

Characteristic 1, entropy and the absolute point

Alain Connes and Caterina Consani

ABSTRACT. We show that the mathematical meaning of working in characteristic one is directly connected to the fields of idempotent analysis and tropical algebraic geometry and we relate this idea to the notion of the absolute point $\text{Spec } \mathbb{F}_1$. After introducing the notion of “perfect” semi-ring of characteristic one, we explain how to adapt the construction of the Witt ring in characteristic $p > 1$ to the limit case of characteristic one. This construction also unveils an interesting connection with entropy and thermodynamics, while shedding a new light on the classical Witt construction itself. We simplify our earlier construction of the geometric realization of an \mathbb{F}_1 -scheme and extend our earlier computations of the zeta function to cover the case of \mathbb{F}_1 -schemes with torsion. Then, we show that the study of the additive structures on monoids provides a natural map $M \mapsto A(M)$ from monoids to sets which comes close to fulfill the requirements for the hypothetical curve $\overline{\text{Spec } \mathbb{Z}}$ over the absolute point $\text{Spec } \mathbb{F}_1$. Finally, we test the computation of the zeta function on elliptic curves over the rational numbers.

Contents

1. Introduction
2. Working in characteristic 1: Entropy and Witt construction
 - 2.1 Additive structure
 - 2.2 Characteristic $p = 2$
 - 2.3 Characteristic $p = 1$ and idempotent analysis
 - 2.4 Witt ring in characteristic $p = 1$ and entropy
 - 2.5 The Witt ring in characteristic $p > 1$ revisited
 - 2.6 \mathbb{B} , \mathbb{F}_1 and the “absolute point”
3. The functorial approach
 - 3.1 Schemes as locally representable \mathbb{Z} -functors: a review
 - 3.2 Monoids: the category \mathfrak{Mo}
 - 3.3 Geometric monoidal spaces
 - 3.4 \mathfrak{Mo} -schemes
4. \mathbb{F}_1 -schemes and their zeta functions
 - 4.1 Torsion free Noetherian \mathbb{F}_1 -schemes
 - 4.2 Extension of the counting functions in the torsion case

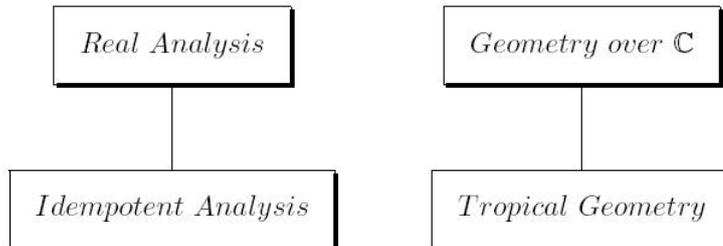
1991 *Mathematics Subject Classification*. Primary 14A15, 14G10; Secondary 11G40.

The authors are partially supported by the NSF grant DMS-FRG-0652164. The first author thanks C. Breuil for pointing out the reference to M. Krasner [Kr]. Both authors acknowledge the paper [Le] of Paul Lescot, that brings up the role of the idempotent semi-field \mathbb{B}

- 4.3 An integral formula for the logarithmic derivative of $\zeta_N(s)$
- 4.4 Analyticity of the integrals
- 4.5 Zeta function of Noetherian \mathbb{F}_1 -schemes
- 5. Beyond \mathbb{F}_1 -schemes
 - 5.1 Modified zeta function
 - 5.2 Modified zeta function and $\overline{\text{Spec}(\mathbb{Z})}$
 - 5.3 Elliptic curves
- 6. Appendix: Primes of bad reduction of an elliptic curve
- References

1. INTRODUCTION

The main goal of this article is to explore the mathematical meaning of working in characteristic one and to relate this idea with the notion of the absolute point $\text{Spec } \mathbb{F}_1$. In the first part of the paper, we explain that an already well established branch of mathematics supplies a satisfactory answer to the question of the meaning of mathematics in characteristic one. Our starting point is the investigation of the structure of fields of positive characteristic $p > 1$, in the degenerate case $p = 1$. The outcome is that this limit case is directly connected to the fields of idempotent analysis (cf. [KM]) and tropical algebraic geometry (cf. [IMS], [Ga]). In parallel with the development of classical mathematics over fields, its “shadow” idempotent version appears in characteristic one



To perform idempotent or tropical mathematics means to perform analysis and/or geometry after replacing the Archimedean local field \mathbb{R} with the locally compact *semi-field* \mathbb{R}_+^{\max} . This latter structure is defined as the locally compact space $\mathbb{R}_+ = [0, \infty)$ endowed with the ordinary product and a new idempotent addition $x \uplus y = \max\{x, y\}$ that appears as the limit case of the conjugates of ordinary addition by the map $x \mapsto x^h$, when $h \rightarrow 0$. The semi-field \mathbb{R}_+^{\max} is trivially isomorphic to the “schedule algebra” (or “max-plus algebra”) $(\mathbb{R} \cup \{-\infty\}, \max, +)$, by means of the map $x \mapsto \log x$. The reason why we prefer to work with \mathbb{R}_+^{\max} in this paper (rather than with the “max-plus” algebra) is that the structure of \mathbb{R}_+^{\max} makes the role of the “Frobenius” more transparent. On a field of characteristic $p > 1$, the arithmetic Frobenius is given by the “additive” map $x \mapsto x^p$. On \mathbb{R}_+^{\max} , the Frobenius flow has the analogous description given by the action $x \mapsto x^\lambda$ ($\lambda \in \mathbb{R}_+^*$) which is also “additive” since it is monotonic and hence compatible with $\max\{x, y\}$.

It is well known that the classification of local fields of positive characteristic reduces to the classification of finite fields of positive characteristic. A local field

of characteristic $p > 1$ is isomorphic to the field $\mathbb{F}_q((T))$ of formal power series with finite order pole at 0, over a finite extension \mathbb{F}_q of \mathbb{F}_p . There is a strong relation between the p -adic field \mathbb{Q}_p of characteristic zero and the field $\mathbb{F}_p((T))$ of characteristic p . The connection is described by the Ax-Kochen theorem [AK] (that depends upon the continuum hypothesis) which states the following isomorphism of ultraproducts

$$(1) \quad \prod_{\omega} \mathbb{Q}_p \sim \prod_{\omega} \mathbb{F}_p((T))$$

for any non-trivial ultrafilter ω on the integers.

The local field $\mathbb{F}_p((T))$ is the unique local field of characteristic p with residue field \mathbb{F}_p . Then, the Ax-Kochen theorem essentially states that, for sufficiently large p , the field \mathbb{Q}_p resembles its simplification $\mathbb{F}_p((T))$, in which addition forgets the carry over rule in the description of a p -adic number as a power series in p^n . The process that allows one to view $\mathbb{F}_p((T))$ as a limit of fields of characteristic zero obtained by adjoining roots of p to the p -adic field \mathbb{Q}_p was described in [Kr]. The role of the Witt vectors is that to define a process going backwards from the simplified rule of $\mathbb{F}_p((T))$ to the original algebraic law holding for p -adic numbers.

In characteristic one, the role of the local field $\mathbb{F}_p((T))$ is played by the local semi-field \mathbb{R}_+^{\max} .

Characteristic 0	$\mathbb{Q}_p, p > 1$	Archimedean \mathbb{R}
Characteristic $\neq 0$	$\mathbb{F}_p((T))$	$p = 1, \mathbb{R}_+^{\max}$

The process that allows one to view \mathbb{R}_+^{\max} as a result of a deformation of the usual algebraic structure on real numbers is known as “dequantization” and can be described as a semi-classical limit in the following way. First of all note that, for $\mathbb{R} \ni h > 0$ one has

$$h \ln(e^{w_1/h} + e^{w_2/h}) \rightarrow \max\{w_1, w_2\} \quad \text{as } h \rightarrow 0.$$

Thus, the natural map

$$D_h : \mathbb{R}_+ \rightarrow \mathbb{R}_+ \quad D_h(u) = u^h$$

satisfies the equation

$$\lim_{h \rightarrow 0} D_h(D_h^{-1}(u_1) + D_h^{-1}(u_2)) = \max\{u_1, u_2\}.$$

In the limit $h \rightarrow 0$, the usual algebraic rules on \mathbb{R}_+ deform to become those of \mathbb{R}_+^{\max} . Moreover, in the limit one also obtains a one-parameter group of automorphisms of \mathbb{R}_+^{\max}

$$\vartheta_{\lambda}(u) = u^{\lambda}, \quad \lambda \in \mathbb{R}_+^{\max}$$

which corresponds to the arithmetic Frobenius in characteristic $p > 1$.

After introducing the notion of “perfect” semi-ring of characteristic 1 (§ 2.3.3), our first main result (*cf.* § 2.4) states that one can adapt the construction of the Witt ring to this limit case of characteristic one. This fact also unveils an interesting deep connection with entropy and thermodynamics, while shedding a new light on the classical Witt construction itself.

Our starting point is the basic physics formula expressing the free energy in terms of entropy from a variational principle. In its simplest mathematical form, it states that

$$(2) \quad \log(e^a + e^b) = \sup_{x \in [0,1]} S(x) + xa + (1-x)b$$

where $S(x) = -x \log x - (1-x) \log(1-x)$ is the entropy of the partition of 1 as $1 = x + (1-x)$.

In Theorem 2.20, we explain how formula (2) allows one to reconstruct addition from its characteristic one degenerate limit. This process has an analogue in the construction of the Witt ring which reconstructs the p -adic numbers from their degenerate characteristic p limit $\mathbb{F}_p((t))$. Interestingly, this result also leads to a reformulation of the Witt construction in complete analogy with the case of characteristic one (*cf.* Proposition 2.23). These developments, jointly with the existing body of results in idempotent analysis and tropical algebraic geometry supply a strong and motivated expectation on the existence of a meaningful notion of “local” mathematics in characteristic one. In fact, they also suggest the existence of a notion of “global” mathematics in characteristic one, pointing out to the possibility that the discrete, co-compact embedding of a global field into a locally compact semi-simple non-discrete ring may have an extended version for semi-fields in semi-rings of characteristic 1.

The second part of the paper reconsiders the study of the “absolute point” initiated in [KS]. It is important to explain the distinction between $\text{Spec } \mathbb{B}$, where \mathbb{B} is the initial object in the category of semi-rings of characteristic 1 (*cf.* [Go]) and the sought for “absolute point” which has been traditionally denoted by $\text{Spec } \mathbb{F}_1$. It is generally expected that $\text{Spec } \mathbb{F}_1$ sits under $\text{Spec } \mathbb{Z}$ in the sense of [TV]

$$(3) \quad \begin{array}{ccc} \text{Spec } \mathbb{Z} & & \text{Spec } \mathbb{B} \\ \downarrow & \swarrow & \\ \text{Spec } \mathbb{F}_1 & & \end{array}$$

In order to reasonably fulfill the property to be “absolute”, $\text{Spec } \mathbb{F}_1$ should also sit under $\text{Spec } \mathbb{B}$. Here, it is important to stress the fact that $\text{Spec } \mathbb{B}$ does not qualify to be the “absolute point”, since there is no morphism from \mathbb{B} to \mathbb{Z} . We refer to [Le] for an interesting approach to algebraic geometry over \mathbb{B} .

Theorem 2.1 singles out the conditions on a bijection s of the set $\mathbb{K} = H \cup \{0\}$ onto itself ($H =$ abelian group), so that s becomes the addition of 1 in a field whose multiplicative structure is that of the monoid \mathbb{K} . These conditions are:

- s commutes with its conjugates for the action of H by multiplication on the monoid \mathbb{K} .
- $s(0) \neq 0$.

The degenerate case of characteristic one appears when one drops the requirement that s is a bijection and replaces it with the idempotent condition $s \circ s = s$, so that s becomes a retraction onto its range. The degenerate structure of \mathbb{F}_1 arises when one drops the condition $s(0) \neq 0$. The trivial solution given by the identity map $s = \text{id}$, then yields such degenerate structure in which, except for the addition of 0, the addition is indeterminate as $0/0$. This fact simply means that, except for 0, one forgets completely the additive structure. This outcome agrees with the point of view developed in the earlier papers [D1], [D2] and [TV].

In [CC2], we have introduced a geometric theory of algebraic schemes (of finite type) over \mathbb{F}_1 which unifies an earlier construction developed in [So] with the approach initiated in our paper [CC1]. This theory is reconsidered and fully developed in the present article. The geometric objects covered by our construction are rational varieties which admit a suitable cell decomposition in toric varieties. Typical examples include Chevalley groups schemes, projective spaces etc. Our initial interest for an algebraic geometry over \mathbb{F}_1 originated with the study of Chevalley schemes as (affine) algebraic varieties over \mathbb{F}_1 . Incidentally, we note that these structures are not toric varieties in general and this shows that the point of view of [D1] and [D2] is a bit too restrictive. Theorem 2.2 of [LL] gives a precise characterization of the schemes studied by our theory in terms of general torifications. This result also points out to a deep relation with tropical geometry that we believe is worth to be explored in details.

On the other hand, one should not forget the fact that the class of varieties covered even by this extended definition of schemes over \mathbb{F}_1 is still extremely restrictive and, due to the rationality requirement, excludes curves of positive genus. Thus, at first sight, one seems still quite far from the real objective which is that to describe the “curve” (of infinite genus) $C = \overline{\text{Spec } \mathbb{Z}}$ over \mathbb{F}_1 , whose zeta function $\zeta_C(s)$ is the complete Riemann zeta function. However, a thorough development of the theory of schemes over \mathbb{F}_1 as initiated in [CC2] shows that any such a scheme X is described (among other data) by a covariant functor \underline{X} from the category \mathfrak{Mo} of commutative monoids to sets. The functor \underline{X} associates to an object M of \mathfrak{Mo} the set of points of X which are “defined over M ”. The adèle class space of a global field \mathbb{K} is a particularly important example of a monoid and this relevant description allows one to evaluate any scheme over \mathbb{F}_1 on such monoid. In [CC2], we have shown that using the simplest example of a scheme over \mathbb{F}_1 , namely the curve $\mathbb{P}_{\mathbb{F}_1}^1$, one constructs a perfect set-up to understand conceptually the spectral realization of the zeros of the Riemann zeta function (and more generally of Hecke L -functions over \mathbb{K}). The spectral realization appears naturally from the (sheaf) cohomology $H^1(\mathbb{P}_{\mathbb{F}_1}^1, \Omega)$ of very simply defined sheaves Ω on the geometric realization of the scheme $\mathbb{P}_{\mathbb{F}_1}^1$. Such sheaves are obtained from the functions on the points of $\mathbb{P}_{\mathbb{F}_1}^1$ defined over the monoid M of adèle classes. Moreover, the computation of the cohomology $H^0(\mathbb{P}_{\mathbb{F}_1}^1, \Omega)$ provides a description of the graph of the Fourier transform which thus appears conceptually in this picture.

The above construction makes use of a peculiar property of the geometric realization of an \mathfrak{Mo} -functor which has no analogue for \mathbb{Z} -schemes (or more generally for \mathbb{Z} -functors). Indeed, the geometric realization of an \mathfrak{Mo} -functor \underline{X} coincides, as a set, with the set of points which are defined over \mathbb{F}_1 , *i.e.* with the value $\underline{X}(\mathbb{F}_1)$ of the functor on the most trivial monoid. After a thorough development of the general theory of \mathfrak{Mo} -schemes (an essential ingredient in the finer notion of an \mathbb{F}_1 -scheme), we investigate in full details their geometric realization, which turn out to

be schemes in the sense of [D1] and [D2]. Then, we show that both the topology and the structure sheaf of an \mathbb{F}_1 -scheme can be obtained in a natural manner on the set $\underline{X}(\mathbb{F}_1)$ of its \mathbb{F}_1 -points.

At the beginning of §4, we shortly recall our construction of an \mathbb{F}_1 -scheme and the description of the associated zeta function, under the (local) condition of no-torsion on the scheme (*cf.* [CC2]). We then remove this hypothesis and compute, in particular, the zeta function of the extensions \mathbb{F}_{1^n} of \mathbb{F}_1 . The general result is stated in Theorem 4.13 and in Corollary 4.14 which present a description of the zeta function of a Noetherian \mathbb{F}_1 -scheme X as the product

$$\zeta(X, s) = e^{h(s)} \prod_{j=0}^n (s-j)^{\alpha_j}$$

of the exponential of an entire function by a finite product of fractional powers of simple monomials. The exponents α_j are rational numbers defined explicitly, in terms of the structure sheaf \mathcal{O}_X in monoids, as follows

$$\alpha_j = (-1)^{j+1} \sum_{x \in X} (-1)^{n(x)} \binom{n(x)}{j} \sum_d \frac{1}{d} \nu(d, \mathcal{O}_{X,x}^\times)$$

where $\nu(d, \mathcal{O}_{X,x}^\times)$ is the number of injective homomorphisms from $\mathbb{Z}/d\mathbb{Z}$ to the group $\mathcal{O}_{X,x}^\times$ of invertible elements of the monoid $\mathcal{O}_{X,x}$. In order to establish this result, we need to study the case of a counting function

$$(4) \quad \# X(\mathbb{F}_{1^n}) = N(n+1)$$

no longer polynomial in the integer $n \in \mathbb{N}$. In [CC2] we showed that the limit formula that was used in [So] to define the zeta function of an algebraic variety over \mathbb{F}_1 , can be replaced by an equivalent integral formula which determines the equation

$$(5) \quad \frac{\partial_s \zeta_N(s)}{\zeta_N(s)} = - \int_1^\infty N(u) u^{-s-1} du$$

describing the logarithmic derivative of the zeta function $\zeta_N(s)$ associated to the counting function $N(q)$. We use this result to treat the case of the counting function of a Noetherian \mathbb{F}_1 -scheme and Nevanlinna theory to uniquely extend the counting function $N(n)$ to arbitrary complex arguments $z \in \mathbb{C}$ and finally we compute the corresponding integrals.

In § 5 we show that the replacement, in formula (5), of the integral by the discrete sum

$$\frac{\partial_s \zeta_N^{\text{disc}}(s)}{\zeta_N^{\text{disc}}(s)} = - \sum_1^\infty N(u) u^{-s-1}$$

only modifies the zeta function of a Noetherian \mathbb{F}_1 -scheme by an exponential factor of an entire function. This observation leads to the Definition 5.2 of a modified zeta function over \mathbb{F}_1 whose main advantage is that of being applicable to the case of an arbitrary counting function with polynomial growth.

In [CC2], we determined the counting distribution $N(q)$, defined for $q \in [1, \infty)$, such that the zeta function (5) gives the complete Riemann zeta function $\zeta_{\mathbb{Q}}(s) =$

$\pi^{-s/2}\Gamma(s/2)\zeta(s)$: *i.e.* such that the following equation holds

$$(6) \quad \frac{\partial_s \zeta_{\mathbb{Q}}(s)}{\zeta_{\mathbb{Q}}(s)} = - \int_1^{\infty} N(u) u^{-s} d^*u.$$

In § 5.2, we use the modified version of zeta function (as described above) to study a simplified form of (14) *i.e.*

$$\frac{\partial_s \zeta(s)}{\zeta(s)} = - \sum_1^{\infty} N(n) n^{-s-1}.$$

This gives, for the counting function $N(n)$, the formula $N(n) = n\Lambda(n)$, where $\Lambda(n)$ is the von-Mangoldt function¹. Using the relation (4), this shows that, for a suitably extended notion of “scheme over \mathbb{F}_1 ”, the hypothetical “curve” $X = \overline{\text{Spec } \mathbb{Z}}$ should fulfill the following requirement

$$(7) \quad \#(X(\mathbb{F}_{1^n})) = \begin{cases} 0, & \text{if } n+1 \text{ is not a prime power} \\ (n+1) \log p, & \text{if } n = p^\ell - 1, p \text{ prime.} \end{cases}$$

This expression is neither functorial nor integer valued, but by reconsidering the theory of additive structures previously developed in §2.1, we show in Corollary 5.4 that the natural construction which assigns to an object M of $\mathfrak{M}\mathfrak{o}$ the set $A(M)$ of maps $s : M \rightarrow M$ such that

- s commutes with its conjugates by multiplication by elements of M^\times
- $s(0) = 1$

comes close to solving the requirements of (7) since it gives (for $n > 1$, φ the Euler totient function)

$$\#(A(\mathbb{F}_{1^n})) = \begin{cases} 0, & \text{if } n+1 \text{ is not a prime power} \\ \frac{\varphi(n)}{\log(n+1)} \log p, & \text{if } n = p^\ell - 1, p \text{ prime.} \end{cases}$$

In § 5.3 we experiment with elliptic curves E over \mathbb{Q} , by computing the zeta function associated to a *specific* counting function on E . The specific function $N(q, E)$ is uniquely determined by the following two conditions:

- For any prime power $q = p^\ell$, the value of $N(q, E)$ is the number² of points of the reduction of E modulo p in the finite field \mathbb{F}_q .
- The function $t(n)$ occurring in the equation $N(n, E) = n + 1 - t(n)$ is weakly multiplicative.

Then, we prove that the obtained zeta function $\zeta_N^{\text{disc}}(s)$ of E fulfills the equation

$$\frac{\partial_s \zeta_N^{\text{disc}}(s)}{\zeta_N^{\text{disc}}(s)} = -\zeta(s+1) - \zeta(s) + \frac{L(s+1, E)}{\zeta(2s+1)M(s+1)}$$

where $L(s, E)$ is the L -function of the elliptic curve, $\zeta(s)$ is the Riemann zeta function and

$$M(s) = \prod_{p \in S} (1 - p^{1-2s})$$

¹with value $\log p$ for powers p^ℓ of primes and zero otherwise

²including the singular point

is a finite product of local factors indexed on the set S of primes at which E has bad reduction. In Example 5.8 we exhibit the singularities of $\zeta_E(s)$ in a concrete case.

2. WORKING IN CHARACTERISTIC 1: ENTROPY AND WITT CONSTRUCTION

In this section we investigate the degeneration of the structure of fields of prime positive characteristic p , in the limit case $p = 1$. A thorough investigation of this process and the algebraic structures of characteristic one, points out to a very interesting link between the fields of idempotent analysis [KM] and tropical geometry [IMS], with the algebraic structure of a degenerate geometry (of characteristic one) obtained as the limit case of geometries over finite fields \mathbb{F}_p . Our main result is that of adapting the construction of the Witt ring to this limit case of characteristic $p = 1$ while unraveling also a deep connection of the Witt construction with entropy and thermodynamics. Remarkably, we find that this process sheds also a new light on the classical Witt construction itself.

2.1 Additive structure.

The multiplicative structure of a field \mathbb{K} is obtained by adjoining an absorbing element 0 to its multiplicative group $H = \mathbb{K}^\times$. Our goal here, is to understand the additional structure on the multiplicative monoid $H \cup \{0\}$ (the multiplicative monoid underlying \mathbb{K}) corresponding to the addition. For simplicity, we shall still denote by \mathbb{K} such monoid.

We first notice that to define an additive structure on \mathbb{K} it is enough to know how to define the operation

$$(8) \quad s_o : \mathbb{K} \rightarrow \mathbb{K} \quad s_o(x) = x + 1 \quad \forall x \in \mathbb{K}$$

since then the definition of the addition follows by setting

$$(9) \quad + : \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K} \quad x + y = x s_o(yx^{-1}) \quad \forall x, y \in \mathbb{K}, x \neq 0.$$

Moreover, with this definition given, one has (using the commutativity of the monoid \mathbb{K})

$$x(y + z) = x y s_o(zy^{-1}) = x y s_o(xzy^{-1}x^{-1}) = x y s_o(xz(xy)^{-1}).$$

Thus, the distributivity follows automatically

$$x(y + z) = xy + xz \quad \forall x, y, z \in \mathbb{K}.$$

The following result characterizes the bijections s of the monoid \mathbb{K} onto itself such that, when enriched by the addition law (9), the monoid \mathbb{K} becomes a field.

THEOREM 2.1. *Let H be an abelian group. Let s be a bijection of the set $\mathbb{K} = H \cup \{0\}$ onto itself that commutes with its conjugates for the action of H by multiplication on the monoid \mathbb{K} . Then, if $s(0) \neq 0$, the operation*

$$(10) \quad x + y := \begin{cases} y, & \text{if } x = 0 \\ s(0)^{-1} x s(s(0) y x^{-1}), & \text{if } x \neq 0 \end{cases}$$

defines a commutative group law on \mathbb{K} . With this law as addition, the monoid \mathbb{K} becomes a commutative field. Moreover the field \mathbb{K} is of characteristic p if and only if

$$s^p = s \circ s \circ \dots \circ s = id$$

PROOF. By replacing s with its conjugate, one can assume, since $s(0) \neq 0$, that $s(0) = 1$. Let $A(x, y) = x + y$ be given as in (10). By definition, one has $A(0, y) = y$. For $x \neq 0$, $A(x, 0) = xs(0) = x$. Thus 0 is a neutral element for \mathbb{K} . The commutation of s with its conjugate for the action of H on \mathbb{K} by multiplication with the element $x \neq 0$ means that

$$(11) \quad s(xs(yx^{-1})) = xs(s(y)x^{-1}) \quad \forall y \in \mathbb{K}.$$

Taking $y = 0$ (and using $s(0) = 1$), the above equation gives

$$(12) \quad s(x) = xs(x^{-1}) \quad \forall x \neq 0.$$

Assume now that $x \neq 0$ and $y \neq 0$, then from (12) one gets

$$A(x, y) = xs(yx^{-1}) = x(yx^{-1})s(xy^{-1}) = ys(xy^{-1}) = A(y, x).$$

Thus A is a commutative law of composition. The associativity of A follows from the commutation of left and right addition which is a consequence of the commutation of the conjugates of s . More precisely, assuming first that all elements involved are non zero, one has

$$\begin{aligned} A(A(x, y), z) &= A(xs(yx^{-1}), z) = A(z, xs(yx^{-1})) = zs(xs(yx^{-1})z^{-1}) \\ &= zs(xz^{-1}s(yx^{-1})). \end{aligned}$$

Using (11) one obtains

$$zs(xz^{-1}s(yx^{-1})) = zxz^{-1}s(s(yz^{-1})zx^{-1}) = xs(s(yz^{-1})zx^{-1})$$

$$A(x, A(y, z)) = A(x, s(yz^{-1})z) = xs(s(yz^{-1})zx^{-1})$$

which yields the required equality. It remains to verify a few special cases. If either x or y or z is zero, the equality follows since 0 is a neutral element. Since we never had to divide by $s(a)$, the above argument applies without restriction. Finally let $\theta = s^{-1}(0)$, then for any $x \neq 0$ one has $A(x, \theta x) = xs(\theta) = 0$. This shows that θx is the inverse of x for the law A . We have thus proven that this law defines an abelian group structure on \mathbb{K} .

Finally, we claim that the distributive law holds. This means that for any $a \in \mathbb{K}$ one has

$$A(ax, ay) = aA(x, y), \quad \forall x, y \in \mathbb{K}.$$

We can assume that all elements involved are $\neq 0$. Then, one obtains

$$A(ax, ay) = axs(ay(ax)^{-1}) = axs(yx^{-1}) = aA(x, y).$$

This suffices to show that \mathbb{K} is a field. □

As a corollary, one obtains the following general uniqueness result

COROLLARY 2.2. *Let H be a finite commutative group and let s_j ($j = 1, 2$) be two bijections of the monoid $\mathbb{K} = H \cup \{0\}$ such that $s_j(0) \neq 0$ and s_j commutes with its conjugates as in Theorem 2.1. Then H is a cyclic group of order $m = p^\ell - 1$ for some prime p and there exists a group automorphism $\alpha \in \text{Aut}(H)$ and an element $g \in H$ such that*

$$s_2 = T \circ s_1 \circ T^{-1}, \quad T(x) = g\alpha(x), \quad \forall x \in H, \quad T(0) = 0.$$

PROOF. By replacing s_j with its conjugate by $g_j = s_j(0)$, one can assume that $s_j(0) = 1$. Each s_j defines on the monoid $\mathbb{K} = H \cup \{0\}$ an additive structure which, in view of Theorem 2.1, turns this set into a finite field \mathbb{F}_q , for some prime power $q = p^\ell$. If m is the order of H , then $m = p^\ell - 1 = q - 1$ and H is the cyclic group of order m . The field \mathbb{F}_q with $q = p^\ell$ elements is unique up to isomorphism. Thus there exists a bijection α from \mathbb{K} to itself, which is an isomorphism with respect to the multiplicative and the additive structures given by s_j . This map sends 0 to 0 and 1 to 1, thus transforms the addition of 1, for the first structure, into the addition of 1 for the second one. Since this map also respects the multiplication, it is necessarily given by a group automorphism $\alpha \in \text{Aut}(H)$. \square

2.2 Characteristic $p = 2$.

We apply the above discussion to a concrete case. In this subsection we work in characteristic two, thus we consider an algebraic closure $\overline{\mathbb{F}}_2$. It is well known that the multiplicative group $(\overline{\mathbb{F}}_2)^\times$ is *non-canonically* isomorphic to the group \mathbb{G}^{odd} of roots of unity in \mathbb{C} of odd order. We consider the monoid $\mathbb{K} = \mathbb{G}^{\text{odd}} \cup \{0\}$. The product between non zero elements in \mathbb{K} is the same as in \mathbb{G}^{odd} and 0 is an absorbing element (*i.e.* $0 \cdot x = x \cdot 0 = 0, \forall x \in \mathbb{K}$). For each positive integer ℓ , there is a unique subgroup $\mu_{(2^\ell - 1)} < \mathbb{G}^{\text{odd}}$ made by the roots of 1 of order $2^\ell - 1$; this is also the subgroup of the invertible elements of the finite subfield $\mathbb{F}_{2^\ell} \subset \overline{\mathbb{F}}_2$. We know how to multiply two elements in \mathbb{K} but we do not know how to add them.

