CHAPTER 5

Adeles over a number field

1. The adelic points of an algebra

Let A is a finite dimensional $\mathbb{Q}$-algebra (not necessarily commutative), it follows immediately that $A(\mathbb{A}_S)$ has the structure of a $\mathbb{A}_S$-algebra extending the $\mathbb{Q}$-algebra structure on A (ie. one has $\delta_S(x \times_A y) = \delta_S(x) \times_{A(\mathbb{A})} \delta_S(y)$ for any $x, y \in A$). This is either a formal consequence of the tensor product construction or this could be checked directly as we will do now.

1.1. General facts about finite dimensional algebras over a field. Let A be a finite n-dimensional algebra over some field k; the multiplication map yield an embedding

$$[\times\cdot] : \begin{array}{ccc} A & \hookrightarrow & \mathrm{End}_k(A) \\ x & \mapsto & [\times x] : y \to xy \end{array}.$$

This map is an embedding because $[\times x](1_A) = x$ is zero iff $x = 0$.

To distinguish between the k-vector space A and the algebra A acting on A (and identified with a subalgebra of $\mathrm{End}_k(A)$ via $[\times\cdot]$, we will sometimes write V_A for the vector space and keep A to designate the subalgebra $[\times\cdot]A$.

One then defines the *trace, norm*, *characteristic polynomial* and minimal polynomial (the unit polynomial generating the ideal of polynomial vanishing at x, in particular it divides $P_{char,x}$) of some $x \in A$ as

$$\mathrm{tr}_{A/k}(x) = \mathrm{tr}([\times x]),\ \mathrm{Nr}_{A/k}(x) := \det([\times x]),$$
$$P_{char,x}(X) := \det(X\mathrm{Id_A} - [\times x]),\ P_{min,x}(X)|P_{char,x}(X).$$

Exercise 5.1. Prove that if A is a field, and $x \neq 0$, there is a basis of A for which the matrix of $[\times x]$ is a product of bloc matrices of $[\times x]$ restricted, $k[x]$ the field generated by x. Consequently

$$P_{char,x}(X) = P_{min,x}(X)^{d/d_x}$$

where $d_x = [k[x] : k]$ is the degree, and

$$\mathrm{tr}_{A/k}(x) = (d/d_x)\mathrm{tr}_{k[x]/k}(x),\ \mathrm{Nr}_{A/k}(x) = \mathrm{Nr}_{k[x]/k}(x)^{d/d_x}.$$

1.1.1. *Presentation as an algebra of matrices.* One can make things a bit more concrete by choosing $\mathcal{B} = \{\mathbf{e}_i\}$ a k-basis of A: this induces an isomorphism of vector space $\iota : A \simeq K^n$

$$\iota : y = \sum_i y_i \mathbf{e}_i \mapsto (y_1, \cdots, y_n) \in k^n$$

and an algebra embedding $\theta : A \hookrightarrow M_n(k)$ defined by the equality

$$\theta(x)\iota(y) = \iota(xy).$$

The linear map θ is injective because if some $\theta(x)$ is the zero endomorphism, one has $0 = \theta(x)\iota(1) = \iota(x)$ hence $x = 0$.

In such a realization, the trace, norm, characteristic and minimal polynomials are just the trace the determinant and the characteristic and minimal polynomials of $n\times n$-matrices.

REMARK 1.1. Observe that if we consider another basis $\mathcal{B}'$, the corresponding matrix algebra $\theta'(A)$ is obtained from $\theta(A)$ by conjugation by a fixed matrix $m_{\mathcal{B},\mathcal{B}'}\in \mathrm{GL}_n(\mathbb{Q})$.

1.2. The algebra of adelic matrices $M_n(\mathbb{A})$. The most basic example of adelic point of an algebra is the algebra of $n\times n$ matrices with adelic entries equipped with the basis of elementary matrices

$$M_n(\mathbb{Q})=\{m=(m_{i,j})_{i,j\leqslant n},\ m_{i,j}\in\mathbb{Q}\}=\sum_{i,j\leqslant n}\mathbb{Q}E_{i,j},$$

where

$$E_{i,j}=(e_{i,j,k,l})_{k,l\leqslant n},\ e_{i,j,k,l}=\delta_{i=k}\delta_{j=l}.$$

is the endomorphism which maps the i-th element of the canonical basis to the j-th element and all other elements to 0. If we replace $\mathbb{Q}$ by the ring $\mathbb{A}_S$ for $S\subset\mathcal{V}_{\mathbb{Q}}$ one obtains

$$M_n(\mathbb{A}_S)=\{m=(m_{i,j})_{i,j\leqslant n},\ m_{i,j}\in\mathbb{A}_S\}==\sum_{i,j\leqslant n}\mathbb{A}_SE_{i,j}$$

$$\prod_{v\in S}{}' M_n(\mathbb{Q}_v)=\{(m_v)_v,\ m_v\in M_n(\mathbb{Q}_v),\ m_p\in M_n(\mathbb{Z}_p)\text{ for a.e. }p\in S\}$$

where

$$M_n(\mathbb{Z}_v)=\sum_{i,j\leqslant n}\mathbb{Z}_vE_{i,j}$$

equipped with the usual addition and multiplication laws.

REMARK 1.2. The lattice $M_n(\mathbb{Z}_v)$ is defined slightly more intrinsically as the set $\mathrm{End}_{\mathbb{Z}_v}(\mathbb{Z}_v^n)$ of $\mathbb{Z}_v$-linear endomorphisms of the lattice $\mathbb{Z}_v^n$ or equivalently the stabilizer of the lattice $\mathbb{Z}_v^n$ inside $M_n(\mathbb{Q}_v)$.

If V is a general $\mathbb{Q}$-vector space with basis $\mathcal{B}=\{\mathbf{e}_i,\ i\leqslant n\}$, we may consider the algebra of linear maps on V

$$\mathrm{End}_{\mathbb{Q}}(V)=\bigoplus_{i,j\leqslant n}\mathbb{Q}E_{i,j}$$

where $E_{i,j}$ is the linear map defined by

$$E_{i,j}(\mathbf{e}_k)=\delta_{k=i}\mathbf{e}_j.$$

We have

$$\begin{aligned}\mathrm{End}_{\mathbb{Q}}(V)(\mathbb{A})=\mathrm{End}_{\mathbb{A}}(V(\mathbb{A}))=\prod_v{}'\,\mathrm{End}_{\mathbb{Q}_v}(V_v)\\ =\{(m_v)_v,\ m_v\in\mathrm{End}_{\mathbb{Q}_v}(V_v),\ m_p\in\mathrm{End}_{\mathbb{Z}_p}(L_{\mathcal{B},p})\text{ for a.e. }p\}\end{aligned}$$

where

$$L_{\mathcal{B},p}=\sum_i\mathbb{Z}_p\mathbf{e}_i,\ \mathrm{End}_{\mathbb{Z}_p}(L_{\mathcal{B},p})=\sum_{i,j}\mathbb{Z}_pE_{i,j}.$$

and $\mathrm{End}_{\mathbb{Z}_p}(L_{\mathcal{B},p})$ is precisely the stabilizer of the lattice $L_{\mathcal{B},p}$ inside $\mathrm{End}_{\mathbb{Q}_v}(V_v)$.

