $\leftrightarrow$ 2) By the theorems 5.22 and 5.9 $\mathfrak{p}\mathcal{O}_K = \prod \mathfrak{P}_i^{e_i}$ where $\{\mathfrak{P}_i\}$ is the full set of prime ideals in $\mathcal{O}_K$ lying over $\mathfrak{p}$, e_i are some positive integers. Suppose $0 \neq a \in \mathcal{O}$. Calculate $\mathrm{v}_{\mathfrak{P}_i}(a)$. The ideal $(a) \subset \mathcal{O}$ may be represented in the form $(a) = \prod \mathfrak{q}_j$, $\mathfrak{q}_j$ being some prime ideals in $\mathcal{O}$. Then $\mathrm{v}_{\mathfrak{P}_i}(a) = \mathrm{v}_{\mathfrak{P}_i}(a\mathcal{O}_K) = \mathrm{v}_{\mathfrak{P}_i}(\prod(\mathfrak{q}_j\mathcal{O}_K))$. If $\mathfrak{q}_j \neq \mathfrak{p}$ then it contains some nonzero element outside $\mathfrak{p}$ thus $\mathfrak{q}_j\mathcal{O}_K$ contains a nonzero element outside $\mathfrak{P}_i$ which implies $\mathrm{v}_{\mathfrak{P}_i}(\mathfrak{q}_j\mathcal{O}_K) = 0$. Therefore $\mathrm{v}_{\mathfrak{P}_i}(a) = \mathrm{v}_{\mathfrak{P}_i}(\mathfrak{p}^{\mathrm{v}_\mathfrak{p}(a)}\mathcal{O}_K) = e_i\mathrm{v}_\mathfrak{p}(a)$. Suppose the $\mathfrak{p}$-adic absolute value on k is given by the formula $||a||_\mathfrak{p} = s^{-\mathrm{v}_\mathfrak{p}(a)}$, then the function $||b||_{\mathfrak{P}_i} \stackrel{\mathrm{def}}{=} s^{-\mathrm{v}_{\mathfrak{P}_i}(b)/e_i}$ defines an absolute value on K extending $||\ ||_\mathfrak{p}$. Clearly $(\mathcal{O}_K)_{\mathfrak{P}_i}$ and $\mathfrak{P}_i(\mathcal{O}_K)_{\mathfrak{P}_i}$ are the corresponding valuation ring and valuation ideal.
Conversely, start with an absolute value function $||\ ||$ on K extending the $\mathfrak{p}$-adic one on

k. Its valuation ring $\mathcal{R} = \{x \in K \text{ such that } ||x|| \leq 1\}$ contains $\mathcal{O}$ and is integrally closed hence $\mathcal{O}_K \subset \mathcal{R}$. Let $\mathfrak{m} \subset \mathcal{R}$ be the maximal ideal. Then $\mathfrak{m} \cap \mathcal{O}_K$ contains $\mathfrak{p}\mathcal{O}_K$ and is prime, hence it coincides with some $\mathfrak{P}_i$. This implies $\forall x \in \mathcal{O}_K \setminus \mathfrak{P}_i \;\; ||x|| = 1$ hence $(\mathcal{O}_K)_{\mathfrak{P}_i} \subset \mathcal{R}$ and $\mathfrak{m} \cap (\mathcal{O}_K)_{\mathfrak{P}_i} = \mathfrak{P}_i(\mathcal{O}_K)_{\mathfrak{P}_i}$. Since $(\mathcal{O}_K)_{\mathfrak{P}_i}$ is a d.v.r the ideal $\mathfrak{P}_i(\mathcal{O}_K)_{\mathfrak{P}_i}$ is principal. Let $\pi \in (\mathcal{O}_K)_{\mathfrak{P}_i}$ be its generator, then $\forall x \in (\mathcal{O}_K)_{\mathfrak{P}_i} \;\; ||x|| = ||\pi||^{\mathrm{v}_{\mathfrak{P}_i}(x)}$. Since K is the field of fractions of the ring $(\mathcal{O}_K)_{\mathfrak{P}_i}$ the same formula holds for all $x \in K$ which ends the proof ■

2) $\leftrightarrow$ 3) By the first part of the proof at least one extension of the absolute value function $||\;||_{\mathfrak{p}}$ from $\widehat{k_{\mathfrak{p}}}$ to K_i does exist, by the Theorem 5.25 it is unique. The map $K \xrightarrow{\pi_i} K_i$ is a ring homomorphism hence an inclusion (K is a field). Now the absolute value on K may be defined using the absolute value on K_i just constructed.