Since we work in characteristic two, the transformation s_o of (8) given by the addition of 1 fulfills $s_o \circ s_o = \text{id}$, *i.e.* s_o is an involution.

Let Σ be the set of *involutions* s of \mathbb{K} which commute with all their conjugates by rotations with elements of \mathbb{G}^{odd} , and which fulfill the condition $s(0) = 1$. Thus an element $s \in \Sigma$ is an involution such that $s(0) = 1$ and it satisfies the identity $s \circ (R \circ s \circ R^{-1}) = (R \circ s \circ R^{-1}) \circ s$, for any rotation $R : \mathbb{K} \rightarrow \mathbb{K}$.

PROPOSITION 2.3. *For any choice of a group isomorphism*

$$(13) \quad j : (\overline{\mathbb{F}}_2)^\times \xrightarrow{\sim} \mathbb{G}^{\text{odd}},$$

the following map defines an element $s \in \Sigma$

$$s : \mathbb{K} \rightarrow \mathbb{K} \quad s(x) = \begin{cases} j(j^{-1}(x) + 1), & \text{if } x \neq 1 \\ 0, & \text{if } x = 1. \end{cases}$$

Moreover, two pairs $(\overline{\mathbb{F}}_2, j)$ are isomorphic if and only if the associated symmetries $s \in \Sigma$ are the same. Each element of Σ corresponds to a uniquely associated pair $(\overline{\mathbb{F}}_2, j)$.

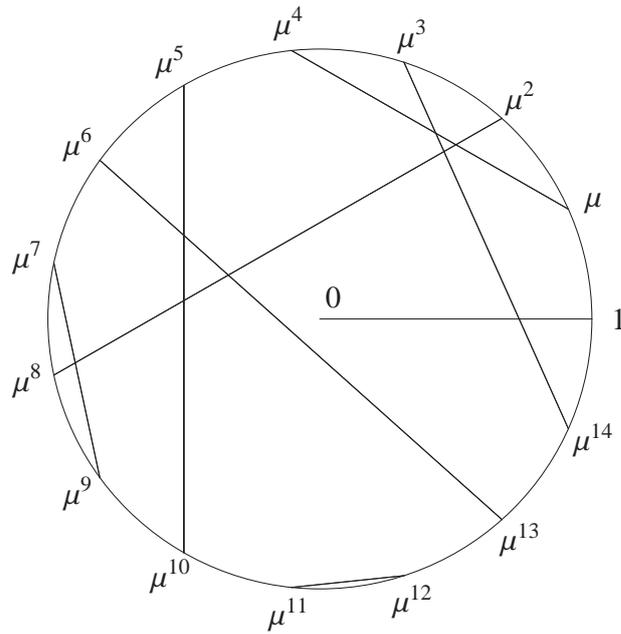


Fig. 1. The symmetry s for \mathbb{F}_{16} represented by the graph G_s with vertices the 15-th roots of 1 and edges $(x, s(x))$.

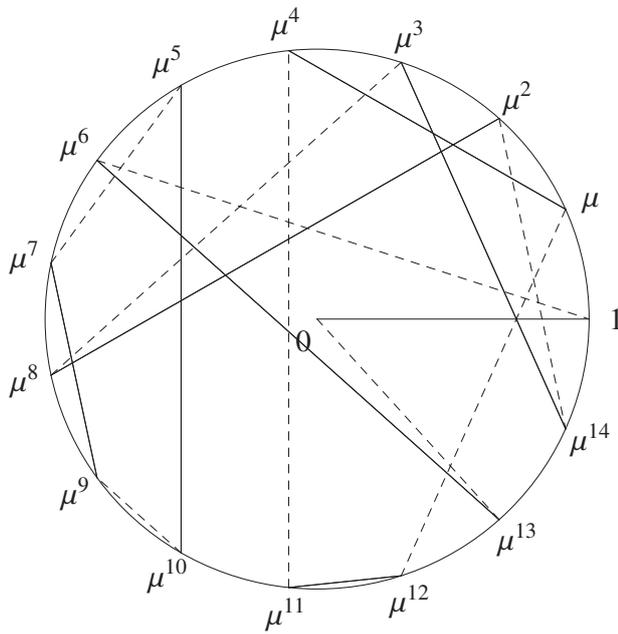


Fig. 2. The commutativity of s with its conjugates by rotations $R \circ s \circ R^{-1}$ means that the union of the graph G_s with a rotated graph $R(G_s)$ (dashed) is a union of quadrilaterals.

PROOF. We first show that $s \in \Sigma$. Since $\text{char}(\overline{\mathbb{F}}_2) = 2$, s is an involution. To show that s commutes with its conjugates by rotations with elements of \mathbb{G}^{odd} , it is enough to check that s commutes with its conjugate by $j(y)$, $y \in (\overline{\mathbb{F}}_2)^\times$. One first uses the distributivity of the addition to see that

$$j(y)s(xj(y)^{-1}) = j(y)j(j^{-1}(xj(y)^{-1})+1) = j(y(j^{-1}(xj(y)^{-1})+1)) = j(j^{-1}(x)+y).$$

The commutativity of the additive structure on $\overline{\mathbb{F}}_2$ gives the required commutation. We now prove the second statement. Given two pairs (\mathbb{K}_i, j_i) ($i = 1, 2$) as in (13), and an isomorphism $\theta : \mathbb{K}_1 \rightarrow \mathbb{K}_2$ such that $j_2 \circ \theta = j_1$, one has

$$s_2(x) = j_2(j_2^{-1}(x) + 1) = j_1 \circ \theta^{-1}(\theta(j_1^{-1}(x)) + 1) = s_1(x)$$

since $\theta(1) = 1$. □

Let $s \in \Sigma$ be an involution of \mathbb{K} satisfying the required properties. We introduce the following operation in \mathbb{K}

$$(14) \quad x + y = \begin{cases} y, & \text{if } x = 0 \\ xs(yx^{-1}), & \text{if } x \neq 0. \end{cases}$$

Then, it follows as a corollary of Theorem 2.1 that the above operation (14) defines a commutative group law on $\mathbb{K} = \mathbb{G}^{\text{odd}} \cup \{0\} \subset \mathbb{C}$. This law and the induced multiplication, turn \mathbb{K} into a field of characteristic 2.

REMARK 2.4. We avoid to refer to $\overline{\mathbb{F}}_p$ as to ‘the’ algebraic closure of \mathbb{F}_p , since for $q = p^n$ a prime power, the finite field \mathbb{F}_q with q elements is well defined only up to isomorphism. In computations, such as the construction of tables of modular characters, one uses an explicit construction of \mathbb{F}_q as the quotient ring $\mathbb{F}_p[T]/(C_n(T))$, where $C_n(T)$ is a specific irreducible polynomial, called Conway’s polynomial. This polynomial is of degree n and fulfills simple algebraic conditions and a normalization property involving the lexicographic ordering (*cf. e.g.* [Lu]). In the particular case of characteristic 2, J. Conway was able to produce *canonically* an algebraic closure $\overline{\mathbb{F}}_2$ using inductively defined operations on the ordinals³ less than ω^{ω^ω} (*cf.* [Co]). His construction also provides one with a natural choice of the isomorphism

$$j : (\overline{\mathbb{F}}_2)^\times \xrightarrow{\sim} \mathbb{G}^{\text{odd}}.$$

In fact, one can use the well ordering to choose the smallest solution as a root of unity of order $2^\ell - 1$ fulfilling compatibility conditions with the previous choices for divisors of ℓ . One obtains this way a well-defined corresponding symmetry s on $\mathbb{G}^{\text{odd}} \cup \{0\}$. Figure 1 shows the restriction of this symmetry to $\mathbb{G}^{15} \cup \{0\}$, while Figure 2 gives the simple geometric meaning of the commutation of s with its conjugates by rotations.

2.3 Characteristic $p = 1$ and idempotent analysis.

To explain how idempotent analysis and the semifield $\mathbb{R}_+^{\text{max}}$ appear naturally in the above framework, we shall no longer require that the map s , which represents the ‘addition of 1’ is a bijection of \mathbb{K} , but we shall instead require that s is a *retraction i.e.* it satisfies the idempotent condition

$$s \circ s = s.$$

³The first author is grateful to Javier Lopez for pointing out this construction of J. Conway.

Before stating the analogue of Theorem 2.1 in this context we will review a few definitions.

The classical theory of rings has been generalized by the more general theory of semi-rings (cf. [Go]).

DEFINITION 2.5. A semi-ring $(R, +, \cdot)$ is a non-empty set R endowed with operations of addition and multiplication such that

- (a) $(R, +)$ is a commutative monoid with neutral element 0
- (b) (R, \cdot) is a monoid with identity 1
- (c) $\forall r, s, t \in R: r(s + t) = rs + rt$ and $(s + t)r = sr + tr$
- (d) $\forall r \in R: r \cdot 0 = 0 \cdot r = 0$
- (e) $0 \neq 1$.

To any semi-ring R one associates a *characteristic*. The set $\mathbb{N}1_R = \{n1_R | n \in \mathbb{N}\}$ is a commutative subsemi-ring of R called the prime semi-ring. The prime semi-ring is the smallest semi-ring contained in R . If $n \neq m \Rightarrow n1_R \neq m1_R$, then $\mathbb{N}1 \simeq \mathbb{N}$ naturally and the semi-ring R is said to have characteristic zero. On the other hand, if it happens that $k1_R = 0_R$, for some $k > 1$, then there is a least positive integer n with $n1_R = 0_R$. In this case, $\mathbb{N}1 \simeq \mathbb{Z}/n\mathbb{Z}$ and one shows that R itself is a ring of positive characteristic. Finally, if $\ell 1_R = m1_R$ for some $\ell \neq m$, $\ell, m \geq 1$ but $k1_R \neq 0$ for all $k \geq 1$, one writes j for $j1_R$ and it follows that $\mathbb{N}1_R = \{0, 1, \dots, n-1\}$. In this case one has (cf. [Go] Proposition 9.7)

PROPOSITION 2.6. Let n be the least positive integer such that $n1_R \in \{i1_R | 1 \leq i \leq n-1\}$ and let $i \in \{1, n-1\}$ with $n1_R = i1_R$. Then the prime semi-ring $\mathbb{N}1_R = \{n1_R | n \in \mathbb{N}\}$ is the following semi-ring $B(n, i)$

$$B(n, i) := \{0, 1, \dots, n-1\}$$

with the following operations, where $m = n - i$

$$x +' y := \begin{cases} x + y, & \text{if } x + y \leq n - 1, \\ \ell, i \leq \ell \leq n - 1, \ell = (x + y) \bmod m & \text{if } x + y \geq n \end{cases}$$

$$x \cdot y := \begin{cases} xy, & \text{if } xy \leq n - 1, \\ \ell, i \leq \ell \leq n - 1, \ell = (xy) \bmod m & \text{if } xy \geq n. \end{cases}$$

The semi-ring $B(n, i)$ is the homomorphic image of $(\mathbb{N}, +, \cdot)$ by the map $\pi : \mathbb{N} \rightarrow R$, $\pi(k) = k$ for $0 \leq k \leq n-1$ and for $k \geq n$, $\pi(k)$ is the unique natural number congruent to $k \bmod m = n - i$ with $i \leq \pi(k) \leq n-1$. In this case we say that R has characteristic (n, i) .

Note that if R is a semi-field the only possibility for the semi-ring $B(n, i)$ is when $n = 2$ and $i = 1$. Indeed the subset $\{\ell, i \leq \ell \leq n-1\}$ is stable under product and hence should contain 1 since a finite submonoid of an abelian group is a subgroup. Thus $i = 1$, but in that case one gets $(n-1) \cdot (n-1) = (n-1)$ which is possible only for $n = 2$. The smallest finite (prime) semi-ring structure arises when $n = 2$ (and $i = 1$). We shall denote this structure by $\mathbb{B} = B(2, 1)$. By construction, $\mathbb{B} = \{0, 1\}$ with the usual multiplication law and an addition requiring the idempotent rule $1 + 1 = 1$.

DEFINITION 2.7. A semi-ring R is said to have characteristic 1 when

$$1 + 1 = 1$$

in R i.e. when R contains \mathbb{B} as the prime sub-semi-ring.

When R is a semi-ring of characteristic 1, we denote the addition in R by the symbol \uplus . Then, it follows from distributivity that

$$a \uplus a = a, \quad \forall a \in R.$$

This justifies the term ‘‘additively idempotent’’ frequently used in semi-ring theory as a synonym for ‘‘characteristic one’’. A semi-ring R is called a *semi-field* when every non-zero element in R has a multiplicative inverse, or equivalently when the set of non-zero elements in R is a (commutative) group for the multiplicative law.

THEOREM 2.8. Let H be an abelian group. Let s be a retraction ($s \circ s = s$) of the set $\mathbb{K} = H \cup \{0\}$ that commutes with its conjugates for the action of H by multiplication on the monoid \mathbb{K} . Then, if $s(0) \neq 0$, the operation

$$(15) \quad x + y = \begin{cases} y, & \text{if } x = 0, \\ s(0)^{-1}xs(s(0)yx^{-1}), & \text{if } x \neq 0 \end{cases}$$

defines a commutative monoid law on \mathbb{K} . With this law as addition, the monoid \mathbb{K} becomes a commutative semi-field of characteristic 1.

PROOF. The proof of Theorem 2.1 applies without modification. Notice that that proof did not use the hypothesis that s is a bijection, except to get the element $\theta = s^{-1}(0)$ which was used to define the additive inverse. The fact that s is a retraction shows that K is of characteristic 1. \square

EXAMPLE 2.9. Let $H = \mathbb{R}_+^*$ be the multiplicative group of the positive real numbers. Let s be the retraction of $\mathbb{K} = H \cup \{0\} = \mathbb{R}_+$ on $[1, \infty) \subset H$ given by

$$s(x) = 1, \quad \forall x \leq 1, \quad s(x) = x, \quad \forall x \geq 1.$$

The conjugate s^λ under multiplication (by λ) is the retraction on $[\lambda, \infty)$ and one easily checks that s commutes with s^λ . The resulting commutative idempotent semi-field is denoted by \mathbb{R}_+^{\max} . Thus \mathbb{R}_+^{\max} is the set \mathbb{R}_+ endowed with the following two operations

- Addition

$$x \uplus y := \max(x, y), \quad \forall x, y \in \mathbb{R}_+$$

- Multiplication is unchanged.

EXAMPLE 2.10. Let H be a group and let 2^H be the set of subsets of H endowed with the following two operations

- Addition

$$(16) \quad X \uplus Y := X \cup Y, \quad \forall X, Y \in 2^H$$

- Multiplication

$$(17) \quad X.Y = \{ab \mid a \in X, b \in Y\}, \quad \forall X, Y \in 2^H.$$

Addition is commutative and associative and admits the empty set as a neutral element. Multiplication is associative and it admits the empty set as an absorbing

element (which we denote by 0 since it is also the neutral element for the additive structure). The multiplication is also distributive with respect to the addition.

EXAMPLE 2.11. Let (M, \uplus) be an idempotent semigroup. Then, one endows the set $\text{End}(M)$ of endomorphisms $h : M \rightarrow M$ such that

$$h(a \uplus b) = h(a) \uplus h(b), \quad \forall a, b \in M$$

with the following operations (cf. [Go], I Example 1.14)

- Addition

$$(h \uplus g)(a) = h(a) \uplus g(a), \quad \forall a \in M, \quad \forall h, g \in \text{End}(M)$$

- Multiplication

$$(h \cdot g)(a) = h(g(a)), \quad \forall a \in M, \quad \forall h, g \in \text{End}(M).$$

For instance, if one lets (M, \uplus) be the idempotent semigroup given by (\mathbb{R}, \max) , the set $\text{End}(M)$ of endomorphisms of M is the set of monotonic maps $\mathbb{R} \rightarrow \mathbb{R}$. $\text{End}(M)$ becomes a semi-ring of characteristic 1 with the above operations.

EXAMPLE 2.12. Let \mathbb{C}_{star} be the set of finitely generated star shaped subsets of the complex numbers \mathbb{C} . Thus an element of \mathbb{C}_{star} is of the form

$$S = \{0\} \bigcup_{z \in F} \{\lambda z \mid z \in F, \lambda \in [0, 1]\}$$

for some finite subset $F \subset \mathbb{C}$. One has a natural injection $\mathbb{C}_{\text{star}} \rightarrow 2^{\mathbb{C}^*}$ given by

$$S \mapsto S \cap \mathbb{C}^*.$$

The image of \mathbb{C}_{star} through this injection is stable under the semi-ring operations (16) and (17) in the semi-ring $2^{\mathbb{C}^*}$, where we view \mathbb{C}^* as a multiplicative group. This shows that \mathbb{C}_{star} is an idempotent semi-ring under the following operations

- Addition

$$X \uplus Y := X \cup Y, \quad \forall X, Y \in \mathbb{C}_{\text{star}}$$

- Multiplication

$$X \cdot Y = \{ab \mid a \in X, b \in Y\}, \quad \forall X, Y \in \mathbb{C}_{\text{star}}$$

2.3.1 Finite semi-field of characteristic 1.

We quote the following result from [Go] (Example 4.28 Chapter 4).

PROPOSITION 2.13. *The semi-field $\mathbb{B} = B(2, 1)$ is the only finite semi-field of characteristic 1.*

The semi-field $\mathbb{B} = B(2, 1)$ is called the Boolean semi-field (cf. [Go], I Example 1.5).

2.3.2 Lattices.

The idempotency of addition in semi-rings of characteristic 1 gives rise to a natural *partial order* which differentiates this theory from that of the more general semi-rings. We recall the following well known fact

PROPOSITION 2.14. *Let (A, \uplus) be a commutative semigroup with an idempotent addition. Define*

$$(18) \quad a \preceq b \quad \Leftrightarrow \quad a \uplus b = b$$

Then (A, \preceq) is a sup-semilattice (i.e. a semilattice in which any two elements have a supremum). Furthermore

$$(19) \quad \max\{a, b\} = a \uplus b.$$

Conversely, if (A, \preceq) is a sup-semilattice and \uplus is defined to satisfy (19), then (A, \uplus) is an idempotent semigroup. These two constructions are inverse to each other.

PROOF. We check that (18) defines a partial order \preceq on A . Let $a, b, c \in A$. The reflexive property ($a \preceq a$) follows from the idempotency of the addition in A i.e. $a \uplus a = a$. The antisymmetric property ($a \preceq b, b \preceq a \Rightarrow a = b$) follows from the commutativity of the addition in A i.e. $b = a \uplus b = b \uplus a = a$. Finally, the transitivity property ($a \preceq b, b \preceq c \Rightarrow a \preceq c$) follows from the associativity of the binary operation \uplus i.e. $a \uplus c = a \uplus (b \uplus c) = (a \uplus b) \uplus c = b \uplus c = c$. Thus (A, \preceq) is a poset and due to the idempotency of the addition, (A, \preceq) is also a semilattice. One defines the join of two elements in A as: $a \vee b := a \uplus b$ and due to the closure property of the law \uplus in A (i.e. $a \uplus b \in A, \forall a, b \in A$), one concludes that (A, \preceq) is a sup-semilattice (the supremum = maximum of two elements in A being their join).

The converse statement follows too since the above statements on the idempotency and associativity of the operation \uplus hold also in reverse and the closure property derives from (19). \square

It follows that any semi-ring of characteristic 1 has a natural partial ordering, denoted \preceq . The addition in the semi-ring is a monotonic operation and 0 is the least element. Distributivity implies that left and right multiplication are semilattice homomorphisms and in particular they are monotonic. Thus, any semi-ring of characteristic 1 may be thought of as a semilattice ordered semigroup.

2.3.3 Perfect semi-rings of characteristic 1.

The following notion is the natural extension to semi-rings of the absence of zero divisors in a ring.

DEFINITION 2.15. *A commutative semi-ring is called multiplicatively-cancellative when the multiplication by any non-zero element is injective.*

We recall, from [Go] Propositions 4.43 and 4.44 the following result which describes the analogue of the Frobenius endomorphism in characteristic p .

PROPOSITION 2.16. *Let R be a multiplicatively-cancellative commutative semi-ring of characteristic 1, then for any integer $n \in \mathbb{N}$, the map $x \mapsto x^n$ is an injective endomorphism of R .*

Recall now that in characteristic $p > 1$ a ring is called *perfect* if the map $x \mapsto x^p$ is surjective.

DEFINITION 2.17. *A multiplicatively-cancellative commutative semi-ring of characteristic 1 is called perfect if the endomorphism $R \rightarrow R, x \mapsto x^n$ is surjective for all n .*

It then follows from Proposition 2.16 that the endomorphism ϑ_n , $x \mapsto x^n$ is bijective and one can invert it and construct the fractional powers

$$\vartheta_\alpha : R \rightarrow R, \quad \vartheta_\alpha(x) = x^\alpha, \quad \forall \alpha \in \mathbb{Q}_+^*.$$

Then, by construction, the ϑ_α 's are automorphisms $\vartheta_\alpha \in \text{Aut}(R)$ for $\alpha \in \mathbb{Q}_+^*$ and they fulfill the following properties

- $\vartheta_n(x) = x^n$ for all $n \in \mathbb{N}$ and $x \in R$.
- $\vartheta_\lambda \circ \vartheta_\mu = \vartheta_{\lambda\mu}$ for all $\lambda, \mu \in \mathbb{Q}_+^*$.
- $\vartheta_\lambda(x)\vartheta_\mu(x) = \vartheta_{\lambda+\mu}(x)$ for all $\lambda, \mu \in \mathbb{Q}_+^*$ and $x \in R$.

2.3.4 Completion.

One can complete a commutative semi-ring of characteristic 1 with respect to any *compatible* metric, *i.e.* a metric d which fulfills the following analogue of the ultrametric inequality

$$d(x \uplus y, z \uplus t) \leq \sup d(x, z), d(y, t), \quad \forall x, y, z, t \in R$$

and the following compatibility with the product

$$d(ax, ay) \leq d(0, a)d(x, y), \quad \forall a, x, y \in R.$$

Let $\rho \in R$, $1 \preceq \rho$, be an invertible element, we denote by R^ρ the union

$$R^\rho = \{0\} \cup_{n \in \mathbb{N}} [\rho^{-n}, \rho^n]$$

The following result will be used below.

PROPOSITION 2.18. *Let R be a perfect commutative semi-ring of characteristic 1 with a compatible metric d . Let $\rho \in R$, $1 \preceq \rho$, be invertible and such that the intervals $[\rho^{-n}, \rho^n]$ are complete and $d(\rho^\alpha, 1) \rightarrow 0$ when $\alpha \rightarrow 0$. Then for any non-zero $x \in R^\rho$, $d(x^\alpha, 1) \rightarrow 0$ when $\alpha \rightarrow 0+$.*

PROOF. Let $\epsilon > 0$ and $\delta > 0$ such that $d(\rho^\alpha, 1) < \epsilon$, $\forall \alpha$, $|\alpha| \leq \delta$. For $x \in [\rho^{-n}, \rho^n]$ and $0 < \alpha < \delta/n$ one has $x^\alpha \in [\rho^{-n\alpha}, \rho^{n\alpha}]$ since θ_α is an automorphism. Thus $\rho^{-n\alpha} \uplus x^\alpha = x^\alpha$, $\rho^{n\alpha} \uplus x^\alpha = \rho^{n\alpha}$ and

$$d(x^\alpha, \rho^{n\alpha}) = d(\rho^{-n\alpha} \uplus x^\alpha, \rho^{n\alpha} \uplus x^\alpha) \leq d(\rho^{-n\alpha}, \rho^{n\alpha}) \leq 2\epsilon$$

so that $d(x^\alpha, 1) \leq 3\epsilon$. □

2.4 Witt ring in characteristic $p = 1$ and entropy.

The places of the global field \mathbb{Q} of the rational numbers fall in two classes: the infinite archimedean place ∞ and the finite places which are labeled by the prime integer numbers. The p -adic completion of \mathbb{Q} at a finite place p determines the corresponding global field \mathbb{Q}_p of p -adic numbers. These local fields have close relatives with simpler structure: the local fields $\mathbb{F}_p((T))$ of formal power series with coefficients in the finite fields \mathbb{F}_p and with finite order pole at 0. We already explained in the introduction that the similarity between the structures of \mathbb{Q}_p and of $\mathbb{F}_p((T))$ is embodied in the Ax-Kochen Theorem (*cf.* [AK]) which states the isomorphism of arbitrary ultraproducts as in (1). By means of the natural construction of the ring of Witt vectors, one recovers the ring \mathbb{Z}_p of p -adic integers from the finite field \mathbb{F}_p .

This construction (*cf.* also §2.5) can be interpreted as a deformation of the ring of formal power series $\mathbb{F}_p[[T]]$ to \mathbb{Z}_p .

It is then natural to wonder on the existence of a similar phenomenon at the infinite archimedean place of \mathbb{Q} . We have already introduced the semi-field of characteristic one \mathbb{R}_+^{\max} as the degenerate version of the field of real numbers. In this subsection we shall describe how the basic physics formula for the free energy involving entropy allows one to move canonically, not only from \mathbb{R}_+^{\max} to \mathbb{R} but in even greater generality from a perfect semi-ring of characteristic 1 to an ordinary algebra over \mathbb{R} . This construction is analogous to the construction of the Witt ring.

Let K be a perfect semi-ring of characteristic 1, and let us first assume that it contains \mathbb{R}_+^{\max} as a sub semi-ring. Thus the operation of raising to a power $s \in \mathbb{Q}_+$ is well defined in K and determines an automorphism $\vartheta_s : K \rightarrow K$, $\vartheta_s(x) = x^s$. We first concentrate on the algebraic aspects and use formally the following infinite sum (for the operation \uplus) to define a new addition

$$x +' y := \sum_{s \in \mathbb{Q} \cap [0,1]}^{\uplus} c(s) x^s y^{1-s}, \quad \forall x, y \in K$$

where the function $c(s) \in \mathbb{R}_+$ is defined by

$$c : [0, 1] \rightarrow \mathbb{R}_+, \quad c(s) = e^{S(s)} = s^{-s}(1-s)^{-(1-s)}.$$

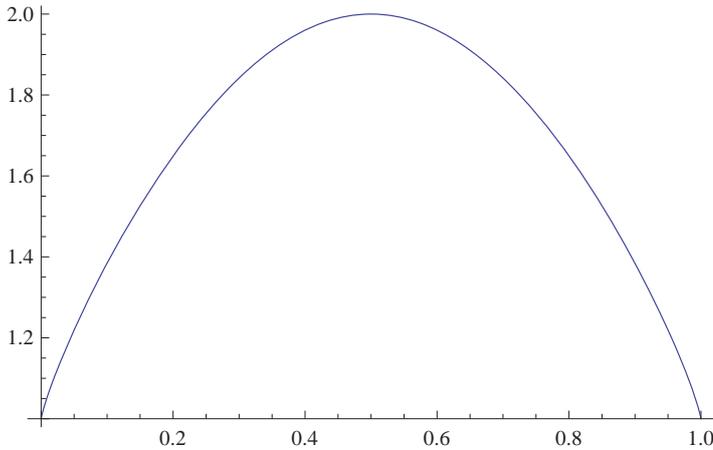


Fig. 3. Graph of $c(x)$.

The property of the function $c(s)$ which ensures the associativity of the addition law $+'$ is the following: for any $s, t \in [0, 1]$ the product $c(s)c(t)^s$ only depends upon the partition of 1 as $st + s(1-t) + (1-s)$. This fact also implies the functional equation

$$(20) \quad c(u)c(v)^u = c(uv)c(w)^{(1-uv)}, \quad w = \frac{u(1-v)}{1-uv}.$$

The function c fulfils the symmetry $c(1-u) = c(u)$ and, by taking it into account, (20) means then that the function on the simplex $\Sigma_2 = \{(s_j) \mid s_j \geq 0, \sum_0^2 s_j = 1\}$ defined by

$$(21) \quad c_2(s_0, s_1, s_2) = c(s_2)c\left(\frac{s_0}{s_0+s_1}\right)^{s_0+s_1}$$

is symmetric under all permutations of the s_j . More generally, for any integer n one may define the function on the n -simplex

$$c_n(s_0, s_1, \dots, s_n) = \prod \gamma(s_j)^{-1}, \quad \gamma(x) = x^x.$$

LEMMA 2.19. *Let $x, y \in \mathbb{R}_+$, then one has*

$$\sup_{s \in [0,1]} c(s) x^s y^{1-s} = x + y.$$

PROOF. Let $x = e^a$ and $y = e^b$. The function

$$f(s) = \log(c(s) x^s y^{1-s}) = S(s) + sa + (1-s)b$$

is strictly concave on the interval $[0, 1]$ and reaches its unique maximum for $s = \frac{e^a}{e^a + e^b} \in [0, 1]$. Its value at the maximum is $\log(e^a + e^b)$. \square

THEOREM 2.20. *Let K be a perfect semi-ring of characteristic 1. Let $\rho \in K$, $1 \preceq \rho$ be invertible and such that for a compatible metric d the intervals $[\rho^{-n}, \rho^n]$ are complete and $d(\rho^\alpha, 1) \rightarrow 0$ when $\alpha \rightarrow 0$. Let $K^\rho = \{0\} \cup_{n \in \mathbb{N}} [\rho^{-n}, \rho^n]$ (cf. §2.3.4). Then the formula*

$$(22) \quad x +_\rho y := \sum_{s \in \mathbb{Q} \cap [0,1]}^{\uplus} \rho^{S(s)} x^s y^{1-s}, \quad \forall x, y \in K^\rho$$

defines an associative law on K^ρ with 0 as neutral element. The multiplication is distributive with respect to this law. These operations turn the Grothendieck group of the additive monoid $(K^\rho, +_\rho)$ into an algebra $W(K, \rho)$ over \mathbb{R} which depends functorially upon (K, ρ) .

