Rend. Lincei Mat. Appl. 35 (2024), 121–154
DOI 10.4171/RLM/1036

Algebraic Geometry, Number Theory. – *On the metaphysics of* $\mathbb{F}_1$,
by Alain Connes and Caterina Consani, communicated on 21 June 2024.

To Yuri Ivanovich Manin, in memory.

Abstract. – In the present paper, dedicated to Yuri Manin, we investigate the general notion of rings of $\mathbb{S}[\mu_{n,+}]$-polynomials and relate this concept to the known notion of number systems. The Riemann–Roch theorem for the ring $\mathbb{Z}$ of the integers that we obtained recently uses the understanding of $\mathbb{Z}$ as a ring of polynomials $\mathbb{S}[X]$ in one variable over the absolute base $\mathbb{S}$, where $1 + 1 = X + X^2$. The absolute base $\mathbb{S}$ (the categorical version of the sphere spectrum) thus turns out to be a strong candidate for the incarnation of the mysterious $\mathbb{F}_1$.

Keywords. – Riemann–Roch, number systems, adeles, zeta function, sphere spectrum, Witt vectors.

Mathematics Subject Classification 2020. – 14C40 (primary); 14G40, 14H05, 11R56 (secondary).

1. Introduction

> *Les mathématiciens du xvi-ème siècle avaient coutume de parler de la "métaphysique du calcul infinitésimal", de la "métaphysique de la théorie des équations". Ils entendaient par là un ensemble d'analogies vagues, difficilement saisissables et difficilement formulables, qui néanmoins leur semblaient jouer un rôle important à un moment donné dans la recherche et la découverte mathématiques.* *(A. Weil, De la métaphysique aux mathématiques, 1960,* [31]*)*

Yuri Manin, to whose memory we dedicate this article, first recognized in [22] the importance of developing a theory of "absolute coefficients" in arithmetic geometry, independently of the early ideas proposed by R. Steinberg [28] and J. Tits [29] in the context of Chevalley groups. In arithmetic, for number fields, the goal is to provide the geometric counterpart to the construction that A. Weil used in his proof of the Riemann hypothesis for function fields. The search for a close analogy between number fields and function fields of curves in positive characteristic induced Manin to postulate the existence of the absolute point "Spec $\mathbb{F}_1$", over which one could apply Weil's strategy to the study of the Riemann zeta function. For the algebraic scheme Spec $\mathbb{Z}$,

one would then use the spectrum of the tensor product "$\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z}$" as a substitute for the self-product of a curve over (the spectrum of) a finite field.

Manin always advocated the fruitfulness of unexpected interactions between different approaches to a mathematical problem. In Sections 2 and 3 we shall discuss two of such unexpected occurrences, in fact two pillars of our joint work in the past fifteen years. Section 2 is about the hypothetical curve[1] $\mathbf{C}$ that we propose as the absolute geometric entity. Section 3 concerns instead the absolute coefficients. The aim of this paper is to sponsor $\mathbb{S}$ the most basic combinatorial form of the sphere spectrum and of an $\mathbb{S}$-algebra, as the most natural candidate for the absolute coefficients (aka $\mathbb{F}_1$). We claim that this algebra is the absolute "field" of constants over which $\mathbb{Z}$ becomes a ring of polynomials in one variable. This point of view is supported by the Riemann–Roch theorem for the ring $\mathbb{Z}$ recently proved in [15], whose formula shows that the genus of $\overline{\operatorname{Spec} \mathbb{Z}}$ is zero. In an earlier result on the same topic [14], the integers were considered as polynomials over $\mathbb{S}[\pm 1]$ with generator $X = 3$. This fact is based on the balanced ternary numeral system[2] which provides a balanced signed-digit representation of the integers as finite sums of powers of the "variable" $X = 3$ with coefficients in the set $\{-1, 0, 1\}$ underlying the pointed multiplicative monoid $\mu_{2,+}$ of quadratic roots of unity. The new version of the Riemann–Roch theorem for the ring $\mathbb{Z}$ in [15] simplifies the earlier version [14] and it also reconciles the formula (and our understanding of this subject) with the classical number theoretic viewpoint. Indeed, in the analogy between number fields and curves over finite fields, the field $\mathbb{Q}$ has genus zero [32] and it is singled out as the only field contained in any other number field. The view of $\mathbb{Z}$ as a ring of polynomials over the absolute base $\mathbb{S}$ selects the generator $X = -2$. The key fact is that any integer can be uniquely written as a sum of powers of -2 [21].

The above special cases of generators X for rings over finite spherical $\mathbb{S}$-algebras justify a systematic and broader study of rings of $\mathbb{S}[\mu_{n,+}]$-polynomials. In Section 5 we introduce the general notion of rings of $\mathbb{S}[\mu_{n,+}]$-polynomials in one and several variables. Let $n > 0$ be an integer, μ_n the multiplicative group of n-th roots of 1, and $\mathbb{S}[\mu_{n,+}]$ the spherical $\mathbb{S}$-algebra of the (pointed) monoid $\mu_{n,+} = \mu_n \cup \{0\}$. We recall that the morphisms of $\mathbb{S}$-algebras $\mathbb{S}[\mu_{n,+}] \to HR$ (R being a ring) correspond bijectively to group homomorphisms $\iota : \mu_n \to R^\times$ [10]. Let $\mathcal{P}(\mu_n)$ be the subset of the set $(\mu_n \cup \{0\})^{\mathbb{N}}$ of sequences with only finitely many non-zero terms. By definition, an element $X \in R$ is an $\mathbb{S}[\mu_{n,+}]$-generator if and only if the evaluation map $\sigma : \mathcal{P}(\mu_n) \to R$, $\sigma((\alpha_j)) = \sum_j \iota(\alpha_j)\, X^j$ is bijective. Proposition 5.8 shows that the pair (R, X) of a ring of $\mathbb{S}[\mu_{n,+}]$-polynomials in one variable is uniquely specified,

(1) We reserve throughout the symbol $\mathbf{C}$ for this entity.

(2) An early occurrence of this numeral system is found in the 1544 book "Arithmetica integra" of Michael Stifel. See also [30]

up to isomorphism, by the map $h : \mu_n \to \mathcal{P}(\mu_n)$, which, in turn, is uniquely defined by the equality $\sigma(h(\xi)) = \iota(\xi) + 1$. In Section 6 we give several examples of rings of $\mathbb{S}[\mu_{n,+}]$-polynomials based on some known number systems. We refer to [2] for a survey on systems of numerations and for references therein contained, but we claim no exhaustiveness. Conceptually, the examples of rings of $\mathbb{S}[\mu_{n,+}]$-polynomials discussed in this article provide an explicit bridge between the p-adic and the complex world. At the geometric level, the rings of polynomials are naturally related to the projective line $\mathbb{P}^1$, and the evaluation at the points 0 and ∞ of $\mathbb{P}^1$ yields, after completion, the following refinement (the lower line) of a classical diagram (upper line). In the upper line, K is the field of fractions of the p-typical Witt ring of the algebraic closure of $\mathbb{F}_q$ ($q = p^\ell$) and $\bar{K}$ is its algebraic closure

$$\begin{array}{ccccccccc}
\bar{\mathbb{F}}_q & \overset{\pi}{\twoheadleftarrow} & W(\bar{\mathbb{F}}_q) & \hookrightarrow & \bar{K} & \supset & \bar{\mathbb{Q}} & \subset & \mathbb{C} \\
\cup & & \cup & & \cup & & \cup & & \| \\
\mathbb{F}_q & \overset{\pi}{\twoheadleftarrow} & W(\mathbb{F}_q) & \hookrightarrow & W(\mathbb{F}_q)[\eta] & \hookleftarrow & R[X^{-1}] & \hookrightarrow & \mathbb{C}
\end{array}$$

In the lower line, X is an $\mathbb{S}[\mu_{n,+}]$-generator of the ring R where $n + 1 = q$. $R[X^{-1}]$ is the ring of Laurent polynomials; the map to $\mathbb{C}$ is the inclusion of $R[X^{-1}]$ in $\mathbb{C}$ by specialization of X, obtained by solving the equations $\sigma(h(\xi)) = \iota(\xi) + 1$, $\xi \in \mu_n$, and using the canonical embedding $\mu_{n,+} \subset \mathbb{C}$. The map from $R[X^{-1}]$ to the finite extension $W(\mathbb{F}_q)[\eta]$ is obtained from the canonical inclusion of R in the projective limit $\varprojlim R_n$ (see Proposition 5.8).

The general theory of rings of $\mathbb{S}[\mu_{n,+}]$-polynomials, together with the role of the absolute base $\mathbb{S}$ in the formulation of the Riemann–Roch theorem [15], suggest the following refinement of the definition of the Arithmetic Site. Originally, this space was defined by the pair of the arithmetic topos $\widehat{\mathbb{N}^\times}$ and the structure sheaf given by the Frobenius action of $\mathbb{N}^\times$ on the tropical semiring $\mathbb{Z}_{\max}$ [11]. The role of the field of constants is here played by the Boolean semifield $\mathbb{B}$. The development of this paper evidently hints to a replacement of the structure sheaf $\mathbb{Z}_{\max}$ by the sheaf of $\mathbb{S}$-algebras obtained from the Frobenius action $X \mapsto X^n$ of $\mathbb{N}^\times$ on the spherical algebra $\mathbb{S}[X]$. This new version of $\mathbb{S}$-arithmetic site provides simultaneously a natural base both at the coefficients and at the geometric levels. The topos $\widehat{\mathbb{N}^\times}$ is the geometric incarnation of the λ-operations in the theory of λ-rings [3] in the context of geometry over $\mathbb{F}_1$. We expect that through a suitable understanding of the "algebraic closure" $\bar{\mathbb{F}}_1$ of the absolute coefficients one may relate the space of points of the $\mathbb{S}$-arithmetic site over $\bar{\mathbb{F}}_1$ with the (points of the) curve $\mathbf{C}$ whose structure is recalled in Section 2.

Finally, these results also point out to the open and interesting question of the classification of rings of $\mathbb{S}[\mu_{n,+}]$-polynomials in several variables which pursues the intuitive statement of Yuri Manin [22]:

The central question we address can be provocatively put as follows: if numbers are similar to polynomials in one variable over a finite field, what is the analog of polynomials in several variables? Or, in more geometric terms, does there exist a category in which one can define "absolute Descartes powers" $\operatorname{Spec}\mathbb{Z}\times\cdots\times\operatorname{Spec}\mathbb{Z}$*?*

2. Adelic and topos theoretic incarnation of $\mathbf{C}$

A first connection between Manin's point of view on $\mathbb{F}_1$ and a seemingly unrelated topic takes place as a by-product of the relations between C. Soulé's perspective on varieties over $\mathbb{F}_1$ (named "Critical Realism" in [23])—motivated by Manin [22] (cf. Section 1.5)—and the work of the first author [6] on the trace formula in noncommutative geometry and the zeros of the Riemann zeta function. In [27], Soulé introduced the following zeta function of a variety X over $\mathbb{F}_1$:

$$\zeta_X(s) := \lim_{q\to 1} Z(X, q^{-s})(q-1)^{N(1)}, \quad s\in\mathbb{R}, \tag{2.1}$$

using the *polynomial* counting function $N(x)\in\mathbb{Z}[x]$ associated with X and the Hasse–Weil exponential series

$$Z(X,T) := \exp\left(\sum_{r\geq 1} N(q^r)\frac{T^r}{r}\right). \tag{2.2}$$

All the examples of varieties considered in op. cit. are rational. Thus, the existence of an underlying curve $\mathbf{C}$ related, in a similar manner, to the Riemann zeta function is subordinated to finding a function $N(q)$ (highly non-polynomial!) that produces, through the use of (2.1), the complete Riemann zeta function $\zeta_{\mathbb{Q}}(s)=\pi^{-s/2}\Gamma(s/2)\zeta(s)$. This is a non-trivial problem since, classically, $N(1)$ in the above formula inputs the Euler characteristic of the geometric space. Thus one might be induced to expect[3] that since for the Riemann zeta-function one ought to have $N(1)=-\infty$, the use of (2.1) should be precluded, and with it also the expectation that $N(q)\geq 0$ for $q\in(1,\infty)$. There is, in fact, a natural way to by-pass this problem by applying the logarithmic derivatives to both sides of (2.1) and then observing that the right-hand side determines the Riemann sums of an integral [7, 8]. In this way, in place of (2.1) one considers the equation:

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

(3) The number of zeros of $\zeta_{\mathbb{Q}}$ is infinite, and so is the dimension of the (mysterious) cohomology $H^1(\mathbf{C})$.