Conversely, start with an absolute value function $||\;||$ on K extending the $\mathfrak{p}$-adic one on k. Consider K as a subspace of the topological space $\mathbf{V}_{\mathfrak{p}}$. By the triangle inequality the function $||\;||$ is continuous on K (cf. the first part of the proof of the previous theorem). Since k is dense in $\widehat{k_{\mathfrak{p}}}$, $K = K \otimes_k k$ is dense in $\mathbf{V}_{\mathfrak{p}} = K \otimes_k \widehat{k_{\mathfrak{p}}}$. This implies that the function $||\;||$ may in a unique way be extended by continuity to the $\widehat{k_{\mathfrak{p}}}$-algebra $\mathbf{V}_{\mathfrak{p}}$ preserving the property $||xy|| = ||x||||y||$ and enjoying the strict triangle inequality. Consider the canonical inclusion $\widehat{k_{\mathfrak{p}}} \hookrightarrow \mathbf{V}_{\mathfrak{p}}$ (i.e. $x \mapsto 1 \otimes x$ for the tensor product structure or $x \mapsto (x, x, \ldots, x)$ for the direct sum structure). By the assumption $||\;||$ extends the $\mathfrak{p}$-adic absolute value on k hence by continuity also that on $\widehat{k_{\mathfrak{p}}}$. Let $I_0 = \{x \in \mathbf{V}_{\mathfrak{p}} \text{ such that } ||x|| = 0\}$. By the triangle inequality I_0 is an ideal, by the multiplicativity of the $||\;||$ it is prime and therefore by the Problem 43 maximal. Let $I_i = \ker(\pi_i : \mathbf{V}_{\mathfrak{p}} \to K_i)$. Since K_i is a field, I_i is maximal. Any nontrivial ideal J of the algebra $\oplus K_i$ is contained in some of the I_i (otherwise $\forall i \; \exists y_i \in J$ such that the i-th coordinate of y_i is invertible, therefore $\sum a_i y_i$, a_i having i-th coordinate 1 others 0, is an invertible element of J). Hence $\{I_i\}$ is the full list of maximal ideals of $\mathbf{V}_{\mathfrak{p}}$. This implies that $\exists i$ such that $I_0 = I_i$. Then by the triangle inequality $||x||$, $x \in \mathbf{V}_{\mathfrak{p}}$ depends only on the residue of $x \mod I_i$ therefore $||x|| = ||\pi_i(x)||_0$ where $||\;||_0$ is a function on K_i which defines an absolute value hence coincides with the unique extension of the $\mathfrak{p}$-adic absolute value from $\widehat{k_{\mathfrak{p}}}$ to K_i ■

Remark. We will use the notation π_i both for the map $\pi_i : \mathbf{V}_{\mathfrak{p}} \to K_i$ and for its restriction to K.

Theorem 5.27. Choose an algebraic closure $\overline{\widehat{k_{\mathfrak{p}}}}/\widehat{k_{\mathfrak{p}}}$ and identify $\overline{k}$ with the subfield of its elements algebraic over k. Then the natural map $\sigma \mapsto \sigma \circ \pi_i$ defines a one-to-one correspondence $\bigcup \Sigma_{K_i/\widehat{k_{\mathfrak{p}}}}^{\overline{\widehat{k_{\mathfrak{p}}}}/\widehat{k_{\mathfrak{p}}}} \xrightarrow{\sim} \Sigma_{K/k}^{\overline{k}/k}$.

Proof. Consider both structures on $\mathbf{V}_{\mathfrak{p}}$. Then there exists a triple correspondence $\bigcup \Sigma_{K_i/\widehat{k_{\mathfrak{p}}}}^{\overline{\widehat{k_{\mathfrak{p}}}}/\widehat{k_{\mathfrak{p}}}} = \mathrm{Hom}_{\widehat{k_{\mathfrak{p}}}-\mathrm{alg}}(\oplus K_i,\ \overline{\widehat{k_{\mathfrak{p}}}}) = \mathrm{Hom}_{\widehat{k_{\mathfrak{p}}}-\mathrm{alg}}(\mathbf{V}_{\mathfrak{p}},\ \overline{\widehat{k_{\mathfrak{p}}}}) = \mathrm{Hom}_{\widehat{k_{\mathfrak{p}}}-\mathrm{alg}}(K \otimes_k \widehat{k_{\mathfrak{p}}},\ \overline{\widehat{k_{\mathfrak{p}}}}) = \Sigma_{K/k}^{\overline{k}/k}$. In fact, according to the proof of the previous theorem $\{I_i\}$ is the full list of maximal ideals of $\oplus K_i$ whence the first canonical equality. By the universal property of the tensor product $\mathrm{Hom}_{k-\mathrm{alg}}(K \otimes_k \widehat{k_{\mathfrak{p}}},\ \overline{\widehat{k_{\mathfrak{p}}}}) = \mathrm{Hom}_{k-\mathrm{alg}}(K,\ \overline{\widehat{k_{\mathfrak{p}}}}) \times \mathrm{Hom}_{k-\mathrm{alg}}(\widehat{k_{\mathfrak{p}}},\ \overline{\widehat{k_{\mathfrak{p}}}})$. The subset of the $\widehat{k_{\mathfrak{p}}}$-linear homomorhisms in the left side corresponds to the subset of the elements in the right side which have the identity map in the second factor. Since the image of K under any inclusion to $\overline{\widehat{k_{\mathfrak{p}}}}$ is contained in $\overline{k}$, the first factor of the right side equals $\Sigma_{K/k}^{\overline{k}/k}$ which establishes the last canonical equality ■