PROOF. Since $1 \preceq \rho$ one has, using the automorphisms ϑ_λ , that

$$1 \preceq \vartheta_\lambda(\rho) = \rho^\lambda, \quad \forall \lambda \in \mathbb{Q}_+.$$

Then it follows that

$$\rho^\lambda \preceq \rho^{\lambda'}, \quad \forall \lambda \leq \lambda'.$$

Thus, using completeness to extend the definition of ρ^λ for real values of λ , one obtains that the following map defines a homomorphism of semi-rings

$$\alpha : (\mathbb{R}_+, \max, \cdot) = \mathbb{R}_+^{\max} \rightarrow K^\rho, \quad \alpha(\lambda) = \rho^{\log \lambda}, \quad \alpha(0) = 0$$

where we have used the invertibility of ρ in K^ρ to make sense of the negative powers of ρ . Let $w(t) = \rho^{S(t)}$ and $I(n) = \frac{1}{n}\mathbb{Z} \cap [0, 1]$. Let x, y be non-zero elements of K^ρ . Then the partial sums

$$s(n) = \sum_{I(n)} w(\alpha) x^\alpha y^{1-\alpha}$$

form a filtered increasing family for the partial order given by divisibility $n|m$. Moreover one has $s(n) \preceq \rho^m$ for a fixed m , independent of n as follows using $w(\alpha) \preceq \rho$ for all $\alpha \in [0, 1]$. Proposition 2.18 shows that the maps

$$\alpha \mapsto w(\alpha), \quad \alpha \mapsto x^\alpha, \quad \alpha \mapsto y^{1-\alpha},$$

are uniformly continuous for the compatible metric d . It follows using the ultrametric inequality

$$d\left(\sum x_i, \sum y_i\right) \leq \text{Sup}(d(x_i, y_i))$$

that the sequence $s(n)$ is a Cauchy sequence. This shows the existence of its limit

$$x +_\rho y := \sum_{s \in \mathbb{Q} \cap [0, 1]}^{\uplus} \rho^{S(s)} x^s y^{1-s}$$

The associativity of the operation $+_\rho$ follows, with $I = \mathbb{Q} \cap (0, 1)$, from

$$\begin{aligned} (x +_\rho y) +_\rho z &= \sum_{s \in I}^{\uplus} w(s) \vartheta_s \left(\sum_{t \in I}^{\uplus} w(t) x^t y^{1-t} \right) z^{1-s} = \\ &= \sum_{s \in I}^{\uplus} \sum_{t \in I}^{\uplus} w(s) w(t)^s x^{ts} y^{(1-t)s} z^{1-s} = \sum_{\Sigma_2}^{\uplus} w_2(s_0, s_1, s_2) x^{s_0} y^{s_1} z^{s_2} \end{aligned}$$

which is symmetric in (x, y, z) by making use of (21) and (20). Moreover, one has by homogeneity the distributivity

$$(x +_\rho y)z = xz +_\rho yz, \quad \forall x, y, z \in K.$$

We let K^ρ be the semi-ring with the operations $+_\rho$ and the multiplication unchanged. If we endow \mathbb{R}_+ with its ordinary addition, we have by applying Lemma 2.19, that

$$\alpha(\lambda_1) +_\rho \alpha(\lambda_2) = \alpha(\lambda_1 + \lambda_2).$$

Thus α defines a homomorphism

$$\tilde{\alpha} : \mathbb{R}_+ \rightarrow (K^\rho, +_\rho, \cdot), \quad \tilde{\alpha}(\lambda) = \rho^{\log \lambda}, \quad \alpha(0) = 0$$

of the semi-ring \mathbb{R}_+ (with ordinary addition) into the semi-ring $(K^\rho, +_\rho, \cdot)$.

Let G be the functor from semi-rings to rings which associates to a semi-ring R the Grothendieck group R^Δ of the additive monoid R with the natural extension of the product (cf. [Gö]). Let $R[\mathbb{Z}/2\mathbb{Z}]$ be the semi-group ring of $\mathbb{Z}/2\mathbb{Z}$. Elements of $R[\mathbb{Z}/2\mathbb{Z}]$ are given by pairs (m_1, m_2) of elements of R . The addition is given coordinate-wise and the product is defined by

$$(m_1, m_2) \cdot (n_1, n_2) = (m_1 n_1 + m_2 n_2, m_1 n_2 + m_2 n_1).$$

One can view the ring $G(R)$ as the quotient of the semi-ring $R[\mathbb{Z}/2\mathbb{Z}]$ by the ideal of diagonal elements $J = \{(x, x) \mid x \in R\}$ or equivalently by the equivalence relation

$$(m_1, m_2) \sim (n_1, n_2) \Leftrightarrow \exists k \in R, \quad m_1 + n_2 + k = m_2 + n_1 + k.$$

This equivalence relation is compatible with the product which turns the quotient $G(R)$ into a ring. We define

$$W(K, \rho) = G((K^\rho, +_\rho, \cdot))$$

One has $G(\mathbb{R}_+) = \mathbb{R}$. By functoriality of G one thus gets a morphism $G(\tilde{\alpha})$ from \mathbb{R} to $W(K, \rho)$. As long as $1 \neq 0$ in $G((K^\rho, +_\rho, \cdot))$ this morphism endows $W(K, \rho)$ with the structure of an algebra over \mathbb{R} . When $1 = 0$ in $G((K^\rho, +_\rho, \cdot))$ one gets the degenerate case $W(K, \rho) = \{0\}$. \square

We did not discuss conditions on ρ which ensure that $(K^\rho, +_\rho, \cdot)$ injects in $W(K, \rho)$, let alone that $W(K, \rho) \neq \{0\}$. The following example shows that the problem comes from how strict the inequality $\rho \preccurlyeq 1$ is assumed to be, *i.e.* where the function $T(x)$ playing the role of absolute temperature actually vanishes.

EXAMPLE 2.21. Let X be a compact space and let $R = C(X, \mathbb{R}_+^{\max})$ be the space of continuous maps from X to the semi-field \mathbb{R}_+^{\max} . We endow R with the operations \max for addition and the ordinary pointwise product for multiplication. The associated semi-ring is a perfect semi-ring of characteristic 1. Let then $\rho \in R$, $1 \preccurlyeq \rho$, it is of the form

$$\rho(x) = e^{T(x)}, \quad \forall x \in X.$$

Let $\beta(x) = 1/T(x)$ if $T(x) > 0$ and $\beta(x) = \infty$ for $T(x) = 0$. Then, the addition $+_\rho$ in R is given by

$$(f +_\rho g)(x) = \left(f(x)^{\beta(x)} + g(x)^{\beta(x)} \right)^{T(x)}, \quad \forall x \in X.$$

This follows from Lemma 2.19 which implies more generally that

$$\sup_{s \in [0,1]} e^{TS(s)} x^s y^{1-s} = (x^\beta + y^\beta)^T, \quad \beta = \frac{1}{T}.$$

Then, provided that $\rho(x) > 1$ for all $x \in X$, the algebra $W(R, \rho)$ is isomorphic, as an algebra over \mathbb{R} , with the real C^* -algebra $C(X, \mathbb{R})$ of continuous functions on X .

2.5 The Witt ring in characteristic $p > 1$ revisited.

In this subsection we explain in which sense we interpret the formula (22) as the analogue of the construction of the Witt ring in characteristic one. Let K be a perfect ring of characteristic p . We start by reformulating the construction of the Witt ring in characteristic $p > 1$. One knows (*cf.* [Se] Chapter II) that there is a strict p -ring R , unique up to canonical isomorphism, such that its residue ring R/pR is equal to K . One also knows that there exists a unique multiplicative section $\tau : K \rightarrow R$ of the residue map. For $x \in K$, $\tau(x) \in R$ is called the Teichmüller representative of x . Every element $z \in R$ can be written uniquely as

$$(23) \quad z = \sum_0^\infty \tau(x_n) p^n.$$

The Witt construction of R is functorial and an easy corollary of its properties is the following

$\frac{1}{125}$	$4T^3$	$\frac{2}{125}$	$3T^3$	$\frac{3}{125}$	$3T^3$	$\frac{4}{125}$	$4T^3$	$\frac{1}{25}$	$4T^2$
$\frac{125}{6}$	$3T^3$	$\frac{125}{7}$	$2T^3$	$\frac{125}{8}$	0	$\frac{125}{9}$	T^3	$\frac{25}{2}$	$3T^2$
$\frac{125}{11}$	$4T^3$	$\frac{125}{12}$	$2T^3$	$\frac{125}{13}$	$2T^3$	$\frac{125}{14}$	$4T^3$	$\frac{25}{3}$	$3T^2 + 2T^3$
$\frac{125}{16}$	0	$\frac{125}{17}$	0	$\frac{125}{18}$	$3T^3$	$\frac{125}{19}$	$3T^3$	$\frac{25}{4}$	$4T^2 + 2T^3$
$\frac{125}{21}$	T^3	$\frac{125}{22}$	$3T^3$	$\frac{125}{23}$	0	$\frac{125}{24}$	$3T^3$	$\frac{1}{5}$	$4T$
$\frac{125}{26}$	$3T^3$	$\frac{125}{27}$	0	$\frac{125}{28}$	$2T^3$	$\frac{125}{29}$	T^3	$\frac{25}{6}$	$3T^2 + 3T^3$
$\frac{125}{31}$	T^3	$\frac{125}{32}$	$2T^3$	$\frac{125}{33}$	$4T^3$	$\frac{125}{34}$	0	$\frac{7}{25}$	$2T^2 + T^3$
$\frac{125}{36}$	$3T^3$	$\frac{125}{37}$	T^3	$\frac{125}{38}$	0	$\frac{125}{39}$	T^3	$\frac{8}{25}$	T^3
$\frac{125}{41}$	$2T^3$	$\frac{125}{42}$	$2T^3$	$\frac{125}{43}$	0	$\frac{125}{44}$	$3T^3$	$\frac{9}{25}$	$T^2 + T^3$
$\frac{125}{46}$	$3T^3$	$\frac{125}{47}$	$2T^3$	$\frac{125}{48}$	$4T^3$	$\frac{125}{49}$	$2T^3$	$\frac{2}{25}$	$3T$
$\frac{125}{51}$	T^3	$\frac{125}{52}$	$3T^3$	$\frac{125}{53}$	$4T^3$	$\frac{125}{54}$	T^3	$\frac{11}{25}$	$4T^3$
$\frac{125}{56}$	$2T^3$	$\frac{125}{57}$	T^3	$\frac{125}{58}$	T^3	$\frac{125}{59}$	T^3	$\frac{12}{25}$	$4T^2 + T^3$
$\frac{125}{61}$	$4T^3$	$\frac{125}{62}$	T^3	$\frac{125}{63}$	T^3	$\frac{125}{64}$	$4T^3$	$\frac{13}{25}$	$4T^2 + T^3$
$\frac{125}{66}$	T^3	$\frac{125}{67}$	T^3	$\frac{125}{68}$	T^3	$\frac{125}{69}$	$2T^3$	$\frac{14}{25}$	$4T^3$
$\frac{125}{71}$	T^3	$\frac{125}{72}$	$4T^3$	$\frac{125}{73}$	$3T^3$	$\frac{125}{74}$	T^3	$\frac{3}{25}$	$3T$
$\frac{125}{76}$	$2T^3$	$\frac{125}{77}$	$4T^3$	$\frac{125}{78}$	$2T^3$	$\frac{125}{79}$	$3T^3$	$\frac{16}{25}$	$T^2 + T^3$
$\frac{125}{81}$	$3T^3$	$\frac{125}{82}$	0	$\frac{125}{83}$	$2T^3$	$\frac{125}{84}$	$2T^3$	$\frac{17}{25}$	T^3
$\frac{125}{86}$	T^3	$\frac{125}{87}$	0	$\frac{125}{88}$	T^3	$\frac{125}{89}$	$3T^3$	$\frac{18}{25}$	$2T^2 + T^3$
$\frac{125}{91}$	0	$\frac{125}{92}$	$4T^3$	$\frac{125}{93}$	$2T^3$	$\frac{125}{94}$	T^3	$\frac{19}{25}$	$3T^2 + 3T^3$
$\frac{125}{96}$	T^3	$\frac{125}{97}$	$2T^3$	$\frac{125}{98}$	0	$\frac{125}{99}$	$3T^3$	$\frac{4}{25}$	$4T$
$\frac{125}{101}$	$3T^3$	$\frac{125}{102}$	0	$\frac{125}{103}$	$3T^3$	$\frac{125}{104}$	T^3	$\frac{21}{25}$	$4T^2 + 2T^3$
$\frac{125}{106}$	$3T^3$	$\frac{125}{107}$	$3T^3$	$\frac{125}{108}$	0	$\frac{125}{109}$	0	$\frac{22}{25}$	$3T^2 + 2T^3$
$\frac{125}{111}$	$4T^3$	$\frac{125}{112}$	$2T^3$	$\frac{125}{113}$	$2T^3$	$\frac{125}{114}$	$4T^3$	$\frac{23}{25}$	$3T^2$
$\frac{125}{116}$	T^3	$\frac{125}{117}$	0	$\frac{125}{118}$	$2T^3$	$\frac{125}{119}$	$3T^3$	$\frac{24}{25}$	$4T^2$
$\frac{125}{121}$	$4T^3$	$\frac{125}{122}$	$3T^3$	$\frac{125}{123}$	$3T^3$	$\frac{125}{124}$	$4T^3$	$\frac{25}{25}$	1
$\frac{125}{125}$		$\frac{125}{125}$		$\frac{125}{125}$		$\frac{125}{125}$			

Table 1. Values of $w_5(\alpha)$ modulo T^4 .

LEMMA 2.22. *For any prime number p , there exists a universal sequence*

$$w(p^n, k) \in \mathbb{Z}/p\mathbb{Z}, \quad 0 < k < p^n$$

such that

$$(24) \quad \tau(x) + \tau(y) = \tau(x + y) + \sum_{n=1}^{\infty} \tau \left(\sum w(p^n, k) x^{\frac{k}{p^n}} y^{1 - \frac{k}{p^n}} \right) p^n.$$

Note incidentally that the fractional powers such as $x^{\frac{k}{p^n}}$ make sense in a perfect ring such as K . The main point here is that formula (24) suffices to reconstruct the whole ring structure on R and allows one to add and multiply series of the form (23).

PROOF. Formula (24) is a special case of the basic formula

$$s_n = S_n(x_0^{1/p^n}, y_0^{1/p^n}, x_1^{1/p^{n-1}}, y_1^{1/p^{n-1}}, \dots, x_n, y_n)$$

(cf. [Se], Chapter II §6) which computes the sum

$$\sum_0^\infty \tau(x_n)p^n + \sum_0^\infty \tau(y_n)p^n = \sum_0^\infty \tau(s_n)p^n.$$

□

We can now introduce a natural map from the set I_p of rational numbers in $[0, 1]$ whose denominator is a power of p , to the maximal compact subring of the local field $\mathbb{F}_p((T))$ as follows

$$w_p : I_p \rightarrow \mathbb{F}_p((T)), \quad w_p(\alpha) = \sum_{\frac{a}{p^n}=\alpha} w(p^n, a)T^n \in \mathbb{F}_p((T)).$$

We can then rewrite equation (24) in a more suggestive form as a deformation of the addition, by first introducing the map

$$\tau : K[[T]] \rightarrow R, \quad \tau\left(\sum_0^\infty z_n T^n\right) = \sum_0^\infty \tau(z_n)p^n.$$

This map is an homeomorphism and is multiplicative on monomials *i.e.*

$$\tau(aT^n Z) = \tau(a)\tau(T)^n\tau(Z), \quad \forall a \in K, Z \in K[[T]].$$

Since τ is not additive, one defines a new addition on $K[[T]]$ by setting

$$X +' Y := \tau^{-1}(\tau(X) + \tau(Y)), \quad \forall X, Y \in K[[T]].$$

PROPOSITION 2.23. *Let us view the ring of formal series $K[[T]]$ as a module over $\mathbb{F}_p[[T]]$. Then one has*

$$x +' y := \sum_{\alpha \in I_p} w_p(\alpha) x^\alpha y^{1-\alpha}, \quad \forall x, y \in K.$$

This formula is analogous to formula (22) of Theorem 2.20 and suggests to develop in a deeper way the properties of the $K[[T]]$ -valued function $w_p(\alpha)$ in analogy with the classical properties of the entropy function $w_1(\alpha) = e^{S(\alpha)}$ taking its values in \mathbb{R}_+^{\max} .

2.6 \mathbb{B} , \mathbb{F}_1 and the “absolute point”.

The semi-rings of characteristic 1 provide a natural framework for a mathematics of finite characteristic $p = 1$. Moreover, the semi-field \mathbb{B} is the initial object among semi-rings of characteristic 1. However, $\text{Spec } \mathbb{B}$ does not fulfill the requirements of the “absolute point” $\text{Spec } \mathbb{F}_1$, as defined in [KS]. In particular, one expects that $\text{Spec } \mathbb{F}_1$ sits under $\text{Spec } \mathbb{Z}$. This property does not hold for $\text{Spec } \mathbb{B}$ since there is no unital homomorphism of semi-rings from \mathbb{B} to \mathbb{Z} .

We conclude this section by explaining how the “naive” approach to \mathbb{F}_1 emerges in the framework of §2.1 and §2.2. First, notice that Proposition 2.3 generalizes to characteristic $p > 2$ by implementing the following modifications:

- The group \mathbb{G}^{odd} is replaced by the group $\mathbb{G}^{(p)}$ of roots of 1 in \mathbb{C} of order prime to p .

- The involution $s^2 = id$ is replaced by a bijection $s : \mathbb{K} \rightarrow \mathbb{K}$ of $\mathbb{K} = \mathbb{G}^{(p)} \cup \{0\}$, satisfying the condition $s^p = id$ and commuting with its conjugates by rotations.

To treat the degenerate case $p = 1$ in §2.3 we dropped the condition that s is a bijection and we replaced it by the idempotency condition $s \circ s = s$. There is however another trivial possibility which is that to leave unaltered the condition $s^p = id$ and simply take $s = id$ for $p = 1$. The limit case is then obtained by implementing the following procedure:

- The group $\mathbb{G}^{(p)}$ is replaced by the group \mathbb{G} of all roots of 1 in \mathbb{C}
- The map s is the identity map on $\mathbb{G} \cup \{0\}$.

The additive structure on

$$(25) \quad \mathbb{F}_{1^\infty} = \mathbb{G} \cup \{0\}$$

degenerates since this case corresponds to setting $s(0) = 0$ in Theorem 2.1, with the bijection s given by the identity map, so that (15) becomes the indeterminate expression $0/0$.

The multiplicative structure on the monoid (25) is the same as the multiplicative structure on the group \mathbb{G} , where we consider $\{0\}$ as an absorbing element. By construction, for each integer n the group \mathbb{G} contains a unique cyclic subgroup \mathbb{G}_n of order n . The tower (inductive limit) of the finite subfields $\mathbb{F}_{p^n} \subset \bar{\mathbb{F}}_p$ is replaced in the limit case $p = 1$ by the inductive limit of commutative monoids

$$\mathbb{F}_{1^n} = \mathbb{G}_n \cup \{0\} \subset \mathbb{G} \cup \{0\}$$

where the inductive structure is partially ordered by divisibility of the index n . Notice that on \mathbb{F}_{1^∞} one can still define

$$0 + x = x + 0 = x \quad \forall x \in \mathbb{F}_{1^\infty}$$

and this simple rule suffices to multiply matrices with coefficients in \mathbb{F}_{1^∞} whose rows have at most one non-zero element. In fact, the multiplicative formula $C_{ik} = \sum A_{ij} B_{jk}$ for the product $C = AB$ of two matrices only makes sense if one can add $0 + x = x + 0 = x$. Hence, with the exception of the special case where 0 is one of the two summands, one considers the addition $x + y$ in \mathbb{F}_{1^∞} to be indeterminate. By construction, $\mathbb{F}_1 = \mathbb{G}_1 \cup \{0\} = \{1\} \cup \{0\}$ is the monoid to which \mathbb{F}_q degenerates when $q = 1$, *i.e.* by considering the addition $1 + 1$ on \mathbb{F}_1 to be indeterminate. From this simple point of view the category of commutative algebras over \mathbb{F}_1 is simply the category $\mathfrak{M}o$ of commutative monoids with a unit 1 and an absorbing element 0. In particular we see that a (commutative) semi-ring of characteristic 1 is in particular a (commutative) algebra over \mathbb{F}_1 in the above sense which is compatible with the absolute property of $\text{Spec } \mathbb{F}_1$ of (3).

REMARK 2.24. By construction, each finite field \mathbb{F}_{p^n} has the same multiplicative structure as the monoid $\mathbb{F}_{1^{p^n-1}}$. However, there exist infinitely many monoidal structures \mathbb{F}_{1^n} which do not correspond to any degeneration of a finite field: $\mathbb{F}_{1^5} = \mathbb{G}_5 \cup \{0\}$ and $\mathbb{F}_{1^9} = \mathbb{G}_9 \cup \{0\}$ are the first two cases. For the sake of clarity, we make it clear that even when $n = p^\ell - 1$ for p a prime number, we shall always consider the algebraic structures $\mathbb{F}_{1^n} = \mathbb{G}_n \cup \{0\}$ only as multiplicative monoids.

3. THE FUNCTORIAL APPROACH

In this chapter we give an overview on the geometric theory of algebraic schemes over \mathbb{F}_1 that we have introduced in our paper [CC2]. The second part of the chapter contains a new result on the geometric realization of an $\mathfrak{M}\mathfrak{o}$ -functor. In fact, our latest development of the study of the algebraic geometry of the \mathbb{F}_1 -schemes shows that, unlike the case of a \mathbb{Z} -scheme, the topology and the structure sheaf of an \mathbb{F}_1 -scheme can be obtained naturally on the set of its rational \mathbb{F}_1 -points.

Our original viewpoint in the development of this theory of schemes over \mathbb{F}_1 has been an attempt at unifying the theories developed on the one side by C. Soulé in [So] and in our earlier paper [CC1] and on the other side by A. Deitmar in [D1], [D2] (following N. Kurokawa, H. Ochiai and M. Wakayama [KOW]), by K. Kato in [Ka] (with the geometry of logarithmic structures) and by B. Töen and M. Vaquié in [TV]. In the earlier §2.6, we have described how to obtain a naive version of \mathbb{F}_1 leading naturally to the point of view developed by A. Deitmar, where \mathbb{F}_1 -algebras are commutative monoids (with the slight difference that in our setup one also requires the existence of an absorbing element 0). It is the analysis performed by C. Soulé in [So] of the extension of scalars from \mathbb{F}_1 to \mathbb{Z} that lead us to

- Reformulate the notion of a scheme in the sense of K. Kato and A. Deitmar, in functorial terms *i.e.* as a covariant functor from the category of (pointed) monoids to the category of sets.
- Prove a new result on the geometric realization of functors satisfying a suitable local representability condition.
- Refine the notion of an \mathbb{F}_1 -scheme by allowing more freedom on the choice of the \mathbb{Z} -scheme obtained by base change.

In this chapter we shall explain this viewpoint in some details, focussing in particular on the description and the properties of the geometric realization of an $\mathfrak{M}\mathfrak{o}$ -functor that was only briefly sketched in [CC2].

Everywhere in this chapter we denote by $\mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}$, $\mathfrak{M}\mathfrak{o}$, $\mathfrak{A}\mathfrak{b}$, $\mathfrak{R}\mathfrak{i}\mathfrak{n}\mathfrak{g}$ respectively the categories of sets, commutative monoids⁴, abelian groups and commutative (unital) rings.

3.1 Schemes as locally representable \mathbb{Z} -functors: a review.

In the following three subsections we will shortly review the basic notions of the theory of \mathbb{Z} -functors and \mathbb{Z} -schemes: we refer to [DG] (Chapters I, III) for a detailed exposition.

DEFINITION 3.1. *A \mathbb{Z} -functor is a covariant functor $\mathcal{F} : \mathfrak{R}\mathfrak{i}\mathfrak{n}\mathfrak{g} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}$.*

Morphisms in the category of \mathbb{Z} -functors are natural transformations (of functors).

Schemes over \mathbb{Z} determine a full subcategory $\mathfrak{S}\mathfrak{c}\mathfrak{h}$ of the category of \mathbb{Z} -functors. In fact, a scheme X over $\mathrm{Spec}\mathbb{Z}$ is *entirely* characterized by the \mathbb{Z} -functor

$$(26) \quad \underline{X} : \mathfrak{R}\mathfrak{i}\mathfrak{n}\mathfrak{g} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}, \quad \underline{X}(R) = \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Spec}R, X).$$

To a ring homomorphism $\rho : R_1 \rightarrow R_2$ one associates the morphism of (affine) schemes $\rho^* : \mathrm{Spec}(R_2) \rightarrow \mathrm{Spec}(R_1)$, $\rho^*(\mathfrak{p}) = \rho^{-1}(\mathfrak{p})$ and the map of sets

$$\rho : \underline{X}(R_1) \rightarrow \underline{X}(R_2), \quad \varphi \rightarrow \varphi \circ \rho^*.$$

⁴with a unit and a zero element

If $\psi : X \rightarrow Y$ is a morphism of schemes then one gets for every ring R a map of sets

$$\underline{X}(R) \rightarrow \underline{Y}(R), \quad \varphi \rightarrow \psi \circ \varphi.$$

The functors of the form \underline{X} , for X a scheme over $\text{Spec } \mathbb{Z}$, are *local* \mathbb{Z} -functors (in the sense that we shall recall in §3.2, Definition 3.2). These functors are also *locally representable* by commutative rings, *i.e.* they have an open cover by representable \mathbb{Z} -subfunctors (in the sense explained in §§ 3.1.2, 3.1.3).

3.2 Local \mathbb{Z} -functors.

For any commutative (unital) ring R , the geometric space $\text{Spec}(R)$ is the set of prime ideals $\mathfrak{p} \subset R$. The topology on $\text{Spec}(R)$ is the Jacobson topology *i.e.* the closed subsets are the sets $V(J) = \{\mathfrak{p} \in \text{Spec}(R) \mid \mathfrak{p} \supset J\}$, where $J \subset R$ runs through the collection of all the ideals of R . The open subsets of $\text{Spec}(R)$ are the complements of the $V(J)$'s *i.e.* they are the sets

$$D(J) = V(J)^c = \{\mathfrak{p} \in \text{Spec}(R) \mid \exists f \in J, f \notin \mathfrak{p}\}.$$

It is well known that the open sets $D(f) = V(fR)^c$, for $f \in R$, form a basis of the topology of $\text{Spec}(R)$. For any $f \in R$ one lets $R_f = S^{-1}R$, where $S = \{f^n \mid n \in \mathbb{Z}_{\geq 0}\}$ denotes the multiplicative system of the non-negative powers of f . One has a natural ring homomorphism $R \rightarrow R_f$. Then, for any scheme X over $\text{Spec } \mathbb{Z}$, the associated functor \underline{X} as in (26) fulfills the following *locality* property. For any finite cover of $\text{Spec}(R)$ by open sets $D(f_i)$, with $f_i \in R$ ($i \in I = \text{finite index set}$) the following sequence of maps of sets is exact

$$(27) \quad \underline{X}(R) \xrightarrow{u} \prod_{i \in I} \underline{X}(R_{f_i}) \xrightarrow[w]{v} \prod_{(i,j) \in I \times I} \underline{X}(R_{f_i f_j}).$$

This means that u is injective and the range of u is characterized as the set $\{z \in \prod_i \underline{X}(R_{f_i}) \mid v(z) = w(z)\}$. The exactness of (27) is a consequence of the fact that a morphism of schemes is defined by local conditions. For \mathbb{Z} -functors we have the following definition

DEFINITION 3.2. *A \mathbb{Z} -functor \mathcal{F} is local if for any object R of $\mathfrak{R}\text{ing}$ and a partition of unity $\sum_{i \in I} h_i f_i = 1$ in R ($I = \text{finite index set}$), the following sequence of sets is exact:*

$$(28) \quad \mathcal{F}(R) \xrightarrow{u} \prod_i \mathcal{F}(R_{f_i}) \xrightarrow[w]{v} \prod_{ij} \mathcal{F}(R_{f_i f_j}).$$

EXAMPLE 3.3. This example shows that locality is not automatically verified by a general \mathbb{Z} -functor.