1.3. Topology of $A(\mathbb{A})$. Let us return to the situation of A being a finite dimensional algebra over $\mathbb{Q}$. As explained above, the choice of some $\mathbb{Q}$-basis $\mathcal{B}$ of V_A, yields an linear isomorphism $\iota : V_A \simeq \mathbb{Q}^n$ in which $\mathcal{B}$ get identified with the canonical basis of $\mathbb{Q}^n$ and which induces a $\mathbb{Q}$-algebra embedding

$$\theta : A \hookrightarrow \theta(A) \subset M_n(\mathbb{Q}).$$

Therefore $A(\mathbb{A})$ is identified with the $\mathbb{A}$-subalgebra $\theta(A)(\mathbb{A}) \subset M_n(\mathbb{A})$. Since the lattice $L_{\mathcal{B}} = \sum \mathbb{Z}\mathbf{e}_i$ is identified with $\mathbb{Z}^n$ under ι one has

$$A(\mathbb{A}) = \prod_v{}' A(\mathbb{Q}_v) = \{(x_v)_v,\ x_v \in A(\mathbb{Q}_v), x_p \in A(L_{\mathcal{B},p}) \text{ for a.e. } p\}$$

where

$$A(L_{\mathcal{B},v}) = \{x_v \in A(\mathbb{Q}_v),\ x_v.L_{\mathcal{B},v} \subset L_{\mathcal{B},v}\} \simeq \theta(A)(\mathbb{Q}_v) \cap M_n(\mathbb{Z}_v)$$

is the stabilizer of the lattice $L_{\mathcal{B},v}$ in $A(\mathbb{Q}_v)$.

In particular $A(L_{\mathcal{B},v})$ is a lattice and the collection of local lattices $(A(L_{\mathcal{B},v}))_v$ obtained from the global lattice

$$\theta(A) \cap \mathrm{M}_n(\mathbb{Z}).$$

The $\mathbb{A}$-algebra as a closed subset of $M_n(\mathbb{A})$ is equipped with the adelic topology which we transport to $A(\mathbb{A})$ via θ. Observe again that this topology does not depend on the choice of the basis $\mathcal{B}$ of A: if one consider another basis, $\theta'(A)$ is obtained from $\theta(A)$ by conjugation by an element of $\mathrm{GL}_n(\mathbb{Q})$ which induce an homeomorphism between $\theta(A)(\mathbb{A})$ and $\theta'(A)(\mathbb{A})$.

Since matrix multiplication and addition are continuous on $M_n(\mathbb{A})$, they are continuous on $\theta(A)(\mathbb{A})$ and therefore

Proposition 5.1. *Equipped with the adelic topology $A(\mathbb{A})$ has the structure of locally compact topological ring in which $\mathbb{A}(\mathbb{Q})$ embeds as a discrete subring and in which the trace norm and characteristic polynomial are continuous maps.*

As for the ideles, some care is necessary to define the topology on the group of invertible elements of $A(\mathbb{A})$,

$$A(\mathbb{A})^\times = \prod_v{}' A(\mathbb{Q}_v)^\times = \{(x_v)_v,\ x_v \in A(\mathbb{Q}_v)^\times,\ \theta(x_p) \in \mathrm{GL}_n(\mathbb{Z}_p)^\times \text{ for a.e. } p\}.$$

We observe that by Cramer formula, for any ring R a matrix $x \in M_n(R)$ is invertible iff $\det x \in R^\times$; therefore

$$A(\mathbb{A}_V)^\times = \{x \in A(\mathbb{A}_V),\ \mathrm{Nr}_{A/k}(x) \in \mathbb{A}_V^\times\}.$$

We may therefore identify $A(\mathbb{A}_V)^\times$ with the following closed subset:

$$\{(x,t) \in A(\mathbb{A}_V) \times \mathbb{A}_V,\ \mathrm{Nr}_{A/k}(x)t = 1\}$$

as for the ideles, the adelic topology on $A(\mathbb{A}_V)^\times$ is the topology corresponding to the relative topology under this identification.

Proposition 5.2. *Equipped with this topology, $A(\mathbb{A}_V)^\times$ is a locally compact topological group and embeds as a closed subgroup of $A(\mathbb{A})$. The group $A^\times$ embeds as a discrete subgroup of $A(\mathbb{A})^\times$*

2. Adelic points of a number field

We now assume that the algebra A is a number field K (a finite extension of $\mathbb{Q}$) and discuss in greater detail the structure of $K(\mathbb{A})$ which is sometimes noted $\mathbb{A}_K$ and is called the *ring of adeles of* K. In particular we discuss the structure of the $\mathbb{Q}_v$-algebra $K_v = K(\mathbb{Q}_v) = K \otimes_{\mathbb{Q}} \mathbb{Q}_v$ for $v \in \mathcal{V}$.

2.1. Etale algebras. Let k be a field and A be a k-algebra. The trace $\mathrm{tr}_{A/k}$ linear form defines a bilinear form (called the trace form) on $A \times A$ as follows

$$\langle x, y\rangle := \mathrm{tr}_{A/k}(xy).$$

Definition 5.1. *A finite dimensional k-algebra A is etale if the trace form is non-degenerate; ie. if the following linear map to the dual A^**

$$x \in A \mapsto x^* \in A^* : y \mapsto x^*(y) = \langle x, y\rangle = \mathrm{tr}_{A/k}(xy)$$

is an isomorphism or equivalently if for some (hence any) basis of A

$$\det((\langle \mathbf{e}_i, \mathbf{e}_j\rangle)_{i,j\leqslant n}) \neq 0.$$

One has the following fundamental result

Theorem 5.1. *A commutative etale k-algebra A decomposes as a k-algebra into a product of finite field extensions of k,*

$$A \simeq \prod_w K_w.$$

This decomposition is unique up to isomorphism.

Proof. We achieve this decomposition by decomposing the vector space $V_A(= A)$ into a direct sum of non-trivial A-invariant $(A.V \subset V)$ vector spaces

$$V_A = \bigoplus_w V_w$$

(which are minimal for this property) therefore we will have the (block matrices) decomposition

$$\mathrm{End}_k(V_A) = \prod_w \mathrm{End}_k(V_w)$$

and therefore A will decompose as

$$A = \prod_w K_w \subset \prod_w \mathrm{End}_k(V_w) \text{ with } K_w = A_{|V_w}$$

the image of the restricted action of A on the subspace $V_{|w}$. The minimality of the V_w then shows that the K_w are fields.

