# COHOMOLOGY DETERMINANTS AND RECIPROCITY LAWS: NUMBER FIELD CASE

M. Kapranov, A. Smirnov

Analogies between number fields and function fields have been a long-time source of inspiration in arithmetic. However, one of the most intriguing problems in this approach, namely the problem of the absolute point, is still far from being satisfactorily understood. The scheme $\mathrm{Spec}(\mathbb{Z})$, the final object in the category of schemes, has dimension 1 with respect to the Zariski topology and at least 3 with respect to the etale topology. This generated a long-standing desire to introduce a more mythical object $P$, the "absolute point" with a natural morphism $\pi_X : X \to P$ given for any arithmetic scheme $X$ so that global invariants of $X$ have an interpretations in terms of a version of direct image with respect to $\pi_X$. This problem involves also the question of the compactification, since even a scheme proper over $\mathbb{Z}$ is still non-compact at the arithmetic infinity.

One theory which successfully addresses these problems is Arakelov geometry [...]. The compactifications provided by it involve Riemannian metrics at the sets of real points of arithmetic schemes, and the cohomological invariants have the form of volumes of fundamental domains of some lattices (given by the direct image to $\mathrm{Spec}(\mathbb{Z})$) with respect to volume forms coming from the metrics. The volume of a convex body is the leading term of the asymptotic of the number of integer points in its dilations. So the analog of Arakelov-type invariants in the more geometric situation is the leading term of the Hilbert polynomial of a coherent sheaf, which describes the asymptotic of the dimension of the space of sections with growing order of poles at the infinity.

Thus the output of the Arakelov theory is essentially Archimedean, having to do with the asymptotics of some integers within the real numbers.

In the present paper we would like to initiate a different approach to the problem of "absolute" cohomological invariants, which can be called Arakelov geometry modulo $n$. Let us describe the main ideas.

First of all, it is an old idea to interpret combinatorics of finite sets as the $q \to 1$ limit of linear algebra over the finite fields $\mathbf{F}_q$. This had lead to frequent consideration of the folklore object $\mathbf{F}_1$, the "field with one element", whose vector spaces are just sets. One can postulate, of course, that $\mathrm{Spec}(\mathbf{F}_1)$ is the absolute point, but the real problem is to develop non-trivial consequences of this point of view.

In [...] the affine line over $\mathbf{F}_1$ was considered; it consists formally of 0 and all the roots of unity. Put slightly differently, this leads to the consideration of "algebraic extensions" of $\mathbf{F}_1$. By analogy with genuine finite field we would like to think that there is exactly one such extension of any given degree $n$, denote it $\mathbf{F}_{1^n}$. Of course, $\mathbf{F}_{1^n}$ does not exist in a rigorous sense, but we can think if a scheme $X$ contains $n$-th roots of unity, then it is defined over $\mathbf{F}_{1^n}$, so that we have a morphism

$$p_X : X \to \mathrm{Spec}(\mathbf{F}_{1^n}). \tag{1}$$

The point of view that adjoining roots of unity is analogous to the extension of the base field goes back, at least, to Weil (Lettre à Artin, Ouevres, vol.1) and Iwasawa [...].

The aim of the "Arakelov geometry modulo $n$" which we propose, is to make sense of the cohomological invariants obtained via the direct image of the morphism (1). One of the most interesting such invariants is the determinant of the cohomology, $\det(Rp_{X*}(\mathcal{F}))$ for a coherent sheaf $\mathcal{F}$ on $X$. In the geometric case the problem of calculating this determinant, as a functor of $\mathcal{F}$, contains the Riemann-Roch problem. In our case, vector spaces over $\mathbf{F}_{1^n}$ are sets with a free action of the group $\mu_n$ of $n$th roots of 1, and it is possible to develop the determinantal formalism (see Section 1 below). The corresponding Riemann-Roch problem involves not volumes, but rather residues modulo $n$ of the numbers of integer points in some polyhedra. The analogs of the direct images of Chern classes (i.e., Deligne's torsors $\langle L, M\rangle$) involve $n$-power residue symbols, and well-definedness of our determinantal formalism implies a very natural proof of the reciprocity law for these symbols. In fact, some modern approaches to the reciprocity law, like the one of Kubota [...], can be viewed as implicitly dealing with linear algebra over $\mathbf{F}_{1^n}$, constructing special bases etc. We use some of Kubota's ideas to develop a theory of "Arakelov compactification" of vector bundles on arithmetic curves; similarly to the standard procedure, our compactification involves some domains in $M \otimes \mathbf{R}$, where $M$ is a module over the ring of integers of a number field, but in our case the domains are of polyhedral nature and well behaved with respect to counting of points modulo $n$ in their dilations.

It is not yet clear how to formulate the correct analog of the Riemann- Roch theorem; what is certain, is that it should be a statement relating residue modulo $n$ of the number of integer points in a polyhedron with $n$-power residue symbols. Several statements of this kind are known, starting from the Gauss' geometric proof of the quadratic reciprocity law.

Let us now explain the contents of the paper in more detail. In Section 1 we discuss in some detail the formalism of absolute fields (algebraic extensions of $\mathbf{F}_1$), linear algebra over such fields, theory of determinants and determinantal torsors.

In Section 2 we develop rudiments of the homological algebra over absolute fields, which will be necessary for us. In particular, we study the analogs of exact sequences. All this formalism is adapted to considering invariants (like dimension) modulo $n$.

In Section 3 we define the cohomological invariants of arithmetic curves which are, informally, related to cohomology of constructible sheaves rather than coherent sheaves. This does not require compactification, but does require working with level $N$ structures. In particular, we define the "resultant torsors" $\langle L, M\rangle$ for two line bundles with level structure. The existence of a good theory of such torsors is equivalent to the reciprocity law of class field theory. We also trace in some detail the analogy between class field theory and the theory of knots and links in the 3-space.

In Section 4 we construct a theory of "modulo $n$ compactifications" of arithmetic curves. In particular, we construct the cohomology of a (coherent) sheaf on the compactified curve. They are, of course, vector spaces over the absolute field. Our approach uses, in a crucial way, the notion of so-called "cohomological domain", a certain technical concept whose role is to make sure that the cohomology as we define it, behaves in the expected way under twisting with very ample sheaf. This is done in the separate Section 5.

# 1 Absolute fields.

## 1.1 The "field" $\mathbf{F}_1$.

Let us briefly recall the folklore imagery related to $\mathbf{F}_1$, the (non-existent) field with one element.