The Grassmannian $\text{Gr}(k, n)$ of the k -dimensional linear spaces in an n -dimensional linear space is defined by the functor which associates to a ring R the set of all complemented submodules of *rank* k of the free (right) module R^n . Since any such complemented submodule is projective, by construction we have

$$\text{Gr}(k, n) : \mathfrak{R}\text{ing} \rightarrow \mathfrak{S}\text{ets}, \quad \text{Gr}(k, n)(R) = \{E \subset R^n \mid E \text{ projective, } \text{rk}(E) = k\}.$$

Let $\rho : R_1 \rightarrow R_2$ be a homomorphism of rings, the corresponding map of sets is given as follows: for $E_1 \in \text{Gr}(k, n)(R_1)$, one lets $E_2 = E_1 \otimes_{R_1} R_2 \in \text{Gr}(k, n)(R_2)$. If one takes a naive definition of the rank, *i.e.* by just requiring that $E \cong R^k$ as an

R -module, one does not obtain a local \mathbb{Z} -functor. In fact, let us consider the case $k = 1$ and $n = 2$ which defines the projective line $\mathbb{P}^1 = \text{Gr}(1, 2)$. To show that locality fails in this case, one takes the algebra $R = C(S^2)$ of continuous functions on the sphere S^2 and the partition of unity $f_1 + f_2 = 1$ subordinate to a covering of S^2 by two disks D_j ($j = 1, 2$), so that $\text{Supp}(f_j) \subset D_j$. One then considers the non-trivial line bundle L on S^2 arising from the identification $S^2 \simeq \mathbb{P}^1(\mathbb{C}) \subset M_2(\mathbb{C})$ which determines an idempotent $e \in M_2(C(S^2))$. The range of e defines a finite projective submodule $E \subset R^2$. The localized algebra R_{f_j} is the same as $C(\overline{D_j})_{f_j}$ and thus the induced module E_{f_j} is free (of rank one). The modules $E_i = E \otimes_R R_{f_i}$ are free submodules of $R_{f_i}^2$ and the induced modules on $R_{f_i f_j}$ are the same. But since E is not free they do not belong to the image of u and the sequence (28) is not exact in this case.

To obtain a local \mathbb{Z} -functor one has to implement a more refined definition of the rank which requires that for any prime ideal \mathfrak{p} of R the induced module on the residue field of R at \mathfrak{p} is a vector space of dimension k .

3.1.2 Open \mathbb{Z} -subfunctors.

The \mathbb{Z} -functor associated to an affine scheme $\text{Spec} A$ ($A \in \text{obj}(\mathfrak{Ring})$) is defined by

$$\mathbf{spec} A : \mathfrak{Ring} \rightarrow \mathfrak{Sets}, \quad \mathbf{spec} A(R) = \text{Hom}_{\mathbb{Z}}(\text{Spec} R, \text{Spec} A) \simeq \text{Hom}_{\mathbb{Z}}(A, R).$$

The open sets of an affine scheme are in general *not* affine and they provide interesting examples of schemes. The subfunctor of $\mathbf{spec} A$

$$\text{Hom}_{\mathbb{Z}}(\text{Spec} R, D(J)) \subset \text{Hom}_{\mathbb{Z}}(\text{Spec} R, \text{Spec} A)$$

associated to the open set $D(J) \subset \text{Spec}(A)$ (for a given ideal $J \subset A$) has the following explicit description

$$\underline{D}(J) : \mathfrak{Ring} \rightarrow \mathfrak{Sets}, \quad \underline{D}(J)(R) = \{\rho \in \text{Hom}_{\mathbb{Z}}(A, R) \mid \rho(J)R = R\}.$$

This follows from the fact that $\text{Spec}(\rho)^{-1}(D(J)) = D(\rho(J)R)$. In general, we say that \mathcal{U} is a subfunctor of a functor $\mathcal{F} : \mathfrak{Ring} \rightarrow \mathfrak{Sets}$ if for each ring R , $\mathcal{U}(R)$ is a subset of $\mathcal{F}(R)$ (with the natural compatibility for the maps).

DEFINITION 3.4. *Let \mathcal{U} be a subfunctor of $\mathcal{F} : \mathfrak{Ring} \rightarrow \mathfrak{Sets}$. One says that \mathcal{U} is open if for any ring A and any natural transformation $\phi : \mathbf{spec} A \rightarrow \mathcal{F}$, the subfunctor of $\mathbf{spec} A$ inverse image of \mathcal{U} by ϕ*

$$\phi^{-1}(\mathcal{U}) : \mathfrak{Ring} \rightarrow \mathfrak{Sets}, \quad \phi^{-1}(\mathcal{U})(R) = \{x \in \mathbf{spec} A(R) \mid \phi(x) \in \mathcal{U}(R) \subset \mathcal{F}(R)\}$$

is of the form $\underline{D}(J)$, for some open set $D(J) \subset \text{Spec}(A)$.

Equivalently, using Yoneda's Lemma, the above definition can be expressed by saying that, given any ring A and an element $z \in \mathcal{F}(A)$, there exists an ideal $J \subset A$ such that, for any $\rho \in \text{Hom}(A, R)$

$$(29) \quad \mathcal{F}(\rho)(z) \in \mathcal{U}(R) \iff \rho(J)R = R.$$

For any open subset $Y \subset X$ of a scheme X the subfunctor

$$\text{Hom}_{\mathbb{Z}}(\text{Spec} R, Y) \subset \text{Hom}_{\mathbb{Z}}(\text{Spec} R, X)$$

is open, and all open subfunctors of \underline{X} arise in this way.

EXAMPLE 3.5. We consider the projective line \mathbb{P}^1 identified with $X = \text{Gr}(1, 2)$. Let $\mathcal{U} \subset X$ be the subfunctor described, on a ring R , by the collection of all submodules of rank one of R^2 which are supplements of the submodule $P = \{(0, y) | y \in R\} \subset R^2$. Let p_1 be the projection on the first copy of R , then:

$$\mathcal{U}(R) = \{E \in \text{Gr}(1, 2) | p_{1|E} \text{ isomorphism}\}.$$

Proving that \mathcal{U} is open is equivalent, using (29), to find for any ring A and $E \in X(A)$ an ideal $J \subset A$ such that for any ring R and $\rho : A \rightarrow R$ one has

$$(30) \quad p_{1|E \otimes_A R} \text{ isomorphism} \iff R = \rho(J)R.$$

It is easy to see that the ideal J given by the annihilator of the cokernel of $p_{1|E}$ satisfies (30) (cf. [DG] Chapter I, Example 3.9).

3.1.3 Covering by \mathbb{Z} -subfunctors.

To motivate the definition of a covering of a \mathbb{Z} -functor, we start by describing the case of an affine scheme. Let \underline{X} be the \mathbb{Z} -functor

$$(31) \quad \underline{X} : \mathfrak{Ring} \rightarrow \mathfrak{Sets}, \quad \underline{X}(R) = \text{Hom}(A, R)$$

that is associated to the affine scheme $\text{Spec}(A)$. We have seen that the open subfunctors $\underline{D}(I) \subset \underline{X}$ correspond to ideals $I \subset A$ with

$$\underline{D}(I)(R) = \{\rho \in \text{Hom}(A, R) | \rho(I)R = R\}.$$

The condition that the open sets $\underline{D}(I_\alpha)$ ($\alpha \in I = \text{index set}$) form a covering of $\text{Spec}(A)$ is expressed algebraically by the equality $\sum_{\alpha \in I} I_\alpha = A$. We want to describe this condition in terms of the open subfunctors $\underline{D}(I_\alpha)$.

LEMMA 3.6. *Let \underline{X} be as in (31). Then $\sum_{\alpha \in I} I_\alpha = A$ if and only if for any field K one has*

$$\underline{X}(K) = \bigcup_{\alpha \in I} \underline{D}(I_\alpha)(K).$$

PROOF. Assume first that $\sum_{\alpha \in I} I_\alpha = A$ (a finite sum) i.e. $1 = \sum_{\alpha} a_\alpha$, with $a_\alpha \in I_\alpha$. Let K be a field, then for $\rho \in \text{Hom}(A, K)$, one has $\rho(a_\alpha) \neq 0$ for some $\alpha \in I$. Then $\rho(a_\alpha)K = K$, i.e. $\rho \in \underline{D}(I_\alpha)(K)$ so that the union of all $\underline{D}(I_\alpha)(K)$ is $\underline{X}(K)$.

Conversely, assume that $\sum_{\alpha} I_\alpha \neq A$. Then there exists a prime ideal $\mathfrak{p} \subset A$ containing all I_α 's. Let K be the field of fractions of A/\mathfrak{p} and let $\rho : A \rightarrow K$ be the natural homomorphism. One has $I_\alpha \subset \text{Ker} \rho$, thus $\rho \notin \bigcup_{\alpha} \underline{D}(I_\alpha)(K)$. \square

Notice that when R is neither a field or a local ring, the equality $\underline{X}(R) = \bigcup_{\alpha} \underline{D}(I_\alpha)(R)$ cannot be expected. In fact the range of a morphism $\rho \in \text{Hom}(\text{Spec}(R), \text{Spec } A) = \underline{X}(R)$ may not be contained in a single open set of the covering of $\text{Spec}(A)$ by the $\underline{D}(I_\alpha)$ so that ρ belongs to none of the $\underline{D}(I_\alpha)(R) = \text{Hom}(\text{Spec}(R), \underline{D}(I_\alpha))$.

DEFINITION 3.7. Let \underline{X} be a \mathbb{Z} -functor. Let $\{\underline{X}_\alpha\}_{\alpha \in I}$ be a family of open subfunctors of \underline{X} . Then, we say that the set $\{\underline{X}_\alpha\}_{\alpha \in I}$ form a covering of \underline{X} if for any field K one has

$$\underline{X}(K) = \bigcup_{\alpha \in I} \underline{X}_\alpha(K).$$

For affine schemes, one recovers the usual notion of an open cover. In fact, any open cover of an affine scheme admits a finite subcover. Indeed, the condition is $\sum_{\alpha} I_{\alpha} = A$ and if it holds one gets $1 = \sum_{\alpha \in F} a_{\alpha}$ for some *finite* subset of indices $F \subset I$. For an arbitrary scheme this finiteness condition may *not* hold. However, since a scheme is always “locally affine”, one can say, calling “quasi-compact” the above finiteness condition, that any scheme is locally quasi-compact.

To conclude this short review of the basic properties of schemes viewed as \mathbb{Z} -functors, we quote the main theorem which allows one to consider a scheme as a local and locally representable \mathbb{Z} -functor.

THEOREM 3.8. The \mathbb{Z} -functors of the form \underline{X} , for X a scheme over $\text{Spec } \mathbb{Z}$ are the \mathbb{Z} -functors which are local and admit an open cover by representable subfunctors.

PROOF. cf. [DG] Chapter I, §1, 4.4. □

3.2 Monoids: the category $\mathfrak{M}\mathfrak{o}$.

We recall that $\mathfrak{M}\mathfrak{o}$ denotes the category of commutative ‘pointed’ monoids $M \cup \{0\}$, i.e. M is a semigroup with a commutative multiplicative operation ‘ \cdot ’ (for simplicity we shall use the notation xy to denote the product $x \cdot y$ in $M \cup \{0\}$) and an identity element 1. Moreover, 0 is an absorbing element in M i.e. $0 \cdot x = x \cdot 0 = 0$, $\forall x \in M$.

The morphisms in $\mathfrak{M}\mathfrak{o}$ are unital homomorphisms of monoids $\varphi : M \rightarrow N$ ($\varphi(1_M) = 1_N$) satisfying the condition $\varphi(0) = 0$.

We also recall (cf. [Gi] p. 3) that an ideal I of a monoid M is a non-empty subset $I \subset M$ such that $I \supseteq xI = \{xi | i \in I\}$ for each $x \in M$. An ideal $I \subset M$ is *prime* if it is a proper ideal $I \subsetneq M$ and $xy \in I \implies x \in I$ or $y \in I \forall x, y \in M$. Equivalently, a proper ideal $\mathfrak{p} \subsetneq M$ is prime if and only if $\mathfrak{p}^c := M \setminus \mathfrak{p}$ is a multiplicative subset of M , i.e. $x \notin \mathfrak{p}, y \notin \mathfrak{p} \implies xy \notin \mathfrak{p}$.

It is a standard fact that the pre-image of a prime ideal by a morphism of monoids is a prime ideal. Moreover, it is also straightforward to verify that the complement $\mathfrak{p}_M = (M^\times)^c$ of the set of invertible elements in a monoid M is a prime ideal in M which contains all other prime ideals of the monoid. This interesting fact points out to one of the main properties that characterize monoids, namely monoids are local algebraic structures.

We recall that the smallest ideal containing a collection of ideals $\{I_\alpha\}$ of a monoid M is the union $I = \cup_{\alpha} I_{\alpha}$.

If $I \subset M$ is an ideal of a monoid M , the relation \sim on M defined by

$$x \sim y \Leftrightarrow x = y \text{ or } x, y \in I$$

is an example of a *congruence* on M , i.e. an equivalence relation on M which is compatible with the product, (cf. [Gr], §1 Proposition 4.6). The quotient monoid

$M/I := M/\sim$ (Rees quotient) is identifiable with the pointed monoid $(M \setminus I) \cup \{0\}$, with the operation defined as follows

$$x \star y = \begin{cases} xy, & \text{if } xy \notin I, \\ 0, & \text{if } xy \in I. \end{cases}$$

Another interesting example of congruence in a monoid is provided by the operation of *localization* at a multiplicative subset $S \subset M$. One considers the congruence \sim on the submonoid $M \times S \subset M \times M$ generated by the relation

$$(m, s) \sim (m', s') \Leftrightarrow \exists u \in S \quad ums' = um's.$$

By introducing the symbol $m/s = (m, s)$, one can easily check that the product $(m/s).(m'/s') = mm'/ss'$ is well-defined on the quotient monoid $S^{-1}M = (M \times S)/\sim$. Assuming $1 \in S$ and $0 \notin S$ one has $0/1 \neq 1/1$ in $S^{-1}M$. A particular case of this construction is when, for $f \in M$, one considers the multiplicative set $S = \{f^n; n \in \mathbb{Z}_{>0}\}$: in analogy with rings, the corresponding quotient monoid $S^{-1}M$ is usually denoted by M_f . It is non-zero except when f is nilpotent. When $f^n \neq 0$ for all $n > 0$, the equality

$$\mathfrak{p}(f) = \{x \in M \mid xM \cap \{f^n \mid n > 0\} = \emptyset\}$$

defines a prime ideal $\mathfrak{p}(f)$ of M and the construction of M_f is a special case of the following localization $M \rightarrow M_{\mathfrak{p}}$ of M at any prime ideal \mathfrak{p} . By definition $M_{\mathfrak{p}}$ is $S^{-1}M$ where $S = \mathfrak{p}^c$ is the complement of \mathfrak{p} . One has $0 \neq 1$ in $M_{\mathfrak{p}}$ for all prime ideals \mathfrak{p} .

For an ideal $I \subset M$, the set $D(I) = \{\mathfrak{p} \subset M \mid \mathfrak{p} \text{ prime ideal, } \mathfrak{p} \not\supseteq I\}$ determines an open set for the natural topology on the set $\text{Spec}(M) = \{\mathfrak{p} \subset M \mid \mathfrak{p} \text{ prime ideal}\}$ (cf. [Ka]). For $I = \cup_{\alpha} I_{\alpha}$ ($\{I_{\alpha}\}$ a collection of ideals), the corresponding open set $D(I)$ satisfies the property $D(\cup_{\alpha} I_{\alpha}) = \cup_{\alpha} D(I_{\alpha})$.

The following equivalent statements characterize the open subsets $D(I) \subset \text{Spec}(M)$.

PROPOSITION 3.9. *Let $\rho : M \rightarrow N$ be a morphism in the category \mathfrak{Mo} and let $I \subset M$ be an ideal. Then, the following conditions are equivalent:*

- (1) $\rho(I)N = N$.
- (2) $1 \in \rho(I)N$.
- (3) $\rho^{-1}((N^{\times})^c)$ is a prime ideal belonging to $D(I)$.
- (4) $\rho^{-1}(\mathfrak{p}) \in D(I)$, for any prime ideal $\mathfrak{p} \subset N$.

PROOF. One has (1) \Leftrightarrow (2). Moreover, $\rho^{-1}((N^{\times})^c) \not\supseteq I$ if and only if $\rho(I) \cap N^{\times} \neq \emptyset$ which is equivalent to (1). Thus (2) \Leftrightarrow (3).

If an ideal $J \subset M$ does not contain I , then the same holds obviously for all the sub-ideals of J . Then (3) \Rightarrow (4) since $\mathfrak{p}_N = (N^{\times})^c$ contains all the prime ideals of N . Taking $\mathfrak{p} = \mathfrak{p}_N$ one gets (4) \Rightarrow (3). \square

The proof of the following lemma is straightforward (cf. [Gi]).

LEMMA 3.10. *Given an ideal $I \subset M$, the intersection of the prime ideals $\mathfrak{p} \subset M$, such that $\mathfrak{p} \supset I$ coincides with the radical of I*

$$\bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \sqrt{I} := \{x \in M \mid \exists n \in \mathbb{N}, x^n \in I\}.$$

Given a commutative group H , the following definition determines a pointed monoid in $\mathfrak{M}\mathfrak{o}$

$$\mathbb{F}_1[H] := H \cup \{0\} \quad (0 \cdot h = h \cdot 0 = 0, \quad \forall h \in H).$$

Thus, in $\mathfrak{M}\mathfrak{o}$ a monoid of the form $\mathbb{F}_1[H]$ corresponds to a field F ($F = F^\times \cup \{0\}$) in the category of commutative rings with unit. It is elementary to verify that the collection of monoids like $\mathbb{F}_1[H]$, for H an abelian group, forms a full subcategory of $\mathfrak{M}\mathfrak{o}$ isomorphic to the category $\mathfrak{A}\mathfrak{b}$ of abelian groups.

In view of the fact that monoids are local algebraic structures, one can also introduce a notion which corresponds to that of the residue field for local rings and related homomorphism. For a commutative monoid M , one defines the pair $(\mathbb{F}_1[M^\times], \epsilon)$ where ϵ is the natural homomorphism

$$(32) \quad \epsilon : M \rightarrow \mathbb{F}_1[M^\times] \quad \epsilon(y) = \begin{cases} 0, & \text{if } y \notin M^\times \\ y, & \text{if } y \in M^\times. \end{cases}$$

The non-invertible elements of M form a prime ideal, thus ϵ is a multiplicative map. The following lemma describes an application of this idea

LEMMA 3.11. *Let M be a commutative monoid and $\mathfrak{p} \subset M$ a prime ideal. Then*

- a) $\mathfrak{p}M_{\mathfrak{p}} \cap (M_{\mathfrak{p}})^\times = \emptyset$.
- b) *There exists a unique homomorphism $\epsilon_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow \mathbb{F}_1[(M_{\mathfrak{p}})^\times]$ such that*
 - $\epsilon_{\mathfrak{p}}(y) = 0, \forall y \in \mathfrak{p}$
 - $\epsilon_{\mathfrak{p}}(y) = y, \forall y \in (M_{\mathfrak{p}})^\times$.

PROOF. a) If $j \in \mathfrak{p}$ then the image of j in $M_{\mathfrak{p}}$ cannot be invertible, since this would imply an equality of the form $sja = sf$ for some $s \notin \mathfrak{p}, f \notin \mathfrak{p}$ and hence a contradiction.

b) The first statement a) shows that the corresponding (multiplicative) map $\epsilon_{\mathfrak{p}}$ fulfills the two conditions. To check uniqueness, note that the two conditions suffice to determine $\epsilon_{\mathfrak{p}}(y)$ for any $y = a/f$ with $a \in M$ and $f \notin \mathfrak{p}$. \square

3.3 Geometric monoidal spaces.

In this subsection we review the construction of the geometric spaces which generalize, in the categorical context of the commutative monoids, the classical theory of the geometric \mathbb{Z} -schemes that we have reviewed in §3.1. We refer to § 9 in [Ka], [D1] and [D2] for further details.

A geometric monoidal space (X, \mathcal{O}_X) is a topological space X endowed with a sheaf of monoids \mathcal{O}_X (the structural sheaf). Unlike the case of the geometric \mathbb{Z} -schemes (cf. [DG], Chapter I, §1 Definition 1.1), there is no need to impose the condition that the stalks of the structural sheaf of a geometric monoidal space are local algebraic structures, since *by construction* any monoid is endowed with this property.

A morphism $\varphi : X \rightarrow Y$ of geometric monoidal spaces is a pair $(\varphi, \varphi^\sharp)$ of a continuous map $\varphi : X \rightarrow Y$ of topological spaces and a homomorphism of sheaves of monoids $\varphi^\sharp : \mathcal{O}_Y \rightarrow \varphi_*\mathcal{O}_X$ which satisfies the property of being *local*, i.e. $\forall x \in X$ the homomorphisms connecting the stalks $\varphi_x^\sharp : \mathcal{O}_{Y, \varphi(x)} \rightarrow \mathcal{O}_{X, x}$ are local, i.e. they fulfill the following definition (cf. [D1])

DEFINITION 3.12. *A homomorphism $\rho : M_1 \rightarrow M_2$ of monoids is local if the following property holds*

$$(33) \quad \rho^{-1}(M_2^\times) = M_1^\times.$$

This locality condition can be equivalently phrased by either one of the following statements

- (1) $\rho^{-1}((M_2^\times)^c) = (M_1^\times)^c$
- (2) $\rho((M_1^\times)^c) \subset (M_2^\times)^c$.

The equivalence of (33) and (1) is clear since $\rho^{-1}(S^c) = \rho^{-1}(S)^c$, for any subset $S \subset M_2$. Clearly (1) implies (2). Conversely, if (2) holds one has $\rho^{-1}((M_2^\times)^c) \supset (M_1^\times)^c$ and using $\rho^{-1}(M_2^\times) \supset M_1^\times$ one gets (1).

We shall denote by \mathfrak{GS} the category of the geometric monoidal spaces.

Notice that by construction the morphism $\epsilon_{\mathfrak{p}}$ of Lemma 3.11 *b)* is *local*. Thus it is natural to consider, for any geometric monoidal space (X, \mathcal{O}_X) , the analogue of the residue field at a point $x \in X$ to be $\kappa(x) = \mathbb{F}_1[\mathcal{O}_{X,x}^\times]$. Then, the associated evaluation map

$$(34) \quad \epsilon_x : \mathcal{O}_{X,x} \rightarrow \kappa(x) = \mathbb{F}_1[\mathcal{O}_{X,x}^\times]$$

satisfies the properties as in *b)* of Lemma 3.11.

For a pointed monoid M in \mathfrak{Mo} , the set $\text{Spec}(M)$ of the prime ideals $\mathfrak{p} \subset M$ is called the *prime spectrum* of M and is endowed with the topology whose closed subsets are the

$$V(I) = \{\mathfrak{p} \in \text{Spec}(M) \mid \mathfrak{p} \supset I\}$$

as I varies among the collection of all ideals of M . Likewise for rings, the subset $V(I) \subset \text{Spec}(M)$ depends only upon the radical of I (*cf.* [B] II, Chpt. 2, §3). Equivalently, one can characterize the topology on $\text{Spec}(M)$ in terms of a basis of open sets of the form $D(fM) = \{\mathfrak{p} \in \text{Spec}(M) \mid f \notin \mathfrak{p}\}$, as f varies in M .

The sheaf \mathcal{O} of monoids associated to $\text{Spec}(M)$ is determined by the following properties:

- The stalk of \mathcal{O} at $\mathfrak{p} \in \text{Spec}(M)$ is $\mathcal{O}_{\mathfrak{p}} = S^{-1}M$, with $S = \mathfrak{p}^c$.
- Let U be an open set of $\text{Spec}(M)$, then a section $s \in \Gamma(U, \mathcal{O})$ is an element of $\prod_{\mathfrak{p} \in U} \mathcal{O}_{\mathfrak{p}}$ such that its restriction $s|_{D(fM)}$ to any open $D(fM) \subset U$ agrees with an element of M_f .
- The homomorphism of monoids $\varphi : M_f \rightarrow \Gamma(D(fM), \mathcal{O})$

$$\varphi(x)(\mathfrak{p}) = a/f^n \in \mathcal{O}_{\mathfrak{p}}, \quad \forall \mathfrak{p} \in D(fM), \quad \forall x = a/f^n \in M_f$$

is an isomorphism.

Note that $D(fM)$ is non-empty when f is not nilpotent, and in that case it contains the prime ideal $\mathfrak{p}(f)$ defined above. Moreover the stalk of \mathcal{O} at $\mathfrak{p}(f)$ is isomorphic to M_f .

For any monoidal geometric space (X, \mathcal{O}_X) one has a canonical morphism $\psi_X : X \rightarrow \text{Spec}(\Gamma(X, \mathcal{O}_X))$, $\psi_X(x) = \mathfrak{p}_x$, such that $s(x) = 0$ in $\mathcal{O}_{X,x}$, $\forall s \in \mathfrak{p}_x$. It is easy to verify that a monoidal geometric space (X, \mathcal{O}_X) is a *prime spectrum* if and only if the morphism ψ_X is an isomorphism.

DEFINITION 3.13. *A monoidal geometric space (X, \mathcal{O}_X) that admits an open cover by prime spectra $\text{Spec}(M)$ is called a geometric $\mathfrak{M}\mathfrak{o}$ -scheme.*

Prime spectra fulfill the following locality property (cf. [D1]) that will be considered again in §3.4 in the functorial definition of an $\mathfrak{M}\mathfrak{o}$ -scheme.

LEMMA 3.14. *Let M be an object in $\mathfrak{M}\mathfrak{o}$ and let $\{W_\alpha\}_{\alpha \in I}$ be an open cover of the topological space $X = \text{Spec}(M)$. Then $W_\alpha = \text{Spec}(M)$, for some index $\alpha \in I$.*

PROOF. The point $\mathfrak{p}_M = (M^\times)^c \in \text{Spec}(M)$ must belong to some open set W_α , hence $\mathfrak{p}_M \in D(I_\alpha)$ for some index $\alpha \in I$ and this is equivalent to $I_\alpha \cap M^\times \neq \emptyset$, i.e. $I_\alpha = M$. \square

3.4 $\mathfrak{M}\mathfrak{o}$ -schemes.

In analogy to and generalizing the theory of \mathbb{Z} -schemes, one develops the theory of $\mathfrak{M}\mathfrak{o}$ -schemes following both the functorial and the geometrical viewpoint.

3.4.1 $\mathfrak{M}\mathfrak{o}$ -functors.

DEFINITION 3.15. *An $\mathfrak{M}\mathfrak{o}$ -functor is a covariant functor $\mathcal{F} : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}$ from commutative (pointed) monoids to sets.*

To a (pointed) monoid M in $\mathfrak{M}\mathfrak{o}$ one associates the $\mathfrak{M}\mathfrak{o}$ -functor

$$\mathbf{spec} M : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s} \quad \mathbf{spec} M(N) = \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, N).$$

Notice that by applying Yoneda's lemma, a morphism of $\mathfrak{M}\mathfrak{o}$ -functors (natural transformation) such as $\varphi : \mathbf{spec} M \rightarrow \mathcal{F}$ is completely determined by the element $\varphi(id_M) \in \mathcal{F}(M)$ and moreover any such element gives rise to a morphism $\mathbf{spec} M \rightarrow \mathcal{F}$. By applying this fact to the functor $\mathcal{F} = \mathbf{spec} N$, for $N \in \text{obj}(\mathfrak{M}\mathfrak{o})$, one obtains an *inclusion* of $\mathfrak{M}\mathfrak{o}$ as a full subcategory of the category of $\mathfrak{M}\mathfrak{o}$ -functors (where morphisms are natural transformations).

An ideal $I \subset M$ defines the sub- $\mathfrak{M}\mathfrak{o}$ -functor $\underline{D}(I) \subset \mathbf{spec} M$

$$\underline{D}(I) : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}, \quad \underline{D}(I)(N) = \{\rho \in \mathbf{spec}(M)(N) \mid \rho(I)N = N\}.$$

Automatic locality.

We recall (cf. §3.2) that for \mathbb{Z} -functors the ‘‘locality’’ property is defined by requiring, on coverings of prime spectra $\text{Spec}(R)$ by open sets $D(f_i)$ of a basis, the exactness of sequences such as (27) and (28). The next lemma shows that locality is automatically verified for any $\mathfrak{M}\mathfrak{o}$ -functor.

First of all, notice that for any $\mathfrak{M}\mathfrak{o}$ -functor \mathcal{F} and any monoid M one has a sequence of maps of sets

$$(35) \quad \mathcal{F}(M) \xrightarrow{u} \prod_{i \in I} \mathcal{F}(M_{f_i}) \xrightleftharpoons[w]{v} \prod_{i, j \in I} \mathcal{F}(M_{f_i f_j})$$

that is obtained by using the open covering of $\text{Spec}(M)$ by the open sets $D(f_i M)$ of a basis ($I =$ finite index set) and the natural homomorphisms $M \rightarrow M_{f_i}$, $M_{f_i} \rightarrow M_{f_i f_j}$.

