INSTITUTE FOR BASIC SCIENCE CENTER FOR GEOMETRY AND PHYSICS QUANTUM MONDAY

GABRIEL C. DRUMMOND-COLE

1. September 8: Jeehoon Park

[The format of quantum Monday, we'll start at roughly 6:40, the talk will start from 7, and this is supposed to be an extremely informal seminar. Some people may want the bread and cheese and wine and then leave, that's fine. We don't know when it's finished. No one is obliged to come. Today, Jeehoon N will start by talking about group representations and homotopy algebra. You are welcome to interrupt his talk. Let's begin, the time when talk is over is not specified, you can leave whenever you want.]

Please don't—[Why? They can leave]—stay, I didn't specify a verb.

This is about A_∞ homotopy theory arising in representations. What I mean is a linear representation of various stuff. It could be a group representation. So G is a group and look at group homomorphisms to a vector space over $\mathbf{k}$, $\rho : G \to Aut_{\mathbf{k}}(V)$. Or an algebra representation. $\mathbf{k}$ is a field, this can be relaxed as a commutative ring with unity but for simplicity I'll assume it's a field, then Λ is a two-sided $\mathbf{k}$-algebra, you can look at ring homomorphisms $\rho : \Lambda \to End_{\mathbf{k}}(V)$.

The third example is Lie algebra representations, and then you can think about Lie algebra representations $\rho : \mathfrak{g} \to End_{\mathbf{k}}(V)$.

We can understand a group representation as a representation of the group ring and a Lie algebra representation as a representation of the enveloping algebra, so three and one are special cases of the second one.

The homotopy theory is so easy that it's kind of a shame that we didn't realize this thing.

Here's the setting, let's concentrate on the second one, let Λ be a $\mathbf{k}$-algebra with unity. Let A be a two-sided Λ-module. I need one additional assumption, which is that V itself is a ring. I'll let A be V. So I have a map $\rho : \Lambda \to End_{\mathbf{k}}(A)$. So $\lambda \cdot a \cdot u$ gives the composition $\rho(\lambda) \circ mult_a \circ \rho(\mu)$.

We have the general theory of Hochschild homology and cohomology. So how do we define Hochschild homology and cohomology? So the enveloping algebra of Λ, called Λ^e, is $\Lambda \otimes_{\mathbf{k}} \Lambda^{opp}$, where Λ^{opp} is the opposite algebra.

The Hochschild (homology) complex. We usually assume that Λ is $\mathbf{k}$-projective. Since $\mathbf{k}$ is a field, this is always true. A projective resolution X of Λ as a Λ^e-module.

Then $HH_n(\Lambda, A)$ is $Tor_n(A, \Lambda)$, which we can compute as

$$H_n(A \otimes_{\mathbf{k}} \tilde{S}(\Lambda), d)$$

Where

$$\cdots \to S_2(\Lambda) \to S_1(\Lambda) \to S_0(\Lambda) \to \Lambda \to 0$$

Here $S_n(\Lambda) := \Lambda^{\otimes n+2}$.

The bimodule structure is:

$$(\mu \otimes \gamma^*)(\lambda_0 \otimes \cdots \otimes \lambda_{n+1}) = u\lambda_0 \otimes \cdots \otimes \lambda_{n+1}\gamma.$$

We see that $S_n(\Lambda) = \Lambda \otimes_k \tilde{S}_n \otimes_k \Lambda$ where $\tilde{S}_n$ is $\Lambda^{\otimes n}$ which is $\Lambda^e \otimes_{\mathbf{k}} \tilde{S}_n(\Lambda)$.

So for $HH(\Lambda, A)$ we get the complex

$$A \otimes_{\Lambda^e} \Lambda^e \otimes_{\mathbf{k}} \tilde{S}_n(\Lambda)$$

which is just $A \otimes_{\mathbf{k}} \tilde{S}_n(\Lambda) = A \otimes_{\mathbf{k}} T^n(\Lambda)$.

So $d_n : A \otimes_{\mathbf{k}} T^n(\Lambda) \to A \otimes_{\mathbf{k}} T^{n+1}(\Lambda)$ goes by

$$d_n(a\otimes\lambda_1\otimes\cdots\otimes\lambda_n) = (a\cdot\lambda_1)\otimes(\lambda_2\otimes\cdots\otimes\lambda_n)+\sum(-1)^i a\otimes\cdots\otimes\lambda_i\lambda_{i+1}\otimes\cdots\otimes\lambda_n+(-1)^n(\lambda_n a)\otimes(\lambda_1\otimes\cdots\otimes\lambda_{n-1})$$

As a proposition, $d_{n-1} \circ d_n = 0$, so $d^2 = 0$.

Now $\mathcal{A}^-n = A \otimes_{\mathbf{k}} T^n(\Lambda)$. That's a degree inversion, d now increases by one. Now consider $\mathcal{A} = (\bigoplus \mathcal{A}^n, d)$. I call that the dual Hochschild cochain complex. If you don't like that name, forget it.

So far everything is standard. Now assume that A is a Λ-algebra. It's got this additional structure. I'll give the example of Heisenberg representations later. There are so many examples. In your area you have some representation, you get a homotopy algebra for free, and you can apply that to see the meaning.

Then I can define a $\mathbf{k}$-algebra structure on $\mathcal{A}$. We have $\mathcal{A}^{-n} \times \mathcal{A}^{-m} \to \mathcal{A}^{-m-n}$. I multiply in $\mathcal{A}$ and tensor the others.

$$(a \otimes (\lambda_1 \otimes \cdots \otimes \lambda_n))(a' \otimes (\lambda'_1 \otimes \cdots \otimes \lambda'_m) = (aa' \otimes \lambda_1 \otimes \cdots \otimes \lambda'_m)$$

So you have an algebra $\mathcal{A}$ with a product and a differential. This is a so-called homotopy probability algebra.

What can we do? This is not a differential graded algebra in general. You could ask if the product and the differential are compatible. You'll see that we almost never get a dga. So d is not a derivation of $\cdot$.

[Jeehoon doesn't want to calculate this on the board but here it is:]

$$d(aa' \otimes \lambda_1 \otimes \cdots \otimes \lambda'_m) = (aa'\lambda_1 \otimes \lambda_2 \otimes \cdots \otimes \lambda'_m)+$$
$$\sum(-1)^i(aa' \otimes \lambda_1 \otimes \cdots \lambda_i\lambda_{i+1} \cdots \otimes \lambda'_m) + (-1)^n(aa' \otimes \lambda_1 \otimes \cdots \lambda_n\lambda'_1 \otimes \cdots \otimes \lambda'_m)+$$
$$\sum(-1)^{i+n}(aa' \otimes \lambda_1 \otimes \cdots \lambda'_i\lambda'_{i+1} \cdots \otimes \lambda'_m) + (-1)^{n+m}\lambda'_m aa'\lambda_1 \otimes \cdots \otimes \lambda'_{m-1}.$$

On the other hand,

$$d(a \otimes \lambda_1 \otimes \cdots \otimes \lambda_n)(a' \otimes \lambda'_1 \otimes \cdots \otimes \lambda'_m) = a\lambda_1 a' \otimes \lambda_2 \otimes \cdots \otimes \lambda'_m+$$
$$\sum(-1)^i aa'(\lambda_1 \otimes \cdots \otimes \lambda_i\lambda_{i+1} \otimes \cdots \otimes \lambda'_m) + (-1)^n\lambda_n aa' \otimes \lambda_1 \otimes \cdots \otimes \lambda'_m$$

whereas

$$(-1)^n(a \otimes \lambda_1 \otimes \cdots \otimes \lambda_n)d(a' \otimes \lambda'_1 \otimes \cdots \otimes \lambda'_m) = (-1)^n a\lambda'_1 a' \otimes \lambda_1 \otimes \cdots \otimes \lambda'_m+$$
$$\sum(-1)^{n+i}aa'(\lambda_1 \otimes \cdots \otimes \lambda'_i\lambda'_{i+1} \otimes \cdots \otimes \lambda'_m) + (-1)^{n+m}\lambda'_m aa' \otimes \lambda_1 \otimes \cdots \otimes \lambda'_m$$

So the desired difference is

$$((aa'\lambda_1 - a\lambda_1 a') \otimes \lambda_2 \otimes \cdots \otimes \lambda'_m) + (-1)^n(aa' \otimes \lambda_1 \otimes \cdots \lambda_n\lambda'_1 \otimes \cdots \otimes \lambda'_m)-$$
$$(-1)^n\lambda_n aa' \otimes \lambda_1 \otimes \cdots \otimes \lambda'_m - (-1)^n a\lambda'_1 a' \otimes \lambda_1 \otimes \cdots \otimes \lambda'_m+$$
$$(-1)^{n+m}(\lambda'_m aa' - a\lambda'_m a')\lambda_1 \otimes \cdots \otimes \lambda'_{m-1}.$$

There is ambiguity in the notation above because $(a\lambda)a'$ is not necessarily equal to $a(\lambda a')$ but even that doesn't resolve the difficulties.