A vector space over $\mathbf{F}_1$ is just a set; the dimension of such a vector space is the cardinality of the set. The general linear group $GL_n(\mathbf{F}_1)$ is the symmetric group $S_n$. The analog of the determinant $\det : GL_n(F) \to F^*$ for $F = \mathbf{F}_1$ is the sign homomorphism $\mathrm{sgn} : S_n \to \{\pm 1\}$. The special linear group $SL_n(\mathbf{F}_1)$ is just the alternating group $A_n$.

Thus, the linear algebra over $\mathbf{F}_1$ is the same as the combinatorics of (finite) sets. For instance, if $X$ is such a set, $|X| = n$, then $k$-elements subsets in $X$ should be thought as $k$-dimensional vector subspaces in $X$ as a $\mathbf{F}_1$-vector space. Their number, $\binom{n}{k}$ is equal to the limit for $q \to 1$ of the cardinalities of $G(k,n)(\mathbf{F}_q)$, the actual Grassmann varieties over actual fields $\mathbf{F}_q$.

## 1.2 Polynomial rings over $\mathbf{F}_1$.

Along with the "field" $\mathbf{F}_1$, we may want to have the polynomial "ring" $\mathbf{F}_1[t]$. Although such a ring does not exist as well, we can say something about objects related to it.

The group $GL_d(\mathbf{F}_1[t])$ is the full braid group $B_d$ on $d$ strings. The canonical homomorphism $f : B_d \to S_d$ should be thought of as $q \to 1$ limit of the evaluation homomorphisms

$$GL_d(\mathbf{F}_q[t]) \to GL_d(\mathbf{F}_q), \quad A(t) \mapsto A(0).$$

The subgroup $P_d = \mathrm{Ker}(\epsilon)$, called the pure braid group, is thus the analog of the congruence subgroup $GL_d(\mathbf{F}_q[t], t)$.

This point of view can be justified as follows. The group $B_d$ is the fundamental group of the space $\mathbf{C}_0^d$ of complex polynomials $x^d + a_1 x^{d-1} + ... + a_d$ without multiple roots, and, accordingly, the subgroup $P_n$ is the fundamental group of the space

$$\mathbf{C}_*^d = \mathbf{C}^d - \bigcup_{i \neq j} \{(x_1, ..., x_d) : x_i = x_j\}.$$

Let now $F$ be an algebraically closed field containing $\mathbf{F}_q$. The space

$$F_*^d = F^d - \bigcup_{(\alpha_1,...,\alpha_d) \in \mathbf{F}_q^d - \{0\}} \left\{(x_1, ..., x_d) : \sum \alpha_i x_i = 0\right\}$$

is acted upon by the group $GL_d(\mathbf{F}_q)$, and the quotient is identified with the space of $q$-polynomials

$$x^{q^d} + a_1 x^{q^{d-1}} + ... + a_{d-1} x^q + a_d x, \quad a_d \neq 0.$$

For every $N \in \mathbf{F}_q[t]$, $N = \sum b_i t^i$, Drinfeld constructed an unramified covering of $F_*^d / GL_d(\mathbf{F}_q)$ with the Galois group $GL_d(\mathbf{F}_q[t]/N)$. This is the moduli space of elliptic $\mathbf{F}_q[t]$-modules of rank $d$ with level $N$ structure, see [...]. Thus the profinite completion of $GL_d(\mathbf{F}_q[t])$ is embedded into the fundamental group of the space of $q$-polynomials.

**(1.3) Algebraic extensions of $\mathbf{F}_1$.** Since we think of $\mathbf{F}_1$ as a "field", we would like to consider its finite extensions. It is natural to think, by analogy with genuine finite fields,

that for any $n$ we have one such extension of degree $n$. Denote it $\mathbf{F}_{1^n}$. We think of $\mathbf{F}_{1^n}$ as containing zero and $\mu_n$, the set of all roots of unity of order $n$. One can, if one wants, say that $\mathbf{F}_{1^n}$ is the monoid $\{0\} \cup \mu_n$.

Equivalently, we introduce the affine line over $\mathbf{F}_1$, to consist of 0 and the roots of unity of all orders. So as a set it is identified with the "algebraic closure" of $\mathbf{F}_1$. Also, the affine line should be regarded as the spectrum of the non-existing ring $\mathbf{F}_1[t]$. For the analog of the evaluation map from the braid group corresponding to a point of the affine line, see n. 1.4 below.

We regard $\mathbf{F}_1$ as the absolute point of the category of schemes, so that every scheme is defined over $\mathbf{F}_1$. We say that a scheme $X$ is defined over $\mathbf{F}_{1^n}$, if the ring of regular functions on $X$ contains $n$th roots of 1. This is in accord with Iwasawa theory [...] where adding roots of unity to a number field replaces the extension of base field for a curve.

**(1.4) Linear algebra over $\mathbf{F}_{1^n}$.** Let us extend the formalism of (1.1) to algebraic extensions of $\mathbf{F}_1$. A vector space over $\mathbf{F}_{1^n}$ is a pointed set $(V, 0 \in V)$ with an action of the group $\mu_n$ free on $V - \{0\}$. The element 0 is fixed under the action. Its addition is really optional; it serves to make the standard constructions with vector spaces sound more familiar. Also, it is always present in natural examples. For a vector space $V$ over $\mathbf{F}_{1^n}$ we denote by $\tilde{V}$ the set $V - \{0\}$.

A linear map $V \to W$ is just a map of $\mu_n$-sets.

A *basis* of a vector space $V$ is, by definition, a subset $B \in \tilde{V}$ such that every $\mu_n$-orbit contains a unique element of $B$. The dimension of $V$ is the cardinality of any basis, i.e., the cardinality of $\tilde{V}/\mu_n$.

The general linear group $GL_d(\mathbf{F}_{1^n})$ is the group of automorphisms of a $d$-dimensional vector space; this is just the wreath product of $S_d$ and $(\mu_n)^d$. It can be viewed as the group of $d$ by $d$ matrices which contain exactly one non-zero element in each row and each column, and this element is a root of unity from $\mu_n$. Given a root of unity $\epsilon \in \mu_n$, we have the "evaluation map"

$$f_\epsilon : B_d = GL_d(\mathbf{F}_1[t]) \to GL_d(\mathbf{F}_{1^n})$$

described as follows. Recall that $B_d$ is generated by elements $\sigma_i, i = 1, ..., d-1$ with relations

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \quad \sigma_i\sigma_j = \sigma_j\sigma_i, \ |i-j| \geq 2.$$

The map $f_\epsilon$ is defined by the condition

$$f_\epsilon(\sigma_i) = \mathbf{1}_{i-1} \oplus \oplus \mathbf{1}_{n-i-1},$$

where by $\mathbf{1}_i$ we denote the unit $i$ by $i$ matrix, and $\oplus$ stands for the direct (block-diagonal) sum of matrices.

