Sur la métaphysique de $\mathbb{F}_1$

Alain Connes, Caterina Consani*

À la mémoire de Yuri Ivanovich Manin.

Résumé : Dans le présent article, dédié à Yuri Manin, nous interrogeons la notion générale d'anneaux de $\mathbb{S}[\mu_{n,+}]$–polynômes et nous relions ce concept à la notion connue de systèmes de numération. Le théorème de Riemann-Roch pour l'anneau $\mathbb{Z}$ des entiers que nous avons obtenu récemment utilise le fait de comprendre $\mathbb{Z}$ comme un anneau de polynômes $\mathbb{S}[X]$ en une variable sur la base absolue $\mathbb{S}$, où $1+1 = X + X^2$. La base absolue $\mathbb{S}$ (la version catégorique du spectre de la sphère) s'avère ainsi être un sérieux candidat pour l'incarnation du mystérieux $\mathbb{F}_1$.

1 Introduction

> Les mathématiciens du XVI^{e} 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, [33])

Yuri Manin, à la mémoire de qui cet article est dédié, a reconnu le premier dans [23] l'importance de développer une théorie des "coefficients absolus" en géométrie arithmétique, indépendamment des idées précédentes de R. Steinberg [30] et J. Tits [31] dans le contexte des groupes de Chevalley. En arithmétique, pour les corps de nombres, le but est de fournir la contrepartie géométrique de la construction qu'A. Weil a utilisée dans sa preuve de l'hypothèse de Riemann pour les corps de fonctions. La recherche d'une analogie proche entre les corps de nombres et les corps de fonctions des courbes en caractéristique positive a amené Manin à postuler l'existence du point absolu "Spec $\mathbb{F}_1$," sur lequel on pouvait appliquer la stratégie de Weil à l'étude de la fonction zeta de Riemann. Pour le schéma algébrique Spec $\mathbb{Z}$, on pourrait alors utiliser le spectre du produit tensoriel "$\mathbb{Z} \otimes_{\mathbb{F}_1} \mathbb{Z}$" comme un substitut du produit d'une courbe par elle-même sur (le spectre d') un corps fini.

Manin plaidait toujours pour la fécondité des interactions entre les différentes approches d'un problème mathématique. Dans les Sections 2 et 3, on discutera de deux telles occurrences inattendues, en fait deux piliers de notre travail commun lors des 15 dernières années. La section 2 traite de la courbe hypothétique [1] $\mathbf{C}$ que nous proposons comme entité géométrique absolue. La section 3 concerne plutôt les coefficients absolus. Le but de cet article est de sponsoriser $\mathbb{S}$ le spectre de la sphère comme forme combinatoire de base, la forme combinatoire la plus basique du spectre de la sphère, et une $\mathbb{S}$-algèbre, comme candidat le plus naturel pour les coefficients absolus (alias $\mathbb{F}_1$). Nous prétendons que cette algèbre est le "corps" absolu des constantes sur lequel $\mathbb{Z}$ devient un anneau de polynômes d'une variable. Ce point de vue est

*Partiellement financée par la subvention n^{o} 691493 de la Fondation Simons.
Traduction de l'article https://arxiv.org/pdf/2307.06748.pdf, Denise Vella-Chemla, juillet 2023.

1. On utilisera dans la suite de ce document la lettre $\mathbf{C}$ pour la désigner.

soutenu par le théorème de Riemann-Roch pour l'anneau $\mathbb{Z}$ récemment démontré dans [14], dont la formule montre que le genre de $\overline{\mathrm{Spec}\,\mathbb{Z}}$ est zéro. Dans un précédent résultat sur le même sujet [13], les entiers étaient considérés comme des polynômes sur $\mathbb{S}[\pm 1]$ avec générateur $X = 3$. Ce fait est basé sur un système de numération équilibré ternaire [2] qui fournit une représentation signée équilibrée des entiers comme sommes finies de puissances de la "variable" $X = 3$ avec coefficients dans l'ensemble $\{-1, 0, 1\}$ sous-tendant le monoïde pointé multiplicatif $\mu_{2,+}$ des racines quadratiques de l'unité. La nouvelle version du théorème de Riemann-Roch pour l'anneau $\mathbb{Z}$ dans [14] simplifie une version précédente [13] et elle réconcilie également la formule (et notre compréhension de ce sujet) avec le point de vue de la théorie des nombres classique. En effet, dans l'analogie entre les corps de nombres et les courbes sur les corps finis, le corps $\mathbb{Q}$ est de genre zéro [32] et il est désigné comme le seul corps contenu dans n'importe quel corps de nombres. Le fait de voir $\mathbb{Z}$ comme un anneau de polynômes sur la base absolue $\mathbb{S}$ sélectionne le générateur $X = -2$. Le fait clé est que tout entier peut être exprimé de manière unique comme somme de puissances de -2 [20].

Les cas particuliers de générateurs ci-dessus X pour les anneaux sur les $\mathbb{S}$-algèbres sphériques finies justifient une étude systématique et étendue des anneaux de $\mathbb{S}[\mu_{n,+}]$–polynômes. Dans la section 5, on introduit la notion générale d'anneaux de $\mathbb{S}[\mu_{n,+}]$–polynômes en une et plusieurs variables. Soit $n > 0$ un entier, μ_n le groupe multiplicatif des racines n-ièmes de l'unité de 1 et $\mathbb{S}[\mu_{n,+}]$ la $\mathbb{S}$-algèbre sphérique du monoïde (pointé) $\mu_{n,+} = \mu_n \cup \{0\}$. On rappelle que les morphismes de $\mathbb{S}$-algèbres $\mathbb{S}[\mu_{n,+}] \to HR$ (R étant un anneau) correspondent bijectivement aux homomorphismes de groupes $\iota : \mu_n \to R^\times$ [11]. Soit $\mathcal{P}(\mu_n)$ le sous-ensemble de l'ensemble $\left(\mu_n \cup \{0\}\right)^{\mathbb{N}}$ des séquences avec seulement un nombre fini de termes non nuls. Par définition, un élément $X \in R$ est un $\mathbb{S}[\mu_{n,+}]$-générateur si et seulement si l'application d'évaluation $\sigma : \mathcal{P}(\mu_n) \to R$, $\sigma((\alpha_j)) = \sum_j \iota(\alpha_j)\, X^j$ est bijective. La proposition 5.8 montre que la paire (R, X) d'un anneau de $\mathbb{S}[\mu_{n,+}]$–polynômes en une variable est spécifiée de manière unique, à isomorphisme près, par l'application $h : \mu_n \to \mathcal{P}(\mu_n)$, qui, en retour, est uniquement définie par l'égalité $\sigma(h(\xi)) = \iota(\xi) + 1$. Dans la section 6, on donne plusieurs exemples d'anneaux de $\mathbb{S}[\mu_{n,+}]$–polynômes basés sur certains systèmes de numération connus. Nous renvoyons à [2] pour un survol des systèmes de numération et pour des références fournies, mais nous ne prétendons pas à l'exhaustivité. Conceptuellement, les exemples d'anneaux de $\mathbb{S}[\mu_{n,+}]$-polynômes discutés dans cet article fournissent un pont explicite entre les mondes p-adique et complexe. Au niveau géométrique, les anneaux de polynômes sont naturellement reliés à la droite projective $\mathbb{P}^1$, et l'évaluation en les points 0 et ∞ de $\mathbb{P}^1$ amène, après complétion, le raffinement suivant (la ligne du dessous) d'un diagramme classique (la ligne du dessus). Dans la ligne du dessus, K est le corps des fractions de l'anneau de Witt p-typique de la fermeture algébrique de $\mathbb{F}_q$ ($q = p^\ell$) et $\overline{K}$ est sa clôture algébrique.

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

Dans la ligne du dessous, X est un $\mathbb{S}[\mu_{n,+}]$-générateur de l'anneau R où $n + 1 = q$. $R[X^{-1}]$ est l'anneau des polynômes de Laurent ; l'application vers $\mathbb{C}$ est l'inclusion de $R[X^{-1}]$ dans $\mathbb{C}$ par spécialisation de X, obtenue en résolvant les équations $\sigma(h(\xi)) = \iota(\xi) + 1$, $\xi \in \mu_n$, et en utilisant le plongement canonique $\mu_{n,+} \subset \mathbb{C}$. L'application de $R[X^{-1}]$ vers l'extension finie $W(\mathbb{F}_q)[\eta]$ est obtenue à partir de l'inclusion canonique de R dans la limite projective $\varprojlim R_n$ (voir la proposition 5.8).

La théorie générale des anneaux de $\mathbb{S}[\mu_{n,+}]$-polynômes, avec le rôle de la base absolue $\mathbb{S}$ dans la formulation du théorème de Riemann-Roch [14], suggère le raffinement suivant de la définition du site arithmétique.

2. Une occurrence plus ancienne d'un tel système de numération peut être trouvée dans le livre de 1544 "Arithmetica integra" de Michael Stifel.

Originellement, cet espace était défini par la paire du topos arithmétique $\widehat{\mathbb{N}^\times}$ et de la structure de faisceau donnée par l'action du Frobenius de $\mathbb{N}^\times$ sur le semi-anneau tropical $\mathbb{Z}_{\max}$ [9]. Le rôle du corps de constantes est ici joué par le semi-corps booléen $\mathbb{B}$. Le développement de cet article suggère de façon évidente de remplacer la structure de faisceau $\mathbb{Z}_{\max}$ par le faisceau des $\mathbb{S}$-algèbres obtenues à partir de l'action du Frobenius $X \mapsto X^n$ de $\mathbb{N}^\times$ sur l'algèbre sphérique $\mathbb{S}[X]$. Cette nouvelle version du site arithmétique fournit simultanément une base naturelle à la fois au niveau des coefficients et au niveau géométrique. Le topos $\widehat{\mathbb{N}^\times}$ est l'incarnation géométrique des λ-opérations dans la théorie des λ-anneaux [3] dans le contexte de la géométrie sur $\mathbb{F}_1$. Nous espérons que par une compréhension adéquate de la "fermeture algébrique" $\overline{\mathbb{F}}_1$ des coefficients absolus, on pourrait relier l'espace des points du site $\mathbb{S}$-arithmétique sur $\overline{\mathbb{F}}_1$ aux (points de la) courbe $\mathbf{C}$ dont la structure est rappelée dans la section 2.
Finalement, ces résultats amènent également à la question ouverte et intéressante de la classification des anneaux de $\mathbb{S}[\mu_{n,+}]$–polynômes en plusieurs variables qui poursuit l'assertion intuitive de Yuri Manin [23] :

> *La question centrale à laquelle nous répondons peut être énoncée de façon provocante comme suit : si les nombres sont semblables à des polynômes en une variable sur un corps fini, quel est l'analogue des polynômes à plusieurs variables ? Ou, en termes plus géométriques, existe-t-il une catégorie dans laquelle on peut définir "des puissances absolues de Descartes"* $\operatorname{Spec}\mathbb{Z}\times\cdots\times\operatorname{Spec}\mathbb{Z}$ *?*

2 Incarnation adélique et topossique de C

Une première connexion entre le point de vue de Manin sur $\mathbb{F}_1$ et un sujet semblant non relié à celui-ci a lieu comme sous-produit des relations entre la perspective de C. Soulé sur les variétés sur $\mathbb{F}_1$ (nommé "réalisme critique" dans [24]) – motivé par [23] (*cf.* §1.5) – et le travail du premier auteur [5] sur la formule de trace en géométrie non-commutative et les zéros de la fonction zeta de Riemann. Dans [29], Soulé a introduit la fonction de zeta suivante d'une variété X sur $\mathbb{F}_1$

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

en utilisant la fonction de comptage *polynomiale* $N(x) \in \mathbb{Z}[x]$ associée à X et la série exponentielle de Hasse-Weil

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

Tous les exemples de variétés considérées dans *op.cit.* sont rationnelles. Par conséquent, l'existence d'une courbe sous-jacente $\mathbf{C}$ reliée, d'une façon similaire, à la fonction zeta de Riemann est subordonnée au fait de trouver une fonction $N(q)$ (hautement non polynomiale !) qui produise, à travers l'utilisation de (2.1), la fonction de Riemann complète $\zeta_{\mathbb{Q}}(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$. Ceci est un problème non trivial puisque, classiquement, $N(1)$ dans la formule ci-dessus représente la caractéristique d'Euler de l'espace géométrique. Donc on peut être amené à s'attendre [3] à ce que puisque pour la fonction zeta de Riemann, on devrait avoir $N(1) = -\infty$, l'utilisation de (2.1) devrait être exclue, et avec elle également l'attente que $N(q) \geq 0$ pour $q \in (1,\infty)$. Il y a, en fait, un moyen naturel de passer outre ce problème en appliquant la dérivée logarithmique aux deux côtés de (2.1) et en observant alors que le côté droit détermine les sommes de Riemann d'une intégrale [7, 8]. De cette manière, au lieu de (2.1), on considère l'équation :

3. Le nombre de zéros de $\zeta_{\mathbb{Q}}$ est infini, et il en est donc de même de la (mystérieuse) cohomologie $H^1(\mathbf{C})$.