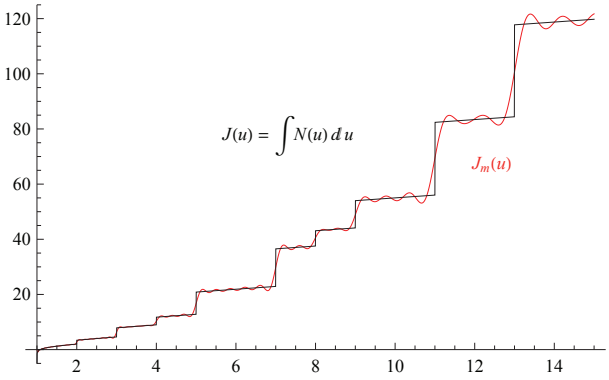


FIGURE 1. Graph of a primitive $J(u)$ of the counting distribution $N(u)$. One has $J(u) \to -\infty$ when $u \to 1$. The wiggly graph is the approximation of $J(u)$ obtained using the symmetric set Z_m of the first $2m$ zeros to perform the sum $J_m(u) = \frac{u^2}{2} - \sum_{Z_m} \mathrm{order}(\rho) \frac{u^{\rho+1}}{\rho+1} + u$.

where $d^*u := du/u$. This integral formula produces the following one for the sought for counting function $N(q)$ associated with $\mathbf{C}$:

$$\frac{\partial_s \zeta_{\mathbb{Q}}(s)}{\zeta_{\mathbb{Q}}(s)} = -\int_1^\infty N(u)\, u^{-s} d^*u. \tag{2.3}$$

The above equation admits a meaningful solution expressible in terms of the *distribution* (cf. Figure 1)

$$N(u) = \frac{d}{du}\varphi(u) + \kappa(u), \quad \varphi(u) := \sum_{n<u} n\, \Lambda(n), \tag{2.4}$$

where $\kappa(u)$ is the distribution that appears in the Riemann–Weil explicit formula

$$\int_1^\infty \kappa(u) f(u) d^*u = \int_1^\infty \frac{u^2 f(u) - f(1)}{u^2 - 1} d^*u + c f(1), \quad c = \frac{1}{2}(\log \pi + \gamma).$$

One shows that the distribution $N(u)$ is positive on $(1, \infty)$, and when written in terms of the non-trivial zeros $\rho \in Z$ of the Riemann zeta function, it is given, in complete analogy with its counterpart holding in the function field case, by

$$N(u) = u - \frac{d}{du}\left(\sum_{\rho \in Z} \mathrm{order}(\rho) \frac{u^{\rho+1}}{\rho+1} \right) + 1, \tag{2.5}$$

where the derivative is taken in the sense of distributions. The value at $u = 1$ of the term

$$\omega(u) = \sum_{\rho \in Z} \mathrm{order}(\rho) \frac{u^{\rho+1}}{\rho+1}$$

is given by $\frac{1}{2} + \frac{\gamma}{2} + \frac{\log 4\pi}{2} - \frac{\zeta'(-1)}{\zeta(-1)}$.

The tension between the positivity of the distribution $N(q)$ for $q > 1$ and the expectation that its value $N(1)$ ought to be $N(1) = -\infty$ is resolved by implementing the theory of distributions. Indeed, even though $N(u)$ is *finite* as a distribution, when one looks at it as a function, its value at $q = 1$ is formally given by

$$N(1) = 2 - \lim_{\varepsilon \to 0} \frac{\omega(1+\varepsilon) - \omega(1)}{\varepsilon} \sim -\frac{1}{2} E \log E, \quad E = \frac{1}{\varepsilon};$$

thus, it is $-\infty$, and this fact reflects, when $\varepsilon \to 0$, the density of the zeros of the zeta function.

We emphasize that the role of the Riemann–Weil explicit analytic formulas in the process of overcoming the initial difficulty through a solution defined by a positive distribution $N(q)$ directly connects the original (classical geometric) viewpoint with the trace formula in [6], thus providing a first geometric description for the points of **C** in terms of the double quotient

$$X_{\mathbb{Q}} := \mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}} / \hat{\mathbb{Z}}^{\times} \tag{2.6}$$

of the adele class space of the rationals $\mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}$, by the maximal compact subgroup $\hat{\mathbb{Z}}^{\times}$ of the idele class group. The main key player in this construction is the scaling action of $\mathbb{R}_+^{\times}$ which provides[4] the above counting distribution $N(u)$, $u \in [1, \infty)$, that determines, in turn, the complete Riemann zeta function via a limiting procedure as $q \to 1$, operated on the Hasse–Weil formula. Noncommutative geometry plays a crucial role in this development mainly by implementing the noncommutative space $\mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}$ which naturally arises as the dual of the BC-system [4].

To achieve a more classical geometric understanding of the double quotient $X_{\mathbb{Q}}$ with its scaling action, in analogy with the action of the Frobenius automorphism on the points of a curve over the algebraic closure of a ground field, one needs to push further the search of other unexpected interactions .... This geometric understanding comes in fact from the interplay among three a priori unrelated theories:

(1) Noncommutative geometry.

(2) Grothendieck topoi.

(3) Tropical geometry.

The natural starting point is the topos $\widehat{\mathbb{N}^{\times}}$, defined in [11] as the Grothendieck presheaf topos dual to the multiplicative monoid $\mathbb{N}^{\times}$ of non-zero positive integers. This space is in fact the geometric incarnation of $\mathbb{N}^{\times}$-actions on sets. These actions often occur in

(4) To remove the divergent logarithmic term from the trace formula [6] one needs to remove from $X_{\mathbb{Q}}$ the orbit of the unit adele 1, i.e. equivalently to subtract the regular representation of $\mathbb{R}_+^{\times}$ as in [24].

the global instances of Frobenius endomorphisms: for λ-rings they were advocated in [3] in the context of varieties over $\mathbb{F}_1$ ("Futurism" in Manin's interpretation, [23]). Special λ-rings R [1, Proposition 5.2] belong naturally to the topos $\widehat{\mathbb{N}^\times}$ since the Adams operations ψ_n turn R into a sheaf of rings on the topos $\widehat{\mathbb{N}^\times}$.

At a very basic algebraic level, a fundamental example of Frobenius action of $\mathbb{N}^\times$ occurs in the theory of semirings (i.e. when one drops the existence of the additive inverse in rings). For a semifield[5] R of "characteristic one" (aka idempotent: i.e. such that $1+1=1$), the map $x \mapsto x^n = \mathrm{Fr}_n(x)$ is an injective endomorphism [18], for any integer $n \in \mathbb{N}^\times$. Thus, one obtains a canonical action of the semigroup $\mathbb{N}^\times$ on any such R. For this reason it is natural to work with sets endowed with an action of $\mathbb{N}^\times$, i.e. with the topos $\widehat{\mathbb{N}^\times}$. Furthermore, one also knows that there is a unique semifield[6] $\mathbb{Z}_{\max}$ whose multiplicative group is infinite cyclic and it is of characteristic one. Given these facts, it is natural to introduce the following space.

DEFINITION 2.7 ([11]). The Arithmetic Site $\mathcal{A} = (\widehat{\mathbb{N}^\times}, \mathcal{O})$ is the topos $\widehat{\mathbb{N}^\times}$ endowed with the *structure sheaf* $\mathcal{O} := \mathbb{Z}_{\max}$, viewed as a semiring in the topos *and* with the action of $\mathbb{N}^\times$ by Frobenius endomorphisms.

The semifield $\mathbb{Z}_{\max}$ and its companion $\mathbb{R}_+^{\max}$ (whose multiplicative group is $\mathbb{R}_+^*$) are familiar objects in tropical geometry where the maximum substitutes the usual addition.

By implementing a straightforward generalization in semi-ringed toposes of the understanding of a point in algebraic geometry, one obtains the following result which determines a bridge connecting noncommutative geometry with (Grothendieck) topos theory.

THEOREM 2.8 ([11]). *The set of points of the arithmetic site $\mathcal{A}$ over $\mathbb{R}_+^{\max}$ is canonically isomorphic to $X_{\mathbb{Q}} = \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}} / \widehat{\mathbb{Z}}^\times$. The action of the Frobenius automorphisms Fr_λ of $\mathbb{R}_+^{\max}$ on these points corresponds to the action of the idele class group on $X_{\mathbb{Q}} = \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}} / \widehat{\mathbb{Z}}^\times$.*

This theorem sheds new light on a geometric intuition of the curve $\mathbf{C}$; in particular, it displays the noncommutative space $X_{\mathbb{Q}}$ as the set of points of $\mathcal{A}$ over the semifield $\mathbb{R}_+^{\max}$, with the scaling action understood as the action of the Galois group $\mathrm{Aut}_{\mathbb{B}}(\mathbb{R}_+^{\max})$ of $\mathbb{R}_+^{\max}$ over the Boolean semifield[7] $\mathbb{B}$. It also suggests that $\mathbb{R}_+^{\max}$ ought to be involved

(5) A semifield is a semiring whose non-zero elements form a group under multiplication.

(6) As a multiplicative monoid $\mathbb{Z}_{\max}$ is obtained by adjoining the zero element $-\infty$ to the infinite cyclic group $\mathbb{Z}$ while the operation which plays the role of addition in the semifield is $(x, y) \mapsto \max(x, y)$.

(7) $\mathbb{B} := \{0, 1\}$ with $1 + 1 = 1$.

in the construction of the "algebraic closure" of $\mathbb{F}_1$, and that the combinatorial core underlying $\mathbf{C}$ is countable since both $\mathbb{N}^\times$ and $\mathbb{Z}_{\max}$ are so. We find it quite remarkable that while the Arithmetic Site is a combinatorial object of countable nature, it comes nonetheless endowed with a one-parameter semigroup of "correspondences" which can be viewed as congruences on the square of this site [11].

The countable set of places of $\mathbb{Q}$ (the points of the Arakelov compactification $\overline{\operatorname{Spec}\mathbb{Z}}$) is the (classically) visible analog of the set of the orbits of the Frobenius automorphism in the function field case. One obtains a better view of the points of $\mathbf{C}$ by considering the periodic orbits C_p (parameterized by primes p) as they occur among the points of the Arithmetic Site $\mathcal{A}$ over $\mathbb{R}_+^{\max}$. One shows that the points of C_p form a circle whose elements are rank-one subgroups of the multiplicative group of $\mathbb{R}_+^{\max}$ of the form

$$H_\mu := \{\mu^{\frac{n}{p^k}} \mid n \in \mathbb{Z},\ k \in \mathbb{N}\}. \tag{2.9}$$

This subgroup is unchanged if one replaces μ with μ^p, and the Frobenius action of $\mathrm{Aut}_{\mathbb{B}}(\mathbb{R}_+^{\max}) = \mathbb{R}_+^*$, $\mu \mapsto \mu^\lambda$, induces the transitive action of the quotient group $\mathbb{R}_+^*/p^{\mathbb{Z}}$. The length of this periodic orbit is $\log p$, and their full collection plays a key role in the trace formula interpretation of the Riemann–Weil explicit formulas in [6]. Moreover, each C_p inherits, as a subspace of the Scaling Site (obtained from the Arithmetic Site by extension of scalars), a structure sheaf (of characteristic one) which turns each periodic orbit into the analog of a classical elliptic curve [12]. In this way, one can still apply several key tools of algebraic geometry, such as rational functions, divisors, etc. A striking new feature of the geometry of a periodic orbit is that the degree of a divisor is a real number. For any divisor D in C_p, there is a corresponding Riemann–Roch problem with solution space $H^0(D)$. The continuous dimension[8] $\mathrm{Dim}_{\mathbb{R}}(H^0(D))$ of this $\mathbb{R}_+^{\max}$-module is defined by the limit

$$\mathrm{Dim}_{\mathbb{R}}\left(H^0(D)\right) := \lim_{n\to\infty} p^{-n} \dim_{\mathrm{top}}\left(H^0(D)^{p^n}\right), \tag{2.10}$$

where $H^0(D)^{p^n}$ is a naturally defined filtration and $\dim_{\mathrm{top}}(\mathcal{E})$ denotes the topological dimension of an $\mathbb{R}_+^{\max}$-module $\mathcal{E}$. The following Riemann–Roch formula holds.

THEOREM 2.11 ([12]).

(i) *Let $D \in \mathrm{Div}(C_p)$ be a divisor with $\deg(D) \geq 0$. Then the limit in (2.10) converges and one has*

$$\mathrm{Dim}_{\mathbb{R}}\left(H^0(D)\right) = \deg(D).$$

(8) In analogy with von-Neumann's continuous dimensions of the theory of type II factors.

(ii) *The following Riemann–Roch formula holds:*

$$\mathrm{Dim}_{\mathbb{R}}\left(H^0(D)\right) - \mathrm{Dim}_{\mathbb{R}}\left(H^0(-D)\right) = \deg(D) \quad \forall D \in \mathrm{Div}(C_p).$$

In view of these results and the leading role played by the Boolean semifield $\mathbb{B}$ among algebraic idempotent structures[9], one might be (wrongly) induced to think of $\mathbb{B}$ as the natural incarnation of $\mathbb{F}_1$. However, this cannot be the case for the straightforward reason[10]:

The ring $\mathbb{Z}$ is not an algebra over $\mathbb{B}$.

