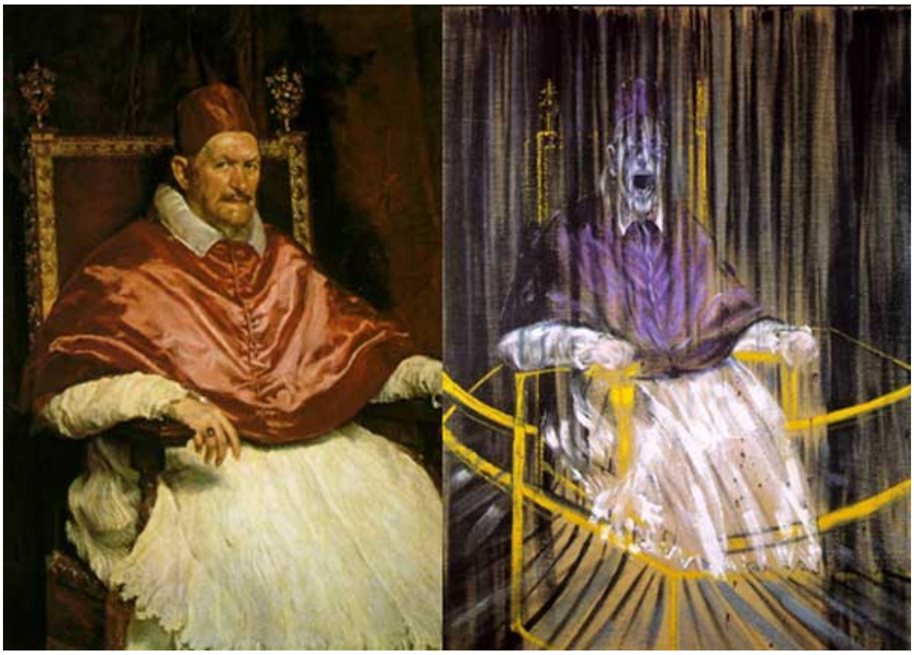
absolute geometry

lieven le bruyn



2011

universiteit antwerpen
neverendingbooks.org

CONTENTS

series 1

BRAVE NEW GEOMETRIES

1.1 Mumford's treasure map

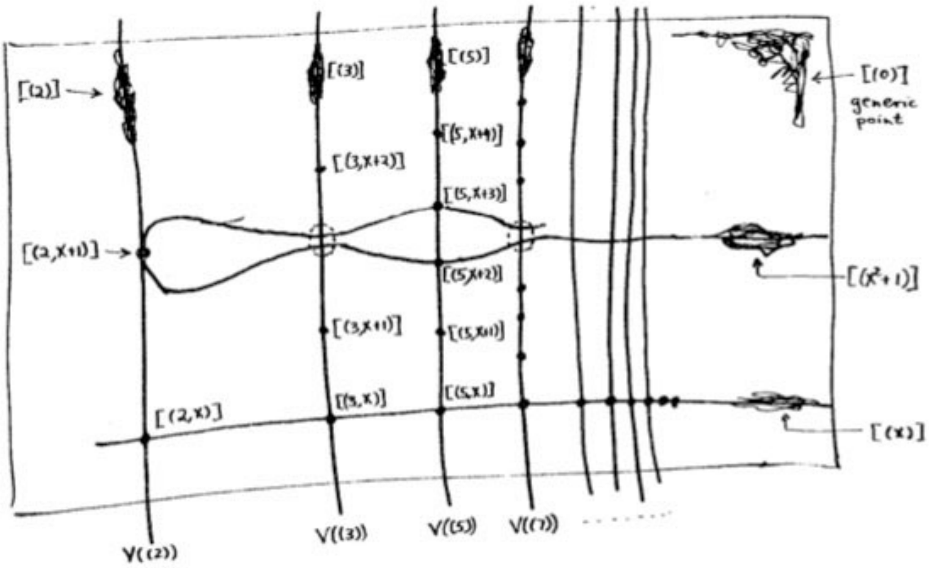
David Mumford did receive earlier this year the 2007 AMS Leroy P. Steele Prize for Mathematical Exposition. The jury honors Mumford for "his beautiful expository accounts of a host of aspects of algebraic geometry". Not surprisingly, the first work they mention are his mimeographed notes of the first 3 chapters of a course in algebraic geometry, usually called "Mumford's red book" because the notes were wrapped in a red cover. In 1988, the notes were reprinted by Springer-Verlag. Unfortunately, the only red they preserved was in the title.

The AMS describes the importance of the red book as follows. "This is one of the few books that attempt to convey in pictures some of the highly abstract notions that arise in the field of algebraic geometry. In his response upon receiving the prize, Mumford recalled that some of his drawings from The Red Book were included in a collection called Five Centuries of French Mathematics. This seemed fitting, he noted: "After all, it was the French who started impressionist painting and isn't this just an impressionist scheme for rendering geometry?""

Fig. 1.1: D. Mumford

These days it is perfectly possible to get a good grasp on difficult concepts from algebraic geometry by reading blogs, watching YouTube or plugging in equations to sophisticated math-programs. In the early seventies though, if you wanted to know what Grothendieck's scheme-revolution was all about you had no choice but to wade through the EGA's and SGA's and they were notorious for being extremely user-unfriendly regarding illustrations...

So the few depictions of schemes available, drawn by people sufficiently fluent in Grothendieck's new geometric language had no less than treasure-map-cult-status and were studied in minute detail. Mumford's red book was a gold mine for such treasure maps. Here's my favorite one, scanned from the original mimeographed notes (it looks somewhat tidier in the Springer-version)



It is the first depiction of $\mathbf{spec}(\mathbb{Z}[x])$, the affine scheme of the ring $\mathbb{Z}[x]$ of all integral polynomials. Mumford calls it the"arithmetic surface" as the picture resembles the one he made before of the affine scheme $\mathbf{spec}(\mathbb{C}[x, y])$ corresponding to the two-dimensional complex affine space $\mathbb{A}^2_{\mathbb{C}}$. Mumford adds that the arithmetic surface is 'the first example which has a real mixing of arithmetic and geometric properties'.

Let's have a closer look at the treasure map. It introduces some new signs which must have looked exotic at the time, but have since become standard tools to depict algebraic schemes.

For starters, recall that the underlying topological space of $\mathbf{spec}(\mathbb{Z}[x])$ is the set of all prime ideals of the integral polynomial ring $\mathbb{Z}[x]$, so the map tries to list them all as well as their inclusions/intersections.

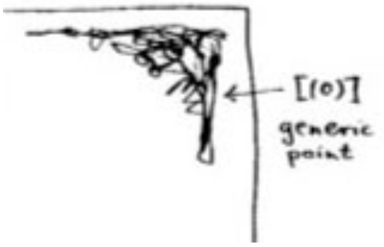
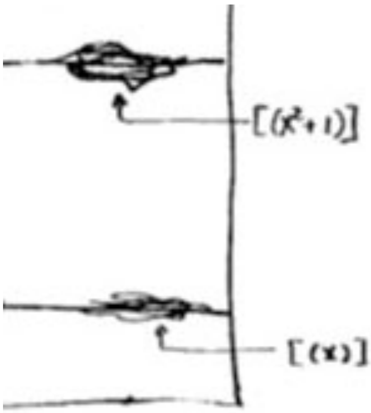


Fig. 1.2: Generic point

The doodle in the right upper corner depicts the 'generic point' of the scheme. That is, the geometric object corresponding to the prime ideal (0) (note that $\mathbb{Z}[x]$ is an integral domain). Because the zero ideal is contained in any other prime ideal, the algebraic/geometric mantra ("inclusions reverse when shifting between algebra and geometry") asserts that the geometric object corresponding to (0) should contain all other geometric objects of the arithmetic plane, so it is just the whole plane! Clearly, it is rather senseless to depict this fact by coloring the whole plane black as then we wouldn't be able to see the finer objects. Mumford's solution to this is to draw a hairy ball, which in this case, is sufficiently thick to include fragments going in every possible direction. In general, one should read these doodles as saying that the geometric object represented by this doodle contains all other objects seen elsewhere in the picture if the hairy-ball-doodle includes stuff pointing in the direction of the smaller object. So, in the case of the object corresponding to (0), the doodle has pointers going everywhere, saying that the geometric object contains all other objects depicted.

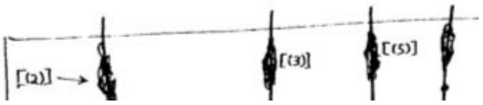
Let's move over to the doodles in the lower right-hand corner.

They represent the geometric object corresponding to principal prime ideals of the form $(p(x))$, where $p(x)$ in an irreducible polynomial over the integers, that is, a polynomial which we cannot write as the product of two smaller integral polynomials. The objects corresponding to such prime ideals should be thought of as 'horizontal' curves in the plane.



The doodles depicted correspond to the prime ideal (x), containing all polynomials divisible by x so when we divide it out we get, as expected, a domain $\mathbb{Z}[x]/(x) \simeq \mathbb{Z}$, and the one corresponding to the ideal (x^2+1), containing all polynomials divisible by x^2+1, which can be proved to be a prime ideals of $\mathbb{Z}[x]$ by observing that after factoring out we get $\mathbb{Z}[x]/(x^2+1) \simeq \mathbb{Z}[i]$, the domain of all Gaussian integers $\mathbb{Z}[i]$. The corresponding doodles (the 'generic points' of the curvy-objects) have a predominant horizontal component as they have the express the fact that they depict horizontal curves in the plane. It is no coincidence that the doodle of (x^2+1) is somewhat bulkier than the one of (x) as the later one must only depict the fact that all points lying on the straight line to its left belong to it, whereas the former one must claim inclusion of all points lying on the 'quadric' it determines.

Apart from these 'horizontal' curves, there are also 'vertical' lines corresponding to the principal prime ideals (p), containing the polynomials, all of which coefficients are divisible by the prime number p. These are indeed prime ideals of $\mathbb{Z}[x]$, because their quotients are $\mathbb{Z}[x]/(p) \simeq (\mathbb{Z}/p\mathbb{Z})[x]$ are domains, being the ring of polynomials over the finite field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. The doodles corresponding to these prime ideals have a predominant vertical component (depicting the 'vertical' lines) and have a uniform thickness for all prime numbers p as each of them only has to claim ownership of the points lying on the vertical line under them.



Right! So far we managed to depict the zero prime ideal (the whole plane) and the principal prime ideals of $\mathbb{Z}[x]$ (the horizontal curves and the vertical lines). Remains to depict the maximal ideals. These are all known to be of the form $\mathfrak{m} = (p, f(x))$ where p is a prime number and $f(x)$ is an irreducible integral polynomial, which remains irreducible when reduced modulo p (that is, if we reduce all coefficients of the integral polynomial $f(x)$ modulo p we obtain an irreducible polynomial in $\mathbb{F}_p[x]$). By the algebra/geometry mantra mentioned before, the geometric object corresponding to such a maximal ideal can be seen as the 'intersection' of an horizontal curve (the object corresponding to the principal prime ideal $(f(x))$) and a vertical line (corresponding to the prime ideal (p)). Because maximal ideals do not contain any other prime ideals, there is no reason to have a doodle associated to $\mathfrak{m}$ and we can just depict it by a "point" in the plane, more precisely the intersection-point of the horizontal curve with the vertical line determined by $\mathfrak{m} = (p, f(x))$. Still, Mumford's treasure map doesn't treat all "points" equally. For ex-

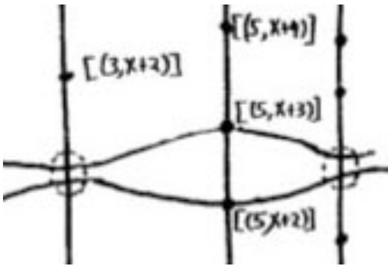


Fig. 1.3: Points

ample, the point corresponding to the maximal ideal $\mathfrak{m}_1 = (3, x+2)$ is depicted by a solid dot ., whereas the point corresponding to the maximal ideal $\mathfrak{m}_2 = (3, x^2+1)$ is represented by a fatter point ◦. The distinction between the two 'points' becomes evident when we look at the corresponding quotients (which we know have to be fields). We have $\mathbb{Z}[x]/\mathfrak{m}_1 = \mathbb{Z}[x]/(3, x+2) = (\mathbb{Z}/3\mathbb{Z})[x]/(x+2) = \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$ whereas $\mathbb{Z}[x]/\mathfrak{m}_2 = \mathbb{Z}[x]/(3, x^2+1) = \mathbb{Z}/3\mathbb{Z}[x]/(x^2+1) = \mathbb{F}_3[x]/(x^2+1) = \mathbb{F}_{3^2}$ because the polynomial x^2+1 remains irreducible over $\mathbb{F}_3$, the quotient $\mathbb{F}_3[x]/(x^2+1)$ is no longer the prime-field $\mathbb{F}_3$ but a quadratic field extension of it, that is, the finite field consisting of 9 elements $\mathbb{F}_{3^2}$. That is, we represent the 'points' lying on the vertical line corresponding to the principal prime ideal (p) by a solid dot . when their quotient (aka residue field is the prime field $\mathbb{F}_p$, by a bigger point ◦ when its residue field is the finite field $\mathbb{F}_{p^2}$, by an even fatter point ◯ when its residue field is $\mathbb{F}_{p^3}$ and so on, and on. The larger the residue field, the 'fatter' the corresponding point.

In fact, the 'fat-point' signs in Mumford's treasure map are an attempt to depict the fact that an affine scheme contains a lot more information than just the set of all prime ideals. In fact, an affine scheme determines (and is determined by) a "functor of points". That is, to every field (or even every commutative ring) the affine scheme assigns the set of its 'points' defined over that field (or ring). For example, the $\mathbb{F}_p$-points of $\mathbf{spec}(\mathbb{Z}[x])$ are the solid . points on the vertical line (p), the $\mathbb{F}_{p^2}$-points of $\mathbf{spec}(\mathbb{Z}[x])$ are the solid . points and the slightly bigger ◦ points on that vertical line, and so on.

This concludes our first attempt to decipher Mumford's drawing, but if we delve a bit deeper, we are bound to find even more treasures...

1.2 Grothendieck's functor of points

A comment-thread well worth following while on vacation was Algebraic Geometry without Prime Ideals at the Secret Blogging Seminar. Peter Woit became [lyric about it :

"My nomination for the all-time highest quality discussion ever held in a blog comment section goes to the comments on this posting at Secret Blogging Seminar, where several of the best (relatively)-young algebraic geometers in the business discuss the foundations of the subject and how it should be taught."

I follow far too few comment-sections to make such a definite statement, but found the contributions by James Borger and David Ben-Zvi of exceptional high quality. They made a case for using Grothendieck's 'functor of points' approach in teaching algebraic geometry instead of the 'usual' approach via prime spectra and their structure sheaves.

Fig. 1.4: A. Grothendieck

The text below was written on december 15th of last year, but never posted. As far as I recall it was meant to be part two of the 'Brave New Geometries'-series starting with the Mumford's treasure map post 1.1. Anyway, it may perhaps serve someone unfamiliar with Grothendieck's functorial approach to make the first few timid steps in that directions.

Allyn Jackson's beautiful account of Grothendieck's life Comme Appele du Neant, part II (the first part of the paper can be found here) contains this gem :

”One striking characteristic of Grothendiecks mode of thinking is that it seemed to rely so little on examples. This can be seen in the legend of the so-called Grothendieck prime. In a mathematical conversation, someone suggested to Grothendieck that they should consider a particular prime number. You mean an actual number? Grothendieck asked. The other person replied, yes, an actual prime number. Grothendieck suggested, All right, take 57. But Grothendieck must have known that 57 is not prime, right? Absolutely not, said David Mumford of Brown University. He doesnt think concretely.

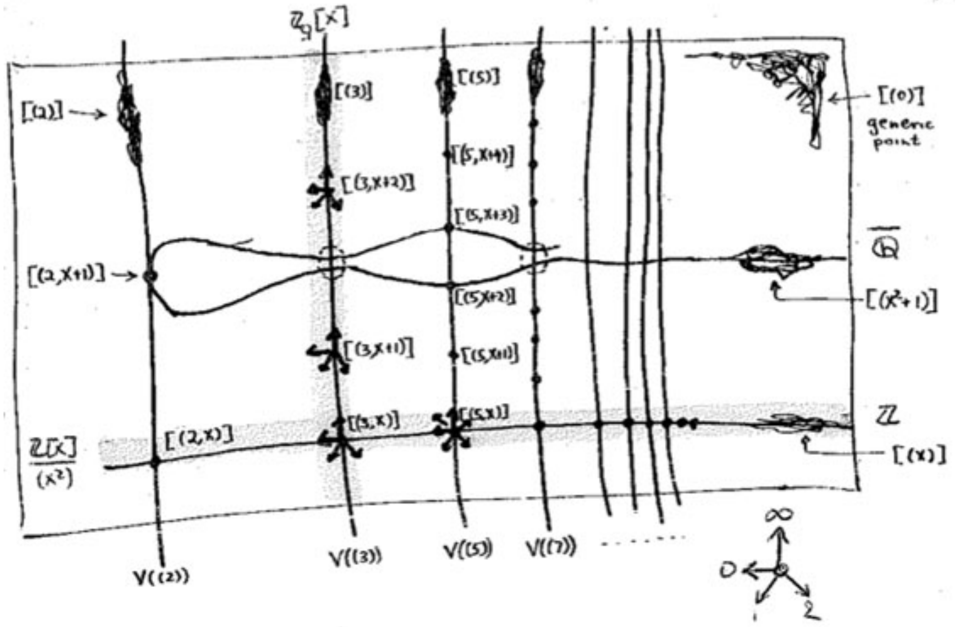
We have seen before how Mumford’s doodles (post 1.1) allow us to depict all ’points’ of the affine scheme $\mathbf{spec}(\mathbb{Z}[x])$, that is, all prime ideals of the integral polynomial ring $\mathbb{Z}[x]$. Perhaps not too surprising, in view of the above story, Alexander Grothendieck pushed the view that one should consider all ideals, rather than just the primes. He achieved this by associating the ’functor of points’ to an affine scheme.

Consider an arbitrary affine integral scheme X with coordinate ring $\mathbb{Z}[X] = \mathbb{Z}[t_1,\ldots,t_n]/(f_1,\ldots,f_k)$, then any ringmorphism $\phi : \mathbb{Z}[t_1,\ldots,t_n]/(f_1,\ldots,f_k) \rightarrow R$ is determined by an n-tuple of elements $(r_1,\ldots,r_n) = (\phi(t_1),\ldots,\phi(t_n))$ from R which must satisfy the polynomial relations $f_i(r_1,\ldots,r_n) = 0$. Thus, Grothendieck argued, one can consider $(r_1,\ldots,r_n)$ an an ’R-point’ of X and all such tuples form a set $h_X(R)$ called the set of R-points of X. But then we have a functor

$$h_X \;:\; \mathtt{comrings} \longrightarrow \mathtt{sets} \qquad R \mapsto h_X(R) = Rings(\mathbb{Z}[t_1,\ldots,t_n]/(f_1,\ldots,f_k), R)$$

So, what is this mysterious functor in the special case of interest to us, that is when $X = \mathbf{spec}(\mathbb{Z}[x])$? Well, in that case there are no relations to be satisfied so any ringmorphism $\mathbb{Z}[x] \rightarrow R$ is fully determined by the image of x which can be any element $r \in R$. That is, $Ring(\mathbb{Z}[x], R) = R$ and therefore Grothendieck’s functor of points $h_{\mathbf{spec}(\mathbb{Z}[x])}$ is nothing but the forgetful functor.

But, surely the forgetful functor cannot give us interesting extra information on Mumford’s drawing? Well, have a look at the slightly extended drawing below :

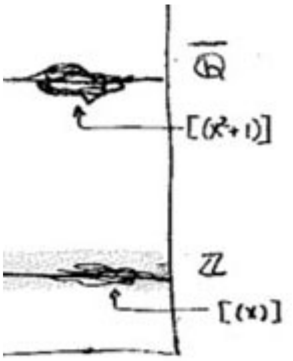


What are these 'smudgy' lines and 'spiky' points? Well, before we come to those let us consider the easier case of identifying the R-points in case R is a domain. Then, for any $r \in R$, the inverse image of the zero prime ideal of R under the ringmap $\phi_r \ : \ \mathbb{Z}[x] \rightarrow R$ must be a prime ideal of $\mathbb{Z}[x]$, that is, something visible in Mumford's drawing. Let's consider a few easy cases :

For starters, what are the $\mathbb{Z}$-points of $\mathbf{spec}(\mathbb{Z}[x])$? Any natural number $n \in \mathbb{Z}$ determines the surjective ringmorphism $\phi_n \ : \ \mathbb{Z}[x] \rightarrow \mathbb{Z}$ identifying $\mathbb{Z}$ with the quotient $\mathbb{Z}[x]/(x-n)$, identifying the 'arithmetic line' $\mathbf{spec}(\mathbb{Z}) = (2),(3),(5),\ldots,(p),\ldots,(0)$ with the horizontal line in $\mathbf{spec}(\mathbb{Z}[x])$ corresponding to the principal ideal $(x-n)$ (such as the indicated line (x)).

When $\mathbb{Q}$ are the rational numbers, then $\lambda = \frac{m}{n}$ with m, n coprime integers, in which case we have $\phi_\lambda^{-1}(0) = (nx - m)$, hence we get again an horizontal line in $\mathbf{spec}(\mathbb{Z}[x])$. For $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$ we have for any λ that $\phi_\lambda^{-1}(0) = (f(x))$ where $f(x)$ is a minimal integral polynomial for which λ is a root. But what happens when $K = \mathbb{C}$ and λ is a trancendental number?

Well, in that case the ringmorphism $\phi_\lambda \ : \ \mathbb{Z}[x] \rightarrow \mathbb{C}$ is injective and therefore $\phi_\lambda^{-1}(0) = (0)$ so we get the whole arithmetic plane! In the case of a finite field $\mathbb{F}_{p^n}$ we have seen that there are 'fat' points in the arithmetic plane, corresponding to maximal ideals $(p, f(x))$ (with $f(x)$ a polynomial of degree n which remains irreducible over $\mathbb{F}_p$), having $\mathbb{F}_{p^n}$ as their residue field. But these are not the only $\mathbb{F}_{p^n}$-points. For, take any element $\lambda \in \mathbb{F}_{p^n}$, then the map ϕ_λ takes $\mathbb{Z}[x]$ to the subfield of $\mathbb{F}_{p^n}$ generated by λ. That is, the $\mathbb{F}_{p^n}$-points of $\mathbf{spec}(\mathbb{Z}[x])$ consists of all fat points with residue field $\mathbb{F}_{p^n}$, together with slightly slimmer points having as their residue field $\mathbb{F}_{p^m}$ where m is a divisor of n. In all, there are precisely p^n (that is, the number of elements of $\mathbb{F}_{p^n}$) such points, as could be expected.



Things become quickly more interesting when we consider R-points for rings containing nilpotent elements.

1.3 Manin's geometric axis

Mumford's drawing (see post 1.1) has a clear emphasis on the vertical direction.

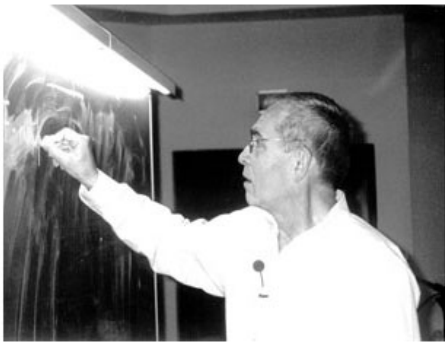
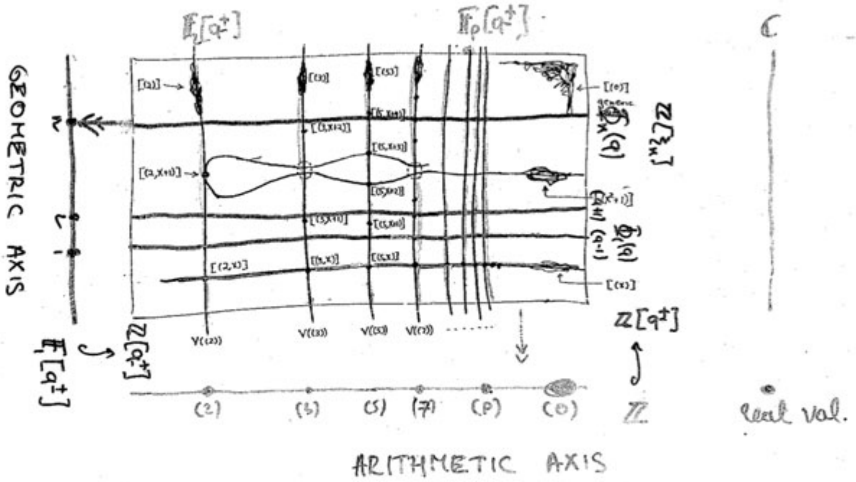


Fig. 1.5: Yu. I. Manin

The set of all vertical lines corresponds to taking the fibers of the natural 'structural morphism' : $\pi \ : \ \mathbf{spec}(\mathbb{Z}[t]) \rightarrow \mathbf{spec}(\mathbb{Z})$ coming from the inclusion $\mathbb{Z} \subset \mathbb{Z}[t]$.

That is, we consider the intersection $P \cap \mathbb{Z}$ of a prime ideal $P \subset \mathbb{Z}[t]$ with the subring of constants. Two options arise : either $P \cap \mathbb{Z} \neq 0$, in which case the intersection is a principal prime ideal (p) for some prime number p (and hence P itself is bigger or equal to $p\mathbb{Z}[t]$ whence its geometric object is contained in the vertical line $\mathbb{V}((p))$, the fiber $\pi^{-1}((p))$ of the structural morphism over (p)), or, the intersection $P \cap \mathbb{Z}[t] = 0$ reduces to the zero ideal (in which case the extended prime ideal $P\mathbb{Q}[x] = (q(x))$ is a principal ideal of the rational polynomial algebra $\mathbb{Q}[x]$, and hence the geometric object corresponding to P is a horizontal curve in Mumford's drawing, or is the whole arithmetic plane itself if $P = 0$).

Because we know already that any 'point' in Mumford's drawing corresponds to a maximal ideal of the form $\mathfrak{m} = (p, f(x))$ (see [last time][1]), we see that every point lies on precisely one of the set of all vertical coordinate axes corresponding to the prime numbers $\mathbb{V}((p)) = \mathbf{spec}(\mathbb{F}_p[x]) = \pi^{-1}((p))$. In particular, two different vertical lines do not intersect (or, in ringtheoretic lingo, the 'vertical' prime ideals $p\mathbb{Z}[x]$ and $q\mathbb{Z}[x]$ are comaximal for different prime numbers $p \neq q$).



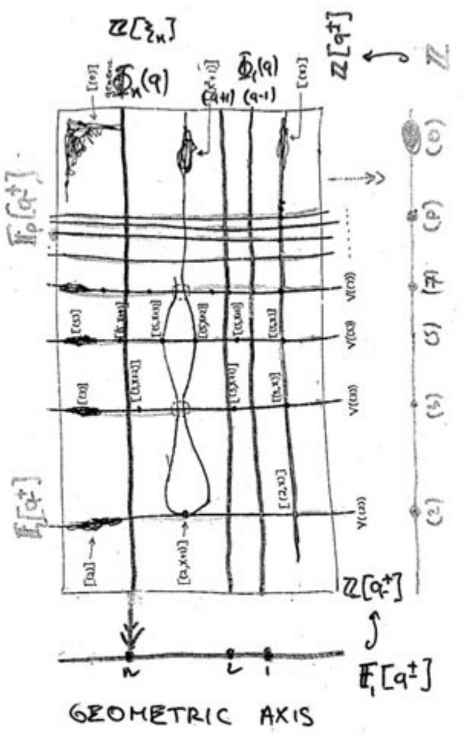
That is, the structural morphism is a projection onto the "arithmetic axis" (which is $\mathbf{spec}(\mathbb{Z})$) and we get the above picture. The extra vertical line to the right of the picture is there because in arithmetic geometry it is customary to include also the archimedean valuations and hence to consider the 'compactification' of the arithmetic axis $\mathbf{spec}(\mathbb{Z})$ which is $\overline{\mathbf{spec}(\mathbb{Z})} = \mathbf{spec}(\mathbb{Z}) \cup v_{\mathbb{R}}$.

Yuri I. Manin is advocating for years the point that we should take the terminology 'arithmetic surface' for $\mathbf{spec}(\mathbb{Z}[x])$ a lot more seriously. That is, there ought to be, apart from the projection onto the 'z-axis' (that is, the arithmetic axis $\mathbf{spec}(\mathbb{Z})$) also a projection onto the 'x-axis' which he calls the 'geometric axis'.

But then, what are the 'points' of this geometric axis and what are their fibers under this second projection?

We have seen above that the vertical coordinate line over the prime number (p) coincides with $\mathbf{spec}(\mathbb{F}_p[x])$, the affine line over the finite field $\mathbb{F}_p$. But all of these different lines, for varying primes p, should project down onto the same geometric axis. Manin's idea was to take therefore as the geometric axis the affine line $\mathbf{spec}(\mathbb{F}_1[x])$, over the virtual field with one element, which should be thought of as being the limit of the finite fields $\mathbb{F}_p$ when p goes to one!

How many points does $\mathbf{spec}(\mathbb{F}_1[x])$ have? Over a virtual object one can postulate whatever one wants and hope for an a posteriori explanation. $\mathbb{F}_1$-gurus tell us that there should be exactly one point of size n on the affine line over $\mathbb{F}_1$, corresponding to the unique degree n field extension $\mathbb{F}_{1^n}$. However, it is difficult to explain this from the limiting perspective...



Over a genuine finite field $\mathbb{F}_p$, the number of points of thickness n (that is, those for which the residue field is isomorphic to the degree n extension $\mathbb{F}_{p^n}$) is equal to the number of monic irreducible polynomials of degree n over $\mathbb{F}_p$. This number is known to be $\frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})p^d$ where $\mu(k)$ is the Moebius function. But then, the limiting number should be $\frac{1}{n}\sum_{d|n}\mu(\frac{n}{d}) = \delta_{n1}$, that is, there can only be one point of size one...