By letting $\lambda_i = 1$ for all i, this simplifies to $(-1)^n aa' \otimes 1 \otimes \cdots \otimes 1$ so this is only 0 if the product in A is identically zero. [End calculation.]

The reason is, once you have this cochain complex, you want to take the cohomology. You should get a new structure on the cohomology too. Then you need this compatibility. We failed. What should we do? We should try again. Failure is the model of success.

We have to observe the failure and see what's wrong. We have to measure the failure of this. I'll provide you a systematic way of measuring the failure, by an A_∞ algebra. This is just one example and there are other things here that you could do, which I'll explain.

This defines a functor from Λ-algebras to homotopy probability algebras. I'm not really looking at the unity in $\mathcal{A}$.

So functoriality, let me say. Now $\mathcal{M}_\Lambda^{alg}$ is the category whose objects are two-sided Λ-algebras but whose morphisms are Λ-module homomorphisms (not a Λ-algebra homomorphism). Think of a group acting on a function space. There is a multiplication there.

Now $HPA_{\mathbf{k}}$ is the category whose objects are triples: a space V, a product $\cdot$, and a differential d. Here V is a graded vector space $\bigoplus V^n$ and the product is a graded associative ring. The degree of d is one and it squares to 0. There is no compatibility assumed between d and $\cdot$. The morphisms are cochain maps (degree zero and $\mathbf{k}$-linear) from V to V'. In particular, they are not necessarily ring homomorphisms.

Theorem 1.1.
$$A \mapsto \mathcal{A}, \cdot, d$$
is a functor from $\mathcal{M}_\Lambda^{alg} to HPA_{\mathbf{k}}$*.Here* $\mathcal{A}$ *is* $A \otimes_k T(V)$*.*

I need to say what to do if you have a Λ-module homomorphism $A \to A'$ and that is, use that on the first factor of $A \otimes T(\Lambda)$ and the identity on the other. Typically A' will be trivial and then you can just take $\mathbf{k}$.

It's easy to check that $(f \otimes id) \circ d = d' \circ (f \otimes id)$ so $f \otimes id$ is a cochain map. You should also check composition but that's obvious as well.

[Long argument about the functor, whether it is evil, whether these categories deserve to be called categories. Break]

Let me move on to ∞-algebras. I'll define another functor from $HPA_{\mathbf{k}}$ to the category of ∞-homotopy algebras. What we are aiming at is, the most well-known homotopy algebras are A_∞ or L_∞ algebras. In particular, I will construct these A_∞ algebras. This is Professor Park's theory, the descendent functor. What I mean is that I'll give you another family of ∞ homotopy algebras. I want to go from a power series to some other kind of homotopy algebra. But let me do A_∞ first.

So I have $(\mathcal{A}, \cdot, d)$, and the point is that, d is not a derivation of $\cdot$. You compute the failure of derivation and define
$$m_2^d(x, y) = d(x \cdot y) - dx \cdot y - (-1)^{|x|} x \cdot dy.$$
So $m_1^d = d$. I want to define a sequence of maps $m_n^d : T^n\mathcal{A} \to \mathcal{A}$. The only constraint should be that $m_1 = d$ and m_2 is this deviation. Now there are many ways to go to m_3. Let me give you one way that will make this an A_∞-algebra structure on $\mathcal{A}$.

The key power series in the A_∞ case is $\frac{1}{1-x} = 1 + x + x^2 + \cdots$. In Chol-Eun's lecture, he used e^b to talk about this. It's not the exponential, of course. I'll extend this d a little bit. I'll introduce an Artinian algebra. This is a cochain complex so you can take the cohomology, right? This can be an infinite dimensional vector space, of course. $H_d(\mathcal{A})$ is $\bigoplus \mathbf{k}e_\alpha$ for an index. Then we can look at the dual space $H_d(\mathcal{A})^*$ with its dual basis $Hom_{\mathbf{k}}(H_d(\mathcal{A}), \mathbf{k})$ and call the dual basis t^α.

So we'll introduce Artinian $\mathbf{k}$-algebras. $\mathfrak{A}rt_{\mathbf{k}}$ has in it this kind: $\mathbf{k}[|t^\alpha|]/(t^\alpha)^{N+1}$ where α ranges over some finite set and the variables don't commute. I guess I should call that $\mathbf{k} \ll t^\alpha \gg$, some other notation. Call this one $\mathfrak{A}$.

So the maximal idal of $\mathfrak{A}$ is $\overline{(t^\alpha)}$. Then I can define, or extend d and m_n^d to $\mathfrak{A} \otimes \mathcal{A}$. The sign conventions are important so I'll write them down:

$$m_n^d(r_1 \otimes a_1, \ldots, r_n \otimes a_n) = (-1)^{|r_1|+|r_2|(1+|a_1|)+\cdots+|r_n|(1+\cdots+|a_n|)} r_1 \cdots r_n \otimes m_n^d(a_1, \ldots, a_n).$$

This is just the Koszul sign when I define the m_n^d so that they all have degree 1.

This, one more thing, is an algebra structure: $(r_1 \otimes a_1)(r_2 \otimes a_2) = (-1)^{|a_1||r_2|} r_1 r_2 \otimes a_1 a_2$. Keep in mind this sign convention.

Then define m_n^d by the following formula, for x in $(\mathfrak{M}_{\mathfrak{A}} \otimes \mathcal{A})^0$:

$$d(\frac{1}{1-x}) = \frac{1}{1-x} M^d(x) \frac{1}{1-x}$$

So expand this and they should both have the same t terms. Here $M^d(x) = \sum m_n^d(x, \cdots, x)$.

Here $x = r \otimes x$. You can write this out.

[What if you change your homotopy theory? What do you do with M^d?]

You have some power series $P(x)$ and you want to compute its derivative but it doesn't commute. You can look infinitesimally at $P(x + \epsilon \otimes \mu)$ and you get

$$a_0 + a_1(x + \epsilon\mu) + a_2(x + \epsilon\mu) + \cdots$$

and you get

$$P(x) + a_1\epsilon\mu + a_2(x\epsilon\mu + \epsilon\mu x) + a_3(x^2\epsilon\mu + x\epsilon\mu x + \epsilon\mu x^2) + \cdots$$

So you can define this to be $P(x) + P(x, \epsilon\mu, x)$ and you can try to define $d(P(x))$ and this will be $\hat{P}(x, M^d(x), x)$. This will be $a_i m_n^d(x, \cdots x)$, that's what looks right to me. This depends on $P(x)$.

If $P(x)$ is $\frac{1}{1-x}$ then $\hat{P}(x)$ is $\frac{1}{1-x}\mu\frac{1}{1-y}$.

Now you compare the $t^{\alpha_n} \cdots t^{\alpha_1}$ terms. You get these $m_n^d : T^n(\mathcal{A}) \to \mathcal{A}$. I didn't change any order. Miraculously, these form an A_∞ algebra. Let me give you a proof, which is straightforward.

The A_∞ relation is that $\sum m_n(x_1 \cdots m_k, \cdots x_n) = 0$

[Some interruptions, questions about the definition of $\hat{P}$.]