Theorem-Definition 5.28. Suppose K/k is normal. Let $G = \mathrm{Gal}\,(K/k)$. Then
1) G acts transitively on the set of ideals $\mathfrak{P}_i \mid \mathfrak{p}$. All the numbers e_i in the product $\mathfrak{p}\mathcal{O}_K = \prod \mathfrak{P}_i^{e_i}$ are the same.
2) The stationary subgroup of the ideal $\mathfrak{P}$ under the action of G (i.e. $G_{\mathfrak{P}} \stackrel{\mathrm{def}}{=} \{g \in G$ such that $g\mathfrak{P} = \mathfrak{P}\}$) is called the decomposition group of the ideal $\mathfrak{P}$. The subgroups $G_{\mathfrak{P}_i}$ are conjugate.
3) $K_i = \pi_i(K)\widehat{k_{\mathfrak{p}}}$, the extensions $K_i/\widehat{k_{\mathfrak{p}}}$ are all isomorphic and Galois, $\mathrm{Gal}\,(K_i/\widehat{k_{\mathfrak{p}}}) \simeq G_{\mathfrak{P}}$.

Proof. 1) Supppose that for some $\mathfrak{P}_1, \mathfrak{P}_2 \mid \mathfrak{p}$ $\forall g \in G\ g(\mathfrak{P}_1) \neq \mathfrak{P}_2$. Choose an element $a \in \mathfrak{P}_1$ such that $(a) + \prod_{i \neq 1} \mathfrak{P}_i = (1)$ (which is possible because $\forall i$ $\mathfrak{P}_1$ and $\mathfrak{P}_i$ are maximal and different thus coprime). Then $\forall g \in G$ $(g(a)) + \prod_{\mathfrak{P} \neq g(\mathfrak{P}_1)} \mathfrak{P} = (1)$. Since $g(\mathfrak{P}_1) \neq \mathfrak{P}_2$ by the assumption, this means that $\forall g \in G$ $g(a) \notin \mathfrak{P}_2$. But $\prod_{g \in G} g(a) = N_{K/k}(a) \in k$. Since $a \in \mathfrak{P}_1$, $N_{K/k}(a) \in \mathfrak{P}_1 \cap k = \mathfrak{p} \subset \mathfrak{P}_2$, therefore $\exists g$ such that $g(a) \in \mathfrak{P}_2$, this contradiction ending the proof of the first statement. The second one is clear since $g(\mathfrak{p}\mathcal{O}_K) = \mathfrak{p}\mathcal{O}_K$ ■
2) If $g(\mathfrak{P}_1) = \mathfrak{P}_2$ then $gG_{\mathfrak{P}_1}g^{-1} = G_{\mathfrak{P}_2}$, now use 1) ■
3) K is dense in $\mathbf{V}_{\mathfrak{p}}$ hence $K\widehat{k_{\mathfrak{p}}} \subset \mathbf{V}_{\mathfrak{p}}$ is a dense $\widehat{k_{\mathfrak{p}}}$-vector subspace. Therefore $K\widehat{k_{\mathfrak{p}}} = \mathbf{V}_{\mathfrak{p}}$ thus $\forall i$ $\pi_i(K)\widehat{k_{\mathfrak{p}}} = K_i$. Suppose $g(\mathfrak{P}_1) = \mathfrak{P}_2$. Then $\forall a \in K$ $\mathrm{v}_{\mathfrak{P}_2}(g(a)) = \mathrm{v}_{\mathfrak{P}_1}(a)$ hence $||g(a)||_{\mathfrak{P}_2} = ||a||_{\mathfrak{P}_1}$ (the two absolute values agree on k). The action of G on K extends to $\mathbf{V}_{\mathfrak{p}}$ by the $\widehat{k_{\mathfrak{p}}}$-linearity, therefore it is continuous. This implies the last formula remains valid on $\mathbf{V}_{\mathfrak{p}}$. From the construction in the Theorem 5.26 one knows that $\{x \in \mathbf{V}_{\mathfrak{p}}$ such that $||x||_{\mathfrak{P}_i} = 0\} = \ker(\pi_i)$, thus $g(\ker(\pi_1)) = \ker(\pi_2)$ which implies $K_1 \simeq K_2$. By the Theorem 3.48 $K_i/\widehat{k_{\mathfrak{p}}}$ is Galois and $\mathrm{Gal}\,(K_i/\widehat{k_{\mathfrak{p}}}) = \mathrm{Gal}\,(\pi_i(K)/\pi_i(K) \cap \widehat{k_{\mathfrak{p}}}) = \mathrm{Gal}\,(K/K \cap \{x \in \mathbf{V}_{\mathfrak{p}}$ such that $\pi_i(x) \in \widehat{k_{\mathfrak{p}}}\})$. The last subfield consists of all the elements $a \in K$ which are

the limits of Cauchy sequences $\{a_j \in k\}$ with respect to the absolute value $||\,||_{\mathfrak{P}_i}$. Clearly if $g(\mathfrak{P}_i) = \mathfrak{P}_i$ then $g(a) = a$. Conversely, any element $h \in \mathrm{Gal}\,(K_i/\widehat{k_\mathfrak{p}})$ preserves the absolute value (the latter being unique by the Theorem 5.25) hence $h|_{\pi_i(K)}$ also preserves the absolute value, therefore after transferring to K it still preserves the absolute value $||\,||_{\mathfrak{P}_i}$. This implies $h(\mathfrak{P}_i) = \mathfrak{P}_i$ ■