Alternatively, one might consider the zeta function counting the number N_n of ideals having a quotient consisting of precisely p^n elements. Then, we have for genuine finite fields $\mathbb{F}_p$ that $\zeta(\mathbb{F}_p[x]) = \sum_{n=0}^{\infty} N_n t^n = 1+pt+p^2t^2+p^3t^3+\ldots$, whence in the limit it should become $1+t+t^2+t^3+\ldots$ and there is exactly one ideal in $\mathbb{F}_1[x]$ having a quotient of cardinality n and one argues that this unique quotient should be the unique point with residue field $\mathbb{F}_{1^n}$ (though it might make more sense to view this as the unique n-fold extension of the unique size-one point $\mathbb{F}_1$ corresponding to the quotient $\mathbb{F}_1[x]/(x^n)$...)

A perhaps more convincing reasoning goes as follows. If $\overline{\mathbb{F}_p}$ is an algebraic closure of the finite field $\mathbb{F}_p$, then the points of the affine line over $\overline{\mathbb{F}_p}$ are in one-to-one correspondence with the maximal ideals of $\overline{\mathbb{F}_p}[x]$ which are all of the form $(x-\lambda)$ for $\lambda \in \overline{\mathbb{F}_p}$. Hence, we get the points of the affine line over the basefield $\mathbb{F}_p$ as the orbits of points over the algebraic closure under the action of the Galois group $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.

'Common wisdom' has it that one should identify the algebraic closure of the field with one element $\overline{\mathbb{F}_1}$ with the group of all roots of unity μ_∞ and the corresponding Galois group $Gal(\overline{\mathbb{F}_1}/\mathbb{F}_1)$ as being generated by the power-maps $\lambda \to \lambda^n$ on the roots of unity. But then there is exactly one orbit of length n given by the n-th roots of unity μ_n, so there should be exactly one point of thickness n in $\mathbf{spec}(\mathbb{F}_1[x])$ and we should then identity the corresponding residue field as $\mathbb{F}_{1^n} = \mu_n$.

Whatever convinces you, let us assume that we can identify the non-generic points of $\mathbf{spec}(\mathbb{F}_1[x])$ with the set of positive natural numbers $1,2,3,\ldots$ with n denoting the unique size n point with residue field $\mathbb{F}_{1^n}$. Then, what are the fibers of the projection onto the geometric axis $\phi\ :\ \mathbf{spec}(\mathbb{Z}[x]) \to \mathbf{spec}(\mathbb{F}_1[x]) = 1,2,3,\ldots$?

These fibers should correspond to 'horizontal' principal prime ideals of $\mathbb{Z}[x]$. Manin proposes to consider $\phi^{-1}(n) = \mathbb{V}((\Phi_n(x)))$ where $\Phi_n(x)$ is the n-th cyclotomic polynomial. The nice thing about this proposal is that all closed points of $\mathbf{spec}(\mathbb{Z}[x])$ lie on one of these fibers!

Indeed, the residue field at such a point (corresponding to a maximal ideal $\mathfrak{m} = (p, f(x))$) is the finite field $\mathbb{F}_{p^n}$ and as all its elements are either zero or an p^n-1-th root of unity, it does lie on the curve determined by $\Phi_{p^n-1}(x)$.

As a consequence, the localization $\mathbb{Z}[x]_{cycl}$ of the integral polynomial ring $\mathbb{Z}[x]$ at the multiplicative system generated by all cyclotomic polynomials is a principal ideal domain (as all height two primes evaporate in the localization), and, the fiber over the generic point of $\mathbf{spec}(\mathbb{F}_1[x])$ is $\mathbf{spec}(\mathbb{Z}[x]_{cycl})$, which should be compared to the fact that the fiber of the generic point in the projection onto the arithmetic axis is $\mathbf{spec}(\mathbb{Q}[x])$ and $\mathbb{Q}[x]$ is the localization of $\mathbb{Z}[x]$ at the multiplicative system generated by all prime numbers).

Hence, both the vertical coordinate lines and the horizontal 'lines' contain all closed points of the arithmetic plane. Further, any such closed point $\mathfrak{m} = (p, f(x))$ lies on the intersection of a vertical line $\mathbb{V}((p))$ and a horizontal one $\mathbb{V}((\Phi_{p^n-1}(x)))$ (if $deg(f(x)) = n$). That is, these horizontal and vertical lines form a coordinate system, at least for the closed points of $\mathbf{spec}(\mathbb{Z}[x])$.

Still, there is a noticeable difference between the two sets of coordinate lines. The vertical lines do not intersect meaning that $p\mathbb{Z}[x] + q\mathbb{Z}[x] = \mathbb{Z}[x]$ for different prime numbers p and q. However, in general the principal prime ideals corresponding to the horizontal lines $(\Phi_n(x))$ and $(\Phi_m(x))$ are not comaximal when $n \neq m$, that is, these 'lines' may have points in common! This will lead to an exotic new topology on the roots of unity... (to be continued).

1.4 Mazur's knotty dictionary

In the previous posts, we have depicted the 'arithmetic line', that is the prime numbers, as a 'line' and individual primes as 'points'.

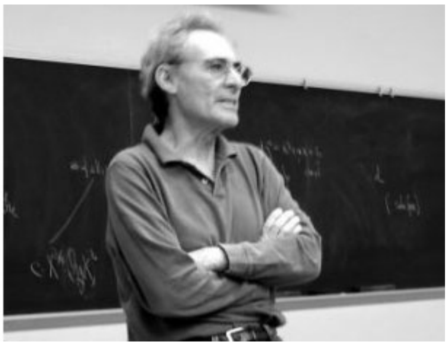


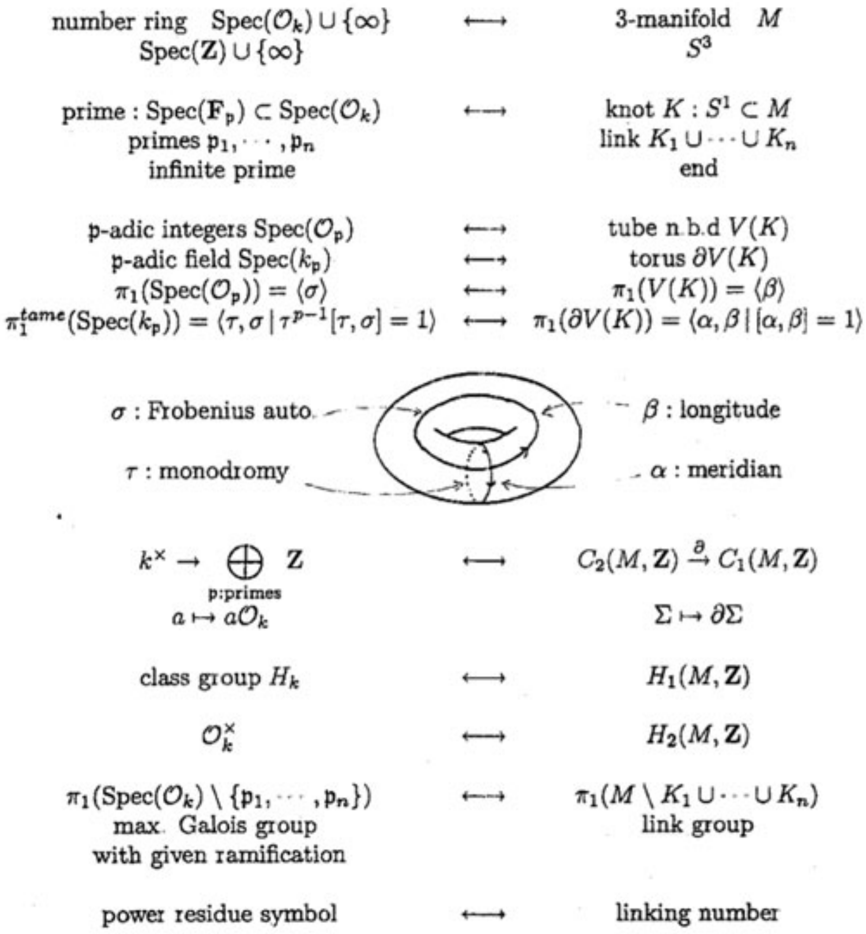
Fig. 1.6: B. Mazur

However, sometime in the roaring 60-ties, Barry Mazur launched the crazy idea of viewing the affine spectrum of the integers, $\mathbf{spec}(\mathbb{Z})$, as a 3-dimensional manifold and prime numbers themselves as knots in this 3-manifold...

After a long silence, this idea was taken up recently by Mikhail Kapranov and Alexander Reznikov (1960-2003) in a talk at the MPI-Bonn in august 1996. Pieter Moree tells the story in his recollections about Alexander (Sacha) Reznikov in Sipping Tea with Sacha :

"Sasha's paper is closely related to his paper where the analogy of covers of three-manifolds and class field theory plays a big role (an analogy that was apparently first noticed by B. Mazur). Sasha and Mikhail Kapranov (at the time also at the institute) were both very interested in this analogy. Eventually, in August 1996, Kapranov and Reznikov both lectured on this (and I explained in about 10 minutes my contribution to Reznikov's proof). I was pleased to learn some time ago that this lecture series even made it into the literature, see Morishita's 'On certain analogies between knots and primes' J. reine angew. Math 550 (2002) 141-167."

Here's a part of what is now called the *Kapranov-Reznikov-Mazur dictionary* :



number ring $\mathrm{Spec}(\mathcal{O}_k) \cup \{\infty\}$ $\mathrm{Spec}(\mathbf{Z}) \cup \{\infty\}$	$\longleftrightarrow$	3-manifold M S^3
prime : $\mathrm{Spec}(\mathbf{F}_\mathfrak{p}) \subset \mathrm{Spec}(\mathcal{O}_k)$ primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ infinite prime	$\longleftrightarrow$	knot $K : S^1 \subset M$ link $K_1 \cup \cdots \cup K_n$ end
$\mathfrak{p}$-adic integers $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$	$\longleftrightarrow$	tube n.b.d $V(K)$
$\mathfrak{p}$-adic field $\mathrm{Spec}(k_\mathfrak{p})$	$\longleftrightarrow$	torus $\partial V(K)$
$\pi_1(\mathrm{Spec}(\mathcal{O}_\mathfrak{p})) = \langle \sigma \rangle$	$\longleftrightarrow$	$\pi_1(V(K)) = \langle \beta \rangle$
$\pi_1^{tame}(\mathrm{Spec}(k_\mathfrak{p})) = \langle \tau, \sigma \mid \tau^{p-1}[\tau, \sigma] = 1 \rangle$	$\longleftrightarrow$	$\pi_1(\partial V(K)) = \langle \alpha, \beta \mid [\alpha, \beta] = 1 \rangle$
σ : Frobenius auto.		β : longitude
τ : monodromy		α : meridian
$k^\times \to \bigoplus_{\mathfrak{p}:\text{primes}} \mathbf{Z}$ $a \mapsto a\mathcal{O}_k$	$\longleftrightarrow$	$C_2(M, \mathbf{Z}) \xrightarrow{\partial} C_1(M, \mathbf{Z})$ $\Sigma \mapsto \partial\Sigma$
class group H_k	$\longleftrightarrow$	$H_1(M, \mathbf{Z})$
$\mathcal{O}_k^\times$	$\longleftrightarrow$	$H_2(M, \mathbf{Z})$
$\pi_1(\mathrm{Spec}(\mathcal{O}_k) \setminus \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\})$ max. Galois group with given ramification	$\longleftrightarrow$	$\pi_1(M \setminus K_1 \cup \cdots \cup K_n)$ link group
power residue symbol	$\longleftrightarrow$	linking number

What is the rationale behind this dictionary? Well, it all has to do with trying to make sense of the (algebraic) fundamental group $\pi_1^{alg}(X)$ of a general scheme X. Recall that for a manifold M there are two different ways to define its fundamental group $\pi_1(M)$: either as the closed loops in a given basepoint upto homotopy or as the automorphism group of the universal cover $\tilde{M}$ of M.

For an arbitrary scheme the first definition doesn't make sense but we can use the second one as we have a good notion of a (finite) cover : an etale morphism $Y \rightarrow X$ of the scheme X. As they form an inverse system, we can take their finite automorphism groups $Aut_X(Y)$ and take their projective limit along the system and call this the algebraic fundamental group $\pi_1^{alg}(X)$.

Hendrik Lenstra has written beautiful course notes on 'Galois theory for schemes' on all of this starting from scratch. Besides, there are also two video-lectures available on this at the MSRI-website : Etale fundamental groups 1 by H.W. Lenstra and Etale fundamental groups 2 by F. Pop.

But, what is the connection with the 'usual' fundamental group in case both of them can be defined? Well, by construction the algebraic fundamental group is always a profinite group and in the case of manifolds it coincides with the profinite completion of the standard fundamental group, that is, $\pi_1^{alg}(M) \simeq \widehat{\pi_1(M)}$ (recall that the cofinite completion is the projective limit of all finite group quotients).

Right, so all we have to do to find a topological equivalent of an algebraic scheme is to compute its algebraic fundamental group and find an existing topological space of which the profinite completion of its standard fundamental group coincides with our algebraic fundamental group. An example : a prime number p (as a 'point' in $\mathbf{spec}(\mathbb{Z})$) is the closed subscheme $\mathbf{spec}(\mathbb{F}_p)$ corresponding to the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. For any affine scheme of a field K, the algebraic fundamental group coincides with the absolute Galois group $Gal(\overline{K}/K)$. In the case of $\mathbb{F}_p$ we all know that this absolute Galois group is isomorphic with the profinite integers $\hat{\mathbb{Z}}$. Now, what is the first topological space coming to mind having the integers as its fundamental group? Right, the circle S^1. Hence, in arithmetic topology we view prime numbers as topological circles, that is, as knots in some bigger space.

But then, what is this bigger space? That is, what is the topological equivalent of $\mathbf{spec}(\mathbb{Z})$? For this we have to go back to Mazur's original paper Notes on etale cohomology of number fields in which he gives an Artin-Verdier type duality theorem for the affine spectrum $X = \mathbf{spec}(D)$ of the ring of integers D in a number field. More precisely, there is a non-degenerate pairing $H^r_{et}(X,F) \times Ext^{3-r}_X(F,\mathbb{G}_m) \rightarrow H^3_{et}(X,F) \simeq \mathbb{Q}/\mathbb{Z}$ for any constructible abelian sheaf F. This may not tell you much, but it is a 'sort of' Poincare-duality result one would have for a compact three dimensional manifold.

Ok, so in particular $\mathbf{spec}(\mathbb{Z})$ should be thought of as a 3-dimensional compact manifold, but which one? For this we have to compute the algebraic fundamental group. Fortunately, this group is trivial as there are no (non-split) etale covers of $\mathbf{spec}(\mathbb{Z})$, so the corresponding 3-manifold should be simple connected... but we now know that this has to imply that the manifold must be S^3, the 3-sphere! Summarizing : in arithmetic topology, prime numbers are knots in the 3-sphere!

More generally (by the same arguments) the affine spectrum $\mathbf{spec}(D)$ of a ring of integers can be thought of as corresponding to a closed oriented 3-dimensional manifold M (which is a cover of S^3) and a prime ideal $\mathfrak{p} \triangleleft D$ corresponds to a knot in M.

But then, what is an ideal $\mathfrak{a} \triangleleft D$? Well, we have unique factorization of ideals in D, that is, $\mathfrak{a} = \mathfrak{p}_1^{n_1} \ldots \mathfrak{p}_k^{n_k}$ and therefore $\mathfrak{a}$ corresponds to a link in M of which the constituent knots are the ones corresponding to the prime ideals $\mathfrak{p}_i$.

And we can go on like this. What should be an element $w \in D$? Well, it will be an embedded surface $S \rightarrow M$, possibly with a boundary, the boundary being the link corresponding to the ideal $\mathfrak{a} = Dw$ and Seifert's algorithm tells us how we can produce surfaces having any prescribed link as its boundary. But then, in particular, a unit $w \in D^*$ should correspond to a closed surface in M.

And all these analogies carry much further : for example the class group of the ring of integers $Cl(D)$ then corresponds to the torsion part $H_1(M,\mathbb{Z})_{tor}$ because principal ideals Dw are trivial in the class group, just as boundaries of surfaces ∂S vanish in $H_1(M,\mathbb{Z})$. Similarly, one may identify the unit group D^* with $H_2(M,\mathbb{Z})$... and so on, and on, and on...

More links to papers on arithmetic topology can be found in John Baez' week 257 or via here.

1.5 Conway's big picture

Conway and Norton showed that there are exactly 171 moonshine functions and associated two arithmetic subgroups to them. We want a tool to describe these and here's where Conway's big picture comes in very handy. All moonshine groups are arithmetic groups, that is, they are commensurable with the modular group. Conway's idea is to view several of these groups as point- or set-wise stabilizer subgroups of finite sets of (projective) commensurable 2-dimensional lattices.

Fig. 1.7: J.H. Conway, S. Norton

Expanding (and partially explaining) the original moonshine observation of McKay and Thompson, John Conway and Simon Norton formulated monstrous moonshine :

To every cyclic subgroup $\langle m \rangle$ of the Monster $\mathbb{M}$ is associated a function

$f_m(\tau) = \frac{1}{q} + a_1 q + a_2 q^2 + \ldots$ with $q = e^{2\pi i \tau}$ and all coefficients $a_i \in \mathbb{Z}$ are characters at m of a representation of $\mathbb{M}$. These representations are the homogeneous components of the so called Moonshine module.

Each f_m is a principal modulus for a certain genus zero congruence group commensurable with the modular group $\Gamma = PSL_2(\mathbb{Z})$. These groups are called the moonshine groups.

Conway and Norton showed that there are exactly 171 different functions f_m and associated two arithmetic subgroups $F(m) \subset E(m) \subset PSL_2(\mathbb{R})$ to them (in most cases, but not all, these two groups coincide).

Whereas there is an extensive literature on subgroups of the modular group (see for instance the series of posts starting here), most moonshine groups are *not* contained in the modular group. So, we need a tool to describe them and here's where *Conway's big picture* comes in very handy.

All moonshine groups are arithmetic groups, that is, they are subgroups G of $PSL_2(\mathbb{R})$ which are *commensurable* with the modular group $\Gamma = PSL_2(\mathbb{Z})$ meaning that the intersection $G \cap \Gamma$ is of finite index in both G and in Γ. Conway's idea is to view several of these groups as point- or set-wise stabilizer subgroups of finite sets of (projective) commensurable 2-dimensional lattices.

Start with a fixed two dimensional lattice $L_1 = \mathbb{Z}e_1 + \mathbb{Z}e_2 = \langle e_1, e_2 \rangle$ and we want to name all lattices of the form $L = \langle v_1 = ae_1 + be_2, v_2 = ce_1 + de_2 \rangle$ that are commensurable to L_1. Again this means that the intersection $L \cap L_1$ is of finite index in both lattices. From this it follows immediately that all coefficients a, b, c, d are rational numbers.

It simplifies matters enormously if we do not look at lattices individually but rather at projective equivalence classes, that is $L = \langle v_1, v_2 \rangle \sim L' = \langle v_1', v_2' \rangle$ if there is a rational number $\lambda \in \mathbb{Q}$ such that $\lambda v_1 = v_1', \lambda v_2 = v_2'$. Further, we are of course allowed to choose a different 'basis' for our lattices, that is, $L = \langle v_1, v_2 \rangle = \langle w_1, w_2 \rangle$ whenever $(w_1, w_2) = (v_1, v_2).\gamma$ for some $\gamma \in PSL_2(\mathbb{Z})$. Using both operations we can get any lattice in a specific form. For example,

$$\langle \tfrac{1}{2}e_1 + 3e_2, e_1 - \tfrac{1}{3}e_2 \overset{(1)}{=} \langle 3e_1 + 18e_2, 6e_1 - 2e_2 \rangle \overset{(2)}{=} \langle 3e_1 + 18e_2, 38e_2 \rangle \overset{(3)}{=} \langle \tfrac{3}{38}e_1 + \tfrac{9}{19}e_2, e_2 \rangle$$

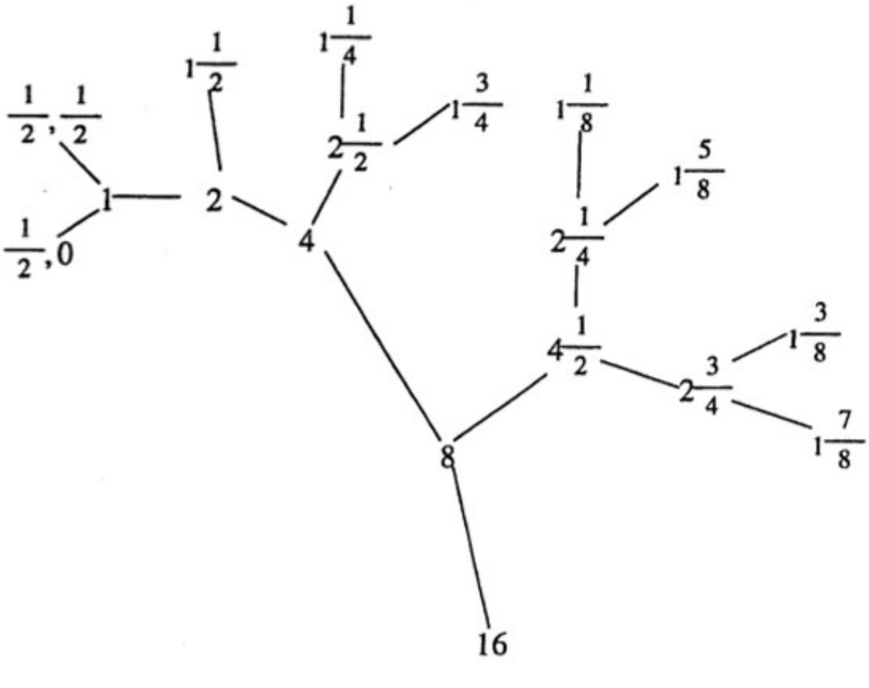
Here, identities (1) and (3) follow from projective equivalence and identity (2) from a base-change. In general, any lattice L commensurable to the standard lattice L_1 can be rewritten uniquely as $L = \langle Me_1 + \frac{g}{h}e_2, e_2 \rangle$ where M a positive rational number and with $0 \leq \frac{g}{h} < 1$.

Another major feature is that one can define a symmetric *hyper-distance* between (equivalence classes of) such lattices. Take $L = \langle Me_1 + \frac{g}{h}e_2, e_2 \rangle$ and $L' = \langle Ne_1 + \frac{i}{j}e_2, e_2 \rangle$ and consider the matrix

$D_{LL'} = \begin{bmatrix} M & \frac{g}{h} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} N & \frac{i}{j} \\ 0 & 1 \end{bmatrix}^{-1}$ and let α be the smallest positive rational number such that all entries of the matrix $\alpha.D_{LL'}$ are integers, then

$\delta(L, L') = det(\alpha.D_{LL'}) \in \mathbb{N}$ defines a symmetric hyperdistance which depends only of the equivalence classes of lattices (**hyper**distance because the log of it behaves like an ordinary distance).

Conway's big picture is the graph obtained by taking as its vertices the equivalence classes of lattices commensurable with L_1 and with edges connecting any two lattices separated by a *prime* number hyperdistance. Here's part of the 2-picture, that is, only depicting the edges of hyperdistance 2.



The 2-picture is an infinite 3-valent tree as there are precisely 3 classes of lattices at hyperdistance 2 from any lattice $L = \langle v_1, v_2 \rangle$ namely (the equivalence classes of) $\langle \frac{1}{2}v_1, v_2 \rangle$, $\langle v_1, \frac{1}{2}v_2 \rangle$ and $\langle \frac{1}{2}(v_1 + v_2), v_2 \rangle$.

Similarly, for any prime hyperdistance p, the p-picture is an infinite p+1-valent tree and the *big picture* is the product over all these prime trees. That is, two lattices at square-free hyperdistance $N = p_1 p_2 \dots p_k$ are two corners of a k-cell in the big picture! (Astute readers of this blog (if such people exist...) may observe that Conway's big picture did already appear here prominently, though in disguise. More on this another time).

The big picture presents a simple way to look at arithmetic groups and makes many facts about them visually immediate. For example, the point-stabilizer subgroup of L_1 clearly is the modular group $PSL_2(\mathbb{Z})$. The point-stabilizer of any other lattice is a certain conjugate of the modular group inside $PSL_2(\mathbb{R})$. For example, the stabilizer subgroup of the lattice $L_N = \langle Ne_1, e_2 \rangle$ (at hyperdistance N from L_1) is the subgroup

$$\begin{bmatrix} a & \frac{b}{N} \\ Nc & d \end{bmatrix} \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in PSL_2(\mathbb{Z})$$

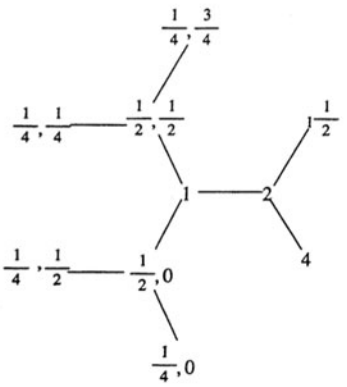


Fig. 1.8: the 4-ball

Now the intersection of these two groups is the modular subgroup $\Gamma_0(N)$ (consisting of those modular group element whose lower left-hand entry is divisible by N). That is, the proper way to look at this arithmetic group is as the joint stabilizer of the two lattices L_1, L_N. The picture makes it trivial to compute the index of this subgroup.

Consider the ball $B(L_1, N)$ with center L_1 and hyper-radius N (on the left, the ball with hyper-radius 4). Then, it is easy to show that the modular group acts transitively on the boundary lattices (including the lattice L_N), whence the index $[\Gamma : \Gamma_0(N)]$ is just the number of these boundary lattices. For N=4 the picture shows that there are exactly 6 of them. In general, it follows from our knowledge of all the p-trees the number of all lattices at hyperdistance N from L_1 is equal to $N \prod_{p|N}(1+\frac{1}{p})$, in accordance with the well-known index formula for these modular subgroups!

But, there are many other applications of the big picture giving a simple interpretation for the Hecke operators, an elegant proof of the Atkin-Lehner theorem on the normalizer of $\Gamma_0(N)$ (the whimsical source of appearances of the number 24) and of Helling's theorem characterizing maximal arithmetical groups inside $PSL_2(\mathbb{C})$ as conjugates of the normalizers of $\Gamma_0(N)$ for square-free N. J.H. Conway's paper "Understanding groups like $\Gamma_0(N)$" containing all this material is a must-read! Unfortunately, I do not know of an online version.

1.6 Langlands versus Connes

This is a belated response to a Math-Overflow exchange between Thomas Riepe and Chandan Singh Dalawat asking for a possible connection between Connes' noncommutative geometry approach to the Riemann hypothesis and the Langlands program.

Here's the punchline : a large chunk of the Connes-Marcolli book Noncommutative Geometry, Quantum Fields and Motives can be read as an exploration of the noncommutative boundary to the Langlands program (at least for GL_1 and GL_2 over the rationals $\mathbb{Q}$).

Recall that Langlands for GL_1 over the rationals is the correspondence, given by the Artin reciprocity law, between on the one hand the abelianized absolute Galois group

$$Gal(\overline{\mathbb{Q}}/\mathbb{Q})^{ab} = Gal(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^*$$

and on the other hand the connected components of the idele classes

$$\mathbb{A}^*_{\mathbb{Q}}/\mathbb{Q}^* = \mathbb{R}^*_+ \times \hat{\mathbb{Z}}^*$$

The locally compact Abelian group of idele classes can be viewed as the nice locus of the horrible quotient space of adele classes $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}^*$. There is a well-defined map

$$\mathbb{A}'_{\mathbb{Q}}/\mathbb{Q}^* \rightarrow \mathbb{R}_+ \qquad (x_\infty, x_2, x_3, \ldots) \mapsto |x_\infty| \prod |x_p|_p$$

from the subset $\mathbb{A}'_{\mathbb{Q}}$ consisting of adeles of which almost all terms belong to $\mathbb{Z}^*_p$. The inverse image of this map over $\mathbb{R}^*_+$ are precisely the idele classes $\mathbb{A}^*_{\mathbb{Q}}/\mathbb{Q}^*$. In this way one can view the adele classes as a closure, or 'compactification', of the idele classes.

This is somewhat reminiscent of extending the nice action of the modular group on the upper-half plane to its badly behaved action on the boundary as in the Manin-Marcolli cave post.

The topological properties of the fiber over zero, and indeed of the total space of adele classes, are horrible in the sense that the discrete group $\mathbb{Q}^*$ acts ergodic on it, due to the irrationality of $log(p_1)/log(p_2)$ for primes p_i. All this is explained well (in the semi-local case, that is using $\mathbb{A}'_Q$ above) in the Connes-Marcolli book (section 2.7).

In much the same spirit as non-free actions of reductive groups on algebraic varieties are best handled using stacks, such ergodic actions are best handled by the tools of noncommutative geometry. That is, one tries to get at the geometry of $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}^*$ by studying an associated non-commutative algebra, the skew-ring extension of the group-ring of the adeles by the action of $\mathbb{Q}^*$ on it. This algebra is known to be Morita equivalent to the Bost-Connes algebra which is the algebra featuring in Connes' approach to the Riemann hypothesis.

It shouldn't thus come as a major surprise that one is able to recover the other side of the Langlands correspondence, that is the Galois group $Gal(\mathbb{Q}(\mu_\infty)/\mathbb{Q})$, from the Bost-Connes algebra as the symmetries of certain states.