LEMMA 3.16. *For any $\mathfrak{M}\mathfrak{o}$ -functor \mathcal{F} the sequence (35) is exact.*

PROOF. By Proposition 2.18, there exists an index $i \in I$ such that $f_i \in M^\times$. We may also assume that $i = 1$. Then, the homomorphism $M \rightarrow M_{f_1}$ is invertible, thus u is injective. Let $(x_i) \in \prod_i \mathcal{F}(M_{f_i})$ be a family, with $x_i \in \mathcal{F}(M_{f_i})$ and such that $v(x_i) = (x_i)_{f_j} = (x_j)_{f_i} = w(x_i)$, for all $i, j \in I$. This gives in particular the equality between the image of $x_i \in \mathcal{F}(M_{f_i})$ under the isomorphism $\mathcal{F}(\rho_{i1}) : \mathcal{F}(M_{f_i}) \rightarrow \mathcal{F}(M_{f_i f_1})$ and $\mathcal{F}(\rho_{i1})(x_1) \in \mathcal{F}(M_{f_i f_1})$. By writing $x_1 = \rho_1(x)$ one finds that $u(x)$ is equal to the family (x_i) . \square

3.4.2 Open $\mathfrak{M}\mathfrak{o}$ -subfunctors.

In exact analogy with the theory of \mathbb{Z} -schemes (cf. §3.1.2), we introduce the notion of open subfunctors of $\mathfrak{M}\mathfrak{o}$ -functors.

DEFINITION 3.17. *We say that a subfunctor $\mathcal{G} \subset \mathcal{F}$ of an $\mathfrak{M}\mathfrak{o}$ -functor \mathcal{F} is open if for any object M of $\mathfrak{M}\mathfrak{o}$ and any morphism of $\mathfrak{M}\mathfrak{o}$ -functors $\varphi : \mathbf{spec} M \rightarrow \mathcal{F}$ there exists an ideal $I \subset M$ satisfying the following property:*

For any object N of $\mathfrak{M}\mathfrak{o}$ and for any $\rho \in \mathbf{spec} M(N) = \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, N)$ one has

$$(36) \quad \varphi(\rho) \in \mathcal{G}(N) \subset \mathcal{F}(N) \Leftrightarrow \rho(I)N = N.$$

To clarify the meaning of the above definition we develop a few examples.

EXAMPLE 3.18. The functor

$$\mathcal{G} : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}, \quad \mathcal{G}(N) = N^\times$$

is an open subfunctor of the (identity) functor \mathcal{D}^1

$$\mathcal{D}^1 : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}, \quad \mathcal{D}^1(N) = N.$$

In fact, let M be a monoid, then by Yoneda's lemma a morphism of functors $\varphi : \mathbf{spec} M \rightarrow \mathcal{D}^1$ is determined by an element $z \in \mathcal{D}^1(M) = M$. For any monoid N and $\rho \in \text{Hom}(M, N)$, one has $\varphi(\rho) = \rho(z) \in \mathcal{D}^1(N) = N$, thus the condition $\varphi(\rho) \in \mathcal{G}(N) = N^\times$ means that $\rho(z) \in N^\times$. One takes for I the ideal generated by z in M : $I = zM$. Then, it is straightforward to check that (36) is fulfilled.

EXAMPLE 3.19. We start with a monoid M and an ideal $I \subset M$ and define the following sub- $\mathfrak{M}\mathfrak{o}$ -functor of $\mathbf{spec}(M)$

$$\underline{D}(I) : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}, \quad \underline{D}(I)(N) = \{\rho \in \text{Hom}(M, N) \mid \rho(I)N = N\}.$$

This means that for all prime ideals $\mathfrak{p} \subset N$, one has $\rho^{-1}(\mathfrak{p}) \not\supset I$ (cf. Proposition 3.9). Next, we show that $\underline{D}(I)$ defines an open subfunctor of $\mathbf{spec} M$. Indeed, for any object A of $\mathfrak{M}\mathfrak{o}$ and any natural transformation $\varphi : \mathbf{spec} A \rightarrow \mathbf{spec} M$ one has $\varphi(\text{id}_A) = \eta \in \mathbf{spec} M(A) = \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, A)$; we can take in A the ideal $J = \eta(I)A$. This ideal fulfills the condition (36) for any object N of $\mathfrak{M}\mathfrak{o}$ and any $\rho \in \text{Hom}_{\mathfrak{M}\mathfrak{o}}(A, N)$. In fact, one has $\varphi(\rho) = \rho \circ \eta \in \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, N)$ and $\varphi(\rho) \in \underline{D}(I)(N)$ means that $\rho(\eta(I))N = N$. This holds if and only if $\rho(J)N = N$.

3.4.3 Open covering by $\mathfrak{M}\mathfrak{o}$ -subfunctors.

There is a natural generalization of the notion of open cover for $\mathfrak{M}\mathfrak{o}$ -functors. We recall that the category $\mathfrak{A}\mathfrak{b}$ of abelian groups embeds as a full subcategory of $\mathfrak{M}\mathfrak{o}$ by means of the functor $H \rightarrow \mathbb{F}_1[H]$.

DEFINITION 3.20. Let \mathcal{F} be an $\mathfrak{M}\mathfrak{o}$ -functor and let $\{\mathcal{F}_\alpha\}_{\alpha \in I}$ ($I =$ an index set) be a family of open subfunctors of \mathcal{F} . One says that $\{\mathcal{F}_\alpha\}_{\alpha \in I}$ is an open cover of \mathcal{F} if

$$(37) \quad \mathcal{F}(\mathbb{F}_1[H]) = \bigcup_{\alpha \in I} \mathcal{F}_\alpha(\mathbb{F}_1[H]), \quad \forall H \in \text{Obj}(\mathfrak{Ab}).$$

Since commutative groups (with a zero-element) replace fields in $\mathfrak{M}\mathfrak{o}$, the above definition is the natural generalization of the definition of open covers for \mathbb{Z} -functors (cf. [DG]) within the category of $\mathfrak{M}\mathfrak{o}$ -functors. The following proposition gives a precise characterization of the properties of the open covers of an $\mathfrak{M}\mathfrak{o}$ -functor.

PROPOSITION 3.21. Let \mathcal{F} be an $\mathfrak{M}\mathfrak{o}$ -functor and let $\{\mathcal{F}_\alpha\}_{\alpha \in I}$ be a family of open subfunctors of \mathcal{F} . Then, the family $\{\mathcal{F}_\alpha\}_{\alpha \in I}$ forms an open cover of \mathcal{F} if and only if

$$\mathcal{F}(M) = \bigcup_{\alpha \in I} \mathcal{F}_\alpha(M), \quad \forall M \in \text{obj}(\mathfrak{M}\mathfrak{o}).$$

PROOF. The condition is obviously sufficient. To show the converse, we assume (37). Let M be a pointed monoid and let $\xi \in \mathcal{F}(M)$, one needs to show that $\xi \in \mathcal{F}_\alpha(M)$ for some $\alpha \in I$. Let $\varphi : \mathbf{spec} M \rightarrow \mathcal{F}$ be the morphism of functors with $\varphi(\text{id}_M) = \xi$. Since each \mathcal{F}_α is an open subfunctor of \mathcal{F} , one can find ideals $I_\alpha \subset M$ such that for any object N of $\mathfrak{M}\mathfrak{o}$ and for any $\rho \in \mathbf{spec} M(N) = \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, N)$ one has

$$(38) \quad \varphi(\rho) \in \mathcal{F}_\alpha(N) \subset \mathcal{F}(N) \Leftrightarrow \rho(I_\alpha)N = N.$$

One applies this to the morphism $\epsilon_M : M \rightarrow \mathbb{F}_1[M^\times] = \kappa$ as in (32). One has $\epsilon_M \in \mathbf{spec}(M)(\kappa)$ and $\varphi(\epsilon_M) \in \mathcal{F}(\kappa) = \bigcup_{\alpha \in I} \mathcal{F}_\alpha(\kappa)$. Thus, $\exists \alpha \in I$ such that $\varphi(\epsilon_M) \in \mathcal{F}_\alpha(\kappa)$. By (38) one concludes that $\epsilon_M(I_\alpha)\kappa = \kappa$ and $I_\alpha \cap M^\times \neq \emptyset$ hence $I_\alpha = M$. Applying then (38) to $\rho = \text{id}_M$ one obtains $\xi \in \mathcal{F}_\alpha(M)$ as required. \square

For $\mathcal{F} = \mathbf{spec} M$ and the $\mathcal{F}_\alpha = \underline{D}(I_\alpha)$ open subfunctors corresponding to ideals $I_\alpha \subset M$, the covering condition in Definition 3.20 is equivalent to state that $\exists \alpha \in I$ such that $I_\alpha = M$. In fact, one takes $H = M^\times$ and $\epsilon : M \rightarrow \mathbb{F}_1[M^\times] = \kappa$. Then, $\epsilon \in \mathbf{spec} M(\mathbb{F}_1[H])$ and $\exists \alpha, \epsilon \in \underline{D}(I_\alpha)(\mathbb{F}_1[H])$ and thus $I_\alpha \cap M^\times \neq \emptyset$ hence $I_\alpha = M$. Let X be a geometric monoidal space and let $U_\alpha \subset X$ be (a family of) open subsets ($\alpha \in I$). One introduces the following $\mathfrak{M}\mathfrak{o}$ -functors

$$(39) \quad \underline{X}_\alpha : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{Sets}, \quad \underline{X}_\alpha(M) := \text{Hom}(\text{Spec}(M), U_\alpha).$$

Notice that $\underline{X}_\alpha(M) \subset \underline{X}(M) := \text{Hom}(\text{Spec}(M), X)$.

PROPOSITION 3.22. The following conditions are equivalent

- (1) $\underline{X} = \bigcup_{\alpha \in I} \underline{X}_\alpha$.
- (2) $X = \bigcup_{\alpha \in I} U_\alpha$.
- (3) $\underline{X}(M) = \bigcup_{\alpha \in I} \underline{X}_\alpha(M) \quad \forall M \in \text{obj}(\mathfrak{M}\mathfrak{o})$.

PROOF. (1) \implies (2). Assume that (2) fails and let $x \notin \bigcup_{\alpha} U_\alpha$. Then the local evaluation map $\epsilon_x : \mathcal{O}_{X,x} \rightarrow \kappa(x)$ of (34) determines a morphism of geometric monoidal spaces $\text{Spec}(\kappa(x)) \rightarrow X$ and for $M = \kappa(x)$ a corresponding element $\epsilon \in \underline{X}(M) = \text{Hom}(\text{Spec}(M), X)$. By applying Definition 3.20, there exists an

index α such that $\epsilon \in \underline{X}_\alpha(M)$ and this shows that $x \in U_\alpha$ so that the open sets U_α 's cover X .

(2) \implies (3). Let $\phi \in \underline{X}(M) = \text{Hom}(\text{Spec}(M), X)$. Then, with \mathfrak{p}_M the maximal ideal of M , one has $\phi(\mathfrak{p}_M) \in X = \bigcup_\alpha U_\alpha$ hence there exists an index α such that $\phi(\mathfrak{p}_M) \in U_\alpha$. It follows that $\phi^{-1}(U_\alpha) \ni \mathfrak{p}_M$ is $\text{Spec}(M)$, and one gets $\phi \in \underline{X}_\alpha(M) = \text{Hom}(\text{Spec}(M), U_\alpha)$.

The implication (3) \implies (1) is straightforward. \square

3.4.4 $\mathfrak{M}\mathfrak{o}$ -schemes.

In view of the fact that an $\mathfrak{M}\mathfrak{o}$ -functor is local, the definition of an $\mathfrak{M}\mathfrak{o}$ -scheme simply involves the local representability.

DEFINITION 3.23. *An $\mathfrak{M}\mathfrak{o}$ -scheme is an $\mathfrak{M}\mathfrak{o}$ -functor which admits an open cover by representable subfunctors.*

We shall consider several elementary examples of $\mathfrak{M}\mathfrak{o}$ -schemes

EXAMPLE 3.24. The affine space \mathcal{D}^n . For a fixed $n \in \mathbb{N}$, we consider the following $\mathfrak{M}\mathfrak{o}$ -functor

$$\mathcal{D}^n : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}, \quad \mathcal{D}^n(M) = M^n$$

This functor is representable since it is described by

$$\mathcal{D}^n(M) = \text{Hom}_{\mathfrak{M}\mathfrak{o}}(\mathbb{F}_1[T_1, \dots, T_n], M),$$

where

$$\mathbb{F}_1[T_1, \dots, T_n] := \{0\} \cup \{T_1^{a_1} \cdots T_n^{a_n} \mid a_j \in \mathbb{Z}_{\geq 0}\}$$

is the pointed monoid associated to the semi-group generated by the variables T_j .

EXAMPLE 3.25. The projective line \mathbb{P}^1 . We consider the $\mathfrak{M}\mathfrak{o}$ -functor \mathbb{P}^1 which associates to an object M of $\mathfrak{M}\mathfrak{o}$ the set $\mathbb{P}^1(M)$ of complemented submodules $E \subset M^2$ of rank one, where the rank is defined locally. By definition, a complemented submodule is the range of an idempotent matrix $e \in M_2(M)$ (i.e. $e^2 = e$) whose rows have *at most*⁵ one non-zero entry. To a morphism $\rho : M \rightarrow N$ in $\mathfrak{M}\mathfrak{o}$, one associates the following map

$$\mathbb{P}^1(\rho)(E) = N \otimes_M E \subset N^2.$$

In terms of projectors $\mathbb{P}^1(\rho)(e) = \rho(e) \in M_2(N)$. The condition of rank one means that for any prime ideal $\mathfrak{p} \in \text{Spec } M$ one has $\epsilon_{\mathfrak{p}}(e) \notin \{0, 1\}$ where $\epsilon_{\mathfrak{p}} : M \rightarrow \mathbb{F}_1[(M_{\mathfrak{p}})^\times]$ is the morphism of Lemma 3.11 b) (where $M_{\mathfrak{p}} = S^{-1}M$, with $S = \mathfrak{p}^c$).

Now, we compare \mathbb{P}^1 with the $\mathfrak{M}\mathfrak{o}$ -functor

$$\mathcal{P}(M) = M \cup_{M^\times} M$$

where the gluing map is given by $x \rightarrow x^{-1}$. In other words, we define on the disjoint union $M \cup M$ an equivalence relation given by (using the identification $M \times \{1, 2\} = M \cup M$)

$$(x, 1) \sim (x^{-1}, 2) \quad \forall x \in M^\times.$$

⁵Note that we need the 0-element to state this condition

We define a natural transformation $e : \mathcal{P} \rightarrow \underline{\mathbb{P}}^1$ by observing that the matrices

$$e_1(a) = \begin{pmatrix} 1 & 0 \\ a & 0 \end{pmatrix}, \quad e_2(b) = \begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix}, \quad a, b \in M$$

are idempotent ($e^2 = e$) and their ranges also fulfill the following property

$$\text{Im } e_1(a) = \text{Im } e_2(b) \iff ab = 1.$$

LEMMA 3.26. *The natural transformation e is bijective on the objects i.e.*

$$\mathcal{P}(M) = M \cup_{M \times} M \cong \underline{\mathbb{P}}^1(M).$$

Moreover, $\underline{\mathbb{P}}^1$ is covered by two copies of representable sub-functors \mathcal{D}^1 .

PROOF. We refer to [CC2] Lemma 3.13. □

EXAMPLE 3.27. Let M be a monoid and let $I \subset M$ be an ideal. Consider the $\mathfrak{M}\mathfrak{o}$ -functor $\underline{D}(I)$ of Example 3.19. The next proposition states that this functor is an $\mathfrak{M}\mathfrak{o}$ -scheme.

PROPOSITION 3.28. 1) *Let $f \in M$ and $I = fM$. Then the subfunctor $\underline{D}(I) \subset \mathbf{spec} M$ is represented by M_f .*

2) *For any ideal $I \subset M$, the $\mathfrak{M}\mathfrak{o}$ -functor $\underline{D}(I)$ is an $\mathfrak{M}\mathfrak{o}$ -scheme.*

PROOF. 1) For any monoid N and for $I = fM$, one has

$$\underline{D}(I)(N) = \{\rho \in \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, N) \mid \rho(f) \in N^\times\}.$$

The condition $\rho(f) \in N^\times$ means that ρ extends to a morphism $\tilde{\rho} \in \text{Hom}(M_f, N)$, by setting

$$\tilde{\rho}\left(\frac{m}{f^n}\right) = \rho(m)\rho(f)^{-n} \in N.$$

Thus one has a canonical and functorial isomorphism $\underline{D}(I)(N) \simeq \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M_f, N)$ which proves the representability of $\underline{D}(I)$ by M_f .

2) For any $f \in I$, the ideal $fM \subset I$ defines a subfunctor of $\underline{D}(fM) \subset \underline{D}(I)$. This sub-functor is open because it is already open in $\mathbf{spec} M$ and because there are less morphisms of type $\text{Spec}(A) \rightarrow \underline{D}(I)$ than those of type $\text{Spec}(A) \rightarrow \text{Spec}(M)$, as $\underline{D}(I)(A) \subset \mathbf{spec} M(A)$. Moreover, by 1), this subfunctor is representable. □

3.4.5 Geometric realization.

In this final subsection we describe the construction of the geometric realization of an $\mathfrak{M}\mathfrak{o}$ -functor (and scheme) following, and generalizing for commutative monoids, the exposition presented in [DG] §1 n. 4 of the geometric realization of a \mathbb{Z} -scheme for rings. Although the general development of this construction presents clear analogies with the case of rings, new features also arise which are specifically inherent to the discussion with monoids. The most important one is that the full sub-category \mathfrak{Ab} of $\mathfrak{M}\mathfrak{o}$ which plays the role of “fields” within monoids, admits a final object. This fact simplifies greatly the description of the geometric realization of an $\mathfrak{M}\mathfrak{o}$ -functor as we show in Proposition 3.32 and in Theorem 3.34.

An $\mathfrak{M}\mathfrak{o}$ -functor \mathcal{F} can be reconstructed by an inductive limit $\varinjlim \mathbf{spec}(M)$ of representable functors, and the geometric realization is then defined by the inductive limit $\varinjlim \mathbf{Spec}(M)$, *i.e.* by trading the $\mathfrak{M}\mathfrak{o}$ -functors $\mathbf{spec}(M)$ for the geometric monoidal spaces $(\mathbf{Spec}(M), \mathcal{O})$. However, some set-theoretic precautions are also needed since the inductive limits which are taken over pairs (M, ρ) , where $M \in \mathbf{obj}(\mathfrak{M}\mathfrak{o})$ and $\rho \in \mathcal{F}(M)$, are indexed over families rather than sets. Another issue arising in the construction is that of seeking that natural transformations of $\mathfrak{M}\mathfrak{o}$ -functors form a set. We bypass this problem by adopting the same caution as in [DG] (*cf.* Conventions g en erales). Thus, throughout this subsection we shall work with *models* of commutative monoids in a fixed suitable *universe* \mathbb{U} . This set up is accomplished by introducing the full subcategory $\mathfrak{M}\mathfrak{o}' \subset \mathfrak{M}\mathfrak{o}$ of models of commutative monoids in $\mathfrak{M}\mathfrak{o}$, *i.e.* of commutative (pointed) monoids whose underlying set is an element of the fixed universe \mathbb{U} . To lighten the notations and the statements we adopt the convention that all the geometric monoidal spaces considered here below only involve monoids in $\mathfrak{M}\mathfrak{o}'$, thus we shall not keep the distinction between the category $\mathfrak{M}\mathfrak{o}\mathfrak{S}$ of $\mathfrak{M}\mathfrak{o}$ -functors and the category $\mathfrak{M}\mathfrak{o}'\mathfrak{S}$ of (covariant) functors from $\mathfrak{M}\mathfrak{o}'$ to $\mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}$.

Given an $\mathfrak{M}\mathfrak{o}$ -functor $\mathcal{F} : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}$, we denote by $\mathcal{M}_{\mathcal{F}}$ the category of \mathcal{F} -*models*, that is the category whose objects are pairs (M, ρ) , where $M \in \mathbf{obj}(\mathfrak{M}\mathfrak{o}')$ and $\rho \in \mathcal{F}(M)$. A morphism $(M_1, \rho_1) \rightarrow (M_2, \rho_2)$ in $\mathcal{M}_{\mathcal{F}}$ is given by assigning a morphism $\varphi : M_1 \rightarrow M_2$ in $\mathfrak{M}\mathfrak{o}'$ such that $\varphi(\rho_1) = \rho_2 \in \mathcal{F}(M_2)$.

For a geometric monoidal space X , *i.e.* an object of the category $\mathfrak{S}\mathfrak{S}$, we recall the definition of the *functor defined by X* (*cf.* (39)). This is the $\mathfrak{M}\mathfrak{o}$ -functor

$$\underline{X} : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s} \quad \underline{X}(M) = \mathbf{Hom}_{\mathfrak{S}\mathfrak{S}}(\mathbf{Spec}(M), X).$$

This definition can of course be restricted to the subcategory $\mathfrak{M}\mathfrak{o}' \subset \mathfrak{M}\mathfrak{o}$ of models.

One also introduces the functor

$$d_{\mathcal{F}} : \mathcal{M}_{\mathcal{F}}^{op} \rightarrow \mathfrak{S}\mathfrak{S}, \quad d_{\mathcal{F}}(M, \rho) = \mathbf{Spec}(M)$$

DEFINITION 3.29. *The geometric realization of an $\mathfrak{M}\mathfrak{o}$ -functor \mathcal{F} is the geometric monoidal space defined by the inductive limit*

$$|\mathcal{F}| = \varinjlim_{(M, \rho) \in \mathcal{M}_{\mathcal{F}}} d_{\mathcal{F}}(M, \rho).$$

The functor $|\cdot| : \mathcal{F} \rightarrow |\mathcal{F}|$ is called the *functor geometric realization*.

For each $(M, \rho) \in \mathbf{obj}(\mathcal{M}_{\mathcal{F}})$, one has a canonical morphism

$$(40) \quad i(\rho) : d_{\mathcal{F}}(M, \rho) = \mathbf{Spec}(M) \rightarrow \varinjlim d_{\mathcal{F}} = |\mathcal{F}|.$$

The following result shows that the functor geometric realization $|\cdot|$ is left adjoint to the functor $\underline{\cdot}$.

PROPOSITION 3.30. *For every geometric monoidal space X there is a bijection of sets which is functorial in X*

$$\varphi(\mathcal{F}, X) : \mathbf{Hom}_{\mathfrak{S}\mathfrak{S}}(|\mathcal{F}|, X) \xrightarrow{\sim} \mathbf{Hom}_{\mathfrak{M}\mathfrak{o}\mathfrak{S}}(\mathcal{F}, \underline{X}), \quad \varphi(\mathcal{F}, X)(f) = g$$

where $\forall (M, \rho) \in \mathbf{obj}(\mathcal{M}_{\mathcal{F}})$

$$g(M) : \mathcal{F}(M) \rightarrow \underline{X}(M), \quad g(M)(\rho) = f \circ i(\rho)$$

and $i(\rho) : \mathbf{Spec}(M) \rightarrow |\mathcal{F}|$ is the canonical morphism of (40).

The functor geometric realization $|\cdot|$ is left adjoint to the functor $\underline{\cdot}$.

PROOF. The proof is similar to the proof given in [DG] (cf. §1 Proposition 4.1). \square

One obtains, in particular, the following morphisms

$$\begin{aligned} \varphi(\mathcal{F}, |\mathcal{F}|) : \text{Hom}_{\mathfrak{G}\mathfrak{S}}(|\mathcal{F}|, |\mathcal{F}|) &\xrightarrow{\sim} \text{Hom}_{\mathfrak{M}\mathfrak{o}\mathfrak{S}}(\mathcal{F}, |\mathcal{F}|), & \varphi(\mathcal{F}, |\mathcal{F}|)(id_{|\mathcal{F}|}) &=: \Psi(\mathcal{F}) \\ \varphi(\underline{X}, X)^{-1} : \text{Hom}_{\mathfrak{M}\mathfrak{o}\mathfrak{S}}(\underline{X}, X) &\xrightarrow{\sim} \text{Hom}_{\mathfrak{G}\mathfrak{S}}(|\underline{X}|, X), & \varphi(\underline{X}, X)^{-1}(id_{\underline{X}}) &=: \Phi(X). \end{aligned}$$

Notice that as a consequence of the fact that the functor $\text{Spec}(\cdot)$ is fully-faithful, $\Psi(\mathfrak{spec}(M))$ is invertible, thus $\text{Spec}(M) \simeq |\mathfrak{spec}(M)|$, i.e. $\Phi(\text{Spec}(M))$ is invertible, for any model M in $\mathfrak{M}\mathfrak{o}'$, cf. also Example 3.35.

We have already said that the covariant functor

$$\mathbb{F}_1[\cdot] : \mathfrak{Ab} \rightarrow \mathfrak{M}\mathfrak{o} \quad H \mapsto \mathbb{F}_1[H]$$

embeds the category of abelian groups as a full subcategory of $\mathfrak{M}\mathfrak{o}$. We shall identify \mathfrak{Ab} to this full subcategory of $\mathfrak{M}\mathfrak{o}$. One has a pair of adjoint functors: $H \mapsto \mathbb{F}_1[H]$ from \mathfrak{Ab} to $\mathfrak{M}\mathfrak{o}$ and $M \mapsto M^\times$ from $\mathfrak{M}\mathfrak{o}$ to \mathfrak{Ab} i.e. one has the following natural isomorphism

$$\text{Hom}_{\mathfrak{M}\mathfrak{o}}(\mathbb{F}_1[H], M) \cong \text{Hom}_{\mathfrak{Ab}}(H, M^\times).$$

Moreover, any $\mathfrak{M}\mathfrak{o}$ -functor $\mathcal{F} : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}$ restricts to \mathfrak{Ab} and gives rise to a functor: its *Weil restriction*

$$\mathcal{F}_{|\mathfrak{Ab}} : \mathfrak{Ab} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}$$

taking values into sets.

Let X be a geometric monoidal space. Then, the Weil restriction $\underline{X}_{|\mathfrak{Ab}}$ of the $\mathfrak{M}\mathfrak{o}$ -functor \underline{X} to the full sub-category $\mathfrak{Ab} \subset \mathfrak{M}\mathfrak{o}$, is a direct sum of *indecomposable* functors, i.e. a direct sum of functors that cannot be decomposed further into a disjoint sum of non-empty sub-functors.

PROPOSITION 3.31. *Let X be a geometric monoidal space. Then the functor*

$$\underline{X}_{|\mathfrak{Ab}} : \mathfrak{Ab} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}, \quad \underline{X}_{|\mathfrak{Ab}}(H) = \text{Hom}_{\mathfrak{G}\mathfrak{S}}(\text{Spec } \mathbb{F}_1[H], X)$$

is the disjoint union of representable functors

$$\underline{X}_{|\mathfrak{Ab}}(\mathbb{F}_1[H]) = \coprod_{x \in X} (\underline{X}_{|\mathfrak{Ab}})_x(\mathbb{F}_1[H]) = \coprod_{x \in X} \text{Hom}_{\mathfrak{Ab}}(\mathcal{O}_{X,x}^\times, H)$$

where x runs through the points of X .

PROOF. Let $\varphi \in \text{Hom}(\text{Spec } \mathbb{F}_1[H], X)$. The unique point $\mathfrak{p} \in \text{Spec } \mathbb{F}_1[H]$ corresponds to the ideal $\{0\}$. Let $\varphi(\mathfrak{p}) = x \in X$ be its image; there is a corresponding map of the stalks

$$\varphi^\# : \mathcal{O}_{X, \varphi(\mathfrak{p})} \rightarrow \mathcal{O}_{\mathfrak{p}} = \mathbb{F}_1[H].$$

This homomorphism is local by hypothesis: this means that the inverse image of $\{0\}$ by $\varphi^\#$ is the maximal ideal of $\mathcal{O}_{X, \varphi(\mathfrak{p})} = \mathcal{O}_{X,x}$. Therefore, the map $\varphi^\#$ is entirely determined by the group homomorphism $\rho : \mathcal{O}_{X,x}^\times \rightarrow H$ obtained as the restriction of $\varphi^\#$. Thus $\varphi \in \text{Hom}(\text{Spec } \mathbb{F}_1[H], X)$ is entirely specified by a point $x \in X$ and a group homomorphism $\rho \in \text{Hom}_{\mathfrak{Ab}}(\mathcal{O}_{X,x}^\times, H)$. \square

We recall that the set underlying the geometric realization of a \mathbb{Z} -scheme can be obtained by restricting the \mathbb{Z} -functor to the full subcategory of fields and passing to a suitable inductive limit (cf. [DG], §4.5). For $\mathfrak{M}\mathfrak{o}$ -schemes this construction simplifies considerably since the full subcategory $\mathfrak{A}\mathfrak{b}$ admits the *final object*

$$\mathbb{F}_1 = \mathbb{F}_1[\{1\}] = \{0, 1\}.$$

Notice though that while \mathbb{F}_1 is a final object for the subcategory $\mathfrak{A}\mathfrak{b} \subset \mathfrak{M}\mathfrak{o}$, it is *not* a final object in $\mathfrak{M}\mathfrak{o}$, in fact the following proposition shows that for any monoid $M \in \text{obj}(\mathfrak{M}\mathfrak{o})$, the set $\text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, \mathbb{F}_1)$ is in canonical correspondence with the points of $\text{Spec } M$.