3. The absolute coefficients, spectra and $\mathbb{S}$

The above undeniable fact led us, once again, to compare Manin's ideas on $\mathbb{F}_1$ with another a priori unrelated topic: this is the world of homotopy theory spectra. Topological spectra greatly generalize cohomology theories; many important invariants in algebraic topology, like ordinary cohomology and K-theory, can be reformulated in terms of spectra, which thus provide a unified treatment for "generalized coefficients". One fundamental discovery in the topological context is that "ring spectra" generalize rings, and in particular, the "sphere spectrum" $\underline{\mathbb{S}}$ becomes more basic than the ring $\mathbb{Z}$, because the latter can be seen as an algebra over the former. This theory of "brave new rings" has proved to be the right framework for cyclic homology; in particular, the theory of Γ-spaces is known to provide a workable model of connective spectra [16]. One usually works at the homotopy level, so it is crucial to handle Kan complexes to obtain a good model structure. However, to take full advantage of this theory for the development of Manin's ideas on $\mathbb{F}_1$ in number theory, we believe that Γ-spaces ought to be viewed in their most basic form, namely as simplicial objects in the category of Γ-sets, so that homotopy theory can play the role of homological algebra corresponding to the "absolute algebra" over the base Γ-ring $\mathbb{S}$ [10]. This Γ-ring is the categorical starting point in the construction of the sphere spectrum $\underline{\mathbb{S}}$, together with the natural functor from Γ-spaces to spectra, and it is exactly this basic combinatorial nature that makes it closer to the sought for $\mathbb{F}_1$. The category $\Gamma\mathfrak{Sets}_*$ of pointed Γ-sets (aka $\mathbb{S}$-modules $\mathfrak{Mod}(\mathbb{S})$) can be directly described as follows. One starts with the small category Γ^{op} as a full subcategory of the category of finite pointed sets whose objects are the pointed finite sets[11] $k_+ := \{0, \dots, k\}$, for $k \geq 0$. In particular, 0_+ is both initial and final in Γ^{op}, making Γ^{op} a *pointed category*. A Γ-set is defined as a (covariant)

(9) $\mathbb{B}$ is, in particular, the only finite semifield that is not a field, cf. [18].
(10) Algebras over $\mathbb{B}$ are of characteristic one.
(11) where 0 is the base point.

functor $\Gamma^{\mathrm{op}} \to \mathfrak{Sets}_*$ between pointed categories, and the morphisms in this category are natural transformations. One lets $\mathbb{S} : \Gamma^{\mathrm{op}} \to \mathfrak{Sets}_*$ be the inclusion functor. The internal hom functor is defined by

$$\underline{\mathrm{Hom}}_{\mathbb{S}}(M, N) := \{k_+ \mapsto \mathrm{Hom}_{\mathbb{S}}\left(M, N(k_+ \wedge -)\right)\}.$$

This formula uniquely defines the smash product of Γ-sets by applying the adjunction

$$\underline{\mathrm{Hom}}_{\mathbb{S}}(M_1 \wedge M_2, N) = \underline{\mathrm{Hom}}_{\mathbb{S}}\big(M_1, \underline{\mathrm{Hom}}_{\mathbb{S}}(M_2, N)\big).$$

The basic construction of $\mathbb{S}$-modules associates to an abelian monoid A with a zero element, the Eilenberg–MacLane functor $M = HA$

$$HA(k_+) = A^k, \quad Hf : HA(k_+) \to HA(n_+), \quad Hf(m)(j) := \sum_{f(\ell)=j} m_\ell,$$

where $m = (m_1, \ldots, m_k) \in HA(k_+)$, and the zero element of A gives meaning to the empty sum. An $\mathbb{S}$-algebra $\mathcal{A}$ is an $\mathbb{S}$-module $\mathcal{A} : \Gamma^{\mathrm{op}} \to \mathfrak{Sets}_*$ endowed with an associative multiplication $\mu : \mathcal{A} \wedge \mathcal{A} \to \mathcal{A}$ and a unit $1 : \mathbb{S} \to \mathcal{A}$.

An ordinary semiring R gives rise to the $\mathbb{S}$-algebra HR, and the corresponding embedding of categories is fully faithful so that no information is lost. In contrast, the basic $\mathbb{S}$-algebra $\mathbb{S}$ now lies under HR for any semiring R.

Given a multiplicative monoid M with a zero element $0 \in M$ such that $0 \times x = x \times 0 = 0$ for all $x \in M$, one defines the spherical $\mathbb{S}$-algebra $\mathbb{S}[M]$ which associates to the pointed set X the smash product $X \wedge M$, where the base point of M is $0 \in M$. One identifies $\mathbb{S}[M][1_+] = 1_+ \wedge M$ with M by sending the base point of $1_+ \wedge M$ to $0 \in M$, and $a \wedge m$ where $a \in 1_+ \setminus \{*\}$ and $m \in M \setminus \{0\}$ to m. To avoid confusion we write $2_+ = \{*, a, b\}$. Besides the base point the elements of $\mathbb{S}[M][2_+] = 2_+ \wedge M$ are given by pairs of the form (a, m) or (b, m) where $m \in M \setminus \{0\}$. One has three natural pointed maps $f : 2_+ \to 1_+$, which are

$$\phi(a) = a, \quad \phi(b) = *, \quad \psi(a) = *, \quad \psi(b) = a, \quad \rho(a) = \rho(b) = a.$$

Let $m \in M \setminus \{0\}$ and consider the pair $z = (b, m) \in \mathbb{S}[M][2_+]$. One has $\phi_*(z) = * = 0$ and $\psi_*(z) = m$. Moreover one has $\rho_*(z) = m$. This means that for the partially defined addition in $\mathbb{S}[M][1_+] = M$, one has $0 + m = m$ for all $m \in M$.

Thus both ordinary rings and monoids fit fully faithfully and naturally [10, Proposition 3.5] in the category of $\mathbb{S}$-algebras yielding a strong argument for viewing $\mathbb{S}$ as the natural candidate for $\mathbb{F}_1$. Nonetheless one needs to test this idea in various ways. For instance, one sees op. cit. that the tensor square of $H\mathbb{Z}$ over $\mathbb{S}$ is non-isomorphic to $H\mathbb{Z}$, and this result provides more ground to the original intuition of Manin in [22]. One may also wonder which advancements this point of view may produce to the

understanding of the ring $\mathbb{Z}$ and its algebraic spectrum Spec $\mathbb{Z}$. We shall now move to a detailed discussion of this topic.

Let $\overline{\text{Spec}\,\mathbb{Z}}$ be the Arakelov compactification of Spec $\mathbb{Z}$ obtained by adding the archimedean place with associated symbol ∞. Then, the new point of view described above provides a natural extension of the classical structure sheaf of Spec $\mathbb{Z}$ to the Arakelov compactification. The crucial points concerning the quest for the curve **C** are two: firstly, this extended structure sheaf $\mathcal{O}$ is still a subsheaf of the constant sheaf $\mathbb{Q}$; the second interesting point is that the global sections of $\mathcal{O}$ form a finite algebra extension of $\mathbb{S}$. This extension is identifiable with the extension by the two roots of unity inside $\mathbb{Q}$ that we used in [9] in the process of showing that Chevalley groups are varieties over $\mathbb{F}_{1^2}$ in the sense of Soulé[12]. The condition that restricts the elements of $H\mathbb{Q}$ at the archimedean place is simple to formulate when one views the functor $H\mathbb{Q}$ as assigning to a finite pointed set F the $\mathbb{Q}$-valued divisors on F. The restriction is then stated by writing that the sum of the absolute values of the involved rational numbers is ≤ 1. One checks that this condition is stable under push-forwards and products and hence it defines a sub-$\mathbb{S}$-algebra of $H\mathbb{Q}$. This sub-$\mathbb{S}$-algebra, defined using a norm, also applies in the context of the adeles of a global field and allows one to transpose the approach due to A. Weil of the Riemann–Roch theorem for function fields to the number field $\mathbb{Q}$ [14].

A divisor D on $\overline{\text{Spec}\,\mathbb{Z}}$ defines a compact *subset* $K = \prod K_v \subset \mathbb{A}_{\mathbb{Q}}$ of the locally compact ring of adeles. When p is a non-archimedean prime, each $K_p \subset \mathbb{Q}_p$ is an additive subgroup; in contrast, the compact subset $K_\infty \subset \mathbb{R}$ is just a symmetric interval whose lack of additive structure prevents one to use Weil's original construction involving the addition map $\psi : \mathbb{Q} \times K \to \mathbb{A}_{\mathbb{Q}}$. On the other hand, one also quickly notices that ψ retains its meaning in the context of $\mathbb{S}$-modules, giving rise to a short complex. Using the Dold-Kan correspondence in the context of $\mathbb{S}$-algebras, one then introduces a Γ-space $H(D)$ which encodes the homological information of the divisor D and only depends upon the linear equivalence class of D (i.e. the divisor class is unchanged under the multiplicative action of $\mathbb{Q}^\times$ on $\mathbb{A}_{\mathbb{Q}}$). As a by-product, one obtains a Riemann–Roch formula for Arakelov divisors on $\overline{\text{Spec}\,\mathbb{Z}}$ of an entirely novel nature that relies on the introduction of three new key notions: (integer) dimension, cohomologies $(H^0(D), H^1(D))$ (attached to a divisor D), and Serre duality. More precisely, the Riemann–Roch formula equates the integer-valued Euler characteristic with a simple modification of the traditional expression (i.e. the degree of the divisor plus log 2).

([12]) Another convincing argument in favor of $\mathbb{S}$-algebras is that the ad-hoc category we introduced in [8] to simplify Soulé's definition of varieties over $\mathbb{F}_1$ is naturally (see [13]) a full subcategory of the category of $\mathbb{S}$-algebras.

THEOREM 3.1 ([14]). *Let D be an Arakelov divisor on $\overline{\operatorname{Spec}\mathbb{Z}}$. Then*

$$\dim_{\mathbb{S}[\pm 1]} H^0(D) - \dim_{\mathbb{S}[\pm 1]} H^1(D) = \lceil \deg_3 D + \log_3 2 \rceil - \mathbf{1}_L. \tag{3.2}$$

Here, $\lceil x \rceil$ denotes the odd function on $\mathbb{R}$ that agrees with the ceiling function on positive reals, and $\mathbf{1}_L$ is the characteristic function of an exceptional set[13] of finite Lebesgue measure.

In (3.2), the Neperian logarithm that is traditionally used to define the degree of a divisor

$$D = \sum_j a_j \{p_j\} + a\{\infty\}$$

in Arakelov geometry is replaced by the logarithm in base 3. This alteration is equivalent to the division by $\log 3$; i.e. $\deg_3(D) := \deg(D)/\log 3$, $\log_3 2 = \log 2/\log 3$.

The number 3 appears unexpectedly in the computation of the dimension of the cohomology of the $\mathbb{S}[\pm 1]$-modules by determining their minimal number of linear generators. For $\dim_{\mathbb{S}[\pm 1]} H^0(D)$ one finds that the most economical way of writing the elements of a symmetric interval $\mathbb{Z} \cap K_\infty$ involves writing integers as polynomials of the form

$$\sum_{j \geq 0} \alpha_j \, 3^j, \quad \alpha_j \in \{-1, 0, 1\}. \tag{3.3}$$

Similarly, in the case of $\dim_{\mathbb{S}[\pm 1]} H^1(D)$, one finds that the best way to approximate elements of the circle $\mathbb{R}/\mathbb{Z}$ is to use Laurent polynomials of the form

$$\sum_{j < 0} \alpha_j \, 3^j, \quad \alpha_j \in \{-1, 0, 1\}. \tag{3.4}$$

The key fact here is that the addition[14] of polynomials $P(X) = \sum_{j \geq 0} \alpha_j \, X^j$, $\alpha_j \in \{-1, 0, 1\}$, with coefficients in $\mathbb{S}[\pm 1]$ is identical to the addition of (truncated) Witt vectors for the finite field $\mathbb{F}_3$. One finds that the addition $P + Q$ of two polynomials of degree $\leq n$ gives a polynomial of degree $\leq n + 1$, and that the only non-obvious rule one has to prescribe is the sum: $1 + 1 := X - 1$. Conceptually, the fundamental point is that the image of the Teichmuller lift for $\mathbb{F}_3$ sits inside $\mathbb{Z}$. At the same time, the Witt vectors with only finitely many non-zero components form a subring of the Witt ring, and this subring is $\mathbb{Z}$!

(13) $L \subset \mathbb{R}$ is the union, for $k \geq 0$, of the intervals $\deg(D) \in (\log \frac{3^k}{2}, \log \frac{3^k+1}{2})$.
(14) Once the addition is defined, the product follows uniquely using $X^j \, X^k = X^{j+k}$.

4. The ring of integers as a ring of polynomials

There is another way to represent the integers as polynomials in one variable, and in this description, the "coefficients" belong to the absolute base $\mathbb{S}$. This representation is known as the *negabinary* representation of numbers

$$n = \sum \alpha_j \, (-2)^j, \quad \alpha_j \in \{0, 1\}. \tag{4.1}$$

The number $X = -2$ is remarkably unique, making the representation of an integer n possible as polynomial $P(X)$ with coefficients $\alpha_j \in \{0, 1\}$. By following the same steps that led us to Theorem 3.1, but working now over the absolute base $\mathbb{S}$, one obtains the following new and simplified version of the Riemann–Roch formula which now involves the logarithm in base 2.