In a similar vein one can read the Connes-Marcolli GL_2-system (section 3.7 of their book) as an exploration of the noncommutative closure of the Langlands-space $GL_2(\mathbb{A}_{\mathbb{Q}})/GL_2(\mathbb{Q})$.

series 2

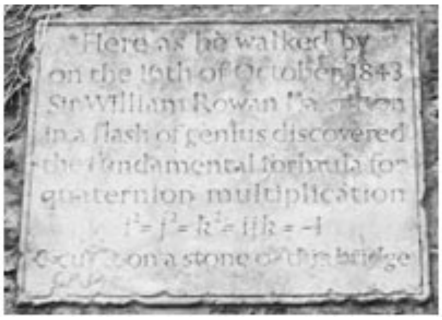
THE ABSOLUTE POINT

2.1 Ceci n'est pas un corps

To Gavin Wraiht a mathematical phantom is a ”nonexistent entity which ought to be there but apparently is not; but nevertheless obtrudes its effects so convincingly that one is forced to concede a broader notion of existence”. Mathematics' history is filled with phantoms getting the kiss of life.

Nobody will deny the ancient Greek were pretty good at maths, but still they were extremely unsure about the status of zero as a number. They asked themselves, ”How can nothing be something?”, and, paradoxes such as of Zeno's depend in large part on that uncertain interpretation of zero. It lasted until the 9th century before Indian scholars were comfortable enough to treat 0 just as any other number.

Italian gamblers/equation-solvers of the early 16th century were baffled by the fact that the number of solutions to quartic equations could vary, seemingly arbitrary, from zero to four until Cardano invented 'imaginary numbers' and showed that there were invariably four solutions provided one allows these imaginary or 'phantom' numbers.


Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication
$i^2 = j^2 = k^2 = ijk = -1$
& cut it on a stone of this bridge

Similar paradigm shifts occurred in mathematics much more recently, for example the discovery of the quaternions by William Hamilton. This object had all the telltale signs of a field-extension of the complex numbers, apart from the fact that the multiplication of two of its numbers a.b did not necessarily give you the same result as multiplying the other way around b.a.

Hamilton was so shaken by this discovery (which he made while walking along the Royal canal in Dublin with his wife on october 16th 1843) that he carved the equations using his penknife into the side of the nearby Broom Bridge (which Hamilton called Brougham Bridge), for fear he would forget it. Today, no trace of the carving remains, though a stone plaque does commemorate the discovery. It reads :

” Here as he walked by, on the 16th of October 1843 , Sir William Rowan Hamilton ,in a flash of genius discovered , the fundamental formula for , quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ & cut it on a stone of this bridge”

The fact that this seems to be the least visited tourist attraction in Dublin tells a lot about the standing of mathematics in society. Fortunately, some of us go to extreme lengths making a pilgrimage to Hamilton's bridge...

Ceci n'est pas une pipe.

In short, the discovery of mathematical objects such as 0, the square root of -1, quaternions or octonions, often allow us to make great progress in mathematics at the price of having to bend the existing rules slightly.

But, to suggest seriously that an unobserved object should exist when even the most basic arguments rule against its existence is a different matter entirely.

Probably, you have to be brought up in the surrealistic tradition of artists such as Renee Magritte, a guy who added below a drawing of a pipe a sentence saying ”This is not a pipe” (Ceci n’est pas une pipe). In short, you have to be Belgian...

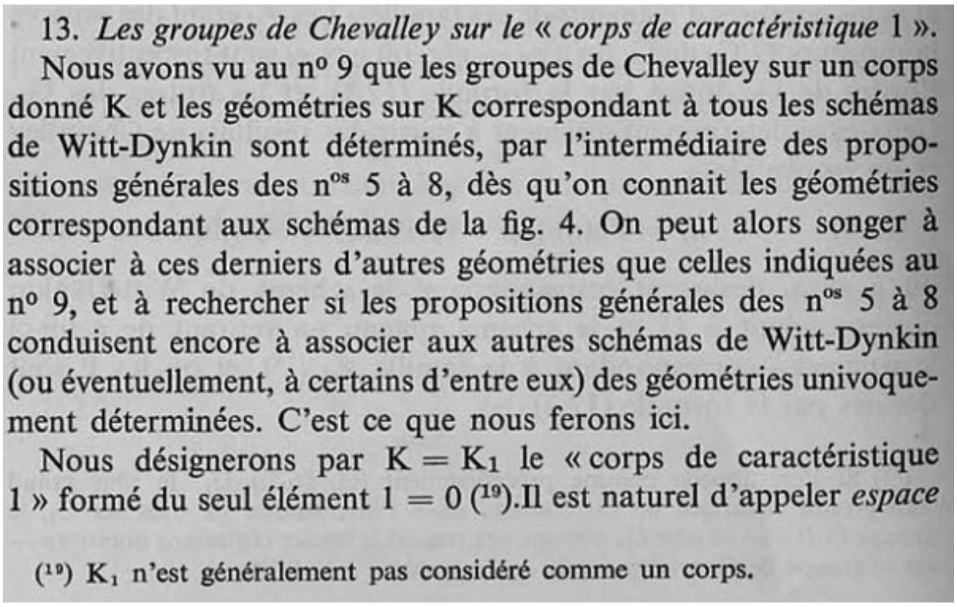
Jacques Tits was a Belgian (today he is a citizen of a far less surrealistic country : France). He is the ’man from Uccle’ (in Mark Ronan’s bestselling Symmetry and the Monster), the guy making finite size replicas of infinite Lie groups. But also the guy who didn’t want to stop there.

Fig. 2.1: J. Tits

He managed to replace the field of complex numbers $\mathbb{C}$ by a finite field $\mathbb{F}_q$, consisting of precisely $q = p^n$ a prime-power elements, but wondered what this group might become if q were to go down to size 1, even though everyone knew that there couldn’t be a field $\mathbb{F}_1$ having just one element as $0 \neq 1$ and these two numbers have to be in any fields DNA.

Tits convinced himself that this elusive field had to exists because his limit-groups had all the characteristics of a finite group co-existing with a Lie group, its companion the Weyl group. Moreover, he was dead sure that the finite geometry associated to his versions of Lie groups would also survive the limit process and give an entirely new combinatorial geometry, featuring objects called ’buildings’ containing ’appartments’ glued along ’walls’ and more terms a real-estate agent might use, but surely not a mathematician...

At the time he was a researcher with the Belgian national science foundation and, having served that agency twenty years myself, I know he had to tread carefully not to infuriate the more traditional committee-members that have to decide on your grant-application every other year. So, when he put his thoughts in writing



13. *Les groupes de Chevalley sur le « corps de caractéristique* 1 ».

Nous avons vu au n$^{\text{o}}$ 9 que les groupes de Chevalley sur un corps donné K et les géométries sur K correspondant à tous les schémas de Witt-Dynkin sont déterminés, par l'intermédiaire des propositions générales des n$^{\text{os}}$ 5 à 8, dès qu'on connait les géométries correspondant aux schémas de la fig. 4. On peut alors songer à associer à ces derniers d'autres géométries que celles indiquées au n$^{\text{o}}$ 9, et à rechercher si les propositions générales des n$^{\text{os}}$ 5 à 8 conduisent encore à associer aux autres schémas de Witt-Dynkin (ou éventuellement, à certains d'entre eux) des géométries univoquement déterminées. C'est ce que nous ferons ici.

Nous désignerons par $K = K_1$ le « corps de caractéristique 1 » formé du seul élément $1 = 0$ [19].Il est naturel d'appeler *espace*

[19] K_1 n'est généralement pas considéré comme un corps.

he added a footnote saying : "K_1 isn't generally considered a field". I'm certain he was doing a Magritte :

$\mathbb{F}_1$ (as we call today his elusive field K_1) ceci n'est pas un corps

2.2 Looking for $\mathbb{F}_1$

There are only a handful of human activities where one goes to extraordinary lengths to keep a dream alive, in spite of overwhelming evidence : religion, theoretical physics, supporting the Belgian football team and ... mathematics.

In recent years several people spend a lot of energy looking for properties of an elusive object : *the field with one element* $\mathbb{F}_1$, or in French : "F-un". The topic must have reached a level of maturity as there was a conference dedicated entirely to it : NONCOMMUTATIVE GEOMETRY AND GEOMETRY OVER THE FIELD WITH ONE ELEMENT.

Fig. 2.2: B. Riemann

In this series I'd like to find out what the fuss is all about, why people would like it to exist and what it has to do with noncommutative geometry. However, before we start two remarks :

The field $\mathbb{F}_1$ *does not exist*, so don't try to make sense of sentences such as "The field with one element is the free algebraic monad generated by one constant (p.26), or the universal generalized ring with zero (p.33)" in the wikipedia-entry. The simplest proof is that in any (unitary) ring we have $0 \neq 1$ so any ring must contain at least two elements. A more highbrow version : the ring of integers $\mathbb{Z}$ is the initial object in the category of unitary rings, so it cannot be an algebra over anything else.

The second remark is that several people have already written blog-posts about $\mathbb{F}_1$. Here are a few I know of : David

Corfield at the n-category cafe and at his old blog, Noah Snyder at the secret blogging seminar, Kea at the Arcadian functor, AC and K. Consani at Noncommutative geometry and John Baez wrote about it in his weekly finds.

The dream we like to keep alive is that we will prove the Riemann hypothesis one fine day by lifting Weil's proof of it in the case of curves over finite fields to rings of integers.

Even if you don't know a word about Weil's method, if you think about it for a couple of minutes, there are two immediate formidable problems with this strategy.

For most people this would be evidence enough to discard the approach, but, we mathematicians have found extremely clever ways for going into denial.

The first problem is that if we want to think of $\mathbf{spec}(\mathbb{Z})$ (or rather its completion adding the infinite place) as a curve over some field, then $\mathbb{Z}$ must be an algebra over this field. However, no such field can exist...

No problem! If there is no such field, let us invent one, and call it $\mathbb{F}_1$. But, it is a bit hard to do geometry over an illusory field. Christophe Soule succeeded in defining varieties over $\mathbb{F}_1$ in a talk at the 1999 Arbeitstagung and in a more recent write-up of it : Les varietes sur le corps a un element.

Fig. 2.3: Ch. Soulé

We will come back to this in more detail later, but for now, here's the main idea. Consider an existent field k and an algebra $k \to R$ over it. Now study the properties of the functor (extension of scalars) from k-schemes to R-schemes. Even if there is no morphism $\mathbb{F}_1 \to \mathbb{Z}$, let us assume it exists and define $\mathbb{F}_1$-varieties by requiring that these guys should satisfy the properties found before for extension of scalars on schemes defined over a field by going to schemes over an algebra (in this case, $\mathbb{Z}$-schemes). Roughly speaking this defines $\mathbb{F}_1$-schemes as subsets of points of suitable $\mathbb{Z}$-schemes.

But, this is just one half of the story. He adds to such an $\mathbb{F}_1$-variety extra topological data 'at infinity', an idea he attributes to J.-B. Bost. This added feature is a $\mathbb{C}$-algebra $\mathcal{A}_X$, which does not necessarily have to be commutative. He only writes : ”Par ignorance, nous resterons tres evasifs sur les proprietes requises sur cette $\mathbb{C}$-algebre.”

Fig. 2.4: A. Connes

The algebra $\mathcal{A}_X$ originates from trying to bypass the second major obstacle with the Weil-Riemann-strategy. On a smooth projective curve all points look similar as is clear for example by noting that the completions of all local rings are isomorphic to the formal power series $k[[x]]$ over the basefield, in particular there is no distinction between 'finite' points and those lying at 'infinity'.

The completions of the local rings of points in $\mathbf{spec}(\mathbb{Z})$ on the other hand are completely different, for example, they have residue fields of different characteristics... Still, local class field theory asserts that their quotient fields have several common features. For example, their Brauer groups are all isomorphic to $\mathbb{Q}/\mathbb{Z}$. However, as $Br(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ and $Br(\mathbb{C}) = 0$, even then there would be a clear distinction between the finite primes and the place at infinity... Alain Connes came up with an extremely elegant solution to bypass this problem in Noncommutative geometry and the Riemann zeta function. He proposes to replace finite dimensional central simple algebras in the definition of the Brauer group by AF (for Approximately Finite dimensional)-central simple algebras over $\mathbb{C}$. This is the origin and the importance of the Bost-Connes algebra.

We will come back to most of this in more detail later, but for the impatient, Connes has written a paper together with Caterina Consani and Matilde Marcolli Fun with $\mathbb{F}_1$ relating the Bost-Connes algebra to the field with one element.

2.3 The $\mathbb{F}_1$ folklore

All esoteric subjects have their own secret (sacred) texts. If you opened the Da Vinci Code (or even better, the original The Holy blood and the Holy grail) you will known about a mysterious collection of documents, known as the ”Dossiers secrets”, deposited in the Bibliothèque nationale de France on 27 April 1967, which is rumored to contain the mysteries of the Priory of Sion, a secret society founded in the middle ages and still active today...

Fig. 2.5: Yu. I. Manin

The followers of F-un, for $\mathbb{F}_1$ the field of one element, have their own collection of semi-secret texts, surrounded by whispers, of which they try to decode every single line in search of enlightenment. Fortunately, you do not have to search the shelves of the Bibliotheque National in Paris, but the depths of the internet to find them as huge, bandwidth-unfriendly, scanned documents.

The first are the lecture notes ”Lectures on zeta functions and motives” by Yuri I. Manin based on a course given in 1991.

One can download a scanned version of the paper from the homepage of Katia Consani as a huge 23.1 Mb file. Of F-un relevance is the first section ”Absolute Motives?” in which ”...we describe a highly speculative picture of analogies between arithmetics over $\mathbb{F}_q$ and over $\mathbb{Z}$, cast in the language reminiscent of Grothendieck's motives. We postulate the existence of a category with tensor product × whose objects correspond not only to the divisors of the Hasse-Weil zeta functions of schemes over $\mathbb{Z}$, but also to Kurokawa's tensor divisors. This neatly leads to the introduction of an ”absolute Tate motive” $\mathbb{T}$, whose zeta function is $\frac{s-1}{2\pi}$, and whose zeroth power is ”the absolute point” which is the base for Kurokawa's direct products. We add some speculations about the role of $\mathbb{T}$ in the ”algebraic geometry over a one-element field”, and in clarifying the structure of the gamma factors at infinity.” (loc.cit. p 1-2)

I'd welcome links to material explaining this section to people knowing no motives.

The second one is the unpublished paper ”Cohomology determinants and reciprocity laws : number field case” by Mikhail Kapranov and A. Smirnov. This paper features in blog-posts at the Arcadian Functor, in John Baez' Weekly Finds and in yesterday's post at Noncommutative Geometry.

You can download every single page (of 15) as a separate file from here. But, in order to help spreading the Fun-gospel, I've made these scans into a single PDF-file which you can download as a 2.6 Mb PDF. In the introduction they say :

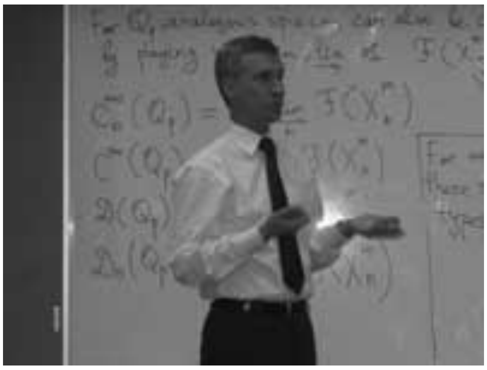


Fig. 2.6: M. Kapranov

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

They manage to deduce higher reciprocity laws in class field theory within the theory of $\mathbb{F}_1$ and its field extensions $\mathbb{F}_{1^n}$. But first, let us explain how they define linear algebra over these *absolute fields*.

Here is a first principle : *in doing linear algebra over these fields, there is no additive structure but only scalar multiplication by field elements.*

So, what are vector spaces over the field with one element? Well, as scalar multiplication with 1 is just the identity map, we have that a vector space is just a set. Linear maps are just set-maps and in particular, a linear isomorphism of a vector space onto itself is a permutation of the set. That is, linear algebra over $\mathbb{F}_1$ is the same as combinatorics of (finite) sets.

A vector space over $\mathbb{F}_1$ is just a set; the dimension of such a vector space is the cardinality of the set. The general linear group $GL_n(\mathbb{F}_1)$ is the symmetric group S_n, the identification via permutation matrices (having exactly one 1 in every row and column).

Some people prefer to view an $\mathbb{F}_1$ vector space as a *pointed set*, the special element being the 'origin' 0 but as $\mathbb{F}_1$ does not have a zero, there is also no zero-vector. Still, in later applications (such as defining exact sequences and quotient spaces) it is helpful to have an origin. So, let us denote for any set S by $S^\bullet = S \cup 0$. Clearly, linear maps between such 'extended' spaces must be maps of pointed sets, that is, sending $0 \to 0$.

The field with one element $\mathbb{F}_1$ has a field extension of degree n for any natural number n which we denote by $\mathbb{F}_{1^n}$ and using the above notation we will define this field as :

$\mathbb{F}_{1^n} = \mu_n^\bullet$ with μ_n the group of all n-th roots of unity. Note that if we choose a primitive n-th root ϵ_n, then $\mu_n \simeq C_n$ is the cyclic group of order n.

Now what is a vector space over $\mathbb{F}_{1^n}$? Recall that we only demand units of the field to act by scalar multiplication, so each 'vector' $\vec{v}$ determines an n-set of linear dependent vectors $\epsilon_n^i \vec{v}$. In other words, any $\mathbb{F}_{1^n}$-vector space is of the form $V^\bullet$ with V a set of which the group μ_n acts freely. Hence, V has $N = d.n$ elements and there are exactly d orbits for the action of μ_n by scalar multiplication. We call d the *dimension* of the vectorspace and a *basis* consists in choosing one representant for every orbits. That is, $B = b_1, \ldots, b_d$ is a basis if (and only if) $V = \epsilon_n^j b_i \ : \ 1 \leq i \leq d, 1 \leq j \leq n$.

So, vectorspaces are free μ_n-sets and hence linear maps $V^\bullet \to W^\bullet$ is a μ_n-map $V \to W$. In particular, a linear isomorphism of V, that is an element of $GL_d(\mathbb{F}_{1^n})$ is a μ_n bijection sending any basis element $b_i \to \epsilon_n^{j(i)} b_{\sigma(i)}$ for a permutation $\sigma \in S_d$.

An $\mathbb{F}_{1^n}$-vectorspace $V^\bullet$ is a free μ_n-set V of $N = n.d$ elements. The dimension $dim_{\mathbb{F}_{1^n}}(V^\bullet) = d$ and the general linear group $GL_d(\mathbb{F}_{1^n})$ is the wreath product of S_d with $\mu_n^{\times d}$, the identification as matrices with exactly one non-zero entry (being an n-th root of unity) in every row and every column. This may appear as a rather sterile theory, so let us give an extremely important example, which will lead us to our second principle for developing absolute linear algebra.

Let $q = p^k$ be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. Assume that $q \cong 1\ mod(n)$. It is well known that the group of units $\mathbb{F}_q^*$ is cyclic of order $q-1$ so by the assumption we can identify μ_n with a subgroup of $\mathbb{F}_q^*$.

Then, $\mathbb{F}_q = (\mathbb{F}_q^*)^\bullet$ is an $\mathbb{F}_{1^n}$-vectorspace of dimension $d = \frac{q-1}{n}$. In other words, $\mathbb{F}_q$ is an $\mathbb{F}_{1^n}$-algebra. But then, any ordinary $\mathbb{F}_q$-vectorspace of dimension e becomes (via restriction of scalars) an $\mathbb{F}_{1^n}$-vector space of dimension $\frac{e(q-1)}{n}$.

Next time we will introduce more linear algebra definitions (including determinants, exact sequences, direct sums and tensor products) in the realm the absolute fields $\mathbb{F}_{1^n}$ and remark that we have to alter the known definitions as we can only use the scalar-multiplication. To guide us, we have the second principle : *all traditional results of linear algebra over $\mathbb{F}_q$ must be recovered from the new definitions under the vector-space identification $\mathbb{F}_q = (\mathbb{F}_q^*)^\bullet = \mathbb{F}_{1^n}$ when $n = q-1$.* (to be continued)

2.4 Absolute linear algebra

Today we will define some basic linear algebra over the absolute fields $\mathbb{F}_{1^n}$ following the Kapranov-Smirnov document. Recall from last time (see post 2.3) that $\mathbb{F}_{1^n} = \mu_n^\bullet$ and that a d-dimensional vectorspace over this field is a pointed set $V^\bullet$ where V is a free μ_n-set consisting of n.d elements. Note that in absolute linear algebra we are not allowed to have addition of vectors and have to define everything in terms of scalar multiplication (or if you want, the μ_n-action). In the hope of keeping you awake, we will include an F-un interpretation of the power residue symbol.

Direct sums of vectorspaces are defined via $V^\bullet \oplus W^\bullet = (V \bigsqcup W)^\bullet$, that is, correspond to the disjoint union of free μ_n-sets. Consequently we have that $dim(V^\bullet \oplus W^\bullet) = dim(V^\bullet) + dim(W^\bullet)$.

For tensor-product we start with $V^\bullet \times W^\bullet = (V \times W)^\bullet$ the vectorspace corresponding to the Cartesian product of free μ_n-sets. If the dimensions of $V^\bullet$ and $W^\bullet$ are respectively d and e, then $V \times W$ consists of n.d.n.e elements, so is of dimension n.d.e. In order to have a sensible notion of tensor-products we have to eliminate the n-factor. We do this by identifying (x, y) with $(\epsilon_n x, \epsilon^{-1} y)$ and call the corresponding vectorspace $V^\bullet \otimes W^\bullet$. If we denote the image of (x, y) by $x \otimes w$ then the identification merely says we can pull the μ_n-action through the tensor-sign, as we'd like to do. With this definition we do indeed have that $dim(V^\bullet \otimes W^\bullet) = dim(V^\bullet)dim(W^\bullet)$.

Fig. 2.7: Gauss

Recall that any linear automorphism A of an $\mathbb{F}_{1^n}$ vectorspace $V^\bullet$ with basis $b_1, \ldots, b_d$ (representants of the different μ_n-orbits) is of the form $A(b_i) = \epsilon_n^{k_i} b_{\sigma(i)}$ for some powers of the primitive n-th root of unity ϵ_n and some permutation $\sigma \in S_d$. We define the determinant $det(A) = \prod_{i=1}^d \epsilon_n^{k_i}$. One verifies that the determinant is multiplicative and independent of the choice of basis.

For example, scalar-multiplication by ϵ_n gives an automorphism on any d-dimensional $\mathbb{F}_{1^n}$-vectorspace $V^\bullet$ and the corresponding determinant clearly equals $det = \epsilon_n^d$. That is, the det-functor remembers *the dimension modulo n*. These mod-n features are a recurrent theme in absolute linear algebra. Another example, which will become relevant when we come to reciprocity laws :

Take $n = 2$. Then, a $\mathbb{F}_{1^2}$ vectorspace $V^\bullet$ of dimension d is a set consisting of 2d elements V equipped with a free involution. Any linear automorphism $A : V^\bullet \to V^\bullet$ is represented by a $d \times d$ matrix having one nonzero entry in every row and column being equal to +1 or -1. Hence, the determinant $det(A) \in \{+1, -1\}$.

On the other hand, by definition, the linear automorphism A determines a permutation $\sigma_A \in S_{2d}$ on the 2d non-zero elements of $V^\bullet$. The connection between these two interpretations is that $det(A) = sgn(\sigma_A)$ the determinant gives the sign of the permutation!

For a prime power $q = p^k$ with $q \equiv 1 \; mod(n)$, [we have seen][2] that the roots of unity $\mu_n \subset \mathbb{F}_q^*$ and hence that $\mathbb{F}_q$ is a vectorspace over $\mathbb{F}_{1^n}$. For any field-unit $a \in \mathbb{F}_q^*$ we have the *power residue symbol*

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

On the other hand, multiplication by a is a linear automorphism on the $\mathbb{F}_{1^n}$-vectorspace $\mathbb{F}_q$ and hence we can look at its F-un determinant $det(a\times)$. The F-un interpretation of a classical lemma by Gauss asserts that the power residue symbol equals $det(a\times)$.

An $\mathbb{F}_{1^n}$-subspace $W^\bullet$ of a vectorspace $V^\bullet$ is a subset $W \subset V$ consisting of full μ_n-orbits. Normally, in defining a *quotient space* we would say that two V-vectors are equivalent when their difference belongs to W and take equivalence classes. However, in absolute linear algebra we are not allowed to take linear combinations of vectors...

The only way out is to define $(V/W)^\bullet$ to correspond to the free μ_n-set (V/W) obtained by identifying all elements of W with the zero-element in $V^\bullet$. But... this will screw-up things if we want to interpret $\mathbb{F}_q$-vectorspaces as $\mathbb{F}_{1^n}$-spaces whenever $q \equiv 1 \; mod(n)$.

For this reason, Kapranov and Smirnov invent the notion of an *equivalence* $f : X^\bullet \to Y^\bullet$ between $\mathbb{F}_{1^n}$-spaces to be a linear map (note that this means a set-theoretic map $X \to Y^\bullet$ such that the inverse image of 0 consists of full μ_n-orbits and is a μ_n-map elsewhere) satisfying the properties that $f^{-1}(0) = 0$ and for every element $y \in Y$ we have that the number of pre-images $f^{-1}(y)$ is congruent to 1 modulo n. Observe that under an equivalence $f : X^\bullet \to Y^\bullet$ we have that $dim(X^\bullet) \equiv dim(Y^\bullet) \; mod(n)$.

This then allows us to define an *exact sequence* of $\mathbb{F}_{1^n}$-vectorspaces to be

$$\begin{tikzcd} 0 \arrow[r] & V_1^\bullet \arrow[r, "\alpha"] & V^\bullet \arrow[r, "\beta"] & V_2^\bullet \arrow[r] & 0 \end{tikzcd}$$

with α a set-theoretic inclusion, the composition $\beta \circ \alpha$ to be the zero-map and with the additional assumption that the map induced by β

$$(V/V_1)^\bullet \to V_2^\bullet$$

is an equivalence. For an exact sequence of spaces as above we have the congruence relation on their dimensions $dim(V_1) + dim(V_2) \equiv dim(V) \; mod(n)$.

More importantly, if as before $q \equiv 1 \; mod(n)$ and we use the embedding $\mu_n \subset \mathbb{F}_q^*$ to turn usual $\mathbb{F}_q$-vectorspaces into absolute $\mathbb{F}_{1^n}$-spaces, then an ordinary exact sequence of $\mathbb{F}_q$-vectorspaces remains exact in the above definition.

2.5 Andre Weil on the Riemann hypothesis

Don't be fooled by introductory remarks to the effect that 'the field with one element was conceived by Jacques Tits half a century ago, etc. etc.'

While this is a historic fact, and, Jacques Tits cannot be given enough credit for bringing a touch of surrealism into mathematics, but this is not the main drive for people getting into $\mathbb{F}_1$, today.

There is a much deeper and older motivation behind most papers published recently on $\mathbb{F}_1$. Few of the authors will be willing to let you in on the secret, though, because if they did, it would sound much too presumptuous...

So, let's have it out into the open : $\mathbb{F}_1$-*mathematics' goal is no less than proving the Riemann Hypothesis*.

And even then, authors hide behind a smoke screen. The 'official' explanation being "we would like to copy Weil's proof of the Riemann hypothesis in the case of function fields of curves over finite fields, by considering $\mathtt{spec}(\mathbb{Z})$ as a 'curve' over an algebra 'dessous' $\mathbb{Z}$ namely $\mathbb{F}_1$". Alas, at this moment, none of the geometric approaches over the field with one element can make this stick.

Believe me for once, the main Jugendtraum of most authors is to get a grip on cyclotomy over $\mathbb{F}_1$. It is no accident that Connes makes a dramatic pause in his YouTubeVideo to let the viewer see this equation on the backboard

$$\mathbb{F}_{1^n} \otimes_{\mathbb{F}_1} \mathbb{Z} = \mathbb{Z}[x]/(x^n - 1)$$

But, what is the basis of all this childlike enthusiasm? A somewhat concealed clue is given in the introduction of the Kapranov-Smirnov paper. They write :

"In [?] the affine line over $\mathbb{F}_1$ was considered; it consists formally of 0 and all the roots of unity. Put slightly differently, this leads to the consideration of "algebraic extensions" of $\mathbb{F}_1$. By analogy with genuine finite fields we would like to think that there is exactly one such extension of any given degree n, denote it by $\mathbb{F}_{1^n}$.

Of course, $\mathbb{F}_{1^n}$ does not exist in a rigorous sense, but we can think if a scheme X contains n-th roots of unity, then it is defined over $\mathbb{F}_{1^n}$, so that there is a morphism

$$p_X \; : \; X \rightarrow \mathtt{spec}(\mathbb{F}_{1^n})$$

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

Fig. 2.8: A. Weil

Okay, so rush down to your library, pick out the first of three volumes of Andre Weil's collected works, look up his letter to Emil Artin written on July 10th 1942 (19 printed pages!), and head for the final section. Weil writes :

"Our proof of the Riemann hypothesis (in the function field case, red.) depended upon the extension of the function-fields by roots of unity, i.e. by constants; the way in which the Galois group of such extensions operates on the classes of divisors in the original field and its extensions gives a linear operator, the characteristic roots (i.e. the eigenvalues) of which are the roots of the zeta-function.

On a number field, the nearest we can get to this is by adjunction of l^n-th roots of unity, l being fixed; the Galois group of this infinite extension is cyclic, and defines a linear operator on the projective limit of the (absolute) class groups of those successive finite extensions; *this should have something to do* *with the roots of the zeta-function of the field.* However, our extensions are ramified (but only at a finite number of places, viz. the prime divisors of l). Thus a preliminary study of similar problems in function-fields might enable one to guess what will happen in number-fields."