$\frac{\partial_s \zeta_N(s)}{\zeta_N(s)} = -\int_1^\infty N(u)\, u^{-s} d^*u$, où $d^*u := du/u$. Cette formule intégrale produit la formule suivante pour le but recherché d'obtenir la fonction de comptage $N(q)$ associée à **C** :

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

L'équation ci-dessus admet une solution qui a du sens exprimable en fonction de la *distribution*

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

où $\kappa(u)$ est la distribution qui apparaît dans la formule explicite de Riemann-Weil

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

On montre que la distribution $N(u)$ est positive sur $(1, \infty)$, et quand on l'écrit en fonction des zéros non triviaux $\rho \in Z$ de la fonction zeta de Riemann, elle est donnée, en parfaite analogie avec sa contrepartie vérifiée dans le cas des corps de fonctions par

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

où la dérivée est prise au sens des distributions. La valeur en $u = 1$ du terme $\omega(u) = \sum_{\rho \in Z} \text{ordre}(\rho)\frac{u^{\rho+1}}{\rho+1}$ est donnée par $\frac{1}{2} + \frac{\gamma}{2} + \frac{\log 4\pi}{2} - \frac{\zeta'(-1)}{\zeta(-1)}$.

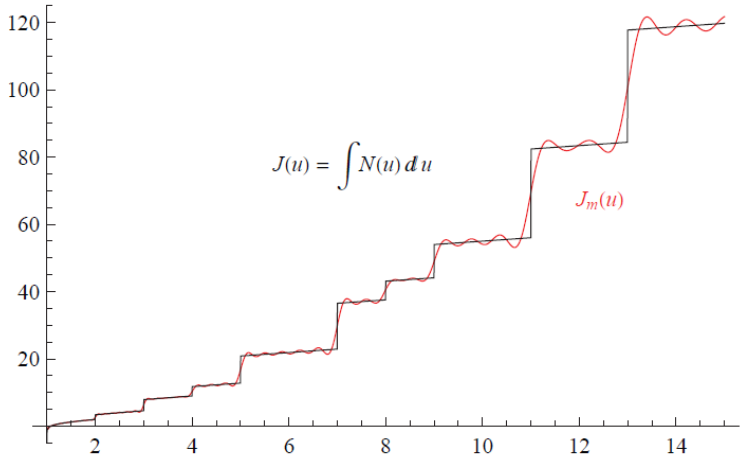


FIG. 1 : Graphe de la primitive $J(u)$ de la distribution de comptage $N(u)$. On a $J(u) \to -\infty$ quand $u \to 1$. Le graphique ondulant est l'approximation de $J(u)$ obtenue en utilisant l'ensemble symétrique Z_m des $2m$ premiers zéros pour calculer la somme $J_m(u) = \frac{u^2}{2} - \sum_{Z_m} \text{ordre}(\rho)\frac{u^{\rho+1}}{\rho+1} + u$.

La tension entre la positivité de la distribution $N(q)$ pour $q > 1$, et l'attente que sa valeur $N(1)$ doive être $N(1) = -\infty$ est résolue en implémentant la théorie des distributions. En effet, même si $N(u)$ est *finie* comme une distribution, quand on la regarde comme une fonction, sa valeur en $q = 1$ est formellement donnée par

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

et ainsi, elle est égale à $-\infty$, et ce fait reflète, quand $\epsilon \to 0$, la densité des zéros de la fonction zeta.

On souligne que le rôle des formules analytiques explicites de Riemann-Weil dans le processus de dépasser la difficulté initiale par une solution définie par une distribution positive $N(q)$, relie directement le point de vue original (en géométrie classique) avec la formule de trace dans [5], fournissant ainsi une première description géométrique pour les points de $\mathbf{C}$ en fonction du double quotient

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

de l'espace des classes d'adèles des rationnels par le sous-groupe compact maximal $\hat{\mathbb{Z}}^{\times}$ du groupe des classes d'idèles. L'ingrédient clé principal dans cette construction est la fonction de mise à l'échelle de $\mathbb{R}_+^{\times}$ qui fournit [4] la distribution de comptage ci-dessus $N(u)$, $u \in [1, \infty)$, qui détermine, en retour, la fonction zeta de Riemann complète via une procédure de limitation lorsque $q \to 1$, opérée sur la formule de the Hasse-Weil. La géométrie non-commutative joue un rôle crucial dans ce développement principalement en implémentant l'espace non-commutatif $X_{\mathbb{Q}}$ qui survient naturellement comme le dual du BC-système [4].

Pour atteindre une compréhension géométrique plus classique de l'espace des classes d'adèles $X_{\mathbb{Q}}$ avec son action de mise à l'échelle, en analogie avec l'action de l'automorphisme de Frobenius sur les points de la courbe sur la fermeture algébrique d'un corps de base, il faut pousser plus loin la recherche d'interactions inaattendues... Cette compréhension géométrique vient en fait de l'interaction entre trois théories a priori non liées :

1. la géométrie non-commutative,
2. les topoi de Grothendieck
3. la géométrie tropicale.

Le point de départ naturel est le topos $\widehat{\mathbb{N}^{\times}}$, défini dans [9] comme le topos de Grothendieck de préfaisceaux dual du monoïde multiplicatif $\mathbb{N}^{\times}$ des entiers positifs non nuls. Cet espace est en fait l'incarnation géométrique des $\mathbb{N}^{\times}$-actions sur les ensembles. Ces actions arrivent souvent en instances globales des endomorphismes de Frobenius : pour les λ-anneaux, elles étaient défendues dans [3] dans le contexte des variétés sur $\mathbb{F}_1$ (dans l'interprétation de Manin, elles sont dites "futuristes", [24]). Les λ-anneaux spéciaux R ([1] Proposition 5.2), appartiennent naturellement au topos $\widehat{\mathbb{N}^{\times}}$ puisque les opérations de Adams ψ_n changent R en un faisceau d'anneaux sur le topos $\widehat{\mathbb{N}^{\times}}$.
À un niveau algébrique très basique, un exemple fondamental d'action de Frobenius de $\mathbb{N}^{\times}$ est fourni par la théorie des semi-anneaux (*i.e.* quand on met de côté l'existence d'inverses additifs dans les anneaux). Pour un semi-anneau [5] R de "caractéristique un" (c'est-à-dire idempotent : *i.e.* tel que $1 + 1 = 1$), l'application $x \mapsto x^n = \mathrm{Fr}_n(x)$ est un endomorphisme injectif [17], pour tout entier $n \in \mathbb{N}^{\times}$. Ainsi, on obtient une action canonique du semi-groupe $\mathbb{N}^{\times}$ sur tout tel R. Pour cette raison, il est naturel de travailler avec le topos

4. Pour supprimer le terme logarithmique divergent de la formule de trace [5], on a besoin de supprimer de $X_{\mathbb{Q}}$ l'orbite de l'adèle unité 1, *i.e.* ou de manière équivalente de soustraire la représentation régulière de $\mathbb{R}_+^{\times}$ comme dans [25].

5. Un semi-corps est un semi-anneau dont les éléments non nuls forment un groupe pour la multiplication.

$\widehat{\mathbb{N}^\times}$ muni d'une action de $\mathbb{N}^\times$. De plus, on sait également qu'il y a un unique semi-corps [6] $\mathbb{Z}_{\max}$ dont le groupe multiplicatif est cyclique infini et il est de caractéristique un. Ces faits étant donnés, il est naturel d'introduire l'espace suivant

Définition 2.7 ([9])**.** Le site arithmétique $\mathscr{A} = (\widehat{\mathbb{N}^\times}, \mathcal{O})$ est le topos $\widehat{\mathbb{N}^\times}$ muni du *faisceau structurel* $\mathcal{O} := \mathbb{Z}_{\max}$, vu comme un semi-anneau dans le topos *et* avec l'action de $\mathbb{N}^\times$ par les endomorphismes de Frobenius.

Le semi-corps $\mathbb{Z}_{\max}$ et son compagnon $\mathbb{R}_+^{\max}$ (dont le groupe multiplicatif est $\mathbb{R}_+^*$), sont des objets familiers en géométrie tropicale où le maximum remplace l'addition usuelle.
En implémentant une généralisation évidente dans les topos semi-annelés de la compréhension d'un point de géométrie algébrique, on obtient le résultat suivant qui détermine un pont reliant la géométrie non-commutative à la théorie des topos (de Grothendieck)

Théorème 2.8 ([9])**.** *L'ensemble des points du site arithmétique $\mathscr{A}$ sur $\mathbb{R}_+^{\max}$ est canoniquement isomorphe à $X_{\mathbb{Q}} = \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}} / \hat{\mathbb{Z}}^\times$. L'action des automorphismes de Frobenius Fr_λ de $\mathbb{R}_+^{\max}$ sur ces points correspond à l'action du groupe des classes d'idèles sur $X_{\mathbb{Q}} = \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}} / \hat{\mathbb{Z}}^\times$.*

Ce théorème amène une lumière nouvelle sur une intuition géométrique de la courbe **C**, en particulier, il montre l'espace non-commutatif $X_{\mathbb{Q}}$ comme l'ensemble des points de **C** sur le semi-corps $\mathbb{R}_+^{\max}$, avec l'action de mise à l'échelle comprise comme l'action du groupe de Galois $\mathrm{Aut}_{\mathbb{B}}(\mathbb{R}_+^{\max})$ de $\mathbb{R}_+^{\max}$ sur le semi-corps booléen [7] $\mathbb{B}$. Cela suggère également que $\mathbb{R}_+^{\max}$ devrait intervenir dans la construction de la "fermeture algébrique" de $\mathbb{F}_1$, et que le cœur combinatoire sous-tendant **C** est dénombrable puisqu'à la fois $\mathbb{N}^\times$ et $\mathbb{Z}_{\max}$ le sont. On trouve assez remarquable qu'alors que le site arithmétique est un objet combinatoire de nature dénombrable, il vienne néanmoins muni d'un semi-groupe à un paramètre de "correspondances" qui peut être vu comme des congruences sur le carré de ce site [9].

L'ensemble dénombrable de places de $\mathbb{Q}$ (les points de la compactification d'Arakelov $\overline{\mathrm{Spec}\ \mathbb{Z}}$), est l'analogue visible (classiquement) de l'ensemble des orbites de l'automorphisme de Frobenius dans le cas des corps de fonctions. On obtient une meilleure vision des points de **C** en considérant les orbites périodiques C_p (paramétrées par les nombres premiers p) lorsqu'elles ont lieu parmi les points du site arithmétique $\mathscr{A}$ sur $\mathbb{R}_+^{\max}$. On montre que les points de C_p forment un cercle dont les éléments sont les sous-groupes de rang un du groupe multiplicatif de $\mathbb{R}_+^{\max}$ de la forme

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

Ce sous-groupe est inchangé si on remplace μ par μ^p, et l'action de Frobenius de $\mathrm{Aut}_{\mathbb{B}}(\mathbb{R}_+^{\max}) = \mathbb{R}_+^*$, $\mu \mapsto \mu^\lambda$, induit l'action transitive du groupe quotient $\mathbb{R}_+^*/p^{\mathbb{Z}}$. La longueur de cette orbite périodique est $\log p$, et leur collection complète joue un rôle clé dans l'interprétation des formules explicites de Riemann-Weil comme une formule de trace dans [5]. De plus, chaque C_p hérite, comme un sous-espace du site de mise à l'échelle (obtenu à partir du site arithmétique par extension des scalaires), d'une structure de faisceau (de caractéristique un) qui transforme toute orbite périodique en l'analogue d'une courbe elliptique classique [10]. De cette manière, on peut encore appliquer plusieurs outils clés de la géométrie algébrique, comme les fonctions rationnelles, les diviseurs, etc. Une nouvelle caractéristique surprenante de cette géométrie

6. Comme monoïde multiplicatif, $\mathbb{Z}_{\max}$ est obtenu en adjoignant l'élément zéro $-\infty$ au groupe cyclique infini $\mathbb{Z}$ alors que l'opération qui joue le rôle d'addition dans le semi-corps est $(x, y) \mapsto \max(x, y)$.

7. $\mathbb{B} := \{0, 1\}$ avec $1 + 1 = 1$.

d'une orbite périodique est que le degré d'un diviseur est un nombre réel. Pour tout diviseur D dans C_p, il y a un problème de Riemann-Roch correspondant avec pour espace des solutions $H^0(D)$. La dimension continue [8] $\mathrm{Dim}_{\mathbb{R}}(H^0(D))$ de ce $\mathbb{R}_+^{\max}$-module est définie par la limite

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

où $H^0(D)^{p^n}$ est une filtration définie naturellement et où $\dim_{\mathrm{top}}(\mathcal{E})$ dénote la dimension topologique d'un $\mathbb{R}_+^{\max}$-module $\mathcal{E}$. La formule de Riemann-Roch suivante est vérifiée

Théorème 2.11 ([10])**.** (*i*) *Soit* $D \in \mathrm{Div}(C_p)$ *un diviseur avec* $\deg(D) \geq 0$. *Alors la limite dans* (2.10) *converge et on a*

$$Dim_{\mathbb{R}}(H^0(D)) = \deg(D).$$

(*ii*) *La formule de Riemann-Roch suivante est vérifiée*

$$Dim_{\mathbb{R}}(H^0(D)) - Dim_{\mathbb{R}}(H^0(-D)) = \deg(D) \qquad \forall D \in \mathrm{Div}(C_p).$$

Au vu de ces résultats et du rôle clé joué par le semi-corps booléen $\mathbb{B}$ parmi les structures algébriques idempotentes [9], on peut (à tort) être amené à penser à $\mathbb{B}$ comme à l'incarnation naturelle de $\mathbb{F}_1$. Pourtant, cela ne peut être le cas pour la raison évidente que [10] :

L'anneau $\mathbb{Z}$ *n'est pas une algèbre sur* $\mathbb{B}$.