So let $x = t_1 \otimes x_1 + t_2 \otimes x_2$. Then let's try to solve

$$d(1 + x + x^2 + \cdots) = (1 + x + x^2 + \cdots)(dx + m_2^d(x, x) + \cdots)(1 + x + x^2 + \cdots)$$

So we expand this and the left side is, well, this is too hard. Let's do $x = ta$, it's linear in t. But if we scale it should still work. So let's count word length in t. $d1, dx, dx^2$, et cetera is the left side. So $dx = dx$ is the first thing. On the right side we have $d(x^2)$, $m_2(x, x) + x \cdot dx + dx \cdot x$, and this tells us m_2 is the deviation from d being a derivation of $\cdot$. Then for the dx^3 we get $m_3(x, x, x) + xm_2(x, x) + m_2(x, x)x + dx \cdot x^2 + xdx \cdot x + x^2 \cdot dx$.

We get all of this with signs and so on. I spent lots of time to get the sign correct. We have to prove that these m_n form an A_∞ algebra.

[Some discussion. What power series are good? What does rescaling mean?]

The definition, we need $d^2 = 0$. So

$$0 = d(d(\frac{1}{1-x})) = d(\frac{1}{1-x}M^d\frac{1}{1-x})$$

As a lemma, we can calculate

$$d(\frac{1}{1-x}\mu\frac{1}{1-x}) = d(\frac{1}{1-x})\mu\frac{1}{1-x} + \frac{1}{1-x}M^d_x\frac{1}{1-x} + \frac{1}{1-x}\mu d(\frac{1}{1-x})$$

where $M^d_x = m^d_1 + m^d_2(\quad, x) + m^d_2(x, \quad) + \cdots$ Then we get

$$d(\frac{1}{1-x})M^d\frac{1}{1-x} + \frac{1}{1-x}M^d_x(M^d(x))\frac{1}{1-x} + (-1)^1\frac{1}{1-x}M^d(x)d(\frac{1}{1-x})$$

and the first and last terms cancel and you get, after multiplying by $1-x$ before and after, you get the quadratic relation you want $M^d_x(M^d(x))$.

Now morphisms. So for a map $f : (\mathcal{A}, \cdot, d) \to (\mathcal{A}', \cdot', d')$, a cochain map, I claim you can find $\underline{\phi}^f = \phi^f_1, \cdots, \phi^f_n : T^n(\mathcal{A}) \to \mathcal{A}$ to be an A_∞ morphism. Define it by $f(\frac{1}{1-x}) = \frac{1}{1-\sum\phi^f_n(x,\ldots,x)} = \Phi^f(x)$.

Theorem 1.2. *$\underline{\phi}^f$ is an A_∞ morphism.*

We see that $f(1 + x + \cdots) = 1 + \Phi^f(x) + \Phi^f(x)^2 + \cdots$, so $f(x) = \phi^f_1(x)$, $f(x^2) = \phi^f_2(x, x) + f(x)f(x)$, so it's measuring the failure of f from being a ring homomorphism.

To prove it, we have $f(d(\frac{1}{1-x})) = f(\frac{1}{1-x}M^d(x)\frac{1}{1-x})$ but it's also $d'f(\frac{1}{1-x}) = d'(\frac{1}{1-\Phi^f(x)})$. Let's expand that first thing. By a similar lemma,

$$f(\frac{1}{1-x}\mu\frac{1}{1-x}) = \frac{1}{1-\Phi^f(x)}\Phi^f_x(\mu)\frac{1}{1-Phi^f(x)}$$

where as before

$$\Phi^f_x(\mu) = \Phi^f(\mu) + \Phi_2(\mu, x) + \Phi_2(x, \mu) + \cdots$$

If we apply this, we get

$$\frac{1}{1-\Phi^f(x)}\Phi^f_X(M^d(x))\frac{1}{1-\Phi^f(x)}$$

and applying the other lemma on the other side we get

$$\frac{1}{1-\Phi^f(x)}M^{d'}(\Phi^f(x))\frac{1}{1-\Phi^f(x)}$$

I think you get a better definition here of A_∞ homotopy from this. Here we have $(A, \cdot, d)$, and then we have a natural notion of homotopy. The descendent functor gives a natural definition of A_∞ homotopy.

2. September 30: Jeehoon Park

Let me briefly review the situation. There's a starting point of the theory which is this. $\mathbf{k}$ is a field and Λ is a $\mathbf{k}$-algebra, not necessarily commutative. Then A is a Λ-algebra. So this Λ-algebra structure, it's a bimodule $\Lambda \times A \to A \leftarrow A \times \Lambda$. You can think of this action as a representation of Λ in $End_{\mathbf{k}}(V)$. So $\lambda \mapsto \rho(\lambda)$. I'd like to apply this theory to this particular example. Let ρ be a $\mathbf{k}$-algebra homomorphism. The representation space is in A. Then we can define a particular Λ-module structure in this way. $\lambda \cdot a = \rho(\lambda) \circ a$ and $a \cdot \lambda = a \circ \rho(\lambda)$.

That's the key example. Given this situation, we can consider the Hochschild (co)homology theory of Λ with values in A, $HH^i(\Lambda, A)$ and $HH_i(\Lambda, A)$. The homology is $H_i(T(\Lambda) \otimes_{\mathbf{k}} A, d)$. The cohomology is the Ext functor $H^i(Hom(T(\Lambda), A), d)$. Let me recall the differentials d.

In the cohomology,

$$d\nu(x_1, \ldots, x_{n+1}) = x_1 \cdot \nu(x_2, \ldots, x_{n+1}) + \sum (-1)^i \nu(x_1, \ldots, x_i x_{i+1}, \ldots, x_{n+1}) + (-1)^{n+1} \nu(x_1, \ldots, x_n) \cdot x_{n+1}.$$

For $a \otimes (x_1 \otimes \cdots \otimes x_n) \in A \otimes T^n(\Lambda)$, the differential takes this element to

$$a \cdot x_1 \otimes (x_2 \otimes \cdots \otimes x_n) + \sum (-1)^i a \otimes (x_1 \otimes \cdots \otimes x_i x_{i+1} \otimes \cdots \otimes x_n) + (-1)^n x_n \cdot a \otimes (x_1 \otimes \cdots \otimes x_{n-1})$$

So let me put a degree zero binary operator $*$ on $Hom(T^m(A), A) \times Hom(T^n(A), A) \to Hom(T^{m+n}A, A)$. Define this as $f * g(x_1, \ldots, x_{m+n}) = f(x_1, \ldots, x_m) \cdot g(x_{m+1} \cdots x_{m+n})$.

On the homology you can also define a product by

$$a_1 \otimes (x_1 \otimes \cdots \otimes x_m) * a_2 \otimes (y_1 \otimes \cdots \otimes y_n)) = (a_1 a_2) \otimes (x_1 \otimes \cdots \otimes y_n)$$

The natural question is whether these are dgas. The answer is no in general. It's hard to find such an example. What people say is that the game is over, we don't study this.

In the example of A from earlier, the Hochschild cochains are a dga. If you start from a Lie algebra it is still the case that these are dgas. The chains are not.

It turns out that there is a theorem that $Hom(T\Lambda, A), d_\rho, *)$ governs deformations of ρ. You can ask whether $\rho + \tilde{\rho}$ is a ring homomorphism from Λ to A. If $\tilde{\rho}$ satisfies the Maurer-Cartan equation of a dga, $Hom(T\Lambda, A, d_\rho, *)$, then $\rho + \tilde{\rho} \in Hom(\Lambda, A)$. This equation is $d_\rho(\tilde{\rho}) + \tilde{\rho} * \tilde{\rho} = 0$.