Definition 5.2. *A subspace $V \subset V_A$ is A-irreducible (for the action of A on V_A) if it is non-zero, A-invariant $(A.V \subset V)$ and minimal for this property: any A-invariant subspace of V is either zero or A.*

Let us show that V_A decomposes as a direct sum of A-irreducible subspaces. Let $V \subset V_A$ be a non-zero A-invariant subspace and of minimal dimension. V is a clearly irreducible. Let $A_{|V} = A \cap \mathrm{End}_k(V)$ be the image of A in $\mathrm{End}_k(V)$; we claim that $A_{|V}$ is a field $(A^*_{|V} = A_{|V} - \{0\})$. Indeed suppose that $x \in A$ acts non-trivially on V $(x.V \neq \{0\})$ and let $V' = \ker[\times x]_{|V}$; by definition $V' \neq V$ and since A is commutative $A.V' = V'$ (ie. V' is

A-invariant) it follows (by minimality of $\dim_k V$) that V' is trivial so that $[\times x]_{|V}$ is injective hence invertible. This proves that $A_{|V}$ is a field. Let

$$V^{\perp} = \{y \in V_A,\ \langle y, V\rangle = 0\}$$

be the subspace orthogonal to V. Since the trace form is non-degenerate one has and orthogonal decomposition

$$V_A = V \bigoplus V^{\perp}$$

and for all $x \in A$ and $y \in V^{\perp}$

$$\langle x.y, V\rangle = \mathrm{tr}(xyV) = \mathrm{tr}(yxV) \subset \mathrm{tr}_{A/k}(yV) = \{0\}$$

so that $x.y \in V^{\perp}$, therefore $V^{\perp}$ is an A-invariant subspace of A. Repeating this argument with $V^{\perp}$ we obtain a direct sum decomposition of V_A into irreducible subspaces

$$V = \bigoplus_w V_w \text{ hence } \mathrm{End}_k(A) \simeq \prod_w \mathrm{End}_k(V_w)$$

hence the decomposition

$$A \simeq \prod_w A_{|V_w} \subset \prod_w \mathrm{End}_k(V_w)$$

where $A_{|V_w} = K_w$ is a field. such decomposition is unique become is one has two such decompositions

$$V_A = \bigoplus_w V_w = \bigoplus_{w'} V'_{w'}$$

by irreducibility we will get

$$V_w \cap V'_{w'} = \begin{cases} 0 \\ V_w = V'_{w'} \end{cases}$$

because $V_w \cap V'_{w'} \subset V_w$ is an A-invariant subspace of an irreducible subspace. □

Let

$$d_w := \dim_k(K_w)$$

be the degree of K_w, we have

$$\dim_k A = \sum_w d_w;$$

if we denote by

$$(x_w)_w \in \prod_w K_w$$

the image of $x \in A$ under the above isomorphism one has

$$\mathrm{tr}_{A/k}(x) = \sum_w \mathrm{tr}_{K_w/k}(x_w), \tag{2.1}$$

$$\mathrm{Nr}_{A/k}(x) = \prod_w \mathrm{Nr}_{K_w/k}(x_w), \tag{2.2}$$

$$P_x(X) = \prod_w P_{x_w}(X). \tag{2.3}$$

Exercise 5.2. Prove that if $A = K$ is a field of characteristic $> \dim_k K$, K is etale.

Exercise 5.3. Prove that if A is a field, A is etale iff A/k is separable. For this consider a basis $\mathcal{B}$ of the shape $\{1, x, \cdots, x^{n-1}\}$

Exercise 5.4. Prove that if A is etale and monogenic (of the shape $A = k[x]$ for some $x \in A$), the above decomposition is obtained as follows: let $P_{char,x}$ be the characteristic polynomial of x then $P_{char,x}$ has no multiple roots (in an algebraic closure of k) and if we decompose it into a product of irreducible polynomials,

$$P_{char,x}(X) = \prod_w P_w(X),$$

one has

$$A \simeq \prod_w K_w \text{ where } K_w \simeq k[X]/P_w(X)k[X].$$

2.2. The local algebras K_v. We return to the special case of $k = \mathbb{Q}_v$ and

$$A = K_v = K \otimes_{\mathbb{Q}} \mathbb{Q}_v$$

for K a finite field extension of $\mathbb{Q}$ of degree n. The algebra K_v is etale because K, as a field of characteristic zero is etale and therefore the determinant of the trace form matrix is not zero in some $\mathbb{Q}$-base of K hence in some $\mathbb{Q}_v$-base of K_v.

By Theorem 5.1, one has a $\mathbb{Q}_v$-algebra isomorphism

$$K_v \simeq \prod_{w \subset \mathcal{V}_{K,v}} K_w,\ d_w = [K_w : \mathbb{Q}_v],\ \sum_{w \subset \mathcal{V}_v} d_w = n$$

where the K_w are finite field extension of $\mathbb{Q}_v$ indexed by some suitable finite set $\mathcal{V}_v$. Since K is a field the projection to the w-factor yields a $\mathbb{Q}$-algebra embedding

$$\delta_w : K \to K_w.$$

Moreover since K is dense in K_v its image by δ_w is dense in K_w.

As we have seen, for any K_w there is a unique way to extend the v-adic absolute value $|\cdot|_v$ from $\mathbb{Q}_v$ to K_w and it is given by the formula

$$|\cdot|_w = |\,\mathrm{Nr}_{K_w/\mathbb{Q}_p}(\cdot)|_v^{1/d_w}.$$

2.3. The local ring of integers. Suppose that $v = p$ is finite; we let

$$\mathcal{O}_w = B_c(0,1)_w$$

be the closed unit ball for the valuation $|\cdot|_w$.

Theorem 5.2. *One has the following*

(1) *The set $\mathcal{O}_w$ is a subring of K_w and a lattice in K_w (in particular open-compact). Any compact subring of K_v is contained into $\mathcal{O}_w$.*
(2) *The group of units is the unit sphere*
$$\mathcal{O}_{K_w}^\times = \{x_w \in K_w,\ |x_w|_w = 1\}.$$
(3) *The ring $\mathcal{O}_w$ is a principal ideal ring whose unique maximal ideal is the open unit ball*
$$\mathfrak{p}_w := B_o(0,1)_w\{x_w \in K_w,\ |x_w|_w < 1\}.$$
(4) *The later is generated by any element π_w in $\mathfrak{p}_w$ of maximal absolute value; any such element is called an uniformizer of $\mathcal{O}_w$. Let $e_w \in \mathbb{N}_{\geqslant 1}$ be such that $p\mathcal{O}_w = \pi_w^{e_v}\mathcal{O}_w$ or equivalently $|\pi_w|_w = p^{-1/f_w}$; that integer is called the ramification index of K_w.*
(5) *The quotient $\mathcal{O}_w/\mathfrak{p}_w$ is an extension of the finite field $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$ called the residual field of K_w. Its degree is noted f_w and is called the inertia degree of K_w.*
(6) *One has the relation $e_w f_w = d_w$.*

(7) *The ring $\mathcal{O}_{K_w}$ is exactly the set of elements of K_w which are roots by some monic $\mathbb{Z}_p$-integral polynomial, or equivalently, whose characteristic is $\mathbb{Z}_p$-integral or equivalently whose minimal polynomial is $\mathbb{Z}_p$-integral.*

PROOF. □

From the above theorem one has

$$|\operatorname{Nr}_{K_w/\mathbb{Q}_p}(\pi_w)|_p = p^{-e_w} = |\mathcal{O}_{K_w}/\mathfrak{p}_w|^{-1}.$$

Since the absolute value $|\cdot|_w$ is non-archimedean, the map

$$x_w \in K_w \mapsto |x_w|_{w,n} = |x|_w^{d_w} = |\operatorname{Nr}_{K_w/\mathbb{Q}_v}(x_w)|_v$$

is also an absolute value equivalent to $|\cdot|_w$; because of the identity

$$|\pi_w|_{w,n} = |\mathcal{O}_{K_w}/\mathfrak{p}_w|^{-1},$$

$|\cdot|_{w,n}$ is called the normalized absolute value at w.