The category of $\mathbf{F}_{1^n}$-vector space is equipped with the operations of direct sum $V \vee W$ and smash product $V \wedge W$. By definition, $V \vee W$ is obtained from the disjoint union $V \coprod W$ by identifying the zero elements, and $V \wedge W$ is obtained from the Cartesian product $V \times W$ by identifying $(V \times 0) \cup (0 \times W)$ with 0. Thus after disregarding the zero elements the operations $\vee, \wedge$ correspond to disjoint inion and Cartesian product of free $\mu_n$-sets.

We introduce also the tensor product $V \otimes W$ as the quotient of $V \wedge W$ by the antidiagonal action of $\mu_n$, i.e., by the identification $x \wedge y = \epsilon x \wedge \epsilon^{-1} y$. Denote by $x \otimes y$ the image of

$x \wedge y$ in $V \otimes W$ and equip $V \otimes W$ with the $\mu_n$-action by the rule $\epsilon(x \otimes y) = (\epsilon x) \otimes y = x \otimes (\epsilon y)$. It is clear that

$$\dim(V \vee W) = \dim(V) + \dim(W), \quad \dim(V \otimes W) = \dim(V) \times \dim(W).$$

**(1.5) Determinants.** Let $V$ be a vector space over $\mathbf{F}_1$ and $A : V \to V$ be its automorphism. Its determinant $\det(A)$ is defined as follows. Choose any basis $e_1, ..., e_d$ of $V$, so that $A(e_i) = \alpha_i e_{\sigma(i)}$ for some permutation $\sigma \in S_d$ and some roots of unity $\alpha_i \in \mu_n$. Then, by definition, $\det(A) = \prod \alpha_i$. One easily verifies the equality $\det(AB) = \det(A)\det(B)$ which implies that $\det(A)$ is independent on the choice of a basis.

Note the absense of any minus signs in our definition of the determinant. We will give an explanation for this later on. Right now let us give two examples justifying our choice.

**1.2.1. Proposition.** *(1.6) Proposition. Let $n = 2$ and let $V$ be a $\mathbf{F}_{1^2}$-vector space, so $\tilde{V}$ is a set with free involution. Let $d = \dim(V)$ and $A : V \to V$ be an automorphism. Then $\det(A) \in \mu_2 = \{\pm 1\}$ coincides with the sign of the permutation $\tilde{V} \to \tilde{V}$ of the $2d$ elements of $\tilde{V}$ given by $A$.*

**(1.7) Power residue symbol as the determinant.** Let $q$ be a prime power and $\mathbf{F}_q$ be a finite field with $q$ elements. Suppose that $q \cong 1 (\mathrm{mod}\, n)$. Then $\mathbf{F}_q$ contains $n$th roots of 1, and we identify $\mu_n$ with the subgroup in $\mathbf{F}_q^*$. Then for every $a \in \mathbf{F}_q^*$ we have the power residue symbol

$$\left(\frac{a}{\mathbf{F}_q}\right)_n = a^{\frac{q-1}{n}} \in \mu_n.$$

On the other hand, the embedding $\mu_n \mathbf{1} \mathbf{F}_q^*$ makes $\mathbf{F}_q$ a vector space over $\mathbf{F}_{1^n}$ in the above defined sense. The multiplication by $a$ is an automorphism of this space. The following fact is a version of a classical lemma of Gauss.

**1.2.2. Proposition.** *(1.8) Proposition. The $n$th power residue symbol $\left(\frac{a}{\mathbf{F}_q}\right)_n$ is equal to the determinant of the multiplication by $a$.*

We leave the proof to the reader.

**(1.9) Determinantal spaces and exterior powers.** Let $A$ be any Abelian group, with operation written multiplicatively. The category of torsors (principal homogeneous spaces) over $A$ has a natural monoidal structure which we denote $\otimes$. Explicitly, if $T, S$ are $A$- torsors, then $T \otimes S$ is generated by symbols $t \otimes s$ with $t \in T, s \in S$ subject to the relations $(at) \otimes s = t \otimes (as)$. The operation $\otimes$ is obviously commutative and associative in the sense that we have natural isomorphisms. When $A$ is the multiplicative group of a field $F$, then this operation corresponds to the tensor product of 1-dimensional $F$-vector spaces.

Let now $V$ be a $d$-dimensional vector space over $\mathbf{F}_{1^n}$. Then $\tilde{V}$ is the union of $\mu_n$-orbits, each of which is a $\mu_n$-torsor. We define the determinantal space $\det(V)$ as the union of zero and the $\otimes$-product of all these torsors:

$$\det(V) = \{0\} \cup \bigotimes_{T \in \tilde{V}/\mu_n} T.$$

It is clear that for an automorphism $f : V \to V$ its determinant $\det(f)$ is just the induced map $\det(V) \to \det(V)$.

Note, in particular, that for every $\epsilon \in \mu_n$ the multiplication by $\epsilon$ defines an isomorphism $V \to V$, and its determinant, which is a map $\det(V) \to \det(V)$, is the multiplication by $\epsilon^{\dim(V)}$. Thus det as a functor recovers the dimensions of $\mathbf{F}_{1^n}$-vector spaces taken modulo $n$. Later we will consider the dimension modulo $n$ as the basic invariant of a vector space (see §2).

More generally, for every $k \leq d$ we define the $k$th exterior power $\bigwedge^k V$ as follows:

$$\bigwedge^k V = \{0\} \cup \coprod_{I \in \tilde{V}/\mu_n, |I|=k} \bigotimes_{T \in I} T.$$

It is convenient to do the tensor algebra in a slightly more systematic way. Fix the following action of the symmetric group $S_k$ on $V^{\otimes k}$:

$$\sigma(x_1 \otimes ... \otimes x_k) = x_{\sigma(1)} \otimes ... \otimes x_{\sigma(k)}.$$

Then $\bigwedge^k V$ is obtained from the quotient $V^{\otimes k}/S_k$ by identifying with 0 every element $x_1 \otimes ... \otimes x_k$ in which some of the $x_i, x_j$ are proportional (with coefficient of proportionality lying in $\mu_n$). We denote by $x_1 \wedge ... \wedge x_k$ the image of $x_1 \otimes ... \otimes x_k$ in $\bigwedge^k V$.

Still another justification for the absense of signs in our determinant theory is given by the following fact.