Theorem 4.2 ([15]). *Let D be an Arakelov divisor on $\overline{\mathrm{Spec}\,\mathbb{Z}}$. Then*

$$\dim_{\mathbb{S}} H^0(D) - \dim_{\mathbb{S}} H^1(D) = \lceil \deg_2 D \rceil' + 1, \tag{4.3}$$

where $\lceil x \rceil'$ is the right continuous function which agrees with ceiling(x) for $x > 0$ non-integer and with $-$ceiling$(-x)$ for $x < 0$ non-integer.

This version of the Riemann–Roch Theorem improves on Theorem 3.1 for the following reasons:

(1) The term $\mathbf{1}_L$ involving the exceptional set L in the original statement (see [14]) has now disappeared from the formula.

(2) The formula (4.3) is in perfect analogy with the Riemann–Roch theorem for curves of genus 0.

(3) The canonical divisor $K = -2\{2\}$ has integral degree $\deg_2(K) = -2$.

Theorem 4.2 fits now perfectly with the tri-lingual text suggested by A. Weil, which supports the analogy between Riemann's transcendental theory of algebraic functions of one variable in the first column, the algebraic geometry of curves over finite fields, in the middle column, and the theory of algebraic number fields in the third column. Indeed, according to Weil:

> *Mais on peut, je crois, en donner une idée imagée en disant que le mathématicien qui étudie ces problèmes, a l'impression de déchiffrer une inscription trilingue. Dans la première colonne se trouve la théorie riemannienne des fonctions algébriques au sens classique. La troisième colonne c'est la théorie arithmétique des nombres algébriques. La colonne du milieu est celle dont la découverte est la plus récente : elle contient la théorie des fonctions algébriques sur un corps de Galois. Ces textes sont l'unique source de nos connaissances sur les langues*

dans lesquels ils sont écrits; de chaque colonne, nous n'avons bien entendu que des fragments ; la plus complète et celle que nous lisons le mieux, encore à présent, c'est la première. Nous savons qu'il y a de grandes différences de sens d'une colonne à l'autre, mais rien ne nous en avertit à l'avance. Á l'usage, on se fait des bouts de dictionnaire, qui permettent de passer assez souvent d'une colonne à la colonne voisine.

In Weil's vision there is, in the middle column (that of function fields), a geometric understanding of the zeta function as the generating function of the number of points of the curve over extensions of the field of constants. In Section 2 we translated in this dictionary the Hasse–Weil formula, thus leading one to the first encounter with the "the curve" $\mathbf{C}$ and the action of $\mathbb{R}_+^*$ on $\mathbf{C}$, analogous to a Galois action. Theorem 4.2 indicates that the role of the field of constants is played by the absolute coefficient ring $\mathbb{S}$. Since the boolean semifield $\mathbb{B}$ can be viewed as an $\mathbb{S}$-algebra, this translation suggests to descend the structures of the Arithmetic and Scaling Sites discussed in Section 2 from $\mathbb{B}$ to $\mathbb{S}$.

5. Rings of $\mathbb{S}[\mu_{n,+}]$-polynomials

Let $n > 0$ be an integer, μ_n the multiplicative group of n-th roots of 1, and $\mathbb{S}[\mu_{n,+}]$ the spherical $\mathbb{S}$-algebra of the (pointed) monoid $\mu_{n,+} = \mu_n \cup \{0\}$. We recall that morphisms of $\mathbb{S}$-algebras $\mathbb{S}[\mu_{n,+}] \to HR$ correspond (bijectively) to group homomorphisms $\iota : \mu_n \to R^\times$ [10]. In this section, we introduce the notion of rings of $\mathbb{S}[\mu_{n,+}]$-polynomials in one (Definition 5.1) and several variables (Remark 5.2) which might play a key role in the search of the "absolute Descartes powers" among ordinary rings. We show that the pair (R, X) of a ring R and an $\mathbb{S}[\mu_{n,+}]$-generator of R is uniquely characterized, up to isomorphism, by the map from μ_n to polynomials with coefficients in the pointed monoid $\mu_{n,+}$, which encodes the addition of 1 into elements of μ_n.

Definition 5.1. Let R be a ring and $\iota : \mu_n \to R^\times$ an injective group homomorphism. An element $X \in R$ is an $\mathbb{S}[\mu_{n,+}]$-generator of R if and only if every element $z \in R$ can be written uniquely as a polynomial $z = \sum_j \iota(\alpha_j)\, X^j$ with coefficients $\alpha_j \in \mu_n \cup \{0\}$.

Remark 5.2. More generally, a finite set $\{X_i \mid i \in \{1, \dots, k\}\}$ $\mathbb{S}[\mu_{n,+}]$-generates R if and only if every element $z \in R$ can be written uniquely as a polynomial

$$z = \sum_j \iota(\alpha_j)\, X^j$$

with coefficients $\alpha_j \in \mu_n \cup \{0\}$, where j is a multi-index $j = (j_1, \dots, j_k) \in \mathbb{N}^k$, and $X^j := \prod X_i^{j_i}$.

Let $\mathcal{P}(\mu_n)$ be the subset of the set $(\mu_n \cup \{0\})^{\mathbb{N}}$ of sequences with only finitely many non-zero terms. Let $X \in R$; then the map $\sigma : \mathcal{P}(\mu_n) \to R$ given by

$$\sigma\big((\alpha_j)\big) := \sum_j \iota(\alpha_j)\, X^j \tag{5.3}$$

is well defined since for $\alpha = (\alpha_j) \in \mathcal{P}(\mu_n)$ the sum $\sum_j \iota(\alpha_j)\, X^j$ defines an element of R. It follows from Definition 5.1 that if X is an $\mathbb{S}[\mu_{n,+}]$-generator, the map σ is a bijection of $\mathcal{P}(\mu_n)$ with R.

The simplest instance of an $\mathbb{S}[\mu_{n,+}]$ generator, with $n+1$ a prime power q, is provided by the following example.

EXAMPLE 5.4. The ring $R = \mathbb{F}_q[X]$ of polynomials over the finite field $\mathbb{F}_q$ has the variable X as $\mathbb{F}_q^\times$-generator.

The next proposition shows that the m-th root of an $\mathbb{S}[\mu_{n,+}]$-generator X of a ring R is an $\mathbb{S}[\mu_{n,+}]$-generator of the R-algebra extension $R[Y]/(Y^m - X)$, hence providing an infinite source of examples.

PROPOSITION 5.5. *Let R be a ring, $\iota : \mu_n \to R^\times$ an injective group homomorphism, $X \in R$ an $\mathbb{S}[\mu_{n,+}]$-generator of R, and $m \in \mathbb{N}$ a positive integer. Then $Y \in R[Y]/(Y^m - X)$ is an $\mathbb{S}[\mu_{n,+}]$-generator of $R[Y]/(Y^m - X)$.*

PROOF. Any element z of $R[Y]/(Y^m - X)$ can be written uniquely as $z = \sum_{j=0}^{m-1} a_j Y^j$, with $a_j \in R$ written uniquely as

$$a_j = \sum_{j,k} \iota(\alpha_{j,k})\, X^k$$

where $\alpha_{j,k} \in \mu_n \cup \{0\}$. Since $Y^m = X$, one obtains the unique finite decomposition

$$z = \sum_{j,k} \iota(\alpha_{j,k}) Y^{j+mk}, \quad \alpha_{j,k} \in \mu_n \cup \{0\}. \qquad \blacksquare$$

The following example is a straightforward generalization of the fact that 3 is an $\mathbb{S}[\pm 1] = \mathbb{S}[\mu_{2,+}]$-generator of the ring $\mathbb{Z}$ of integers.

EXAMPLE 5.6. Let $m \in \mathbb{N}$ be a positive integer, and $\varepsilon = \pm 1$. Then $X = (3\varepsilon)^{1/m}$ is an $\mathbb{S}[\pm 1]$-generator of the subring $R = \mathbb{Z}[X]$ of the number field $\mathbb{Q}((3\varepsilon)^{1/m})$.

Indeed, the polynomial $X^m - 3\varepsilon$ is irreducible; thus every element $z \in R$ can be written uniquely as a sum

$$z = \sum_{j=0}^{m-1} a_j X^j, \quad a_j \in \mathbb{Z}.$$

In turns, every a_j can be uniquely written as $a_j = \sum_{j,k} \alpha_{j,k} (3\varepsilon)^k$, where $\alpha_{j,k} \in \{-1, 0, 1\}$. Since $3\varepsilon = X^m$, one obtains the unique decomposition

$$z = \sum_{j,k} \alpha_{j,k} X^{j+mk}, \quad \alpha_{j,k} \in \{-1, 0, 1\}.$$

An interesting case is for $m = 2$ and $\varepsilon = -1$ since then the ring $R = \mathbb{Z}[\sqrt{-3}]$ is an order of the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$.

Notice that in Example 5.6 the addition is specified by an equality of the following form:

$$1 + 1 = P(X), \quad P(X) = \sum_j \alpha_j X^j, \quad \alpha_j \in \{-1, 0, 1\}, \tag{5.7}$$

with $P(X) = \varepsilon X^m - 1$. A simple algebraic presentation of the form (5.7) holds when working over $\mu_{n,+}$ for $n = 1, 2$.

The following result states the uniqueness of a similar polynomial presentation in the general case.

PROPOSITION 5.8. *Let R be a ring, $\iota : \mu_n \to R^\times$ an injective group homomorphism, and $X \in R$ an $\mathbb{S}[\mu_{n,+}]$-generator of R. For a polynomial decomposition*

$$z = \sum_j \iota(\alpha_j) X^j \in R,$$

let $\deg(z)$ *be the smallest integer m such that $\alpha_j = 0$ for all $j > m$. Then, the following results hold:*

(i) *Let $m \in \mathbb{N}$, and let $J_m = \langle X^m \rangle \subset R$ be the ideal generated by X^m. Any element $z \in R$ admits a unique decomposition as $z = a + b$ where $\deg(a) < m$ and $b \in J_m$.*

(ii) *The quotient $R_m := R/J_m$ is a finite ring whose elements are uniquely written as $\sum_{j=0}^{m-1} \iota(\alpha_j) X^j$, with $\alpha_j \in \mu_{n,+} = \mu_n \cup \{0\}$.*

(iii) *The quotient $R_1 := R/J_1$ is a finite field with $n + 1$ elements and $\iota : \mu_{n,+} \to R$ is a multiplicative section of the quotient map $R \to R_1$.*

(iv) *The canonical ring homomorphism $\pi : R \to \varprojlim R_m$ is injective.*

(v) *The pair (R, X) is uniquely specified, up to isomorphism, by the map $h : \mu_n \to \mathcal{P}(\mu_n)$ which is uniquely defined by the equality $\sigma(h(\xi)) = \iota(\xi) + 1$.*

PROOF. (i) Let $z = \sum_j \iota(\alpha_j) X^j$. By writing z as

$$z = \sum_{j=0}^{m-1} \iota(\alpha_j) X^j + \sum_{j=m}^{\deg(z)} \iota(\alpha_j) X^j = a + X^m c \tag{5.9}$$

one obtains the required decomposition with $b = X^m c$. The uniqueness of such decomposition then follows from the uniqueness of the decomposition as in Definition 5.1.

(ii) Follows from (i). In particular, one easily checks that R_m has cardinality $\#(R_m) = (n+1)^m$.

(iii) By construction the map $\iota : \mu_{n,+} \to R$ is a multiplicative section of the quotient map $R \to R_1$. It follows that the non-zero elements of R_1 form the multiplicative group μ_n so that R_1 is a field with $n+1$ elements.

(iv) The components of $z = \sum_j \iota(\alpha_j)\, X^j \in R$ are uniquely determined by $\pi(x)$.

(v) Let (R', X') be a second pair corresponding to the same map $h : \mu_n \to \mathcal{P}(\mu_n)$. Let $\rho : R \to R'$ be the bijective map defined by

$$\rho\Big(\sum_j \iota(\alpha_j)\, X^j\Big) := \sum_j \iota'(\alpha_j)\, X'^j, \quad \alpha_j \in \mu_n \cup \{0\}.$$

One has by construction

$$\deg(a) < m \implies \rho(a + X^m b) = \rho(a) + (X')^m \rho(b), \quad \forall b. \tag{5.10}$$

In particular one also has $\rho(J_m) = J'_m$ for all m. Thus ρ induces a bijection

$$\rho_m : R_m \to R'_m.$$

By (iii), to show that ρ is a ring homomorphism, it is enough to verify that each ρ_m is a ring homomorphism.