2.4. Archimedean absolute values. When $v = \infty$, K_w is a finite algebraic extension of $\mathbb{R}$ so is either $\mathbb{R}$ or $\mathbb{C}$ and d_w is either 1 or 2. In the first case the absolute value is unchanged, and when $K_w = \mathbb{C}$, $z = x + iy$, one has

$$|z|_w = |\operatorname{Nr}_{\mathbb{C}/\mathbb{R}}(z)|^{1/2} = |x^2 + y^2|_\infty^{1/2} = |z\overline{z}|_\infty^{1/2} = |z|_\mathbb{C}$$

is the usual absolute value on the complex numbers and one defines the normalized absolute value as

$$|z|_{\mathbb{C},n} = |z|_\mathbb{C}^2 = x^2 + y^2.$$

REMARK 2.1. Observe that $|z|_{\mathbb{C},n}$ does not satisfy the triangle inequality so in this case there is a slight abuse of notations.

2.5. Comparison with the intrinsic construction of the ring of adeles of a number field. By restriction this defines an absolute value on K.

THEOREM 5.3. *The absolute value $|\cdot|_w$ for w varying over the set $\mathcal{V}_{K,v}$ form a set of representatives of the equivalence classes of absolute values on K whose restriction to $\mathbb{Q}$ is equivalent to $|\cdot|_v$. Consequently the set $\bigcup_{v\in\mathcal{V}_\mathbb{Q}} \mathcal{V}_w = \mathcal{V}_K$ is a set of representatives of the equivalence classes of all possible absolute values on K (the set of places of K).*

PROOF. Exercise. □

DEFINITION 5.3. *We say that the absolute values in $\mathcal{V}_{K,v}$ is the set of absolute values w above v or which divide v and this is written $w|v$. Consequently*

$$K_v = \prod_{w|v} K_w.$$

If $v = p$ is finite the absolute value w will be called finite (or non-archimedean) and infinite (or archimedean) otherwise. The set of finite places is noted $\mathcal{V}_{K,f}$ and the infinite ones $\mathcal{V}_{K,\infty}$

PROOF. Exercise. □

From this discussion we get two equivalent constructions of the ring of adeles of K: choosing $\mathcal{B}$ a $\mathbb{Q}$-basis of K and setting L the associated lattice we have

$$K(\mathbb{A}) = \mathbb{A}_K = \prod_{v\in\mathcal{V}_\mathbb{Q}}{}' K_v = \{(x_v) \in K \otimes_\mathbb{Q} \mathbb{Q}_v,\ x_p \in L_p \text{ for a.e. } p\}$$

and a more intrisic one

$$K(\mathbb{A}) = \mathbb{A}_K = \prod_{w\in\mathcal{V}_K}{}' K_w = \{(x_w)_{\mathcal{V}_K},\ x_w \in K_w,\ x_w \in L_w \text{ for a.e. } w \text{ finite}\}.$$

here L_w is the closure of L inside K_w.

2.5.1. *The adelic absolute value.*

DEFINITION 5.4. *The adelic absolute value of K is the continuous function on $\mathbb{A}_K^\times$ defined by*

$$|\cdot|_{\mathbb{A}_K} : x \in \mathbb{A}_K^\times \mapsto |\operatorname{Nr}_{K/\mathbb{Q}}(x)|_{\mathbb{A}} \in \mathbb{R}_{>0}.$$

We have for $x = (x_v)_{v\in\mathcal{V}_\mathbb{Q}} = (x_w)_{w\in\mathcal{V}_K}$

$$|x|_{\mathbb{A}_K} = \prod_v |\operatorname{Nr}_{K_v/\mathbb{Q}_v}(x_v)|_v = \prod_w |\operatorname{Nr}_{K_w/\mathbb{Q}_v}(x_w)|_w = \prod_w |x_w|_w^{d_w} = \prod_w |x_w|_{w,n}.$$

In particular we obtain

THEOREM 5.4 (Artin product formula). *For any $x_K \in K^\times$*

$$|x_K|_{\mathbb{A}_K} = \prod_w |x_K|_{w,n} = |\operatorname{Nr}_{K/\mathbb{Q}}(x_K)|_{\mathbb{A}} = 1.$$

Since the adelic absolute value is continuous, its kernel

$$\mathbb{A}_K^{(1)} = \{x \in \mathbb{A}_K^\times,\ |x|_{\mathbb{A}_K} = 1\}$$

is a closed subgroup. We have the following important generalization of

THEOREM 5.5. *The subgroup $K^\times$ is a discrete subgroup of $\mathbb{A}_K^{(1)}$ and the quotient $K^\times\backslash\mathbb{A}_K^{(1)}$ is compact.*

3. Classical Algebraic number Theory vs. Adelic Number Theory

As is proven in any classical course in algebraic number theory, the field K contains a very specific subring which is in many respect canonical: this ring is defined algebraically as the *integral closure* of $\mathbb{Z}$ in K, that is the set of elements of K which are annihilated by a unitary polynomial with integral coefficients: this ring is called *the ring of integers of K*.

In this section with retrieve these from the adelic viewpoint and discuss its main properties.

4. The ring of integers as an intersection of balls

We consider the intersection of the unit balls associated to the various absolute values w on K, or in other terms the local rings

$$\mathcal{O}_w = B_c(0,1)_w = \{x_w \in K_w,\ |x_w|_w \leqslant 1\},$$

which we denote by

$$\mathcal{O}_K = \bigcap_{w\in\mathcal{V}_K} \mathcal{O}_{K_w} \cap K = \bigcap_p \mathcal{O}_p \cap K$$

(here we have noted $\mathcal{O}_p := \prod_{w|p} \mathcal{O}_{K_w} \subset K_p$). As we show below this analytically defined object is the ring of integers of K:

THEOREM 5.6. *The set $\mathcal{O}_K$ has the following properties*

- *$\mathcal{O}_K$ is a ring.*

- *$\mathcal{O}_K$ is a lattice.*
- *$\mathcal{O}_K$ is the set of elements of K which are roots of some monic polynomial with integral coefficient or equivalently whose characteristic or minimal polynomial has integral coefficients; therefore $\mathcal{O}_K$ is called the ring of integers of K.*

Proof. $\mathcal{O}_K$ is a ring as an intersection of rings. For any $x \in \mathcal{O}_K$ we have for any p

$$P_{char,x,K}(X) = \prod_w P_{char,x,K_w}(X) \in \mathbb{Z}_p[X]$$

therefore $P_{char,x,K}(X)$ has integral coefficients; conversely any element of K who characteristic polynomial is integral is contained in $\mathcal{O}_w$ for every w hence in $\mathcal{O}_K$. The equivalence of this caracteriszation to the integrality of the minimal polynomial or some annahilating polynomial follows from Gauss lemma.

We observe that K contains a lattice (hence contains a basis of K); this follows from *for any $x \in K$ there exists some non zero $m \in \mathbb{Z}$ such that $nx \in \mathcal{O}_K$*; indeed let

$$P_{char,x}(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0,\ a_i \in \mathbb{Q}$$

we have for $m \neq 0$ an integer

$$\begin{aligned} P_{char,mx}(X) &= \det(X\mathrm{Id} - \theta(mx)) = m^n \det(\frac{X}{m}\mathrm{Id} - \theta(x)) \\ &= m^n((\frac{X}{m})^n + a_{n-1}(\frac{X}{m})^{n-1} + \cdots + a_0) = X^n + a_{n-1}mX^{n-1} + \cdots + m^n a_0 \end{aligned}$$

is integral for m sufficiently divisible.