A few years later, in 1947, he makes this a bit more explicit in his marvelous essay "L'avenir des mathematiques" (The future of mathematics). Weil is still in shell-shock after the events of the second WW, and writes in beautiful archaic French sentences lasting forever :

"L'hypothèse de Riemann, après qu'on eu perdu l'espoir de la démontrer par les méthodes de la théorie des fonctions, nous apparaît aujourd'hui sous un jour nouveau, qui la montre inséparable de la conjecture d'Artin sur les fonctions L, ces deux problèmes étant deux aspects d'une mme question arithmético-algébrique, *o l'étude simultanée de toutes les extensions cyclotomiques d'un corps de nombres donné jouera sans doute le rle décisif.*

L'arithmétique gausienne gravitait autour de la loi de réciprocité quadratique; nous savons maintenant que celle-ci n'est qu'un premier example, ou pour mieux dire le paradigme, des lois dites "du corps de classe", qui gouvernent les extensions abéliennes des corps de nobres algébriques; nous savons formuler ces lois de manière à leur donner l'aspect d'un ensemble cohérent; mais, si plaisante à l'il que soit cette faade, nous ne savons si elle ne masque pas des symmétries plus cachées.

Les automorphismes induits sur les groupes de classes par les automorphismes du corps, les propriétés des restes de normes dans les cas non cycliques, le passage à la limite (inductive ou projective) *quand on remplace le corps de base par des extensions, par example cyclotomiques, de degré indéfiniment croissant, sont autant de questions sur lesquelles notre ignorance est à peu près complète, et dont l'étude contient peut-tre la clef de l'hypothese de Riemann*; étroitement liée à celles-ci est l'étude du conducteur d'Artin, et en particulier, dans le cas local, la recherche de la représentation dont la trace s'exprime au moyen des caractères simples avec des coefficients égaux aux exposants de leurs conducteurs.

Ce sont là quelques-unes des directions qu'on peut et qu'on doit songer à suivre afin de pénétrer dans le mystère des extensions non abéliennes; il n'est pas impossible que nous touchions là à des principes d'une fécondité extraordinaire, et que le premier pas décisif une fois fait dans cette voie doive nous ouvrir l'accès à de vastes domaines dont nous souponnons à peine l'existence; car jusqu'ici, pour amples que soient nos généralisations des résultats de Gauss, on ne peut dire que nus les ayons vraiment dépassés."

2.6 Connes-Consani $\mathbb{F}_1$-geometry (1)

A couple of weeks ago, Alain Connes and Katia Consani arXived their paper "On the notion of geometry over $\mathbb{F}_1$". Their subtle definition is phrased entirely in Grothendieck's scheme-theoretic language of representable functors and may be somewhat hard to get through if you only had a few years of mathematics.

Fig. 2.9: K. Consani

I'll try to give the essence of their definition of an *affine scheme over* $\mathbb{F}_1$ (and illustrate it with an example) in a couple of posts. All you need to know is what a finite Abelian group is (if you know what a cyclic group is that'll be enough) and what a commutative algebra is. If you already know what a functor and a natural transformation is, that would be great, but we'll deal with all that abstract nonsense when we'll need it.

So take two finite Abelian groups A and B, then a group-morphism is just a map $f : A \to B$ preserving the group-data. That is, f sends the unit element of A to that of B and f sends a product of two elements in A to the product of their images in B. For example, if $A = C_n$ is a cyclic group of order n with generator g and $B = C_m$ is a cyclic group of order m with generator h, then every groupmorphism from A to B is entirely determined by the image of g let's say that this image is h^i. But, as $g^n = 1$ and the conditions on a group-morphism we must have that $h^{in} = (h^i)^n = 1$ and therefore m must divide i.n. This gives you all possible group-morphisms from A to B.

They are plenty of finite abelian groups and many group-morphisms between any pair of them and all this stuff we put into one giant sack and label it $\mathbf{abelian}$. There is another, even bigger sack, which is even simpler to describe. It is labeled $\mathbf{sets}$ and contains all sets as well as all maps between two sets.

Right! Now what might be a *map* $F : \mathbf{abelian} \to \mathbf{sets}$ between these two sacks? Well, F should map any abelian group A to a set F(A) and any group-morphism $f : A \to B$ to a map between the corresponding sets $F(f) : F(A) \to F(B)$ and do all of this nicely. That is, F should send compositions of group-morphisms to compositions of the corresponding maps, and so on. If you take a pen and a piece of paper, you're bound to come up with the exact definition of a *functor* (that's what F is called).

You want an example? Well, lets take F to be the map sending an Abelian group A to its set of elements (also called A) and which sends a groupmorphism $A \to B$ to the same map from A to B. All F does is 'forget' the extra group-conditions on the sets and maps. For this reason F is called the *forgetful functor*. We will denote this particular functor by $\underline{\mathbb{G}}_m$, merely to show off.

Luckily, there are lots of other and more interesting examples of such functors. Our first class we will call *maxi-functors* and they are defined using a finitely generated $\mathbb{C}$-algebra R. That is, R can be written as the quotient of a polynomial algebra

$$R = \frac{\mathbb{C}[x_1,\ldots,x_d]}{(f_1,\ldots,f_e)}$$

by setting all the polynomials f_i to be zero. For example, take R to be the ring of Laurent polynomials

$$R = \mathbb{C}[x,x^{-1}] = \frac{\mathbb{C}[x,y]}{(xy-1)}$$

Other, and easier, examples of $\mathbb{C}$-algebras is the *group-algebra* $\mathbb{C}A$ of a finite Abelian group A. This group-algebra is a finite dimensional vectorspace with basis e_a, one for each element $a \in A$ with multiplication rule induced by the relations $e_a.e_b = e_{a.b}$ where on the left-hand side the multiplication . is in the group-algebra whereas on the right hand side the multiplication in the index is that of the group A. By choosing a different basis one can show that the group-algebra is really just the direct sum of copies of $\mathbb{C}$ with componentwise addition and multiplication

$$\mathbb{C}A = \mathbb{C} \oplus \ldots \oplus \mathbb{C}$$

with as many copies as there are elements in the group A. For example, for the cyclic group C_n we have

$$\mathbb{C}C_n = \frac{\mathbb{C}[x]}{(x^n-1)} = \frac{\mathbb{C}[x]}{(x-1)} \oplus \frac{\mathbb{C}[x]}{(x-\zeta)} \oplus \frac{\mathbb{C}[x]}{(x-\zeta^2)} \oplus \ldots \oplus \frac{\mathbb{C}[x]}{(x-\zeta^{n-1})} = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \ldots \oplus \mathbb{C}$$

The *maxi-functor* associated to a $\mathbb{C}$-algebra R is the functor

$$\mathbf{maxi}(R) : \mathbf{abelian} \to \mathbf{sets}$$

which assigns to a finite Abelian group A the set of all algebra-morphism $R \to \mathbb{C}A$ from R to the group-algebra of A. But wait, you say (i hope), we also needed a functor to do something on groupmorphisms $f : A \to B$. Exactly, so to f we have an algebra-morphism $f' : \mathbb{C}A \to \mathbb{C}B$ so the functor on morphisms is defined via composition

$\mathbf{maxi}(R)(f) : \mathbf{maxi}(R)(A) \to \mathbf{maxi}(R)(B) \qquad \phi : R \to \mathbb{C}A \mapsto f' \circ \phi : R \to \mathbb{C}A \to \mathbb{C}B$

So, what is the maxi-functor $\mathbf{maxi}(\mathbb{C}[x, x^{-1}]$? Well, any $\mathbb{C}$-algebra morphism $\mathbb{C}[x, x^{-1}] \to \mathbb{C}A$ is fully determined by the image of x which must be a unit in $\mathbb{C}A = \mathbb{C} \oplus \ldots \oplus \mathbb{C}$. That is, all components of the image of x must be non-zero complex numbers, that is

$\mathbf{maxi}(\mathbb{C}[x, x^{-1}])(A) = \mathbb{C}^* \oplus \ldots \oplus \mathbb{C}^*$

where there are as many components as there are elements in A. Thus, the sets $\mathbf{maxi}(R)(A)$ are typically huge which is the reason for the maxi-terminology.

Next, let us turn to *mini-functors*. They are defined similarly but this time using finitely generated $\mathbb{Z}$-algebras such as $S = \mathbb{Z}[x, x^{-1}]$ and the integral group-rings $\mathbb{Z}A$ for finite Abelian groups A. The structure of these integral group-rings is a lot more delicate than in the complex case. Let's consider them for the smallest cyclic groups (the 'isos' below are only approximations!)

$\mathbb{Z}C_2 = \frac{\mathbb{Z}[x]}{(x^2-1)} = \frac{\mathbb{Z}[x]}{(x-1)} \oplus \frac{\mathbb{Z}[x]}{(x+1)} = \mathbb{Z} \oplus \mathbb{Z}$

$\mathbb{Z}C_3 = \frac{\mathbb{Z}[x]}{(x^3-1)} = \frac{\mathbb{Z}[x]}{(x-1)} \oplus \frac{\mathbb{Z}[x]}{(x^2+x+1)} = \mathbb{Z} \oplus \mathbb{Z}[\rho]$

$\mathbb{Z}C_4 = \frac{\mathbb{Z}[x]}{(x^4-1)} = \frac{\mathbb{Z}[x]}{(x-1)} \oplus \frac{\mathbb{Z}[x]}{(x+1)} \oplus \frac{\mathbb{Z}[x]}{(x^2+1)} = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}[i]$

For a $\mathbb{Z}$-algebra S we can define its *mini-functor* to be the functor

$\mathbf{mini}(S) : \mathbf{abelian} \to \mathbf{sets}$

which assigns to an Abelian group A the set of all $\mathbb{Z}$-algebra morphisms $S \to \mathbb{Z}A$. For example, for the algebra $\mathbb{Z}[x, x^{-1}]$ we have that

$\mathbf{mini}(\mathbb{Z}[x, x^{-1}]\ (A) = (\mathbb{Z}A)^*$

the set of all invertible elements in the integral group-algebra. To study these sets one has to study the units of cyclotomic integers. From the above decompositions it is easy to verify that for the first few cyclic groups, the corresponding sets are $\pm C_2, \pm C_3$ and $\pm C_4$. However, in general this set doesn't have to be finite. It is a well-known result that the group of units of an integral group-ring of a finite Abelian group is of the form

$(\mathbb{Z}A)^* = \pm A \times \mathbb{Z}^{\oplus r}$

where $r = \frac{1}{2}(o(A) + 1 + n_2 - 2c)$ where $o(A)$ is the number of elements of A, n_2 is the number of elements of order 2 and c is the number of cyclic subgroups of A. So, these sets can still be infinite but at least they are a lot more manageable, explaining the **mini**-terminology.

Now, we would love to go one step deeper and define *nano-functors* by the same procedure, this time using finitely generated algebras over $\mathbb{F}_1$, the field with one element. But as we do not really know what we might mean by this, we simply define a *nano-functor* to be a *subfunctor* of a *mini-functor*, that is, a nano-functor N has an associated mini-functor $\mathbf{mini}(S)$ such that for all finite Abelian groups A we have that $N(A) \subset \mathbf{mini}(S)(A)$.

For example, the forgetful functor at the beginning, which we pompously denoted $\underline{\mathbb{G}}_m$ is a nano-functor as it is a subfunctor of the mini-functor $\mathbf{mini}(\mathbb{Z}[x, x^{-1}])$.

Now we are almost done : an affine $\mathbb{F}_1$-scheme in the sense of Connes and Consani is a pair consisting of a nano-functor N and a maxi-functor $\mathbf{maxi}(R)$ such that two rather strong conditions are satisfied :

- there is an *evaluation* 'map' of functors $e \ : \ N \rightarrow \mathbf{maxi}(R)$
- this pair determines uniquely a 'minimal' mini-functor $\mathbf{mini}(S)$ of which N is a subfunctor

of course we still have to turn this into proper definitions but that will have to await another post. For now, suffice it to say that the pair $(\underline{\mathbb{G}_m}, \mathbf{maxi}(\mathbb{C}[x,x^{-1}]))$ is a $\mathbb{F}_1$-scheme with corresponding uniquely determined mini-functor $\mathbf{mini}(\mathbb{Z}[x,x^{-1}])$, called the *multiplicative group scheme*.

2.7 Connes-Consani $\mathbb{F}_1$-geometry (2)

In the foregoing section we have seen how an affine $\mathbb{C}$-algebra R gives us a *maxi-functor* (because the associated sets are typically huge)

$$\mathbf{maxi}(R) \ : \ \mathbf{abelian} \rightarrow \mathbf{sets} \qquad A \mapsto Hom_{\mathbb{C}-alg}(R, \mathbb{C}A)$$

Substantially smaller sets are produced from finitely generated $\mathbb{Z}$-algebras S (therefore called *mini-functors*)

$$\mathbf{mini}(S) \ : \ \mathbf{abelian} \rightarrow \mathbf{sets} \qquad A \mapsto Hom_{\mathbb{Z}-alg}(S, \mathbb{Z}A)$$

Both these functors are 'represented' by existing geometrical objects, for a maxi-functor by the complex affine variety $X_R = \mathbf{max}(R)$ (the set of maximal ideals of the algebra R) with complex coordinate ring R and for a mini-functor by the integral affine scheme $X_S = \mathbf{spec}(S)$ (the set of all prime ideals of the algebra S).

The 'philosophy' of $\mathbb{F}_1$-mathematics is that an object over this virtual field with one element $\mathbb{F}_1$ records the essence of possibly complicated complex- or integral- objects in a small combinatorial thing.

For example, an n-dimensional complex vectorspace $\mathbb{C}^n$ has as its integral form a lattice of rank n $\mathbb{Z}^{\oplus n}$. The corresponding $\mathbb{F}_1$-objects only records the dimension n, so it is a finite set consisting of n elements (think of them as the set of base-vectors of the vectorspace).

Similarly, all base-changes of the complex vectorspace $\mathbb{C}^n$ are given by invertible matrices with complex coefficients $GL_n(\mathbb{C})$. Of these base-changes, the only ones leaving the integral lattice $\mathbb{Z}^{\oplus n}$ intact are the matrices having all their entries integers and their determinant equal to ± 1, that is the group $GL_n(\mathbb{Z})$. Of these integral matrices, the only ones that shuffle the base-vectors around are the permutation matrices, that is the group S_n of all possible ways to permute the n base-vectors. In fact, this example also illustrates Tits' original motivation to introduce $\mathbb{F}_1$: the finite group S_n is the Weyl-group of the complex Lie group $GL_n(\mathbb{C})$.

So, we expect a geometric $\mathbb{F}_1$-object to determine a much smaller functor from finite abelian groups to sets, and, therefore we call it a nano-functor

$$\mathbf{nano}(N) \ : \ \mathbf{abelian} \rightarrow \mathbf{sets} \qquad A \mapsto N(A)$$

but as we do not know yet what the correct geometric object might be we will only assume for the moment that it is a subfunctor of some mini-functor $\mathbf{mini}(S)$. That is, for every finite abelian group A we have an inclusion of sets $N(A) \subset Hom_{\mathbb{Z}-alg}(S, \mathbb{Z}A)$ in such a way that these inclusions are compatible with morphisms. Again, take pen and paper and you are bound to discover the correct definition of what is called a *natural transformation*, that is, a 'map' between the two functors $\mathbf{nano}(N) \rightarrow \mathbf{mini}(S)$.

Right, now to make sense of our virtual $\mathbb{F}_1$-geometrical object $\mathbf{nano}(N)$ we have to connect it to properly existing complex- and/or integral-geometrical objects.

Let us define a *gadget* to be a couple $(\mathbf{nano}(N), \mathbf{maxi}(R))$ consisting of a nano- and a maxi-functor together with a 'map' (that is, a natural transformation) between them

$e \; : \; \mathbf{nano}(N) \rightarrow \mathbf{maxi}(R)$

The idea of this map is that it visualizes the elements of the set $N(A)$ as $\mathbb{C}A$-points of the complex variety X_R (that is, as a collection of $o(A)$ points of X_R, where $o(A)$ is the number of elements of A).

In the example we used before(the forgetful functor) with $N(A) = A$ any group-element $a \in A$ is mapped to the algebra map $\mathbb{C}[x, x^{-1}] \rightarrow \mathbb{C}A$, $x \mapsto e_a$ in $\mathbf{maxi}(\mathbb{C}[x, x^{-1}])$. On the geometry side, the points of the variety associated to $\mathbb{C}A$ are all algebra maps $\mathbb{C}A \rightarrow \mathbb{C}$, that is, the $o(A)$ *characters* $\chi_1, \ldots, \chi_{o(A)}$. Therefore, a group-element $a \in A$ is mapped to the $\mathbb{C}A$-point of the complex variety $\mathbb{C}^* = X_{\mathbb{C}[x,x^{-1}]}$ consisting of all character-values at $a : \chi_1(a), \ldots, \chi_{o(A)}(g)$.

In mathematics we do not merely consider objects (such as the gadgets defined just now), but also the morphisms between these objects. So, what might be a morphism between two gadgets

$(\mathbf{nano}(N), \mathbf{maxi}(R)) \rightarrow (\mathbf{nano}(N'), \mathbf{maxi}(R'))$

Well, naturally it should be a 'map' (that is, a natural transformation) between the nano-functors $\phi \; : \; \mathbf{nano}(N) \rightarrow \mathbf{nano}(N')$ together with a morphism between the complex varieties $X_R \rightarrow X_{R'}$ (or equivalently, an algebra morphism $\psi \; : \; R' \rightarrow R$) such that the extra gadget-structure (the evaluation maps) are preserved.

That is, for every finite Abelian group A we should have a commuting diagram of maps

$$\begin{tikzcd}
N(A) \arrow[r, "\phi(A)"] \arrow[d, "e_N(A)"] & N'(A) \arrow[d, "e_{N'}(A)"] \\
Hom_{\mathbb{C}-alg}(R, \mathbb{C}A) \arrow[r, "-\circ\psi"] & Hom_{\mathbb{C}-alg}(R', \mathbb{C}A)
\end{tikzcd}$$

Not every gadget is a $\mathbb{F}_1$-variety though, for those should also have an integral form, that is, define a mini-functor. In fact, as we will see next time, an affine $\mathbb{F}_1$-variety is a gadget determining a unique mini-functor $\mathbf{mini}(S)$.

2.8 Connes-Consani $\mathbb{F}_1$-geometry (3)

A quick recap of the previous sections. We are trying to make sense of affine varieties over the elusive field with one element $\mathbb{F}_1$, which by Grothendieck's scheme-philosophy should determine a functor

$\mathbf{nano}(N) \; : \; \mathbf{abelian} \rightarrow \mathbf{sets} \qquad A \mapsto N(A)$

from finite Abelian groups to sets, typically giving pretty small sets $N(A)$. Using the $\mathbb{F}_1$-mantra that $\mathbb{Z}$ should be an algebra over $\mathbb{F}_1$ any $\mathbb{F}_1$-variety determines an integral scheme by extension of scalars, as well as a complex variety (by extending further to $\mathbb{C}$). We have already connected the complex variety with the original functor into a **gadget** that is a couple $(\mathbf{nano}(N), \mathbf{maxi}(R))$ where R is the coordinate ring of a complex affine variety X_R having the property that every element of $N(A)$ can be realized as a $\mathbb{C}A$-point of X_R. Ringtheoretically this simply means that to every element $x \in N(A)$ there is an algebra map $N_x \; : \; R \rightarrow \mathbb{C}A$.

Today we will determine which gadgets determine an integral scheme, and do so uniquely, and call them the sought for affine schemes over $\mathbb{F}_1$.

Let's begin with our example : $\mathbf{nano}(N) = \underline{\mathbb{G}}_m$ being the forgetful functor, that is $N(A) = A$ for every finite Abelian group, then the complex algebra $R = \mathbb{C}[x, x^{-1}]$ partners up to form a gadget because to every element $a \in N(A) = A$ there is a natural algebra map $N_a : \mathbb{C}[x, x^{-1}] \to \mathbb{C}A$ defined by sending $x \mapsto e_a$. Clearly, there is an obvious integral form of this complex algebra, namely $\mathbb{Z}[x, x^{-1}]$ but we have already seen that this algebra represents the mini-functor

$$\mathbf{min}(\mathbb{Z}[x, x^{-1}]) \; : \; \mathbf{abelian} \to \mathbf{sets} \qquad A \mapsto (\mathbb{Z}A)^*$$

and that the group of units $(\mathbb{Z}A)^*$ of the integral group ring $\mathbb{Z}A$ usually is a lot bigger than $N(A) = A$. So, perhaps there is another less obvious $\mathbb{Z}$-algebra S doing a much better job at approximating N? That is, if we can formulate this more precisely...

In general, every $\mathbb{Z}$-algebra S defines a gadget $\mathbf{gadget}(S) = (\mathbf{mini}(S), \mathbf{maxi}(S \otimes_{\mathbb{Z}} \mathbb{C}))$ with the obvious (that is, extension of scalars) evaluation map

$$\mathbf{mini}(S)(A) = Hom_{\mathbb{Z}-alg}(S, \mathbb{Z}A) \to Hom_{\mathbb{C}-alg}(S \otimes_{\mathbb{Z}} \mathbb{C}, \mathbb{C}A) = \mathbf{maxi}(S \otimes_{\mathbb{Z}} \mathbb{C})(A)$$

Right, so how might one express the fact that the integral affine scheme X_T with integral algebra T is the 'best' integral approximation of a gadget $(\mathbf{nano}(N), \mathbf{maxi}(R))$. Well, to begin its representing functor should at least contain the information given by N, that is, $\mathbf{nano}(N)$ is a **sub-functor** of $\mathbf{mini}(T)$ (meaning that for every finite Abelian group A we have a natural inclusion $N(A) \subset Hom_{\mathbb{Z}-alg}(T, \mathbb{Z}A)$). As to the "best"-part, we must express that all other candidates factor through T. That is, suppose we have an integral algebra S and a morphism of gadgets (as defined last time)

$$f \; : \; (\mathbf{nano}(N), \mathbf{maxi}(R)) \to \mathbf{gadget}(S) = (\mathbf{mini}(S), \mathbf{maxi}(S \otimes_{\mathbb{Z}} \mathbb{C}))$$

then there ought to be $\mathbb{Z}$-algebra morphism $T \to S$ such that the above map f factors through an induced gadget-map $\mathbf{gadget}(T) \to \mathbf{gadget}(S)$.

Fine, but is this definition good enough in our trivial example? In other words, is the "obvious" integral ring $\mathbb{Z}[x, x^{-1}]$ the best integral choice for approximating the forgetful functor $N = \underline{\mathbb{G}}_m$? Well, take any finitely generated integral algebra S, then saying that there is a morphism of gadgets from $(\underline{\mathbb{G}}_m, \mathbf{maxi}(\mathbb{C}[x, x^{-1}])$ to $\mathbf{gadget}(S)$ means that there is a $\mathbb{C}$-algebra map $\psi : S \otimes_{\mathbb{Z}} \mathbb{C} \to \mathbb{C}[x, x^{-1}]$ such that for every finite Abelian group A we have a commuting diagram

$$\begin{tikzcd}
A \arrow[r] \arrow[d, "e"'] & Hom_{\mathbb{Z}-alg}(S, \mathbb{Z}A) \arrow[d] \\
Hom_{\mathbb{C}-alg}(\mathbb{C}[x, x^{-1}], \mathbb{C}A) \arrow[r, "- \circ \psi"] & Hom_{\mathbb{C}-alg}(S \otimes_{\mathbb{Z}} \mathbb{C}, \mathbb{C}A)
\end{tikzcd}$$

Here, e is the natural evaluation map defined before sending a group-element $a \in A$ to the algebra map defined by $x \mapsto e_a$ and the vertical map on the right-hand side is extensions by scalars. From this data we must be able to show that the image of the algebra map

$$\begin{tikzcd}
S \arrow[r, "i"] & S \otimes_{\mathbb{Z}} \mathbb{C} \arrow[r, "\psi"] & \mathbb{C}[x, x^{-1}]
\end{tikzcd}$$

is contained in the integral subalgebra $\mathbb{Z}[x, x^{-1}]$. So, take any generator z of S then its image $\psi(z) \in \mathbb{C}[x, x^{-1}]$ is a Laurent polynomial of degree say d (that is, $\psi(z) = c_{-d}x^{-d} + \ldots c_{-1}x^{-1} + c_0 + c_1 x + \ldots + c_d x^d$ with all coefficients a priori in $\mathbb{C}$ and we need to talk them into $\mathbb{Z}$).

Now comes the basic **trick** : take a cyclic group $A = C_N$ of order $N > d$, then the above commuting diagram applied to the generator of C_N (the evaluation of which is the natural projection map $\pi : \mathbb{C}[x.x^{-1}] \to \mathbb{C}[x, x^{-1}]/(x^N - 1) = \mathbb{C}C_N$) gives us the commuting diagram

$$\begin{tikzcd}
S \arrow[r] \arrow[d] & S \otimes_{\mathbb{Z}} \mathbb{C} \arrow[r, "\psi"] & \mathbb{C}[x,x^{-1}] \arrow[d, "\pi"] \\
\mathbb{Z}C_n = \dfrac{\mathbb{Z}[x,x^{-1}]}{(x^N-1)} \arrow[rr, "j"] & & \dfrac{\mathbb{C}[x,x^{-1}]}{(x^N-1)}
\end{tikzcd}$$

where the horizontal map j is the natural inclusion map. Tracing $z \in S$ along the diagram we see that indeed all coefficients of $\psi(z)$ have to be integers! Applying the same argument to the other generators of S (possibly for varying values of N) we see that , indeed, $\psi(S) \subset \mathbb{Z}[x,x^{-1}]$ and hence that $\mathbb{Z}[x,x^{-1}]$ is the best integral approximation for $\underline{\mathbb{G}}_m$.

That is, we have our first example of an affine variety over the field with one element $\mathbb{F}_1$: $(\underline{\mathbb{G}}_m, \mathbf{maxi}(\mathbb{C}[x,x^{-1}]) \to \mathbf{gadget}(\mathbb{Z}[x,x^{-1}])$.

What makes this example work is that the infinite group $\mathbb{Z}$ (of which the complex group-algebra is the algebra $\mathbb{C}[x,x^{-1}]$) has enough finite Abelian group-quotients. In other words, $\mathbb{F}_1$ doesn't see $\mathbb{Z}$ but rather its profinite completion $\hat{\mathbb{Z}} = \underset{\leftarrow}{lim}\mathbb{Z}/N\mathbb{Z}$... (to be continued when we'll consider noncommutative $\mathbb{F}_1$-schemes)

In general, an affine $\mathbb{F}_1$-scheme is a gadget with morphism of gadgets $(\mathbf{nano}(N), \mathbf{maxi}(R)) \to \mathbf{gadget}(S)$ provided that the integral algebra S is the best integral approximation in the sense made explicit before. This rounds up our first attempt to understand the Connes-Consani approach to define geometry over $\mathbb{F}_1$ apart from one important omission : we have only considered functors to $\mathbf{sets}$, whereas it is crucial in the Connes-Consani paper to consider more generally functors to **graded** sets. In the final part of this series we'll explain what that's all about.

series 3

NONCOMMUTATIVE GEOMETRY

3.1 The Bost-Connes coset space

By now, everyone remotely interested in Connes' approach to the Riemann hypothesis, knows the one line mantra

one can use noncommutative geometry to extend Weil's proof of the Riemann-hypothesis in the function field case to that of number fields

But, can one go beyond this sound-bite in a series of blog posts? A few days ago, I was rather optimistic, but now, after reading-up on the Connes-Consani-Marcolli project, I feel overwhelmed by the sheer volume of their work (and by my own ignorance of key tools in the approach). The most recent account takes up half of the 700+ pages of the book Noncommutative Geometry, Quantum Fields and Motives by Alain Connes and Matilde Marcolli...

So let us set a more modest goal and try to understand one of the first papers Alain Connes wrote about the RH : Noncommutative geometry and the Riemann zeta function. It is only 24 pages long and relatively readable. But even then, the reader needs to know about class field theory, the classification of AF-algebras, Hecke algebras, etc. etc. Most of these theories take a book to explain. For example, the first result he mentions is the main result of local class field theory which appears only towards the end of the 200+ pages of Jean-Pierre Serre's Local Fields, itself a somewhat harder read than the average blogpost...

Anyway, we will see how far we can get. Here's the plan : I'll take the heart-bit of their approach : the **Bost-Connes system**, and will try to understand it from an algebraist's viewpoint. Today we will introduce the groups involved and describe their cosets.

For any commutative ring R let us consider the group of triangular 2×2 matrices of the form

$$P_R = \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} \mid b \in R, a \in R^*$$

(that is, a in an invertible element in the ring R). This is really an affine group scheme defined over the integers, that is, the coordinate ring

$\mathbb{Z}[P] = \mathbb{Z}[x, x^{-1}, y]$ becomes a Hopf algebra with comultiplication encoding the group-multiplication. Because

$$\begin{bmatrix} 1 & b_1 \\ 0 & a_1 \end{bmatrix} \begin{bmatrix} 1 & b_2 \\ 0 & a_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \times b_2 + b_1 \times a_2 \\ 0 & a_1 \times a_2 \end{bmatrix}$$

we have $\Delta(x) = x \otimes x$ and $\Delta(y) = 1 \otimes y + y \otimes x$, or x is a group-like element whereas y is a skew-primitive. If $R \subset \mathbb{R}$ is a subring of the real numbers, we denote by P_R^+ the subgroup of P_R consisting of all matrices with $a > 0$. For example,

$\Gamma_0 = P^+_{\mathbb{Z}} = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z}$

which is a subgroup of $\Gamma = P^+_{\mathbb{Q}}$ and our first job is to describe the cosets.