To show that ρ_m is additive it is enough to show that one can compute all the components of a sum

$$\sum_{j=0}^{m-1} \alpha_j\, X^j + \sum_{j=0}^{m-1} \beta_j\, X^j = \sum_{j=0}^{m-1} \gamma_j\, X^j \tag{5.11}$$

using only the map $h : \mu_n \to \mathcal{P}(\mu_n)$. To do this one first determines a map F from k-tuples of elements of $\mu_{n,+}$ to pairs (x, Z) where $x \in \mu_{n,+}$ and where Z is a $(k-1)$-tuple of elements of $\mathcal{P}(\mu_n)$. The map h determines uniquely a symmetric map

$$\begin{aligned} &H : \mu_{n,+} \times \mu_{n,+} \to \mu_{n,+} \times \mathcal{P}(\mu_n), \quad H(\xi,\eta) = (\xi+\eta, 0) \quad \text{if } \xi\eta = 0 \\ &H(\xi,\eta) = \big(H_0(\xi,\eta), P(\xi,\eta)\big), \quad H_0(\xi,\eta) + XP(\xi,\eta) = \eta\, h(\xi\eta^{-1}) \quad \text{if } \eta \neq 0. \end{aligned} \tag{5.12}$$

To define F one proceeds by induction on k. For $k = 1$ one lets $F(x) = x$. For $k = 2$ one lets $F_2 = H$. We denote the two components of $F_k : \mu_{n,+}^{k-1} \times \mu_{n,+} \to \mu_{n,+} \times \mathcal{P}(\mu_n)^{k-1}$ as $F_k^{(1)}$ and $F_k^{(2)}$. To pass from $k-1$ to k one lets

$$F_k^{(1)}(\alpha,\eta) := \big(H_0\big(F_{k-1}^{(1)}(\alpha),\eta\big)\big), \quad F_k^{(2)}(\alpha,\eta) := \big(F_{k-1}^{(2)}(\alpha), P\big(F_{k-1}^{(1)}(\alpha),\eta\big)\big),$$

where in the last expression we append the polynomial $P(F_{k-1}^{(1)}(\alpha),\eta)$ to the list $F_{k-1}^{(2)}(\alpha)$, thus obtaining a list of $k-1$ polynomials.

To compute the components γ_j of the sum (5.11), we build by induction on k, two lists. The first $R(k)$ is the list of the coefficients already computed and it is the single list given by $(\gamma_0, \gamma_1, \dots, \gamma_{k-1})$. The second $C(k)$ (called the carry-over) is a list of polynomials with coefficients in $\mu_{n,+}$ and it is encoded as the list of their coefficients. Each such list ℓ of coefficients has $m-k$ terms, all in $\mu_{n,+}$. We denote by $f(\ell) \in \mu_{n,+}$ the first term of the list ℓ and by $t(\ell)$ the list obtained by dropping the first element of the list ℓ; it has $m-k-1$ terms. The step to obtain $R(k+1), C(k+1)$ from $\alpha, \beta, R(k), C(k)$ is

$$R(k+1) := F^{(1)}\big(\alpha_k, \beta_k, \big(f(\ell)\big)_{\ell \in C(k)}\big)$$

and

$$C(k+1) := \big(t(\ell)\big)_{\ell \in C(k)}, \quad F^{(2)}\big(\alpha_k, \beta_k, \big(f(\ell)\big)_{\ell \in C(k)}\big)$$

where one replaces each element of $F^{(2)}(\alpha_k, \beta_k, (f(\ell))_{\ell \in C(k)})$ by the list of its first $m-k$ coefficients.

More concretely one first obtains $\gamma_0 = F_2^{(1)}(\alpha_0, \beta_0)$ while the carry-over delivers the polynomial $P(\alpha_0, \beta_0) = F_2^{(2)}(\alpha_0, \beta_0)$. Thus $R(1) = (\gamma_0)$, $C(1)$ has one element which is the list of the first $m-1$ coefficients of $P(\alpha_0, \beta_0)$. One then trims the elements α, β and considers the sum

$$\sum_{j=1}^{m-1} \alpha_j X^j + \sum_{j=1}^{m-1} \beta_j X^j + XP(\alpha_0, \beta_0). \tag{5.13}$$

All terms in (5.13) are divisible by X and one can use F_3 to compute the sum of the three terms α_1, β_1, p_0 where p_0 is the constant term of $P(\alpha_0, \beta_0)$. This operation delivers the next term

$$\gamma_1 = F_3^{(1)}(\alpha_1, \beta_1, p_0)$$

of (5.11) and adjoins the two polynomials of the list $F_3^{(2)}(\alpha_1, \beta_1, p_0)$ to the list of carry-over consisting of the single polynomial $P(\alpha_0, \beta_0)$ with its first term p_0 deleted. The carry-over list consists now of three terms ℓ_1, ℓ_2, ℓ_3. One then uses F_5 to compute the sum of the 5 terms : α_2, β_2 and the three terms $f(\ell_1), f(\ell_2), f(\ell_3)$ from the carry-over. This adds 4 terms to the list of carry-over which has now 7 terms, where the three previous ones have been trimmed by deleting their lowest term. After k such steps the carry-over list has $2^k - 1$ elements and one proceeds as follows. One uses F_{2^k+1} to compute the sum of the $2^k + 1$ terms given by α_k, β_k together with the terms $f(\ell)$ of the carry-over list. This operation delivers γ_k and adjoins 2^k terms to the carry-over list which now consists of $2^{k+1} - 1$ terms. This process terminates when $k = m$ and $R(m)$ delivers universal formulas for the terms $\gamma_j, 0 \leq j \leq m-1$ using only α, β and the map h.

The fact that the coefficients γ_j can be computed using only α, β and the map h proves that ρ is additive since one can use the same formula to compute $\alpha + \beta$ in R_m and $\rho_m(\alpha) + \rho_m(\beta)$ in R'_m. The multiplicativity of ρ follows by bilinearity from $\rho(\alpha X^n \times \beta X^m) = \rho(\alpha X^n)\rho(\beta X^m)$. This shows that $\rho : R \to R'$ is a ring isomorphism and by construction one has $\rho(X) = X'$. ∎

DEFINITION 5.14. The map

$$h : \mu_n \to \mathcal{P}(\mu_n), \quad \sigma\big(h(\xi)\big) = \iota(\xi) + 1 \tag{5.15}$$

which characterizes the pair (R, X) (by Proposition 5.8) is called the *hold* of the pair (R, X).

COROLLARY 5.16. *Let n be such that there exists a polynomial ring in one generator over $\mathbb{S}[\mu_{n,+}]$; then $n + 1$ is a prime power.*

PROOF. This follows from Proposition 5.8 (iii). ∎

REMARK 5.17. The proof of Proposition 5.8 (v) is stated so that one can, by following it, write a computer program which can be used to test the additive structure of the ring R_m. This will be relevant in Section 6 to determine in the various examples the rings R_m.

The map $h : \mu_n \to \mathcal{P}(\mu_n)$ of (5.15) determines the addition $H : \mu_{n,+} \times \mu_{n,+} \to \mu_{n,+} \times \mathcal{P}(\mu_n)$, (5.12), of pairs of elements of $\mu_{n,+}$ using the compatibility with multiplication by elements of μ_n.

Proposition 5.8 shows that a pair (R, X), where X is an $\mathbb{S}[\pm 1]$-generator of R, i.e. $n = 2$, is uniquely characterized by the polynomial $P(X)$ as in (5.7). The polynomial $P(X) = -1$ produces the pair $(\mathbb{F}_3[X], X)$, while $P(X) = X - 1$ determines the pair $(\mathbb{Z}, 3)$.

When $n = 2$, the constant term of the polynomial $P(X)$ in (5.7) is necessarily equal to -1. Indeed, had the constant term be 0 or 1, one would contradict the uniqueness of the decomposition of Definition 5.1 by the equality $1 = P(X) - 1$. This also shows that $R_1 = \mathbb{F}_3$.

REMARK 5.18. It is not true that a random choice of a polynomial with coefficients in $\mathbb{S}[\pm 1]$ and constant coefficient -1 corresponds to a pair. A simple case is with $P(X) = -1 + X + X^2$. Indeed, in the following lines we show that 5 is not represented by any polynomial. With this rule, one has $1 + 1 + 1 + 1 = 1 + X + X^2$. Adding 1 to both sides gives

$$\begin{aligned} 1 + 1 + 1 + 1 + 1 &= -1 + X + X^2 + X + X^2 \\ &= -1 + X(-1 + X + X^2) + X^2(-1 + X + +X^2) \\ &= -1 - X + X^3 + X^3 + X^4 \end{aligned}$$

$$= -1 - X + X^3(-1 + X + X^2) + X^4$$
$$= -1 - X - X^3 + X^4 + X^4 + X^5.$$

Then, when working in R_n (i.e. modulo X^n) the number 5 is represented by

$$5 = -1 - X - X^3 - X^4 - X^5 - \cdots - X^{n-1} \in R_n$$

and this expression is of degree $n-1$ for any n and thus does not correspond to a finite sum of powers of X.

6. Examples

In this section we give examples of polynomial rings (R, X) in one generator X over $\mathbb{S}[\mu_{n,+}]$ where R is of characteristic zero. The ring R is embedded as a subring of $\mathbb{C}$ by solving for $X \in \mathbb{C}$ the equations $\sigma(h(\xi)) = \iota(\xi) + 1$, $\xi \in \mu_n$, using the canonical embedding $\mu_{n,+} \subset \mathbb{C}$. The projective limit $\varprojlim R_n$ is, in these examples, a finite extension of the ring of p-adic integers $\mathbb{Z}_p$. While one can use the axiom of choice to show the existence of an embedding of the p-adic field $\mathbb{Q}_p$ in the field of complex numbers, such embeddings have the status of a chimera. Indeed, the continuity of measurable characters of compact groups applied to the additive group $\mathbb{Z}_p$ shows that an embedding of the p-adic field $\mathbb{Q}_p$ in the field of complex numbers is automatically non-measurable. On the other hand, the next examples will show that polynomial rings (R, X) in one generator X over $\mathbb{S}[\mu_{n,+}]$ provide instances of explicit interactions of p-adic fields (and their finite extensions) with the complex numbers. These interactions are given by pairs of embeddings with dense ranges

$$\mathbb{F}_q \overset{\pi}{\twoheadleftarrow} W(\mathbb{F}_q) \hookrightarrow W(\mathbb{F}_q)[\eta] \hookleftarrow R[X^{-1}] \hookrightarrow \mathbb{C}$$

of the ring of Laurent polynomials $R[X^{-1}]$. The left embedding in the above diagram is in a finite algebraic extension $W(\mathbb{F}_q)[\eta]$ of the Witt ring $W(\mathbb{F}_q)$. The field of fractions of the ring $W(\mathbb{F}_q)[\eta]$ is a finite extension of the p-adic field. Most of these examples come from known number systems and have their origin in the search of optimal manners of encoding numbers [21]. In each case, the quotient $R_1 = R/(XR)$ is the finite field $\mathbb{F}_q$, $q = n + 1$, and the multiplicative semi-group isomorphism

$$j : \mathbb{F}_q \sim \mu_{n,+} \subset \mathbb{C}$$

serves as a guide, using the addition in the finite field $\mathbb{F}_q$, for the terms of degree 0 in the construction of the map h. Note that the choice of j for $\overline{\mathbb{F}}_q$ plays a key role in the construction by Quillen [25] of the relation between the algebraic K-theory of $\mathbb{F}_q$ and the Adams operations.

6.1. *Polynomial rings in one generator over* $\mathbb{S} = \mathbb{S}[\mu_{1,+}]$

When working over $\mathbb{S} = \mathbb{S}[\mu_{1,+}]$ there is no cancelation since there is no minus sign available. Thus starting from two non-zero elements x, y the equality $x + y = 0$ can only be verified in the projective limit $\varprojlim R_m$. We compute this projective limit in the next examples.

6.1.1. *The polynomial ring* $(\mathbb{Z}, -2)$

The ring $\mathbb{Z}$ admits the generator $X = -2$ over $\mathbb{S}$. The hold is given by $1 + 1 = P(X) = X + X^2$. The values of the polynomials of degree n at $X = -2$ are reported for the first values of n in the following table:

n	$\{p(-2) : \deg p = n\}$
0	$[0, 1] \cap \mathbb{Z}$
1	$[-2, -1] \cap \mathbb{Z}$
2	$[2, 5] \cap \mathbb{Z}$
3	$[-10, -3] \cap \mathbb{Z}$
4	$[6, 21] \cap \mathbb{Z}$
5	$[-42, -11] \cap \mathbb{Z}$
6	$[22, 85] \cap \mathbb{Z}$

Let us look, for example, at the computation of $1 + 1 + X$. One gets

$$1 + 1 + X = X + X^2 + X = X(1 + 1 + X)$$

and iterating this step one gets that $1 + 1 + X \in J_m = \langle X^m \rangle R$, $\forall m$. This shows that $1 + 1 + X = 0$ in $\varprojlim R_m$. Next we relate the degree of the polynomial $p(X)$ with the absolute value of the integer $p(-2)$. Let

$$j(n) := \frac{1}{3}(-2)^n - \frac{1}{2}(-1)^n + \frac{1}{6} \quad n \in \mathbb{N}. \tag{6.1}$$

The degree n of a polynomial $p(X)$ with coefficients in $\{0, 1\}$ specifies the sign of the integer $p(-2)$ as $(-1)^n$ and provides lower and upper bounds on the modulus $|p(-2)|$ as follows:

$$\big|j(n-1)\big| < \big|p(-2)\big| \leq \big|j(n+1)\big|.$$

Given an integer $m \in \mathbb{Z}$, the first inequality provides the following bound, on the degree of the polynomial p such that $p(-2) = m$:

$$\deg(p) \leq \log_2\big(3|m| + 2\big) + 1.$$

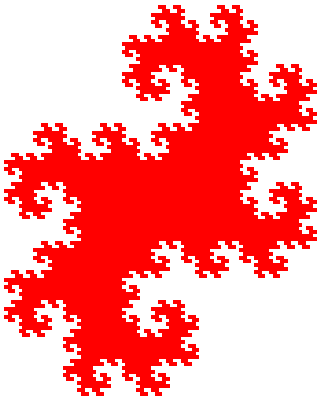


FIGURE 2. Gaussian integers as $\mathbb{S}$-polynomials in degree ≤ 12.