3 Coefficients absolus, spectres et $\mathbb{S}$.

Le fait indéniable ci-dessus nous a amenés, une fois encore, à comparer les idées de Manin sur $\mathbb{F}_1$ avec un autre sujet a priori non relié : c'est le monde des spectres de la théorie de l'homotopie. Les spectres topologiques généralisent grandement les théories de la cohomologie ; des invariants très importants en topologie algébrique, comme la cohomologie ordinaire et la K-théorie, peuvent être reformulés en fonction des spectres, ce qui fournit un traitement unifié pour les "coefficients généralisés". Une découverte fondamentale dans le contexte topologique est que les "spectres d'anneaux" généralisent les anneaux, et en particulier, le "spectre de la sphère" $\underline{\mathbb{S}}$ devient plus basique que l'anneau $\mathbb{Z}$, parce que ce dernier peut être vu comme une algèbre sur le premier. Cette théorie des "nouveaux anneaux courageux" s'est avérée être le cadre correct pour l'homologie cyclique ; en particulier, la théorie des Γ-espaces est connue pour fournir un modèle fonctionnel de spectres connectifs [15]. On travaille habituellement au niveau homotopique, et donc il est crucial de traiter les complexes de Kan pour obtenir une structure modélisante correcte. Pourtant, pour tirer un complet avantage de cette théorie pour le développement des idées de Manin sur $\mathbb{F}_1$ en théorie des nombres, nous pensons que les Γ-espaces devraient être vus dans leur forme la plus basique, notamment comme des objets simpliciaux dans la catégorie des Γ-ensembles, de telle façon que la théorie de l'homotopie puisse jouer le rôle de l'algèbre homologique correspondant à l'"algèbre absolue" sur le Γ-anneau de base $\mathbb{S}$ [11]. Ce Γ-anneau est le point de départ catégorique dans la construction du spectre de la sphère $\underline{\mathbb{S}}$, avec le foncteur naturel des Γ-espaces vers les spectres, et c'est exactement cette nature combinatoire de base qui le rend plus proche de ce que l'on recherche pour $\mathbb{F}_1$. La catégorie $\Gamma\mathfrak{Sets}_*$ des Γ-ensembles pointés (par exemple les $\mathbb{S}$-modules $\mathfrak{Mod}(\mathbb{S})$) peut être directement décrite comme suit. On

8. En analogie avec les dimensions continues de von Neumann de la théorie des facteurs de type II.
9. $\mathbb{B}$ est, en particulier, le seul semi-corps qui ne soit pas un corps *cf.* [17].
10. Les algèbres sur $\mathbb{B}$ sont de caractéristique un.

commence avec la petite catégorie Γ^{op} comme catégorie complète des ensembles finis pointés dont les objets sont les ensembles finis pointés [11] $k_+ := \{0, \dots, k\}$, pour $k \geq 0$. En particulier, 0_+ est à la fois initial et terminal dans Γ^{op}, faisant de Γ^{op} une *catégorie pointée*. Un Γ-ensemble est défini comme un foncteur (covariant) $\Gamma^{op} \longrightarrow \mathfrak{Sets}_*$ entre les catégories pointées et les morphismes dans cette catégorie sont des transformations naturelles. On dénote par $\mathbb{S} : \Gamma^{op} \longrightarrow \mathfrak{Sets}_*$ le foncteur d'inclusion. Le hom foncteur interne est défini par

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

Cette formule définit de manière unique le smash produit des Γ-ensembles en appliquant l'adjonction

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

La construction de base des $\mathbb{S}$-modules associe à un monoïde abélien A un élément zéro, le foncteur d'Eilenberg-MacLane $M = HA$

$$HA(k_+) = A^k, \qquad Hf : HA(k_+) \to HA(n_+),$$

$$Hf(m)(j) := \sum_{f(\ell)=j} m_\ell,$$

où $m = (m_1, \dots, m_k) \in HA(k_+)$, et l'élément nul de A donne un sens à la somme vide. Une $\mathbb{S}$-algèbre $\mathcal{A}$ est un $\mathbb{S}$-module $\mathcal{A} : \Gamma^{op} \longrightarrow \mathfrak{Sets}_*$ muni d'une multiplication associative $\mu : \mathcal{A} \wedge \mathcal{A} \to \mathcal{A}$ et d'une unité $1 : \mathbb{S} \to \mathcal{A}$.
Un semi-anneau ordinaire R donne naissance à la $\mathbb{S}$-algèbre HR, et le plongement correspondant des catégories est pleinement fidèle de telle façon qu'aucune information n'est perdue. Par contraste, la $\mathbb{S}$-algèbre de base $\mathbb{S}$ sous-tend maintenant HR pour tout semi-anneau R.

Étant donné un monoïde multiplicatif M avec un élément $0 \in M$ tel que $0 \times x = x \times 0 = 0$ pour tout $x \in M$, on définit la $\mathbb{S}$-algèbre sphérique $\mathbb{S}[M]$ qui associe à l'ensemble pointé X le smash produit $X \wedge M$, où le point de base de M est $0 \in M$. On identifie $\mathbb{S}[M][1_+] = 1_+ \wedge M$ à M en envoyant le point de base de $1_+ \wedge M$ sur $0 \in M$, et $a \wedge m$ où $a \in 1_+ \setminus \{*\}$ et $m \in M \setminus \{0\}$ sur m. Pour éviter toute confusion, on écrit $2_+ = \{*, a, b\}$. Outre le point de base, les éléments de $\mathbb{S}[M][2_+] = 2_+ \wedge M$ sont donnés par paires de la forme (a, m) ou (b, m) où $m \in M \setminus \{0\}$. On a trois applications naturellement pointées $f : 2_+ \to 1_+$, qui sont

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

Appelons $m \in M \setminus \{0\}$ et considérons la paire $z = (b, m) \in \mathbb{S}[M][2_+]$. On a $\phi_*(z) = * = 0$ et $\psi_*(z) = m$. De plus, on a $\rho_*(z) = m$. Cela signifie que pour l'addition partiellement définie dans $\mathbb{S}[M][1_+] = M$, on a $0 + m = m$ pour tout $m \in M$.

Ainsi, à la fois les anneaux ordinaires et les monoïdes s'adaptent pleinement fidèlement et naturellement [11] (proposition 3.5), dans la catégorie des $\mathbb{S}$-algèbres amenant un argument fort pour voir $\mathbb{S}$ comme la candidate naturelle pour $\mathbb{F}_1$. Néanmoins, on a besoin de tester cette idée de différentes manières. Par exemple, on voit *op.cit.* que le carré tensoriel de $H\mathbb{Z}$ sur $\mathbb{S}$ n'est pas isomorphe à $H\mathbb{Z}$, et ce résultat fournit plus de base à l'intuition originale de Manin dans [23]. On peut aussi se demander quelles avancées ce point de vue peut produire pour comprendre l'anneau $\mathbb{Z}$ et son spectre algébrique $\mathrm{Spec}\,\mathbb{Z}$. Nous allons maintenant nous tourner vers une discussion détaillée de ce sujet.

11. où 0 est le point de base.

Soit $\overline{\mathrm{Spec}\,\mathbb{Z}}$ la compactification d'Arakelov de $\mathrm{Spec}\,\mathbb{Z}$ obtenue en ajoutant la place archimédienne au symbole associé ∞. Alors, le nouveau point de vue décrit ci-dessus fournit une extension naturelle de la structure classique de faisceau de $\mathrm{Spec}\,\mathbb{Z}$ à la compactification d'Arakelov. Les points cruciaux concernant la quête de la courbe $\mathbf{C}$ sont au nombre de deux : premièrement, cette structure de faisceaux étendue $\mathcal{O}$ est encore un sous-faisceau du faisceau constant $\mathbb{Q}$; le second point intéressant est que les sections globales de $\mathcal{O}$ forment une extension d'algèbre finie de $\mathbb{S}$. Cette extension est identifiable à l'extension par les deux racines de l'unité à l'intérieur de $\mathbb{Q}$ que nous avons utilisée dans [6] dans le processus destiné à montrer que les groupes de Chevalley sont des variétés sur $\mathbb{F}_{1^2}$ au sens de Soulé [12]. La condition qui restreint les éléments de $H\mathbb{Q}$ à la place archimédienne est simple à formuler quand on voit le foncteur $H\mathbb{Q}$ comme assignant à un ensemble fini pointé F les diviseurs $\mathbb{Q}$-valués sur F. La restriction est alors établie en écrivant que la somme des valeurs absolues des nombres rationnels impliqués est ≤ 1. On vérifie que cette condition est stable par push-forwards et produits et que par conséquent, elle définit une sous-$\mathbb{S}$-algèbre de $H\mathbb{Q}$. Cette sous-$\mathbb{S}$-algèbre, définie en utilisant une norme s'applique également dans le contexte des adèles d'un corps global et nous permet de transposer l'approche due à A. Weil du théorème de Riemann-Roch pour les corps de fonctions au corps de nombres $\mathbb{Q}$ [13].
Un diviseur D sur $\overline{\mathrm{Spec}\,\mathbb{Z}}$ définit un *sous-ensemble* compact $K = \prod K_v \subset \mathbb{A}_{\mathbb{Q}}$ de l'anneau localement compact des adèles. Quand p est un nombre premier non archimédien, chaque $K_p \subset \mathbb{Q}_p$ est un sous-groupe additif, par contraste, le sous-ensemble compact $K_\infty \subset \mathbb{R}$ est juste un intervalle symétrique dont le manque de structure additive empêche d'utiliser la construction originale de Weil faisant intervenir l'application d'addition $\psi : \mathbb{Q} \times K \to \mathbb{A}_{\mathbb{Q}}$. D'un autre côté, on note aussi rapidement que ψ conserve sa signification dans le contexte des $\mathbb{S}$-modules, donnant naissance à un complexe court. En utilisant la correspondance de Dold-Kan dans le contexte des $\mathbb{S}$-algèbres, on introduit alors un Γ-espace $H(D)$ qui code l'information homologique du diviseur D et dépend seulment de la classe d'équivalence linéaire de D (*i.e.* la classe du diviseur est inchangée selon l'action multiplicative de $\mathbb{Q}^\times$ sur $\mathbb{A}_{\mathbb{Q}}$). Comme sous-produit, on obtient une formule de Riemann-Roch pour les diviseurs d'Arakelov sur $\overline{\mathrm{Spec}\,\mathbb{Z}}$ d'une nature entièrement nouvelle qui repose sur l'introduction de trois nouvelles notions clés : la dimension (entière), les cohomologies $(H^0(D), H^1(D))$ (attachées à un diviseur D), et la dualité de Serre. Plus précisément, la formule de Riemann-Roch rend égales la caractéristique d'Euler de valeur entière avec une modification simple de l'expression habituelle (*i.e.* le degré du diviseur plus log 2).

Théorème 3.1 ([13]). *Soit D un diviseur d'Arakelov sur $\overline{\mathrm{Spec}\,\mathbb{Z}}$. Alors*

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

Ici, $\lceil x \rceil$ dénote la fonction impaire sur $\mathbb{R}$ qui coïncide avec la fonction plafond sur les réels positifs et $\mathbf{1}_L$ est la fonction caractéristique d'un ensemble exceptionnel [13] de mesure de Lebesgue finie.

Dans (3.2), le logarithme népérien traditionnellement utilisé pour définir le degré d'un diviseur $D = \sum_j a_j\{p_j\} + a\{\infty\}$ en géométrie d'Arakelov, est remplacé par le logarithme en base 3. Cette modification est équivalente à une division par $\log 3$ i.e. $\deg_3(D) := \deg(D)/\log 3$, $\log_3 2 = \log 2/\log 3$.
Le nombre 3 apparaît de manière inattendue dans le calcul de la dimension de la cohomologie des $\mathbb{S}[\pm 1]$-modules en déterminant leur nombre minimal de générateurs linéaires. Pour $\dim_{\mathbb{S}[\pm 1]} H^0(D)$, on trouve que

12. Un autre argument convaincant en faveur des $\mathbb{S}$-algèbres est que la catégorie ad-hoc que nous avions introduite dans [7] pour simplifier la définition de Soulé des variétés sur $\mathbb{F}_1$, est naturellement (voir [12]) une sous-catégorie complète de la catégorie des $\mathbb{S}$-algèbres.

13. $L \subset \mathbb{R}$ est l'union, pour $k \geq 0$, des intervalles $\deg(D) \in \left(\log \frac{3^k}{2}, \log \frac{3^k+1}{2}\right)$.

la façon la plus économique d'écrire les éléments d'un intervalle symétrique $\mathbb{Z} \cap K_\infty$ implique d'écrire les entiers comme des polynômes de la forme

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

De façon similaire, dans le cas de $\dim_{\mathbb{S}[\pm 1]} H^1(D)$, on trouve que la meilleure façon d'approximer les éléments du cercle $\mathbb{R}/\mathbb{Z}$ est d'utiliser des polynômes de Laurent de la forme

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

L'élément clé ici est que l'addition [14] des polynômes $P(X) = \sum_{j\geq 0} \alpha_j \, X^j, \ \ \alpha_j \in \{-1, 0, 1\}$ avec coefficients dans $\mathbb{S}[\pm 1]$ est identique à l'addition de vecteurs de Witt (tronqués) pour le corps fini $\mathbb{F}_3$. On trouve que l'addition $P + Q$ de deux polynômes de degré $\leq n$ donnent un polynôme de degré $\leq n + 1$, et que la seule règle qui ne soit pas évidente que l'on doive imposer est la somme : $1 + 1 := X - 1$. Conceptuellement, le point fondamental est que l'image de l'ascenseur de Teichmüller pour $\mathbb{F}_3$ est à l'intérieur de $\mathbb{Z}$. En même temps, les vecteurs de Witt avec seulement un nombre fini de composants non nuls forment un sous-anneau de l'anneau de Witt, et son sous-anneau est $\mathbb{Z}$!