Theorem 5.29. Extend the bilinear form $Tr_{K/k}(ab)$ from K to $\mathbf{V}_\mathfrak{p}$ by $\widehat{k_\mathfrak{p}}$-linearity. Use notation $\langle\ ,\ \rangle$ for the resulting form. Then $\langle a, b\rangle = \sum Tr_{K_i/\widehat{k_\mathfrak{p}}}(\pi_i(a)\pi_i(b))$.

Proof. Theorem 5.27 immediately implies $\forall x \in K\ Tr_{K/k}(x) = \sum Tr_{K_i/\widehat{k_\mathfrak{p}}}(\pi_i(x))$ whence the statement of the Theorem for $a, b \in \pi(K)$, the general case being a consequence of the $\widehat{k_\mathfrak{p}}$-linearity ■

Theorem 5.30. Extend the definitions of the lattice, of the index and of the dual lattice to $\widehat{\mathcal{O}_\mathfrak{p}}$-submodules of the $\widehat{k_\mathfrak{p}}$-algebra $\mathbf{V}_\mathfrak{p}$ (for the definition of the dual lattice use the bilinear form $\langle\ ,\ \rangle$ just defined). Suppose M, N are $\mathcal{O}$-lattices in K. Then $M\widehat{\mathcal{O}_\mathfrak{p}}, N\widehat{\mathcal{O}_\mathfrak{p}}$ are $\widehat{\mathcal{O}_\mathfrak{p}}$-lattices in $\mathbf{V}_\mathfrak{p}$ and
1) $(M : N)_\mathcal{O}\widehat{\mathcal{O}_\mathfrak{p}} = (M\widehat{\mathcal{O}_\mathfrak{p}} : N\widehat{\mathcal{O}_\mathfrak{p}})_{\widehat{\mathcal{O}_\mathfrak{p}}}$.
2) $D_\mathcal{O}(N)\widehat{\mathcal{O}_\mathfrak{p}} = D_{\widehat{\mathcal{O}_\mathfrak{p}}}(N\widehat{\mathcal{O}_\mathfrak{p}})$.
3) $\mathfrak{d}_\mathcal{O}(N)\widehat{\mathcal{O}_\mathfrak{p}} = \mathfrak{d}_{\widehat{\mathcal{O}_\mathfrak{p}}}(N\widehat{\mathcal{O}_\mathfrak{p}})$.

Proof. Since $\mathcal{O}_\mathfrak{p} \subset \widehat{\mathcal{O}_\mathfrak{p}}$ one may suppose that M and N are free modules (just change $\mathcal{O}$ to $\mathcal{O}_\mathfrak{p}$). If $\{x_j\}$ is a $\mathcal{O}$-basis of M then $\{x_j\}$ is a $\widehat{\mathcal{O}_\mathfrak{p}}$-basis of $M\widehat{\mathcal{O}_\mathfrak{p}}$, the same is true for N. Since $\langle\ ,\ \rangle$ is obtained from the trace bilinear form by the $\widehat{k_\mathfrak{p}}$-linearity, also the calculation of the dual basis leads to the same result in whichever space it is performed, whence the Theorem ■

Theorem 5.31. Suppose M, N are $\widehat{\mathcal{O}_\mathfrak{p}}$-lattices in $\mathbf{V}_\mathfrak{p} = \oplus K_i$ such that $M = \oplus\pi_i(M)$ and the same property holds for N.Then
1) $(M : N)_{\widehat{\mathcal{O}_\mathfrak{p}}} = \prod(\pi_i(M) : \pi_i(N))_{\widehat{\mathcal{O}_\mathfrak{p}}}$.
2) $D_{\widehat{\mathcal{O}_\mathfrak{p}}}(N) = \oplus D_{\widehat{\mathcal{O}_\mathfrak{p}}}(\pi_i(N))$.
3) $\mathfrak{d}_{\widehat{\mathcal{O}_\mathfrak{p}}}(N) = \prod \mathfrak{d}_{\widehat{\mathcal{O}_\mathfrak{p}}}(\pi_i(N))$.