As an example, let G be the Galois group $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ which is the limit of finite Galois groups $K/\mathbb{Q}$, with $\mathbf{k} = \overline{\mathbb{F}_p}$. Consider

$$\rho : G \to GL_n(\overline{mathbbF_p}^n) = Aut_{\overline{\mathbb{F}_p}}(\overline{\mathbb{F}_p}^n)$$

and you can ask whether you can lift:

$$\begin{tikzcd}
 & GL_n(\mathfrak{a}) \arrow[d] \\
G \arrow[ur] \arrow[r] & GL_n(\overline{\mathbb{F}_p})
\end{tikzcd}$$

where $\mathfrak{a}$ is a local Artinian ring with residue field $\overline{\mathbb{F}_p}$. If you are not a number theorist you can think about $\overline{\mathbb{F}_p}[x]/(x^n)$.

The theorem says that you can study the lifting by looking at the cochain complex, so you have

$$\rho : \underbrace{\overline{\mathbb{F}_p}[G]}_{\Lambda} \to \underbrace{M_n(\overline{\mathbb{F}_p})}_{A}.$$

In this setting, the tangent space is governed as follows. $H^1(G, V_{ad})$. This governs the freedom. But V_{ad} is basically $M_n(\overline{\mathbb{F}_p})$ with the group action that for γ in G and m a matrix, $m \mapsto \gamma \cdot m \cdot \gamma^{-1}$.

You have a Hochschild cohomology complex for the group cohomology. The only difference is that we use $\gamma m - m\gamma$. These should give the same answer. But you look at this

$$H^1(Hom(T(\overline{\mathbb{F}_p}[G]), M_n(\overline{\mathbb{F}_p})), \delta, *)$$

If you change things a little bit, this will be a differential.

I use δ here instead of d_ρ; let me write it down. $d_\rho(a)(x)$, for instance, is $x \cdot a - a \cdot x$. On the other hand, $\delta(a)(x) = a - \rho(x) a \rho^{-1}(x)$. They have the same homology, but the first one is a dga and the second one is not.

Let me recall some constructions, though.

The descendant A_∞ algebra is defined as

$$d(\frac{1}{1+x}) = \frac{1}{x-1} M^d(x) \frac{1}{1-x}.$$

Here $\sum t^i \otimes x_i = x \in (\mathscr{M}_{\mathfrak{a}} \otimes \mathcal{A})^0$ and $M^d(x) = \sum m_n^d(x, \ldots, x)$ Depending on this power series, there are different ways to measure this. So remember, the left side is $1 + x + x^2 + \cdots$

I want $\mathfrak{a}$ to be $\mathbf{k} \ll t_1, \ldots, t_n \gg$ and the maximal ideal is generated by the t_i.

[Some discussion. Then a break.]

3. October 14, 2013

Calin Lazaroiu, Non-Markovian categories of open quantum systems

I want to talk about "open quantum systems" which are quantum physical systems which are in interaction with the environment. They are *not* isolated. We need a mathematical model for this.

The most general mathematical description of a "quantum system" is a pair $(\mathcal{H}, \rho)$ where $\mathcal{H}$ is a Hilbert space which I'll take to be separable and ρ is a so-called density operator on $\mathcal{H}$. I'll denote the convex set of density operators by $\bar{B}_1^+(\mathcal{H})$.

Everyone knows that a Hilbert space $\mathcal{H}$ (I will consider all Hilbert spaces to be over the complex numbers) is a pair, a vector space over $\mathbb{C}$ endowed with a Hermitian scalar product $\langle , \rangle$, a bilinear map $\mathcal{H} \times \mathcal{H} \to \mathbb{C}$, such that the norm is complete, every Cauchy sequence converges.

There's a well-developed theory of Hilbert spaces. In particular there's a notion of Hilbert dimension.

Proposition 3.1. *Any Hilbert space admits an* orthonormal basis*, that is a family (e_i) of elements e_i such that $\langle e_i, e_j \rangle$ is the Kronecker δ, and such that for any vector x in $\mathcal{H}$ the sum $\sum |\langle x, e_i \rangle| < \infty$ and $\sum \langle x, e_i \rangle e_i = x$*

Proposition 3.2. *Any two Hilbert space bases have the same cardinality which is denoted $hdim\mathcal{H}$ and called the Hilbert dimension.*

Now I can explain what separable means.

Definition 3.1. *The Hilbert space $\mathcal{H}$ is called* separable *if $hdim\mathcal{H} \leq \aleph_0$, that is, if the dimension is finite or countable (these are mutually exclusive).*

In the finite case, this is unitarilly isomorphic to $\mathbb{C}^n$ with the standard inner product; in the countable case it's ℓ_2, the space of square summable sequences. The scalar product is

$$\langle a, b\rangle = \sum_{n=0}^{\infty} a_n \bar{b}_n$$

which is absolutely convergent.

There are nonphysical Hilbert spaces that are not separable, but a space of states is always separable.

So ρ is called a "mixed" state and the set of them is $\bar{B}_1^+$. Let's see this. So $B(\mathcal{H})$ is the set of bounded operators, $||Tx|| \leq ||T||||x||$ for some unique $||T|| \geq 0$. This is equivalent to being continuous. This set of bounded operators is a Banach space.

$B_1(\mathcal{H})$ within $B(\mathcal{H})$ is the set of trace class operators, those such that $tr(|T|) < \infty$. This is a Banach space. You can define Schatten classes, define $B_p(\mathcal{H})$, bounded operators such that $tr(|T|)^{\frac{1}{p}} < \infty$. The theorem is that $B_p(\mathcal{H})$ is a Banach space and $B_p(\mathcal{H}) \circ B_q(\mathcal{H}) \subset B_{\frac{pq}{p+q}}$. There's something a little wrong here, but I don't remember the actual details.

So $B_1(\mathcal{H})$ has a dual which is $B_\infty(\mathcal{H})$, compact operators. Well, anyway, what's $B_1^+(\mathcal{H})$ with the property that $T \geq 0$. This means the spectrum of T is inside the positive real line. Then $\bar{B}_1^+(\mathcal{H})$, well, these are the ρ such that the trace of ρ, well, this is a self-adjoint operator, they have trace 1. The space, the set of such is a convex set. It's the set of all states. There's a notion of pure states, which project onto a one-dimensional space. So take $V \subset \mathcal{H}$ a closed subspace, consider orthogonal projector P_V onto V. Since V is closed this is bounded and trace class. Take ρ to be $\frac{1}{dim\ V} P_V$. If the dimension of V is one, this is called pure. In general by the spectral theorem, you can write any such ρ as a series $\lambda_n P_n + P_0$, where P_n are projectors onto a subspace of $\mathcal{H}$ and $\sum \lambda_n = 1$.

So a quantum system is $(\mathcal{H}, \rho)$. This describes the state ρ of the quantum system with Hilbert space $\mathcal{H}$. This is very rigorous and well-defined.

Now that's the basis of the theory of closed quantum systems. So what's an open quantum system? The modern way to think about this is as a category. Make a category of quantum systems. Here the story is not so simple. Most morphisms are actions of unitary operators. Simplest: take $U \in \mathcal{U}(\mathcal{H}_1, \mathcal{H}_2)$, the set of unitary operators. This is empty unless they have the same Hilbert dimension. Define a category, sometimes called the category of pointed Hilbert spaces and unitary maps $Hilb_U^\bullet$, with objects pairs $(\mathcal{H}, \rho)$ (everything is separable) and morphisms unitary operators U such that $Ad_U(\rho) = \rho'$. That is, $U\rho U^{-1} = \rho'$.

That's a natural thing. Unfortunately, it's rather useless. That describes only physical processes involving *isolated* or *closed* quantum systems (I'm giving you the physics language) in which quantum systems do not interact with anything else.

You have some box where you put a quantum system, with some hydrogen atoms or whatever, and you say it's perfectly isolated, no energy can flow into or out of the system. In reality you can't make a closed systems. This is an idealization. You get a differential equation if you start with a one-parameter family $U = e^{itH}$ and you get the so-called Von Neumann equation, which if you evaluate you get the Schrödinger equation.

Physics and logic and common sense say that there's no such thing as an isolated (closed) quantum system. So all quantum systems are actually open, non-isolated. So that trivial category, there's maybe interesting functional analysis but nothing interesting categorically.

In modern languages, what replaces $Hilb_U^\bullet$ as a *good* category of open quantum systems? This should match up well with the lab.