**1.2.3. Proposition.** *(1.10) Proposition. Let $q$ be a prime power, $\mathbf{F}_q$ be a field with $q$ elements and $n = q - 1$. Identify $\mu_n$ with $\mathbf{F}_q^*$. Let $V$ be any $\mathbf{F}_q$-vector space. Then the determinant of $V$ regarded as a $\mathbf{F}_{1^n}$-vector space is identified with the standard top exterior power of $V$ regarded as $\mathbf{F}_q$-vector space (the identification being equivariant with respect to the group $\mathrm{Aut}_{\mathbf{F}_q}(V)$).*

*In particular, for every $\mathbf{F}_q$-linear automorphism $f : V \to V$ the two possible definitions of the determinant of $f$ coincide.*

*Proof.* In view of our definition of the determinant over $\mathbf{F}_{1^n}$, our statement amounts to a statement of pure $\mathbf{F}_q$-linear algebra which can be stated as the existence of the natural isomorphism

$$\det_{\mathbf{F}_q}(V) \to \bigotimes_{L \in P(V)} L, \tag{1.11}$$

where on the right stands the (ordinary) tensor product of all the 1-dimensional $\mathbf{F}_q$-vector subspaces in $V$. By $P(V)$ we denote the projectivization of $V$.

By definition, the right hand side of (1.11) is generated by elements $x_\phi = \bigotimes_{L \in P(V)} \phi(L)$ for all sections $\phi$ of the natural projection $V - \{0\} \to P(V)$. If $\phi, \psi$ are two such elements, then we have

$$x_\psi = \left( \prod_{L \in P(V)} \frac{\psi(L)}{\phi(L)} \right) x_\phi.$$

On the othen hand, the space $\det_{\mathbf{F}_q}(V)$ is spanned by symbols $v_1 \wedge ... \wedge v_d$, for all the bases $v_1, ..., v_d$ of $V$ with the standard relations of antisymmetry and multi-linearity. We now define a map $\det_{\mathbf{F}_q}(V) \to \det_{\mathbf{F}_{1^n}}(V)$ as follows.

Let $v_1, ..., v_d$ be a basis of $V$. Consider the following system of representatives of the $\mathbf{F}_q^*$-action on $V - \{0\}$: In other words, this is the natural lifting into $V - \{0\}$ of the natural cell decomposition of $P(V)$ associated with the basis $v_1, ..., v_d$.

**1.2.4. Lemma.** *(1.12) Lemma. The element $x(v_1, ..., v_d) \in \bigotimes_{L \in P(V)} L$ given by the tensor product of the set of representatives just constructed, depends on $v_1, ..., v_d$ in an antisymmetric and multilinear way.*

*Proof.* (a) Antisymmetry: Suppose we interchange $v_i$ and $v_{i+1}$. Consider first for simplicity the case $i = 1$. Denote by $P^1$ the projectivization of the $\mathbf{F}_q$-subspace in $V$ spanned by $v_1, v_2$. The elements $x(v_1, v_2, ..., v_d)$ and $x(v_2, v_1, ..., v_d)$ differ by the factor which is the product over all $L \in P^1$ of the ratios of the representatives of the first and second family lying in $L$. If $L = \mathbf{F}_q v_1$ or $\mathbf{F}_q v_2$, then the corresponding representatives are the same. If $L$ is spanned by $v_1 + av_2$ with $a \in \mathbf{F}_q^*$, then the ratio of the two representatives is equal to $a^{-1}$. Thus

$$\frac{x(v_1, v_2, ..., v_d)}{x(v_2, v_1, ..., v_d)} = \prod_{a \in \mathbf{F}_q^*} a^{-1} = -1.$$

In the vase when we interchange $v_i$ and $v_{i+1}$ with $i > 1$, we have essentially the same picture but directly multiplied by $(\mathbf{F}_q)^{i-1}$. Thus the ratio of the two elements of det will be $(-1)^{q^{i-1}}$. This quantity always equal to 1 in the field $\mathbf{F}_q$: if $q$ is odd, then we raise $(-1)$ to an odd power and get $(-1)$, while if $q$ is even, then $(-1) = 1$.
(b) Multilinearity: It is enough to prove that, first, $x(v_1, ..., v_d)$ is unchanged under elementary transformations, i.e., replacement of $v_i$ by $v_i + \lambda v_j$ and, second, the multiplication of one of the $v_i$ by $\lambda \in \mathbf{F}_q$ multiplies $x(v_1, ..., v_d)$ by $\lambda$. To prove the first statement it is enough, by antisymmetry, to consider the case $i = 2, j = 1$. But for two bases differing by such a transformation, the corresponding sets of representatives are the same. To prove the second statement, it is enough to multiply $v_1$ by $\lambda$. But $x(\lambda v_1, v_2, ..., v_d) = \lambda x(v_1, v_2, ..., v_d)$ by definition. Lemma 1.12 and Proposition 1.10 are proved.

# 2 Homological algebra over absolute fields.

In this section we fix an integer $n$, denote the group $\mu_n$ of $n$th roots of 1 simply by $\mu$ and write simply $F$ instead of $\mathbf{F}_{1^n}$.

The category of finite-dimensional $F$-spaces will be denoted by $\mathcal{M}$. This category is non-linear, so the natural replacement of homological algebra would be the theory of closed model categories of Quillen [...]. However, it seems that $\mathcal{M}$ does not allow a closed model structure, and we define only certain rudiments of such a structure.

**(2.1) Cofibrations.** The role of cofibrations will be played by embeddings of $F$-spaces. If $f : V \hookrightarrow W$ is such an embedding, we denote by $V/W$ the result of contraction of $W$ into 0. Occasionally we will also deal with quotients of Abelian groups (which may also be $F$-spaces). To avoid confusion, the group-theoretic quotient will be always denoted $\frac{W}{V}$.

It is clear that we have a canonical isomorphism

$$\det(V) \otimes \det(W/V) \to \det(W).$$

**(2.2) Fibrations and equivalences.** Let $f : V \to W$ be a morphism of $F$-vector spaces. We say that $f$ is a fibration if for each $w_1, w_2 \in W$ we have the congruence $|f^{-1}(w_1)| \equiv |f^{-1}(w_2)| \pmod{n}$.

We say that $f$ is an equivalence if $f^{-1}(0) = 0$ and for every non-zero $w \in W$ the cardinality of $f^{-1}(w)$ is congruent to 1 modulo $n$. Thus every equivalence in our sense is a fibration.

Clearly, if $f$ is an equivalence, then $\dim(V) \cong \dim(W) \pmod n$.

We denote by $\mathcal{M}^*$ the subcategory in $\mathcal{M}$ with the same objects as $\mathcal{M}$ and morphisms which are the equivalences.