The projective limit $\varprojlim R_m$ is here the ring $\mathbb{Z}_2$ of 2-adic integers, and the elements of $\mathbb{Z}$ inside $\mathbb{Z}_2$ are characterized by the fact that their sequence of digits is eventually constant.

Next, we turn to quadratic fields for which the study of number systems in [19, 20] provides an exhaustive list of examples. One easily deduces from op. cit. the following.

PROPOSITION 6.2. *The quadratic fields K whose ring of integers admit an $\mathbb{S}$-generator are*

- $\mathbb{Q}(\sqrt{-1})$ *with generator* $X = -1 + \sqrt{-1}$ *of the ring* $\mathbb{Z}[\sqrt{-1}]$ *of integers of* K.
- $\mathbb{Q}(\sqrt{-2})$ *with generator* $X = \sqrt{-2}$ *of the ring* $\mathbb{Z}[\sqrt{-2}]$ *of integers of* K.
- $\mathbb{Q}(\sqrt{-7})$ *with generator* $X = \frac{1}{2}(1 + \sqrt{-7})$ *of the ring of integers of* K.

PROOF. The norm $N(\alpha)$ of an $\mathbb{S}$-generator is equal to 2; thus the set

$$N_0(\alpha) := \{0, \dots, N(\alpha) - 1\}$$

defining a canonical number system in the sense of [19, 20] is $\{0, 1\}$ and the result follows from [20, Theorem 1] in the complex case and Satz 1 of [19] in the real case. ∎

6.1.2. The polynomial ring $(\mathbb{Z}[i], -1 + i)$

Here, we consider the ring $R = \mathbb{Z}[i]$ of Gaussian integers (sometimes called binarions; see [5]) with $X = -1 + i$ as $\mathbb{S}[\mu_{1,+}] = \mathbb{S}$-generator. Indeed, every Gaussian integers can be written uniquely as a finite sum of powers of X ([17, 26] and Figure 2). One has the equality $1 + 1 = P(X) = X^2 + X^3$, which allows one to compute the sum of any pair of polynomials with coefficients in $\{0, 1\}$.

PROPOSITION 6.3. *Let* $R = \mathbb{Z}[i]$, $X = -1 + i$.

(i) *The ideal of* $R = \mathbb{Z}[i]$ *generated by* X^2 *is the same as the ideal generated by* 2.

(ii) *The ring* R_m *for* $m = 2k$ *is* $\mathbb{Z}/(2^k\mathbb{Z})[X]$ *where* $X^2 = -2 - 2X$.

(iii) *The ring* R_m *for* $m = 2k+1$ *is* $\mathbb{Z}/(2^{k+1}\mathbb{Z}) \oplus \mathbb{Z}/(2^k\mathbb{Z})\ X$ *where* $X^2 = -2-2X$.

(iv) *The projective limit* $\varprojlim R_m$ *is the ring* $\mathbb{Z}_2[i] \sim \mathbb{Z}_2[X]$ *where* $X^2 = -2 - 2X$.

PROOF. (i) The element $U = (1 + X) \in R$ is a unit since $U^4 = 1$ and one has

$$X^2 = -2 - 2X \in 2R, \quad 2 = -(1 + X)^{-1}X^2 \in X^2R.$$

(ii) By (i) the ideal $X^{2k}R$ is equal to 2^kR. One has $R = \mathbb{Z}[i]$ and $R/(2^kR) = \mathbb{Z}/(2^k\mathbb{Z})[i] = \mathbb{Z}/(2^k\mathbb{Z})[X]$ with $X^2 = -2 - 2X$; thus one gets (ii).

(iii) Let $m = 2k + 1$. Any element of R is of the form $z = a + bX$ where $a, b \in \mathbb{Z}$. In R one has $2^{k+1} \in X^{2k+2}R \subset J_m$ and $2^kX \in X^{2k+1}R = J_m$. Thus the homomorphism $\mathbb{Z}[X] \to R_m$ induces a surjective homomorphism from $\mathbb{Z}/(2^{k+1}\mathbb{Z}) \oplus \mathbb{Z}/(2^k\mathbb{Z})\ X$ to R_m. It is bijective since the cardinalities are equal.

(iv) The extension $\mathbb{Q}_2[i]$ is totally ramified of index $e = 2$ (see [26, Chapter 2, Section 4.2, Example 1]). The polynomial X^2+2X+2 is an Eisenstein polynomial which defines $\mathbb{Q}_2[i]$ as its splitting field. The valuation of X is one half of the valuation of 2. ∎

6.1.3. The polynomial ring $(\mathbb{Z}[\sqrt{-2}], \sqrt{-2})$

The element $X := \sqrt{-2}$ is an $\mathbb{S}[\mu_{1,+}] = \mathbb{S}$-generator of the ring of integers $\mathbb{Z}[\sqrt{-2}]$ of the imaginary quadratic field $\mathbb{Q}(\sqrt{-2})$. This follows directly from Section 6.1.1 and Proposition 5.5. The hold is given by the polynomial $P(X) = X^4 + X^2$. A straightforward analogue of Proposition 6.3 holds.

6.1.4. The polynomial ring $(\mathcal{O}(\mathbb{Q}(\sqrt{-7})), \frac{1}{2}(1 + \sqrt{-7}))$

The element $X := \frac{1}{2}(1 + \sqrt{-7})$ is an $\mathbb{S}[\mu_{1,+}] = \mathbb{S}$-generator of the ring $\mathcal{O}(\mathbb{Q}(\sqrt{-7}))$ of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-7})$. The hold is given by the polynomial $P(X) = X^3 + X$. Let F be the fundamental domain of $\mathcal{O}(\mathbb{Q}(\sqrt{-7}))$ given by the parallelogram with vertices $0, 1, X, X + 1$. Figure 3 shows the neighborhood of $0 \in \mathbb{C}$ obtained as the union of the translations $F + p(X)$ by polynomials $p(X)$ of degree ≤ 11.

PROPOSITION 6.4. *Let* $R = \mathcal{O}(\mathbb{Q}(\sqrt{-7}))$, $X = \frac{1}{2}(1 + \sqrt{-7})$.

(i) *The ring* R_m *is* $\mathbb{Z}/(2^m\mathbb{Z})$.

(ii) *The projective limit* $\varprojlim R_m$ *is the ring* $\mathbb{Z}_2$.

(iii) *The element* $X \in \varprojlim R_m = \mathbb{Z}_2$ *is the only solution divisible by* 2 *in the ring* $\mathbb{Z}_2$ *for the equation* $2 + X + X^2 = 0$.

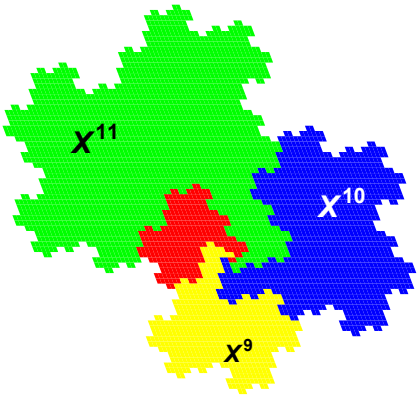


FIGURE 3. Polynomials of degree ≤ 11 for $X = \frac{1}{2}(1+\sqrt{-7})$.

PROOF. The hold is given by $P(X) = X^3 + X$ and one has

$$P(X) - 2 = (X-1)(X^2 + X + 2).$$

By Hensel's Lemma, the equation $2 + X + X^2 = 0$ admits a unique solution α in $\mathbb{Z}_2$ of the form $\alpha = 1 + 2\varepsilon$ and a unique solution of the form $\beta = 2(1 + 2\varepsilon')$. In fact one has $\alpha\beta = 2$ and $\alpha + \beta = -1$. The homomorphism $\rho : \mathbb{Z}[\frac{1}{2}(1+\sqrt{-7})] \to \mathbb{Z}_2$ given by $\rho(\frac{1}{2}(1+\sqrt{-7})) = \beta$ is well defined since β is a solution of the equation $2 + X + X^2 = 0$. Moreover β is the product of 2 by a unit of $\mathbb{Z}_2$ (but this fails in $R = \mathcal{O}(\mathbb{Q}(\sqrt{-7}))$). The projection X_m of β in $\mathbb{Z}_2/(2^m\mathbb{Z}_2) = \mathbb{Z}/(2^m\mathbb{Z})$ fulfills $P(X_m) = 2$ and X_m is the product of 2 by a unit. Thus the ideals generated by powers of X_m are the same as those generated by powers of 2. This proves the three assertions (i), (ii), and (iii). ∎

6.2. *Polynomial rings in one generator over* $\mathbb{S}[\pm 1]$

6.2.1. *The polynomial ring* $(\mathbb{Z}, 3)$

The case of the $\mathbb{S}[\pm 1]$-generator $3 \in \mathbb{Z}$ is particularly relevant because, as shown in [14], the addition coincides with that of the Witt vectors in $W(\mathbb{F}_3) = \mathbb{Z}_3$.

PROPOSITION 6.5. *Suppose* $R = \mathbb{Z}$, $X = 3$ *is an* $\mathbb{S}[\pm 1]$*-generator of* R. *The hold is* $P(X) = -1 + X$.

(i) *The ring* R_m *is* $\mathbb{Z}/(3^m\mathbb{Z})$.

(ii) *The projective limit* $\varprojlim R_m$ *is the ring* $W(\mathbb{F}_3) = \mathbb{Z}_3$.

(iii) *The set of Witt vectors with only finitely many non-zero components forms a subring of* $W(\mathbb{F}_3)$ *isomorphic to* $\mathbb{Z}$.

In order to organize the next examples we give the list of imaginary quadratic field extensions of $\mathbb{Q}$ generated by rings of $\mathbb{S}[\pm 1]$-polynomials in one variable.

PROPOSITION 6.6. *The imaginary quadratic fields K generated by rings of $\mathbb{S}[\pm 1]$-polynomials in one variable are*

- $\mathbb{Q}(\sqrt{-2})$ *with generator* $X = 1 + \sqrt{-2}$ *of the ring* $\mathbb{Z}[\sqrt{-2}]$ *of integers of* K.
- $\mathbb{Q}(\sqrt{-3})$ *with generator* $X = \sqrt{-3}$ *of* $\mathbb{Z}[\sqrt{-3}]$ *(not a UFD).*
- $\mathbb{Q}(\sqrt{-11})$ *with generator* $X = \frac{1}{2}(1 + \sqrt{-11})$ *of the ring of integers of* K.

PROOF. Let $P(X) = -1 + \sum_{j=1}^{n-1} a(j)X^j + \varepsilon X^n$, $\varepsilon \in \{\pm 1\}$, $a(j) \in \{-1, 0, 1\}$, be the carry-over leading to an imaginary quadratic extension. The roots of the polynomial $P(X) - 2$ are algebraic integers, and we assume that one of them, say α, is quadratic imaginary. Let $q(x) = x^2 - bx + c$ be its minimal polynomial. It has integral coefficients so $b, c \in \mathbb{Z}$, and by definition, it divides $P(X) - 2$. The constant coefficient c must be equal to 3. Indeed it divides the constant coefficient -3 of $P(X) - 2$, and since $b^2 - 4c < 0$, it is positive. It cannot be equal to 1 since in that case one would get $b \in \{-1, 0, 1\}$, and $\alpha \in \{i, j, -j\}$ which contradicts the injectivity of the map σ. For $c = 3$ the possible values of b are $b = 0$ which gives the solution $\alpha = \sqrt{-3}$, $b = \pm 1$ which gives the solutions $\alpha = \frac{1}{2}(\pm 1 \pm i\sqrt{11})$, $b = \pm 2$ which gives the solutions $\alpha = \pm 1 \pm i\sqrt{2}$, and finally $b = \pm 3$. We shall now show that this last choice which gives $\alpha = \frac{1}{2}(\pm 3 \pm i\sqrt{3})$ does not give a solution. To prove this it is enough to show that the polynomial $3 + 3X + X^2$ cannot divide a polynomial $P(X) - 2$ with P of the above form. We thus assume an equality of the form

$$(3 + 3X + X^2)\left(\sum_{j=0}^{n-2} b(j)X^j\right) = -3 + \sum_{j=1}^{n-1} a(j)X^j + \varepsilon X^n, \quad \varepsilon \in \{\pm 1\},\ a(j) \in \{-1, 0, 1\}.$$