For any geometric monoidal scheme X , we denote by $X^\mathfrak{c}$ its underlying set.

PROPOSITION 3.32. (1) For any object M of $\mathfrak{M}\mathfrak{o}$, the map

$$\varphi : \text{Spec}(M)^\mathfrak{c} \rightarrow \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, \mathbb{F}_1) \quad \mathfrak{p} \mapsto \varphi_{\mathfrak{p}}$$

$$(41) \quad \varphi_{\mathfrak{p}}(x) = 0, \quad \forall x \in \mathfrak{p}, \quad \varphi_{\mathfrak{p}}(x) = 1, \quad \forall x \notin \mathfrak{p}$$

determines a natural bijection of sets.

(2) For any $\mathfrak{M}\mathfrak{o}$ -functor \mathcal{F} , there is a canonical isomorphism $|\mathcal{F}|^\mathfrak{c} \simeq \mathcal{F}(\mathbb{F}_1)$.

(3) Let X be a geometric monoidal space, and $\mathcal{F} = \underline{X}$. Then, there is a canonical bijection $\underline{X}(\mathbb{F}_1) \simeq X$.

PROOF. (1) The map φ is well-defined since the complement of a prime ideal \mathfrak{p} in a monoid is a multiplicative set. To define the inverse of φ , one assigns to $\rho \in \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, \mathbb{F}_1)$ its kernel which is a prime ideal of M that uniquely determines ρ .

(2) The set $|\mathcal{F}|^\mathfrak{c}$, i.e. the set underlying $\varinjlim d_{\mathcal{F}}$ is canonically in bijection with

$$Z = \varinjlim_{(M, \rho) \in \mathcal{M}_{\mathcal{F}}} (\text{Spec}(M))^\mathfrak{c}$$

By (1), one has a canonical bijection

$$\text{Spec}(M)^\mathfrak{c} \simeq \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, \mathbb{F}_1)$$

and using the identification

$$\mathcal{F} = \varinjlim_{(M, \rho) \in \mathcal{M}_{\mathcal{F}}} \mathfrak{spec}(M)$$

we get the canonical bijection

$$Z = \varinjlim_{(M, \rho) \in \mathcal{M}_{\mathcal{F}}} \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, \mathbb{F}_1) = \varinjlim_{(M, \rho) \in \mathcal{M}_{\mathcal{F}}} \mathfrak{spec}(M)(\mathbb{F}_1) = \mathcal{F}(\mathbb{F}_1).$$

(3) An element $\rho \in \mathcal{F}(\mathbb{F}_1) = \underline{X}(\mathbb{F}_1)$ is a morphism of geometric spaces $\text{Spec } \mathbb{F}_1 \rightarrow X$ and the image of the unique (closed) point of $\text{Spec } \mathbb{F}_1$ is a point $x \in X$ which uniquely determines ρ . Conversely any point $x \in X$ determines a morphism $(\varphi, \varphi^\sharp)$ of geometric spaces $\text{Spec } \mathbb{F}_1 \rightarrow X$. The homomorphism of sheaves of monoids $\varphi^\sharp : \varphi^{-1}\mathcal{O}_X \rightarrow \mathcal{O}_{\mathbb{F}_1}$ is uniquely determined by its locality property, and sends $\mathcal{O}_{X,x}^\times$ to 1 and the complement of $\mathcal{O}_{X,x}^\times$ (i.e. the maximal ideal \mathfrak{m}_x) to 0. \square

Proposition 3.32 shows how to describe concretely the set underlying the geometric realization $|\mathcal{F}|$ of an $\mathfrak{M}\mathfrak{o}$ -functor \mathcal{F} in terms of the set $\mathcal{F}(\mathbb{F}_1)$. To describe

the topology of $|\mathcal{F}|$ directly on $\mathcal{F}(\mathbb{F}_1)$, we use the following construction of sub-functors of \mathcal{F} defined in terms of arbitrary subsets $P \subset \mathcal{F}(\mathbb{F}_1)$. It corresponds to the construction of [DG] I, §1, 4.10.

PROPOSITION 3.33. *Let \mathcal{F} be an $\mathfrak{M}\mathfrak{o}$ -functor and $P \subset \mathcal{F}(\mathbb{F}_1)$ be a subset of the set $\mathcal{F}(\mathbb{F}_1)$. For $M \in \text{obj}(\mathfrak{M}\mathfrak{o})$ and $\rho \in \mathcal{F}(M)$ the following two conditions are equivalent:*

a) *For every homomorphism $\varphi \in \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, \mathbb{F}_1)$ one has*

$$\mathcal{F}(\varphi)(\rho) \in P \subset \mathcal{F}(\mathbb{F}_1)$$

b) *For every $H \in \text{obj}(\mathfrak{A}\mathfrak{b})$ and every homomorphism $\varphi \in \text{Hom}(M, \mathbb{F}_1[H])$ one has*

$$\mathcal{F}(\varphi)(\rho) \in \bigcup_{x \in P} (\mathcal{F}_{|\mathfrak{A}\mathfrak{b}|_x}(\mathbb{F}_1[H]))$$

where P is viewed as a subset of $\varinjlim \mathcal{F}_{|\mathfrak{A}\mathfrak{b}|_x} \simeq |\mathcal{F}|$.

The above equivalent conditions define a sub-functor $\mathcal{F}_P \subset \mathcal{F}$.

It is clear that a) defines a sub-functor $\mathcal{F}_P \subset \mathcal{F}$. We shall omit the proof of the equivalence between the conditions a) and b) which is only needed to carry on the analogy with the construction in [DG] I, §1, 4.10.

Thus, we adopt a) as the definition of the sub-functor $\mathcal{F}_P \subset \mathcal{F}$.

Notice that one can reconstruct P from \mathcal{F}_P using the equality

$$P = \mathcal{F}_P(\mathbb{F}_1) \subset \mathcal{F}(\mathbb{F}_1).$$

Let X be a geometric monoidal space. If one endows the subset $P \subset X$ with the induced topology from X and with the structural sheaf $\mathcal{O}_{X|_P}$, the functor \underline{X}_P gets identified with $\underline{P} \subset \underline{X}$. Moreover, if P is an open subset in X , then \underline{X}_P is an open sub-functor of \underline{X} . In particular, if $\mathcal{F} = \mathfrak{spec}(M)$ then $P \subset \text{Spec}(M) = |\mathcal{F}|$ is open if and only if \mathcal{F}_P is an open sub-functor of $\mathfrak{spec}(M)$.

More generally, the following results hold for arbitrary $\mathfrak{M}\mathfrak{o}$ -functors.

THEOREM 3.34. *Let \mathcal{F} be an $\mathfrak{M}\mathfrak{o}$ -functor. The following facts hold*

(1) *A subset $P \subset |\mathcal{F}| = \mathcal{F}(\mathbb{F}_1)$ is open if and only if for every $(M, \rho) \in \text{obj}(\mathcal{M}_{\mathcal{F}})$ the set of prime ideals $\mathfrak{p} \in \text{Spec } M$ such that $\varphi_{\mathfrak{p}}(\rho) \in P$ is open in $\text{Spec } M$.*

(2) *The map $P \rightarrow \mathcal{F}_P$ induces a bijection of sets between the collection of open subsets of $|\mathcal{F}| = \mathcal{F}(\mathbb{F}_1)$ and the open sub-functors of \mathcal{F} .*

(3) *The structure sheaf of $|\mathcal{F}| = \mathcal{F}(\mathbb{F}_1)$ is given by*

$$\mathcal{O}(U) = \text{Hom}_{\mathfrak{M}\mathfrak{o}\mathfrak{S}}(\mathcal{F}_U, \mathcal{D}), \quad \forall U \subset |\mathcal{F}| \text{ open,}$$

where $\mathcal{D} : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{S}\mathfrak{e}\mathfrak{t}\mathfrak{s}$, $\mathcal{D}(M) = M$ is the functor affine line.

PROOF. (1) By definition of the topology on the inductive limit $|\mathcal{F}| = \varinjlim_{(M, \rho) \in \mathcal{M}_{\mathcal{F}}} d_{\mathcal{F}}$, a subset P of $|\mathcal{F}|$ is open if and only if its inverse image under the canonical maps $i(\rho)$ of (40) is open. Using the identification $|\mathcal{F}| \simeq \mathcal{F}(\mathbb{F}_1)$ one obtains the required statement.

(2) We give the simple direct argument (cf. also [DG] I, §1 Proposition 4.12). Let \mathcal{F}_1 be an open sub-functor of \mathcal{F} . By Definition 3.17, given an object M of $\mathfrak{M}\mathfrak{o}$ and

an element $\xi \in \mathcal{F}(M)$, there exists an ideal $I \subset M$, $I = I(M, \xi)$, such that for any object N of $\mathfrak{M}\mathfrak{o}$ and for any $\rho \in \mathfrak{spec} M(N) = \text{Hom}_{\mathfrak{M}\mathfrak{o}}(M, N)$ one has

$$\mathcal{F}(\rho)\xi \in \mathcal{F}_1(N) \subset \mathcal{F}(N) \Leftrightarrow \rho(I)N = N.$$

Take $N = \mathbb{F}_1$ and $\rho = \varphi_{\mathfrak{p}}$ for $\mathfrak{p} \in \text{Spec} M$, then one gets

$$\mathcal{F}(\varphi_{\mathfrak{p}})(\xi) \in \mathcal{F}_1(\mathbb{F}_1) \Leftrightarrow 1 \in \varphi_{\mathfrak{p}}(I) \Leftrightarrow \mathfrak{p} \in D(I)$$

which shows that $D(I)$ and hence the radical of $I = I(M, \xi)$ is determined by the subset $P = \mathcal{F}_1(\mathbb{F}_1) \subset \mathcal{F}(\mathbb{F}_1)$. Now take $N = M$ and $\rho = id_M$, then one has

$$\xi \in \mathcal{F}_1(M) \subset \mathcal{F}(M) \Leftrightarrow I = M,$$

and this holds if and only if $D(I) = \text{Spec} M$ or equivalently $\varphi_{\mathfrak{p}}(\xi) \in \mathcal{F}_1(\mathbb{F}_1)$ for all $\mathfrak{p} \in \text{Spec} M$ which is the definition of the sub-functor associated to the open subset $P = \mathcal{F}_1(\mathbb{F}_1) \subset \mathcal{F}(\mathbb{F}_1)$.

(3) By using the above identifications, the proof is the same as in [DG] I, §1 Proposition 4.14. The structure of monoid on $\mathcal{O}(U) = \text{Hom}_{\mathfrak{M}\mathfrak{o}\mathfrak{e}}(\mathcal{F}_U, \mathcal{D})$ is given by

$$(\alpha\beta)(M)(x) = \alpha(M)(x)\beta(M)(x) \in M, \quad \forall x \in \mathcal{F}_U(M), \quad \alpha, \beta \in \mathcal{O}(U).$$

□

EXAMPLE 3.35. Let $M \in \text{obj}(\mathfrak{M}\mathfrak{o})$. The map $\mathfrak{p} \mapsto \varphi_{\mathfrak{p}}$ as in (41) defines a natural bijection $\text{Spec} M \simeq |\mathfrak{spec} M| = \text{Hom}(M, \mathbb{F}_1)$ and using the topology defined by (1) of Theorem 3.34, one can check directly that this map is an homeomorphism. One can also verify directly that the structure sheaf of $|\mathfrak{spec} M|$ as defined by (3) of Theorem 3.34 coincides with the structure sheaf of $\text{Spec} M$. Thus $\text{Spec}(M) \simeq |\mathfrak{spec}(M)|$, i.e. $\Phi(\text{Spec}(M))$ and $\Psi(\mathfrak{spec}(M))$ are invertible, for any object M in $\mathfrak{M}\mathfrak{o}$.

COROLLARY 3.36. *Let X be a geometric monoidal space. If $\mathcal{F} \subset \underline{X}$ is an open sub-functor of \underline{X} , then $|\mathcal{F}| \subset |\underline{X}|$ is an open subset of X .*

PROOF. For the proof we refer to [DG] I, §1 Corollary 4.15. □

The following result describes a property which *does not hold* in general for \mathbb{Z} -schemes and provides a natural map $\mathcal{F}(M) \rightarrow |\mathcal{F}| \simeq \mathcal{F}(\mathbb{F}_1)$, $\forall M \in \text{obj}(\mathfrak{M}\mathfrak{o})$ and any $\mathfrak{M}\mathfrak{o}$ -functor \mathcal{F} .

PROPOSITION 3.37. *Let \mathcal{F} be an $\mathfrak{M}\mathfrak{o}$ -functor, then the following facts hold*

1) *For any monoid $M \in \text{obj}(\mathfrak{M}\mathfrak{o})$ there exists a canonical map*

$$\pi_M : \mathcal{F}(M) \rightarrow |\mathcal{F}| \simeq \mathcal{F}(\mathbb{F}_1)$$

such that

$$\pi_M(\rho) = \varphi_{\mathfrak{p}_M}(\rho), \quad \forall \rho \in \mathcal{F}(M).$$

2) *Let U be an open subset of $|\mathcal{F}| = \mathcal{F}(\mathbb{F}_1)$ and \mathcal{F}_U the associated subfunctor of \mathcal{F} , then*

$$\mathcal{F}_U(M) = \pi_M^{-1}(U) \subset \mathcal{F}(M).$$

PROOF. 1) follows from the definition of the map $\varphi_{\mathfrak{p}_M}$.
 2) By Theorem 3.34, the set $W = \{\mathfrak{p} \in \text{Spec } M \mid \varphi_{\mathfrak{p}}(\rho) \in U\}$ is open in $\text{Spec } M$. Thus by Proposition 2.18, one has $W = \text{Spec}(M)$ if and only if $\mathfrak{p}_M \in W$ which gives the required statement using the definition of the sub-functor \mathcal{F}_U as in Proposition 3.33. \square

The next result establishes the equivalence between the category of $\mathfrak{M}\mathfrak{o}$ -schemes and the category of geometric $\mathfrak{M}\mathfrak{o}$ -schemes, using sufficient conditions for the morphisms

$$\Psi(\mathcal{F}) : \mathcal{F} \rightarrow \underline{|\mathcal{F}|}, \quad \Phi(X) : \underline{|X|} \rightarrow X$$

to be invertible. This result generalizes Example 3.35 where this invertibility has been proven in the case $\mathcal{F} = \mathfrak{spec } M$, $X = \text{Spec } M$ and for objects M of $\mathfrak{M}\mathfrak{o}$.

THEOREM 3.38. (1) *Let X be a geometric $\mathfrak{M}\mathfrak{o}$ -scheme. Then $\underline{|X|}$ is an $\mathfrak{M}\mathfrak{o}$ -scheme and the morphism $\Phi(X) : \underline{|X|} \rightarrow X$ is invertible.*

(2) *Let \mathcal{F} be an $\mathfrak{M}\mathfrak{o}$ -scheme then the geometric monoidal space $|\mathcal{F}|$ is a geometric $\mathfrak{M}\mathfrak{o}$ -scheme and $\Psi(\mathcal{F}) : \mathcal{F} \rightarrow \underline{|\mathcal{F}|}$ is invertible.*

Thus, the two functors $|\cdot|$ and $\underline{\cdot}$ induce quasi-inverse equivalences between the category of $\mathfrak{M}\mathfrak{o}$ -schemes and the category of geometric $\mathfrak{M}\mathfrak{o}$ -schemes.

PROOF. (1) In view of Proposition 3.32, for any geometric scheme X the map $\Phi(X) : \underline{|X|} \rightarrow X$ induces a bijection of the underlying sets. If $\{U_i\}_{i \in \mathbb{U}}$ is a covering of X by prime spectra, it follows that $\Phi(U_i) : \underline{|U_i|} \rightarrow U_i$ is an isomorphism. Moreover, since U_i is an open subset of X , it follows from Corollary 3.36 that $\underline{|U_i|}$ is an open subspace of $\underline{|X|}$. Thus, the topologies on the spaces $\underline{|X|}$ and X as well as the related structural sheaves get identified by means of $\Phi(X)$. Hence $\Phi(X)$ is invertible.

(2) Let \mathcal{F} be an $\mathfrak{M}\mathfrak{o}$ -scheme, we shall show that $|\mathcal{F}|$ is a geometric $\mathfrak{M}\mathfrak{o}$ -scheme. We let $\{\mathfrak{U}_i\}_{i \in \mathbb{U}}$ be an open covering of \mathcal{F} by (functors) prime spectra such that $\{\mathfrak{U}_{ij\alpha}\}$ is an open covering of $\mathfrak{U}_i \cap \mathfrak{U}_j$ by (functors) prime spectra. Then, $\{|\mathfrak{U}_i|\}$ is an open covering of $|\mathcal{F}|$ by prime spectra, thus $|\mathcal{F}|$ verifies the condition of Definition 3.13 and is a geometric $\mathfrak{M}\mathfrak{o}$ -scheme. In view of the fact that $\Psi(\mathfrak{U}_i) : \mathfrak{U}_i \rightarrow \underline{|\mathfrak{U}_i|}$ is invertible, the composite of $\Psi(\mathfrak{U}_i)^{-1}$ and the inclusion $\mathfrak{U}_i \hookrightarrow \mathcal{F}$ gives a collection of morphisms $\Psi_i^{-1}(\mathcal{F}) : \underline{|\mathfrak{U}_i|} \rightarrow \mathcal{F}$. Moreover one has $\Psi_i^{-1}(\mathcal{F})|_{\underline{|\mathfrak{U}_{ij\alpha}|}} = \Psi_j^{-1}(\mathcal{F})|_{\underline{|\mathfrak{U}_{ij\alpha}|}}$, for all i, j, α . The automatic locality of \mathcal{F} then shows that the Ψ_i^{-1} assemble to a single morphism $\underline{|\mathcal{F}|} \rightarrow \mathcal{F}$ which is the inverse of $\Psi(\mathcal{F}) : \mathcal{F} \rightarrow \underline{|\mathcal{F}|}$. In fact Proposition 3.21 shows that this inverse is surjective. \square

4. \mathbb{F}_1 -SCHEMES AND THEIR ZETA FUNCTIONS

A general formalism of category theory allows one to glue together two categories connected by a pair of adjoint functors (cf. [CC2] §4). This construction is particularly interesting when applied to the functorial formalism that describes the most common examples of schemes (of finite type) over \mathbb{F}_1 that we have reviewed so far. In all these cases in fact, the two categories naturally involved *i.e.* $\mathfrak{M}\mathfrak{o}$ and $\mathfrak{R}\mathfrak{i}\mathfrak{n}\mathfrak{g}$ are linked by a pair of natural adjoint functors. These are

$$\beta : \mathfrak{M}\mathfrak{o} \rightarrow \mathfrak{R}\mathfrak{i}\mathfrak{n}\mathfrak{g}, \quad \beta(M) = \mathbb{Z}[M]$$

which associates to a monoid the convolution ring $\mathbb{Z}[M]$ and the forgetful functor

$$\beta^* : \mathfrak{Ring} \rightarrow \mathfrak{Mo} \quad \beta^*(R) = R.$$

which associates to a ring its underlying structure of multiplicative monoid. The resulting glued category $\mathfrak{MR} = \mathfrak{Ring} \cup_{\beta, \beta^*} \mathfrak{Mo}$ defines the most natural categorical framework on which one introduces the notions of an \mathbb{F}_1 -functor and of a scheme over \mathbb{F}_1 .

DEFINITION 4.1. *An \mathbb{F}_1 -functor is a covariant functor from the category $\mathfrak{MR} = \mathfrak{Ring} \cup_{\beta, \beta^*} \mathfrak{Mo}$ to the category of sets.*

The conditions imposed in the original definition of a variety over \mathbb{F}_1 (cf. [So]) are now applied to a covariant functor $\mathcal{X} : \mathfrak{MR} \rightarrow \mathfrak{Sets}$. Such a functor determines a scheme (of finite type) over \mathbb{F}_1 if it also fulfills the following properties.

DEFINITION 4.2. *An \mathbb{F}_1 -scheme is an \mathbb{F}_1 -functor $\mathcal{X} : \mathfrak{MR} \rightarrow \mathfrak{Sets}$, such that:*

- *The restriction $X_{\mathbb{Z}}$ of \mathcal{X} to \mathfrak{Ring} is a \mathbb{Z} -scheme.*
- *The restriction \underline{X} of \mathcal{X} to \mathfrak{Mo} is an \mathfrak{Mo} -scheme.*
- *The natural transformation $e : \underline{X} \circ \beta^* \rightarrow X_{\mathbb{Z}}$ associated to a field is a bijection (of sets).*

Morphisms of \mathbb{F}_1 -schemes are natural transformations of the corresponding functors.

4.1 Torsion free Noetherian \mathbb{F}_1 -schemes.

The first theorem stated in this subsection shows that for any Noetherian, torsion-free \mathbb{F}_1 -scheme the function counting the number of rational points (for the associated \mathbb{Z} -scheme) over a finite field \mathbb{F}_q is *automatically* polynomial. The same theorem also provides a complete description of its zeta function over \mathbb{F}_1 (originally introduced upside-down in [So]).

By following *op.cit.* (§ 6 Lemme 1) and implementing the correction concerning the inversion in the formula of the zeta function, the definition of the zeta-function of an algebraic variety $X = (\underline{X}, X_{\mathbb{C}}, e_X)$ over \mathbb{F}_1 such that $\#X_{\mathbb{Z}}(\mathbb{F}_q) = N(q)$, with $N(x)$ a polynomial function and $\#\underline{X}(\mathbb{F}_{1^n}) = N(q)$ if $n = q - 1$, is given as the limit

$$(42) \quad \zeta_X(s) := \lim_{q \rightarrow 1} Z(X, q^{-s})(q-1)^{N(1)}.$$

Here, the function $Z(X, q^{-s})$ (*i.e.* the Hasse-Weil exponential series) is defined by

$$Z(X, T) := \exp \left(\sum_{r \geq 1} N(q^r) \frac{T^r}{r} \right).$$

One obtains

$$N(x) = \sum_{k=0}^d a_k x^k \implies \zeta_X(s) = \prod_{k=0}^d (s-k)^{-a_k}.$$

For instance, in the case of the projective line \mathbb{P}^1 one has $\zeta_{\mathbb{P}^1}(s) = \frac{1}{s(s-1)}$.

We say that an \mathbb{F}_1 -scheme is Noetherian if the associated \mathfrak{Mo} and \mathbb{Z} -schemes are Noetherian (cf. [CC2] Definition 4.12). An \mathbb{F}_1 -scheme is said to be torsion free if the groups $\mathcal{O}_{X,x}^{\times}$ of the invertible elements of the monoids $\mathcal{O}_{X,x}$ (X is the associated geometric \mathfrak{Mo} -scheme) are torsion free $\forall x \in X$. The following result is related to Theorem 1 of [D3], but applies also to non-toric varieties.

THEOREM 4.3. *Let \mathcal{X} be a torsion free, Noetherian \mathbb{F}_1 -scheme and let X be the geometric realization of its restriction \underline{X} to $\mathfrak{M}\mathfrak{o}$. Then*

(1) *There exists a polynomial $N(x+1)$ with positive integral coefficients such that*

$$\# X(\mathbb{F}_{1^n}) = N(n+1), \quad \forall n \in \mathbb{N}.$$

(2) *For each finite field \mathbb{F}_q , the cardinality of the set of points of the \mathbb{Z} -scheme $X_{\mathbb{Z}}$ which are rational over \mathbb{F}_q is equal to $N(q)$.*

(3) *The zeta function of \mathcal{X} has the following description*

$$(43) \quad \zeta_{\mathcal{X}}(s) = \prod_{x \in X} \frac{1}{\left(1 - \frac{1}{s}\right)^{\otimes n(x)}},$$

where \otimes denotes Kurokawa's tensor product and $n(x)$ is the local dimension of X at the point x .

In (43), we use the convention that when $n(x) = 0$ the expression

$$\left(1 - \frac{1}{s}\right)^{\otimes n(x)} = s.$$

We refer to [Ku] and [M] for the details of the definition of Kurokawa's tensor products and zeta functions and to [CC2] for the proof of the Theorem.

4.2 Extension of the counting functions in the torsion case.

The remaining part of this section is dedicated to the computation of the zeta function of an arbitrary Noetherian \mathbb{F}_1 -scheme \mathcal{X} . For simplicity, we will always denote by X the geometric realization (*i.e.* the geometric monoidal scheme) of the restriction \underline{X} of \mathcal{X} to $\mathfrak{M}\mathfrak{o}$ and we will shortly refer to X as to the \mathbb{F}_1 -scheme. In the general case, we shall prove that the counting function

$$\# X(\mathbb{F}_{1^n}) = N_X(n+1), \quad \forall n \in \mathbb{N}$$

of an \mathbb{F}_1 -scheme is no longer a polynomial function of n and that its description involves periodic functions. First, we will show that there is a *canonical* extension of the counting function $N_X(n)$ to the complex plane, as an entire function $N_X(z)$, whose growth is well controlled. Then, we will explain how to compute the zeta function (42) using $N_X(q)$ for arbitrary real values of $q \geq 1$.

The simplest example of a Noetherian \mathbb{F}_1 -scheme is $X = \text{Spec}(\mathbb{F}_{1^m})$. The number of rational points of X over \mathbb{F}_{1^n} is the cardinality of the set of group homomorphisms $\text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$, *i.e.*

$$(44) \quad \# X(\mathbb{F}_{1^n}) = \# \text{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \text{gcd}(n, m).$$

This is a *periodic* function of n . More generally the following statement holds.

LEMMA 4.4. *Let X be a Noetherian \mathbb{F}_1 -scheme. The counting function is a finite sum of monomials of the form*

$$(45) \quad \# X(\mathbb{F}_{1^n}) = \sum_{x \in X} n^{n(x)} \prod_j \text{gcd}(n, m_j(x))$$

where $n(x)$ denotes the local dimension at $x \in X$ and the natural numbers $m_j(x)$ are the orders of the finite cyclic groups which compose the residue “field” $\kappa(x) = \mathbb{F}_1[\mathcal{O}_{X,x}^\times]$ i.e.

$$\mathcal{O}_{X,x}^\times = \mathbb{Z}^{n(x)} \prod_j \mathbb{Z}/m_j(x)\mathbb{Z}.$$

PROOF. It follows from the proof of the first part of Theorem 4.3 that

$$\# X(\mathbb{F}_{1^n}) = \sum_{x \in X} \text{Hom}_{\mathfrak{Ab}}(\mathcal{O}_{X,x}^\times, \mathbb{Z}/n\mathbb{Z})$$

and the result follows from (44). \square

We continue by explaining how to extend canonically a function such as (45) to an entire function on the complex plane.

4.2.1 Extension of functions from \mathbb{Z} to \mathbb{C} .

Let $f(z)$ be an entire function of $z \in \mathbb{C}$ and let $T(R, f)$ be its *characteristic function*:

$$T(R, f) = \frac{1}{2\pi} \int_0^{2\pi} \log^+ |f(Re^{i\theta})| d\theta.$$

This function may be interpreted as the average magnitude of $\log^+ |f(z)|$. One sets

$$\log^+ x = \begin{cases} \log x, & \text{if } x \geq 1 \\ 0, & \text{if } 0 < x < 1 \end{cases}$$

and one denotes by

$$N(a, R) = \sum_{\substack{f(z)=a \\ |z| < R}} \log \left| \frac{R}{z} \right|$$

the sum over the zeros of $(f - a)(z)$ inside the disk of radius R . The First Fundamental Theorem of Nevanlinna theory states as follows

THEOREM 4.5. (*First Fundamental Theorem*) *If $a \in \mathbb{C}$ then*

$$N(a, R) \leq T(R, f) - \log |f(0) - a| + \epsilon(a, R)$$

where

$$|\epsilon(a, R)| \leq \log^+ |a| + \log 2.$$

When $a = 0$ and f has a zero of order n at 0, the inequality applied to $F(z) = f(z)z^{-n}$ shows that for $R \geq 1$,

$$N'(0, R) = \sum_{\substack{f(z)=0 \\ |z| < R, z \neq 0}} \log \left| \frac{R}{z} \right| \leq T(R, f) - \log |F(0)| + \log 2,$$

since $T(R, f) \geq T(R, F)$ for $R \geq 1$. If an entire function $f(z)$ vanishes on $\mathbb{Z} \subset \mathbb{C}$, one has

$$N'(0, R) \geq \sum_{\substack{z \in \mathbb{Z} \setminus \{0\} \\ |z| < R}} \log \left| \frac{R}{z} \right| \sim 2R$$

and hence the above inequality shows that when $R \rightarrow \infty$

$$(46) \quad \underline{\lim} \frac{T(R, f)}{R} \geq 2.$$

We shall now use this inequality to prove the following result.