To show that $\mathcal{O}_K$ is a lattice it is sufficient to show that $\mathcal{O}_K$ is discrete in K_∞ : by a well known lemma $\mathcal{O}_K$ will then be a finitely generated $\mathbb{Z}$-module clearly of maximal rank since it generated K as a $\mathbb{Q}$-vector space. To prove discretness it is sufficient to observe that if $x_\infty \in K_\infty \subset M_n(\mathbb{R})$ has sufficiently small coefficients in some fixed basis of K_∞ and integral characteristic polynomial, all the coefficient excepted for the dominant one have to be 0 and therefore $x = 0$. □

Exercise 5.5 (Orders of a number field). An order $\mathcal{O} \subset K$ is a subring of K which is also a lattice. Prove the order are exactly the subsets of K of the shape: for $L \subset K$ a lattice

$$\mathcal{O}(L) := \{x \in K,\ xL \subset L\} = \mathrm{End}_K(L) \cap K.$$

Prove that any order[1] is contained in $\mathcal{O}_K$: $\mathcal{O}_K$ is also called the maximal order. Prove, more generally that any subring $R \subset K$ which is finitely generated as a $\mathbb{Z}$-module is contained into $\mathcal{O}_K$.

4.1. The ideals of $\mathcal{O}_K$. By convention an ideal[2] $\mathfrak{a} \subset \mathcal{O}_K$ (a $\mathcal{O}_K$-module contained into $\mathcal{O}_K$) is always non-zero. It is useful to slightly extend the definition of ideal:

Definition 5.5. *A fractional $\mathcal{O}_K$-ideal $\mathfrak{a} \subset K$ is a non-zero $\mathcal{O}_K$-module for which there exist $\lambda \in K^\times$ such that $\lambda\mathfrak{a} \subset \mathcal{O}_K$. The set of fractional ideals is noted $J(\mathcal{O}_K)$ or J_K. We also denote by $P(\mathcal{O}_K) = P_K = \{\lambda\mathcal{O}_K,\ \lambda \in K^\times\}$ the subset of principal ideals*

Lemma 5.1. *A fractional ideal $\mathfrak{a}$ is a $\mathbb{Z}$-lattice in K. In particular, $\mathcal{O}_K \cap \mathfrak{a}$ is of finite index in both $\mathcal{O}_K$ and $\mathfrak{a}$.*

[1]andd more generally, any subring of $\mathcal{O}_K$ which is finitely generated as a $\mathbb{Z}$-module

[2]or an $\mathcal{O}_K$-ideal

PROOF. $\square$

THEOREM 5.7. *The set of fractional ideals has the following structural properties:*

- *The set of fractional ideals has a natural structure of commutative group with unit element $\mathcal{O}_K$ and multiplication given by*

$$\mathfrak{a}.\mathfrak{b} = \langle ab,\ a \in \mathfrak{a},\ b \in \mathfrak{b}\rangle = \text{ the ideal generated by product of elements of } \mathfrak{a} \text{ and } \mathfrak{b},$$

- *The prime ideals of $\mathcal{O}_K$ are generator of that group and wrt the above multiplication law, every ideal decompose in a unique way as a product of powers of primes ideals,*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},\ v_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ for a.e. } \mathfrak{p}.$$

  The integer $v_{\mathfrak{p}}(\mathfrak{a})$ is the valuatin at $\mathfrak{p}$ of the fractional ideal $\mathfrak{a}$.
- *In other terms, J_K is isomorphic to the free (commutative) $\mathbb{Z}$-module generated by the set of prime $\mathcal{O}_K$-ideals* $\mathrm{Spec}(\mathcal{O}_K)$, *$Div(\mathrm{Spec}(\mathcal{O}_K))$ say; that is the set of finite integral linear combinations of the symbols $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$*

$$\sum_{\mathfrak{p}} v_{\mathfrak{p}}.\mathfrak{p},\ v_{\mathfrak{p}} \in \mathbb{Z},\ v_{\mathfrak{p}} = 0 \text{ for a.e. } \mathfrak{p}.$$

- *Some basic calculus for integers remains valid for fractional ideals:*

$$\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow \forall \mathfrak{p}\ v_{\mathfrak{p}}(\mathfrak{a}) \geqslant v_{\mathfrak{p}}(\mathfrak{b})$$

  in which case one says that $\mathfrak{b}$ divides $\mathfrak{a}$ which is written

$$\mathfrak{b}|\mathfrak{a};$$

  in addition

$$\mathfrak{a} + \mathfrak{b} = \langle a + b,\ a \in \mathfrak{a},\ b \in \mathfrak{b}\rangle = \prod_{\mathfrak{p}} \mathfrak{p}^{\min(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))} = g.c.d(\mathfrak{a}, \mathfrak{b})$$

$$\mathfrak{a} \cap \mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{\max(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b}))} = l.c.m(\mathfrak{a}, \mathfrak{b}).$$

Because of this result the set of prime ideals is particularly important:

PROPOSITION 5.3. *A prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is maximal. The quotient $\mathcal{O}_K/\mathfrak{p} = k_{\mathfrak{p}}$ is a finite finite.*

PROOF. Since $\mathfrak{p}$ is a lattice the quotient $\mathcal{O}_K/\mathfrak{p} = k_{\mathfrak{p}}$ is a finite integral ring hence is a field so $\mathfrak{p}$ is maximal. $\square$

DEFINITION 5.6. *The field $k_{\mathfrak{p}}$ called the residue field at $\mathfrak{p}$, its characteristic p the residual characteristic and its degree $f_{\mathfrak{p}} = [k_{\mathfrak{p}} : \mathbb{F}_p]$ is called the residual degree.*

PROPOSITION 5.4. *A prime ideal $\mathfrak{p}$ a characteristic p iff $p \subset \mathfrak{p}$ or equivalently $\mathfrak{p}|p\mathcal{O}_K$ also written $\mathfrak{p}|p$. The valuation $v_{\mathfrak{p}}(p\mathcal{O}_K)$ is also noted $e_{\mathfrak{p}}$ and is called the ramification index of p at $\mathfrak{p}$. One has the relation*

$$n = \sum_{\mathfrak{p}|p} e_{\mathfrak{p}} f_{\mathfrak{p}}.$$

Here we retrive these statement from the adelic viewpoint:
Let $\mathfrak{a} \subset K$ be an ideal, one associates to $\mathfrak{a}$ the sequence of local lattices

$$(\mathfrak{a}_w)_w, \mathfrak{a}_w \in \mathcal{L}(K_w), \text{ for a.e. finite } w, \; \mathfrak{a}_w = \mathcal{O}_w.$$

By density the $\mathcal{O}_K$-action on $\mathfrak{a}$ extend to an $\mathcal{O}_{K_w}$-action on $\mathfrak{a}_w$; since $\mathcal{O}_w$ is a principal ideal ring, $\mathfrak{a}_w$ is of the shape

$$\mathfrak{a}_w = \alpha_w \mathcal{O}_w, \; \alpha_w \in K_w^\times, \; \alpha_w \in \mathcal{O}_{K_w}^\times \text{ for a.e. } w.$$