Proof. 1) Since $\widehat{\mathcal{O}_\mathfrak{p}}$ is a principal ideal ring, M and N are free $\widehat{\mathcal{O}_\mathfrak{p}}$-modules. By the assumption the transition matrix is a block matrix, hence its determinant equals the product of the determinants of the blocks■

2) By the Theorem 5.29 the subspaces K_i are pairwise orthogonal, the restriction of the $\langle\ ,\ \rangle$ to K_i coinciding with the $Tr_{K_i/\widehat{k_\mathfrak{p}}}(ab)$-bilinear form ■
3) Now use 1) for $M = D_{\widehat{\mathcal{O}}_\mathfrak{p}}(N)$ ■

Remark. The statement of the Theorem is not true for general $\widehat{\mathcal{O}}_\mathfrak{p}$-lattices.

We are now going to study an important particular case where two theorems above are applicapble.

Definition 5.32. Suppose I is an $\mathcal{O}_K$- f.i. in K. Then its norm $N_{K/k}(I) \stackrel{\text{def}}{=} (\mathcal{O}_K : I)_\mathcal{O}$.

Definition-Theorem 5.33. Let $\mathcal{O}_i$ be the valuation ring in K_i (i.e. $\mathcal{O}_i \stackrel{\text{def}}{=} \{x \in K_i$ such that $||x|| \leq 1\}$, $||\ ||$ being the unique absolute value on K_i which extends the $\mathfrak{p}$-adic absolute value on $\widehat{k_\mathfrak{p}}$). Then
1) $\mathcal{O}_i$ is the integral closure of $\widehat{\mathcal{O}}_\mathfrak{p}$ in K_i.
2) $\{$the topological closure of $\mathcal{O}_K\mathcal{O}_\mathfrak{p}$ in $\mathbf{V}_\mathfrak{p}\} = \mathcal{O}_K\widehat{\mathcal{O}}_\mathfrak{p} = \oplus\mathcal{O}_i$.

Proof. 1) By the Theorem 2.3 $\mathcal{O}_i$ is integrally closed therefore contains the integral closure of the subring $\widehat{\mathcal{O}}_\mathfrak{p}$. Conversely, if $x \in K_i$ lies outside $\mathcal{O}_i$ then $||x|| > 1$ hence x cannot be integral over $\widehat{\mathcal{O}}_\mathfrak{p}$ by the Theorem 2.4 ■
2) Since any element of $\mathcal{O}_K\widehat{\mathcal{O}}_\mathfrak{p}$ is integral over $\widehat{\mathcal{O}}_\mathfrak{p}$, 1) implies $\mathcal{O}_K\widehat{\mathcal{O}}_\mathfrak{p} \subset \oplus\mathcal{O}_i$. Since $\mathcal{O}_K\widehat{\mathcal{O}}_\mathfrak{p}$ is topologically closed in $\mathbf{V}_\mathfrak{p}$, it now suffices to prove that $\mathcal{O}_K\mathcal{O}_\mathfrak{p}$ is dense in $\oplus\mathcal{O}_i$. We already know (cf. the proof of the Theorem 5.28) that K is dense in $\mathbf{V}_\mathfrak{p}$, hence $\oplus\mathcal{O}_i$ is a topological closure of $K \cap \oplus\mathcal{O}_i$. Suppose $x \in K$ is such that $x \in \oplus\mathcal{O}_i$. This implies $\forall\mathfrak{P}_i \mid \mathfrak{p}\ \ ||x||_{\mathfrak{P}_i} \leq 1$ hence the decomposition of the f.i. (x) in primes contains only non-negative powers of ideals $\mathfrak{P}_i \mid \mathfrak{p}$, thus $x \in \mathcal{O}_K\mathcal{O}_\mathfrak{p}$. Therefore $K \cap \oplus\mathcal{O}_i \subset \mathcal{O}_K\mathcal{O}_\mathfrak{p}$ which ends the proof ■

Theorem 5.34. 1) Suppose I is an $\mathcal{O}_K$-f.i. in K. Then $I\widehat{\mathcal{O}}_\mathfrak{p}$ fits the assumption of the Theorem 5.31.
2) $N_{K/k}(I)\widehat{\mathcal{O}}_\mathfrak{p} = \prod N_{K_i/\widehat{k_\mathfrak{p}}}(\pi_i(I)\mathcal{O}_i)$.
3) $N_{K/k} : \mathcal{F}(\mathcal{O}_K) \to \mathcal{F}(\mathcal{O})$ is a group homomorphism .
4) $\pi_i(\mathfrak{D}_{K/k})\mathcal{O}_i = \mathfrak{D}_{K_i/\widehat{k_\mathfrak{p}}}$.
5) $\mathfrak{d}_{K/k}\widehat{\mathcal{O}}_\mathfrak{p} = \prod \mathfrak{d}_{K_i/\widehat{k_\mathfrak{p}}}$.
6) $N_{K/k}(\mathfrak{D}_{K/k}) = \mathfrak{d}_{K/k}$.