If you can stand to read those papers, which are not mathematical but not clear, you have to be a physicist to read those papers, they're not clean. They try to do this thing. There's an ideology, the current ideology has objects the same, $(\mathcal{H}, \rho)$. But what are the morphisms? The morphisms ~~maybe~~ (they changed their minds) are "completely positive" maps. This comes from Shudaishan. He also showed these weren't right. A positive map is a linear map $B_1(\mathcal{H}) \to B_1(\mathcal{H}')$ which takes the cone of positive trace class operators into the cone of positive trace class operators. It's completely positive if f remains positive after tensoring with the identity on any finite dimensional Hilbert space.

Any unitary map $U \in \mathcal{U}(\mathcal{H}_1, \mathcal{H}_2)$ has the property that $Ad\ U : \bar{B}_1^+ \to \bar{B}_1^+(\mathcal{H}')$ is completely positive. Moreover $Ad\ U$ has a completely positive inverse. Even further, a completely positive map has a completely positive inverse if and only if it is $Ad\ U$.

Every operator from a finite dimensional Hilbert space to itself is bounded, so $B_1(\mathcal{H})$ is just the space of $n \times n$ matrices, and $id_{B_1(\mathcal{H})} \cong id_{Mat(n,\mathbb{C})}$.

For a map to be completely positive, it must be positive. For physical reasons you think it should be positive. The complete positivity, it's claimed that a nice class of processes is described by completely positive maps. So we should use them as morphisms. Then we can describe both unitary and non-unitary evolutions, and you get some Markov evolution. This was done rigorously. That was done by a Swedish mathematician. In this approach, unitary evolution is replaced by Markovian evolution while under good technical assumptions, von Neumann's equation is replaced by Lindblad's master equation. There's a paper in 1976 or something and there are a couple of generalizations.

People recently found systems that don't follow Lindblad's equation. So the mathematical assumptions are very weak, the only way out is to drop the completely positive assumption. So you need to replace that with something else. That's an extra assumption, physically untenable.

This goes up to very recent papers discussing why this isn't enough. If you predict something that is disavowed by experiment, you go home and think again. There's a lot of activity.

It was in working in decoherence and quantum information theory that they came upon this being not enough. After the break I'll tell you how the answer comes from homotopy theory.

[break]

How would we go beyond the completely positive maps? A linear map f is completely positive if and only if there is a completely positive map from $B_1(\mathcal{H})$ to $B_1(\mathcal{H}_E)$ for some other Hilbert space $\mathcal{H}_E$ so that you can couple with the environment (there is a partial trace map $\mathcal{H} \otimes \mathcal{H}_E$ down to $\mathcal{H}$), taking the lift, rotating using a closed morphism, a unitary map, and then projecting back down.

How would you generalize this map? One way to is to let the system interact with the environment. So the mixed state might not be of tensor product form. It could be $\bar{e}(\rho)$, some $\bar{e}$.

The no-go theorem says there is no trace preserving psotive linear map $\bar{e}$ which is not just a tensor product $id \otimes e$. There are no sections in linear positive maps. You have to do something else. You could relax positivity or linearity of $\bar{e}$. Nonlinearity would produce many problems. Negativity would also be a problem. The whole composite would preserve positivity, but that's only on some subspace. It's physically untenable. That's the current status.

Let me tell you how we think this could be answered. If you know a little bit about algebraic homotopy theory. Instead of finding a lift, define the morphisms to be such diagrams.

$$\begin{tikzcd}
\bar{B}_1^+(\mathcal{H}\otimes\mathcal{H}_E) \arrow[r] \arrow[d, "tr_{\mathcal{H}_E}"] & \bar{B}_1^+(\mathcal{H}'\otimes\mathcal{H}'_E) \arrow[d, "tr_{\mathcal{H}'_E}"'] \\
\bar{B}_1^+(\mathcal{H}) & \bar{B}_1^+(\mathcal{H}')
\end{tikzcd}$$

So let me make a first definition of a category of open quantum systems.

The objects are pairs $(\mathcal{H}, \rho)$ with $\mathcal{H}$ a separable Hilbert space and ρ in $\bar{B}_1^+(\mathcal{H})$.

Morphisms are quadruples $\mathcal{H}_E, \mathcal{H}'_E, \hat{\rho}, U$ where $\mathcal{H}_E$ and $\mathcal{H}_{E'}$ are separable, U is a unitary morphism $\mathcal{H}\otimes\mathcal{H}_E, \mathcal{H}'\otimes\mathcal{H}'_E$, a $\hat{\rho}\in\bar{B}_1^+(\mathcal{H}\otimes\mathcal{H}_E)$ such that the partial trace over $\mathcal{H}_E$ of $\hat{\rho}$ is ρ and so that the partial trace over $\mathcal{H}'_E$ of $Ad_U\hat{\rho}$ is ρ'.

The identities are $(\mathbb{C}, \mathbb{C}, \rho, \mathrm{id}_{\mathcal{H}\otimes\mathbb{C}})$. The composition is a complicated diagram.

$$\begin{tikzcd}
\bar{B}_1^+(\mathcal{H}_1 \otimes \mathcal{H}_{E,1} \otimes \mathcal{H}_2 \otimes \mathcal{H}'_{E,2} \arrow[rr, "Ad_{U_12}\otimes id"] \arrow[d, "tr_{H_2 \otimes \mathcal{H}'_{E'_2}}"] & & \bar{B}_1^+(\mathcal{H}_2^{\otimes 2} \otimes \mathcal{H}_{E,2} \otimes \mathcal{H}'_{E,2} \arrow[rr, "Ad_{23}\otimes id"] \arrow[dl, "tr_{H_2 \otimes \mathcal{H}'_{E,2}}"'] \arrow[dr, "tr_{H_2 \otimes H_{E,2}}"] & & \bar{B}_1^+(\mathcal{H}_3 \otimes \mathcal{H}_{E,3} \otimes \mathcal{H}_2 \otimes \mathcal{H}_{E,2}) \arrow[d, "tr_{\mathcal{H}_2 \otimes \mathcal{H}_{E,2}}"] \\
\bar{B}_1^+(\mathcal{H}_1 \otimes \mathcal{H}'_{E,1}) \arrow[r, "Ad_{12}"] \arrow[dd] & \bar{B}_1^+(\mathcal{H}_2 \otimes \mathcal{H}_{E,2}) \arrow[dr] & & \bar{B}_1^+(\mathcal{H}_2 \otimes \mathcal{H}'_{E,2}) \arrow[r, "Ad_{U_23}"] \arrow[dl] & \bar{B}_1^+(\mathcal{H}_3 \otimes \mathcal{H}'_{E,3}) \arrow[d] \\
\bar{B}_1^+(\mathcal{H}_1) & & \bar{B}_1^+(\mathcal{H}_2) & & \bar{B}_1^+(\mathcal{H}_3)
\end{tikzcd}$$

Explicitly, the composition

$$\mathcal{H}'_{E,2}, \mathcal{H}_{E,3}, \hat{\rho}'_2, U_{23} \circ \mathcal{H}_{E,1}, \mathcal{H}_{E,2}, \hat{\rho}_1, U_{12}$$

is

$$\mathcal{H}_{E_1} \otimes \mathcal{H}_2 \otimes \mathcal{H}'_{E_2}, \mathcal{H}_{E_3} \otimes \mathcal{H}_2 \otimes \mathcal{H}_{E_2}, \hat{\rho}_1 \otimes \hat{\rho}'_2, Ad_{(U_{23} \otimes id) \circ (U_{12} \otimes id)}$$