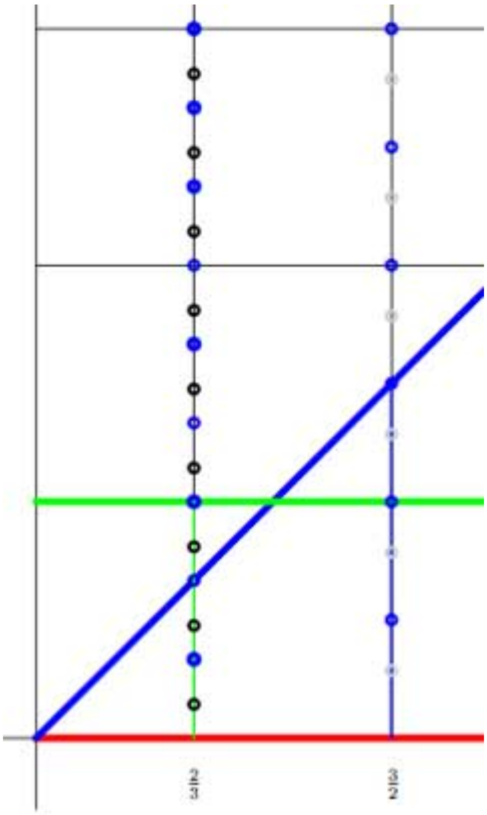


Fig. 3.1: double cosets

The *left* cosets Γ/Γ_0 are the subsets $\gamma\Gamma_0$ with $\gamma \in \Gamma$. But,

$$\begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b+n \\ 0 & a \end{bmatrix}$$

so if we represent the matrix $\gamma = \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix}$ by the point (a,b) in the right halfplane, then for a given positive rational number a the different cosets are represented by all $b \in [0,1) \cap \mathbb{Q} = \mathbb{Q}/\mathbb{Z}$. Hence, the left cosets are all the rational points in the region between the red and green horizontal lines. For fixed a the cosets correspond to the rational points in the green interval (such as over $\frac{2}{3}$ in the picture on the left.

Similarly, the *right* cosets $\Gamma_0\backslash\Gamma$ are the subsets $\Gamma_0\gamma$ and as

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} = \begin{bmatrix} 1 & b+na \\ 0 & a \end{bmatrix}$$

we see similarly that the different cosets are precisely the rational points in the region between the lower red horizontal and the blue diagonal line. So, for fixed a they correspond to rational points in the blue interval (such as over $\frac{3}{2}$) $[0,a) \cap \mathbb{Q}$. But now, let us look at the *double coset space* $\Gamma_0\backslash\Gamma/\Gamma_0$. That is, we want to study the orbits of the action of Γ_0, acting on the right, on the left-cosets Γ/Γ_0, or equivalently, of the action of Γ_0 acting on the left on the right-cosets $\Gamma_0\backslash\Gamma$. The crucial observation to make is that these actions have **finite orbits**, or equivalently, that Γ_0 is an *almost normal subgroup* of Γ meaning that $\Gamma_0 \cap \gamma\Gamma_0\gamma^{-1}$ has finite index in Γ_0 for all $\gamma \in \Gamma$. This follows from

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b+m+an \\ 0 & a \end{bmatrix}$$

and if n varies then an takes only finitely many values *modulo* $\mathbb{Z}$ and their number depends only on the denominator of a. In the picture above, the blue dots lying on the line over $\frac{2}{3}$ represent the double coset

$\Gamma_0 \begin{bmatrix} 1 & \frac{2}{3} \\ 0 & \frac{2}{3} \end{bmatrix}$ and we see that these dots split the left-cosets with fixed value $a = \frac{2}{3}$ (that is, the green line-segment) into three chunks (3 being the denominator of a) and split the right-cosets (the line-segment under the blue diagonal) into two subsegments (2 being the numerator of a). Similarly, the blue dots on the line over $\frac{3}{2}$ divide the left-cosets in two parts and the right cosets into three parts.

This shows that the Γ_0-orbits of the right action on the left cosets Γ/Γ_0 for each matrix $\gamma \in \Gamma$ with $a = \frac{2}{3}$ consist of exactly three points, and we denote this by writing $L(\gamma) = 3$. Similarly, all Γ_0-orbits of the left action on the right cosets $\Gamma_0\backslash\Gamma$ with this value of a consist of two points, and we write this as $R(\gamma) = 2$.

For example, on the above picture, the black dots on the line over $\frac{2}{3}$ give the matrices in the double coset of the matrix

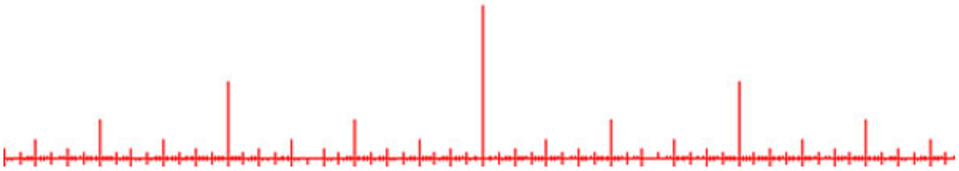
$$\gamma = \begin{bmatrix} 1 & \frac{1}{7} \\ 0 & \frac{2}{3} \end{bmatrix}$$

and the gray dots on the line over $\frac{3}{2}$ determine the elements of the double coset of

$$\gamma^{-1} = \begin{bmatrix} 1 & -\frac{3}{14} \\ 0 & \frac{3}{2} \end{bmatrix}$$

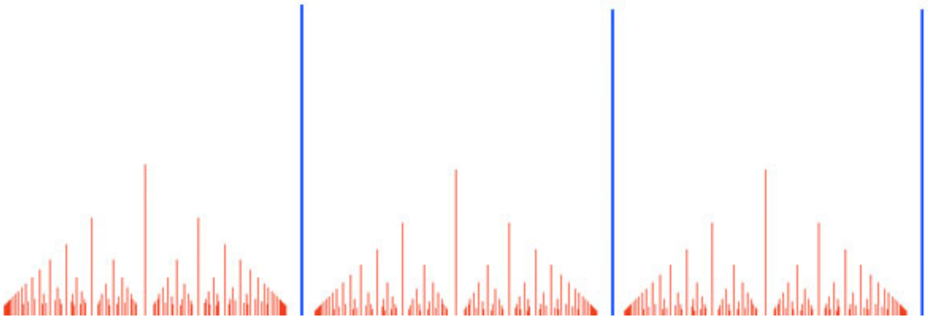
and one notices (in general) that $L(\gamma) = R(\gamma^{-1})$. But then, the double cosets with $a = \frac{2}{3}$ are represented by the rational b's in the interval $[0, \frac{1}{3})$ and those with $a = \frac{3}{2}$ by the rational b's in the interval $\frac{1}{2}$. In general, the double cosets of matrices with fixed $a = \frac{r}{s}$ with $(r, s) = 1$ are the rational points in the line-segment over a with $b \in [0, \frac{1}{s})$.

That is, the **Bost-Connes double coset space** $\Gamma_0\backslash\Gamma/\Gamma_0$ are the rational points in a horrible **fractal comb**. Below we have drawn only the part of the dyadic values, that is when $a = \frac{r}{2^t}$ in the unit interval



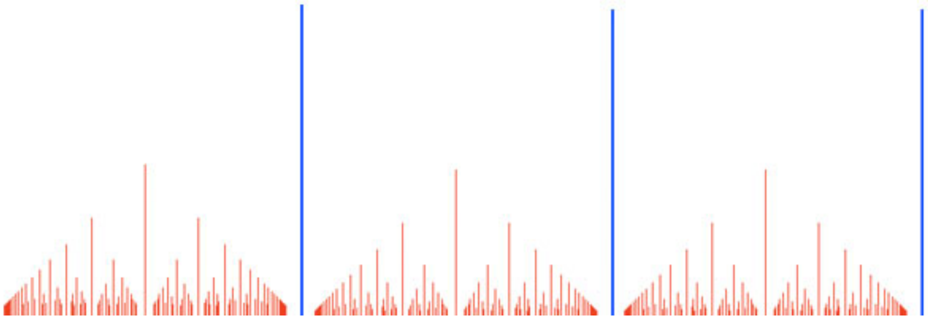
and of course we have to super-impose on it similar pictures for rationals with other powers as their denominators. Fortunately, NCG excels in describing such fractal beasts...

Here is a slightly better picture of the coset space, drawing the part over all rational numbers contained in the 15-th Farey sequence. The blue segments of length one are at 1,2,3,...



3.2 The Bost-Connes algebra

As before, Γ is the subgroup of the rational linear group $GL_2(\mathbb{Q})$ consisting of the matrices $\begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix}$ with $a \in \mathbb{Q}_+$ and Γ_0 the subgroup of all matrices $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ with $n \in \mathbb{N}$. Above, we have seen that the *double coset space* $\Gamma_0\backslash\Gamma/\Gamma_0$ can be identified with the set of all rational points in the *fractal comb* consisting of all couples (a, b) with $a = \frac{m}{n} \in \mathbb{Q}_+$ and $b \in [0, \frac{1}{n}) \cap \mathbb{Q}$



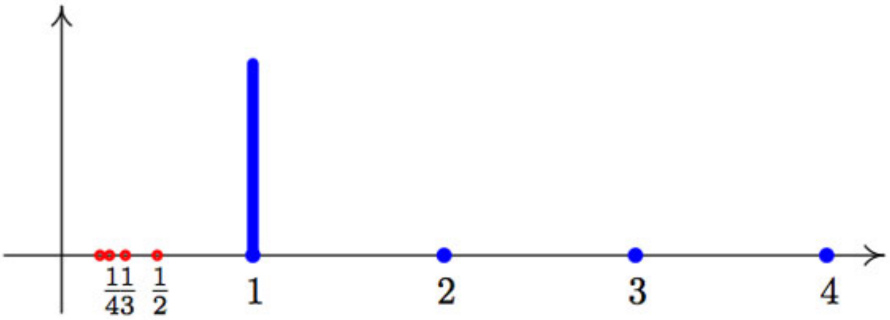
The blue spikes are at the positive natural numbers $a = 1, 2, 3, \ldots$. Over $a = 1$ they correspond to the matrices $\begin{bmatrix} 1 & \gamma \\ 0 & 1 \end{bmatrix}$ with $\gamma \in [0, 1) \cap \mathbb{Q}$ and as matrix-multiplication of such matrices corresponds to addition of the γ we see that these cosets can be identified with the additive group $\mathbb{Q}/\mathbb{Z}$ (which will reappear at a later stage as the multiplicative group of all roots of unity).

The Bost-Connes *Hecke algebra* $\mathcal{H} = \mathcal{H}(\Gamma, \Gamma_0)$ is the *convolution algebra* of all complex valued functions with finite support on the double coset space $\Gamma_0 \backslash \Gamma / \Gamma_0$. That is, as a vector space the algebra has as basis the functions e_X with $X \in \Gamma_0 \backslash \Gamma / \Gamma_0$ (that is, X is a point of the fractal comb) and such that $e_X(X) = 1$ and $e_X(Y) = 0$ for all other double cosets $Y \neq X$. The algebra product on $\mathcal{H}$ is the convolution-product meaning that if f, f' are complex functions with finite support on the Bost-Connes space, then they can also be interpreted as Γ_0-bi-invariant functions on the group Γ (for this just means that the function is constant on double cosets) and then $f * f'$ is the function defined for all $\gamma \in \Gamma$ by

$f * f'(\gamma) = \sum_{\mu \in \Gamma/\Gamma_0} f(\mu) f'(\mu^{-1}\gamma)$

Last time we have seen that the coset-space Γ/Γ_0 can be represented by all rational points (a, b) with $b < 1$. At first sight, the sum above seems to be infinite, but, f and f' are non-zero only at finitely many double cosets and we have see last time that Γ_0 acts on one-sided cosets with finite orbits. Therefore, $f * f$ is a well-defined Γ_0-bi-invariant function with finite support on the fractal comb $\Gamma_0 \backslash \Gamma / \Gamma_0$. Further, observe that the unit element of $\mathcal{H}$ is the function corresponding to the identity matrix in Γ.

Looking at fractal-comb picture it is obvious that the Bost-Connes Hecke algebra $\mathcal{H}$ is a huge object. Today, we will prove the surprising result that it can be generated by the functions corresponding to the tiny portion of the comb, shown below.



That is, we will show that $\mathcal{H}$ is generated by the functions $e(\gamma)$ corresponding to the double-coset $X_\gamma = \begin{bmatrix} 1 & \gamma \\ 0 & 1 \end{bmatrix}$ (the rational points of the blue line-segment over 1, or equivalently, the elements of the group $\mathbb{Q}/\mathbb{Z}$), together with the functions ϕ_n corresponding to the double-coset $X_n = \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix}$ for all $n \in \mathbb{N}_+$ (the blue dots to the right in the picture) and the functions ϕ_n^* corresponding to the double cosets $X_{1/n} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{n} \end{bmatrix}$ (the red dots to the left).

Take a point in the fractal comb $X = \begin{bmatrix} 1 & \gamma \\ 0 & \frac{m}{n} \end{bmatrix}$ with $(m,n) = 1$ and $\gamma \in [0, \frac{1}{n}) \cap \mathbb{Q} \subset [0,1) \cap \mathbb{Q}$. Note that as $\gamma < \frac{1}{n}$ we have that $n\gamma < 1$ and hence $e(n\gamma)$ is one of the (supposedly) generating functions described above.

Because $X = \begin{bmatrix} 1 & \gamma \\ 0 & \frac{m}{n} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & m \end{bmatrix} \begin{bmatrix} 1 & n\gamma \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{n} \end{bmatrix} = X_m X_{n\gamma} X_{1/n}$ we are aiming for a relation in the Hecke algebra $\phi_m * e(n\gamma) * \phi_n^* = e_X$. This is 'almost' true, except from a coefficient.

Let us prove first the equality of functions $e_X * \phi_n = n\phi_m * e(n\gamma)$. To do this we have to show that they have the same value for all points $Y \in \Gamma_0 \backslash \Gamma / \Gamma_0$ in the fractal comb. Let us first study the function on the right hand side.

$\phi_m * e(n\gamma) = \sum_{g \in \Gamma/\Gamma_0} \phi_m(g) e(n\gamma)(g^{-1}Y)$. Because $X_m\Gamma_0$ is already a double coset (over m we have a comb-spike of length one, so all rational points on it determine at the same time a one-sided and a double coset. Therefore, $\phi_m(g)$ is zero unless $g = X_m$ and then the value is one. Next, let us consider the function on the left-hand side. $e_X * \phi_n(Y) = \sum_{g \in \Gamma/\Gamma_0} e_X(g)\phi_m(g^{-1}Y)$. We have to be a bit careful here as the double cosets over $a = \frac{m}{n}$ are different from the left cosets. Recall from last time that the left-cosets over a are given by all rational points of the form (a,b) with $b < 1$ whereas the double-cosets over a are represented by the rational points of the form (a,b) with $b < \frac{1}{n}$ and hence the Γ_0-orbits over a all consist of precisely n elements g. That is, $e_X(g)$ is zero for all $g \in \Gamma/\Gamma_0$ except when g is one of the following matrices

$$g \in \begin{bmatrix} 1 & \gamma \\ 0 & \frac{m}{n} \end{bmatrix}, \begin{bmatrix} 1 & \gamma + \frac{1}{n} \\ 0 & \frac{m}{n} \end{bmatrix}, \begin{bmatrix} 1 & \gamma + \frac{2}{n} \\ 0 & \frac{m}{n} \end{bmatrix}, \ldots, \begin{bmatrix} 1 & \gamma + \frac{n-1}{n} \\ 0 & \frac{m}{n} \end{bmatrix}$$

Further, $\phi_n(g^{-1}Y)$ is zero unless $g^{-1}Y \in \Gamma_0 \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix} \Gamma_0$, or equivalently, that $Y \in \Gamma_0 g \Gamma_0 \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix} \Gamma_0 = \Gamma_0 g \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix} \Gamma_0$ and for each of the choices for g we have that

$$\begin{bmatrix} 1 & \gamma + \frac{k}{n} \\ 0 & \frac{m}{n} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & n \end{bmatrix} = \begin{bmatrix} 1 & n\gamma + k \\ 0 & m \end{bmatrix} \sim \begin{bmatrix} 1 & n\gamma \\ 0 & m \end{bmatrix}$$

Therefore, the function $e_X * \phi_n$ is zero at every point of the fractal comb unless at $\begin{bmatrix} 1 & n\gamma \\ 0 & m \end{bmatrix}$ where it is equal to n. This proves the claimed identity of functions and as one verifies easily that $\phi_n^* * \phi_n = 1$, it follows that all base vectors e_X of $\mathcal{H}$ can be expressed in the claimed generators

$$e_X = n\phi_m * e(n\gamma) * \phi_n^*$$

Bost and Connes use slightly different generators, namely with $\mu_n = \frac{1}{\sqrt{n}}\phi_n$ and $\mu_n^* = \sqrt{n}\phi_n^*$ in order to have all relations among the generators being defined over $\mathbb{Q}$ (as we will see another time). This will be important later on to have an action of the cyclotomic Galois group $Gal(\mathbb{Q}^{cycl}/\mathbb{Q})$ on certain representations of $\mathcal{H}$.

3.3 Bost-Connes for ringtheorists

Over the last days I've been staring at the Bost-Connes algebra to find a ringtheoretic way into it. I have had some chats about it with the resident graded-guru but all we came up with so far is that it seems to be an extension of Fred's definition of a 'crystalline' graded algebra. Knowing that several excellent ringtheorists keep an eye on my stumblings here, let me launch an appeal for help :

What is the most elegant ringtheoretic framework in which the Bost-Connes Hecke algebra is a motivating example?

Let us review what we know so far and extend upon it with a couple of observations that may (or may not) be helpful to you. The algebra $\mathcal{H}$ is the algebra of $\mathbb{Q}$-valued functions (under the convolution product) on the double coset-space $\Gamma_0 \backslash \Gamma / \Gamma_0$ where

$$\Gamma = \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} \ : \ a, b \in \mathbb{Q}, a > 0 \text{ and } \Gamma_0 = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \ : \ n \in \mathbb{N}_+$$

We have seen that a $\mathbb{Q}$-basis is given by the characteristic functions X_γ (that is, such that $X_\gamma(\gamma') = \delta_{\gamma,\gamma'}$) with γ a rational point represented by the couple (a, b) (the entries in the matrix definition of a representant of γ in Γ) lying in the fractal comb defined by the rule that $b < \frac{1}{n}$ if $a = \frac{m}{n}$ with $m, n \in \mathbb{N}, (m, n) = 1$. Last time we have seen that the algebra $\mathcal{H}$ is generated as a $\mathbb{Q}$-algebra by the following elements (changing notation)

$$\begin{cases} X_m = X_{\alpha_m} & \text{with } \alpha_m = \begin{bmatrix} 1 & 0 \\ 0 & m \end{bmatrix} \ \forall m \in \mathbb{N}_+ \\ X_n^* = X_{\beta_n} & \text{with } \beta_n = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1}{n} \end{bmatrix} \ \forall n \in \mathbb{N}_+ \\ Y_\gamma = X_\gamma & \text{with } \gamma = \begin{bmatrix} 1 & \gamma \\ 0 & 1 \end{bmatrix} \ \forall \lambda \in \mathbb{Q}/\mathbb{Z} \end{cases}$$

Using the tricks of last time (that is, figuring out what functions convolution products represent, knowing all double-cosets) it is not too difficult to prove the *defining relations among these generators* to be the following ((if someone wants the details, tell me and I'll include a 'technical post' or consult the Bost-Connes original paper but note that this scanned version needs 26.8Mb))

(1) : $X_n^* X_n = 1, \forall n \in \mathbb{N}_+$ (

2) : $X_n X_m = X_{nm}, \forall m, n \in \mathbb{N}_+$ (

3) : $X_n X_m^* = X_m^* X_n$, whenever $(m, n) = 1$ (

4) : $Y_\gamma Y_\mu = Y_{\gamma+\mu}, \forall \gamma, mu \in \mathbb{Q}/\mathbb{Z}$

(5) : $Y_\gamma X_n = X_n Y_{n\gamma}, \ \forall n \in \mathbb{N}_+, \gamma \in \mathbb{Q}/\mathbb{Z}$

(6) : $X_n Y_\lambda X_n^* = \frac{1}{n} \sum_{n\delta=\gamma} Y_\delta, \ \forall n \in \mathbb{N}_+, \gamma \in \mathbb{Q}/\mathbb{Z}$

Simple as these equations may seem, they bring us into rather uncharted ringtheoretic territories. Here a few fairly obvious ringtheoretic ingredients of the Bost-Connes Hecke algebra $\mathcal{H}$

the group-algebra of $\mathbb{Q}/\mathbb{Z}$

The equations (4) can be rephrased by saying that the subalgebra generated by the Y_γ is the rational groupalgebra $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ of the (additive) group $\mathbb{Q}/\mathbb{Z}$. Note however that $\mathbb{Q}/\mathbb{Z}$ is a torsion group (that is, for all $\gamma = \frac{m}{n}$ we have that $n.\gamma = (\gamma + \gamma + \ldots + \gamma) = 0$). Hence, the groupalgebra has LOTS of zero-divisors. In fact, this group-algebra doesn't have any good ringtheoretic properties except for the fact that it can be realized as a limit of finite groupalgebras (semi-simple algebras)

$\mathbb{Q}[\mathbb{Q}/\mathbb{Z}] = \underset{\rightarrow}{lim}\ \mathbb{Q}[\mathbb{Z}/n\mathbb{Z}]$

and hence is a quasi-free (or formally smooth) algebra, BUT far from being finitely generated...

the grading group $\mathbb{Q}^+_\times$

The multiplicative group of all positive rational numbers $\mathbb{Q}^+_\times$ is a torsion-free Abelian ordered group and it follows from the above defining relations that $\mathcal{H}$ is graded by this group if we give

$deg(Y_\gamma) = 1,\ deg(X_m) = m,\ deg(X_n^*) = \frac{1}{n}$

Now, graded algebras have been studied extensively in case the grading group is torsion-free abelian ordered AND finitely generated, HOWEVER $\mathbb{Q}^+_\times$ is infinitely generated and not much is known about such graded algebras. Still, the ordering should allow us to use some tricks such as taking leading coefficients etc.

the endomorphisms of $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$

We would like to view the equations (5) and (6) (the latter after multiplying both sides on the left with X_n^* and using (1)) as saying that X_n and X_n^* are normalizing elements. Unfortunately, the algebra morphisms they induce on the group algebra $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ are NOT isomorphisms, BUT endomorphisms. One source of algebra morphisms on the group-algebra comes from group-morphisms from $\mathbb{Q}/\mathbb{Z}$ to itself. Now, it is known that

$Hom_{grp}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \simeq \hat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$. A class of group-morphisms of interest to us are the maps given by multiplication by n on $\mathbb{Q}/\mathbb{Z}$. Observe that these maps are *epimorphisms* with a cyclic order n kernel. On the group-algebra level they give us the epimorphisms

$\mathbb{Q}[\mathbb{Q}/\mathbb{Z}] \longrightarrow^{\phi_n} \mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$

such that $\phi_n(Y_\lambda) = Y_{n\lambda}$ whence equation (5) can be rewritten as $Y_\lambda X_n = X_n \phi_n(Y_\lambda)$, which looks good until you think that ϕ_n is not an automorphism...

There are even other (non-unital) algebra endomorphisms such as the map $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}] \rightarrow^{\psi_n} R_n$ defined by $\psi_n(Y_\lambda) = \frac{1}{n}(Y_{\frac{\lambda}{n}} + Y_{\frac{\lambda+1}{n}} + \ldots + Y_{\frac{\lambda+n-1}{n}})$ and then, we can rewrite equation (6) as $Y_\lambda X_n^* = X_n^* \psi_n(Y_\lambda)$, but again, note that ψ_n is NOT an automorphism.

almost strongly graded, but not quite...

Recall from last time that the characteristic function X_a for any double-coset-class $a \in \Gamma_0 \backslash \Gamma / \Gamma_0$ represented by the matrix $a = \begin{bmatrix} 1 & \lambda \\ 0 & \frac{m}{n} \end{bmatrix}$ could be written in the Hecke algebra as $X_a = nX_m Y_{n\lambda} X_n^* = nY_\lambda X_m X_n^*$. That is, we can write the Bost-Connes Hecke algebra as

$\mathcal{H} = \oplus_{\frac{m}{n} \in \mathbb{Q}^+_\times} \mathbb{Q}[\mathbb{Q}/\mathbb{Z}] X_m X_n^*$

Hence, if only the morphisms ϕ_n and ψ_m would be automorphisms, this would say that $\mathcal{H}$ is a strongly $\mathbb{Q}^+_\times$-algebra with part of degree one the groupalgebra of $\mathbb{Q}/\mathbb{Z}$.

However, they are not. But there is an extension of the notion of strongly graded algebras which Fred has dubbed *crystalline graded algebras* in which it is sufficient that the algebra maps are all epimorphisms. (maybe I'll post about these algebras, another time). However, this is not the case for the ψ_m...

So, what is the most elegant ringtheoretic framework in which the algebra $\mathcal{H}$ fits??? Surely, you can do better than *generalized crystalline graded algebra...*

3.4 BC stands for bi-crystalline graded

Towards the end of the last section, I freaked-out because I realized that the commutation morphisms with the X_n^* were given by non-unital algebra maps. I failed to notice the obvious, that algebras such as $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ have plenty of *idempotents* and that this mysterious 'non-unital' morphism was nothing else but multiplication with an idempotent...

Here a sketch of a ringtheoretic framework in which the Bost-Connes Hecke algebra $\mathcal{H}$ is a motivating example (the details should be worked out by an eager 20-something). Start with a *suitable* semi-group S, by which I mean that one must be able to invert the elements of S and obtain a group G of which all elements have a canonical form $g = s_1 s_2^{-1}$. Probably semi-groupies have a name for these things, so if you know please drop a comment.

The next ingredient is a *suitable* ring R. Here, suitable means that we have a semi-group morphism $\phi : S \to End(R)$ where $End(R)$ is the semi-group of all ring-endomorphisms of R satisfying the following two (usually strong) conditions :

1. Every $\phi(s)$ has a right-inverse, meaning that there is an ring-endomorphism $\psi(s)$ such that $\phi(s) \circ \psi(s) = id_R$ (this implies that all $\phi(s)$ are in fact *epi-morphisms* (surjective)), and

2. The composition $\psi(s) \circ \phi(s)$ usually is NOT the identity morphism id_R (because it is zero on the kernel of the epimorphism $\phi(s)$) but we require that there is an idempotent $E_s \in R$ (that is, $E_s^2 = E_s$) such that $\psi(s) \circ \phi(s) = id_R E_s$

The point of the first condition is that the S-semi-group graded ring $A = \oplus_{s \in S} X_s R$ is **crystalline** graded (crystalline group graded rings were introduced by Fred Van Oystaeyen and Erna Nauwelaarts) meaning that for every $s \in S$ we have in the ring A the equality $X_s R = R X_s$ where this is a free right R-module of rank one. One verifies that this is equivalent to the existence of an epimorphism $\phi(s)$ such that for all $r \in R$ we have $r X_s = X_s \phi(s)(r)$.

The point of the second condition is that this semi-graded ring A can be naturally embedded in a G-graded ring $B = \oplus_{g=s_1 s_2^{-1} \in G} X_{s_1} R X_{s_2}^*$ which is *bi-crystalline* graded meaning that for all $r \in R$ we have that $r X_s^* = X_s^* \psi(s)(r) E_s$.

It is clear from the construction that under the given conditions (and probably some minor extra ones making everything stand) the group graded ring B is determined fully by the semi-group graded ring A.

what does this general ringtheoretic mumbo-jumbo have to do with the BC- (or Bost-Connes) algebra $\mathcal{H}$?

In this particular case, the semi-group S is the multiplicative semi-group of positive integers $\mathbb{N}_\times^+$ and the corresponding group G is the multiplicative group $\mathbb{Q}_\times^+$ of all positive rational numbers.

The ring R is the rational group-ring $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ of the torsion-group $\mathbb{Q}/\mathbb{Z}$. Recall that the elements of $\mathbb{Q}/\mathbb{Z}$ are the rational numbers $0 \leq \lambda < 1$ and the group-law is ordinary addition and forgetting the integral part (so merely focussing on the 'after the comma' part). The group-ring is then

$\mathbb{Q}[\mathbb{Q}/\mathbb{Z}] = \oplus_{0 \leq \lambda < 1} \mathbb{Q} Y_\lambda$ with multiplication linearly induced by the multiplication on the base-elements $Y_\lambda . Y_\mu = Y_{\lambda+\mu}$.

The epimorphism determined by the semi-group map $\phi : \mathbb{N}_\times^+ \to End(\mathbb{Q}[\mathbb{Q}/\mathbb{Z}])$ are given by the algebra maps defined by linearly extending the map on the base elements $\phi(n)(Y_\lambda) = Y_{n\lambda}$ (observe that this is indeed an epimorphism as every base element $Y_\lambda = \phi(n)(Y_{\frac{\lambda}{n}})$.

The right-inverses $\psi(n)$ are the ring morphisms defined by linearly extending the map on the base elements $\psi(n)(Y_\lambda) = \frac{1}{n}(Y_{\frac{\lambda}{n}} + Y_{\frac{\lambda+1}{n}} + \ldots + Y_{\frac{\lambda+n-1}{n}})$ (check that these are indeed ring maps, that is that $\psi(n)(Y_\lambda).\psi(n)(Y_\mu) = \psi(n)(Y_{\lambda+\mu})$.

These are indeed right-inverses satisfying the idempotent condition for clearly $\phi(n) \circ \psi(n)(Y_\lambda) = \frac{1}{n}(Y_\lambda + \ldots + Y_\lambda) = Y_\lambda$ and

$$\begin{aligned} \psi(n) \circ \phi(n)(Y_\lambda) = & \quad \psi(n)(Y_{n\lambda}) = \tfrac{1}{n}(Y_\lambda + Y_{\lambda+\frac{1}{n}} + \ldots + Y_{\lambda+\frac{n-1}{n}}) & (3.1) \\ = & \quad Y_\lambda.(\tfrac{1}{n}(Y_0 + Y_{\frac{1}{n}} + \ldots + Y_{\frac{n-1}{n}})) = Y_\lambda E_n & (3.2) \end{aligned}$$

and one verifies that $E_n = \frac{1}{n}(Y_0 + Y_{\frac{1}{n}} + \ldots + Y_{\frac{n-1}{n}})$ is indeed an idempotent in $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$. In the previous posts in this series we have already seen that with these definitions we have indeed that the BC-algebra is the bi-crystalline graded ring

$B = \mathcal{H} = \oplus_{\frac{m}{n} \in \mathbb{Q}^+_\times} X_m \mathbb{Q}[\mathbb{Q}/\mathbb{Z}] X_n^*$

and hence is naturally constructed from the skew semi-group graded algebra $A = \oplus_{m \in \mathbb{N}^+_\times} X_m \mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$.