4 L'anneau des entiers comme anneau de polynômes

Il y a une autre manière de représenter les entiers comme polynômes d'une variable, et dans cette description, les "coefficients" appartiennent à la base absolue $\mathbb{S}$. Cette représentation est connue comme la représentation *négabinaire* des nombres

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

Le nombre $X = -2$ est remarquablement unique, rendant la représentation d'un entier n possible comme polynôme $P(X)$ à coefficients $\alpha_j \in \{0, 1\}$. En suivant les mêmes étapes qui nous ont amenés au théorème 3.1, mais en travaillant maintenant sur la base absolue $\mathbb{S}$, on obtient la version suivante nouvelle et simplifiée de la formule de Riemann-Roch qui fait intervenir maintenant le logarithme en base 2.

Théorème 4.2 ([14]). *Soit D un diviseur d'Arakelov sur $\overline{\operatorname{Spec} \mathbb{Z}}$. Alors*

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

où $\lceil x \rceil'$ est la fonction continue à droite qui coïncide avec plafond(x) pour $x > 0$ non entier et avec $-$plafond$(-x)$ pour $x < 0$ non entier.

Cette version du théorème de Riemann-Roch améliore le théorème 3.1 pour les raisons suivantes :

1. Le terme $\mathbf{1}_L$ faisant intervenir l'ensemble exceptionnel L dans l'assertion originale (voir [13]) a maintenant disparu de la formule.
2. La formule (4.3) est maintenant en parfaite analogie avec le théorème de Riemann-Roch pour les courbes de genre 0.

14. une fois que l'addition est définie, le produit suit en utilisant uniquement $X^j \, X^k = X^{j+k}$

3. Le diviseur canonique $K = -2\{2\}$ a un degré entier $\deg_2(K) = -2$.

Le théorème 4.2 correspond maintenant exactement avec le texte trilingue suggéré par A. Weil, qui soutient l'analogie entre la théorie transcendantale de Riemann des fonctions algébriques d'une variable dans la première colonne, la géométrie algébrique sur les courbes sur des corps finis dans la colonne du milieu et la théorie des corps de nombres algébriques dans la troisième colonne. En effet, selon 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. À l'usage, on se fait des bouts de dictionnaire, qui permettent de passer assez souvent d'une colonne à la colonne voisine.*

Dans la vision de Weil, il y a, dans la colonne du milieu (celle des corps de fonctions), une compréhension géométrique de la fonction zeta comme fonction génératrice du nombre de points de la courbe sur les extensions du corps des constantes. Dans la section 2, on traduit dans ce dictionnaire la formule de Hasse-Weil, en amenant à la première rencontre de "la courbe" $\mathbf{C}$ et l'action de $\mathbb{R}_+^*$ sur $\mathbf{C}$, analogue à l'action de Galois. Le théorème 4.2 indique que le rôle du corps des constantes est joué par l'anneau de coefficients absolus $\mathbb{S}$. Puisque le semi-corps booléen $\mathbb{B}$ peut être vu comme une $\mathbb{S}$-algèbre, cette traduction suggère de faire descendre les structures du site arithmétique et du site de mise à l'échelle dont il a été question dans la section 2 de $\mathbb{B}$ à $\mathbb{S}$.

5 Anneaux de $\mathbb{S}[\mu_{n,+}]$-polynômes

Soit $n > 0$ un entier, μ_n le groupe multiplicatif des racines n-ièmes de 1 et $\mathbb{S}[\mu_{n,+}]$ la $\mathbb{S}$-algèbre sphérique du monoïde (pointé) $\mu_{n,+} = \mu_n \cup \{0\}$. On rappelle que les morphismes de $\mathbb{S}$-algèbres $\mathbb{S}[\mu_{n,+}] \to HR$ correspondent (bijectivement) aux homomorphismes de groupes $\iota : \mu_n \to R^\times$ [11]. Dans cette section, on introduit la notion d'anneaux de $\mathbb{S}[\mu_{n,+}]$-polynômes en une (Définition 5.1) et plusieurs variables (Remarque 5.2) qui peut jouer un rôle clé dans la recherche des "puissances absolues de Descartes" parmi les anneaux ordinaires. On montre que la paire (R, X) d'un anneau R et d'un $\mathbb{S}[\mu_{n,+}]$-générateur de R est caractérisée de manière unique, à isomorphisme près, par l'application de μ_n vers les polynômes à coefficients dans le monoïde pointé $\mu_{n,+}$, qui code l'addition de 1 en éléments de μ_n.

Définition 5.1. Soit R un anneau, $\iota : \mu_n \to R^\times$ un homomorphisme injectif de groupes. Un élément $X \in R$ est un $\mathbb{S}[\mu_{n,+}]$-générateur de R si et seulement si tout élément $z \in R$ peut s'écrire de manière unique comme un polynôme $z = \sum_j \iota(\alpha_j)\, X^j$ à coefficients $\alpha_j \in \mu_n \cup \{0\}$.

Remarque 5.2. Plus généralement, un ensemble fini $\{X_i \mid i \in \{1, \dots, k\}\}$, $\mathbb{S}[\mu_{n,+}]$-engendre R si et seulement si tout élément $z \in R$ peut s'écrire de manière unique comme un polynôme $z = \sum_j \iota(\alpha_j)\, X^j$ à coefficients $\alpha_j \in \mu_n \cup \{0\}$, où j est un multi-index $j = (j_1, \dots, j_k) \in \mathbb{N}^k$, et $X^j := \prod X_i^{j_i}$.

Soit $\mathcal{P}(\mu_n)$ le sous-ensemble de l'ensemble $\left(\mu_n \cup \{0\}\right)^{\mathbb{N}}$ de séquences avec seulement un nombre fini de termes non nuls. Soit $X \in R$, alors l'application $\sigma : \mathcal{P}(\mu_n) \to R$, donnée par

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

est bien définie puisque pour $\alpha = (\alpha_j) \in \mathcal{P}(\mu_n)$ la somme $\sum_j \iota(\alpha_j)\, X^j$ définit un élément de R. Il découle de la définition 5.1 que si X est un $\mathbb{S}[\mu_{n,+}]$-générateur, l'application σ est une bijection entre $\mathcal{P}(\mu_n)$ et R.

L'exemple le plus simple d'un $\mathbb{S}[\mu_{n,+}]$-générateur, avec $n+1$ une puissance de nombre premier q, est fourni par l'exemple suivant :

Exemple 5.4. l'anneau $R = \mathbb{F}_q[X]$ des polynômes sur le corps fini $\mathbb{F}_q$ a la variable X comme $\mathbb{F}_q^\times$-générateur.

La proposition montre que la m-ième racine du $\mathbb{S}[\mu_{n,+}]$-générateur X d'un anneau R est un $\mathbb{S}[\mu_{n,+}]$-générateur de l'extension de la R-algèbre $R[Y]/(Y^m - X)$, cela fournissant par conséquent une multitude d'exemples.

Proposition 5.5. *Soit R un anneau, $\iota : \mu_n \to R^\times$ étant un homomorphisme injectif de groupes, $X \in R$ un $\mathbb{S}[\mu_{n,+}]$-générateur de R et $m \in \mathbb{N}$ un entier positif. Alors $Y \in R[Y]/(Y^m - X)$ est un $\mathbb{S}[\mu_{n,+}]$-générateur de $R[Y]/(Y^m - X)$.*

Démonstration. Tout élément z de $R[Y]/(Y^m - X)$ peut s'écrire de manière unique comme $z = \sum_{j=0}^{m-1} a_j Y^j$, avec $a_j \in R$ écrit de manière unique comme $a_j = \sum_{j,k} \iota(\alpha_{j,k})\, X^k$ où $\alpha_{j,k} \in \mu_n \cup \{0\}$. Puisque $Y^m = X$, on obtient l'unique décomposition finie

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

□

L'exemple suivant est une généralisation évidente du fait que 3 est un $\mathbb{S}[\pm 1] = \mathbb{S}[\mu_{2,+}]$-générateur de l'anneau $\mathbb{Z}$ des entiers.

Exemple 5.6. Soit $m \in \mathbb{N}$ un entier positif, et $\epsilon = \pm 1$. Alors $X = (3\epsilon)^{1/m}$ est un $\mathbb{S}[\pm 1]$-générateur du sous-anneau $R = \mathbb{Z}[X]$ du corps de nombres $\mathbb{Q}((3\epsilon)^{1/m})$.
En effet, le polynôme $X^m - 3\epsilon$ est irréductible, donc tout élément $z \in R$ peut être écrit de manière unique comme une somme

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

En retour, tout a_j peut s'écrire de manière unique comme $a_j = \sum_{j,k} \alpha_{j,k}\, (3\epsilon)^k$, où $\alpha_{j,k} \in \{-1, 0, 1\}$. Puisque $3\epsilon = X^m$, on obtient la décomposition unique

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

Un cas intéressant est celui de $m = 2$ et $\epsilon = -1$ puisqu'alors, l'anneau $R = \mathbb{Z}[\sqrt{-3}]$ est un ordre de l'anneau des entiers du corps imaginaire quadratique $\mathbb{Q}(\sqrt{-3})$.

Notons que dans l'exemple 5.6, l'addition est spécifiée par une égalité de la forme suivante

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

avec $P(X) = \epsilon X^m - 1$. Une présentation algébrique simple de la forme (5.7) est vérifiée quand on travaille sur $\mu_{n,+}$ pour $n = 1, 2$.

Le résultat suivant établit l'unicité d'une présentation polynomiale similaire dans le cas général.

Proposition 5.8. *Soit R un anneau, $\iota : \mu_n \to R^\times$ un homomorphisme injectif de groupes, $X \in R$ un $\mathbb{S}[\mu_{n,+}]$-générateur de R. Pour une décomposition polynomiale $z = \sum_j \iota(\alpha_j) X^j \in R$, soit* $\deg(z)$ *le plus petit entier m tel que $\alpha_j = 0$ pour tout $j > m$. Alors, on a le résultat suivant*

(i) Soit $m \in \mathbb{N}$, et $J_m = \langle X^m \rangle \subset R$ l'idéal engendré par X^m. Tout élément $z \in R$ admet une unique décomposition additive $z = a + b$ où $\deg(a) < m$ et $b \in J_m$.

(ii) Le quotient $R_m := R/J_m$ est un anneau fini dont les éléments s'écrivent de manière unique comme $\sum_{j=0}^{m-1} \iota(\alpha_j) X^j$, avec $\alpha_j \in \mu_{n,+} = \mu_n \cup \{0\}$.

(iii) Le quotient $R_1 := R/J_1$ est un corps fini avec $n+1$ éléments et $\iota : \mu_{n,+} \to R$ est une section multiplicative de l'application quotient $R \to R_1$.

(iv) L'homomorphisme canonique d'anneaux $\pi : R \to \varprojlim R_m$ est injectif.

(v) La paire (R, X) est spécifiée de manière unique, à isomorphisme près, par l'application $h : \mu_n \to \mathcal{P}(\mu_n)$ qui est définie de manière unique par l'égalité $\sigma(h(\xi)) = \iota(\xi) + 1$.

Démonstration. (i) Soit $z = \sum_j \iota(\alpha_j) X^j$. En écrivant z comme

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

on obtient la décomposition requise avec $b = X^m c$. L'unicité d'une telle décomposition découle alors de l'unicité de la décomposition comme dans la définition 5.1.

(ii) découle de (i). En particulier, on vérifie aisément que R_m a pour cardinalité $\#(R_m) = (n+1)^m$.

(iii) Par construction, l'application $\iota : \mu_{n,+} \to R$ est une section multiplicative de l'application quotient $R \to R_1$. Il découle de cela que les éléments non nuls de R_1 forment le groupe multiplicatif μ_n de telle façon que R_1 est un corps à $n+1$ éléments.

(iv) Les composants de $z = \sum_j \iota(\alpha_j) X^j \in R$ sont déterminés de manière unique par $\pi(x)$.