Proposition 3.3. *This is in fact a category, in fact a bicategory with 2-morphisms given by pairs $w = (w_1, w_2)$ such that w_1 and w_2 are in W, a wide subcategory generated by Ad_U for U unitary and $tr_{\mathcal{H}_E}$ (partial trace) so that the diagram commutes*

$$\begin{tikzcd}
 & \bar{B}_1^+(\mathcal{H}_1 \otimes \mathcal{H}_{E,1}), \hat{\rho}_1 \arrow[r, "Ad_U"] \arrow[dl, "tr_{\mathcal{H}_{E,1}}"] \arrow[dd, "w_1"] & \bar{B}_1^+(\mathcal{H}_2 \otimes \mathcal{H}_{E,2}), \hat{\rho}_2 \arrow[dd, "w_2"] \arrow[dr] & \\
\bar{B}_1^+(\mathcal{H}_1), \rho_1 & & & \bar{B}_1^+(\mathcal{H}_2), \rho_2 \\
 & \bar{B}_1^+(\mathcal{H}_1 \otimes \mathcal{H}'_{E,1}), \hat{\rho}' \arrow[r, "Ad_{U'}"'] \arrow[ul, "tr_{\mathcal{H}'_{E,1}}"'] & \bar{B}_1^+(\mathcal{H}_2 \otimes \mathcal{H}'_{E,2}, \hat{\rho}_2 \arrow[ur] &
\end{tikzcd}$$

So to do the right thing with these, you should take final one-morphisms, Kan extensions in the bicategory sense. This has a physical interpretation. So the important thing is that this is related to making renormalizing group flow into a functor. Usually this is defined via an approximation scheme. We can define this as a functor and think this is the correct definition for a number of reasons.

How do you relate this back? Let $\rho = e^{-H}$ for H a Hamiltonian. Then $\mathcal{H} = \mathcal{H}_{eff} \otimes \mathcal{H}_E$. Then $tr_{\mathcal{H}_E}(\rho) = e^{-\mathcal{H}_{eff}}$. That's the rough idea.

Of course, there's much more than this. This really should be done more generally. This can be done for C^* algebras and for von Neumann algebras. The most general version is in terms of C^* algebras and states on those.

There is another way to define a bicategory of quantum systems. A bicategory of open quantum systems and completely positive maps. How does it relate to this? We think it embeds into our bicategory. All of this story, of course, has a connection to homotopy theory. This does behave a bit like a calculus of fractions. Then you can ask an awful lot of mathematical questions. Does this extend to non-separable Hilbert spaces? What about C^* algebras? But now there's a category.

[Some discussion of renormalization group flow.]

4. Kim Dohyeong, Introduction to descent

I'll begin by discussing what I mean by descent. This is not a rigorously defined term. Instead it's a set of techniques to attack diophantine problems. I'll explain what those are. It's especially for those using arithmetic or geometric symmetries. I'd rather view it as a theme on which you can play many variations. I'll introduce several explicit realizations of this method and this will bring the idea of descent. This is for non-number theorists, so I want to avoid all the technicalities as much as possible.

Let $\mathbb{Z}$ be the ring of integers and $\mathbb{Q}$ the field of rationals. If N is a nonzero integer, then you can think about the localization of $\mathbb{Z}$ at N, the ring of fractions $\mathbb{Z}[\frac{1}{N}] = \{\frac{a}{N^r}\}$ for $r \in \mathbb{Z}$ and $a \in \mathbb{Z}$. We'll always let R be one of these; we have inclusions $\mathbb{Z} \subset \mathbb{Z}[\frac{1}{N}] \subset \mathbb{Q}$ but the second gap is much bigger than the first.

Let X be a variety of finite type over R We can safely assume that X is a curve because it's already hard enough. But if you like you can enlarge into stacks or schemes or something.

A Diophantine question is like whether $X(R)$ is empty or whether it's finite or you want to ask for an algorithm to produce $X(R)$ without knowing its finiteness. These are basic questions. Is there a solution? Are there only finitely many? Can we compute them explicitly? You can ask all of these questions varying X. You want to consider X having a certain property and you want to know whether some property is true or not. When R is $\mathbb{Z}$ this is a famous problem of Hilbert; I forgot the number. This question, whether $X(\mathbb{Z}) = \emptyset$, is as hard as the halting problem, to determine whether a particular code stops or not. This implies in particular that there is no algorithm for this.

For X in some special class of varieties we can probably answer this.

For $R = \mathbb{Q}$, we don't know how difficult this problem is. I think that it's in the realm of logic that, they predict that this can be solved by an algorithm, but I don't know the current state of the art. People also illustrate this situation by saying that $\mathbb{Z} \subset \mathbb{Q}$ is perhaps not definable in first order logic. It suggests that $\mathbb{Q}$ and $\mathbb{Z}$ should behave very differently in terms of solving equations. You want to write down a finite set of conditions to define $\mathbb{Z}$ in $\mathbb{Q}$. We expect that this doesn't exist.

We do, though, have some knowledge about curves and I can tell you some of what we know about them. Projective smooth curves are classified by genus.

I'll exclude the case when $g = 0$. The case when $g = 1$ is elliptic and $g > 1$ is called hyperbolic.

	finite over $\mathbb{Z}$	algorithm	finite over $\mathbb{Q}$
elliptic$\setminus\{p\}$	$\surd$	not known	not known
elliptic	$\surd$	modulo BSD conjecture	modulo BSD conjecture
hyperbolic	$\surd$	not known	$\surd$

Already for curves the situation is unstable. These questions, the algorithms, are the effective Mordell conjecture. Why is it called that? His conjecture was the following statement early in the twentieth century. So $X/\mathbb{Z}$, let's have it be either an elliptic curve minus a point or $\mathbb{P}^1$ minus three points or hyperbolic (often any of these is called hyperbolic) then $X/\mathbb{Z}$ is finite. He did not ask for an algorithm. That's much stronger than knowing the finiteness. An algorithm is more or less equivalent to a bound on P which is more or less the same as the exact number of $\mathbb{Z}$-solutions.

Let me give a set of examples. I'll write down equations.

$$x^2 + y^2 = p$$

$$x^2 + ny^2 = p$$

$$x^2 - ny^2 = 1$$

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2 = 0$$

$$y^2 = x^3 + ax + b(\text{with no multiple roots})$$

$$y^2 = f(x)(\text{hyperbolic if } deg(f) \geq 5$$

$$x^2 + y^2 = 1$$

$$ax^n + by^m = 1$$

for p a prime and n, a, b in $\mathbb{Z}$ or $\mathbb{Q}$.

This is the end of section zero.

4.1. **Local methods.** Our problem is that $X(\mathbb{Q})$ or $X(\mathbb{Z})$ is not structured. It's not their fault but it's the limitation of our current knowledge. We get an algebraic variety or topological space over $\mathbb{C}$ but that's not what we have for $\mathbb{Z}$. Consider $\mathbb{Q} \subset \mathbb{Q}_v$ whecre $\mathbb{Q}_v$ is either $\mathbb{R}$ or the p-adic completion of $\mathbb{Q}$.

There are many constructions of real numbers but one is using metrics and completion. We give a metric on $\mathbb{Q}$ and complete it. We consider a p-adic metric. A funny thing is that if you complete $\mathbb{Z}$ inside $\mathbb{Q}$ you get $\mathbb{Z}$ again (p-adically). But we'll talk about it. Given $a \in \mathbb{Z}$, we can write

$$a = a_0 + a_1 p + \cdots + a_n p^n + \cdots$$

This expansion will stop. The p-adic numbers we allow infinite sequences. If k is the minimum of i such that $a_i \neq 04$ then define $|a|_p$ to be p^{-k}. This defines the absolute value. As a proposition, you get infinite formal power series considering $\mathbb{Z}$ with $|\cdot|_p$. The completion of that is $\sum a_i p^i$. Call this $\mathbb{Z}_p$ If you allow finitely many terms with negative exponent, you get the so-called $\mathbb{Q}_p$.

Let's solve an equation over $\mathbb{R}$. Is $X(\mathbb{R})$ empty? The mean value theorem and some inequalities implies the answer. If you are given ten polynomial equations in twenty variables it might not be trivial. If there was a solution. Then you can refine your inequalities by dividing your intervals. You'll be able to get a solution in that small interval.