This (probably) explains why the BC-algebra $\mathcal{H}$ is itself usually called and denoted in C^*-algebra papers the skew semigroup-algebra $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}] \bowtie \mathbb{N}^+_\times$ as this subalgebra (our crystalline semi-group graded algebra A) determines the Hecke algebra completely.

Finally, the bi-crystalline idempotents-condition works well in the settings of von Neumann regular algebras (such as all limits of finite dimensional semi-simples, for example $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$) because such algebras excel at *idempotents galore...*

3.5 Adeles and Ideles

Before we can even attempt to describe the adelic description of the Bost-Connes Hecke algebra and its symmetries, we'd probably better recall the construction and properties of adeles and ideles. Let's start with the p-adic numbers $\hat{\mathbb{Z}}_p$ and its field of fractions $\hat{\mathbb{Q}}_p$. For p a prime number we can look at the finite rings $\mathbb{Z}/p^n\mathbb{Z}$ of all integer classes modulo p^n. If two numbers define the same element in $\mathbb{Z}/p^n\mathbb{Z}$ (meaning that their difference is a multiple of p^n), then they certainly define the same class in any $\mathbb{Z}/p^k\mathbb{Z}$ when $k \leq n$, so we have a sequence of ringmorphisms between finite rings

$\ldots \rightarrow^{\phi_{n+1}} \mathbb{Z}/p^n\mathbb{Z} \rightarrow^{\phi_n} \mathbb{Z}/p^{n-1}\mathbb{Z} \rightarrow^{\phi_{n-1}} \ldots \rightarrow^{\phi_3} \mathbb{Z}/p^2\mathbb{Z} \rightarrow^{\phi_2} \mathbb{Z}/p\mathbb{Z}$

The ring of *p-adic integers* $\hat{\mathbb{Z}}_p$ can now be defined as the collection of all (infinite) sequences of elements $(\ldots, x_n, x_{n-1}, \ldots, x_2, x_1)$ with $x_i \in \mathbb{Z}/p^i\mathbb{Z}$ **such that** $\phi_i(x_i) = x_{i-1}$ for all natural numbers i. Addition and multiplication are defined componentwise and as all the maps ϕ_i are ringmorphisms, this produces no compatibility problems.

One can put a topology on $\hat{\mathbb{Z}}_p$ making it into a compact ring. Here's the trick : all components $\mathbb{Z}/p^n\mathbb{Z}$ are finite so they are compact if we equip these sets with the discrete topology (all subsets are opens). But then, Tychonov's product theorem asserts that the product-space $\prod_n \mathbb{Z}/n\mathbb{Z}$ with the product topology is again a compact topological space. As $\hat{\mathbb{Z}}_p$ is a closed subset, it is compact too.

By construction, the ring $\hat{\mathbb{Z}}_p$ is a domain and hence has a field of fraction which we will denote by $\hat{\mathbb{Q}}_p$. These rings give the p-local information of the rational numbers $\mathbb{Q}$. We will now 'glue together' these local data over all possible prime numbers p into *adeles*.

So, forget the above infinite product used to define the p-adics, below we will work with another infinite product, one factor for each prime number.

The *adeles* $\mathcal{A}$ are the restricted product of the $\hat{\mathbb{Q}}_p$ over $\hat{\mathbb{Z}}_p$ for all prime numbers p. By 'restricted' we mean that elements of $\mathcal{A}$ are exactly those infinite vectors $a = (a_2, a_3, a_5, a_7, a_{11}, \ldots) = (a_p)_p \in \prod_p \hat{\mathbb{Q}}_p$ such that all but finitely of the components $a_p \in \hat{\mathbb{Z}}_p$. Addition and multiplication are defined component-wise and the restriction condition is compatible with both addition and multiplication. So, $\mathcal{A}$ is the *adele ring*. Note that most people call this $\mathcal{A}$ the finite Adeles as we didn't consider infinite places, i will distinguish between the two notions by writing adeles resp. Adeles for the finite resp. the full blown version. The adele ring $\mathcal{A}$ has as a subring the infinite product $\mathcal{R} = \prod_p \hat{\mathbb{Z}}_p$. If you think of $\mathcal{A}$ as a version of $\mathbb{Q}$ then $\mathcal{R}$ corresponds to $\mathbb{Z}$ (and next time we will see that there is a lot more to this analogy).

The *ideles* are the group of invertible elements of the ring $\mathcal{A}$, that is, $\mathcal{I} = \mathcal{A}^*$. That s, an element is an infinite vector $i = (i_2, i_3, i_5, \ldots) = (i_p)_p$ with all $i_p \in \hat{\mathbb{Q}}_p^*$ and for all but finitely many primes we have that $i_p \in \hat{\mathbb{Z}}_p^*$.

As we will have to do explicit calculations with ideles and adeles we need to recall some facts about the structure of the unit groups $\hat{\mathbb{Z}}_p^*$ and $\hat{\mathbb{Q}}_p^*$. If we denote $U = \hat{\mathbb{Z}}_p^*$, then projecting it to the unit group of each of its components we get for each natural number n an exact sequence of groups

$1 \to U_n \to U \to (\mathbb{Z}/p^n\mathbb{Z})^* \to 1$. In particular, we have that $U/U_1 \simeq (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ as the group of units of the finite field $\mathbb{F}_p$ is cyclic of order p-1. But then, the induced exact sequence of finite abelian groups below splits

$1 \to U_1/U_n \to U/U_n \to \mathbb{F}_p^* \to 1$ and as the unit group $U = \underset{\leftarrow}{lim} U/U_n$ we deduce that $U = U_1 \times V$ where $\mathbb{F}_p^* \simeq V = x \in U | x^{p-1} = 1$ is the specified unique subgroup of U of order p-1. All that remains is to determine the structure of U_1. If $p \neq 2$, take $\alpha = 1 + p \in U_1 - U_2$ and let $\alpha_n \in U_1/U_n$ denote the image of α, then one verifies that α_n is a cyclic generator of order p^{n-1} of U_1/U_n.

But then, if we denote the isomorphism $\theta_n : \mathbb{Z}/p^{n-1}\mathbb{Z} \to U_1/U_n$ between the ADDITIVE group $\mathbb{Z}/p^{n-1}\mathbb{Z}$ and the MULTIPLICATIVE group U_1/U_n by the map $z \mapsto \alpha_n^z$, then we have a compatible commutative diagram

[tex]

$$\begin{tikzcd}
\mathbb{Z}/p^n\mathbb{Z} \arrow[r, "\theta_{n+1}"] \arrow[d] & U_1/U_{n+1} \arrow[d] \\
\mathbb{Z}/p^{n-1}\mathbb{Z} \arrow[r, "\theta_n"] & U_1/U_n
\end{tikzcd}$$

[/tex]

and as $U_1 = \underset{\leftarrow}{lim}\, U_1/U_n$ this gives an isomorphism between the multiplicative group U_1 and the additive group of $\hat{\mathbb{Z}}_p$. In case $p = 2$ we have to start with an element $\alpha \in U_2 - U_3$ and repeat the above trick. Summarizing we have the following structural information about the unit group of p-adic integers

$$\hat{\mathbb{Z}}_p^* \simeq \begin{cases} \hat{\mathbb{Z}}_{p,+} \times \mathbb{Z}/(p-1)\mathbb{Z}\ (p \neq 2) \\ \hat{\mathbb{Z}}_{2,+} \times \mathbb{Z}/2\mathbb{Z}\ (p = 2) \end{cases}$$

Because every unit in $\hat{\mathbb{Q}}_p^*$ can be written as $p^n u$ with $u \in \hat{\mathbb{Z}}_p^*$ we deduce from this also the structure of the unit group of the p-adic field

$$\hat{\mathbb{Q}}_p^* \simeq \begin{cases} \mathbb{Z} \times \hat{\mathbb{Z}}_{p,+} \times \mathbb{Z}/(p-1)\mathbb{Z}\ (p \neq 2) \\ \mathbb{Z} \times \hat{\mathbb{Z}}_{2,+} \times \mathbb{Z}/2\mathbb{Z}\ (p = 2) \end{cases}$$

Right, now let us start to make the connection with the apparently abstract ringtheoretical post from last time where we introduced **semigroup crystalline graded** rings without explaining why we wanted that level of generality.

Consider the semigroup $\mathcal{I} \cap \mathcal{R}$, that is all ideles $i = (i_p)_p$ with all $i_p = p^{n_p} u_p$ with $u_p \in \hat{\mathbb{Z}}_p^*$ and $n_p \in \mathbb{N}$ with $n_p = 0$ for all but finitely many primes p. Then, we have an exact sequence of semigroups

$1 \rightarrow \mathcal{G} \rightarrow \mathcal{I} \cap \mathcal{R} \rightarrow^{\pi} \mathbb{N}^+_{\times} \rightarrow 1$ where the map is defined (with above notation) $\pi(i) = \prod_p p^{n_p}$ and exactness follows from the above structural results when we take $\mathcal{G} = \prod_p \hat{\mathbb{Z}}_p^*$.

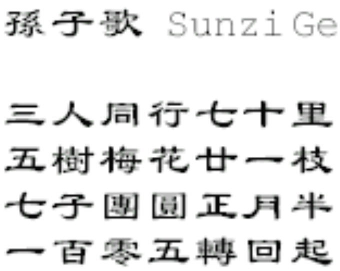
This gives a glimpse of where we are heading. Last time we identified the Bost-Connes Hecke algebra $\mathcal{H}$ as a bi-crystalline group graded algebra determined by a $\mathbb{N}^+_{\times}$-semigroup crystalline graded algebra over the group algebra $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$. Next, we will extend this construction starting from a $\mathcal{I} \cap \mathcal{R}$-semigroup crystalline graded algebra over the same group algebra. The upshot is that we will have a natural action by automorphisms of the group $\mathcal{G}$ on the Bost-Connes algebra. And... the group $\mathcal{G} = \prod_p \hat{\mathbb{Z}}_p^*$ is the Galois group of the cyclotomic field extension $\mathbb{Q}^{cyc}$!

But, in order to begin to understand this, we will need to brush up our rusty knowledge of algebraic number theory...

3.6 Chinese remainders and adele-classes

Oystein Ore mentions the following puzzle from Brahma-Sphuta-Siddhanta (Brahma's Correct System) by Brahmagupta :

”An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?”



孫子歌 Sunzi Ge

三人同行七十里
五樹梅花廿一枝
七子團圓正月半
一百零五轉回起

Here's a similar problem from ”Advanced Number Theory” by Harvey Cohn (always, i wonder how one might 'discreetly request' these remainders...) :

Exercise 5 : In a game for guessing a person's age x, one discreetly requests three remainders : r1 when x is divided by 3, r2 when x is divided by 4, and r3 when x is divided by 5. Then x=40 r1 + 45 r2 + 36 r3 modulo 60.

Clearly, these problems are all examples of the Chinese Remainder Theorem.

Chinese because one of the first such problems was posed by Sunzi (4th century AD) in the book Sunzi Suanjing. (according to ChinaPage the answer is contained in the song on the left hand side.)

```
There are certain things whose number is unknown.
Repeatedly divided by 3, the remainder is 2;
by 5 the remainder is 3;
and by 7 the remainder is 2.
```

```
What will be the number?
```

The Chinese Remainder Theorem asserts that when $N = n_1 n_2 \dots n_k$ with the n_i pairwise coprime, then there is an isomorphism of abelian groups $\mathbb{Z}/N\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$. Equivalently, given coprime numbers n_i one can always solve the system of congruence identities

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

and all integer solutions are congruent to each other modulo $N = n_1 n_2 \dots n_k$.

We will need this classical result to prove that $\mathbb{Q}/\mathbb{Z} \simeq \mathcal{A}/\mathcal{R}$ where (as before) $\mathcal{A}$ is the additive group of all *adeles* and where $\mathcal{R}$ is the subgroup $\prod_p \mathbb{Z}_p$ (i'll drop all 'hats' from now on, so the p-adic numbers are $\mathbb{Q}_p = \hat{\mathbb{Q}}_p$ and the p-adic integers are denoted $\mathbb{Z}_p = \hat{\mathbb{Z}}_p$).

As we will have to do calculations with p-adic numbers, it is best to have them in a canonical form using **digits**. A system of digits $\mathbf{D}$ of $\mathbb{Q}_p$ consists of zero and a system of representatives of units of $\mathbb{Z}_p^*$ modulo $p\mathbb{Z}_p$. The most obvious choice of digits is $\mathbf{D} = 0, 1, 2, \dots, p-1$ which we will use today. ((later we will use another system of digits, the Teichmuller digits using $p-1$-th root of unities in $\mathbb{Q}_p$.)) Fixing a set of digits $\mathbf{D}$, any p-adic number $a_p \in \mathbb{Q}_p$ can be expressed uniquely in the form

$a_p = \sum_{n=deg(a_p)}^{\infty} a_p(n)p^n$ with all 'coefficients' $a_p(n) \in \mathbf{D}$ and $deg(a_p)$ being the lowest p-power occurring in the description of a_p.

Recall that an adele is an element $a = (a_2, a_3, a_5, \dots) \in \prod_p \mathbb{Q}_p$ such that for almost all prime numbers p $a_p \in \mathbb{Z}_p$ (that is $deg(a_p) \geq 0$). Denote the finite set of primes p such that $deg(a_p) < 0$ with $\mathbf{P} = p_1, \dots, p_k$ and let $d_i = -deg(a_{p_i})$. Then, with $N = p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}$ we have that $Na_{p_i} \in \mathbb{Z}_{p_i}$. Observe that for all other prime numbers $q \notin \mathbf{P}$ we have $(N, q) = 1$ and therefore N is invertible in $\mathbb{Z}_q$.

Also $N = p_i^{d_i} K_i$ with $K_i \in \mathbb{Z}_{p_i}^*$. With respect to the system of digits $\mathbf{D} = 0, 1, \dots, p-1$ we have

$$Na_{p_i} = \underbrace{K_i \sum_{j=0}^{d_i - 1} a_{p_i}(-d_i + j)p_i^j}_{=\alpha_i} + K_i \textstyle\sum_{j \geq d_i} a_{p_i}(-d_i + j)p_i^j \in \mathbb{Z}_{p_i}$$

Note that $\alpha_i \in \mathbb{Z}$ and the Chinese Remainder Theorem asserts the existence of an integral solution $M \in \mathbb{Z}$ to the system of congruences

$$\begin{cases} M \equiv \alpha_1 \text{ modulo } p_1^{d_1} \\ M \equiv \alpha_2 \text{ modulo } p_2^{d_2} \\ \vdots \\ M \equiv \alpha_k \text{ modulo } p_k^{d_k} \end{cases}$$

But then, for all $1 \leq i \leq k$ we have $Na_{p_i} - M = p_i^{d_i} \sum_{j=0}^{\infty} b_i(j)p^j$ (with the $b_i(j) \in \mathbf{D}$) and therefore

$a_{p_i} - \frac{M}{N} = \frac{1}{K_i} \sum_{j=0}^{\infty} b_i(j)p^j \in \mathbb{Z}_{p_i}$

But for all other primes $q \notin \mathbf{P}$ we have that $\alpha_q \in \mathbb{Z}_q$ and that $N \in \mathbb{Z}_q^*$ whence for those primes we also have that $\alpha_q - \frac{M}{N} \in \mathbb{Z}_q$.

Finally, observe that the diagonal embedding of $\mathbb{Q}$ in $\prod_p \mathbb{Q}_p$ lies entirely in the adele ring $\mathcal{A}$ as a rational number has only finitely many primes appearing in its denominator. Hence, identifying $\mathbb{Q} \subset \mathcal{A}$ via the diagonal embedding we can rephrase the above as

$a - \frac{M}{N} \in \mathcal{R} = \prod_p \mathbb{Z}_p$

That is, any adele class $\mathcal{A}/\mathcal{R}$ has as a representant a rational number. But then, $\mathcal{A}/\mathcal{R} \simeq \mathbb{Q}/\mathbb{Z}$ which will allow us to give an adelic version of the Bost-Connes algebra!

Btw. there were 301 eggs.

3.7 ABC on Adelic Bost-Connes

The adelic interpretation of the Bost-Connes Hecke algebra $\mathcal{H}$ is based on three facts we've learned in the previous sections :

1. The diagonal embedding of the rational numbers $\delta : \mathbb{Q} \to \prod_p \mathbb{Q}_p$ has its image in the adele ring $\mathcal{A}$.
2. There is an exact sequence of semigroups $1 \to \mathcal{G} \to \mathcal{I} \cap \mathcal{R} \to \mathbb{N}^+_\times \to 1$ where $\mathcal{I}$ is the idele group, that is the units of $\mathcal{A}$, where $\mathcal{R} = \prod_p \mathbb{Z}_p$ and where $\mathcal{G}$ is the group (!) $\prod_p \mathbb{Z}_p^*$.
3. There is an isomorphism of additive groups $\mathbb{Q}/\mathbb{Z} \simeq \mathcal{A}/\mathcal{R}$.

Because $\mathcal{R}$ is a ring we have that $a\mathcal{R} \subset \mathcal{R}$ for any $a = (a_p)_p \in \mathcal{I} \cap \mathcal{R}$. Therefore, we have an induced 'multiplication by a' morphism on the additive group $\mathcal{A}/\mathcal{R} \to^{a.} \mathcal{A}/\mathcal{R}$ which is an epimorphism for all $a \in \mathcal{I} \cap \mathcal{R}$.

In fact, it is easy to see that the equation $a.x = y$ for $y \in \mathcal{A}/\mathcal{R}$ has precisely $n_a = \prod_p p^{d(a)}$ solutions. In particular, for any $a \in \mathcal{G} = \prod_p \mathbb{Z}_p^*$, multiplication by a is an isomorphism on $\mathcal{A}/\mathcal{R} = \mathbb{Q}/\mathbb{Z}$.

But then, we can form the [crystalline semigroup graded][3] skew-group algebra $\mathbb{Q}(\mathbb{Q}/\mathbb{Z}) \bowtie (\mathcal{I} \cap \mathcal{R})$. It is the graded vectorspace $\oplus_{a \in \mathcal{I} \cap \mathcal{R}} X_a \mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ with commutation relation $Y_\lambda X_a = X_a Y_{a\lambda}$ for the base-vectors Y_λ with $\lambda \in \mathbb{Q}/\mathbb{Z}$. Recall from the bi-crystalline section we need to use approximation (or the Chinese remainder theorem) to determine the class of $a\lambda$ in $\mathbb{Q}/\mathbb{Z}$.

We can also extend it to a bi-crystalline graded algebra because multiplication by $a \in \mathcal{I} \cap \mathcal{R}$ has a left-inverse which determines the commutation relations $Y_\lambda X_a^* = X_a^*(\frac{1}{n_a})(\sum_{a.\mu=\lambda} Y_\mu)$. Let us call this bi-crystalline graded algebra $\mathcal{H}_{big}$, then we have the following facts

1. For every $a \in \mathcal{G}$, the element X_a is a unit in $\mathcal{H}_{big}$ and $X_a^{-1} = X_a^*$. Conjugation by X_a induces on the subalgebra $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ the map $Y_\lambda \to Y_{a\lambda}$.
2. Using the diagonal embedding δ restricted to $\mathbb{N}^+_\times$ we get an embedding of algebras $\mathcal{H} \subset \mathcal{H}_{big}$ and conjugation by X_a for any $a \in \mathcal{G}$ sends $\mathcal{H}$ to itself. However, as the $X_a \notin \mathcal{H}$, the induced automorphisms are now outer!

Summarizing : the Bost-Connes Hecke algebra $\mathcal{H}$ encodes a lot of number-theoretic information :

- the *additive* structure is encoded in the sub-algebra which is the group-algebra $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$

- the *multiplicative* structure in encoded in the epimorphisms given by multiplication with a positive natural number (the commutation relation with the X_m
- the *automorphism group* of $\mathbb{Q}/\mathbb{Z}$ extends to outer automorphisms of $\mathcal{H}$

That is, the Bost-Connes algebra can be seen as a **giant mashup** of number-theory of $\mathbb{Q}$. So, if one can prove something specific about this algebra, it is bound to have interesting number-theoretic consequences.

But how will we study $\mathcal{H}$? Well, the bi-crystalline structure of it tells us that $\mathcal{H}$ is a 'good'-graded algebra with part of degree one the group-algebra $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$. This group-algebra is a formally smooth algebra and we study such algebras by studying their finite dimensional representations.

Hence, we should study 'good'-graded formally smooth algebras (such as $\mathcal{H}$) by looking at their *graded* representations. This will then lead us to Connes' "fabulous states"...

3.8 God given time

If you ever sat through a lecture by Alain Connes you will know about his insistence on the 'canonical dynamic nature of noncommutative manifolds'. If you haven't, he did write a blog post Heart bit 1 about it.

"I'll try to explain here that there is a definite "supplément d'me" obtained in the transition from classical (commutative) spaces to the noncommutative ones. The main new feature is that "noncommutative spaces generate their own time" and moreover can undergo thermodynamical operations such as cooling, distillation etc... "

Here a section from his paper A view of mathematics:

"Indeed even at the coarsest level of understanding of a space provided by measure theory, which in essence only cares about the quantity of points in a space, one nds unexpected completely new features in the noncommutative case. While it had been long known by operator algebraists that the theory of von-Neumann algebras represents a far reaching extension of measure theory, the main surprise which occurred at the beginning of the seventies is that such an algebra M inherits from its noncommutativity a *god-given time evolution*:

$\delta : \mathbb{R} \to Out(M)$

where $OutM = AutM/IntM$ is the quotient of the group of automorphisms of M by the normal subgroup of inner automorphisms. This led in my thesis to the reduction from type III to type II and their automorphisms and eventually to the classification of injective factors. "

Even a commutative manifold has a kind of dynamics associated to it. Take a suitable vectorfield, consider the flow determined by it and there's your 'dynamics', or a one-parameter group of automorphisms on the functions. Further, other classes of noncommutative algebras have similar features. For example, Cuntz and Quillen showed that also formally smooth algebras (the noncommutative manifolds in the algebraic world) have natural Yang-Mills flows associated to them, giving a one-parameter subgroup of automorphisms.

Let us try to keep far from mysticism and let us agree that by 'time' (let alone 'god given time') we mean a one-parameter subgroup of algebra automorphisms of the noncommutative algebra. In nice cases, such as some von-Neumann algebras this canonical subgroup is canonical in the sense that it is unique upto inner automorphisms.

In the special case of the Bost-Connes algebra these automorphisms σ_t are given by $\sigma_t(X_n) = n^{it}X_n$ and $\sigma_t(Y_\lambda) = Y_\lambda$.

This one-parameter subgroup is crucial in the definition of the so called KMS-states (for Kubo-Martin and Schwinger) which is our next goal.

3.9 KMS, Gibbs and the zeta-function

Time to wrap up this series on the Bost-Connes algebra. Here's what we have learned so far : the convolution product on double cosets

$\begin{bmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{bmatrix} \setminus \begin{bmatrix} 1 & \mathbb{Q} \\ 0 & \mathbb{Q}_{>0} \end{bmatrix} / \begin{bmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{bmatrix}$

is a noncommutative algebra, the Bost-Connes Hecke algebra $\mathcal{H}$, which is a bi-crystalline graded algebra (somewhat weaker than 'strongly graded') with part of degree one the group-algebra $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$. Further, $\mathcal{H}$ has a natural one-parameter family of algebra automorphisms σ_t defined by $\sigma_t(X_n) = n^{it}X_n$ and $\sigma_t(Y_\lambda) = Y_\lambda$.

For any algebra A together with a one-parameter family of automorphisms σ_t one is interested in *KMS-states* or *Kubo-Martin-Schwinger states* with parameter β, KMS_β (this parameter is often called the 'inverse temperature' of the system) as these are suitable equilibria states. Recall that a **state** is a special linear functional ϕ on A (in particular it must have norm one) and it belongs to KMS_β if the following commutation relation holds for all elements $a, b \in A$

$\phi(a\sigma_{i\beta}(b)) = \phi(ba)$

Let us work out the special case when A is the matrix-algebra $M_n(\mathbb{C})$. To begin, all algebra-automorphisms are inner in this case, so any one-parameter family of automorphisms is of the form

$\sigma_t(a) = e^{itH}ae^{-itH}$

where e^{itH} is the matrix-exponential of the $n \times n$ matrix H. For any parameter β we claim that the linear functional

$\phi(a) = \frac{1}{tr(e^{-\beta H})}tr(ae^{-\beta H})$

is a KMS-state.Indeed, we have for all matrices $a, b \in M_n(\mathbb{C})$ that

$\phi(a\sigma_{i\beta}(b)) = \frac{1}{tr(e^{-\beta H})}tr(ae^{-\beta H}be^{\beta H}e^{-\beta H})$

$= \frac{1}{tr(e^{-\beta H})}tr(ae^{-\beta H}b) = \frac{1}{tr(e^{-\beta H})}tr(bae^{-\beta H}) = \phi(ba)$

(the next to last equality follows from cyclic-invariance of the trace map). These states are usually called *Gibbs states* and the normalization factor $\frac{1}{tr(e^{-\beta H})}$ (needed because a state must have norm one) is called the *partition function* of the system. Gibbs states have arisen from the study of ideal gases and the place to read up on all of this are the first two chapters of the second volume of "Operator algebras and quantum statistical mechanics" by Ola Bratelli and Derek Robinson.

This gives us a method to construct KMS-states for an arbitrary algebra A with one-parameter automorphisms σ_t : take a simple n-dimensional representation $\pi : A \mapsto M_n(\mathbb{C})$, find the matrix H determining the image of the automorphisms $\pi(\sigma_t)$ and take the Gibbs states as defined before.

Let us return now to the Bost-Connes algebra $\mathcal{H}$. We don't know any finite dimensional simple representations of $\mathcal{H}$ but, sure enough, have plenty of **graded** simple representations. By the usual strongly-graded-yoga they should correspond to simple finite dimensional representations of the part of degree one $\mathbb{Q}[\mathbb{Q}/\mathbb{Z}]$ (all of them being one-dimensional and corresponding to characters of $\mathbb{Q}/\mathbb{Z}$).

Hence, for any $u \in \mathcal{G} = \prod_p \hat{\mathbb{Z}}_p^*$ we have a graded simple $\mathcal{H}$-representation $S_u = \oplus_{n \in \mathbb{N}_+} \mathbb{C} e_n$ with action defined by

$$\begin{cases} \pi_u(X_n)(e_m) = e_{nm} \\ \pi_u(Y_\lambda)(e_m) = e^{2\pi i n u.\lambda} e_m \end{cases}$$

Here, $u.\lambda$ is computed using the 'chinese-remainder-identification' $\mathcal{A}/\mathcal{R} = \mathbb{Q}/\mathbb{Z}$.

Even when the representations S_u are not finite dimensional, we can mimic the above strategy : we should find a linear operator H determining the images of the automorphisms $\pi_u(\sigma_t)$. We claim that the operator is defined by $H(e_n) = log(n)e_n$ for all $n \in \mathbb{N}_+$. That is, we claim that for elements $a \in \mathcal{H}$ we have

$$\pi_u(\sigma_t(a)) = e^{itH} \pi_u(a) e^{-itH}$$

So let us compute the action of both sides on e_m when $a = X_n$. The left hand side gives $\pi_u(n^{it} X_n)(e_m) = n^{it} e_{mn}$ whereas the right-hand side becomes

$$e^{itH} \pi_u(X_n) e^{-itH}(e_m) = e^{itH} \pi_u(X_n) m^{-it} e_m =$$

$$e^{itH} m^{-it} e_{mn} = (mn)^{it} m^{-it} e_{mn} = n^{it} e_{mn}$$

proving the claim. For any parameter β this then gives us a KMS-state for the Bost-Connes algebra by

$$\phi_u(a) = \frac{1}{Tr(e^{-\beta H})} Tr(\pi_u(a) e^{-\beta H})$$

Finally, let us calculate the normalization factor (or partition function) $\frac{1}{Tr(e^{-\beta H})}$. Because $e^{-\beta H}(e_n) = n^{-\beta} e_n$ we have for that the trace

$$Tr(e^{-\beta H}) = \sum_{n \in \mathbb{N}_+} \frac{1}{n^\beta} = \zeta(\beta)$$

is equal to the Riemann zeta-value $\zeta(\beta)$ (at least when $\beta > 1$).

Summarizing, we started with the definition of the Bost-Connes algebra $\mathcal{H}$, found a canonical one-parameter subgroup of algebra automorphisms σ_t and computed that the natural equilibria states with respect to this 'time evolution' have as their partition function the Riemann zeta-function. Voila!

series 4

THE ABSOLUTE POINT REVISITED

4.1 The absolute point, coming of age at 25?

For years now some people whisper that geometry over 'the absolute point', or 'the field with one element', will soon lead to a proof of the most enigmatic of all millennium one-million-dollar questions : the Riemann hypothesis.

Even child prodigies have to deliver something verifiable by the age of 25, or face being remembered as yet another unfulfilled promise. Hopefully, 2010 will be the year we see the absolute point finally mature, at 25.

But, isn't the 'field with one element'-idea much older? Wasn't Jacques Tits the one who thought of it first, way back in 1957? Well, technically, he didn't call it the field with one element, but rather the 'field of characteristic one', and, his interest was in the relation between (finite) Lie groups and their associated Weyl groups. He surely never claimed a possible application to the Riemann hypothesis.