(v) Soit (R', X') une seconde paire correspondant à la même application $h : \mu_n \to \mathcal{P}(\mu_n)$. Soit $\rho : R \to R'$ l'application bijective définie par

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

On a par construction

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

En particulier, on a également $\rho(J_m) = J'_m$ pour tout m. Par conséquent, ρ induit une bijection $\rho_m : R_m \to R'_m$. Par (iii), pour montrer que ρ est un homomorphisme d'anneaux, il suffit de vérifier que chaque ρ_m est un

homomorphisme d'anneaux.
Pour montrer que ρ_m est additif, il suffit de montrer qu'on peut calculer tous les termes d'une somme

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

en utilisant seulement l'application $h : \mu_n \to \mathcal{P}(\mu_n)$. Pour faire cela, on détermine d'abord une application F de l'ensemble des k-tuples d'éléments de $\mu_{n,+}$ vers l'ensemble des paires (x, Z) où $x \in \mu_{n,+}$ et où Z est un $(k-1)$-tuple d'éléments de $\mathcal{P}(\mu_n)$. L'application h détermine de manière unique une application symétrique

$$H : \mu_{n,+} \times \mu_{n,+} \to \mu_{n,+} \times \mathcal{P}(\mu_n), \quad H(\xi, \eta) = (\xi + \eta, 0) \text{ si } \xi\,\eta = 0$$
$$H(\xi, \eta) = (H_0(\xi, \eta), P(\xi, \eta)), \quad H_0(\xi, \eta) + X\,P(\xi, \eta) = \eta\; h(\xi\,\eta^{-1}) \text{ si } \eta \neq 0 \tag{5.12}$$

Pour définir F, on procède par induction sur k. Pour $k = 1$, on pose $F(x) = x$. Pour $k = 2$, on pose $F_2 = H$. On dénote les deux composantes de $F_k : \mu_{n,+}^{k-1} \times \mu_{n,+} \to \mu_{n,+} \times \mathcal{P}(\mu_n)^{k-1}$ par $F_k^{(1)}$ et $F_k^{(2)}$. Pour passer de $k-1$ à k, on pose

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

où dans la dernière expression, on concatène le polynôme $P(F_{k-1}^{(1)}(\alpha), \eta)$ à la liste $F_{k-1}^{(2)}(\alpha)$, en obtenant ainsi une liste de $k-1$ polynômes.
Pour calculer les composants γ_j de la somme (5.11), on construit par induction sur k, deux listes. La première $R(k)$ est la liste des coefficients déjà calculés et c'est la seule liste donnée par $(\gamma_0, \gamma_1, \ldots, \gamma_{k-1})$. La seconde $C(k)$, (appelée la retenue), est la liste des polynômes à coefficients dans $\mu_{n,+}$ et elle est codée comme la liste de leurs coefficients. Chaque telle liste ℓ de coefficients a $m-k$ termes, tous dans $\mu_{n,+}$. On dénote par $f(\ell) \in \mu_{n,+}$ le premier terme de la liste ℓ et par $t(\ell)$ la liste obtenue en éliminant le premier élément de la liste ℓ, elle a $m-k-1$ termes. L'étape pour obtenir $R(k+1), C(k+1)$ à partir de $\alpha, \beta, R(k), C(k)$ est

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

et

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

quand on remplace chaque élément de $F^{(2)}(\alpha_k, \beta_k, (f(\ell))_{\ell \in C(k)})$ par la liste de ses $m-k$ premiers coefficients. Plus concrètement, on obtient d'abord $\gamma_0 = F_2^{(1)}(\alpha_0, \beta_0)$ où la retenue supérieure fournit le polynôme $P(\alpha_0, \beta_0) = F_2^{(2)}(\alpha_0, \beta_0)$. Ainsi $R(1) = (\gamma_0)$, $C(1)$ a un élément qui est la liste des $m-1$ premiers coefficients de $P(\alpha_0, \beta_0)$. On coupe alors les éléments α, β et on considère la somme

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

Tous les termes dans (5.13) sont divisibles par X et on peut utiliser F_3 pour calculer la somme des trois termes α_1, β_1, p_0 où p_0 est le terme constant de $P(\alpha_0, \beta_0)$. Cette opération livre le prochain terme

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

de (5.11), et adjoint les deux polynômes de la liste $F_3^{(2)}(\alpha_1, \beta_1, p_0)$ à la liste des retenues constituée du seul polynôme $P(\alpha_0, \beta_0)$ avec son premier terme p_0 effacé. La liste des retenues est constituée maintenant de

trois termes ℓ_1, ℓ_2, ℓ_3. On utilise alors F_5 pour calculer la somme des 5 termes : α_2, β_2 et des trois termes $f(\ell_1), f(\ell_2), f(\ell_3)$ de la retenue. Cela ajoute 4 termes à la liste de retenues qui a maintenant 7 termes, dont les trois premiers ont été coupés en effaçant leur terme le plus bas. Après k telles opérations, la retenue a $2^k - 1$ éléments et on procède comme suit. On utilise F_{2^k+1} pour calculer la somme des $2^k + 1$ termes donnée par α_k, β_k ensemble avec les termes $f(\ell)$ de la liste des retenues. Cette opération fournit γ_k et adjoint 2^k termes à la liste de retenues qui est constituée maintenant de $2^{k+1} - 1$ termes. Ce processus s'arrête quand $k = m$ et $R(m)$ fournit les formules universelles pour les termes γ_j, $0 \le j \le m-1$ en utilisant seulement α, β et l'application h.

Le fait que les coefficients γ_j puissent être calculés en utilisant seulement α, β et l'application h prouve que ρ est additive puisqu'on peut utiliser la même formule pour calculer $\alpha + \beta$ dans R_m et $\rho_m(\alpha) + \rho_m(\beta)$ dans R'_m. La multiplicativité de ρ découle par bilinéarité de $\rho(\alpha X^n \times \beta X^m) = \rho(\alpha X^n)\rho(\beta X^m)$. Cela montre que $\rho : R \to R'$ est un isomorphisme d'anneaux et par construction, on a $\rho(X) = X'$. □

Définition 5.14. L'application

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

qui caractérise la paire (R, X) (par la proposition 5.8) est appelé la *clé* de la paire (R, X).

Corollaire 5.16. *Soit n tel qu'il existe un anneau de polynômes à un générateur sur $\mathbb{S}[\mu_{n,+}]$, alors $n+1$ est une puissance de nombre premier.*

Démonstration. Cela découle de la proposition 5.8 (*iii*). □

Remarque 5.17. La preuve de la proposition 5.8 (v) est établie de telle façon que l'on puisse, en la suivant, écrire un programme d'ordinateur qui pourrait être utilisé pour tester la structure additive de l'anneau R_m. Il sera pertinent dans la section 6 de déterminer dans les divers exemples les anneaux R_m.
L'application $h : \mu_n \to \mathcal{P}(\mu_n)$ de (5.15) détermine l'addition $H : \mu_{n,+} \times \mu_{n,+} \to \mu_{n,+} \times \mathcal{P}(\mu_n)$, (5.12), de paires d'éléments de $\mu_{n,+}$ en utilisant la compatibilité avec la multiplication par des éléments de μ_n.
La proposition 5.8 montre qu'une paire (R, X), où X est un $\mathbb{S}[\pm 1]$-générateur de R, *i.e.* $n = 2$, est caractérisée de manière unique par le polynôme $P(X)$ comme dans (5.7). Le polynôme $P(X) = -1$ produit la paire $(\mathbb{F}_3[X], X)$, alors que $P(X) = X - 1$ détermine la paire $(\mathbb{Z}, 3)$.
Quand $n = 2$, le terme constant du polynôme $P(X)$ dans (5.7) est nécessairement égal à -1. En effet, si le terme constant était 0 ou 1, cela contredirait l'unicité de la décomposition de la définition 5.1 par l'égalité $1 = P(X) - 1$. Cela montre également que $R_1 = \mathbb{F}_3$.

Remarque 5.18. Il n'est pas vrai qu'un choix aléatoire de polynôme avec coefficients dans $\mathbb{S}[\pm 1]$ et coefficient constant -1 correspond à une paire. Il y a un cas simple avec $P(X) = -1 + X + X^2$. En effet, dans les lignes ci-après, on montre que 5 n'est représenté par aucun polynôme. Avec cette règle, on a $1 + 1 + 1 + 1 = 1 + X + X^2$. Ajouter 1 aux deux côtés donne

$$\begin{aligned} &1 + 1 + 1 + 1 + 1 = -1 + X + X^2 + X + X^2 = -1 + X(-1 + X + X^2) + X^2(-1 + X + \\ &+ X^2) = -1 - X + X^3 + X^3 + X^4 = -1 - X + X^3(-1 + X + X^2) + X^4 = \\ &= -1 - X - X^3 + X^4 + X^4 + X^5. \end{aligned}$$

Alors, quand on travaille dans R_n (*i.e.* modulo X^n), le nombre 5 est représenté par

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

et cette expression est de degré $n-1$ pour tout n et ainsi, elle ne correspond pas à une somme finie de puissances de X.

6 Exemples

Dans cette section, on fournit des exemples d'anneaux de polynômes (R, X) à un générateur X sur $\mathbb{S}[\mu_{n,+}]$ où R est de caractéristique zéro. L'anneau R est plongé comme sous-anneau de $\mathbb{C}$ en résolvant pour $X \in \mathbb{C}$ les équations $\sigma(h(\xi)) = \iota(\xi) + 1$, $\xi \in \mu_n$, en utilisant l'intégration canonique $\mu_{n,+} \subset \mathbb{C}$. La limite projective $\varprojlim R_n$ est, dans ces exemples, une extension finie de l'anneau des entiers p-adiques $\mathbb{Z}_p$. Alors qu'on peut utiliser l'axiome du choix pour montrer l'existence d'un plongement du corps p-adique $\mathbb{Q}_p$ dans le corps des nombres complexes, de tels plongements ont le statut de chimères. En effet, la continuité des caractères mesurables des groupes compacts appliquée au groupe additif $\mathbb{Z}_p$ montre qu'un plongement du corps p-adique $\mathbb{Q}_p$ dans le corps des nombres complexes est automatiquement non mesurable. D'un autre côté, les exemples suivants montreront que les anneaux de polynômes (R, X) à un générateur X sur $\mathbb{S}[\mu_{n,+}]$ fournissent des instances d'interactions explicites des corps p-adiques (et de leurs extensions finies) avec les nombres complexes. Ces interactions sont données par paires de plongements avec domaines denses

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

de l'anneau des polynômes de Laurent $R[X^{-1}]$. Le plongement gauche dans le diagramme ci-dessus est dans une extension algébrique finie $W(\mathbb{F}_q)[\eta]$ de l'anneau de Witt $W(\mathbb{F}_q)$. L'anneau des fractions de l'anneau $W(\mathbb{F}_q)[\eta]$ est une extension finie du corps p-adique. La plupart de ces exemples viennent de systèmes de numération connus et ont leur origine dans la recherche de manières optimales de coder les nombres [20]. Dans chaque cas, le quotient $R_1 = R/(XR)$ est le corps fini $\mathbb{F}_q$, $q = n+1$, et l'isomorphisme entre semi-groupes multiplicatifs $j : \mathbb{F}_q \sim \mu_{n,+} \subset \mathbb{C}$ sert de guide, en utilisant l'addition dans le corps fini $\mathbb{F}_q$, pour les termes de degré 0 dans la construction de l'application h. Notons que le choix de j pour $\overline{\mathbb{F}}_q$ joue un rôle clé dans la construction par Quillen [27] de la relation entre la K-théorie algébrique de $\mathbb{F}_q$ et les opérations de Adams.

6.1 Anneaux de polynômes à un générateur sur $\mathbb{S} = \mathbb{S}[\mu_{1,+}]$

Quand on travaille sur $\mathbb{S} = \mathbb{S}[\mu_{1,+}]$, il n'y a pas d'annulation puisqu'il n'y a pas de signe moins. Ainsi, à partir des deux éléments non nuls x, y, l'égalité $x + y = 0$ peut seulement être vérifiée dans la limite projective $\varprojlim R_m$. On calcule cette limite projective dans les prochains exemples.

6.1.1 L'anneau polynomial $(\mathbb{Z}, -2)$

L'anneau $\mathbb{Z}$ admet le générateur $X = -2$ sur $\mathbb{S}$. La clé est donnée par $1 + 1 = P(X) = X + X^2$. Les valeurs des polynômes de degré n, en $X = -2$ sont reportées pour les premières valeurs de n dans la table suivante

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	$[22, 85] \cap \mathbb{Z}$

Voyons, par exemple, le calcul de $1 + 1 + X$. On obtient

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

et en itérant cette étape, on obtient que $1 + 1 + X \in J_m = \langle X^m \rangle R$, $\forall m$. Cela montre que $1 + 1 + X = 0$ dans $\varprojlim R_m$. Ensuite, on relie le degré du polynôme $p(X)$ à la valeur absolue de l'entier $p(-2)$. Posons

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

Le degré n d'un polynôme $p(X)$ à coefficients dans $\{0, 1\}$ spécifie le signe de l'entier $p(-2)$ comme étant $(-1)^n$ et fournit des limites inférieure et supérieure sur le module $|p(-2)|$ comme suit

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

Étant donné un entier $m \in \mathbb{Z}$, la première inégalité fournit la limite suivante, sur le degré du polynôme p tel que $p(-2) = m$

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

La limite projective $\varprojlim R_m$ est ici l'anneau $\mathbb{Z}_2$ des entiers 2-adiques, et les éléments de $\mathbb{Z}$ dans $\mathbb{Z}_2$ sont caractérisés par le fait que leur séquence de chiffres est éventuellement constante.