Proof. 1) As in the proof of Theorem 5.30 one may suppose $\mathcal{O}$ is a d.v.r, thus I is a principal f.i. If $I = \mathcal{O}_K$ the statement is covered by the previous theorem. Otherwise $I = a\mathcal{O}_K$ for some $a \in K$. The $\widehat{\mathcal{O}}_\mathfrak{p}$-lattice $\oplus\pi_i(I\widehat{\mathcal{O}}_\mathfrak{p})$ consists of the vectors $x = \{x_i\}$ such that $\forall i\ ||x_i|| \leq ||a||_{\mathfrak{P}_i}$. Then $a^{-1}x$ has integer (i.e. lying in $\mathcal{O}_i$) coordinates hence $a^{-1}x \in \mathcal{O}_K\widehat{\mathcal{O}}_\mathfrak{p}$ by the $\mathcal{O}_K$-case, thus $x \in I\widehat{\mathcal{O}}_\mathfrak{p}$ ■
2) Use Theorems 5.30 and 5.31 for $M = \mathcal{O}_K,\ N = I$ ■
3) If $I = a\mathcal{O}_K$ then $N_{K/k}(I) = N_{K/k}(a)\mathcal{O}$ by the definition, hence $N_{K/k}$ is a homomorphism on the subgroup of principal fractional ideals. For the general case use 2) (all the fractional ideals in the right side are principal) ■
4)-5) Use theorems 5.30 and 5.31 ■
6) $N_{K/k}(\mathfrak{D}_{K/k}) = (\mathcal{O}_K : (D_\mathcal{O}(\mathcal{O}_K))^{-1})_\mathcal{O} =$ (by 3) above) $(\mathcal{O}_K : D_\mathcal{O}(\mathcal{O}_K))_\mathcal{O}^{-1} = (D_\mathcal{O}(\mathcal{O}_K) : \mathcal{O}_K)_\mathcal{O} = \mathfrak{d}_{K/k}$ ■

Definition 5.35. 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 5.36. 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. See problems 46 and 47 ■

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 5.37. 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 $||x|| \stackrel{\mathrm{def}}{=} ||N(x)||^{\frac{1}{n}}$.

Proof. 1) If K/k is Galois then the action of the Galois group G preserves the absolute value (cf. Theorem 5.28) 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 5.38. 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 $n = \sum e_i f_i$ 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 5.39. 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

$\mathfrak{P}^{i-1}/\mathfrak{P}^i) = e\,Tr(\bullet x \text{ acting on } \mathcal{O}_K/\mathfrak{P}) = e\,Tr_{K_\mathfrak{P}/k_\mathfrak{p}}(\overline{x})$ which ends the proof for the trace. The proof for the norm is the same ■

Theorem 5.40. $\mathrm{v}_\mathfrak{P}(\mathfrak{D}_{K/k}) \geq e-1$.

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 $\mathrm{v}_\mathfrak{p}(\mathfrak{d}_{K/k}) \geq (e-1)f \Rightarrow \mathrm{v}_\mathfrak{P}(\mathfrak{D}_{K/k}) = \frac{1}{n}\mathrm{v}_\mathfrak{P}(N_{/k}(\mathfrak{D}_{K/k})) = \frac{1}{n}\mathrm{v}_\mathfrak{P}(\mathfrak{d}_{K/k}) = \frac{e}{n}\mathrm{v}_\mathfrak{p}(\mathfrak{d}_{K/k}) \geq \frac{e(e-1)f}{n} = e-1$ (by the theorems 5.34, 5.37 and 5.38) ■

Definition 5.41. 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 5.42. 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 5.40 ■
$\Rightarrow e = 1 \Rightarrow \mathfrak{p}\mathcal{O}_K = \mathfrak{P} \Rightarrow \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = K_\mathfrak{P}$. 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 5.39 $\overline{\det Tr(x_i x_j)} = \det Tr(\overline{x_i x_j}) \neq 0$, therefore $\mathfrak{d}_{K/k} \not\subset \mathfrak{p}$ ■

Theorem 5.43. 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 5.39. Further, by the Problem 48, $D_\mathcal{O}(\mathcal{O}_K) \cap k = (Tr_{K/k}(\mathcal{O}_K))^{-1}$. 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 5.40 now ends the proof of the second equality ■

Definition-Theorem 5.44. 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 $\overline{P_1 P_2} = T^n$ 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 5.45 (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_Π 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 5.37 $\mathrm{v}_{\mathfrak{P}}(\Pi) = \frac{1}{n}\mathrm{v}_{\mathfrak{P}}(a_0) = \frac{e}{n}\mathrm{v}_{\mathfrak{p}}(a_0) = \frac{e}{n}$. Since $e \le n$, $n = e$ 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 2.19) fits), then $\#T = \#k_{\mathfrak{p}}$. For $-\infty \le r \le \infty$ 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 $\forall r\ \alpha(r) \in \mathbf{Z}$, $\beta(r) \in \mathbf{Z}$, $0 \le \beta(r) \le e-1$. The sum above becomes a polynomial in Π 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_Π is monic, since $K = k(\Pi)$, $\deg(P_\Pi) = n = e$. If a_0 is the free term of P_Π then $a_0 = \pm N_{K/k}(\Pi)$ hence by the assumption and by the Theorem 5.37 $\mathrm{v}_{\mathfrak{p}}(a_0) = 1$. 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 $\{V_r = \ker(\bullet\Pi^r), 1 \le r \le n\}$ 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 5.46 (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) $[K : k] = n = [(k_{\mathfrak{p}})_{\overline{P}} : k_{\mathfrak{p}}] \le [K_{\mathfrak{P}} : k_{\mathfrak{p}}] = f \le n$. 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 $[K_{\mathfrak{P}} : k_{\mathfrak{p}}] = \deg(P_{\overline{x}}) \le \deg(\overline{P_x}) = \deg(P_x) \le [K : k]$. 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 $\{x^i,\ 0\le i\le n-1\}$. Since $e=1$, by the Theorem 5.39 $\det Tr(\overline{x^{i+j}})=\overline{\det Tr(x^{i+j})}$. 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 5.42 and 5.20. 3) $\mathcal{O}[x]=\mathcal{O}_K$ ■