**2.0.5. Proposition.** *(2.3) Proposition. Let $f : V \to W$ be an equivalence and $B = \{w_1, ..., w_d\}$ be a basis of $W$. Then $f^{-1}(B)$ is a basis of $V$. Moreover, the rule*

$$w_1 \wedge ... \wedge w_d \mapsto \bigwedge_{v \in f^{-1}(B)} v$$

*defines an isomorphism $\det(W) \to \det(V)$. This isomorphism is independent on the choice of a basis $B$.*

We denote by $\det(f) : \det(V) \to \det(W)$ the isomorphism inverse to one constructed in Proposition 2.3.

Let $\mathcal{P}$ be the category of 1-dimensional $F$-vector spaces and their isomorphisms. Then det extends to a covariant functor $\mathcal{M}^* \to \mathcal{P}$. Since every morphism in $\mathcal{P}$ is an isomorphism, this shows that the category obtained from $\mathcal{M}^*$ by formally inverting all the morphisms, is non-trivial.

**2.0.6. Definition.** *(2.4) Definition. A sequence of $F$-vector spaces and their morphisms*

$$S = \left\{ 0 \to V' \xrightarrow{\alpha} V \xrightarrow{\beta} V'' \to 0 \right\} \tag{2.4.1}$$

*is called exact, if $\alpha$ is a set-theoretic injection, the composition $\beta\alpha$ is equal to 0, and the map from $V/\alpha(V')$ to $V''$ induced by $\beta$, is an equivalence.*

It is clear that for an exact sequence we have

$$\dim(V) \equiv \dim(V') + \dim(V'') \pmod n.$$

**(2.5) Examples.** (a) For every $V$ the map $(V \times F)/(0 \times F) \to V$ is an equivalence.

(b) Let $q$ be a prime power, and $n$ be a divisor of $q-1$. Let us identify $\mu = \mu_n$ with the group of $n$-th roots of unity inside the finite field $\mathbf{F}_q$. Then any $\mathbf{F}_q$-vector space becomes an $F$-vector space, and every short exact sequence of $\mathbf{F}_q$-vector spaces and $\mathbf{F}_q$-linear operators is exact in the sense of Definition 2.3.

**(2.6) Determinants and exact sequences.** The category $\mathcal{P}$ of 1-dimensional vector spaces and their isomorphisms is naturally a Picard category, i.e., a symmetric monoidal category with every object functorially invertible. The operation on $\mathcal{P}$ is given by the tensor product $\otimes$ (which corresponds to the the product $\odot$ on $\mu$-torsors).

Given an exact sequence $S$ as in (2.3.1), the functoriality of det on equivalences gives an isomorphism

$$\lambda_S : \det(V') \otimes \det(V'') \to \det(V)$$

which is natural with respect to equivalences of short exact sequences.

**(2.7) Exact complexes.** Let

$$0 \to V^0 \xrightarrow{d_0} V^1 \xrightarrow{d_1} V^1 \xrightarrow{d_2} ... \xrightarrow{d_{n-1}} V^n \to 0$$

be a sequence of $F$-vector spaces and their morphisms. Such a sequence is called a complex, if the composition $d_i \circ d_{i-1}$ is the zero map for every $i$. A sequence is called exact, if it is a complex and for every $i$ the sequence

$$0 \to \mathrm{Im}(d_{i-1}) \hookrightarrow V^i \xrightarrow{d_i} \mathrm{Im}(d_i) \to 0$$

is exact.

For any graded $F$-space $V^\bullet = (V^i, i \in \mathbf{Z})$ we define

$$\det(V^\bullet) = \bigotimes \det(V^i)^{(-1)^i}.$$

In particular, every complex gives a graded $F$-space.

**2.0.7. Proposition.** *(2.8) Proposition. If $V^\bullet = (V^i, d_i)$ is an exact complex, then there is a natural identification*

$$\mathrm{Eu} : \det(V^\bullet) \to \mu.$$

*This isomorphism depends on the maps in the complex. We will denote by $\langle V^\bullet \rangle \in \det(V^\bullet)$ the inverse image of $1 \in \mu$ under the isomorphism Eu.*

# 3 Class field theory and level structures.

**(3.1) Three-dimensional point of view on** $\mathrm{Spec}(\mathbf{Z})$**.** A considerable part of class field theory can be viewed as an analog of the theory of knots and links in 3-manifolds.

More precisely, the spectrum of a finite field $\mathbf{F}_q$ can be naturally visualized as a circle, because, similarly to the circle, it has one connected unramified cover $\mathrm{Spec}(\mathbf{F}_{q^m})$ for every $m \geq 1$. The Frobenius element, generating $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$ is represented by the monodromy along the circle.

Let now $K$ be a number field, $A$ its ring of integers and $X = \mathrm{Spec}(A)$. Then it is natural to visualize $X$ as a 3-dimensional manifold. The spectra of prime residue fields of $A$ can be thus viewed as circles inside this 3-manifold which can be knotted, linked etc. This point of view was advocated by Y. Manin and B. Mazur. It is in agreement with the fact that the etale cohomological dimension of $X$ is equal to 3, see [...].

**(3.2) Legendre symbols and linking numbers.** Recall one of the definitions of the linking number. Let $M$ be a compact 3-manifold and $C, D$ be two non-intersecting embedded circles in $M$. Suppose that $C$ is homologous to 0. Then there exists a connected Galois covering $\tilde{M} \to M$ with Galois group $\mathbf{Z}$ ramified along $C$. The monodromy along $D$ in this covering is thus an integer $(C, D)$ called the linking number of $C$ and $D$. In the case when $D$ is also homologous to 0, the number $(D, C)$ is defined and we have

$$(D, C) = (C, D) \tag{3.2.1}$$

If $C$ is homologous to 0 modulo $n$, we can, by using $\mathbf{Z}/n$-coverings, define the intersection index modulo $n$.

Another, more standard, definition of $(C, D)$ is as the intersection number $(\sigma \cdot D)$ where $\sigma$ is a 2-chain bounding $C$.

Now the Legendre symbol of quadratic reciprocity is the arithmetic analog of the mod. 2 linking number. Namely, take $X = \mathrm{Spec}(\mathbf{Z})$ and let $p \in \mathbf{Z}$ be a prime of the form $4k + 1$. Then the scheme $\tilde{X}$, the spectrum of the ring of integers of $\mathbf{Q}[\sqrt{p}]$, is a double

cover of $X$ ramified only at $p$. If $q$ is another prime number, then the Legendre symbol $\left(\frac{p}{q}\right)$ is the element of $\mathrm{Gal}(\tilde{X}/X) = \{\pm 1\}$ corresponding to the Frobenius at $q$, i.e., in our visualization, to the monodromy along the circle $\mathrm{Spec}(\mathbf{F}_q) \imath X$. Thus $\left(\frac{p}{q}\right)$ can be viewed as the linking number of the "circles" $\mathrm{Spec}(\mathbf{F}_p)$ and $\mathrm{Spec}(\mathbf{F}_q)$ in the "3-fold" $\mathrm{Spec}(\mathbf{Z})$. If both $p, q$ are of the form $4k+1$, then the Gauss reciprocity law shows that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, which is the analog of (3.2.1).