PROPOSITION 4.6. *Let $N(n)$ be a real function on \mathbb{Z} of the form*

$$(47) \quad N(n) = \sum_{j \geq 0} T_j(n) n^j$$

where the $T_j(n)$'s are periodic functions with integral periods. Then, there exists a unique polynomial $Q(n)$ and a unique entire function $f : \mathbb{C} \rightarrow \mathbb{C}$ such that

- $\overline{f(\bar{z})} = f(z)$.
- $\overline{\lim} \frac{T(R, f)}{R} < 2$.
- $N(n) - (-1)^n Q(n) = f(n) \quad \forall n \in \mathbb{Z}$.

PROOF. Choose $L \in \mathbb{N}$ such that all the $T_j(n)$ fulfill $T_j(m + L) = T_j(m)$, for all $m \in \mathbb{Z}$. For each $j \in \mathbb{N}$, one has a Fourier expansion of the form

$$T_j(m) = \sum_{\alpha \in I_L} t_{j, \alpha} e^{2\pi i \alpha m} + s_j (-1)^m, \quad I_L = \left\{ \frac{k}{L} \mid |k| < L/2 \right\},$$

where $t_{j, -\alpha} = \bar{t}_{j, \alpha}$ for $\alpha \in I_L$ and $s_j \in \mathbb{R}$. We define $Q(n) = \sum_j s_j n^j$ and the function $f(z)$ by

$$f(z) = \sum_j \sum_{\alpha \in I_L} t_{j, \alpha} e^{2\pi i \alpha z} z^j.$$

One has $\overline{f(\bar{z})} = f(z)$. Since $|\alpha| \leq c < \frac{1}{2}$, $\forall \alpha \in I_L$, one gets that

$$\log^+ |f(Re^{i\theta})| \leq 2\pi R c |\sin\theta| + o(R)$$

which in turn implies $\overline{\lim} \frac{T(R, f)}{R} < 2$, using $\int_0^{2\pi} |\sin\theta| d\theta = 4$ and $c < 1/2$. The equality $N(n) - (-1)^n Q(n) = f(n)$ for all $n \in \mathbb{Z}$ holds by construction and it remains to show the uniqueness. This amounts to show that a non-zero entire function $f(z)$ such that $\overline{f(\bar{z})} = f(z)$ and $f(n) = (-1)^n Q(n)$ for all $n \in \mathbb{Z}$ and for some polynomial $Q(n)$ automatically fulfills (46). For $x \in \mathbb{R}$ one has $f(x) \in \mathbb{R}$. Let $s_k n^k$ be the leading term of $Q(n) = \sum_j s_j n^j$. Then, outside a finite set of indices n the sign of $Q(n)$ is independent of n for $n > 0$ and for $n < 0$. It follows that the function f changes sign in each interval $[n, n + 1]$ and hence admits at least one zero in such intervals. Thus, $N'(0, R) = \sum_{\substack{f(z)=0 \\ |z| < R, z \neq 0}} \log \left| \frac{R}{z} \right|$ fulfills

$$\underline{\lim} \frac{N(0, R)}{R} \geq 2$$

and hence, by Theorem 4.5 one gets

$$\underline{\lim} \frac{T(R, f)}{R} \geq 2.$$

The uniqueness follows. □

DEFINITION 4.7. Let $N(n)$ be a real function on \mathbb{Z} of the form (47). Then the canonical extension $N(z)$, $z \in \mathbb{C}$ is given by

$$N(z) = f(z) + \cos(\pi z)Q(z)$$

where f and Q are uniquely determined by Proposition 4.6.

We shall explicitly compute this extension in the case of the function $N_X(q)$ for $X = \text{Spec}(\mathbb{F}_1[H])$.

4.2.2. The counting function for $X = \text{Spec}(\mathbb{F}_1[H])$.

Let H be a finitely generated abelian group. In this subsection we compute the counting function $N_X(n)$ for $X = \text{Spec}(\mathbb{F}_1[H])$. We start by considering the cyclic case $H = \mathbb{Z}/m\mathbb{Z}$.

LEMMA 4.8. Let $X = \text{Spec}(\mathbb{F}_1^m)$. Then, the canonical extension of the counting function $N_X(n)$ is given by

$$(48) \quad N(z) = \sum_{d|m} \frac{\varphi(d)}{d} \left(\sum_{|k| < d/2} e^{2i\pi \frac{(z-1)k}{d}} + \epsilon_d \cos(\pi(z-1)) \right), \quad z \in \mathbb{C}$$

where $\epsilon_d = 1$ if $d \in \mathbb{Z}$ is even and $\epsilon_d = 0$ otherwise.

PROOF. It follows from (44) that $N(n) = \gcd(n-1, m)$. Moreover, one also knows that

$$\gcd(n, m) = \sum_{\substack{d|n \\ d|m}} \varphi(d)$$

where φ is the Euler totient function. Thus

$$(49) \quad \gcd(n, m) = \sum_{d|m} \frac{\varphi(d)}{d} \sum e^{2i\pi \frac{nk}{d}}$$

where the sum $\sum e^{2i\pi \frac{nk}{d}}$ is taken over all characters of the additive group $\mathbb{Z}/d\mathbb{Z}$ evaluated on $n \bmod d$. This sum can be written as

$$\sum e^{2i\pi \frac{nk}{d}} = \sum_{|k| < d/2} e^{2i\pi \frac{nk}{d}} + \epsilon_d \cos(\pi n)$$

which gives the canonical extension of $N(n)$ after a shift of one in the variable. \square

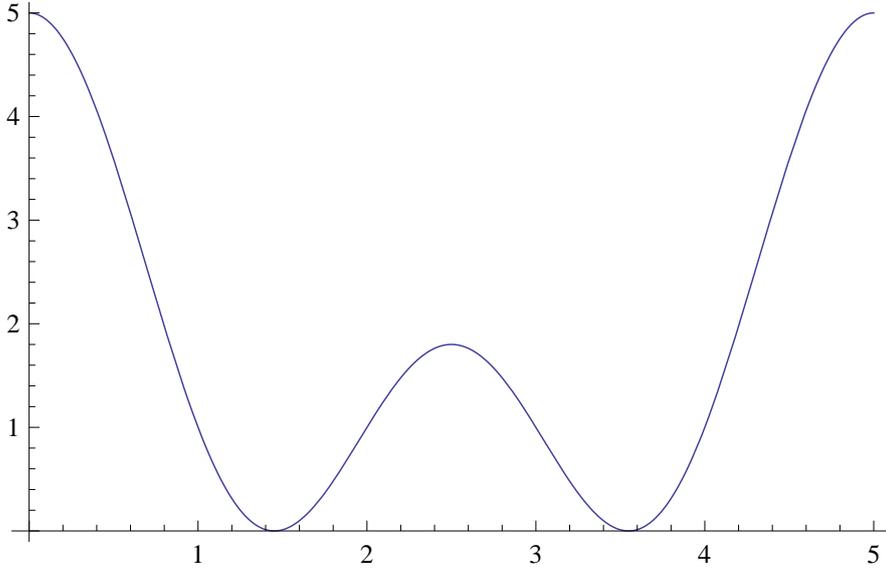


Fig. 4. The graph of the canonical extension of $N(q)$, for $X = \text{Spec}(\mathbb{F}_1[\mathbb{Z}/5\mathbb{Z}])$.

There is a conceptual explanation for the expansion (48). Let C_d be the d -th cyclotomic polynomial

$$C_d(x) = \prod_{r|d} (x^{d/r} - 1)^{\mu(r)}.$$

One has the decomposition into irreducible factors over \mathbb{Q}

$$x^m - 1 = \prod_{d|m} C_d(x)$$

which determines the decomposition

$$\mathbb{Q}[\mathbb{Z}/m\mathbb{Z}] = \bigoplus_{d|m} \mathbb{K}_d$$

where $\mathbb{K}_d = \mathbb{Q}(\xi_d)$ is the cyclotomic field extension of \mathbb{Q} by a primitive d -th root of 1. This decomposition corresponds to a factorization of the zeta function

$$\zeta_X(s) = \prod_p \zeta_{X/\mathbb{F}_p}(s)$$

as a product

$$\zeta_X(s) = \prod_{d|m} \zeta_{X/\mathbb{K}_d}(s)$$

where each term of the product is in turns a product of L -functions

$$\zeta_{X/\mathbb{K}_d}(s) = \prod_{\chi \in \hat{G}(d)} L(s, \chi), \quad G(d) = (\mathbb{Z}/d\mathbb{Z})^*$$

and the order of $G(d)$ is $\varphi(d)$. The decomposition

$$\zeta_X(s) = \prod_{d|m} \prod_{\chi \in \hat{G}(d)} L(s, \chi)$$

corresponds precisely to the decomposition (49).

Let now $H = \prod_j \mathbb{Z}/m_j\mathbb{Z}$ be a finite abelian group. Then, the extension of the group ring $\mathbb{Z}[H]$ over \mathbb{Q} can be equivalently interpreted as the tensor product

$$\mathbb{Q}[H] = \bigotimes_j \left(\bigoplus_{d|m_j} \mathbb{K}_d \right).$$

In fact, by applying the Galois correspondence, the decomposition of H into finite cyclic groups corresponds to the disjoint union of orbits for the action of the Galois group $\hat{\mathbb{Z}}^*$ on the cyclotomic extension $\mathbb{Q}^{\text{ab}}/\mathbb{Q}$ (i.e. the maximal abelian extension of \mathbb{Q}). If we denote the group H additively, two elements $x, y \in H$ are on the same Galois orbit if and only if $\{nx \mid n \in \mathbb{Z}\} = \{ny \mid n \in \mathbb{Z}\}$ i.e. if and only if they generate the same subgroup of H . Thus, the set Z of orbits is the set of cyclic subgroups of H .

For a cyclic group C of order d we let, as in (48)

$$(50) \quad N(z, C) = \frac{\varphi(d)}{d} \left(\sum_{|k| < d/2} e^{2i\pi \frac{(z-1)k}{d}} + \epsilon_d \cos(\pi(z-1)) \right).$$

Then, we obtain the following

LEMMA 4.9. *Let $\Gamma = \mathbb{Z}^k \times H$ be a finitely generated abelian group (H is a finite abelian torsion group) and $X = \text{Spec}(\mathbb{F}_1[\Gamma])$. Then, the canonical extension of the counting function $N_X(q)$ is given by*

$$(51) \quad N(z) = (z-1)^k \sum_{C \subset H} N(z, C), \quad z \in \mathbb{C}$$

where the sum is over the cyclic subgroups $C \subset H$.

PROOF. It is enough to show that the function $N(n+1)$ as in (51) gives the number of homomorphisms from Γ to $\mathbb{Z}/n\mathbb{Z}$. Indeed, as a function of z it is already in the canonical form of Definition 4.7. Then, by duality we just need to compare the number $\iota(n, H)$ of homomorphisms ρ from $\mathbb{Z}/n\mathbb{Z}$ to H with $\sum_{C \subset H} N(n+1, C)$. The cyclic subgroup $C = \text{Im } \rho$ is uniquely determined, thus

$$\iota(n, H) = \sum_{C \subset H} \mu(n, C)$$

where $\mu(n, C)$ is the number of surjective homomorphisms from $\mathbb{Z}/n\mathbb{Z}$ to C . If d denotes the order of C , this number is 0 unless $d|n$ and in the latter case it is $\varphi(d)$, thus using (50) it coincides in all cases with $N(n+1, C)$. \square

4.3 An integral formula for the logarithmic derivative of $\zeta_N(s)$.

Let $N(q)$ be a real-valued continuous function on $[1, \infty)$ satisfying a polynomial bound $|N(q)| \leq Cq^k$ for some finite positive integer k and a fixed positive integer constant C . Then the associated generating function is

$$Z(q, T) = \exp \left(\sum_{r \geq 1} N(q^r) T^r / r \right)$$

and one knows that the power series $Z(q, q^{-s})$ converges for $\Re(s) > k$. The zeta function over \mathbb{F}_1 associated to $N(q)$ is defined as follows

$$\zeta_N(s) := \lim_{q \rightarrow 1} (q-1)^s Z(q, q^{-s}), \quad \chi = N(1).$$

This definition requires some care to assure its convergence. To eliminate the ambiguity in the extraction of the finite part, one works instead with the logarithmic derivative

$$\frac{\partial_s \zeta_N(s)}{\zeta_N(s)} = - \lim_{q \rightarrow 1} F(q, s)$$

where

$$F(q, s) = -\partial_s \sum_{r \geq 1} N(q^r) \frac{q^{-rs}}{r}.$$

One then has (cf. [CC2])

LEMMA 4.10. *With the above notations and for $\Re(s) > k$*

$$\lim_{q \rightarrow 1} F(q, s) = \int_1^\infty N(u) u^{-s} d^*u, \quad d^*u = du/u$$

and

$$(52) \quad \frac{\partial_s \zeta_N(s)}{\zeta_N(s)} = - \int_1^\infty N(u) u^{-s} d^*u.$$

4.4 Analyticity of the integrals.

The statement of Lemma 4.10 and the explicit form of the function $N(q)$ as in Lemma 4.8 clearly indicate that one needs to analyze basic integrals of the form

$$(53) \quad f(s, a) = \int_1^\infty e^{iau} u^{-s} d^*u.$$

LEMMA 4.11. *For $a > 0$*

$$(54) \quad f(s, a) = a^s \int_a^\infty e^{iu} u^{-s} d^*u$$

defines an entire function of $s \in \mathbb{C}$.

PROOF. For $\Re(s) > 0$, the integral in (54) is absolutely convergent. Integrating by parts one obtains

$$\int_a^\infty e^{iu} u^{-s-1} du + \int_a^\infty \frac{1}{i} e^{iu} (-s-1) u^{-s-2} du = \left[\frac{1}{i} e^{iu} u^{-s-1} \right]_a^\infty$$

which supplies the equation

$$(55) \quad af(s, a) = -i(s+1)f(s+1, a) + ie^{ia}.$$

This shows that f is an entire function of s , since after iterating (55) the variable s can be moved to the domain of absolute convergence. \square

The function $f(s, a)$ as in (53) can be expressed in terms of hypergeometric functions in the following way

$$f(s, a) = e^{-\frac{1}{2}i\pi s} a^s \Gamma(-s) + i \frac{a}{s-1} H\left[\frac{1-s}{2}, \left(\frac{3}{2}, \frac{3-s}{2}\right), -\frac{a^2}{4}\right] + \frac{1}{s} H\left[-\frac{s}{2}, \left(\frac{1}{2}, \frac{2-s}{2}\right), -\frac{a^2}{4}\right]$$

where the hypergeometric function H is defined by

$$H(\alpha, (\beta, \gamma), z) = \sum_{k=0}^{\infty} \frac{(\alpha)_k}{(\beta)_k (\gamma)_k} \frac{z^k}{k!}.$$

One sets $(x)_k = \prod_{j=0}^{k-1} (x+j)$. Note that the formulas simplify as follows

$$\frac{1}{s-1} H\left[\frac{1-s}{2}, \left(\frac{3}{2}, \frac{3-s}{2}\right), -\frac{a^2}{4}\right] = \sum_{k=0}^{\infty} \frac{(-a^2)^k}{(2k+1)!(s-(2k+1))}$$

and

$$\frac{1}{s} H\left[-\frac{s}{2}, \left(\frac{1}{2}, \frac{2-s}{2}\right), -\frac{a^2}{4}\right] = \sum_{k=0}^{\infty} \frac{(-a^2)^k}{(2k)!(s-2k)}.$$

By using (53) and expanding the exponential in powers of a in the integral

$$\int_0^1 e^{iau} u^{-s} d^*u = \sum_{n=0}^{\infty} \int_0^1 \frac{(iau)^n}{n!} u^{-s} d^*u$$

the resulting expression for $f(s, a)$ in terms of hypergeometric functions becomes

$$(56) \quad f(s, a) = e^{-\frac{1}{2}i\pi s} a^s \Gamma(-s) + \sum_{n=0}^{\infty} \frac{(ia)^n}{n!(s-n)}.$$

Thus one gets

LEMMA 4.12. *For $a > 0$, the following identity holds*

$$f(s, a) = e^{-\frac{1}{2}i\pi s} a^s \Gamma(-s) - \sum_{\text{poles}} \frac{\text{residue}}{s-n}.$$

PROOF. The last term of the expression (56) is a sum of the form $\sum_{\text{poles } g} \frac{\text{residue}(g)}{s-n}$ where $g(s) = e^{-\frac{1}{2}i\pi s} a^s \Gamma(-s)$. This suffices to conclude the proof since one knows from Lemma 4.11 that $f(s, a)$ is an entire function of s . One can also check directly that the expression for the residues as in (56) is correct by using *e.g.* the formula of complements. \square

4.5 Zeta function of Noetherian \mathbb{F}_1 -schemes.

The above discussion has shown that the elementary constituents of the zeta function of a Noetherian \mathbb{F}_1 -scheme are of the following type

$$(57) \quad \xi_d(s) = s^{-\frac{\varphi(d)}{d}} e^{-\frac{\varphi(d)}{d} H_d(s)}$$

where $H_d(s)$ is the primitive, vanishing for $\Re(s) \rightarrow \infty$, of the entire function

$$(58) \quad \partial_s H_d(s) = \sum_{\substack{|k| \leq d/2 \\ k \neq 0}} e^{-i\frac{2\pi k}{d}} f\left(s, \frac{2\pi k}{d}\right).$$

When d is even, one divides by 2 the contribution of $k = \frac{d}{2}$. Note that, by Lemma 4.12, the function $\partial_s H_d(s)$ is obtained by applying the transformation

$$F \mapsto F - \sum_{\text{poles}} \frac{\text{residue}}{s-n}$$

to the function

$$F_d(s) = \Gamma(-s) \sum_{\substack{|k| \leq d/2 \\ k \neq 0}} \cos\left(\frac{2\pi k}{d} + \frac{\pi s}{2}\right) \left(2\pi \frac{k}{d}\right)^s.$$

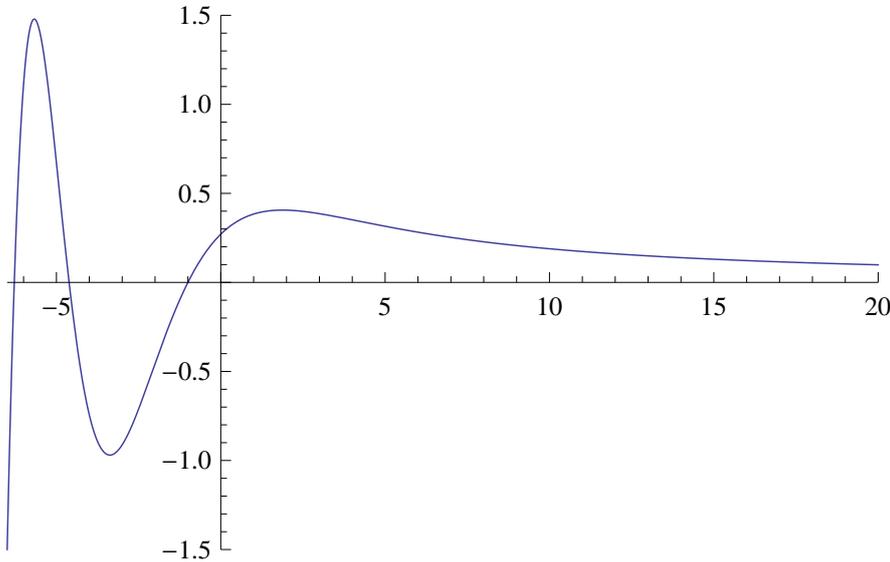


Fig. 5. Graph of the function $\partial_s H_d(s)$ for $d = 3$.

THEOREM 4.13. *Let X be a Noetherian \mathbb{F}_1 -scheme. Then the zeta function of X over \mathbb{F}_1 is a finite product*

$$(59) \quad \zeta_X(s) = \prod_{x \in X} \zeta_{X_x}(s)$$

where X_x denotes the constituent of X over the residue field $\kappa(x) = \mathbb{F}_1[\mathcal{O}_{X,x}^*]$ and $\mathcal{O}_{X,x}^* = \Gamma$ is a finitely generated abelian group such as $\Gamma = H \times \mathbb{Z}^n$ ($H =$ finite torsion group). The zeta function of each constituent X_x takes the following form

$$(60) \quad \zeta_{X_x}(s) = \prod_{k \geq 0} \zeta(\mathbb{F}_1[H], s - n + k)^{(-1)^k \binom{n}{k}}$$

where $\zeta(\mathbb{F}_1[H], s)$ is the product

$$\zeta(\mathbb{F}_1[H], s) = \prod_{d \mid |H|} \xi_d(s)^{\gamma(H,d)}$$

where $\gamma(H, d)$ denotes the number of cyclic subgroups $C \subset H$ of order d .

PROOF. The proof of (59) follows the same lines as that given in Theorem 4.3. The expression (60) for $\zeta_{X_x}(s)$ in terms of $\zeta(\mathbb{F}_1[H], s)$ follows from (51) and the simple translation in s that the multiplication of the counting function by a power of q generates using Lemma 4.10. By (51) and (50) it remains to show that the zeta function $Z_d(s)$ associated to the counting function (50) coincides with $\xi_d(s)$ defined in (57). By Lemma 4.10 and (52) the logarithmic derivative of $Z_d(s)$ is

$$\frac{\partial_s Z_d(s)}{Z_d(s)} = - \int_1^\infty \frac{\varphi(d)}{d} \left(\sum_{|k| < d/2} e^{2i\pi \frac{(u-1)k}{d}} + \epsilon_d \cos(\pi(u-1)) \right) u^{-s} d^* u.$$

The term coming from $k = 0$ contributes with $-\frac{\varphi(d)}{d} \frac{1}{s}$ and thus corresponds to the fractional power $s^{-\frac{\varphi(d)}{d}}$ in (57). The other terms contribute with integrals of the form

$$I(s, \alpha) = \int_1^\infty e^{2\pi i \alpha (u-1)} u^{-s} d^* u.$$

One has

$$I(s, \alpha) = e^{-2\pi i \alpha} \int_1^\infty e^{2\pi i \alpha u} u^{-s} d^* u = e^{-2\pi i \alpha} (2\pi \alpha)^s \int_{2\pi \alpha}^\infty e^{iv} v^{-s} d^* v.$$

Thus with the notation (54) one obtains

$$I(s, \alpha) = e^{-ia} f(s, a), \quad a = 2\pi \alpha.$$

The equality $Z_d(s) = \xi_d(s)$ follows using (58). \square

COROLLARY 4.14. *Let X be a Noetherian \mathbb{F}_1 -scheme. Then the zeta function of X is the product*

$$\zeta_X(s) = e^{h(s)} \prod_{j=0}^n (s-j)^{\alpha_j}$$

of an exponential of an entire function $h(s)$ by a finite product of fractional powers of simple monomials. The exponents α_j are rational numbers given explicitly by

$$(61) \quad \alpha_j = (-1)^{j+1} \sum_{x \in X} (-1)^{n(x)} \binom{n(x)}{j} \sum_d \frac{1}{d} \nu(d, \mathcal{O}_{X,x}^\times)$$

where $n(x)$ is the local dimension (i.e. the rank of $\mathcal{O}_{X,x}^\times$), and $\nu(d, \mathcal{O}_{X,x}^\times)$ is the number of injective homomorphisms from $\mathbb{Z}/d\mathbb{Z}$ to $\mathcal{O}_{X,x}^\times$.

PROOF. By (57) one has

$$\zeta(\mathbb{F}_1[H], s) = \prod_{d||H|} \xi_d(s)^{\gamma(H,d)} = s^{-\epsilon_H} e^{-\sum_{d||H|} \frac{\varphi(d)\gamma(H,d)}{d} H_d(s)}$$

where

$$\epsilon_H = \sum_{d||H|} \frac{\varphi(d)\gamma(H,d)}{d}.$$

Next, by (60) one has

$$\zeta(\mathbb{F}_1[\Gamma], s) = \prod_{k \geq 0} \zeta(\mathbb{F}_1[H], s - n + k)^{(-1)^k \binom{n}{k}}$$

which is a product of the form

$$\zeta(\mathbb{F}_1[\Gamma], s) = \prod_{k \geq 0} (s - j)^{-(-1)^{n-j} \binom{n}{j} \epsilon_H} e^{h(s)}$$

where $h(s)$ is an entire function. Thus one gets that the exponent α_j of $(s - j)$ is

$$\alpha_j = (-1)^{j+1} \sum_{x \in X} (-1)^{n(x)} \binom{n(x)}{j} \sum_{d||H_x|} \frac{\varphi(d)\gamma(H_x, d)}{d}$$

where $n(x)$ is the local dimension and H_x is the finite group in the decomposition of $\mathcal{O}_{X,x}^\times$. The above expression gives (61) since $\varphi(d)\gamma(H_x, d)$ is the number of injective homomorphisms from $\mathbb{Z}/d\mathbb{Z}$ to $\mathcal{O}_{X,x}^\times$. \square

5. BEYOND \mathbb{F}_1 -SCHEMES

One may naturally wonder on the adeptness of the method of the computation of the zeta function over \mathbb{F}_1 that we have described in the above section, for a possible generalization beyond the case of \mathbb{Z} -schemes associated to Noetherian \mathbb{F}_1 -schemes. In [C2], we have already given evidence on the effectiveness of the integral formula of Lemma 4.10 of §4.3, by showing that there exists a *uniquely* defined distribution $N(u)$ on $[1, \infty)$ which describes the counting function for the hypothetical curve $C = \overline{\text{Spec } \mathbb{Z}}$ over \mathbb{F}_1 whose zeta function $\zeta_C(s)$ (over \mathbb{F}_1) coincides with the completed Riemann zeta function $\zeta_{\mathbb{Q}}(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s)$ over \mathbb{C} .

The goal of this section is to show that as long as one is only interested in the singularities of the zeta function, one may, in the case of Noetherian \mathbb{F}_1 -schemes, replace the integral which appears in (52) by the corresponding infinite sum *i.e.*

$$(62) \quad - \int_1^\infty N(u) u^{-s} d^*u \rightsquigarrow - \sum_{n \geq 1} N(n) n^{-s-1},$$

which is now defined without any need for interpolation. This substitution provides one with a natural definition of a modified zeta function that is defined by the formula

$$\frac{\partial_s \zeta_N^{\text{disc}}(s)}{\zeta_N^{\text{disc}}(s)} = - \sum_{n=1}^{\infty} N(n) n^{-s-1}.$$

In § 5.3 we compute this function for a *particular* choice of the extension of the counting function $N(q)$ in the case of elliptic curves over \mathbb{Q} .

5.1 Modified zeta function.

Within the category of the Noetherian \mathbb{F}_1 -schemes, one has the following result

PROPOSITION 5.1. *The replacement (62) in the definition of the logarithmic derivative $\frac{\partial_s \zeta_N(s)}{\zeta_N(s)}$ as in (52), does not alter the singularities of the zeta function associated to a Noetherian \mathbb{F}_1 -scheme. In fact, the ratio of these two zeta functions $\zeta_N(s)$ and $\zeta_N^{\text{disc}}(s)$ is the exponential of an entire function.*

PROOF. It is enough to treat the case of a counting function $N(u)$, of the real variable u , of the form

$$N(u) = \frac{\varphi(d)}{d} u^\ell \left(\sum_{|k| < d/2} e^{2i\pi \frac{(u-1)k}{d}} + \epsilon_d \cos(\pi(u-1)) \right)$$

and show that the following is an entire function of $s \in \mathbb{C}$

$$h(s) = \int_1^\infty N(u) u^{-s} d^*u - \sum_{n=1}^{\infty} N(n) n^{-s-1}.$$

Notice that the term u^ℓ generates a shift in s and thus we can assume that $\ell = 0$. Let $G(d) = (\mathbb{Z}/d\mathbb{Z})^*$ be the multiplicative group of residues modulo d which are prime to d . By extending the characters $\chi \in \hat{G}(d)$ by 0 on residues modulo d which are not prime to d , one obtains the equality

$$\sum_{\chi \in \hat{G}(d)} \chi(n) = \begin{cases} \varphi(d), & \text{if } n = 1 \\ 0, & \text{if } n \neq 1. \end{cases}$$

Thus, the restriction of $N(u)$ to the integers agrees with the following sum

$$N(n) = \sum_{\chi \in \hat{G}(d)} \chi(n)$$

and one gets

$$\sum_{n \geq 1} N(n) n^{-s-1} = \sum_{\chi \in \hat{G}(d)} L(\chi, s+1).$$

When $\chi \neq 1$, the function $L(\chi, s+1)$ is entire, thus the only singularity arises from the function $L(1, s+1)$ which is known to have a unique pole at $s=0$ with residue $\prod_{p|d}(1 - \frac{1}{p})$. The only singularity of the integral $\int_1^\infty N(u) u^{-s} d^*u$ is due to the contribution of the constant term *i.e.*

$$\int_1^\infty \frac{\varphi(d)}{d} u^{-s} d^*u = \frac{\varphi(d)}{d} \frac{1}{s}.$$

Thus the equality $\prod_{p|d}(1 - \frac{1}{p}) = \frac{\varphi(d)}{d}$ shows that the function $h(s)$ is entire. \square

We can therefore adopt the following definition

DEFINITION 5.2. *Let X be an \mathbb{F}_1 -scheme. The modified zeta function $\zeta_X^{\text{disc}}(s)$ is defined by*

$$(63) \quad \frac{\partial_s \zeta_X^{\text{disc}}(s)}{\zeta_X^{\text{disc}}(s)} = - \sum_{n \geq 1} N(n) n^{-s-1}$$

where $N(n+1) = \#X(\mathbb{F}_{1^n})$.