Definition-Theorem 5.47 (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 $\sigma_{\mathfrak{p}}(x \mod \mathfrak{P})\stackrel{\text{def}}{=}\sigma(x) \mod \mathfrak{P}'$ 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 5.22 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 5.48. 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 2.20 there exists a unique $y\in\mathcal{O}_{K'}$ such that $P_x(y)=0$ and $y \mod \mathfrak{P}'=\overline{y}$. Define σ by the formula $\sigma(x)=y$, then $\sigma_{\mathfrak{p}}=\gamma$ and such σ 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 γ is an isomorphism. If in addition K'/k is unramified then $[K':k]=[K'_{\mathfrak{P}'}:k_{\mathfrak{p}}]=[\gamma(K_{\mathfrak{P}}):k_{\mathfrak{p}}]\le[\sigma(K):k]$ hence $K'=\sigma(K)$ ■

Theorem 5.49 (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 5.46 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 5.36.

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. $\forall g \in G$ $g(K_0)$ is unramified (being unramified, K_0 is generated over k by a root of a Henselian polynomial, then $g(K_0)$ is generated by another root of the same polynomial, thus also unramified), hence 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 5.48, 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 5.50. The field $\mathbf{C}_p$ (or the Tate field).

The function 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 5.51.The field $\mathbf{C}_p$ contains some elements which are transcendental over $\mathbf{Q}_p$.

Proof. Search x in the form $x = \sum_{i=0}^{\infty} \zeta_i p^i$ where $\zeta_0 = 1$ and all the ζ_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 $x_n = \sum_{i=0}^{n} \zeta_i p^i$. 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 ζ_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 ζ_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 τ. 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 2.4 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 ζ_i making the degree of ζ_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 5.52 (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 $\alpha = \alpha_1, \alpha_2, \ldots \alpha_n \in k^{\mathrm{sep}}$. Suppose $\beta \in k^{\mathrm{sep}}$ and $\forall i \geq 2\ \ ||\alpha - \beta|| < ||\alpha - \alpha_i||$. Then $\alpha \in k(\beta)$.

Proof. If α' is conjugate to α 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 α and α' 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 α which is algebraic over k may admit rational approximation more close to α than some of its conjugates. Indeed, if $\beta \in k$ then all the numbers $\beta - \alpha_i$ are conjugate hence have the same absolute value.

Theorem 5.53. $\mathbf{C}_p$ is algebraically closed.

Proof. Suppose $\alpha \in \overline{\mathbf{C}_p}$, the roots of $P \stackrel{\text{def}}{=} P_{\alpha,\mathbf{C}_p}$ being $\alpha = \alpha_1, \alpha_2, \dots \alpha_n \in \overline{\mathbf{C}_p}$. WLOG one may suppose that α is integral over $\mathcal{O}_{\mathbf{C}_p}$ (otherwise multiply α 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 $\mathrm{v}_p(\text{a polynomial}) \stackrel{\text{def}}{=} \min \mathrm{v}_p(\text{coefficients})$. Suppose $\{\beta_j\}$ are the roots of Q. Then $\sum\limits_j \mathrm{v}_p(\alpha-\beta_j) = \mathrm{v}_p(Q(\alpha)) = \mathrm{v}_p(Q(\alpha)-P(\alpha)) \geq \mathrm{v}_p(Q-P)) > n \max\limits_{i\geq 2} \mathrm{v}_p(\alpha-\alpha_i)$. Therefore $\exists j_0$ such that $\mathrm{v}_p(\alpha-\beta_{j_0}) > \max\limits_{i\geq 2} \mathrm{v}_p(\alpha-\alpha_i)$ thus $\forall i (2 \leq i \leq n)\ ||\alpha-\beta_{j_0}|| < ||\alpha-\alpha_i||$. Using the Krasner lemma one concludes that $\alpha \in \mathbf{C}_p(\beta_{j_0}) = \mathbf{C}_p$. ■

Definition-Theorem 5.54. For a power series $F(T) = \sum\limits_{i=0}^{\infty} a_i T^i \in \mathbf{C}_p[[T]]$ define $\mathrm{v}_p(F) \stackrel{\text{def}}{=} \liminf \frac{\mathrm{v}_p(a_i)}{i}$. ($\mathrm{v}_p(F)$ 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 2.11. 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 Problem 51 ■