What is this Riemann-idea all about, and when was it first uttered? Well, given the analogy between integers and polynomials over finite fields, one might hope that $\mathbf{spec}(\mathbb{Z})$ would be a kind of curve over this 'absolute point' $\mathbf{spec}(\mathbb{F}_1)$. As a consequence, the product $\mathbf{spec}(\mathbb{Z}) \times_{\mathbf{spec}(\mathbb{F}_1)} \mathbf{spec}(\mathbb{Z})$ would not only make sense, but be a surface bearing some kind of intersection theory, so one could then perhaps mimic Weils proof of the Riemann hypothesis over function fields.

James Borger writes in a footnote to his recent paper Lambda-rings and the field with one element : "The origins of this idea are unknown to me. Manin (in his paper Lectures on zeta functions and motives) mentions it explicitly. According to Smirnov (letter to Yuri Manin, September 29th 2003), the idea occurred to him in 1985 and he mentioned it explicitly in a talk in Shafarevich's seminar in 1990. It may well be that a number of people have had the idea independently since the appearance of Weil's proof."

I've glanced through Manin's paper and didn't find an explicit mention of the Riemann-idea. Sure, on page one he mentions 'Descartes' products of $\mathbf{spec}(\mathbb{Z})$, and the paper is all about motives and the connection with zeta-functions and at several times he makes a point to the effect that a further study of the geometry over the absolute point $\mathbf{spec}(\mathbb{F}_1)$ might be interesting, but I didn't find the claimed quote.

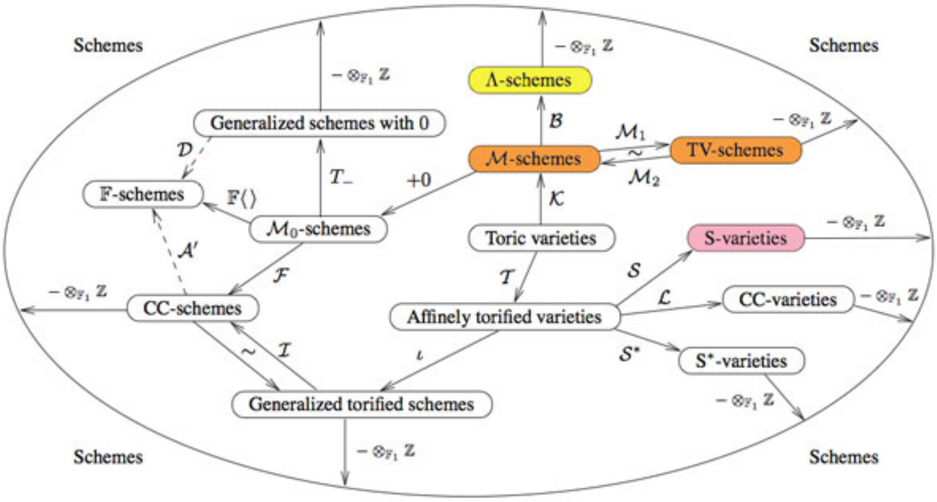
The Smirnov letterS (there is one dated September 29th and one November 29th) are mentioned in Manin's paper The notion of dimension in geometry and algebra. In the body of the paper, they are only referenced once : "Answer 3: dim Spec $\mathbb{Z} = \infty$? This guess involves the conjectural existence of a geometrical world defined over an absolute point Spec F1 where F1 is a mythical field with one element. For some insights about this world, see [Ti], [Sm1], [Sm2] (the letters), [KapSm], [Ma2], [Sou]."

Evidently, Borger's information is based on a private conversation with Yuri I. Manin, and I'd love to hear the full story. Anyway, we can safely date the Riemann-absolute-point idea back as far back as 1985!

4.2 Art and the absolute point (1)

In his paper Cyclotomy and analytic geometry over $\mathbb{F}_1$ Yuri I. Manin sketches and compares four approaches to the definition of a geometry over $\mathbb{F}_1$, the elusive field with one element. He writes : "Preparing a colloquium talk in Paris, I have succumbed to the temptation to associate them with some dominant trends in the history of art."

Remember that the search for the absolute point ***spec***$(\mathbb{F}_1)$ originates from the observation that ***spec***$(\mathbb{Z})$, the set of all prime numbers together with 0, is too large to serve as the terminal object in Grothendieck's theory of commutative schemes. The last couple of years have seen a booming industry of proposals, to the extent that Javier Lopez Pena and Oliver Lorscheid decided they had to draw a map of $\mathbb{F}_1$-land.

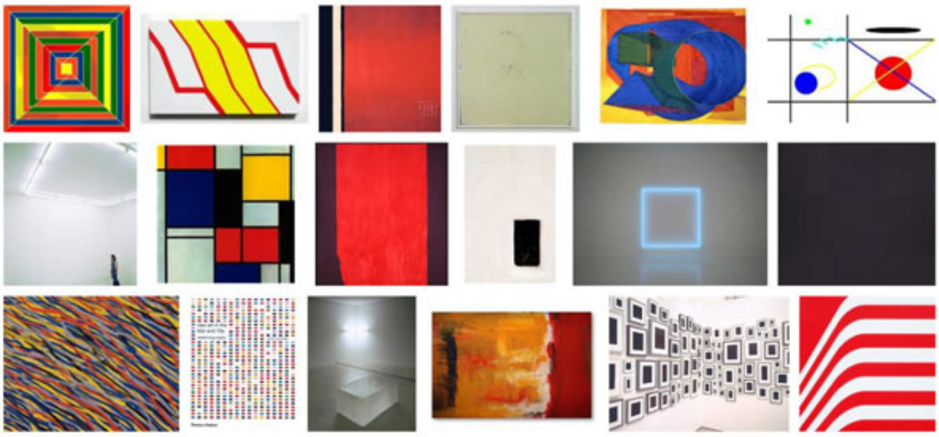

Schemes
Schemes
$- \otimes_{\mathbb{F}_1} \mathbb{Z}$
$- \otimes_{\mathbb{F}_1} \mathbb{Z}$
Λ-schemes
$- \otimes_{\mathbb{F}_1} \mathbb{Z}$
Generalized schemes with 0
$\mathcal{B}$
$\mathcal{M}_1$
$\sim$
$\mathcal{M}_2$
$\mathcal{M}$-schemes
TV-schemes
$\mathcal{D}$
$\mathbb{F}$-schemes
$\mathbb{F}\langle\rangle$
$\mathcal{T}_-$
+0
$\mathcal{M}_0$-schemes
$\mathcal{K}$
Toric varieties
S-varieties
$- \otimes_{\mathbb{F}_1} \mathbb{Z}$
$\mathcal{A}'$
$\mathcal{F}$
$\mathcal{S}$
$\mathcal{T}$
$- \otimes_{\mathbb{F}_1} \mathbb{Z}$
CC-schemes
$\mathcal{L}$
CC-varieties
$- \otimes_{\mathbb{F}_1} \mathbb{Z}$
Affinely torified varieties
$\sim$
$\mathcal{I}$
ι
$\mathcal{S}^*$
S*-varieties
$- \otimes_{\mathbb{F}_1} \mathbb{Z}$
Generalized torified schemes
Schemes
$- \otimes_{\mathbb{F}_1} \mathbb{Z}$
Schemes

Manin only discusses the colored proposals (TV=Toen-Vaquie, M=Deitmar, S=Soule and Λ=Borger) and compares them to these art-history trends.

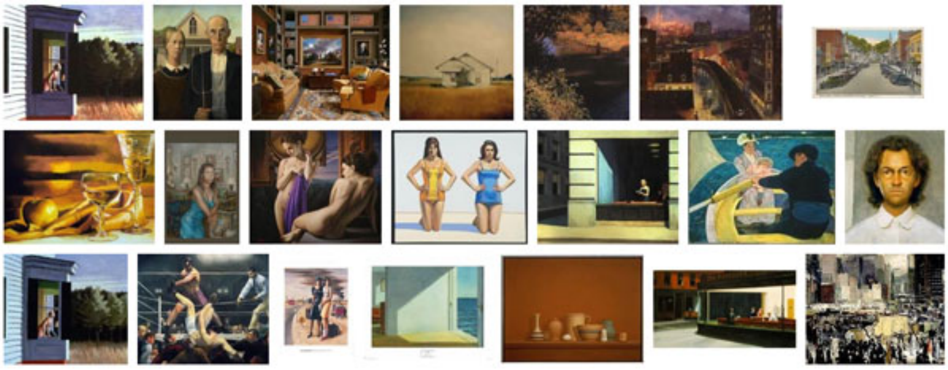
Toen and Vaquie : Abstract Expressionism

In Under ***spec***($\mathbb{Z}$) Bertrand Toen and Michel Vaquie argue that geometry over $\mathbb{F}_1$ is a special case of algebraic geometry over a symmetric monoidal category, taking the simplest example namely sets and direct products. Probably because of its richness and abstract nature, Manin associates this approach to Abstract Expressionism (a.o. Karel Appel, Jackson Pollock, Mark Rothko, Willem de Kooning).

Deitmar : Minimalism



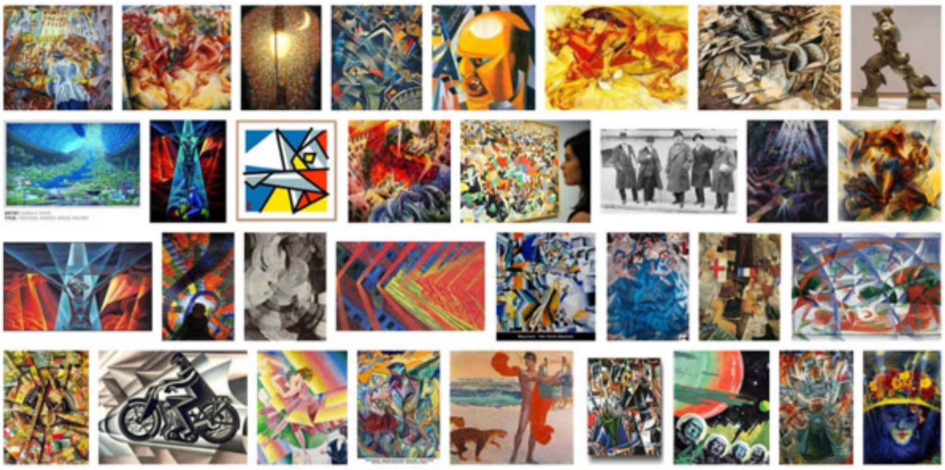
Because monoids are the 'commutative algebras' in sets with direct products, an equivalent proposal is that of Anton Deitmar in Schemes over $\mathbb{F}_1$ in which the basic affine building blocks are spectra of monoids, topological spaces whose points are submonoids satisfying a primeness property. Because Deitmar himself calls this approach a 'minimalistic' one it is only natural to associate to it Minimalism where the work is stripped down to its most fundamental features. Prominent artists associated with this movement include Donald Judd, John McLaughlin, Agnes Martin, Dan Flavin, Robert Morris, Anne Truitt, and Frank Stella.



Soule : Critical Realism

in Les varietes sur le corps a un element Christophe Soule defines varieties over $\mathbb{F}_1$ to be specific schemes X over $\mathbb{Z}$ together with a form of 'descent data' as well as an additional $\mathbb{C}$-algebra, morally the algebra of functions on the real place. Because of this Manin associates to it Critical Realism in philosophy. There are also 'realism' movements in art such as American Realism (o.a. Edward Hopper and John Sloan).

Borger : Futurism



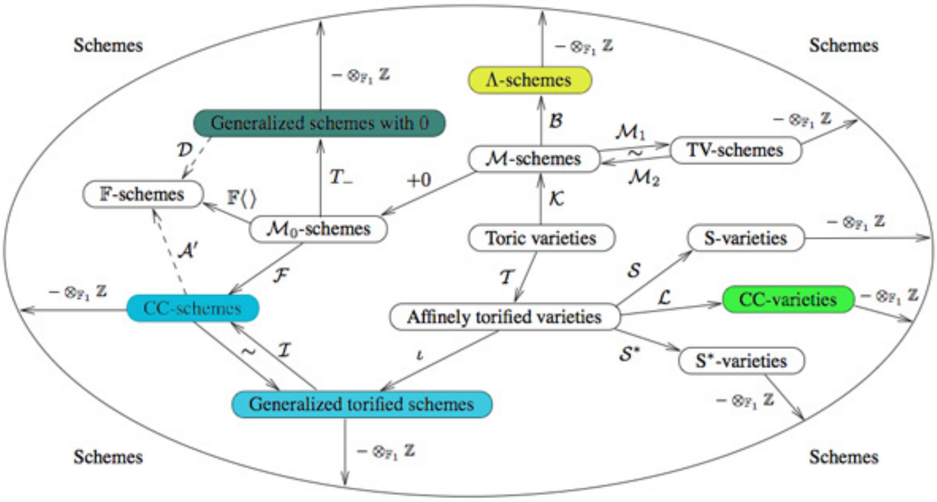
James Borger's paper Lambda-rings and the field with one element offers a totally new conception of the descent data from $\mathbb{Z}$ to $\mathbb{F}_1$, namely that of a λ-ring in the sense of Grothendieck. Because Manin expects this approach to lead to progress in the field, he connects it to Futurism, an artistic and social movement that originated in Italy in the early 20th century.

4.3 Art and the absolute point (2)

In the previous section, we did recall Manin's comparisons between some approaches to geometry over the absolute point ***spec***$(\mathbb{F}_1)$ and trends in the history of art.

In the comments to that post, Javier Lopez-Pena wrote that he and Oliver Lorscheid briefly contemplated the idea of extending Manin's artsy-dictionary to all approaches they did draw on their Map of $\mathbb{F}_1$-land.

So this time, we will include here Javier's and Oliver's insights on the colored pieces below in their map : CC=Connes-Consani, Generalized torified schemes=Lopez Pena-Lorscheid, Generalized schemes with 0=Durov and, this time, Λ=Manin-Marcolli.



Durov : romanticism

In his 568 page long Ph.D. thesis New Approach to Arakelov Geometry Nikolai Durov introduces a vast generalization of classical algebraic geometry in which both Arakelov geometry and a more exotic geometry over $\mathbb{F}_1$ fit naturally. Because there were great hopes and expectations it would lead to a big extension of algebraic geometry, Javier and Oliver associate this approach to romantism. From wikipedia : "The modern sense of a romantic character may be expressed in Byronic ideals of a gifted, perhaps misunderstood loner, creatively following the dictates of his inspiration rather than the standard ways of contemporary society."

Manin and Marcolli : impressionism

Yuri I. Manin in Cyclotomy and analytic geometry over $\mathbb{F}_1$ and Matilde Marcolli in Cyclotomy and endomotives develop a theory of analytic geometry over $\mathbb{F}_1$ based on analytic functions 'leaking out of roots of unity'. Javier and Oliver depict such functions as 'thin, but visible brush strokes at roots of 1' and therefore associate this approach to impressionism. Frow wikipedia : 'Characteristics of Impressionist paintings include: relatively small, thin, yet visible brush strokes; open composition; emphasis on accurate depiction of light in its changing qualities (often accentuating the effects of the passage of time); common, ordinary subject matter; the inclusion of movement as a crucial element of human perception and experience; and unusual visual angles.'

Connes and Consani : cubism

In On the notion of geometry over $\mathbb{F}_1$ Alain Connes and Katia Consani develop their extension of Soule's approach. A while ago I've done a couple of posts on this. Javier and Oliver associate this approach to cubism (a.o. Pablo Picasso and Georges Braque) because of the weird juxtapositions of the simple monoidal pieces in this approach.

Lopez-Pena and Lorscheid : deconstructivism

Torified varieties and schemes were introduced by Javier Lopez-Pena and Oliver Lorscheid in Torified varieties and their geometries over $\mathbb{F}_1$ to get lots of examples of varieties over the absolute point in the sense of both Soule and Connes-Consani. Because they were fragmenting schemes into their ”fundamental pieces” they associate their approach to deconstructivism.

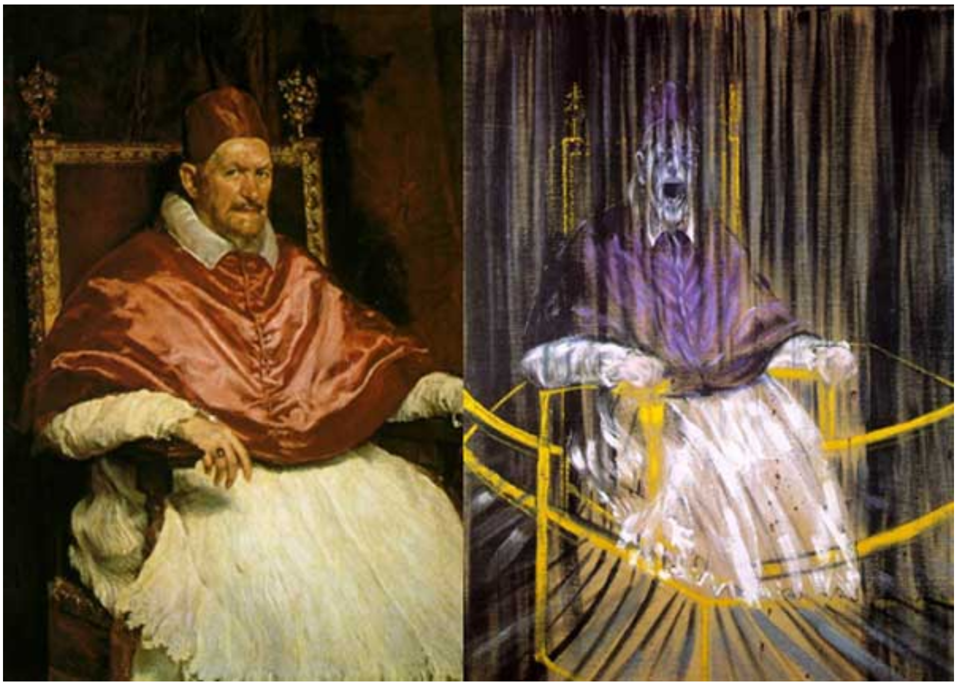
4.4 Art and the absolute point (3)

We have recalled comparisons between approaches to define a geometry over the absolute point and art-historical movements, first those due to Yuri I. Manin, subsequently some extra ones due to Javier Lopez Pena and Oliver Lorscheid.

In these comparisons, the art trend appears to have been chosen more to illustrate a key feature of the approach or an appreciation of its importance, rather than giving a visual illustration of the varieties over $\mathbb{F}_1$ the approach proposes.

Some time ago, we've had a couple of posts trying to depict noncommutative varieties, first the illustrations used by Shahn Majid and Matilde Marcolli, and next my own mental picture of it.

In this post, we'll try to do something similar for affine varieties over the absolute point. To simplify things drastically, I'll divide the islands in the Lopez Pena-Lorscheid map of $\mathbb{F}_1$ land in two subsets : the *former approaches* (all but the Λ-schemes) and the *current approach* (the Λ-scheme approach due to James Borger).



The former approaches : Francis Bacon ”The Pope” (1953)

The general consensus here was that in going from $\mathbb{Z}$ to $\mathbb{F}\_1$ one looses the additive structure and retains only the multiplicative one. Hence, ’commutative algebras’ over $\mathbb{F}\_1$ are (commutative) monoids, and mimicking Grothendieck’s functor of points approach to algebraic geometry, a scheme over $\mathbb{F}_1$ would then correspond to a functor

$h_Z \; : \; \mathbf{monoids} \longrightarrow \mathbf{sets}$

Such functors are described largely by combinatorial data (see for example the recent blueprint-paper by Oliver Lorscheid), and, if the story would stop here, any Rothko painting could be used as illustration.

Most of the former approaches add something though (buzzwords include ’Arakelov’, ’completion at ∞’, ’real place’ etc.) in order to connect the virtual geometric object over $\mathbb{F}\_1$ with existing real, complex or integral schemes. For example, one can make the virtual object visible via an evaluation map $h\_Z \rightarrow h\_X$ which is a natural transformation, where X is a complex variety with its usual functor of points h_X and to connect both we associate to a monoid M its complex monoid-algebra $\mathbb{C}M$. An integral scheme Y can then be said to be ’defined over $\mathbb{F}\_1$’, if h_Z becomes a subfunctor of its usual functor of points h_Y (again, assigning to a monoid its integral monoid algebra $\mathbb{Z}M$) and Y is the ’best’ integral scheme approximation of the complex evaluation map.

To illustrate this, consider the painting Study after Velzquez’s Portrait of Pope Innocent X by Francis Bacon (right-hand painting above) which is a distorted version of the left-hand painting Portrait of Innocent X by Diego Velzquez.

Here, Velzquez’ painting plays the role of the complex variety which makes the combinatorial gadget h_Z visible, and, Bacon’s painting depicts the integral scheme, build up from this combinatorial data, which approximates the evaluation map best.

All of the former approaches more or less give the same very small list of integral schemes defined over $\mathbb{F}_1$, none of them motivic interesting.

The current approach : Jackson Pollock "No. 8" (1949)

An entirely different approach was proposed by James Borger in [Λ-rings and the field with one element][6]. He proposes another definition for commutative $\mathbb{F}$_1-algebras, namely λ-rings (in the sense of Grothendieck's Riemann-Roch) and he argues that the λ-ring structure (which amounts in the sensible cases to a family of endomorphisms of the integral ring lifting the Frobenius morphisms) can be viewed as descent data from $\mathbb{Z}$ to $\mathbb{F}$_1.

The list of integral schemes of finite type with a λ-structure coincides roughly with the list of integral schemes defined over $\mathbb{F}$_1 in the other approaches, but Borger's theory really shines in that it proposes long sought for mystery-objects such as $\mathbf{spec}(\mathbb{Z}) \times$ _$\mathbf{spec}(\mathbb{F}$_1$)\mathbf{spec}(\mathbb{Z})$. If one accepts Borger's premise, then this object should be the geometric object corresponding to the Witt-ring $W(\mathbb{Z})$. Recall that the role of Witt-rings in $\mathbb{F}$_1-geometry was anticipated by Manin in Cyclotomy and analytic geometry over $\mathbb{F}_1$.

But, Witt-rings and their associated Witt-spaces are huge objects, so one needs to extend arithmetic geometry drastically to include such 'integral schemes of infinite type'. Borger has made a couple of steps in this direction in The basic geometry of Witt vectors, II: Spaces.

To depict these new infinite dimensional geometric objects I've chosen for Jackson Pollock's painting No. 8. It is no coincidence that Pollock-paintings also appeared in the depiction of noncommutative spaces. In fact, Matilde Marcolli has made the connection between λ-rings and noncommutative geometry in Cyclotomy and endomotives by showing that the Bost-Connes endomotives are universal for λ-rings.

4.5 Big Witt rings for everybody

Next time you visit your math-library, please have a look whether these books are still on the shelves : Michiel Hazewinkel's Formal groups and applications, William Fulton's and Serge Lange's Riemann-Roch algebra and Donald Knutson's lambda-rings and the representation theory of the symmetric group.

I wouldn't be surprised if one or more of these books are borrowed out, probably all of them to the same person. I'm afraid I'm that person in Antwerp...

Lately, there's been a renewed interest in λ-rings and the endo-functor W assigning to a commutative algebra its ring of big Witt vectors, following Borger's new proposal for a geometry over the absolute point.

Fig. 4.1: H.W. Lenstra

However, as Hendrik Lenstra writes in his 2002 course-notes on the subject Construction of the ring of Witt vectors : ”The literature on the functor W is in a somewhat unsatisfactory state: nobody seems to have any interest in Witt vectors beyond applying them for a purpose, and they are often treated in appendices to papers devoting to something else; also, the construction usually depends on a set of implicit or unintelligible formulae. Apparently, anybody who wishes to understand Witt vectors needs to construct them personally. That is what is now happening to myself.”

Before doing a series on Borger’s paper, we’d better run through Lenstra’s elegant construction in a couple of posts. Let A be a commutative ring and consider the multiplicative group of all ’one-power series’ over it $\Lambda(A) = 1 + tA[[t]]$. Our aim is to define a commutative ring structure on $\Lambda(A)$ taking as its ADDITION the MULTIPLICATION of power series.

That is, if $u(t), v(t) \in \Lambda(A)$, then we define our addition $u(t) \oplus v(t) = u(t) \times v(t)$. This may be slightly confusing as the ZERO-element in $\Lambda(A), \oplus$ will then turn be the constant power series 1...

We are now going to define a multiplication $\otimes$ on $\Lambda(A)$ which is distributively with respect to $\oplus$ and turns $\Lambda(A)$ into a commutative ring with ONE-element the series $(1-t)^{-1} = 1 + t + t^2 + t^3 + \ldots$.

We will do this inductively, so consider $\Lambda_n(A)$ the (classes of) one-power series truncated at term n, that is, the kernel of the natural augmentation map between the multiplicative group-units $A[t]/(t^{n+1})^* \rightarrow A^*$. Again, taking multiplication in $A[t]/(t^{n+1})$ as a new addition rule $\oplus$, we see that $(\Lambda_n(A), \oplus)$ is an Abelian group, whence a $\mathbb{Z}$-module.

For all elements $a \in A$ we have a scaling operator ϕ_a (sending $t \rightarrow at$) which is an A-ring endomorphism of $A[t]/(t^{n+1})$, in particular multiplicative wrt. ×. But then, ϕ_a is an additive endomorphism of $(\Lambda_n(A), \oplus)$, so is an element of the endomorphism-RING $End_{\mathbb{Z}}(\Lambda_n(A))$. Because composition (being the multiplication in this endomorphism ring) of scaling operators is clearly commutative ($\phi_a \circ \phi_b = \phi_{ab}$) we can define a commutative RING E being the subring of $End_{\mathbb{Z}}(\Lambda_n(A))$ generated by the operators ϕ_a.

The action turns $(\Lambda_n(A), \oplus)$ into an E-module and we define an E-module morphism $E \rightarrow \Lambda_n(A)$ by $\phi_a \mapsto \phi_a((1-t)^{-1}) = (1-at)^{-a}$.

All of this looks pretty harmless, but the upshot is that we have now equipped the image of this E-module morphism, say $L_n(A)$ (which is the additive subgroup of $(\Lambda_n(A), \oplus)$ generated by the elements $(1-at)^{-1})$ with a commutative multiplication $\otimes$ induced by the rule $(1-at)^{-1} \otimes (1-bt)^{-1} = (1-abt)^{-1}$.

Explicitly, $L_n(A)$ is the set of one-truncated polynomials $u(t)$ with coefficients in A such that one can find elements $a_1, \ldots, a_k \in A$ such that $u(t) \equiv (1-a_1t)^{-1} \times \ldots \times (1-a_k)^{-1}\ mod\ t^{n+1}$. We multiply $u(t)$ with another such truncated one-polynomial $v(t)$ (taking elements $b_1, b_2, \ldots, b_l \in A$) via

$$u(t) \otimes v(t) = ((1-a_1t)^{-1} \oplus \ldots \oplus (1-a_k)^{-1}) \otimes ((1-b_1t)^{-1} \oplus \ldots \oplus (1-b_l)^{-1})$$

and using distributivity and the multiplication rule this gives the element $\prod_{i,j}(1-a_ib_jt)^{-1}\ mod\ t^{n+1} \in L_n(A)$. Being a ring-quotient of E we have that $(L_n(A), \oplus, \otimes)$ is a commutative ring, and, from the construction it is clear that L_n behaves functorially.

For rings A such that $L_n(A) = \Lambda_n(A)$ we are done, but in general $L_n(A)$ may be strictly smaller. The idea is to use functoriality and do the relevant calculations in a larger ring $A \subset B$ where we can multiply the two truncated one-polynomials and observe that the resulting truncated polynomial still has all its coefficients in A.

Here's how we would do this over $\mathbb{Z}$: take two irreducible one-polynomials u(t) and v(t) of degrees r resp. s smaller or equal to n. Then over the complex numbers we have $u(t) = (1 - \alpha_1 t) \ldots (1 - \alpha_r t)$ and $v(t) = (1 - \beta_1) \ldots (1 - \beta_s t)$. Then, over the field $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$ we have that $u(t), v(t) \in L_n(K)$ and hence we can compute their product $u(t) \otimes v(t)$ as before to be $\prod_{i,j}(1 - \alpha_i \beta_j t)^{-1} \ mod \ t^{n+1}$. But then, all coefficients of this truncated K-polynomial are invariant under all permutations of the roots α_i and the roots β_j and so is invariant under all elements of the Galois group. But then, these coefficients are algebraic numbers in $\mathbb{Q}$ whence integers. That is, $u(t) \otimes v(t) \in \Lambda_n(\mathbb{Z})$. It should already be clear from this that the rings $\Lambda_n(\mathbb{Z})$ contain a lot of arithmetic information!

For a general commutative ring A we will copy this argument by considering a free overing $A^{(\infty)}$ (with 1 as one of the base elements) by formally adjoining roots. At level 1, consider M_0 to be the set of all non-constant one-polynomials over A and consider the ring

$A^{(1)} = \bigotimes_{f \in M_0} A[X]/(f) = A[X_f, f \in M_0]/(f(X_f), f \in M_0)$

The idea being that every one-polynomial $f \in M_0$ now has one root, namely $\alpha_f = \overline{X_f}$ in $A^{(1)}$. Further, $A^{(1)}$ is a free A-module with basis elements all α_f^i with $0 \leq i < deg(f)$.

Good! We now have at least one root, but we can continue this process. At level 2, M_1 will be the set of all non-constant one-polynomials over $A^{(1)}$ and we use them to construct the free overing $A^{(2)}$ (which now has the property that every $f \in M_0$ has at least two roots in $A^{(2)}$). And, again, we repeat this process and obtain in succession the rings $A^{(3)}, A^{(4)}, \ldots$. Finally, we define $A^{(\infty)} = \underset{\rightarrow}{lim} \ A^{(i)}$ having the property that every one-polynomial over A splits entirely in linear factors over $A^{(\infty)}$.