What about over $\mathbb{Q}_p$ or $\mathbb{Z}_p$? The role played by the mean value theorem is replaced by Hensel's lemma. I'm assuming the curve is smooth, even the special fiber is smooth. Suppose you have a point P in $X_p(\mathbb{F}_p)$ where X_p is a special fiber of $X/\mathbb{Z}_p$ and P is a smooth point. Then there is a $Q \in X(\mathbb{Z}_p)$ such that Q mod $p = P$. If you found a solution in a special fiber (and there are only finitely many candidates) then it must come from a point over $\mathbb{Z}_p$.

The problem is, suppose we have proved $X(\mathbb{Q}_v) = \emptyset$ for some v. Then $X(R)$ is empty for $R = \mathbb{Z}, \mathbb{Z}[\frac{1}{N}], \mathbb{Q}$. The difficult part is the converse. Suppose you know $X(\mathbb{Q}_v)$ is nonempty for every v? Can you say anything over $\mathbb{Z}, \mathbb{Z}[\frac{1}{n}], \mathbb{Q}$? This is called the Hasse principle but it's only true in one case I know of, so I wouldn't call it a principle. For a quadratic hypersurface $X(\mathbb{Q}_v) \neq 0$ for all v implies $X(\mathbb{Q}) = X(\mathbb{Z}) \neq 0$. You may ask whether this gives an algorithm, but it doesn't since $X(\mathbb{Q}_v)$ takes infinitely many operations. As stated this is not algorithmic.

The problem becomes interesting when $X(\mathbb{Q}_v)$ is non-empty. Identifying $X(\mathbb{Q})$ inside it is of analytic or topological flavor. In the next part I'll talk about a variation that is of algebraic flavor. These are defined by analytic data so you don't expect to recover solutions over $\mathbb{Q}$ by algebraic means.

That was a remark. The second remark is, approximation of transcendentals in $\mathbb{R}$ by rationals helps to solve diophantine equations. There are only two examples where you can deduce results out of approximation theory.

$$x^2 - dy^2 = 1$$

is related to approximation of $\sqrt{d}$ by rationals.

$$y^2 = x^3 + ax + b$$

is related to something similar by Siegel and Thue.

I think that I don't want to talk about this more but this partially justifies the first remark. I'll give the third remark and then take a break. There are similar quadratics, we can apply Hasse's principle, let's look at $x^2 + ny^2 = p$. This problem is of historical importance. Amazingly, class field theory gives an algorithm to classify solutions, to determine if $X(\mathbb{Z}) = \emptyset$. If $n = 1$ then p must be $1 \mod 4$. To do it for all n you need to go to class field theory and that gives you the answer. I'll begin section two later.

4.2. **étale descent (1980s).** Grothiendieck suggested this. Everything up to now has been from the nineteenth century. It's a matter of taste but I'd take this as the theme for descent. The ideas are most transparent, it's simplest, it's strongest. So X is a curve over $\mathbb{Q}$. I'll work there because I'm more comfortable there. Assume that $X(\mathbb{Q})$ is nonempty. This may be a problem for some equations. Further, fix $b \in X(\mathbb{Q})$. Also fix $\overline{\mathbb{Q}}$, an algebraic closure of $\mathbb{Q}$. Most of the problem lies in understanding the algebraic closure, because whatever you do it boils down to properties of the closure. Then we have an exact sequence

$$1 \to \pi_1(\bar{X}, \bar{b}) \to \pi_1(X, b) \to Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to 1.$$

Here $\bar{b}$ is in $X(\overline{\mathbb{Q}})$, it's the base change of b to consider it as living in $\overline{\mathbb{Q}}$.

I'll give a topological picture for this. Let me draw a picture. I have a base, which I view as a surface. This is not a basepoint. Its base is *Spec* $\mathbb{Q}$. You've fixed a section b. I'll draw a section above it. Fixing $\overline{Q}$ amounts to fixing a universal cover of the base. If you think of étale sites, pull back the bundle, you have the same thing, a bundle over *Spec* $\overline{\mathbb{Q}}$ and can pull back b to $\bar{b}$. Resolve the fiber as well to get something simply connected. You can resolve fiber by fiber continuously. This is not possible if you don't have a preferred choice of base. Fixing the basepoint amounts to fixing a universal cover. Then you can patch together universal covers as you move around. So we often say that the kernel is the algebraic fundamental group and that the cokernel is the arithmetic part. An element of the Galois group is a loop in the base. Suppose you have a path in the base, you can lift it to a path in the universal cover. Then you can lift that picture to the resolved fibers. Above the original base you get instead an automorphism of the fiber instead, which is an element of the appropriate group.

So explicitly, $G_{\mathbb{Q}} := Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\pi_1(X_{\overline{\mathbb{Q}}}, \bar{b})$

The idea is to use this action to study $X(\mathbb{Q})$.

Theorem 4.1. *(Belyi, Ihara, others) Let X be $\mathbb{P}^1 - \{0, 1, \infty\}$. Then the G_Q-action is faithful.*

This is striking in the sense that this is the simplest hyperbolic curve you can think of. But still the action is a faithful embedding. Other hyperbolic surfaces it'll be almost faithful at least. Up to finite error it will be for hyperbolic curves. This gives you hope that this action might be useful.

Proposition 4.1. *There is a canonical map from $X(\mathbb{Q}) \hookrightarrow H^1(G_{\mathbb{Q}}, \pi_1(X_{\overline{\mathbb{Q}}}, \bar{b}))$. This takes $c \mapsto \pi_1(X_{\overline{\mathbb{Q}}}; b, c)$ and I'll explain what that is.*

If you have b and c in your base, then you can identify the fibers above b and above c. You can only do this up to the ambiguity of the fundamental group.

Conjecture 4.1. *Grothiendieck's anabelian section conjecture*
Suppose X is hyperbolic. Let me name the inclusion κ (for Kummer). Then κ is bijective.

I want to view this conjecture from several viewpoints. Suppose you have some understanding of $G_{\mathbb{Q}}$. You have an explicit presentation for the fundamental group. You consider inverse limits of topological coverings. It's the profinite completion of the free group on two generators. Then in principle we expect to compute the right hand side in an algorithmic way. Then this will give an algorithm to compute $X(\mathbb{Q})$. So eventually this may produce an algorithm.

I don't know how to compute the right hand side, but for elliptic curve it's computable.

Maybe some people know but I don't know how to compute the right hand side. But I don't. Instead, I'll look for computable variants of $\pi_1^{et}(X_{\overline{\mathbb{Q}}}, \bar{b})$. Of course, κ will not be bijective any more.

The most naive variant is a small quotient of the fundamental group. In some sense this isn't helpful because we know so little about $\overline{\mathbb{Q}}$. So we reduce the difficulty to $G_{\mathbb{Q}}$ but that's hard.

The first variant has X an elliptic curve. In this case $\pi_1(X_{\overline{\mathbb{Q}}}, \bar{b}) = \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$ where $\hat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$. If $X(\mathbb{C})$ is $\mathbb{C}/L$, this is a covering of the elliptic curve, sending $x + \tau y$ to $mx + n\tau y$. For every pair (m, n) you have this map and they are all finite coverings. So passing to the projective limit you get this product of profinite completions. Let's consider the smallest quotient, not in a strict sense, consider $z \mapsto 2z$. This is a degree four covering. This corresponds to a quotient of π_1 which is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ which is the group of deck transformations. This is $\frac{1}{2}L/L$ which is $X[2]$ which is $\{p \in X \text{ such that } 2P = b\}$ viewing b as the origin. The notation [2] means the order two points.

This descends to the quotient as multiplication by 2 is defined over $\mathbb{Q}$. So $G_{\mathbb{Q}}$ acts on $X[2]$ which is $\pi 1(X_{\overline{\mathbb{Q}}})/2\pi_1(X_{\overline{\mathbb{Q}}})$.

Now I want to explain what people do with this. It goes back to Euler who realized that using the action of $G_{\mathbb{Q}}$ on $X[2]$ can tell you something about elliptic curves.

Here I have a map that goes from $E(\mathbb{Q})$ to $H^1(G_{\mathbb{Q}}, E[2])$. I need to change from X to E, it's too demanding. The right hand side is killed by 2, so there's no hope of having this be injective. So quotient by $2E(\mathbb{Q})$ and it is injective. So κ is not surjective any more but the right hand side can be computed explicitly.