The number α_w is called a local generator of $\mathfrak{a}$ at the place w; α_w is uniquely defined up to multiplication by an element of $\mathcal{O}_{K_w}^\times$ and we may take α_w to be some power of some uniformizer π_w, say

$$\alpha_w = \pi_w^{v_w(\alpha_w)}.$$

In particular the quantity

$$v_w(\mathfrak{a}) = v_w(\alpha_w) \in \mathbb{Z},$$

does not depend on the choice of α_w and are called the local valuation and the local norm of $\mathfrak{a}$ at the place w. We have therefore constructed a map

$$\mathfrak{a} \in J(\mathcal{O}_K) \mapsto a_f \widehat{\mathcal{O}}_K^\times = (a_w \mathcal{O}_{K_w}^\times)_{w \in \mathcal{V}_{K,f}} \in \mathbb{A}_{K,f}^\times / \widehat{\mathcal{O}_K}^\times$$

where

$$\mathbb{A}_{K,f}^\times = \prod_{w \in \mathcal{V}_{K,f}}{}' K_w^\times$$

is the group of finite ideles of K and

$$\widehat{\mathcal{O}_K}^\times = \prod_{w \in \mathcal{V}_{K,f}} \mathcal{O}_{K_w}^\times$$

is a maximal open-compact subgroup of $\mathbb{A}_{K,f}^\times$.

THEOREM 5.8. *The above map is a group isomorphism. Under this isomorphism, the set of prime ideals* $\mathrm{Spec}(\mathcal{O}_K)$ *correspond to the classes of ideles* $\pi_w \widehat{\mathcal{O}}_K^\times$ *for* $w \in \mathcal{V}_{K,f}$ *(the idele noted* π_w *is the one whose* w*-component is the uniformizer* π_w *and all other components are equal to* 1*).*

PROOF. □

4.2. The norm of an ideal.

DEFINITION 5.7. *The norm (or index) of a fractional ideal* $\mathfrak{a}$ *is the rational number*

$$\mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{a}) = \frac{[\mathcal{O}_K : \mathcal{O}_K \cap \mathfrak{a}]}{[\mathfrak{a} : \mathcal{O}_K \cap \mathfrak{a}]} \in \mathbb{Q}_{>0}.$$

PROPOSITION 5.5. *The norm is a group homomorphism. Under the isomorphism* $J_K \simeq \mathbb{A}_K^\times / \widehat{\mathcal{O}}_K^\times$ *it correspond to*

$$a_f \widehat{\mathcal{O}}_K^\times \mapsto |a_f|_{\mathbb{A}_K}^{-1} = |\,\mathrm{Nr}_{K/\mathbb{Q}}(a_f)|_{\mathbb{A}}^{-1} = \prod_p \prod_{\mathfrak{p}|p} |\,\mathrm{Nr}_{K_\mathfrak{p}/\mathbb{Q}_p}(a_w)|_p^{-1} = \prod_p \prod_{\mathfrak{p}|p} p^{f_\mathfrak{p} v_w(a_w)}.$$

For $\lambda \in K^\times$*, one has the formula*

$$\mathrm{Nr}(\lambda \mathcal{O}_K) = |\,\mathrm{Nr}_{K/\mathbb{Q}}(\delta_f(\lambda))|_{\mathbb{A}}^{-1} = |\,\mathrm{Nr}_{K/\mathbb{Q}}(\lambda)|_\infty.$$

4.3. Two finiteness theorems in algebraic number theory. In the classical algebraic number theory there are two important finitness theorems, one concerning the *ideal class group* of $\mathcal{O}_K$ (due to Dedekind), the other concerning the structure of the group of units $\mathcal{O}_K^\times$ (due to Dirichlet). We describe these theorems in the classical setting and show that they are equivalent to the compactness of the adelic quotient $K^\times\backslash\mathbb{A}_K^{(1)}$.

Let $\mathfrak{a}\subset K$ be a fractional ideal. We have seen that for every non-archimedean place $w\subset\mathcal{V}_{K,f}$ the local $\emptyset_w$-fractional ideal $\mathfrak{a}_w\subset K_w$is principal. We then say that $\mathfrak{a}$ is *locally principal.* Obviously any principal ideal is locally principal and a natural question is whether the converse holds :*is a locally principal ideal globally principal ?.*

The obstruction to this question is measured by

Definition 5.8. *The ideal class group of $\mathcal{O}_K$ is the quotient of the group of fractional ideals by the principal ones*

$$Cl_K=Cl(\mathcal{O}_K)=J_K/P_K;$$

in other terms this is the set of classes of fractional $\mathcal{O}_K$-ideals modulo homothety:

$$\mathfrak{a}\sim\mathfrak{b}\Leftrightarrow\exists\lambda\in K^\times,\ \mathfrak{a}=\lambda\mathfrak{b}.$$

Obviously any fractional ideal is is principal if and only if Cl_K is trivial. This is not always the case but one is not so far away from it since

Theorem 5.9 (Finiteness of the class group). *The ideal class group Cl_K is finite.*

Exercise 5.6. More generally let $\mathcal{O}\subset K$ be an order and let $J(\mathcal{O})$ be the set of fractional $\mathcal{O}$-ideals. One that and ideal $\mathfrak{a}\subset J(\mathcal{O})$ is locally principal if for every non-archimedean place w, $\mathfrak{a}_w 0 a_w\mathcal{O}_w$ for some $a_w\in K_w^\times$. It is not always the case that any fractional $\mathcal{O}$-ideal is principal. The objective of this exercise is to prove the following statement:*if $\mathcal{O}$ is monogenic, that is $\mathcal{O}=\mathbb{Z}[x]$ for some $x\in K$, then every fractional ideal is locally principal.*

Regarding the group of unit $\mathcal{O}_K^\times$ we consider the group of infinite ideles

$$K_\infty^\times=\prod_{w|\infty}K_w^\times\simeq(\mathbb{R}^\times)^{n_1}\times(\mathbb{C}^\times)^{n_2},\ n_1+2n_2=n.$$

We have the embedding

$$\delta_\infty:\mathcal{O}_K^\times\hookrightarrow K_\infty^\times.$$

Because of the product formula, the image of $\mathcal{O}_K^\times$ is contained into the smaller subgroup of infinite ideles whose adelic modulus is 1

$$K_\infty^{(1)}=K_\infty^\times\cap\mathbb{A}_K^{(1)}=\{x_\infty=(x_w)_{w|\infty},\ |x_\infty|_{\mathbb{A}_K}=\prod_{w|\infty}|x_w|_{w,n}=1\}$$

indeed for $x\in\mathcal{O}_K^\times$, $|x_w|_w=1$ for every finite w.