By Proposition 5.1, the singularities of this modified zeta function are the same as the singularities of $\zeta_X(s)$: *cf.* Corollary 4.14. The advantage of this more general definition is that it requires no choice of an interpolating function. This means that one can define $\zeta_X^{\text{disc}}(s)$, up to a multiplicative normalization factor, by just requiring some polynomial control on the size of growth of the finite set $X(\mathbb{F}_{1^n})$.

REMARK 5.3. There is a superficial resemblance between the right hand side of (63) that defines the logarithmic derivative of $\zeta_X^{\text{disc}}(s)$ and the “absolute” Igusa zeta function associated in [DKK] to an \mathbb{F}_1 -scheme. However, there is a shift of 1 in the argument n which is not easy to eliminate and that introduces a fundamental difference. Thus, in terms of points defined over \mathbb{F}_{1^n} we obtain

$$\sum_{n \geq 1} N(n) n^{-s-1} = \sum_{n \geq 1} X(\mathbb{F}_{1^{n-1}}) n^{-s-1}.$$

On the other hand, the zeta function associated in [DKK] is given by

$$\zeta^I(s, X) = \sum_{n \geq 1} X(\mathbb{F}_{1^n}) n^{-s}.$$

The shift of 1 in s is easily accounted for, but not the replacement of $X(\mathbb{F}_{1^{n-1}})$ by $X(\mathbb{F}_{1^n})$. In the next subsection we will show how this shift manifests itself in a concrete example.

5.2 Modified zeta function and $\overline{\text{Spec } \mathbb{Z}}$.

In [CC2], we have shown how to determine the counting distribution $N(q)$, defined for $q \in [1, \infty)$ in such a way that the zeta function as in (52) gives the complete Riemann zeta function, *i.e.* so that the following equation holds

$$(64) \quad \frac{\partial_s \zeta_{\mathbb{Q}}(s)}{\zeta_{\mathbb{Q}}(s)} = - \int_1^\infty N(u) u^{-s} d^*u,$$

where

$$\zeta_{\mathbb{Q}}(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s).$$

Moreover, using convergence in the sense of distributions one obtains

$$N(q) = q - \sum_{\rho \in \mathbb{Z}} \text{order}(\rho) q^\rho + 1.$$

This is in perfect analogy with the theory for function fields. Indeed, for a smooth curve X over a finite field \mathbb{F}_{q_0} and for any power $q = q_0^\ell$ of the order q_0 of the finite field of constants one has

$$\#X(\mathbb{F}_q) = N(q) = q - \sum_{\rho \in \mathbb{Z}} \text{order}(\rho) q^\rho + 1.$$

In the above formula, we have written the complex eigenvalues of the characteristic polynomial of the Frobenius operator acting on the cohomology of the curve in the form $\alpha = q_0^\rho$.

While these results supply a strong indication on the coherence of the quest for an arithmetic theory over \mathbb{F}_1 , they also indicate that the similarities with the geometry over finite fields are also elusive and that the \mathbb{F}_1 -counterpart of the classical theory will be richer in new ingredients. In this section, we will study what type of additional information one can gather about the hypothetical curve $C = \text{Spec } \mathbb{Z}$ by using the modified zeta function, *i.e.* the simplified formula (72). Since this simplified formula clearly neglects the contribution of the archimedean place, it seems natural to replace the complete zeta function $\zeta_{\mathbb{Q}}(s)$ by the Riemann zeta function $\zeta(s)$. Thus, the simplified form of (64) takes the form

$$\frac{\partial_s \zeta(s)}{\zeta(s)} = - \sum_1^\infty N(n) n^{-s-1}.$$

This supplies for the counting function $N(n)$ the formula

$$N(n) = n\Lambda(n)$$

where $\Lambda(n)$ is the von-Mangoldt function with value $\log p$ for powers p^ℓ of primes and zero otherwise. We now use the relation $N(n+1) = \#X(\mathbb{F}_{1^{n+1}})$ of Definition 5.2 and conclude that the sought for “scheme over \mathbb{F}_1 ” should fulfill the following condition

$$(65) \quad \#(X(\mathbb{F}_{1^n})) = \begin{cases} 0, & \text{if } n+1 \text{ is not a prime power} \\ (n+1) \log p, & \text{if } n = p^\ell - 1, p \text{ prime.} \end{cases}$$

The two obvious difficulties are that $(n+1) \log p$ is not an integer, and that multiples $m = nk$ of numbers of the form $n = p^\ell - 1$ are no longer of a similar form, while there are morphisms from \mathbb{F}_{1^n} to \mathbb{F}_{1^m} . This shows that functoriality can only hold in a more restrictive manner. Moreover, at first sight, it seems hopeless to find a natural construction starting from a monoid M which singles out among the monoids $M = \mathbb{F}_1[\mathbb{Z}/n\mathbb{Z}] = \mathbb{Z}/n\mathbb{Z} \cup \{0\}$ those for which $n = p^\ell - 1$, for some prime power. However, this is precisely what is achieved by the study of the additive structure in §2.1. Indeed, one has

COROLLARY 5.4. *Let $M = \mathbb{F}_1[\mathbb{Z}/n\mathbb{Z}] = \mathbb{Z}/n\mathbb{Z} \cup \{0\}$ viewed as a commutative (pointed) monoid. Then, $n = p^\ell - 1$ for a prime power p^ℓ if and only if the following set $A(M)$ is non-empty. $A(M)$ is the set of maps $s : M \rightarrow M$ such that*

- s commutes with its conjugates by multiplication by elements of M^\times
- $s(0) = 1$.

PROOF. This would follow from Corollary 2.2 if we assumed that s is bijective. So, we need to prove that this assumption is unnecessary. The proof of Theorem 2.1 shows that, for $s \in A(M)$, M becomes a semi-field, where we use (10) to define the addition. Moreover since M is finite, if it is not a field M contains a (prime) semi-ring $B(n, i)$ for finite n and i . As explained after Proposition 2.6, this implies $n = 2$ and $i = 1$ so that M is an idempotent semi-field. Finally, by Proposition 2.13 one gets that unless M is a field it is equal to \mathbb{B} . Thus we obtain that the cardinality of M is a prime power. \square

The cardinality of the set $A(M)$ can be explicitly computed. By using Corollary 2.2 and the fact that the automorphisms of the finite field \mathbb{F}_q are powers of the Frobenius, one gets for⁶ $n > 1$

$$\#(A(\mathbb{F}_{1^n})) = \begin{cases} 0, & \text{if } n + 1 \text{ is not a prime power} \\ \varphi(p^\ell - 1)/\ell, & \text{if } n = p^\ell - 1, p \text{ prime} \end{cases}$$

where φ is the Euler totient function. This produces a result which, although not exactly equal to the (non-integer) value as in (65), comes rather close. Moreover, one should acknowledge the fact that even though the definition of $A(M)$ is natural it is only functorial for isomorphisms and not for arbitrary morphisms.

5.3 Elliptic curves.

Definition 5.2 applies any time one has a reasonable guess for the definition of an extension of the counting function of points from the case $q = p^\ell$ to the case of an arbitrary positive integer. For elliptic curves E over \mathbb{Q} , one may use the associated modular form

$$F_E(\tau) = \sum_{n=1}^{\infty} a(n)q^n, \quad q = e^{2\pi i\tau}$$

since the sequence $a(n)$ of the coefficients of the above series is defined for all values of n . Moreover, these Fourier coefficients also fulfill equations

$$(66) \quad N(p, E) = \#E(\mathbb{F}_p) = p + 1 - a(p)$$

at each prime number p of good reduction for the curve E . This choice is, however, a bit too naive since (66) does not continue to hold at prime powers.

We say that a function $t(n)$ is weakly multiplicative when

$$t(nm) = t(n)t(m) \text{ if } n \text{ is relatively prime to } m$$

We define the function $t(n)$ as the only weakly multiplicative function which agrees with $a(p)$ at each prime and for which (66) continues to hold for prime powers. Then we have the following result

LEMMA 5.5. *Let $t(n)$ be the only weakly multiplicative function such that $t(1) = 1$ and*

$$(67) \quad N(q, E) = q + 1 - t(q)$$

⁶one has $\#(A(\mathbb{F}_1)) = 2$.

for any prime power q . Then, the generating function

$$R(s, E) = \sum_{n \geq 0} t(n) n^{-s}$$

has the following description

$$(68) \quad R(s, E) = \frac{L(s, E)}{\zeta(2s-1)M(s)}.$$

$L(s, E)$ is the L -function of the elliptic curve, $\zeta(s)$ is the Riemann zeta function, and

$$M(s) = \prod_{p \in S} (1 - p^{1-2s})$$

is a finite product of simple factors over the set S of primes of bad reduction for E .

PROOF. One has an Euler product for the L -function $L(s, E) = \sum a(n)n^{-s}$ of the elliptic curve of the form

$$L(s, E) = \prod_p L_p(s, E).$$

For almost all primes, *i.e.* for $p \notin S$ with S a finite set

$$(69) \quad L_p(s, E) = ((1 - \alpha_p p^{-s})(1 - \bar{\alpha}_p p^{-s}))^{-1} = \sum_{n=0}^{\infty} a(p^n) p^{-ns}$$

where $\alpha_p = \sqrt{p} e^{i\theta_p}$. Since the function $t(n)$ is weakly multiplicative one has an Euler product

$$(70) \quad R(s, E) = \sum_{n \geq 0} t(n) n^{-s} = \prod_p \left(\sum_{n \geq 0} t(p^n) p^{-ns} \right) = \prod_p R_p(s, E).$$

Let $p \notin S$ be a prime of good reduction. Then for $q = p^\ell$, one has

$$N(q, E) = q + 1 - \alpha_p^\ell - \bar{\alpha}_p^\ell.$$

We now show that

$$(71) \quad (1 - p^{1-2s}) \sum_{n=0}^{\infty} a(p^n) p^{-ns} = \sum_{n=0}^{\infty} t(p^n) p^{-ns}.$$

This relation follows from (69) and the equality

$$\frac{(1 - p x^2)}{(1 - \alpha_p x)(1 - \bar{\alpha}_p x)} = \frac{1}{(1 - \alpha_p x)} + \frac{1}{(1 - \bar{\alpha}_p x)} - 1$$

for $x = p^{-s}$. The above formula appears in the expression of the Poisson kernel (*cf.* [R] §§ 5.24, 11.5)

$$P_r(\theta) = \sum_{-\infty}^{\infty} r^{|n|} e^{in\theta} = \frac{1 - r^2}{1 - 2r \cos \theta + r^2}.$$

Using (71) one gets

$$(72) \quad R_p(s, E) = (1 - p^{1-2s}) \sum_{n=0}^{\infty} a(p^n) p^{-ns}.$$

When $p \in S$, the local factor $L_p(s, E)$ of the L -function takes one of the following descriptions (*cf.* [Si] Appendix C §16)

- $L_p(s, E) = \sum_{n=0}^{\infty} p^{-ns}$ when E has split multiplicative reduction at p .
- $L_p(s, E) = \sum_{n=0}^{\infty} (-1)^n p^{-ns}$ when E has non-split multiplicative reduction at p .
- $L_p(s, E) = 1$ when E has additive reduction at p .

We prove now that in any of the above cases one has

$$(73) \quad R_p(s, E) = L_p(s, E).$$

One knows that in the singular case, the elliptic curve has exactly one singular point. This point is already defined over \mathbb{F}_p since if a cubic equation has a double root this root is rational (*cf.* Appendix 6). Thus, for any power $q = p^\ell$ one has

$$N(q, E) = 1 + N_{\text{ns}}(q, E)$$

where the cardinality $N_{\text{ns}}(q, E)$ of the set of the non-singular points is given, for any power $q = p^\ell$, as follows (*cf.* [Si] exercise 3.5 page 104)

- $N_{\text{ns}}(q, E) = q - 1$, if E has split multiplicative reduction over \mathbb{F}_q .
- $N_{\text{ns}}(q, E) = q + 1$, if E has non-split multiplicative reduction over \mathbb{F}_q .
- $N_{\text{ns}}(q, E) = q$, if E has additive reduction over \mathbb{F}_q .

Thus, it follows from the definition (67), that the value $t(p^\ell)$ assumes one of the following three descriptions

- $t(p^\ell) = 1$ for all ℓ , if E has split multiplicative reduction at p .
- $t(p^\ell) = (-1)^\ell$, if E has non-split multiplicative reduction at p .
- $t(p^\ell) = 0$, if E has additive reduction at p .

The second case arises since the split property of E depends upon the parity of ℓ . The equality (73) is checked for all primes of bad reduction $p \in S$. Together with (72) and (70), this implies (68). \square

REMARK 5.6. Note that the function $N(n) = n + 1 - t(n)$ is always positive. Indeed, it is enough to show that for all n one has $|t(n)| \leq n$. Since $t(n)$ is weakly multiplicative, it is enough to show the above inequality when $n = p^k$ is a prime power. In the case of good reduction, one has $t(p^k) = \alpha_p^k + \bar{\alpha}_p^k$ and since the modulus of α_p is \sqrt{p} one gets

$$|t(q)| \leq 2\sqrt{q}, \quad q = p^k.$$

This proves that $|t(q)| \leq q$ for all q satisfying $2\sqrt{q} \leq q$ *i.e.* when $q \geq 4$. For $q = 2$ one has $2\sqrt{2} \cong 2.828 < 3$ and since $|t(2)|$ is an integer one obtains $|t(2)| \leq 2$. Similarly, for $q = 3$ one has $2\sqrt{3} \cong 3.4641 < 4$ and thus $|t(3)| \leq 3$. In the case of bad reduction one has always $|t(q)| \leq 1$.

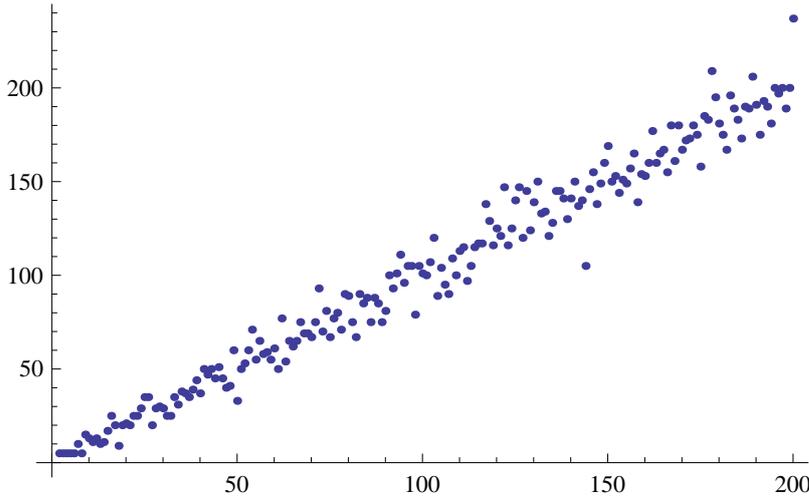


FIG. 6.. Graph of the function $N(n) = n + 1 - t(n)$ for $n \leq 200$, for the elliptic curve of the Example 5.8.

Definition 5.2 gives the following equation for the modified zeta function $\zeta_N^{\text{disc}}(s)$ associated to the counting function $N(q, E)$

$$\frac{\partial_s \zeta_N^{\text{disc}}(s)}{\zeta_N^{\text{disc}}(s)} = - \sum_{n=1}^{\infty} (n + 1 - t(n)) n^{-s-1} = -\zeta(s+1) - \zeta(s) + R(s+1, E).$$

Using Lemma 5.5 we then obtain

THEOREM 5.7. *Let E be an elliptic curve over \mathbb{Q} and let $L(s, E)$ be the associated L -function. Then the modified zeta function $\zeta_N^{\text{disc}}(s)$ of E fulfills the following equality*

$$\frac{\partial_s \zeta_N^{\text{disc}}(s)}{\zeta_N^{\text{disc}}(s)} = -\zeta(s+1) - \zeta(s) + \frac{L(s+1, E)}{\zeta(2s+1)M(s+1)}$$

where $\zeta(s)$ is the Riemann zeta function.

The Riemann zeta function has trivial zeros at the points $-2n$ for $n \geq 1$. They generate singularities of $\zeta_E(s)$ at the points $s = -n - \frac{1}{2}$, i.e. at $s = -\frac{3}{2}, -\frac{5}{2}, \dots$. If RH holds, the non-trivial zeros of the Riemann zeta function generate singularities at points which have real part $-\frac{1}{4}$. Note that the poles of the archimedean local factor $N_E^{s/2} (2\pi)^{-s} \Gamma(s)$ ($N_E =$ conductor) of the L -function of E determine trivial zeros. These zeros occur for $s \in -\mathbb{N}$ and do not cancel the above singularities. Finally, we have all the zeros of $M(s+1)$. Each factor $(1 - p^{-(2s-1)})$ contributes by an arithmetic progression with real part $-\frac{1}{2}$

$$s \in -\frac{1}{2} + \bigcup_{p \in S} \frac{\pi i}{\log p} \mathbb{Z}.$$

Note that the pole at $-\frac{1}{2}$ has order the cardinality of S .

For a better understanding of the role played by the primes of bad reduction we consider the following example.

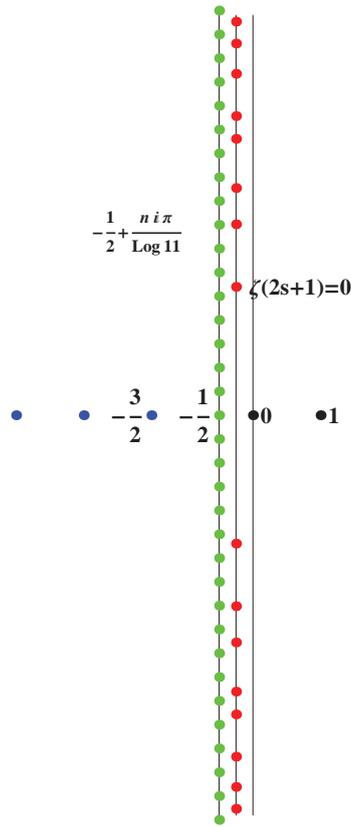


Fig. 7. Singularities of $\zeta_N^{\text{disc}}(s)$

EXAMPLE 5.8. Let us consider the elliptic curve in $\mathbb{P}^2(\mathbb{Q})$ given by the zeros of the homogeneous equation

$$E : Y^2Z + YZ^2 = X^3 - X^2Z - 10XZ^2 - 20Z^3.$$

Then the sequence $a(n)$ is given by the coefficients of the modular form

$$F_E(q) = \sum_{n=1}^{\infty} a(n)q^n = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2.$$

These coefficients are easy to compute, for small values of n , using the Euler formula

$$\prod_{n=1}^{\infty} (1 - q^n) = 1 + \sum_{n=1}^{\infty} (-1)^n (q^{(3n^2-n)/2} + q^{(3n^2+n)/2}).$$

The first values are

$$a(0) = 0, a(1) = 1, a(2) = -2, a(3) = -1, a(4) = 2, a(5) = 1, a(6) = 2, a(7) = -2, \dots$$

The function $N(n)$ is given by $N(n) = n + 1 - t(n)$. It is important to check that it takes positive values. Its graph is depicted in Figure 6. In this example, the only

prime of bad reduction is $p = 11$ and the singularities of the modified zeta function $\zeta_N^{\text{disc}}(s)$ are described in Figure 7.

The challenging question is that to define a natural functor \underline{E} to finite sets, such that $\#\underline{E}(\mathbb{F}_{1^n}) = N(n+1)$ for all n .

6. APPENDIX: PRIMES OF BAD REDUCTION OF AN ELLIPTIC CURVE

In this appendix we supply more details on the process of counting of points used in the proof of Lemma 5.5. In order to reduce modulo p an elliptic curve E over \mathbb{Q} , the first step is to take an equation of the curve which is in minimal Weierstrass form over the local field \mathbb{Q}_p *i.e.* of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_j \in \mathbb{Z}_p$ such that the power of p dividing the discriminant is minimal. Such a minimal Weierstrass equation can always be found (*cf.* [Si] Proposition VII 1.3) and is unique up to a change of variables of the form

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t$$

for $u \in \mathbb{Z}_p^*$ and $r, s, t \in \mathbb{Z}_p$. One then considers the reduced equation

$$(74) \quad y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

where \bar{a}_j is the residue of a_j modulo p . This equation is unique up to the standard changes of coordinates on \mathbb{F}_p and defines a curve over \mathbb{F}_p . One then looks for points of this curve *i.e.* solutions of equation (74) (together with the point at ∞), in the extensions \mathbb{F}_q , $q = p^\ell$. When $p > 2$, one can always write the reduced equation in the form

$$y^2 = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6.$$

Thus assuming $p \neq 2$, a singular point has second coordinate $y = 0$ while x is the common root of $x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6 = 0$, with $3x^2 + 2\bar{a}_2x + \bar{a}_4 = 0$. This proves that the elliptic curve has a unique singular point and that both its coordinates belong to \mathbb{F}_p . After a translation of x one can then write the equation of the curve in the form $y^2 = x^2(x - \beta)$ with $\beta \in \mathbb{F}_p$. There are three cases

- $\beta = 0$ is the case of additive reduction: one has a cusp at $(0, 0)$.
- $\beta \neq 0$, $-\beta \in \mathbb{F}_p^2$ means split multiplicative reduction.
- $\beta \neq 0$, $-\beta \notin \mathbb{F}_p^2$ is the remaining case of non-split multiplicative reduction.

Let now \mathbb{K} be a perfect field of characteristic 2. One starts with a Weierstrass equation in general form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then, when the curve is singular it can be written, using affine transformations of (x, y) with coefficients in \mathbb{K} , in the form

$$(75) \quad y^2 = x^3 + a_4x + a_6.$$

We refer to [Si] (Appendix A, Propositions 1.2 and 1.1) for details. Indeed, the curve is singular if and only if its discriminant vanishes (*cf.* Proposition 1.2 in *op.cit.*). Then, one can use the description of the curve as in Proposition 1.1 c) of *op.cit.* to deduce that $a_3 = 0$, since $\Delta = 0$. The point at ∞ is always non-singular.

A point (x, y) is singular if and only if (75) holds together with $3x^2 + a_4 = 0$. This equation is equivalent to $x^2 = a_4$ and uniquely determines x since the field is perfect. Then one gets $y^2 = a_6$ since $x^3 + a_4x = x(x^2 + a_4) = 0$. This in turns uniquely determines y since \mathbb{K} is perfect. Thus, for any finite field of characteristic two, one concludes that, if the curve is singular, it has exactly one singular point. In fact, for elliptic curves over \mathbb{Q} , there are only 4 cases to look at in characteristic two. They correspond to the values $a_4 \in \{0, 1\}$ and $a_6 \in \{0, 1\}$.

One can always assume that $a_6 = 0$ by replacing y with $y + 1$, if needed. For $a_4 = a_6 = 0$ one has a cusp at $(0, 0)$ and the points over \mathbb{F}_q are labeled by the x coordinate. Thus there are $q + 1$ points over \mathbb{F}_q when $q = 2^\ell$. For $a_4 = 1$, $a_6 = 0$, the singular point is $P = (1, 0)$. After shifting x by 1 the equation becomes $y^2 = x^2(x + 1)$ and thus the singular point is also a cusp. The points over \mathbb{F}_q are labeled as $(1 + t^2, t(1 + t^2))$ for $t \in \mathbb{F}_q$ (together with the point at ∞). Again, there are $q + 1$ points over \mathbb{F}_q when $q = 2^\ell$.

References

- [AK] J. Ax and S. Kochen, *Diophantine problems over local fields I*, American Journal of Mathematics **87** (1965), 605–630.
- [B] N. Bourbaki, *Algèbre commutative*, Éléments de Math. Hermann, Paris (1961–65).
- [CC1] A. Connes and C. Consani, *On the notion of geometry over \mathbb{F}_1* , Journal of Algebraic Geometry arXiv:08092926v2 [mathAG] (to appear).
- [CC2] A. Connes and C. Consani, *Schemes over \mathbb{F}_1 and zeta functions*, Compositio Mathematica arXiv:0903.2024v3 [mathAG,NT] (to appear).
- [Co] J. Conway, *On Numbers and Games*, Academic Press, London (1976).
- [D1] A. Deitmar, *Schemes over \mathbb{F}_1* , Number Fields and Function Fields Two Parallel Worlds (Ed. by G. van der Geer, B. Moonen, R. Schoof), Progr. in Math **239** (2005).
- [D2] A. Deitmar, *F1-schemes and toric varieties*, in Contributions to Algebra and Geometry **49** 2 (2008), 517–525.
- [D3] A. Deitmar, *Remarks on zeta functions and K-theory over F1*, Proc. Japan Acad. Ser. A Math. Sci. **82** 8 (2006), 141–146.
- [DG] M. Demazure and P. Gabriel, *Groupes algébriques*, Masson & CIE, Éditeur Paris (1970).
- [DKK] A. Deitmar, S. Koyama and N. Kurokawa, *Absolute zeta functions*, Proc. Japan Acad. Ser. A Math. Sci. **84** 8 (2008), 138–142.
- [Ga] A. Gathmann, *Tropical algebraic geometry*, Jahresber. Deutsch. Math.-Verein **108** 1 (2006), 3–32.
- [Gi] R. Gilmer, *Commutative semigroup rings*, University of Chicago Press (1980).
- [Go] J. Golan, *Semi-rings and their applications (Updated and expanded version of The theory of semi-rings, with applications to mathematics and theoretical computer science)*, Kluwer Academic Publishers, Dordrecht (1999).
- [Gr] P. A. Grillet, *Semigroups. An introduction to the structure theory*, Mercel Dekker, Inc. New-York, Basel, Hong Kong (1995).
- [IMS] I. Itenberg, G. Mikhalkin and E. Shustin, *Tropical algebraic geometry Second edition*, Oberwolfach Seminars 35, Birkhuser Verlag, Basel (2009), x+104 pp.
- [KM] V. Kolokoltsov and V. Maslov, *Idempotent analysis and its applications. Translation of Idempotent analysis and its application in optimal control (Russian) in “Nauka” Moscow, 1994. Translated by V. E. Nazaikinskii. With an appendix by Pierre Del Moral.*, Mathematics and its Applications, Kluwer Academic Publishers Group, Dordrecht **401** (1997).
- [KS] M. Kapranov and A. Smirnov, *Cohomology determinants and reciprocity laws (prepublication)*.
- [KOW] N. Kurokawa, H. Ochiai and A. Wakayama, *Absolute Derivations and Zeta Functions*, Documenta Math. Extra Volume: Kazuya Katos Fiftieth Birthday (2003), 565–584.
- [Ka] K. Kato, *Toric Singularities*, American Journal of Mathematics **116** 5 (1994), 1073–1099.
- [Kr] M. Krasner, *Approximation des corps valués complets de caractéristique $p \neq 0$ par ceux de caractéristique 0*, Colloque d’algèbre supérieure, tenu à Bruxelles du 19 au 22 décembre

- 1956, Centre Belge de Recherches Mathématiques Établissements Ceuterick, Louvain; Librairie Gauthier-Villars, Paris, 129–206.
- [Ku] N. Kurokawa, *Multiple zeta functions: an example in Zeta functions in geometry (Tokyo, 1990)*, Adv. Stud. Pure Math. **21** (1992), 219–226.
- [LL] J. Lopez Pena and O. Lorscheid, *Mapping \mathbb{F}_1 -land: An overview of geometries over the field with one element* arXiv:0909.0069.
- [Le] P. Lescot, *Algèbre absolue* arXiv:0911.1989.
- [Lu] F. Luebeck, www.math.rwth-aachen.de/Frank.Luebeck/data/ConwayPol/index.html.
- [M] Y. I. Manin, *Lectures on zeta functions and motives (according to Deninger and Kurokawa)*, Astérisque **228** (4) (1995), 121–163.
- [R] W. Rudin, *Functional analysis*, International Series in Pure and Applied Mathematics. McGraw-Hill, Inc., New York (1991), xviii+424 pp.
- [Se] J. P. Serre, *Local fields*, Graduate Texts in Mathematics 67, Springer-Verlag, New York (1979).
- [Si] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York (1986), xii+400 pp.
- [So] C. Soulé, *Les variétés sur le corps à un élément*, Mosc. Math. J. 4 no. 1 (2004), 217–244.
- [TV] B. Töen and M. Vaquié, *Au dessous de Spec(Z)*, K-theory Journal arXiv:0509.684v4 (to appear).

COLLÈGE DE FRANCE, 3 RUE D'ULM, 75231, PARIS CEDEX 05, FRANCE, AND DEPARTMENT OF MATHEMATICS, 1326 STEVENSON CENTER, VANDERBILT UNIVERSITY, NASHVILLE, TN 37240, USA

E-mail address: alain@connes.org

DEPARTMENT OF MATHEMATICS, THE JOHNS HOPKINS UNIVERSITY, BALTIMORE, MD 21218, USA

E-mail address: kc@math.jhu.edu