If, however, $p = 4k+3$, then there is no covering of $X$ ramified only at $p$ (by taking $\sqrt{p}$ we get ramification at $p$ and 2, while by taking $\sqrt{-p}$ we get ramification at $p$ and $\infty$). This means that in this case $\mathrm{Spec}(\mathbf{F}_p) \imath \mathrm{Spec}(\mathbf{Z})$ should be regarded as a circle not homologous to 0. So before going further we discuss how the notion of linking number generalizes to such circles.

**(3.3) Linking torsors.** Let $M$ be any 3-manifold. It is possible to associate to any two homology classes $c, d \in H_1(M, \mathbf{Z})$ a certain $\mathbf{Z}$-torsor $\langle c, d \rangle$ with the following properties:

1. There are natural isomorphisms

$$\langle c + c', d \rangle \simeq \langle c, d \rangle \otimes \langle c', d \rangle, \quad \langle c, d + d' \rangle \simeq \langle c, d \rangle \otimes \langle c, d' \rangle, \quad \langle d, c \rangle = \langle c, d \rangle,$$

   where $\otimes$ is the natural monoidal structure on the category of $\mathbf{Z}$-torsors

2. If $c = 0$, then $\langle c, d \rangle$ is canonically identified with $\mathbf{Z}$.

3. For any two non-intersecting oriented 1-dimensional submanifolds $C, D \imath M$ of homology classes $c$ and $d$ there is a naturally defined element $(C, D) \in \langle c, d \rangle$, and these elements satisfy the properties:

$$(C+C', D) = (C, D)+(C', D), \quad (C, D+D') = (C, D)+(C, D'), \quad (C, D) = -(D, C).$$

4. If $C, C'$ are two circles of the same homology class $c$, and $D$ is a circle of homology class $d$, then we have the equality of integers

$$(C, D) - (C', D) = (\sigma \cdot D),$$

   where the integer on the left is the difference of two elements of the $\mathbf{Z}$-torsor $\langle c, d \rangle$ and $\sigma$ is a 2-chain such that $\partial\sigma = C - C'$.

   In fact, one can define $\langle c, d \rangle$ to be generated by symbols $(C, D)$ with $C \in c$, $D \in d$ which are subject to relations from (4).

**(3.4) Class field theory.** Let $K$ be a number field containing $\mu_n$, the group of $n$th roots of unity, $A$ its ring of integers, $X = \mathrm{Spec}(A)$. Thus $X$ can be thought of as a scheme over the absolute field $\mathbf{F}_{1^n}$, see §1.

The part of the class field theory for $F$ related to cyclic degree $n$ extensions of $F$ can be reformulated in a way very similar to (3.3).

If $N$ is an ideal of $A$, and $L$ is a line bundle on $X$, we call a level $N$ structure on $L$ a trivialization of $L$ modulo $N$ plus a choice of a direction (called positive) in the completion $L_v$ for every real archimedean valuation $v$ of $K$. (Since we assume that $K$ contains $\mu_n$, real valuations will be not present if $n > 2$). If $f$ is a rational section of $L$, we say that $f \equiv 1 (\mathrm{mod}\ N)$, if the divisor of $f$ is relatively prime to $N$, the image of $f$ under the composite map $L \to L/NL \to A/N$ is equal to 1, and the image of $f$ in each $L_v$, where $v$ is a real valuation, is positive (lies in the distinguished half-line).

**3.0.8. Theorem.** *(3.5) Theorem. There exist:*

1. *An ideal $N_1A$ lying over $n$.*
2. *A rule which associates to every two line bundles $L, M$ on $X$ with level $N$ structure a $\mu_n$-torsor $\langle L, M\rangle$.*
3. *A rule which associates to every sections $l \in L$, $m \in M$ which are relatively prime and congruent to 1 modulo $N$ an element $(l,m)_n \in \mu_n$ with the following properties:*
4. *There are natural isomorphisms*

$$\langle L\otimes L', M\rangle \simeq \langle L, M\rangle\otimes\langle L', M\rangle, \quad \langle L, M\otimes M'\rangle \simeq \langle L, M\rangle\otimes\langle L, M'\rangle, \quad \langle M, L\rangle = \langle L, M\rangle,$$

5. *If $L = \mathcal{O}_X$ with trivial level $N$ structure, then $\langle L, M\rangle$ is canonically identified with $\mu_n$.*
6. *We have equalities $(l\otimes l', m)_n = (l,m)_n(l',m)_n$, and $(L, m\otimes m')_n = (l,m)_n(l,m')_n$.*
7. *(reciprocity law): We have $(l,m)_n = (m,l)_n$.*
8. *If $f$ is an element of $A$ congruent to 1 modulo $N$, then for any $M$ and any section $m \in M$, $m \equiv 1 (\mathrm{mod}\, N)$ relative prime to $f$, then the element $(f,m) \in \langle \mathcal{O}_X, M\rangle \simeq \mu_n$ is equal to the product of power residue symbols*

$$\prod_{v\in X}\left(\frac{f}{\mathbf{F}_v}\right)_n^{\mathrm{ord}_v(m)},$$

**3.0.9. Corollary.** *(3.6) Corollary. If $f, g \in A$ are two coprime elements congruent to 1 modulo $N$, then*

$$\prod_v \left(\frac{f}{\mathbf{F}_v}\right)_n^{\mathrm{ord}_v(g)} = \prod_v \left(\frac{g}{\mathbf{F}_v}\right)_n^{\mathrm{ord}_v(g)}.$$

This is the reciprocity law in the classical form. It can be used to recover the whole structure given by Theorem 3.5.

**(3.7) Line bundles with level structure.** We preserve the notation of n. 3.4. Denote by $\widetilde{\mathrm{Pic}}(X)$ the group of line bundles $L$ on $X$ with level $N$ structure. Denote by $K^*(N)$ the multiplicative group of $f \in K$ which are totally positive, relatively prime to $N$ and congruent to 1 modulo $N$. In Theorem 3.5, we are free to enlarge $N$. In the sequel we will always make the following assumption on $N$:

**3.0.10. Remark.** *(3.8) Assumption. For every $f \in K^*(N)$ we have the congruence*

$$\mathrm{Norm}_{K/\mathbf{Q}}(f) \equiv 1 (\mathrm{mod}\, n^2).$$

This will be true, for instance, if $N$ is divisible by (the lifting into $A$ of) $n^2$.