But then, for all $u(t), v(t) \in \Lambda_n(A)$ we can compute $u(t) \otimes v(t) \in \Lambda_n(A^{(\infty)})$. Remains to show that the resulting truncated one-polynomial has all its entries in A. The ring $A^{(\infty)} \otimes_A A^{(\infty)}$ contains two copies of $A^{(\infty)}$ namely $A^{(\infty)} \otimes 1$ and $1 \otimes A^{(\infty)}$ and the intersection of these two rings in exactly A (here we use the freeness property and the additional fact that 1 is one of the base elements). But then, by functoriality of L_n, the element $u(t) \otimes v(t) \in L_n(A^{(\infty)} \otimes_A A^{(\infty)})$ lies in the intersection $\Lambda_n(A^{(\infty)} \otimes 1) \cap \Lambda_n(1 \otimes A^{(\infty)}) = \Lambda_n(A)$. Done!

Hence, we have endo-functors Λ_n in the category of all commutative rings, for every number n. Reviewing the construction of L_n one observes that there are natural transformations $L_{n+1} \rightarrow L_n$ and therefore also natural transformations $\Lambda_{n+1} \rightarrow \Lambda_n$. Taking the inverse limits $\Lambda(A) = \underset{\leftarrow}{lim} \Lambda_n(A)$ we therefore have the 'one-power series' endo-functor $\Lambda : \mathbf{comm} \rightarrow \mathbf{comm}$ which is 'almost' the functor W of big Witt vectors. Next time we'll take you through the identification using 'ghost variables' and how the functor Λ can be used to define the category of λ-rings.

4.6 Lambda-rings for formula-phobics

In 1956, Alexander Grothendieck (middle) introduced λ-rings in an algebraic-geometric context to be commutative rings A equipped with a bunch of operations λ^i (for all numbers $i \in \mathbb{N}_+$) satisfying a list of rather obscure identities.

Fig. 4.2: A. Grothendieck

From the easier ones, such as

$\lambda^0(x) = 1, \lambda^1(x) = x, \lambda^n(x+y) = \sum_i \lambda^i(x)\lambda^{n-i}(y)$

to those expressing $\lambda^n(x.y)$ and $\lambda^m(\lambda^n(x))$ via specific universal polynomials. An attempt to capture the essence of λ-rings without formulas?

Lenstra's elegant construction (see post 4.5) of the 1-power series rings $(\Lambda(A), \oplus, \otimes)$ requires only one identity to remember

$$(1-at)^{-1} \otimes (1-bt)^{-1} = (1-abt)^{-1}.$$

Still, one can use it to show the existence of ring-morphisms $\gamma_n : \Lambda(A) \to A$, for all numbers $n \in \mathbb{N}_+$. Consider the formal 'logarithmic derivative'

$$\gamma = \frac{tu(t)'}{u(t)} = \sum_{i=1}^{\infty} \gamma_i(u(t))t^i \ : \ \Lambda(A) \to A[[t]]$$

where $u(t)'$ is the usual formal derivative of a power series. As this derivative satisfies the chain rule, we have

$$\gamma(u(t) \oplus v(t)) = \frac{t(u(t)v(t))'}{u(t)v(t)} = \frac{t(u(t)'v(t)+u(t)v(t)'}{u(t)v(t))} = \frac{tu(t)'}{u(t)} + \frac{tv(t)'}{v(t)} = \gamma(u(t)) + \gamma(v(t))$$

and so all the maps $\gamma_n : \Lambda(A) \to A$ are additive. To show that they are also multiplicative, it suffices by functoriality to verify this on the special 1-series $(1-at)^{-1}$ for all $a \in A$. But,

$$\gamma((1-at)^{-1}) = \frac{t\frac{a}{(1-at)^2}}{(1-at)} = \frac{at}{(1-at)} = at + a^2t^2 + a^3t^3 + \ldots$$

That is, $\gamma_n((1-at)^{-1}) = a^n$ and Lenstra's identity implies that γ_n is indeed multiplicative! A first attempt :

hassle-free definition 1 : a commutative ring A is a λ-ring if and only if there is a ringmorphism $s_A : A \to \Lambda(A)$ splitting γ_1, that is, such that $\gamma_1 \circ s_A = id_A$.

In particular, a λ-ring comes equipped with a multiplicative set of ring-endomorphisms $s_n = \gamma_n \circ s_A : A \to A$ satisfying $s_m \circ s_m = s_{mn}$. One can then define a λ-ringmorphism to be a ringmorphism commuting with these endo-morphisms.

The motivation being that λ-rings are known to form a subcategory of commutative rings for which the 1-power series functor is the right adjoint to the functor forgetting the λ-structure. In particular, if A is a λ-ring, we have a ringmorphism $A \to \Lambda(A)$ corresponding to the identity morphism.

But then, what is the connection to the usual one involving all the operations λ^i? Well, one ought to recover those from $s_A(a) = (1 - \lambda^1(a)t + \lambda^2(a)t^2 - \lambda^3(a)t^3 + ...)^{-1}$.

For s_A to be a ringmorphism will require identities among the λ^i. I hope an expert will correct me on this one, but I'd guess we won't yet obtain all identities required. By the very definition of an adjoint we must have that s_A is a morphism of λ-rings, and, this would require defining a λ-ring structure on $\Lambda(A)$, that is a ringmorphism $s_{AH} : \Lambda(A) \to \Lambda(\Lambda(A))$, the so called Artin-Hasse exponential, to which I'd like to return later.

For now, we can define a multiplicative set of ring-endomorphisms $f_n : \Lambda(A) \to \Lambda(A)$ from requiring that $f_n((1-at)^{-1}) = (1-a^nt)^{-1}$ for all $a \in A$. Another try?

hassle-free definition 2 : A is a λ-ring if and only if there is splitting s_A to γ_1 satisfying the compatibility relations $f_n \circ s_A = s_A \circ s_n$.

But even then, checking that a map $s_A : A \to \Lambda(A)$ is a ringmorphism is as hard as verifying the lists of identities among the λ^i. Fortunately, we get such a ringmorphism for free in the important case when A is of 'characteristic zero', that is, has no additive torsion. Then, a ringmorphism $A \to \Lambda(A)$ exists whenever we have a multiplicative set of ring endomorphisms $F_n : A \to A$ for all $n \in \mathbb{N}_+$ such that for every prime number p the morphism F_p is a lift of the Frobenius, that is, $F_p(a) \in a^p + pA$.

Perhaps this captures the essence of λ-rings best (without the risk of getting an headache) : in characteristic zero, they are the (commutative) rings having a multiplicative set of endomorphisms, generated by lifts of the Frobenius maps.

series 5

SMIRNOV'S APPROACHT TO THE ABC-CONJECTURE

5.1 Smirnov's letters

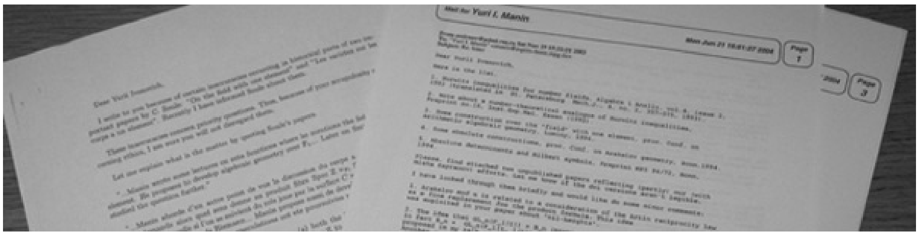
In the paper The notion of dimension in geometry and algebra, Yuri I. Manin writes :

"This guess involves the conjectural existence of a geometrical world defined over an absolute point Spec $\mathbb{F}\_1$ where $\mathbb{F}\_1$ is a mythical field with one element. For some insights about this world, see J. Tits, Sur les analogues algebriques des groupes semisimples complexes, A. Smirnov, Hurwitz inequalities for number fields, A. Smirnov, Letters to Yu. Manin of Sept. 29 and Nov. 29, 2003, M. Kapranov, A. Smirnov, Cohomology determinants and reciprocity laws: number field case, Yu. Manin, Threedimensional hyperbolic geometry as ∞adic Arakelov geometry, C. Soule, Les varietes sur le corps a un element."

The first of two letters from Alexandr Smirnov to Manin also appears in the paper Lambda-rings and the field with one element by James Borger :

"The second purpose is to prove the Riemann hypothesis. With the analogy between integers and polynomials in mind, we might hope that Spec $\mathbb{Z}$ would be a kind of curve over Spec $\mathbb{F}_1$, that Spec $\mathbb{Z} \times$ Spec $\mathbb{Z}$ would not only make sense but be a surface bearing some kind of intersection theory, and that we could then mimic over $\mathbb{Z}$ Weils proof of the Riemann hypothesis over function fields. The origins of this idea are unknown to me. Manin Yuri Manin, Lectures on zeta functions and motives (according to Deninger and Kurokawa) mentions it explicitly. According to Smirnov (Alexandr L. Smirnov, Letter to Y. Manin. September 29, 2003), the idea occurred to him in 1985 and he mentioned it explicitly in a talk in Shafarevichs seminar in 1990. It may well be that a number of people have had the idea independently since the appearance of Weils proof."

I thank Yuri I. Manin and James Borger for providing me with copies of these letters. Some of their content is crucial to understand the genesis of Smirnov's paper A. Smirnov, Hurwitz inequalities for number fields, which is the first paper we will study in the seminar.



From Smirnov's letter to Yu. I. Manin, dated september 29th 2003 (links added):

”As to my investigations, I work on the topic since 1985. Till then the subject has been paid next to no attention, with the exception of a paper by J. Tits (1957) and the idea (due to D. Quillen?) to interpret the Barrat-Priddy-Quillen Theorem as the equality $K(\mathbb{F}_1) = \pi^{st}(S^0)$. ”

”My initial goal was (and still is) to construct a ”world” which contains algebraic geometry as well as arithmetic, and where all constructions from algebraic geometry (including $\mathsf{Spec}\ \mathbb{Z} \times \mathsf{Spec}\ \mathbb{Z}$) would be available. From the beginning I believed that this could give an approach to the Riemann hypothesis (similar to Weil's approach). I started with the idea, known for me from a seminar (early 80-s), that sets can be considered as vectorspaces over $\mathbb{F}_1$. I believed that this idea was promising in view of the mentioned interpretation of the Barrat-Priddy-Quillen Theorem. ”

”Since I couldn't invent $\mathsf{Spec}\ \mathbb{Z} \times \mathsf{Spec}\ \mathbb{Z}$, I worked out a strategy which I have adhered: ”

- ”If we can't develop the whole desired theory, we should invent as many objects over $\mathbb{F}_1$ as possible and establish connections between them.”
- ”Since the situation is extremely rigid, any flexibility of constructions would lead to essential progress.”

”The idea to construct finite extensions of $\mathbb{F}\_1$ (thus getting the missing flexibility) and the suggestion to consider the monoids $0 \cap \boldsymbol{\mu}$ as a naive technical approximation to these extensions arose precisely from this strategy. Having on hand the extensions, I discovered I could effectively work with a number of new objects over $\mathbb{F}\_1$, for instance with $\mathbb{P}^n$. Thus I decided to handle intersection theory (which is part of Weil's approach to the Riemann hypothesis) on the surface

$$\mathbb{P}^1/\mathbb{F}_1 \times \mathsf{Spec}\ \mathbb{Z}$$

instead of the more complicated $\mathsf{Spec}\ \mathbb{Z} \times \mathsf{Spec}\ \mathbb{Z}$. The Hurwitz genus formula for a map of curves $f : X \to Y$ can be viewed as an example of using intersection theory on the surface $X \times Y$, and I started with it.”

” I succeeded in stating a certain approximation to the Hurwitz formula for the ”map”

$$f : \mathsf{Spec}\ \mathbb{Z} \to \mathbb{P}^1/\mathbb{F}_1 \qquad \text{where } f \in \mathbb{Q}$$

It was somewhat surprising (and confirming the importance of the approach) that this approximation gave very profound assertions like the ABC-conjecture and others. An impulse to publish these results was given to me by M. Kapranov after he and V. Voevodsky learned about them (1988 or 1989).”

5.2 Curves

Fix a perfect field k (say a finite field) with algebraic closure $\overline{k}$ and absolute Galois group $G = \mathrm{Gal}(\overline{k}/k)$.

Our aim is to study smooth projective k-curves via their function fields. This will allow us later to associate 'curves' to number fields. We need two categories:

Curves/k

The *objects* are smooth projective algebraic curves defined over k (that is, a smooth closed subvariety C of dimension one of some projective space $\mathbb{P}^n(\overline{k})$ defined by a set of homogeneous polynomials all of their coefficients belonging to k). We will call such objects *curves* defined over k.

The *morphisms* will be surjective algebraic maps $C \to C'$ defined over k (that is, all coordinate functions have their coefficients in k). Remember that any non-constant rational map between two curves is automatically surjective. We will call such morphisms *covers*.

$\mathsf{1Fields}/k$

The *objects* are field extensions K of k of transcendence degree one with k as their 'field of constants'. That is, $K \cap \overline{k} = k$.

The *morphisms* will be field inclusions $K \hookrightarrow K'$ fixing k.

Main result: These categories are (anti)-equivalent to each other. Details are in section I.6 of Robin Hartshorne's Algebraic Geometry when $k = \overline{k}$ and modifications for the general case are in section II.2 of Joseph Silverman's The Arithmetic of Elliptic Curves.

Sketch of proof: The direction from curves to fields is straightforward. The contravariant functor $\mathsf{Curves}/k \longrightarrow \mathsf{1Fields}/k$ assigns to a curve C its function field $k(C)$ (the field consisting of all rational functions $f : C \to \overline{k}$ defined over k). This functor associates to a cover $\phi : C \mapsto C'$ the field-inclusion $\phi^* : k(C') \to k(C)$ obtained by composition (that is, $\phi^*(f) = f \circ \phi : C \to \overline{k}$ for all $f \in k(C')$).

Conversely, the contravariant functor $\mathsf{1Fields}/k \longrightarrow \mathsf{Curves}/k$ assigns to a field K of transcendence degree one

- the *geometric* points $C(\overline{k})$ of the curve C, which is the set of all discrete valuations rings in $K \otimes \overline{k}$ with residue field $\overline{k}$. The Galois group G acts on this set, and,
- the *schematic* points of C are the G-orbits of this action. Equivalently, these are the discrete valuation rings of K with residue field a finite field extension L of k. The degree of such a scheme-point is the size of the G-orbit (or the k-dimension of the residue field L of the discrete valuation ring).

Example: Under this equivalence, the purely transcendental field $k(x)$ corresponds to the projective line $\mathbb{P}^1$ over k. Its geometric points $\mathbb{P}^1(\overline{k})$ are the points

$$\{[\alpha : 1] \; : \; \alpha \in \overline{k}\} \cup \{\infty = [1:0]\}$$

The discrete valuation ring of $\overline{k}(x)$ corresponding to $[\alpha : 1]$ has uniformizing parameter $x - \alpha$ and the one corresponding to ∞ has uniformising parameter $\frac{1}{x}$. The Galois group fixes ∞ and acts on the point $[\alpha : 1]$ as it does on $\alpha \in \overline{k}$. Hence, the schematic points of $\mathbb{P}^1$ are ∞ together with all irreducible monic polynomials in $k[x]$.

Under the equivalence, the set of all non-constant maps $C \mapsto \mathbb{P}^1$ corresponds to the set of all k-field morphisms $k(x) \hookrightarrow k(C)$ and as these are determined by the image of x they are determined by $f \in k(C)$. The cover corresponding to f

$$C(\overline{k}) \mapsto \mathbb{P}^1(\overline{k}) \quad \text{maps} \quad P \mapsto [f(P) : 1]$$

if f is regular in P and to ∞ otherwise.

5.3 What is $\mathbb{P}^1$ over $\mathbb{F}_1$?

The short answer : The geometric points of the projective line $\mathbb{P}^1$ over the 'field with one element' $\mathbb{F}_1$ form the set $\{0, \infty\} \cup \boldsymbol{\mu}$ with $\boldsymbol{\mu}$ the group of all roots of unity. Its schematic points form the set $\{\infty, 0\} \cup \{[1], [2], [3], [4], \cdots\}$ and the degree of the point $[n]$ equals $\phi(n)$.

The longer answer : We have seen in the previous section that the geometric points of $\mathbb{P}^1$ over the finite field $\mathbb{F}_p$ form the set

$$\{0=[0:1],\ \infty=[1:0]\} \cup \{\alpha=[\alpha:1]\ :\ \alpha \in \overline{\mathbb{F}}_p^*\}$$

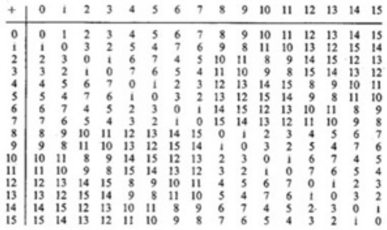
Claim : the multiplicative group of the non-zero elements of the algebraic closure $\overline{\mathbb{F}}_p^*$ is isomorphic as group to the group $\boldsymbol{\mu}^{(p)}$ of all roots of unity of order prime to p.

Clearly, any element $\alpha \in \mathbb{F}^*\_p^n$ has order some divisor of p^n-1 and hence is prime to p. Conversely, if $(m,p)=1$ then $\overline{p}$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ and therefore for some n we have $p^n \cong 1\ mod(m)$. But then, $m|p^n-1$ and there are primitive m-th roots of unity in $\mathbb{F}\_p^n$.

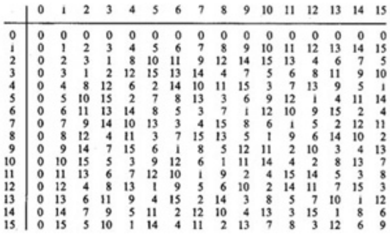
However, describing this correspondence explicitly from a given construction of $\overline{\mathbb{F}}_p$ is very challenging. For example, John Conway proved in ONAG that $\overline{\mathbb{F}}_2$ can be identified with all ordinals smaller than ω^{ω^ω} equipped with nim-addition and multiplication.

Finding the correspondence between small ordinals and odd roots of unity is the topic of the post The odd knights of the round table (and follow-up posts here and here).

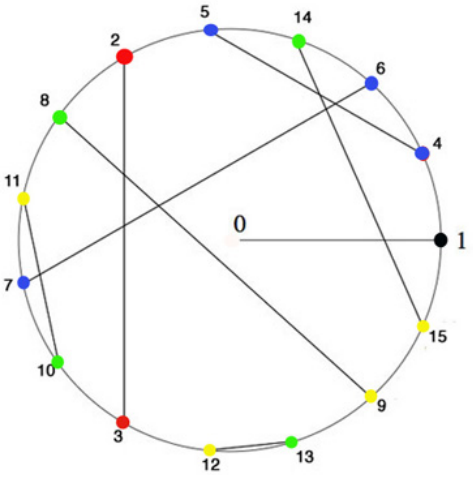
Below is the correpondence between $\mathbb{F}_{2^4}^*$ (identified with the ordinals from 1 to 15) and the 15-th roots of unity (nim-addition and nim-multiplication tables on the left). The lines describe the involution $x \mapsto x+1$.



+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	3	1	8	10	11	9	12	14	15	13	4	6	7	5
3	0	3	1	2	12	15	13	14	4	7	5	6	8	11	9	10
4	0	4	8	12	6	2	14	10	11	15	3	7	13	9	5	1
5	0	5	10	15	2	7	8	13	3	6	9	12	1	4	11	14
6	0	6	11	13	14	8	5	3	7	1	12	10	9	15	2	4
7	0	7	9	14	10	13	3	4	15	8	6	1	5	2	12	11
8	0	8	12	4	11	3	7	15	13	5	1	9	6	14	10	2
9	0	9	14	7	15	6	1	8	5	12	11	2	10	3	4	13
10	0	10	15	5	3	9	12	6	1	11	14	4	2	8	13	7
11	0	11	13	6	7	12	10	1	9	2	4	15	14	5	3	8
12	0	12	4	8	13	1	9	5	6	10	2	14	11	7	15	3
13	0	13	6	11	9	4	15	2	14	3	8	5	7	10	1	12
14	0	14	7	9	5	11	2	12	10	4	13	3	15	1	8	6
15	0	15	5	10	1	14	4	11	2	13	7	8	3	12	6	9



The schematic points of $\mathbb{P}^1$ over $\mathbb{F}\_p$ is the set of all $Gal(\overline{\mathbb{F}}\_p/\mathbb{F}_p) = \hat{\mathbb{Z}}$-orbits on the geometric points, and the degree of a scheme-point is the number of geometric points in the orbit.

Assigning to such a Galois-orbit $\mathcal{O}$ the polynomial $\prod\_\alpha \in \mathcal{O}(x-\alpha)$ identifies the schematic points of $\mathbb{P}^1/\mathbb{F}\_p$ with all irreducible polynomials in $\mathbb{F}_p[x]$ (together with ∞) and the point-degree coincides with the degree of the polynomial.

Concretely : say we have an explicit identification of $\mathbb{F}\_p^{n*}$ with all p^n-1-th roots of unity, then we can find all irreducible polynomials in $\mathbb{F}\_p[x]$ of degree a divisor of n by studying the orbits of these roots of unity under the power-map $z \mapsto z^p$.

In the picture above, we have indicated the different orbits of $\mathbb{F}_{2^4}$ with different colors. There are two orbits of length one : $\{0\}$ corresponding to x and $\{1\}$ corresponding to $x+1$. One orbit of length two $\{2,3\}$ corresponding to the irreducible polynomial x^2+x+1 (check the tables to verfify that this is indeed $(x-2)(x-3)$) and three orbits of length four

$\{4,6,5,7\} \leftrightarrow x^4+x+1$ $\{11,12,9,15\} \leftrightarrow x^4+x^3+1$ $\{14,8,13,10\} \leftrightarrow x^4+x^3+x^2+x+1$

By *analogy* we can now define the geometric points of $\mathbb{P}^1$ over the field with one element $\mathbb{F}$_1 to be the set

$\{0,\infty\} \cup \boldsymbol{\mu}^{(1)}$

where $\boldsymbol{\mu}^{(1)}$ are all roots of unity of order prime to 1, that is just all of them : $\boldsymbol{\mu}$. The schematic points of $\mathbb{P}^1/\mathbb{F}$_1 are then the orbits of this set under the action of the Galois group $Gal(\mathbb{Q}(\boldsymbol{\mu})/\mathbb{Q})$.

One checks that these orbits correspond to $\{0,\infty\}$ and $\{[1],[2],[3],[4],\cdots\}$ where $[n]$ is the orbit consisting of all primitive n-th roots of unity. Consequently, the degree of the scheme-point $[n]$ is equal to $\phi(n)$ with ϕ the Euler function.

5.4 The genus of a curve

We are working towards the proof of the Riemann-Hurwitz genus formula. We want to use only fields and their discrete valuations so that we can port some of this later to number fields.

Above we have seen that any field K of transcendence degree 1 over k with $K \cap \overline{k} = k$ is really the function field $K = k(C)$ of a smooth projective curve C defined over k.

A geometric point $P \in C$ is a discrete valuation ring $\mathcal{O}_P$ in the extended field $K^e = K \otimes \overline{k} = \overline{k}(C)$.

Aim: To determine the genus of C from K^e and the discrete valuation rings $\mathcal{O}_P$.

Divisors: For $f \in K^e$ and $P \in C$ we denote the valuation of f in the discrete valuation ring $\mathcal{O}$_P by ord _$P(f)$ (that is, $f = ut^{\mathrm{ord}\text{ \_}P(f)}$ for t is a uniformizer and u a unit in $\mathcal{O}$_P). We **claim** that there are only finitely many $P \in C$ such that ord _$P(f) \neq 0$ and that $\sum$_$P \in C\,\mathrm{ord}_P(f) = 0$.

We can assume that $f \notin \overline{k}$ and so the subring $\overline{k}[f] \subset K^e$ is a polynomial ring. Let R be the integral closure of $\overline{k}[f]$ in K^e (which is a finite field extension of $\overline{k}(f)$ say of dimension r). Then R is a Dedekind domain, projective of rank r over $\overline{k}[f]$ and there are maximal ideals $\mathcal{P}$_i in R such that

$$(f) = \mathcal{P}\text{\_}1^{e\text{\_}1} \cdots \mathcal{P}\text{\_}s^{e\text{\_}s}$$

Because the localization of R at $\mathcal{P}$_i is a discrete valuation ring with residue field $\overline{k}$, each $\mathcal{P}$_i defines a point P_$i \in C$ and we have $\sum$_ie_$i = r$. Similarly, let S be the integral closure of the polynomial algebra $\overline{k}[\frac{1}{f}]$ in K^e, then there are maximal ideals $\mathcal{Q}$_j (corresponding to points Q_$j \in C$) such that

$$\left(\frac{1}{f}\right) = \mathcal{Q}\text{\_}1^{f\text{\_}1} \cdots \mathcal{Q}\text{\_}t^{f\text{\_}t}$$

and $\sum$_jf_$j = r$. But then the *divisor* of f satisfies the claims

$$\mathrm{div}(f) = \sum\text{\_}P \in C\,\mathrm{ord}\text{ \_}P(f)[P] = \sum\text{\_}i = 1^s e\text{\_}i[P\text{\_}i] - \sum\text{\_}j = 1^t f\text{\_}j[Q\text{\_}j]$$

Differentials forms: Consider the K^e-vectorspace Ω_C spanned by all 'differential forms' $\mathrm{d}f$ where $f \in K^e$, subject to the usual rules:

* $\mathrm{d}(f+g) = \mathrm{d}f + \mathrm{d}g$ for all $f, g \in K^e$. * $\mathrm{d}(fg) = f\,\mathrm{d}g + g\,\mathrm{d}f$ for all $f, g \in K^e$. * $\mathrm{d}a = 0$ for all $a \in \overline{k}$.

We *claim* that Ω_C has dimension one. More precisely, if $x \in K^e$ is transcendental over $\overline{k}$ such that K^e is a finite separable field extension of the subfield $\overline{k}(x)$, then $\Omega\_C = K^e \mathrm{d}x$.

The *proof* is a computation. Let $g \in K^e$ have a minimal polynomial over $\overline{k}(x)$ of the form

$$G(Y) = Y^n + f\_1 Y^{n-1} + \cdots + f\_n - 1Y + f_n$$

with all $f_i \in \overline{k}(x)$. Now consider these two polynomials in $\overline{k}(x)[Y]$:

$G\_1(Y) = nY^{n-1} + (n-1)f\_1 Y^{n-2} + \cdots + f_{n-1}$, and

$G\_2(Y) = Y^n + \frac{\partial f\_1}{\partial x} Y^{n-1} + \cdots + \frac{\partial f\_n - 1}{\partial x} Y + \frac{\partial f\_n}{\partial x}$.

By the above equations among differential forms we get

$$0 = \mathrm{d}G(g) = G\_2(g)\,\mathrm{d}x + G\_1(g)\,\mathrm{d}g$$

Because $G_1(g) \neq 0$ by separability, it follows that $\mathrm{d}g \in K^e \mathrm{d}x$. Done!

Genus: In particular, if t is a uniformizing parameter of the discrete valuation ring $\mathcal{O}\_P$, then for any differential form $\omega \in \Omega\_C$ there is a unique $f \in K^e$ such that $\omega = f\,\mathrm{d}t$. We define $\operatorname{ord}\_P(\omega) = \operatorname{ord}\_P(f)$. Clearly, this number depends only on ω (and P), but not on the choice of uniformizer (check!).

Slightly more involved is the *claim* that $\operatorname{ord}_P(\omega) \neq 0$ for finitely many $P \in C$.

Here's the *idea :* Take $x \in K^e$ such that K^e is a finite separable extension of $\overline{k}(x)$ of dimension r, write $\omega = f\,\mathrm{d}x$ and consider the corresponding cover $x \colon C \to \mathbb{P}^1$. As before, there are at most r points of C lying over a point $Q \in \mathbb{P}^1$. Now, write $K^e = \overline{k}(x)(\alpha)$ and let $D \in \overline{k}(x)$ be the discriminant of the minimal polynomial of α over $\overline{k}(x)$. Then, away from the finite number of poles and zeroes of D, there are precisely r points of C lying over any point $Q \in \mathbb{P}^1$. So, removing a finite number of points from C, in the remaining $P \in C$ we have $f(P) \neq 0, \infty$, $x(P) \neq \infty$ and $x - x(P)$ is a uniformizer of $\mathcal{O}\_P$. But in such points we have $\operatorname{ord}\_P(\omega) = \operatorname{ord}\_P(f\,\mathrm{d}(x - x(P))) = 0$.

The number $\sum\_P \in C \operatorname{ord}_P(\omega)$ is thus well-defined and we *claim* that it doesn't depend on the choice of differential form. For, any other form can be written as $\omega' = f\omega$ for some $f \in K^e$ and then we have

$$\sum\_P \in C \operatorname{ord}\_P(\omega') = \sum\_P \in C(\operatorname{ord}\_P(f) + \operatorname{ord}\_P(\omega))$$

and we know already that $\sum\_P \in C \operatorname{ord}_P(f) = 0$. The **genus** g_C of the curve C is then determined from that number by $2g\_C - 2 = \sum\_P \in C \operatorname{ord}\_P(\omega)$.

Example: Take the projective line $\mathbb{P}^1$ corresponding to the purely transcendental field $\overline{k}(x)$ and consider $\omega = \mathrm{d}x$. In a point $\alpha \neq \infty$ we know that $x - \alpha$ is a uniformizer, so

$$\operatorname{ord}\_\alpha(\omega) = \operatorname{ord}\_\alpha(\mathrm{d}x) = \operatorname{ord}\_\alpha(\mathrm{d}(x-\alpha)) = 0$$

In ∞ the uniformizer is $\frac{1}{x}$, whence

$$\operatorname{ord}\_\infty(\omega) = \operatorname{ord}\_\infty(\mathrm{d}x) = \operatorname{ord}\_\infty\left(-x^2\,\mathrm{d}\left(\frac{1}{x}\right)\right) = -2$$

Thus, $\sum\_P \in \mathbb{P}^1 \operatorname{ord}\_P(\omega) = -2$ and so the genus of the projective line $g_{\mathbb{P}^1} = 0$.