Ensuite, voyons les corps quadratiques pour lesquels l'étude des systèmes de numération dans [18, 19] fournit une liste exhaustive d'exemples. On déduit aisément de *op.cit.* ce qui suit

Proposition 6.2. *Les corps quadratiques K dont l'anneau des entiers admet un $\mathbb{S}$-générateur sont*

- $\mathbb{Q}(\sqrt{-1})$ *avec le générateur* $X = -1 + \sqrt{-1}$ *de l'anneau* $\mathbb{Z}[\sqrt{-1}]$ *des entiers de* K.
- $\mathbb{Q}(\sqrt{-2})$ *avec le générateur* $X = \sqrt{-2}$ *de l'anneau* $\mathbb{Z}[\sqrt{-2}]$ *des entiers de* K.
- $\mathbb{Q}(\sqrt{-7})$ *avec le générateur* $X = \frac{1}{2}\left(1 + \sqrt{-7}\right)$ *de l'anneau des entiers de* K.

Démonstration. La norme $N(\alpha)$ d'un $\mathbb{S}$-générateur est égale à 2, par conséquent, l'ensemble $N_0(\alpha) := \{0, \ldots, N(\alpha) - 1\}$ définissant un système de numération canonique au sens de [18, 19] est $\{0, 1\}$ et le résultat découle du théorème 1 de [19] dans le cas complexe et de la première phrase de [18] dans le cas réel. □

6.1.2 L'anneau de polynômes $(\mathbb{Z}[i], -1+i)$

Ici, on considère l'anneau $R = \mathbb{Z}[i]$ des entiers de Gauss (parfois appelés binarions ; voir [22]) avec $X = -1 + i$ comme $\mathbb{S}[\mu_{1,+}] = \mathbb{S}$-générateur. En effet, tout entier de Gauss peut s'écrire de manière unique comme une somme finie de puissances de X ([16, 28] et Figure 2). On a l'égalité $1 + 1 = P(X) = X^2 + X^3$, qui nous permet de calculer la somme de toute paire de polynômes à coefficients dans $\{0, 1\}$.

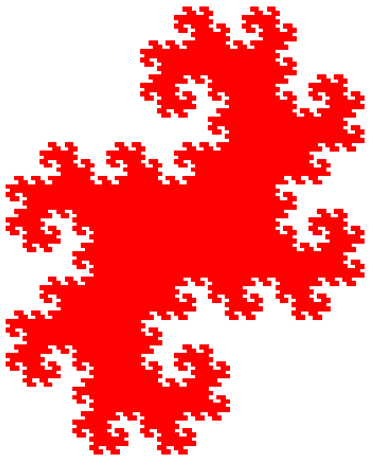


FIG. 2 : Entiers de Gauss comme $\mathbb{S}$-polynômes de degré ≤ 12

Proposition 6.3. *Soit $R = \mathbb{Z}[i]$, $X = -1 + i$.*
(i) L'idéal de $R = \mathbb{Z}[i]$ engendré par X^2 est le même que l'idéal engendré par 2.
(ii) L'anneau R_m pour $m = 2k$ est $\mathbb{Z}/(2^k\mathbb{Z})[X]$ où $X^2 = -2 - 2X$.
(iii) L'anneau R_m pour $m = 2k + 1$ est $\mathbb{Z}/(2^{k+1}\mathbb{Z}) \oplus \mathbb{Z}/(2^k\mathbb{Z})\, X$ où $X^2 = -2 - 2X$.
(iv) La limite projective $\varprojlim R_m$ est l'anneau $\mathbb{Z}_2[i] \sim \mathbb{Z}_2[X]$ où $X^2 = -2 - 2X$.

Démonstration. (i) L'élément $U = (1 + X) \in R$ est une unité puisque $U^4 = 1$ et on a

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

(ii) Par (i), l'idéal $X^{2k}R$ est égal à 2^kR. On a $R = \mathbb{Z}[i]$ et $R/(2^kR) = \mathbb{Z}/(2^k\mathbb{Z})[i] = \mathbb{Z}/(2^k\mathbb{Z})[X]$ avec $X^2 = -2 - 2X$, ainsi on obtient (ii).
(iii) Posons $m = 2k + 1$. Tout élément de R est de la forme $z = a + bX$ où $a, b \in \mathbb{Z}$. Dans R, on a $2^{k+1} \in X^{2k+2}R \subset J_m$ et $2^kX \in X^{2k+1}R = J_m$. Ainsi l'homomorphisme $\mathbb{Z}[X] \to R_m$ induit un homomorphisme surjectif de $\mathbb{Z}/(2^{k+1}\mathbb{Z}) \oplus \mathbb{Z}/(2^k\mathbb{Z})\, X$ vers R_m. Il est bijectif puisque les cardinaux sont égaux.
(iv) L'extension $\mathbb{Q}_2[i]$ est totalement ramifiée d'indice $e = 2$ (voir [28], 4.2). Le polynôme $X^2 + 2X + 2$ est un polynôme de Eisenstein qui définit $\mathbb{Q}_2[i]$ comme son corps de séparation. La valuation de X est la moitié de la valuation de 2. □

6.1.3 L'anneau de polynômes $\left(\mathbb{Z}[\sqrt{-2}], \sqrt{-2}\right)$

L'élément $X := \sqrt{-2}$ est un $\mathbb{S}[\mu_{1,+}] = \mathbb{S}$-générateur de l'anneau des entiers $\mathbb{Z}[\sqrt{-2}]$ du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-2})$. Cela découle directement de §6.1.1 et de la proposition 5.5. La clé est fournie par le polynôme $P(X) = X^4 + X^2$. Un analogue évident de la proposition 6.3 est vérifié.

6.1.4 L'anneau de polynômes $\left(\mathcal{O}(\mathbb{Q}(\sqrt{-7})), \frac{1}{2}(1+\sqrt{-7})\right)$

L'élément $X := \frac{1}{2}\left(1+\sqrt{-7}\right)$ est un $\mathbb{S}[\mu_{1,+}] = \mathbb{S}$-générateur de l'anneau $\mathcal{O}(\mathbb{Q}(\sqrt{-7}))$ d'entiers du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-7})$. La clé est donnée par le polynôme $P(X) = X^3 + X$. Soit F le domaine fondamental de $\mathcal{O}(\mathbb{Q}(\sqrt{-7}))$ donné par le parallélogramme de sommets $0, 1, X, X+1$. La figure 3 montre le voisinage de $0 \in \mathbb{C}$ obtenu comme l'union des translations $F + p(X)$ par les polynômes $p(X)$ de degré ≤ 11.

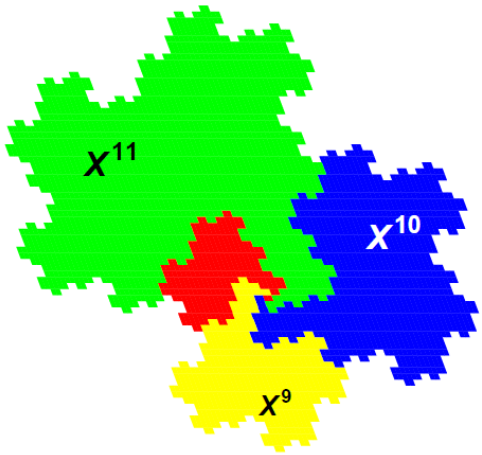


FIG. 3 : Polynômes de degré ≤ 11 pour $X = \frac{1}{2}\left(1+\sqrt{-7}\right)$

Proposition 6.4. *Soit* $R = \mathcal{O}(\mathbb{Q}(\sqrt{-7}))$, $X = \frac{1}{2}\left(1+\sqrt{-7}\right)$.
(i) *L'anneau* R_m *est* $\mathbb{Z}/(2^m\mathbb{Z})$.
(ii) *La limite projective* $\varprojlim R_m$ *est l'anneau* $\mathbb{Z}_2$.
(iii) *L'élément* $X \in \varprojlim R_m = \mathbb{Z}_2$ *est la seule solution divisible par* 2 *dans l'anneau* $\mathbb{Z}_2$ *pour l'équation* $2 + X + X^2 = 0$.

Démonstration. La clé est donnée par $P(X) = X^3 + X$ et on a $P(X) - 2 = (X-1)\left(X^2 + X + 2\right)$. Par le lemme de Hensel, l'équation $2 + X + X^2 = 0$ admet une solution unique α dans $\mathbb{Z}_2$ de la forme $\alpha = 1 + 2\epsilon$ et une solution unique de la forme $\beta = 2(1 + 2\epsilon')$. En fait, on a $\alpha\beta = 2$ et $\alpha + \beta = -1$. L'homomorphisme $\rho : \mathbb{Z}[\frac{1}{2}\left(1+\sqrt{-7}\right)] \to \mathbb{Z}_2$ donné par $\rho\left(\frac{1}{2}\left(1+\sqrt{-7}\right)\right) = \beta$ est bien défini puisque β est une solution de l'équation $2 + X + X^2 = 0$. De plus, β est le produit de 2 par une unité de $\mathbb{Z}_2$ (mais cela échoue dans $R = \mathcal{O}(\mathbb{Q}(\sqrt{-7}))$). La projection X_m de β dans $\mathbb{Z}_2/(2^m\mathbb{Z}_2) = \mathbb{Z}/(2^m\mathbb{Z})$ respecte la contrainte $P(X_m) = 2$ et X_m est le produit de 2 par une unité. Ainsi, les idéaux engendrés par les puissances de X_m sont les mêmes que ceux engendrés par les puissances de 2. Cela prouve les trois assertions (i), (ii), (iii). □

6.2 Anneaux de polynômes à un générateur sur $\mathbb{S}[\pm 1]$

6.2.1 L'anneau de polynômes $(\mathbb{Z}, 3)$

Le cas du $\mathbb{S}[\pm 1]$-générateur $3 \in \mathbb{Z}$ est particulièrement pertinent parce que, comme cela a été montré dans [13], l'addition coïncide avec celle des vecteurs de Witt dans $W(\mathbb{F}_3) = \mathbb{Z}_3$.

Proposition 6.5. *Soit $R = \mathbb{Z}$, $X = 3$ est un $\mathbb{S}[\pm 1]$-générateur de R. La clé est $P(X) = -1 + X$.*
(i) L'anneau R_m est $\mathbb{Z}/(3^m\mathbb{Z})$.
(ii) La limite projective $\varprojlim R_m$ est l'anneau $W(\mathbb{F}_3) = \mathbb{Z}_3$.
(iii) L'ensemble des vecteurs de Witt avec seulement un nombre fini de composants non nuls forme un sous-anneau de $W(\mathbb{F}_3)$ isomorphe à $\mathbb{Z}$.

Pour organiser les prochains exemples, on donne la liste des extensions des corps quadratiques imaginaires de $\mathbb{Q}$ engendrées par les anneaux de $\mathbb{S}[\pm 1]$-polynômes en une variable.

Proposition 6.6. *Les corps quadratiques imaginaires K engendrés par les anneaux de $\mathbb{S}[\pm 1]$-polynômes en une variable sont*

- $\mathbb{Q}(\sqrt{-2})$ *avec générateur $X = 1 + \sqrt{-2}$ de l'anneau $\mathbb{Z}[\sqrt{-2}]$ des entiers de K.*
- $\mathbb{Q}(\sqrt{-3})$ *avec générateur $X = \sqrt{-3}$ de $\mathbb{Z}[\sqrt{-3}]$ (domaine qui n'est pas à factorisation unique).*
- $\mathbb{Q}(\sqrt{-11})$ *avec générateur $X = \frac{1}{2}(1 + \sqrt{-11})$ de l'anneau des entiers de K.*

Démonstration. Soit $P(X) = -1 + \sum_{j=1}^{n-1} a(j)X^j + \epsilon X^n$, $\epsilon \in \{\pm 1\}$, $a(j) \in \{-1, 0, 1\}$, la retenue amenant à une extension quadratique imaginaire. Les racines du polynôme $P(X) - 2$ sont des entiers algébriques, et on suppose que l'un d'entre eux, disons α, est imaginaire quadratique. Soit $q(x) = x^2 - bx + c$ son polynôme minimal. Il a des coefficients entiers de telle façon que $b, c \in \mathbb{Z}$, et par définition, il divise $P(X) - 2$. Le coefficient constant c doit être égal à 3. En effet, il divise le coefficient constant -3 de $P(X) - 2$ et puisque $b^2 - 4c < 0$ il est positif. Il ne peut pas être égal à 1 parce que dans ce cas, on obtiendrait $b \in \{-1, 0, 1\}$, et $\alpha \in \{i, j, -j\}$ ce qui contredit l'injectivité de l'application σ. Pour $c = 3$, les valeurs possibles de b sont $b = 0$ qui donne la solution $\alpha = \sqrt{-3}$, $b = \pm 1$ qui donne les solutions $\alpha = \frac{1}{2}\left(\pm 1 \pm i\sqrt{11}\right)$, $b = \pm 2$ qui donne les solutions $\alpha = \pm 1 \pm i\sqrt{2}$, et finalement $b = \pm 3$. On va maintenant montrer que ce dernier choix qui donne $\alpha = \frac{1}{2}\left(\pm 3 \pm i\sqrt{3}\right)$ ne donne pas de solution. Pour prouver cela, il suffit de montrer que le polynôme $3 + 3X + X^2$ ne peut diviser un polynôme $P(X) - 2$ avec P de la forme ci-dessus. On suppose par conséquent une égalité de la forme

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

Puisque les coefficients de $P - 2$ sont entiers et puisque le coefficient principal de $3 + 3X + X^2$ est 1, les coefficients $b(j)$ sont des entiers. On obtient $b(0) = -1$, $3b(1) - 3 = a(1)$, mais $a(1) \in \{-1, 0, 1\}$ et ainsi, en travaillant modulo 3, on obtient $a(1) = 0$ et par conséquent $b(1) = 1$. En considérant le coefficient de X^2, on obtient $3b(1) + 3b(2) - 1 = a(2)$ qui donne $a(2) = -1$ et $b(2) = -b(1) = -1$. On peut maintenant procéder par induction pour montrer que $b(j) = (-1)^{j+1}$. En effet, le coefficient of X^j est $b(j-2) + 3b(j-1) + 3b(j) = a(j)$ et si on sait que $b(j-2) = (-1)^{j-1}$ et $b(j-1) = (-1)^j$, on obtient $a(j) = b(j-2)$ et $3b(j-1) + 3b(j) = 0$ de telle façon que $b(j) = (-1)^{j+1}$. Cela fonctionne pour $j \leq n - 2$. Le coefficient de X^{n-1} est $b(n-3) + 3b(n-2) = a(n-1)$ et cela aboutit à une contradiction puisqu'on obtient $a(n-1) = b(n-3)$ (en travaillant modulo 3) ce qui contredit le fait que $b(n-2) \neq 0$. □

6.2.2 L'anneau de polynômes $(\mathcal{O}(\mathbb{Q}[\sqrt{-11}]), \frac{1}{2}\left(1+\sqrt{-11}\right))$

Cette section est destinée à fournir une preuve détaillée de ce que $X := \frac{1}{2}\left(1+\sqrt{-11}\right)$ est un $\mathbb{S}[\pm 1]$-générateur de l'anneau des entiers du corps de nombres $\mathbb{Q}(\sqrt{-11})$. La raison pour laquelle les détails de la preuve sont fournis est que nous souhaitons insister sur le fait que dans un tel cas, et contrairement au cas où l'on travaille sur $\mathbb{S}$, on peut explicitement contrôler les annulations dans les calculs.