Let $\mathrm{Div}(X, N)$ be the group of divisors on $X$ relatively prime to $N$. Then, clearly,

$$\widetilde{\mathrm{Pic}}(X) = \mathrm{Div}(X,N)/\{\mathrm{div}(f),\ f \in K^*(N)\}.$$

As far as modulo $n$ phenomena are concerned, line (and vector) bundles on $X$ with level $N$ structure behave like bundles on a compact curve, even though $X$ itself is not compactified in any sense. For instance, the $\mu_n$-torsor $\langle L, M\rangle$ has the meaning of the direct image

$$\int_{X/\mathrm{Spec}(\mathbf{F}_{1^n})} c_1(L)c_1(M),$$

cf. [Deligne].

In addition, such line bundles have a notion of degree which takes values in $\mathbf{Z}/n$. It is defined as follows. Let us use the language of Sections 1 and 2, in particular, use linear algebra over the absolute field $F = \mathbf{F}_{1^n}$. For an ideal $D \imath A$ relatively prime to $N$ we set

$$\deg_n(D) = \dim_F(A/D) \pmod n.$$

**3.0.11. Proposition.** *(3.9) Proposition. (a) For two ideals $D_1, D_2 \imath A$ prime to $N$ we have $\deg_n(D_1D_2) \equiv \deg_n(D_1) + \deg_n(D_2) \pmod n$.*
*(b) If $f \in A \cap K^*(N)$, then $\deg_n(\mathrm{div}(f)) \equiv 0 \pmod n$.*

*Proof.* (a) Let $\Delta_i = \mathrm{Norm}_{K/\mathbf{Q}}(D_i)$. Then $\Delta_i$ is an ideal in $\mathbf{Z}$; let $d_i$ be its positive generator. Clearly $|A/D_i| = |\mathbf{Z}/\Delta_i| = d_i$. Thus $\deg_n(D_i) \equiv (d_i - 1)/n \pmod n$, and $\deg_n(D_1 + D_2) \equiv (d_1d_2 - 1)/n \pmod n$. Our statement amounts to the congruence

$$\frac{d_1d_2 - 1}{n} \equiv \frac{d_1 - 1}{n} + \frac{d_2 - 1}{n} \pmod n.$$

This can be rewritten as

$$(d_1 - 1)(d_2 - 1) \equiv 1 \pmod{n^2},$$

which is true by Assumption 3.8.

(b) Set, as before, $d$ to be the positive generator of $\mathrm{Norm}_{K/\mathbf{Q}}(f)$. Then $d \equiv 1 \pmod{n^2}$ by Assumption 3.8 and, on the other hand, $\deg_n(\mathrm{div}(f)) \equiv (d - 1)/n \pmod n$.

**3.0.12. Corollary.** *(3.10) Corollary. The map $\deg_n$ extends to a well defined homomorphism*

$$\deg_n : \widetilde{\mathrm{Pic}}(X) \to \mathbf{Z}/n.$$

*Proof.* Any element of $K^*(N)$ is a ratio of two elements of $A \cap K^*(N)$.

# 4 Compactified arithmetic curves.

As in the previous sections, we denote by $K$ a number field containing the group $mu = \mu_n$ of $n$th roots of 1, by $A$ its ring of integers and by $X$ the spectrum of $A$. We also choose an ideal $N$ in $A$ as in Section 3.

Although line bundles on $X$ with level $N$ structure possess the degree modulo $n$ and possess also the torsors $\langle L, M\rangle$, they do not possess finite-dimensional spaces of global sections or cohomology. In the geometric situation, however, an important step is the comparison of $\langle L, M\rangle$ with the determinant of the cohomology. So we introduce objects for which such determinants make sense.

**(4.1) Fundamental domains.** We will do some polyhedral constructions in the real vector space $K_{\mathbf{R}} = K \otimes \mathbf{R}$. In fact, tensoring with $\mathbf{R}$ is not really necessary, but it helps visualization.

Let us fix some terminology related to subsets of any real vector space $V$. We will call a (convex) polytope the convex hull of a finite set of points (so, in particular, this is a closed subset of $V$). A polytope $P$ has *faces*, which are (closed) subpolytopes in $P$. By a *polyhedral domain* we mean a subset in $V$ of the form $P - Q$ where $P$ is a polytope and $Q$ is the union of the interiors of some faces of $P$.

The ring $A$ is a lattice in $K_{\mathbf{R}}$, as is any projective $A$-submodule in $K$ of rank 1, for instance, any fractional ideal.

If $\Lambda$ is such a submodule, we will call a *fundamental polytope* for $\Lambda$ a convex polytope $P \in K_{\mathbf{R}}$ with the following property: for any two $\alpha, \beta \in \Lambda$ the intersection of the two translates $(P + \alpha) \cap (P + \beta)$ is a face of both of them. Of course, an obvious choice of a fundamental polytope would be a "cube" of the lattice, but we will need other choices (see below).

A *set of representatives* for $\Lambda$ is a polyhedral domain $B \in K_{\mathbf{R}}$ such that the composite projection $B \hookrightarrow K_{\mathbf{R}} \to K_{\mathbf{R}}/\Lambda$ is a bijection.

For example, when $K = \mathbf{Q}$, then $[0, 1]$ is a fundamental polytope for $\Lambda = \mathbf{Z}$, while $[0, 1)$ is a set of representatives.

**(4.2) Definition.** Let $B \imath K_{\mathbf{R}}$ be a $\mu$-invariant subset containing 0. We say that $B$ is a controlled domain, if there exist subsets $B_f, B_c \imath B$ and a fractional ideal $\Lambda \imath K$ with the following properties:

1. We have $B = B_f \cup B_c$ and $B_f \cap B_c = \emptyset$.
2. The set $B_f$ is a set of representatives for $\Lambda$.
3. For any $x \in B_c \cap K$ the ideal $(x : \Lambda) = \{\alpha \in A | \alpha x \in Lambda\}$ is divisible by any prime ideal in $A$ which divides $n$.

**(4.3) Example.** In the case $K = \mathbf{Q}$ the interval $[-1, 1]$ is a controlled domain. Indeed, we can take $B_f = [-1, 1)$ to be the half-open interval, $B_c = \{1\}$ and $\Lambda = 2\mathbf{Z}$.

In general, a controlled domain can be viewed as a replacement of this interval. The following fact will be proved in the next section.