By the polar decompositions

$$x\in\mathbb{R}\mapsto(|x|_\infty,\mathrm{sgn}(x))\in\mathbb{R}_{>0}\times\{\pm1\}$$

and

$$z\in\mathbb{C}\mapsto(|z|_\mathbb{C},z/|z|_\mathbb{C})\in\mathbb{R}_{>0}\times S^1$$

and the logarithm map $\log:\mathbb{R}_{>0}\mapsto\mathbb{R}$, one has the group isomorphisms

$$K_\infty^\times\simeq(\mathbb{R}_{>0})^{n_1+n_2}\times\{\pm1\}^{n_1}\times(S^1)^{n_2}\simeq\mathbb{R}^{n_1+n_2}\times\{\pm1\}^{n_1}\times(S^1)^{n_2}$$

and

$$K_\infty^{(1)} \simeq \mathbb{R}^{n_1+n_2-1} \times \{\pm 1\}^{n_1} \times (S^1)^{n_2},$$

the first factor being the kernel of the linear form

$$(u_1, \cdots, u_{n_1+n_2}) \in \mathbb{R}^{n_1+n_2} \mapsto u_1 + \cdots + u_{n_1} + 2(u_{n_1+1} + \cdots + u_{n_1+n_2})$$

THEOREM 5.10 (Dirichlet unit's theorem). *The image of $\mathcal{O}_K^\times$ in $K_\infty^{(1)}$ is discrete and cocompact. Consequently $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $n_1 + n_2 - 1$.*

THEOREM 5.11. *Theorem 5.5 is equivalent to the two finiteness theorems of Dirichlet and Dedekind.*

PROOF. □

5. Duality, Discriminant and Ramification

As we have seen already, the fact that K is equipped with a natural non-degenerate quadratic form

$$\langle x, y\rangle_{L/\mathbb{Q}} = \mathrm{tr}_{K/\mathbb{Q}}(xy),$$

play an important role in the understanding of the local algebras K_p and their factorization into a product of local fields.

Here we use again this trace form to give an alternative proof of the fact that $\mathcal{O}_K$ is a lattice.

For this we disccuss the notion of duality relative to lattices.

DEFINITION 5.9. *Let k be either $\mathbb{Q}$ or $\mathbb{Q}_v$ and let V be a finite dimenstional k-vector space equipped with a non-degenerate bilinear form $\langle ., .\rangle$. Given $L \subset V$ a $\mathbb{Z}_v$-lattice, the dual lattice L^* is the lattice*

$$L^* = \{x \in V,\ \langle x, L\rangle \subset \mathbb{Z}_v\} = \{x \in V,\ \forall y \in V,\ \langle x, y\rangle \subset \mathbb{Z}_v\}.$$

L^* is indeed a lattice because if $\mathcal{B} = \{\mathbf{e}_i\}$ is a basis of L,

$$L^* = \sum_i \mathbb{Z}_v \mathbf{e}_i^*$$

where $\mathcal{B}^* = \{\mathbf{e}_i^*\}$ is the *dual* basis of $\mathcal{B}$ relative to $\langle\cdot,\cdot\rangle$ (ie. the basis corresponding to the dual basis of $\mathcal{B}$ in V^* under the isomorphism $V \simeq V^*$ induced by $\langle\cdot,\cdot\rangle$):

$$\langle \mathbf{e}_i, \mathbf{e}_j^*\rangle = \delta_{i=j} = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

The dual lattice construction has the following properties (proofs are left as exercises)

$$L^{**} = L$$

$$L \subset L' \Leftrightarrow L'^* \subset L$$

$$(L + L')^* = L^* \cap L'^*.$$

5.1. Duality for ideals. We are now ready to give another proof that

THEOREM 5.12. *$\mathcal{O}_K$ is finitely generated.*

PROOF. We have seen that $\mathcal{O}_K$ contains a lattice say $L\subset\mathcal{O}_K$ and let L^* be the dual lattice. We claim that $\mathcal{O}_K\subset L^*$ hence is finitely generated. Indeed for any $x\in\mathcal{O}_K$ and $y\in L\subset\mathcal{O}_K$ we have $xy\in\mathcal{O}_K.L\subset\mathcal{O}_K.\mathcal{O}_K=\mathcal{O}_K$ since $\mathcal{O}_K$ is a ring; in particular $\mathrm{tr}_{L/\mathbb{Q}}(xy)\in\mathbb{Z}$ the later being the coefficient of degree $n-1$ of $P_{char,xy}\in\mathbb{Z}[X]$. □

We can apply that construction to $\mathcal{O}_K$ or to fractional $\mathcal{O}_K$-ideals: for $\mathfrak{a}\in J_K$ we have the dual lattice

$$\mathfrak{a}^*=\{x\in K,\ \mathrm{tr}_{K/\mathbb{Q}}(x\mathfrak{a})\subset\mathbb{Z}\}.$$

PROPOSITION 5.6. *The dual lattice $\mathfrak{a}^*$ is a fractional ideal. Moreover if $(\mathfrak{a}_w)_w$ are the local $\mathcal{O}_{K_w}$ fractional ideals associated to $\mathfrak{a}$, the local ideals associated to $\mathfrak{a}^*$ are $(\mathfrak{a}^*_w)_w$ where*

$$\mathfrak{a}^*_w=\{x\in K_w,\ \mathrm{tr}_{K_w/\mathbb{Q}_v}(x\mathfrak{a}_w)\subset\mathbb{Z}_v\}$$

is the dual of $\mathfrak{a}_w$ wrt the quadratic form $\langle .,.\rangle_{K_w/\mathbb{Q}_v}=\mathrm{tr}_{K_w/\mathbb{Q}_v}(.\times.)$.

PROOF. For any prime p, let $\mathfrak{a}_p$ be the closure of $\mathfrak{a}$ in K_p; clearly

$$\mathfrak{a}^*_p=\{x\in K_p,\ \mathrm{tr}_{K/\mathbb{Q}}(x\mathfrak{a})\subset\mathbb{Z}_p\}.$$

Let us recall as a quadratic space $(K_p,\langle .,.\rangle_{K_p/\mathbb{Q}_p})$ decompose into an orthogonal sum

$$(K_p,\langle .,.\rangle_{K_p/\mathbb{Q}_p})=\bigoplus_{w|p}(K_w,\langle .,.\rangle_{K_w/\mathbb{Q}_p}).$$

This implies that $\mathfrak{a}_p\subset K_p$ decompose as the orthogonal sum of the $\mathfrak{a}_w$ adn from there is it clear that $\mathfrak{a}^*_p$ is the orthogonal sum of the $\mathfrak{a}^*_w$. □

COROLLARY 5.1. *One has the formula*

$$\mathfrak{a}^*=\mathfrak{a}^{-1}\mathcal{O}^*_K$$

where

$$\mathcal{O}^*_K=\{x\in K,\ \forall y\in\mathcal{O}_K,\ \mathrm{tr}_{K/\mathbb{Q}}(xy)\in\mathbb{Z}\}.$$

is the dual of the ring of integers $\mathcal{O}_K$.