Proposition 6.7. *Soit $\mathcal{O}$ l'anneau des entiers du corps de nombres $\mathbb{Q}(\sqrt{-11})$.*
(i) $X := \frac{1}{2}\left(1+\sqrt{-11}\right)$ est un $\mathbb{S}[\pm 1]$-générateur de $\mathcal{O}$. La clé de $(\mathcal{O}, X)$ est $P(X) = -1 + X - X^2$.
(ii) La limite projective $\varprojlim R_m$ est l'anneau $W(\mathbb{F}_3) = \mathbb{Z}_3$.

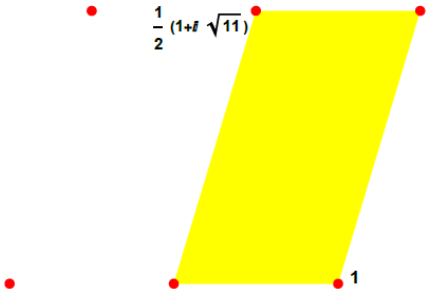
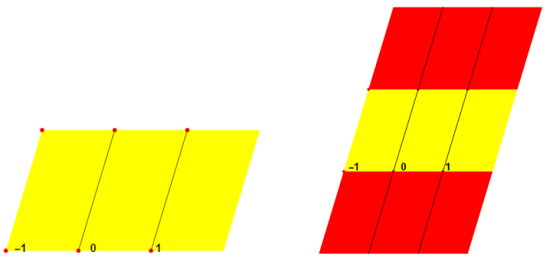


FIG. 4 : Domaine fondamental du réseau $\mathcal{O}$

La preuve nécessite un lemme préliminaire. On rappelle d'abord quelques résultats classiques concernant l'anneau des entiers $\mathcal{O}$ du corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-11})$. Le discriminant de K est $d = -11$. Ainsi, comme $-11 \sim 1$ modulo 4, le réseau $\mathcal{O}$ est $\mathbb{Z} + \mathbb{Z}X$ où $X := \frac{1}{2}\left(1+\sqrt{-11}\right)$. Par construction on a

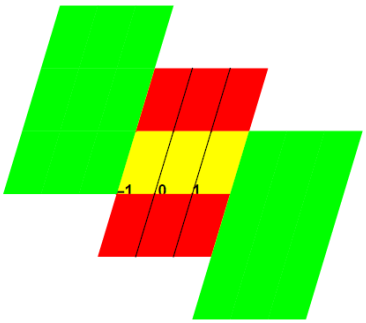
$$1 + 1 = P(X), \qquad P(X) = -1 + X - X^2. \tag{6.8}$$

On veut montrer que tout élément $z \in \mathcal{O}$ peut s'écrire de manière unique comme un polynôme $z = \sum_j \alpha_j X^j$, avec $\alpha_j \in \{-1, 0, 1\}$. La figure 5 montre le translaté du domaine fondamental du réseau, alors que les figures suivantes fournissent une esquisse de quelques étapes du processus de représentation des éléments de $\mathcal{O}$ en fonction des polynômes de degré $\leq n$, montrant ceux décrits par des polynômes de degré $= n$ avec une nouvelle couleur.

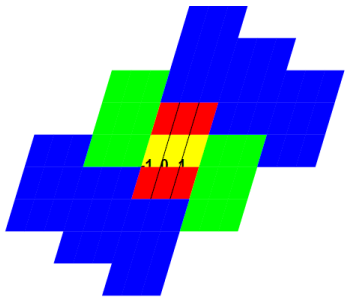


Première étape, polynômes de degré 0 Seconde étape, polynômes de degré ≤ 1

FIG. 5 : Les deux premières étapes

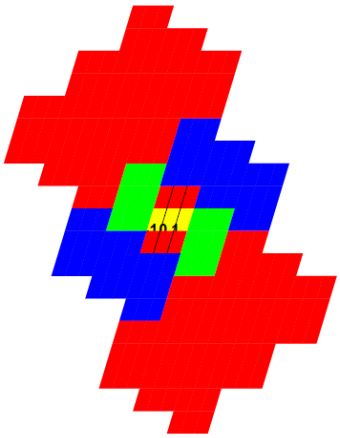


Etape 3, polyn. de deg. ≤ 2

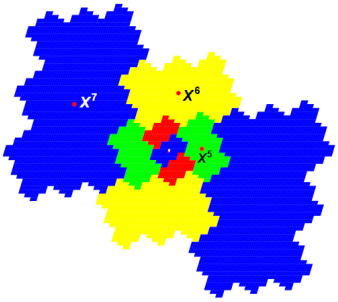


Etape 4, polyn. de deg. ≤ 3

FIG. 6 : Les troisième et quatrième étapes



Etape 5, polyn. de deg. ≤ 4



Etape 8, polyn. de deg. ≤ 7

FIG. 7 : Les cinquième et huitième étapes

En comparant les figures 5 (gauche et droite), 6 (gauche et droite), 7 (gauche et droite), on remarque que la translation $z \mapsto z+1$ n'augmente pas le degré du polynôme de plus de 2 unités. Le prochain lemme fournit une preuve formelle de ce fait.

Lemme 6.9. *Let* $z = \sum_{j=0}^{n} \alpha_j X^j \in \mathcal{O}$, $\alpha_j \in \{-1, 0, 1\}$. *Alors il existe des coefficients* $\beta_j \in \{-1, 0, 1\}$, *avec* $0 \leq j \leq n+2$, *tels que* $z + 1 = \sum_{j=0}^{n+2} \beta_j X^j$.

Démonstration. On procède par induction sur l'entier n. Pour $n = 0$, le résultat découle de (6.8). Supposons que le résultat est prouvé jusqu'à $n-1$, alors il existe des coefficients $\gamma_j \in \{-1, 0, 1\}$ tels que

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

Considérons une somme telle que $\gamma_n X^n + \gamma_{n+1} X^{n+1} + \alpha_n X^n$ et exprimons-la sans aller au-delà de X^{n+2}. Si $\gamma_{n+1} = 0$, cela découle à nouveau de (6.8). On peut alors supposer que $\gamma_{n+1} = \pm 1$ et également qu'à la fois γ_n et α_n sont non nuls et égaux puisque sinon, la somme $\gamma_n X^n + \alpha_n X^n$ aurait un degré d'au plus n. Le seul

cas à exclure alors est quand γ_n, α_n, et γ_{n+1} sont tous égaux (et non nuls), puisque seulement dans ce cas, on obtient un terme en X^{n+3} à partir de la somme

$$X^n + X^n + X^{n+1} = X^n(1 + 1 + X) = X^n(-1 + X + X - X^2) =$$
$$= X^n(-1 - X + X^2 - X^2 - X^3) = -X^n - X^{n+1} - X^{n+3}.$$

Pour exclure ce cas, on ajoute à l'hypothèse d'induction la condition que si le dernier terme β_{n+2} du polynôme de degré $n+2$ représentant $z+1$ est non nul, alors le terme β_{n+1} est nul ou du signe opposé. Cette condition est remplie pour $n = 0$, et si on la suppose pour $n-1$, elle est aussi vérifiée pour n. En effet, les seuls cas quand $\beta_{n+2} \neq 0$ ont lieu soit lorsque $\gamma_{n+1} = 0$, auquel cas β_{n+1} et β_{n+2} ont des signes opposés, soit quand $\gamma_{n+1} = \epsilon = \pm 1$ auquel cas $\gamma_n = \alpha_n = -\epsilon$, ce qui donne

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

impliquant que $\beta_{n+1} = 0$ dans ce cas. Ainsi l'hypothèse d'induction est encore vérifiée pour n, et cela conclut la preuve. □

Démonstration. (de la proposition 6.7) Le lemme 6.9 est vérifié pour la loi abstraite d'addition définie en utilisant (6.8) sur la limite projective de R_n. La preuve montre que les éléments de cette limite projective, qui ont seulement un nombre fini de coordonnées non nulles, sont stables par addition de 1. En utilisant (5.10), il s'ensuit qu'ils sont également stables par addition de n'importe quel monôme et par conséquent qu'ils forment un groupe additif A. Par conséquent, il reste à montrer que l'application $\rho : A \to \mathbb{C}$ définie par

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

est injective. Soit $\sum_j \alpha_j X^j \in \ker \rho$, alors $\sum_j \alpha_j z^j = 0$ et donc, z vérifie l'équation $E(z) = 0$ à coefficients entiers dont le coefficient principal est 1 et le terme constant est ± 1. Le polynôme E est ainsi un multiple du polynôme minimal $z^2 - z + 3$ de l'extension de corps. Le polynôme quotient a des coefficients entiers ; ainsi, on obtient une contradiction en utilisant le produit de termes constants. □

6.2.3 L'anneau de polynômes $\left(\mathbb{Z}[\sqrt{-3}], \sqrt{-3}\right)$

L'élément $X := \sqrt{-3}$ est un $\mathbb{S}[\mu_{2,+}] = \mathbb{S}[\pm 1]$-générateur de l'anneau $\mathbb{Z}[\sqrt{-3}]$ et ce dernier est un ordre maximal dans l'anneau des entiers du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-3})$. Cela découle directement de §6.1.1 et la proposition 5.5. La clé est donnée par le polynôme $P(X) = -1 - X^2$. Un analogue évident de la proposition 6.3 est vérifié.

6.2.4 L'anneau de polynômes $\left(\mathcal{O}(\mathbb{Q}(\sqrt{-2})), 1 + \sqrt{-2}\right)$

On obtient de façon similaire que $P(X) = -1 - X + X^2 - X^3$ est la clé associée au $\mathbb{S}[\pm 1]$-générateur $1 + \sqrt{-2}$ de l'anneau des entiers du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-2})$

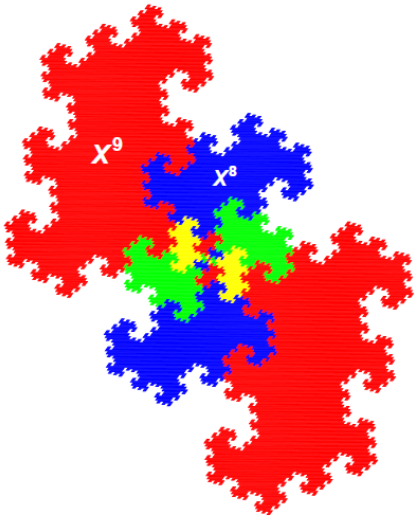


FIG. 8 : Polynômes de degré ≤ 9 pour $X = 1 + i\sqrt{2}$

Proposition 6.10. *Soit $\mathcal{O}$ l'anneau des entiers du corps de nombres $\mathbb{Q}(\sqrt{-2})$.*
(i) $X := 1 + \sqrt{-2}$ est un $\mathbb{S}[\pm 1]$-générateur de $\mathcal{O}$. La clé de $(\mathcal{O}, X)$ est $P(X) = -1 - X + X^2 - X^3$.
(ii) La limite projective $\varprojlim R_m$ est l'anneau $W(\mathbb{F}_3) = \mathbb{Z}_3$.

La figure 8 reproduit le motif obtenu en fournissant en entrée les polynômes de degré ≤ 9. Dans ce cas, l'analogue du lemme 6.9 est vérifié avec la borne $n + 3$ plutôt qu'$n + 2$.

6.3 Anneaux de polynômes à un générateur sur $\mathbb{S}[\mu_{3,+}]$

Dans le prochain exemple, le corps R_1 est le corps fini $\mathbb{F}_4$. On dénote par $\mu_{3,+} \subset \mathbb{C}$ les solutions de $x(x^3 - 1) = 0$, $j = \exp(2\pi i/3)$ et $\mathbb{Z}(j) \subset \mathbb{Q}(j)$ l'anneau des entiers du corps quadratique imaginaire $\mathbb{Q}(j)$.