Definition 5.55. The Newton polygon $N(F)$ of a power series $F(T) = 1 + \sum\limits_{i=1}^{\infty} a_i T^i \in 1 + T\mathbf{C}_p[[T]]$ 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 $l_j(F)$ 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 polynomial 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 5.56. $\mathrm{v}_p(F) = \sup \lambda_j(F)$. 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 $\mathrm{v}_p(a_i) - c - \lambda_{\max} i$. If $\mathrm{v}_p(x) = -\mathrm{v}_p(F)$ then $\mathrm{v}_p(a_i x^i)$ differs from the said distance by a constant so that they both either do tend or do not tend to infinity simultaneously ■

Theorem 5.57. 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 $F(T) = 1 + \sum_{s=1}^{n} a_s T^s = \prod_{i=1}^{n} (1 - \frac{T}{\alpha_i})$, 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 α_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 λ_i hence the statement of the theorem. Since the function v_p is Galois-invariant, the polynomials $F_{\lambda_j(F)}$ have coefficients in k ■

Theorem 5.58 (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 $n(\lambda, F) \stackrel{\text{def}}{=} \sum_{\lambda_j(F) \leq \lambda} l_j(F)$ (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 non-increasing $\mathrm{v}_p(\alpha_k)$. Then $\forall r \#(k$ such that $\mathrm{v}_p(\alpha_k) \geq r) < \infty$ and the infinite product $\prod_{k=1}^{\infty}(1-\alpha_k^{-1}x)$ converges to $F(x)$ for all $x \in \mathbf{C}_p$.

Proof. Try yourself or see any book, for example Neal Koblitz's "p-adic Numbers, p-adic Analysis and Zeta-Functions".

Problems. (the deadline for 41 - 42 is November, 24th; for 43 - 45 December, 1st, for 46-50 December, 15th, for 51-53 December, 21st).

41. Suppose $N = \langle\{e_i\}\rangle$, $M = \langle\{g_i\}\rangle$ are free $\mathcal{O}$-lattices in $\mathcal{O}_K$. Prove that $(D_{\mathcal{O}}(N) : D_{\mathcal{O}}(M))_{\mathcal{O}} = (M : N)_{\mathcal{O}}$.
42. Prove that if $N = \langle\{e_i\}\rangle$ is a free $\mathcal{O}$-lattice in $\mathcal{O}_K$ then $\mathfrak{d}_{\mathcal{O}}(N) = (\det Tr(e_i e_j))$.
43. Suppose k is a field. Prove that any finite-dimensional commutative k-algebra without zero divisors is a field.
44. Suppose $K = \mathbf{Q}(\sqrt{d})$, d a squarefree integer. Calculate Δ_K.
45. Suppose $\mathcal{O}$ is a Dedekind domain, $I \subset \mathcal{O}$ a nontrivial nonzero ideal. Prove that the quotient ring $\mathcal{O}/I$ is a principal ideal ring.
46. Prove that $e(\mathfrak{p}_3/\mathfrak{p}_1) = e(\mathfrak{p}_3/\mathfrak{p}_2)e(\mathfrak{p}_2/\mathfrak{p}_1)$ if $\mathfrak{p}_3 \mid \mathfrak{p}_2 \mid \mathfrak{p}_1$ (cf. Theorem 5.36).
47. Prove that $f(\mathfrak{p}\widehat{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{p}) = e(\mathfrak{p}\widehat{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{p}) = 1$. **48**. Prove that $D_{\mathcal{O}}(\mathcal{O}_K) \cap k = (Tr_{K/k}(\mathcal{O}_K))^{-1}$.
49. Suggest an example of the $\mathbf{Z}_p$-lattice $N \subset \mathbf{Q}_p \oplus \mathbf{Q}_p$ such that $\mathfrak{d}_{\mathbf{Z}_p}(N) \neq \mathfrak{d}_{\mathbf{Z}_p}(\pi_1(N))\mathfrak{d}_{\mathbf{Z}_p}(\pi_2(N))$.
50. Let $k = \mathbf{Q}_p$, $P(T) = T^2 - 5$.
1) Suggest the necessary and sufficient condition on p for $P(T)$ to be irreducible.
2) If P is irreducible let $K = k_P$. Calculate e and f.
51. Prove the continuity statement from Theorem 5.54.
52. Extend v_p from $\overline{\mathbf{Q}_p}^*$ to $\mathbf{C}_p^*$ by continuity. Describe the group $\mathrm{v}_p(\mathbf{C}_p^*)$.
53. Describe the Newton polygon of the power series $F(T) = -\log(1-T)/T = \sum_{i=1}^{\infty} \frac{T^{i-1}}{i}$ and calculate $\mathrm{v}_p(F_k)$. Does the power series $F(x)$ converge when $\mathrm{v}_p(x) = -\mathrm{v}_p(F)$?