PROOF. If is sufficient to compute $\mathfrak{a}^*_w$ for every finite place w: write $\mathfrak{a}_w=a_w\mathcal{O}_{K_w}$, we have

$$\begin{aligned}\mathfrak{a}^*_w=\{x\in K_w,\ \mathrm{tr}_{K_w/\mathbb{Q}_v}(xa_w\mathcal{O}_{K_w})\subset\mathbb{Z}_v\}\\ =\{x=a_wy,\ y\in K_w,\ \mathrm{tr}_{K_w/\mathbb{Q}_v}(y\mathcal{O}_{K_w})\subset\mathbb{Z}_v\}=a_w^{-1}\mathcal{O}^*_{K_w}.\end{aligned}$$

□

5.2. Different and discriminant. Because of the above result the fractional ideal $\mathcal{O}^*_K$ is of some importance and we will discuss it in greater details. Since

$$\mathrm{tr}_{K/\mathbb{Q}}(\mathcal{O}_K.\mathcal{O}_K)=\mathrm{tr}_{K/\mathbb{Q}}(\mathcal{O}_K)\subset\mathbb{Z}$$

we have he inclusion

$$\mathcal{O}_K\subset\mathcal{O}^*_K$$

or in different terms (using the decomposition into prime ideals) we have

$$\mathcal{O}^*_K=\prod_{\mathfrak{p}}\mathfrak{p}^{v_{\mathfrak{p}}(\mathcal{O}^*_K)}\text{ with }v_{\mathfrak{p}}(\mathcal{O}^*_K)\leqslant 0.$$

We make the following

DEFINITION 5.10. *The different ideal* $\mathfrak{d}_K$ *is defined as the inverse of* $\mathcal{O}_K^*$ *in* J_K

$$\mathfrak{d}_K = (\mathcal{O}_K^*)^{-1} = \prod_{\mathfrak{p}} \mathfrak{p}^{-v_{\mathfrak{p}}(\mathcal{O}_K^*)} \subset \mathcal{O}_K.$$

The norm of the different $\mathfrak{d}_K$ *is called the discriminant of* $\mathcal{O}_K$

$$\mathrm{disc}(\mathcal{O}_K) = \mathrm{Nr}_{K/\mathbb{Q}}(\mathfrak{d}_K) \in \mathbb{N}_{\geqslant 1}.$$

For any finite place w *define the local different and the local discriminant at* w *by*

$$\mathfrak{d}_{\mathfrak{p}} = (\mathcal{O}_{K_{\mathfrak{p}}}^*)^{-1} = \pi_{\mathfrak{p}}^{-v_{\mathfrak{p}}(\mathcal{O}_K^*)}\mathcal{O}_{K_{\mathfrak{p}}}$$
$$\mathrm{disc}(\mathcal{O}_{K_{\mathfrak{p}}}) = \mathrm{Nr}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\mathfrak{d}_{\mathfrak{p}})).$$

We have the following formulas

PROPOSITION 5.7. *Let* $\mathcal{B} = \{\mathbf{e}_i\}$ *be any basis of* $\mathcal{O}_K$*, one has*

$$\mathrm{disc}(\mathcal{O}_K) = |\det(\mathrm{tr}_{K/\mathbb{Q}}(\mathbf{e}_i\mathbf{e}_j))|.$$

Similarly for any prime $\mathfrak{p}$ *and* $\mathcal{B}_{\mathfrak{p}} = \{\mathbf{e}_i\}$ *any basis of* $\mathcal{O}_{K_{\mathfrak{p}}}$

$$\mathrm{disc}(\mathcal{O}_{K_{\mathfrak{p}}}) = |\det(\mathrm{tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\mathbf{e}_i\mathbf{e}_j))|_p^{-1}$$

PROOF. By definition $\mathrm{disc}(\mathcal{O}_K) = [\mathcal{O}_K : \mathfrak{d}_K] = [\mathcal{O}_K^* : \mathcal{O}_K]$ and the later is obtained is $|\det((m_{i,j}))|$ where the m_{ij} are the coordinates of $\mathbb{Z}$-basis $\mathcal{B}$ of $\mathcal{O}_K$ in the dual basis $\mathcal{B}^*$,

$$\mathbf{e}_i = \sum_j m_{ij}\mathbf{e}_j^*.$$

By definition of the dual basis we have

$$m_{ij} = \langle \mathbf{e}_i, \mathbf{e}_j\rangle_{K/\mathbb{Q}}.$$

□

5.3. Ramification. We have the following classical definition:

DEFINITION 5.11. *A prime ideal* $\mathfrak{p} \subset \mathcal{O}_K$ *is ramified if its ramification index* $e_{\mathfrak{p}} > 1$*. A natural prime* p *is ramified in* $\mathcal{O}_K$ *if there is some prime ideal* $\mathfrak{p} \subset \mathcal{O}_K$ *dividing* p *which is ramified. Prime or prime ideal which are not ramified are called unramified.*

The following result shows that there are only finitely many ramified primes:

THEOREM 5.13. *Given* $\mathfrak{p}$ *a prime ideal, one has the equivalence*

$$v_{\mathfrak{p}}(\mathfrak{d}_K) > 0 \Leftrightarrow e_{\mathfrak{p}} > 1.$$

Consequently a prime number p *is ramified if and only if it divides the discriminant* $\mathrm{disc}(\mathcal{O}_K)$*.*

PROOF. We prove the implication

$$e_{\mathfrak{p}} > 1 \Rightarrow v_{\mathfrak{p}}(\mathfrak{d}_K) > 0$$

and leave the converse as an exercise. Under the assumption $e_{\mathfrak{p}} > 1$ we want to show that $\mathfrak{p}|\mathfrak{d}_K$ or equivalently that $p|\det(\mathrm{tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\mathbf{e}_i\mathbf{e}_j))$ where $\mathcal{B}_{\mathfrak{p}} = \{\mathbf{e}_i\}$ is a basis of $\mathcal{O}_{K_{\mathfrak{p}}}$. For this we consider the quotient $k_{\mathfrak{p},p} = \mathcal{O}_{K_{\mathfrak{p}}}/p\mathcal{O}_{K_{\mathfrak{p}}}$; this is a finite dimensional $\mathbb{F}_p$-algebra of dimension $d_{\mathfrak{p}}$ which equipped with the bilinear form $\langle .,.\rangle_{K_{\mathfrak{p}}/\mathbb{Q}_p} \,(\mathrm{mod}\, p)$,

$$\langle .,.\rangle_{\mathfrak{p},p} : (x \,(\mathrm{mod}\, p), y \,(\mathrm{mod}\, p)) \in k_{\mathfrak{p},p}^2 \mapsto \mathrm{tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(xy) \,(\mathrm{mod}\, p)$$

(verify that this is well defined). The set $\mathcal{B}\,(\mathrm{mod}\,p)$ form an basis of $k_{\mathfrak{p},p}$ (because it is generating of the right cardinality) and $\det(\mathrm{tr}_{K_\mathfrak{p}/\mathbb{Q}_p}(\mathbf{e}_i\mathbf{e}_j))\,(\mathrm{mod}\,p)$ is the determinant of the trace form $\langle .,.\rangle_{K_\mathfrak{p}/\mathbb{Q}_p}\,(\mathrm{mod}\,p)$ in that basis. Let us assume that $e_\mathfrak{p} > 1$, and let $\pi_\mathfrak{p}$ be some uniformizer. Under our assumption, the element $\pi_\mathfrak{p}\,(\mathrm{mod}\,p)$ is a non-zero nilpotent element of $k_{\mathfrak{p},p}$ of nilpotent index $e_\mathfrak{p}$, in particular for any $x\,(\mathrm{mod}\,p) \in k_{\mathfrak{p},p}$, $x\pi_\mathfrak{p}\,(\mathrm{mod}\,p)$ is nilpotent and

$$\mathrm{tr}_{K_\mathfrak{p}/\mathbb{Q}_p}(x\pi) \equiv 0\,(\mathrm{mod}\,p)$$

which shows that the bilinear form $\langle .,.\rangle_\mathfrak{p}\,(\mathrm{mod}\,p)$ is degenerate hence equals $0\,(\mathrm{mod}\,p)$. $\square$