Since the coefficients of $P - 2$ are integers and the leading coefficient of $3 + 3X + X^2$ is 1, the coefficients $b(j)$ are integers. We get $b(0) = -1$, $3b(1) - 3 = a(1)$, but $a(1) \in \{-1, 0, 1\}$ and thus working modulo 3 one gets $a(1) = 0$ and hence $b(1) = 1$. Considering the coefficient of X^2 we get $3b(1) + 3b(2) - 1 = a(2)$ which gives $a(2) = -1$ and $b(2) = -b(1) = -1$. We can now work by induction to show that $b(j) = (-1)^{j+1}$. Indeed the coefficient of X^j is $b(j-2) + 3b(j-1) + 3b(j) = a(j)$ and if we know that $b(j-2) = (-1)^{j-1}$ and $b(j-1) = (-1)^j$ we get $a(j) = b(j-2)$ and $3b(j-1) + 3b(j) = 0$ so that $b(j) = (-1)^{j+1}$. This works for $j \leq n-2$. The coefficient of X^{n-1} is $b(n-3) + 3b(n-2) = a(n-1)$ and this gives a contradiction

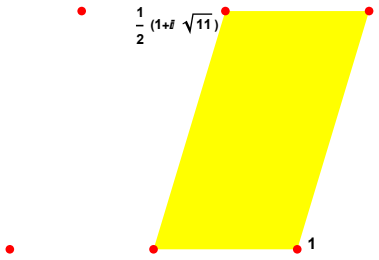


FIGURE 4. Fundamental domain of the lattice $\mathcal{O}$.

since one gets $a(n-1) = b(n-3)$ (working modulo 3) which contradicts the fact that $b(n-2) \neq 0$. ∎

6.2.2. The polynomial ring $(\mathcal{O}(\mathbb{Q}[\sqrt{-11}]), \frac{1}{2}(1+\sqrt{-11}))$

This section is dedicated to a detailed proof that $X := \frac{1}{2}(1+\sqrt{-11})$ is an $\mathbb{S}[\pm 1]$-generator of the ring of integers of the number field $\mathbb{Q}(\sqrt{-11})$. The reason for providing the details of the proof is that we want to emphasize that in such a case, and unlike working over $\mathbb{S}$, one can explicitly control the cancelations in the computations.

PROPOSITION 6.7. *Let $\mathcal{O}$ be the ring of integers of the number field $\mathbb{Q}(\sqrt{-11})$.*

(i) $X := \frac{1}{2}(1+\sqrt{-11})$ *is an $\mathbb{S}[\pm 1]$-generator of $\mathcal{O}$. The hold of $(\mathcal{O}, X)$ is $P(X) = -1 + X - X^2$.*

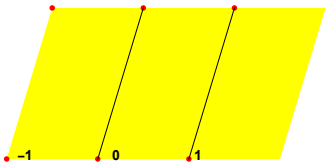
(ii) *The projective limit $\varprojlim R_m$ is the ring $W(\mathbb{F}_3) = \mathbb{Z}_3$.*

The proof requires a preliminary lemma. We first recall some classical results concerning the ring of integers $\mathcal{O}$ of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-11})$. The discriminant of K is $d = -11$. Thus since $-11 \sim 1$ modulo 4, the lattice $\mathcal{O}$ is $\mathbb{Z} + \mathbb{Z}X$ where $X := \frac{1}{2}(1+\sqrt{-11})$. By construction one has

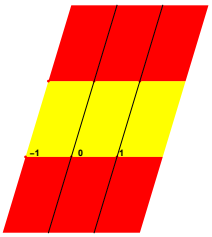
$$1 + 1 = P(X), \quad P(X) = -1 + X - X^2. \tag{6.8}$$

One wants to show that every element $z \in \mathcal{O}$ can be written uniquely as a polynomial $z = \sum_j \alpha_j X^j$, with $\alpha_j \in \{-1, 0, 1\}$. Figure 4 shows the translates of the fundamental domain of the lattice, while the next figures provide a sketch of a few steps of the process of representing elements of $\mathcal{O}$ in terms of polynomials of degree $\leq n$, showing those described by polynomials of degree $= n$ with a new color.

By comparing Figures 5 (a), 5 (b), 6 (a), 6 (b), 7 (a), and 7 (b), one notices that the translation $z \mapsto z + 1$ does not increase the degree of the polynomial by more than 2 units. The next lemma provides a formal proof of this fact.

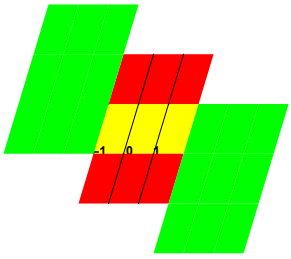


(A) First step, polynomials of degree 0

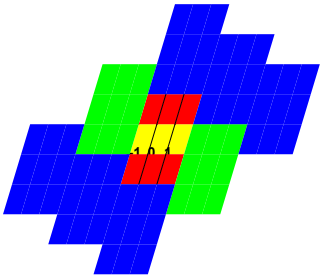


(B) Second step, polynomials of degree ≤ 1

FIGURE 5. The first two steps.

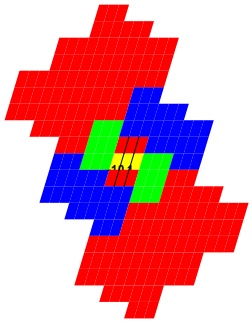


(A) Third step, polynomials of degree ≤ 2

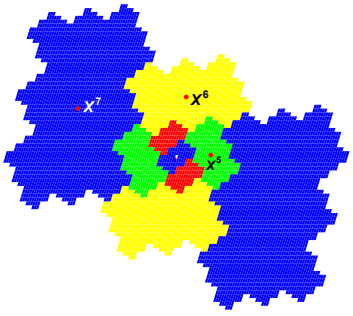


(B) Fourth step, polynomials of degree ≤ 3

FIGURE 6. The third and fourth steps.



(A) Fifth step, polynomials of degree ≤ 4



(B) Eighth step, polynomials of degree ≤ 7

FIGURE 7. The fifth and eighth steps.

LEMMA 6.9. *Let $z = \sum_{j=0}^{n} \alpha_j X^j \in \mathcal{O}$, $\alpha_j \in \{-1, 0, 1\}$. Then there exist coefficients $\beta_j \in \{-1, 0, 1\}$, with $0 \leq j \leq n+2$, such that $z + 1 = \sum_{j=0}^{n+2} \beta_j X^j$.*

PROOF. We proceed by induction on the integer n. For $n = 0$, the result follows from (6.8). Let us assume that the result is proved up to $n-1$; then there exist coefficients $\gamma_j \in \{-1, 0, 1\}$ such that

$$z = \left(\sum_{j=0}^{n-1} \alpha_j X^j \right) + \alpha_n X^n \implies z + 1 = \left(\sum_{j=0}^{n+1} \gamma_j X^j \right) + \alpha_n X^n.$$

Let us consider a sum such as $\gamma_n X^n + \gamma_{n+1} X^{n+1} + \alpha_n X^n$ and express it without going beyond X^{n+2}. If $\gamma_{n+1} = 0$, this follows again from (6.8). We can thus assume that $\gamma_{n+1} = \pm 1$ and also that both γ_n and α_n are non-zero and equal since otherwise the sum $\gamma_n X^n + \alpha_n X^n$ would have degree at most n. The only case to exclude then is when γ_n, α_n, and γ_{n+1} are all equal (and non-zero) since only in that case would one get a term in X^{n+3} from the sum

$$\begin{aligned} X^n + X^n + X^{n+1} &= X^n(1 + 1 + X) = X^n(-1 + X + X - X^2) \\ &= X^n(-1 - X + X^2 - X^2 - X^3) \\ &= -X^n - X^{n+1} - X^{n+3}. \end{aligned}$$

To exclude this case, one adds to the induction hypothesis the condition that if the last term β_{n+2} of the polynomial of degree $n+2$ representing $z+1$ is non-zero, then the term β_{n+1} is zero or of the opposite sign. This condition is fulfilled for $n = 0$, and if we assume it for $n-1$, it holds also for n. Indeed, the only cases when $\beta_{n+2} \neq 0$ arise when either $\gamma_{n+1} = 0$, in which case β_{n+1} and β_{n+2} have opposite signs, or $\gamma_{n+1} = \varepsilon = \pm 1$, in which case $\gamma_n = \alpha_n = -\varepsilon$, which gives

$$\gamma_n X^n + \gamma_{n+1} X^{n+1} + \alpha_n X^n = -\varepsilon X^n (1 + 1 - X) = \varepsilon X^n + \varepsilon X^{n+2},$$

implying that $\beta_{n+1} = 0$ in this case. Thus the induction hypothesis still holds for n, and this concludes the proof. ∎

PROOF OF PROPOSITION 6.7. Lemma 6.9 holds for the abstract law of addition defined using (6.8) on the projective limit of the R_n. The proof shows that the elements of this limit, which have only a finite number of non-zero coordinates, are stable under the addition of 1. Using (5.10), it follows that they are also stable under the addition of any monomial and hence that they form an additive group A. Thus, it remains to show that the map $\rho : A \to \mathbb{C}$ defined by

$$\rho\Big(\sum_j \alpha_j X^j \Big) := \sum_j \alpha_j z^j, \quad z = \frac{1}{2}(1 + \sqrt{-11})$$

is injective. Let $\sum_j \alpha_j X^j \in \ker \rho$; then $\sum_j \alpha_j z^j = 0$ and thus z fulfills an equation $E(z) = 0$ with integral coefficients whose leading coefficient is 1 and the constant term is ± 1. The polynomial E is thus a multiple of the minimal polynomial $z^2 - z + 3$ of the field extension. The quotient polynomial has integral coefficients; thus, one gets a contradiction using the product of constant terms. ∎

6.2.3. The polynomial ring $(\mathbb{Z}[\sqrt{-3}], \sqrt{-3})$

The element $X := \sqrt{-3}$ is an $\mathbb{S}[\mu_{2,+}] = \mathbb{S}[\pm 1]$-generator of the ring $\mathbb{Z}[\sqrt{-3}]$ and the latter is a maximal order in the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$. This follows directly from Section 6.1.1 and Proposition 5.5. The hold is given by the polynomial $P(X) = -1 - X^2$. A straightforward analogue of Proposition 6.3 holds.

6.2.4. The polynomial ring $(\mathcal{O}(\mathbb{Q}(\sqrt{-2})), 1 + \sqrt{-2})$

One obtains similarly that $P(X) = -1 - X + X^2 - X^3$ is the hold associated with the $\mathbb{S}[\pm 1]$ generator $1 + \sqrt{-2}$ of the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-2})$.

PROPOSITION 6.10. *Let $\mathcal{O}$ be the ring of integers of the number field $\mathbb{Q}(\sqrt{-2})$.*

(i) *$X := 1 + \sqrt{-2}$ is an $\mathbb{S}[\pm 1]$-generator of $\mathcal{O}$. The hold of $(\mathcal{O}, X)$ is $P(X) = -1 - X + X^2 - X^3$.*

(ii) *The projective limit $\varprojlim R_m$ is the ring $W(\mathbb{F}_3) = \mathbb{Z}_3$.*

Figure 8 reproduces the pattern obtained by inputting polynomials of degree ≤ 9. In this case, the analog of Lemma 6.9 holds with the bound $n + 3$ instead of $n + 2$.

6.3. Polynomial rings in one generator over $\mathbb{S}[\mu_{3,+}]$

In the next proposition/example, the field R_1 is the finite field $\mathbb{F}_4$. One lets $\mu_{3,+} \subset \mathbb{C}$ be the solutions of $x(x^3 - 1) = 0$, $j = \exp(2\pi i/3)$, and $\mathbb{Z}(j) \subset \mathbb{Q}(j)$ the ring of integers of the quadratic imaginary field $\mathbb{Q}(j)$.

PROPOSITION 6.11.

(i) *The number $-2 \in \mathbb{Z}(j)$ is an $\mathbb{S}[\mu_{3,+}]$-generator of the ring $R = \mathbb{Z}(j)$.*

(ii) *The hold is given by*

$$h(1) = X + X^2, \quad h(j) = j^2 X + j^2, \quad h(j^2) = jX + j.$$

(iii) *The field R_1 is the finite field $\mathbb{F}_4$.*

(iv) *The projective limit $\varprojlim R_m$ is the Witt ring $W(\mathbb{F}_4)$ and the ring R_m is the quotient of $W(\mathbb{F}_4)$ by $2^m\, W(\mathbb{F}_4)$.*

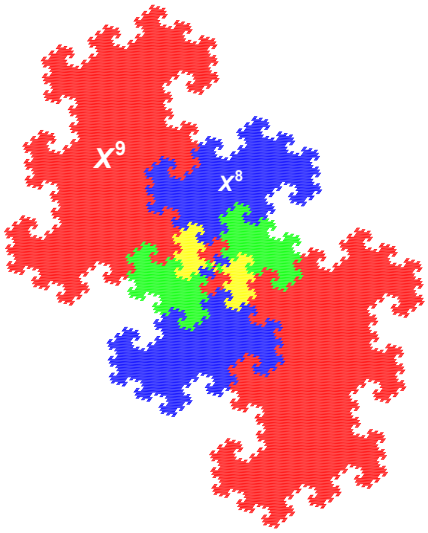


FIGURE 8. Polynomials of degree ≤ 9 for $X = 1 + i\sqrt{2}$.