**4.0.13. Theorem.** *(4.4) Theorem. If $n$ is any prime power, $n = p^t$ and $K$ is any number field containing $\mu_n$, then there exists a controlled domain in $K_{\mathbf{R}}$.*

**4.0.14. Definition.** *(4.5) Definition. A compact curve over $\mathbf{F}_{1^n}$ is a pair $\bar{X} = (X, B)$, where $X = \mathrm{Spec} A$ with $A$ the ring of integers of a number field $K$ containing $\mu_n$, and $B \imath K_{\mathbf{R}}$ is a controlled domain such that $\mu_n \imath B$.*

In the remainder of this section we assume that $X$ and $B$ are chosen.

**4.0.15. Definition.** *(4.6) Definition. A line bundle over $\bar{X}$ is a pair $L = (M_L, B_L)$ where $M_L$ is a projective $A$-module of rank 1 and $B_L \imath M_L \otimes \mathbf{R}$ is a subset which is $K$-linearly isomorphic to $B \imath K_{\mathbf{R}}$.*

We denote $H^0(\bar{X}, L) = M_L \cap B_L$. This is a vector space over $F = \mathbf{F}_{1^n}$. For any divisor $D$ on $X$ we denote by $\mathcal{O}(D) \imath K$ the corresponding fractional ideal and denote by $L(D)$

the pair formed by $M_L(D) = M_L \otimes \mathcal{O}(D)$ and the same set $B_L$. We will denote by $\mathcal{O}_{\bar{X}}$ or simply $\mathcal{O}$ the pair $(A, B)$.

Suppose that $D$ is positive, i.e., $\mathcal{O}(D)$ is an ideal in $A$. Then $M_L \imath M_L(D)$ and the quotient can be viewed as a skyscraper sheaf on $X$ with support on the support of $D$. We denote this sheaf by $L(D)|_D$, and think of the quotient group $M_L(D)/M_L$ as the space of global sections (over $X$ or $\bar{X}$) of this sheaf. Thus we have a sequence

$$0 \to H^0(\bar{X}, L) \to H^0(\bar{X}, L(D)) \to H^0(X, L(D)|_D \to 0 \tag{4.7}$$

When $D$ is prime to $n$, the sets in this sequence are $F$-vector spaces, where $F = \mathbf{F}_{1^n}$.

**4.0.16. Definition.** *(4.8) Definition. A line bundle $L$ over $\bar{X}$ is called acyclic (or is said to have no higher cohomology) if for any positive divisor $D$ in $A$ the sequence (4.7) is exact in the sense of Section 2.*

**4.0.17. Theorem.** *(4.9) Theorem. For any line bundle $L$ on $\bar{X}$ there is a positive divisor $D$ prime to $n$ such that for any divisor $D' \geq D$ prime to $n$ the line bundle $L(D)$ is acyclic.*

*Proof.*

**4.0.18. Corollary.** *(4.10) Corollary (Riemann-Roch modulo $n$). There exists a number $g = g(\bar{X}) \in \mathbf{Z}/n$ such that for $D \gg 0$ we have*

$$\dim H^0(\bar{X}, \mathcal{O}(D)) = \deg_n(D) + 1 - g \pmod{n}.$$

*Here the number $\deg_n(D)$ was defined in Section 3.*

**(2.7) Homotopy colimits.** Since we have defined only rudiments of a closed model structure, we can define homotopy limits and colimits only in special cases. Here is the situation we will be using.

Let $I$ be a finite category and $\Phi : I \to \mathcal{M}$ be a functor, i.e., a diagram of $F$-spaces of type $I$. Suppose that all the morphism $\Phi(\alpha)$, $\alpha \in \mathrm{Mor}(I)$ are embeddings. A system consisting of an object $C \in \mathcal{M}$ and morphisms $\beta_i : \Phi(i) \to C$ is called a homotopy colimit of $\Phi$, if:

1. $\beta(i)\Phi(\alpha) = \beta_j$ for every $\alpha : j \to i$ in $I$.
2. The natural morphism $\mathrm{colim}_I \Phi \to C$ existing by the property (1), is an equivalence.

**(2.8) Examples.** (a) A sequence (2.4.1) is exact if and only if $V''$ is a homotopy colimit of the diagram

(b): Exact (homotopy cocartesian) squares. A commutative square will be called exact, or homotopy cocartesian, if the maps in the diagram are embeddings and $V_{11}$ is a homotopy limit of this diagram.

In a similar way one defines exact cubes of an arbitrary dimension $d$. By definition, such a functor is a commutative diagram consisting of $f$-spaces $V_S$ where $S$ runs over subsets in $\{1, ..., d\}$, and there is a map $V_S \to V_T$ when $S \imath T$. A cube is called exact if in the subdiagram formed by the $V_S, S \neq \{1, ..., d\}$ all the maps are embeddings and $V_{\{1,...,d\}}$ is a homotopy limit of this diagram.

**4.0.19. Proposition.** *(2.9) Proposition. If $(V_S)$ is an exact $d$-dimensional cube, then we have a natural isomorphism*

$$\bigotimes \det(V_S)^{(-1)^{|S|}} \simeq \mu.$$

**(4.2) Example: the cyclotomic field.** Let $n = p^t$ where $p$ is a prime number, and let $K = \mathbf{Q}(\sqrt[n]{1})$ be the $n$th cyclotomic field. Let $A = \mathbf{Z}[\sqrt[n]{1}]$ be its ring of integers. The only ideal in $A$ lying over $p$ is $\Lambda = (1-\zeta)$ where $\zeta$ is any primitive root of 1. Consider the set

$$P = \left\{ \sum_{\epsilon \in \mu_n} a_\epsilon \epsilon \right\}, \quad a_\epsilon \in [0,1].$$

This is clearly a polytope, since it is the image of the cube $[0,1]^{\mu_n}$ under the natural projection to $K_{\mathbf{R}}$.

**4.0.20. Proposition.** *(4.2.1) Proposition. $P$ is a fundamental polytope for $\Lambda$.*

Proof. Fix a primitive root $\zeta \in \mu_n$. An $\mathbf{R}$-basis of $K_{\mathbf{R}}$ and a $\mathbf{Z}$-basis of $A$ is provided by the powers $\zeta^i$, where $1 \leq i \leq n$ and $(i,n) = 1$. Thus the cube

$$Q = \left\{ \sum_{(i,n)=1} a_i \zeta^i \right\}, \quad a_i \in [0,1]$$

is a fundamental polytope for $A$. Now $P$ is the union of $n$ rotated cubes $\zeta^j Q$ where $0 \leq j \leq n-1$, and the intersection of any two of these cubes is a face of both of them. This can be verified in a straightforward way.