Proposition 6.11. *(i) Le nombre $-2 \in \mathbb{Z}(j)$ est un $\mathbb{S}[\mu_{3,+}]$-générateur de l'anneau $R = \mathbb{Z}(j)$.*
(ii) La clé est donnée par

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

(iii) Le corps R_1 est le corps fini $\mathbb{F}_4$.
(iv) La limite projective $\varprojlim R_m$ est l'anneau de Witt $W(\mathbb{F}_4)$ et l'anneau R_m est le quotient de $W(\mathbb{F}_4)$ par $2^m\, W(\mathbb{F}_4)$.

Démonstration. Appelons $J = 2\mathbb{Z}(j) \subset \mathbb{Z}(j)$, alors J^n est l'idéal engendré par X^n où $X = -2$. Appelons $\sigma : \mathcal{P}(\mu_3) \to R = \mathbb{Z}(j)$ l'application définie par (5.3). Pour chaque n, la composition $\pi_n \circ \sigma$, à partir du sous-ensemble $\mathcal{P}^{n-1}(\mu_3) \subset \mathcal{P}(\mu_3)$ formé des polynômes de degré $< n$ vers l'anneau quotient $R_n = R/J^n$, est surjective et par conséquent injective puisque les cardinaux de la source et de la cible sont égaux. Il s'ensuit que l'application $\sigma : \mathcal{P}(\mu_3) \to R = \mathbb{Z}(j)$ est injective. Pour montrer qu'elle est surjective, on utilise la méthode générale faisant intervenir la limite des sous-ensembles

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

où F est le domaine fondamental pour $\mathbb{Z}(j)$. On observe que le passage de n à $n + 1$ affecte seulement Z_n sur sa frontière et que Z_n contient un disque ouvert centré en 0.

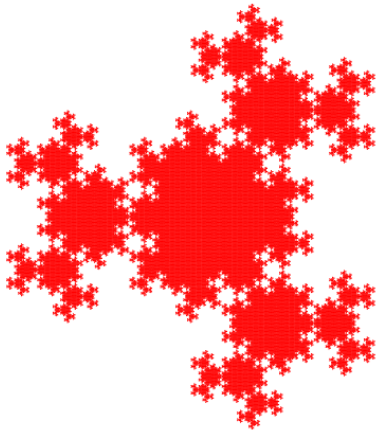


FIG. 9 : Polynômes de degré ≤ 7 pour $X = -2$

6.4 Les anneaux de polynômes à un générateur sur $\mathbb{S}[\mu_{4,+}]$

Proposition 6.12. (*i*) *Le nombre* $X = 1 + 2i$ *est un* $\mathbb{S}[\mu_{4,+}]$*-générateur de l'anneau* $R = \mathbb{Z}(i)$.
(*ii*) *La clé est donnée par* $h(0) = 1$ *et*

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

(*iii*) *Le corps* R_1 *est le corps fini* $\mathbb{F}_5$.
(*iv*) *La limite projective* $\varprojlim R_m$ *est l'anneau de Witt* $W(\mathbb{F}_5) = \mathbb{Z}_5$ *et l'anneau* R_m *est le quotient de* $W(\mathbb{F}_5)$ *par* $5^m\,W(\mathbb{F}_5)$.

Démonstration. Dans le corps p-adique $\mathbb{Z}_5$, il existe une unique racine carrée de -1 égal à 2 modulo 5 (voir [28], §6.7). Soit $\rho : \mathbb{Z}(i) \to \mathbb{Z}_5$ l'unique morphisme tel que, modulo 5, on a $\rho(i) = 2$. Alors $\rho(X) = 5u$ où u est une unité dans $\mathbb{Z}_5$. Le morphisme ρ restreint à $\mu_{4,+} = \{0, 1, i, -1, -i\}$ donne une section multiplicative de l'application quotient $R \to R/XR$. On a $\mathbb{Z}_5/\rho(X)^m\mathbb{Z}_5 = \mathbb{Z}/5^m\mathbb{Z}$ et le morphisme ρ induit un isomorphisme $R_m \simeq \mathbb{Z}_5 = \mathbb{Z}/5^m\mathbb{Z}$. Les assertions (*iii*) et (*iv*) en découlent, ainsi que l'injectivité de l'application $\sigma : \mathcal{P}(\mu_4) \to R = \mathbb{Z}(i)$. On peut prouver la surjectivité de σ comme pour la proposition 6.11 en utilisant la Figure 10. Les assertions (*i*) et (*ii*) s'ensuivent. □

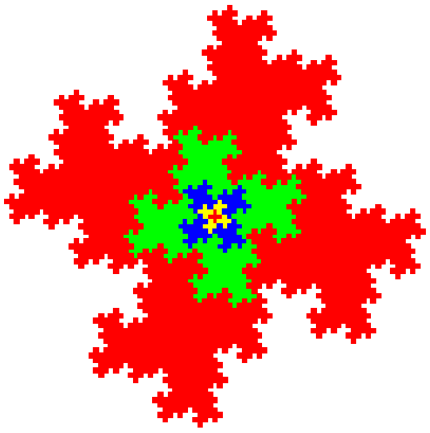


FIG. 10 : Polynômes de degré ≤ 4 pour $X = 1 + 2i$

6.5 Les anneaux de polynômes à un générateur sur $\mathbb{S}[\mu_{6,+}]$

Proposition 6.13. (*i*) *Le nombre* $X = 2 - j$ *est un* $\mathbb{S}[\mu_{6,+}]$*-générateur de l'anneau* $R = \mathbb{Z}(j)$.
(*ii*) *La clé est donnée par* $h(j) = j + 1$, $h(j^2) = j^2 + 1$, $h(0) = 1$ *et*

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

(*iii*) *Le corps* R_1 *est le corps fini* $\mathbb{F}_7$.
(*iv*) *La limite projective* $\varprojlim R_m$ *est l'anneau de Witt* $W(\mathbb{F}_7) = \mathbb{Z}_7$ *et l'anneau* R_m *est le quotient de* $W(\mathbb{F}_7)$ *par* $7^m\, W(\mathbb{F}_7)$.

La preuve peut se déduire de [28], §4.6.

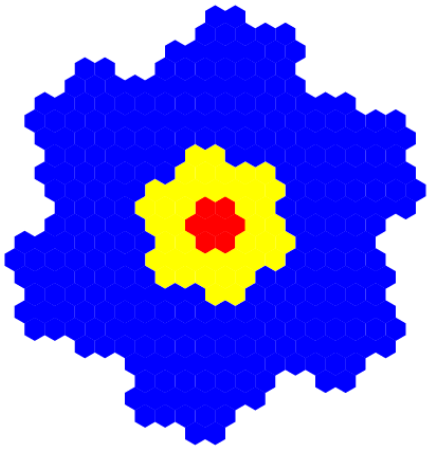


FIG. 11 : Polynômes de degré ≤ 2 pour $X = \frac{5}{2} - \frac{i\sqrt{3}}{2}$

Références

[1] M. F. Atiyah, D.O Tall, *Group representations, λ-rings and the J-homomorphism*. Topology **8** (1969) 253–297. 2

[2] G. Barat, V. Berthé, P. Liardet, J. Thuswaldner, *Dynamical directions in numeration*, Ann. Inst. Fourier (Grenoble) **56** (2006), no. 7, 1987–2092. 1

[3] J. Borger, Λ*-rings and the field with one element*, arXiv :0906.3146 1, 2

[4] J.B. Bost, A. Connes, *Hecke algebras, Type III factors and phase transitions with spontaneous symmetry breaking in number theory*, Selecta Math. (New Series) **1** (1995) no.3, 411–457. 2

[5] 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. 2, 2, 4, 2

[6] A. Connes, C. Consani *On the notion of geometry over* $\mathbb{F}_1$, Journal of Algebraic Geometry **20** no. 3 (2011), 525–557. 3

[7] A. Connes, C. Consani, *Schemes over* $\mathbb{F}_1$ *and zeta functions*, Compositio Mathematica **146** (6), (2010) 1383–1415. 2, 12

[8] A. Connes, C. Consani, *From monoids to hyperstructures : in search of an absolute arithmetic*, dans Casimir Force, Casimir Operators and the Riemann Hypothesis, de Gruyter (2010), 147–198. 2

[9] A. Connes, C. Consani, *Geometry of the Arithmetic Site*. Adv. Math. **291** (2016), 274–329. 1, 2, 2.7, 2.8, 2

[10] A. Connes, C. Consani, *Geometry of the Scaling Site*, Selecta Math. (N.S.) **23** (2017), no. 3, 1803–1850. 2, 2.11

[11] A. Connes, C. Consani, *Absolute algebra and Segal's Gamma sets*, J. Number Theory **162** (2016), 518–551. 1, 3, 5

[12] A. Connes, C. Consani, *On Absolute Algebraic Geometry, the affine case*, Advances in Mathematics, **390**, article no. 107909 (2021). 12

[13] A. Connes, C. Consani, *Riemann-Roch for* $\overline{\mathrm{Spec}\,\mathbb{Z}}$. Bulletin des Sciences Mathématiques **187** (2023). 1, 3, 3.1, 1, 6.2.1

[14] A. Connes, C. Consani, *Riemann-Roch for the ring* $\mathbb{Z}$. Comptes Rendus Mathématiques (à paraître) (2023) 1, 4.2

[15] B. Dundas, T. Goodwillie, R. McCarthy, *The local structure of algebraic K-theory*. Algebra and Applications, 18. Springer-Verlag London, Ltd., London, (2013). 3

[16] W. Gilbert, *Radix representation of quadratic fields*. Journal of Mathematical Analysis and Applications. **83**, 264–274, (1981). 6.1.2

[17] J. Golan, *Semi-rings and their applications*, Version mise à jour et augmentée de The theory of semi-rings, with applications to mathematics and theoretical computer science *Longman Sci. Tech.*, Harlow, 1992. Kluwer Academic Publishers, Dordrecht, (1999). 2, 9

[18] I. Katai, B. Kovacs, *Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen*. Acta Sci. Math. (Szeged) **42** (1980), no. 1-2, 99–107. 6.1.1, 6.1.1

[19] I. Katai, B. Kovacs, *Canonical number systems in imaginary quadratic fields*. Acta Math. Acad. Sci. Hungar. **37** (1981), nos. 1–3, 159–164. 6.1.1, 6.1.1

[20] D. Knuth, *The art of computer programming*. Vol. 2 : Seminumerical algorithms. Troisième édition, Addison-Wesley, (1998). 1, 6

[21] S. Lang, *Algebraic Number Theory*. Addison Wesley, (1970).

[22] https://en.wikipedia.org/wiki/Complex-base_system 6.1.2

[23] Yu.I. Manin, *Lectures on zeta functions and motives (according to Deninger and Kurokawa)*. Columbia University Number Theory Seminar (New York, 1992). Astérisque No. 228 (1995), 4, 121–163. 1, 2, 3

[24] Yu.I. Manin, *Cyclotomy and Analytic Geometry over* F_1. Quanta of maths, 385–408, Clay Math. Proc., **11**, Amer. Math. Soc., Providence, RI, (2010). 2, 2

[25] R. Meyer, *On a representation of the idele class group related to primes and zeros of L-functions*. Duke Math. J. **127** (2005), N.3, 519–595. 4

[26] J. Neukirch, *Algebraic number theory*. Traduit de la version originale en allemand de 1992 et avec une note de Norbert Schappacher. Avec un avant-propos de G. Harder. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, (1999).

[27] 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. 6

[28] A. Robert, *A course in p-adic analysis*. Graduate Texts in Mathematics, **198**, Springer-Verlag, New York, 2000. 6.1.2, 6.1.2, 6.4, 6.5

[29] C. Soulé, *Les variétés sur le corps à un élément*. Mosc. Math. J. **4** (2004), no. 1, 217–244. 2

[30] R. Steinberg, *A geometric approach to the representations of the full linear group over a Galois field*, Transactions of the AMS, **71**, no. 2 (1951), pp. 274–282. 1

[31] J. Tits, *Sur les analogues algébriques des groupes semi-simples complexes*. Colloque d'algèbre supérieure, Bruxelles 19–22 décembre 1956, Centre Belge de Recherches Mathématiques Établissements Ceuterick, Louvain ; Librairie Gauthier-Villars, Paris (1957), 261–289. 1

[32] A. Weil *Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques*, Œuvres scientifiques / Collected papers I. 1926–1951. Springer, Heidelberg, (2014). 1

[33] A. Weil *De la métaphysique aux mathématiques*, Oeuvres scientifiques / Collected papers II. 1951–1964. Springer, Heidelberg, (2014). 1

[34] A. Weil *Basic number theory*. Réimpression de la seconde édition (1973). Classics in Mathematics. Springer-Verlag, Berlin, (1995).

[35] http://solbakkn.com/math/triadic-nums.htm

Alain Connes
COLLÈGE DE FRANCE
3 Rue d'Ulm
F-75005 Paris, France
IHES
35 Rte de Chartres
91440 Bures-sur-Yvette, France
Email : alain@connes.org

Caterina Consani
Département de Mathématiques
UNIVERSITÉ JOHNS HOPKINS
3400 N Charles Street
Baltimore MD 21218, USA
Email : cconsan1@jhu.edu