PROOF. Let $J = 2\mathbb{Z}(j) \subset \mathbb{Z}(j)$; then J^n is the ideal generated by X^n where $X = -2$. Let $\sigma : \mathcal{P}(\mu_3) \to R = \mathbb{Z}(j)$ be the map defined by (5.3). For each n the composition $\pi_n \circ \sigma$, from the subset $\mathcal{P}^{n-1}(\mu_3) \subset \mathcal{P}(\mu_3)$ formed of polynomials of degree $< n$ to the quotient ring $R_n = R/J^n$, is surjective and hence injective since the cardinalities of source and target are the same. It follows that the map $\sigma : \mathcal{P}(\mu_3) \to R = \mathbb{Z}(j)$ is injective. To show that it is surjective one uses the general method involving the limit of the subsets

$$Z_n := (-2)^{-n}\big(\sigma\big(\mathcal{P}^n(\mu_3) + F\big)\big) \subset \mathbb{C},$$

where F is a fundamental domain for $\mathbb{Z}(j)$. One observes that passing from n to $n+1$ only alters Z_n on its boundary and that Z_n contains an open disk centered at 0 (cf. Figure 9). ∎

6.4. *Polynomial rings in one generator over* $\mathbb{S}[\mu_{4,+}]$

In this case, we have the following.

PROPOSITION 6.12.

(i) *The number* $X = 1 + 2i$ *is an* $\mathbb{S}[\mu_{4,+}]$*-generator of the ring* $R = \mathbb{Z}(i)$.

(ii) *The hold is given by* $h(0) = 1$ *and*

$$h(1) = i - i\,X, \quad h(i) = -i + X, \quad h(-i) = -1 - i\,X.$$

(iii) *The field* R_1 *is the finite field* $\mathbb{F}_5$.

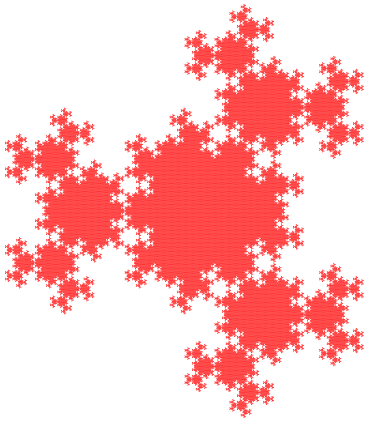


FIGURE 9. Polynomials of degree ≤ 7 for $X = -2$.

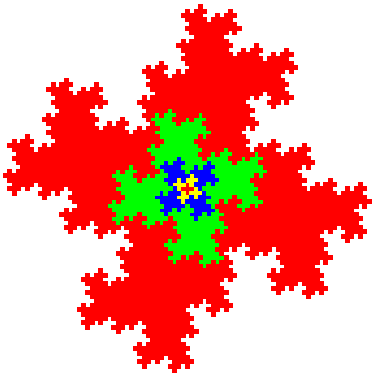


FIGURE 10. Polynomials of degree ≤ 4 for $X = 1 + 2i$.

(iv) *The projective limit* $\varprojlim R_m$ *is the Witt ring* $W(\mathbb{F}_5) = \mathbb{Z}_5$ *and the ring* R_m *is the quotient of* $W(\mathbb{F}_5)$ *by* $5^m\, W(\mathbb{F}_5)$.

PROOF. In the p-adic field $\mathbb{Z}_5$ there exists a unique square root of -1 equal to 2 modulo 5 (see [26, Section 6.7]). Let $\rho : \mathbb{Z}(i) \to \mathbb{Z}_5$ be the unique morphism such that, modulo 5, one has $\rho(i) = 2$. Then $\rho(X) = 5u$ where u is a unit in $\mathbb{Z}_5$. The morphism ρ restricted to $\mu_{4,+} = \{0, 1, i, -1, -i\}$ gives a multiplicative section of the quotient map $R \to R/XR$. One has $\mathbb{Z}_5/\rho(X)^m\mathbb{Z}_5 = \mathbb{Z}/5^m\mathbb{Z}$ and the morphism ρ induces an isomorphism

$$R_m \simeq \mathbb{Z}_5 = \mathbb{Z}/5^m\mathbb{Z}.$$

Statements (iii) and (iv) follow, as well as the injectivity of the map $\sigma : \mathcal{P}(\mu_4) \to R = \mathbb{Z}(i)$. One can prove the surjectivity of σ as for Proposition 6.11 using Figure 10. Statements (i) and (ii) follow. ∎

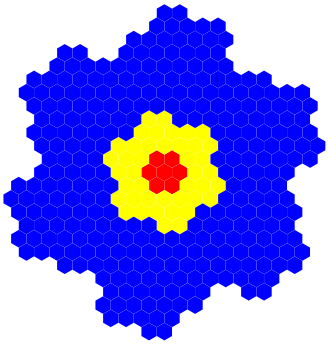


FIGURE 11. Polynomials of degree ≤ 2 for $X = \frac{5}{2} - \frac{i\sqrt{3}}{2}$.

6.5. *Polynomial rings in one generator over* $\mathbb{S}[\mu_{6,+}]$

The following proposition holds (see also Figure 11).

PROPOSITION 6.13.

(i) *The number* $X = 2 - j$ *is an* $\mathbb{S}[\mu_{6,+}]$*-generator of the ring* $R = \mathbb{Z}(j)$.

(ii) *The hold is given by* $h(j) = j + 1$, $h(j^2) = j^2 + 1$, $h(0) = 1$, *and*

$$h(1) = X + j, \quad h(-j^2) = -j^2 X + j^2, \quad h(-j) = -1 + X.$$

(iii) *The field* R_1 *is the finite field* $\mathbb{F}_7$.

(iv) *The projective limit* $\varprojlim R_m$ *is the Witt ring* $W(\mathbb{F}_7) = \mathbb{Z}_7$ *and the ring* R_m *is the quotient of* $W(\mathbb{F}_7)$ *by* 7^m $W(\mathbb{F}_7)$.

The proof can be easily deduced from [26, Section 4.6].

FUNDING. – The research was supported in part by the Simons Foundation Collaboration grant no. 691493.

REFERENCES

[1] M. F. ATIYAH – D. O. TALL, Group representations, λ-rings and the J-homomorphism. *Topology* **8** (1969), 253–297. Zbl 0159.53301 MR 0244387

[2] G. BARAT – V. BERTHÉ – P. LIARDET – J. THUSWALDNER, Dynamical directions in numeration. *Ann. Inst. Fourier (Grenoble)* **56** (2006), no. 7, 1987–2092. Zbl 1138.37005 MR 2290774

[3] J. BORGER, Lambda-rings and the field with one element. 2009, arXiv:0906.3146v1.

[4] J.-B. BOST – A. CONNES, Hecke algebras, type III factors and phase transitions with spontaneous symmetry breaking in number theory. *Selecta Math. (N.S.)* **1** (1995), no. 3, 411–457. Zbl 0842.46040 MR 1366621

[5] Complex-base system. https://en.wikipedia.org/wiki/Complex-base_system visited on 30 July 2024.

[6] A. Connes, Trace formula in noncommutative geometry and the zeros of the Riemann zeta function. *Selecta Math. (N.S.)* **5** (1999), no. 1, 29–106. Zbl 0945.11015 MR 1694895

[7] A. Connes – C. Consani, From monoids to hyperstructures: in search of an absolute arithmetic. In *Casimir force, Casimir operators and the Riemann hypothesis*, pp. 147–198, Walter de Gruyter, Berlin, 2010. Zbl 1234.14002 MR 2777715

[8] A. Connes – C. Consani, Schemes over $\mathbb{F}_1$ and zeta functions. *Compos. Math.* **146** (2010), no. 6, 1383–1415. Zbl 1201.14001 MR 2735370

[9] A. Connes – C. Consani, On the notion of geometry over $\mathbb{F}_1$. *J. Algebraic Geom.* **20** (2011), no. 3, 525–557. Zbl 1227.14006 MR 2786665

[10] A. Connes – C. Consani, Absolute algebra and Segal's Γ-rings: au dessous de $\overline{\mathrm{Spec}(\mathbb{Z})}$. *J. Number Theory* **162** (2016), 518–551. Zbl 1409.14046 MR 3448278

[11] A. Connes – C. Consani, Geometry of the arithmetic site. *Adv. Math.* **291** (2016), 274–329. Zbl 1368.14038 MR 3459019

[12] A. Connes – C. Consani, Geometry of the scaling site. *Selecta Math. (N.S.)* **23** (2017), no. 3, 1803–1850. Zbl 1406.11118 MR 3663595

[13] A. Connes – C. Consani, On absolute algebraic geometry the affine case. *Adv. Math.* **390** (2021), article no. 107909. Zbl 1478.14047 MR 4291468

[14] A. Connes – C. Consani, Riemann-Roch for $\overline{\mathrm{Spec}\,\mathbb{Z}}$. *Bull. Sci. Math.* **187** (2023), article no. 103293. Zbl 1529.14003 MR 4609943

[15] A. Connes – C. Consani, Riemann-Roch for the ring $\mathbb{Z}$. *C. R. Math. Acad. Sci. Paris* **362** (2024), 229–235. Zbl 07842305 MR 4745331

[16] B. I. Dundas – T. G. Goodwillie – R. McCarthy, *The local structure of algebraic K-theory*. Algebr. Appl. 18, Springer, London, 2013. Zbl 1272.55002 MR 3013261

[17] W. J. Gilbert, Radix representations of quadratic fields. *J. Math. Anal. Appl.* **83** (1981), no. 1, 264–274. Zbl 0472.10011 MR 0632342

[18] J. S. Golan, *Semirings and their applications*. Kluwer Academic Publishers, Dordrecht, 1999. Zbl 0947.16034 MR 1746739

[19] I. Kátai – B. Kovács, Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen. *Acta Sci. Math. (Szeged)* **42** (1980), no. 1-2, 99–107. Zbl 0386.10007 MR 0576942

[20] I. Kátai – B. Kovács, Canonical number systems in imaginary quadratic fields. *Acta Math. Acad. Sci. Hungar.* **37** (1981), no. 1-3, 159–164. Zbl 0477.10012 MR 0616887

[21] D. E. Knuth, *The art of computer programming. Vol. 2. Seminumerical algorithms*. 3rd edn., Addison-Wesley, Reading, MA, 1998. Zbl 0895.68054 MR 3077153

[22] Y. Manin, Lectures on zeta functions and motives (according to Deninger and Kurokawa). *Astérisque* **228** (1995), 121–163. MR 1330931

[23] Y. I. MANIN, Cyclotomy and analytic geometry over $\mathbb{F}_1$. In *Quanta of maths*, pp. 385–408, Clay Math. Proc. 11, American Mathematical Society, Providence, RI, 2010. Zbl 1231.14018 MR 2732059

[24] R. MEYER, On a representation of the idele class group related to primes and zeros of L-functions. *Duke Math. J.* **127** (2005), no. 3, 519–595. Zbl 1079.11044 MR 2132868

[25] D. QUILLEN, On the cohomology and K-theory of the general linear groups over a finite field. *Ann. of Math. (2)* **96** (1972), 552–586. Zbl 0249.18022 MR 0315016

[26] A. M. ROBERT, *A course in p-adic analysis*. Grad. Texts in Math. 198, Springer, New York, 2000. Zbl 0947.11035 MR 1760253

[27] C. SOULÉ, Les variétés sur le corps à un élément. *Mosc. Math. J.* **4** (2004), no. 1, 217–244. Zbl 1103.14003 MR 2074990

[28] R. STEINBERG, A geometric approach to the representations of the full linear group over a Galois field. *Trans. Amer. Math. Soc.* **71** (1951), 274–282. Zbl 0045.30201 MR 0043784

[29] J. TITS, Sur les analogues algébriques des groupes semi-simples complexes. In *Colloque d'algèbre supérieure, tenu à Bruxelles du 19 au 22 décembre 1956*, pp. 261–289, Centre Belge Rech. Math., Établissements Ceuterick, Louvain, 1957. Zbl 0084.15902 MR 0108765

[30] Triadic numbers. http://solbakkn.com/math/triadic-nums.htm visited on 30 July 2024.

[31] A. WEIL, De la métaphysique aux mathématiques. In *Oeuvres scientifiques/collected papers. II. 1951–1964*, pp. xxii+561, Springer Collect. Works Math., Springer, Heidelberg, 2014. Zbl 1317.01045 MR 3309921

[32] A. WEIL, Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques. In *Oeuvres scientifiques/Collected papers. I. 1926–1951*, pp. xxii+578, Springer Collect. Works Math., Springer, Heidelberg, 2014. Zbl 1317.01044 MR 3328832

Received 23 July 2023

Alain Connes
Collège de France
3 rue d'Ulm, 75005 Paris
Institut des Hautes Études Scientifiques (IHES)
35 route de Chartres, 91440 Bures-sur-Yvette, France
alain@connes.org

Caterina Consani
Department of Mathematics, The Johns Hopkins University
3400 N Charles Street, Baltimore, MD 21218, USA
cconsan1@jhu.edu