Mordell proved for $\mathbb{Q}$ (and Weil generally) that $E(\mathbb{Q})$ is $\mathbb{Z}^g$ times a finite Abelian group that can be computed algorithmically. The rest is determining the number g. So we hope to recover some information about g, maybe an exact formula, out of this inclusion.

Here come the local computations. There are obviously classes in $H^1(G_{\mathbb{Q}}, E[2])$ which cannot be in the image of κ. Obvious means local here. So let me draw a diagram.

$$\begin{tikzcd}
E(\mathbb{Q})/2E(\mathbb{Q}) \arrow[r, "\kappa"] \arrow[d, hook] & H^1(G_{\mathbb{Q}}, E[2]) \arrow[d, "loc_v"] \\
E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) \arrow[r, "\kappa"'] & H^1(G_{\mathbb{Q}_v}, E[2](\mathbb{Q}_v)
\end{tikzcd}$$

You need your solution to land in the bottom right, so you only want to look at the intersections of the preimages as v varies. This is called the Selmer group $Sel(\mathbb{Q}, E[2])$.

Definition 4.1.

$$Ш(E/\mathbb{Q}) := Ker(H^1(G_{\mathbb{Q}}, E)) \to \bigoplus_v H^1(\mathbb{Q}_v, E)$$

It's hard to compute the right hand side. But when you replace E with $E[2]$ it's possible. Let me make a proposition which is that the following is an exact sequence:

Proposition 4.2.

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \overset{\kappa}{\to} Sel(\mathbb{Q}, E[2]) \overset{E(2)\hookrightarrow E}{\to} Ш(E/\mathbb{Q})[2] \to 0$$

If Ш was known to be finite, we could recover this easily.

[some discussion]

If $r \leq 1$, the analytic rank (in this case $r = g$), then Ш is known to be finite; we understand some part of it, the p-primary part one at a time. Only sometimes is it successful. We don't have a single example when the rank is at least two. The analytic rank is the order of the L function of E at $s = 1$. This is the definition of r. We know nothing if $r > 1$. It's been that way for twenty years.

I'll tell you what I do to compute the Selmer group.

[What's descent?] It's computing the Selmer group to get the points on the elliptic curve. From the information out of the group action we'll get some points. This is a toy version of the anabelian section conjecture. It's descent because of Euler's terminology "infinite descent" or maybe Fermat, he wanted to prove a solution didn't exist. He looked for a hypothetical point, you should have $\frac{1}{2}p$. By proving that such a cohomology class doesn't exist, you see that p doesn't exist. Going from p to $\frac{1}{2}p$, that's descent. So you might have to go to some power of two, infinite descent. Now we can do descent over any finite cover. It's all the same line of thought.

[What's Minhyong doing?] He's using another realization of the etale fundamental group. He's using unipotent sheaves, which is like extensions of constant sheaves. It's a successive extension of constant sheaves, but maybe nontrivial extensions.

This is computing the Selmer group. I'll give the simplest example. This is $y^2 = x(x-a)(x-b)$, where a and b are rational. I gave this in affine coordinates. Something you can prove easily is that $E[2]$ is $\{(a, 0), (b, 0), (0, 0), \infty\}$. Then $H^1(G_{\mathbb{Q}}, E[2])$ is $Hom_{Gp}(G_{\mathbb{Q}}, \mathbb{Z}/2 \times \mathbb{Z}/2) = \{F/\mathbb{Q} | Gal(F/\mathbb{Q}) \subset \mathbb{Z}/2 \times \mathbb{Z}/2\}$. Consider the kernel of a homomorphism, extend this, and this is isomorphic to the image of what you started with, which is in the target group $\mathbb{Z}/2 \times \mathbb{Z}/2$. Anyway, this last is the same as $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. The correspondence is $N_1, N_2 \to \mathbb{Q}(N_1, N_2)$.

So we need the local condition from before, being in the intersection of the preimages of loc_v. This implies that F is unramified at v, for which $E \mod v$ is smooth. You have to look in the bad places too, with non-smooth reduction, but there are finitely many of these and in these places it's algorithmically computable what is going on there.

So we first classify $F/\mathbb{Q}$ which is unramified for every good place v and verify local conditions for bad places one by one. This is reduce to classifying Abelian extensions satisfying certain local conditons, and that's exactly what class field theory does for you. It lets you compute Abelian extensions of number fields with proscribed ramifications. Given K classify F/K with $Gal(F/K)$ abelian and ramification conditions. If you can compute the unramified ones, you can get the rest of them fairly easily. But this can be computationally intensive. We can't possibly compute degree 5, we can probably do degree 3.

Say $a = 1$ and $b = -1$. Then F is $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2})$. Two is the only bad prime. These are all the extensions of $\mathbb{Q}$ in which 2 ramifies. I might need $\mathbb{Q}(\mu_8)$, an eighth root of unity. Maybe not. So I have three candidates. For these three I know what the cohomology class is. I go down and verify whether these are in the image of κ_v. So v is good if it is not 2 or ∞. It's bad if it's 2 or ∞.

The next thing is how this fails when X has large genus.

5. Kim Dohyeong, Introduction to descent,II (October 28)

I'll start with my plan. I realized that last week I did not give a table of contents, I apologize for that. My plan is, I'll begin by reviewing what I did last week, but not all of it. I'll recall 2-descent and the étale fundamental group exact sequence. Then I will talk about moving from 2-descent to ℓ-descent (here ℓ is a prime) and ℓ^∞ descent, some more slight generalization of the 2-descent that I'll review. So then I'll move to standard conjectures. I will view these as computing ℓ^∞ descent using L-functions.

This forces us to think about motives and automorphic representations. So probably I should have this be section three, motives and automorphic representations. This is reciprocities, et cetera. From the conjectures in section two I'll motivate why we think about motives and why we have to move to automorphic representations. We're forced to work with these.

Lastly, I'll talk about p-adic deformations which will lead us to Iwasawa theory, and in the fifth place talk about nonabelian descent and nonabelian Iwasawa theory.

0. Reviewing 2-descent
1. From 2-descent to ℓ-descent
2. Standard conjectures
3. Motives and automorphic representations
4. p-adic deformations and Iwasawa theory
5. nonabelian descent and nonabelian Iwasawa theory

Maybe at the end I'll talk about some speculations.

6. Review

Let $X/\mathbb{Q}$ be a smooth algebraic curve and suppose it's non-empty. Fix a basepoint b in $X/\mathbb{Q}$. Fix also an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Then $G_{\mathbb{Q}}$, the *absolute Galois group*, is the Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$. Then we have an exact sequence, where as $X(\mathbb{Q})$ sits inside $X(\overline{\mathbb{Q}})$, so b goes to $\bar{b}$:

$$1 \to \pi_1(\overline{X}, \bar{b}) \to \pi_1(X, b) \to G_{\mathbb{Q}} \to 1$$

$G_{\mathbb{Q}}$ acts on $\pi_1(\overline{X}, \bar{b})$. and we have the map $\kappa : X(\mathbb{Q}) \to H^1(G_{\mathbb{Q}}, \pi_1 X_{\overline{\mathbb{Q}}}, \bar{b})$. We'd like to compute the left side but in descent we will compute the right side instead.

Suppose E is an elliptic curve. What is the universal cover of $(E, \mathcal{O})$? These are pointed covers. This factors through the multiplication by n map. In a special case, where $n = 2$, then $\pi_1(E_{\overline{\mathbb{Q}}}, \bar{b})$ surjects on $\pi_1(E_{\overline{\mathbb{Q}}}, \bar{b}) \otimes_{\hat{\mathbb{Z}}} \hat{\mathbb{Z}}/2\hat{\mathbb{Z}}$. Here the hat denotes profinite completion.

Then $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ embeds in $H^1(G_{\mathbb{Q}}, E[2])$. This factor through a group called Selmer group. So $Sel(E[2], \mathbb{Q})$ sits inside $H^1(G_{\mathbb{Q}}, E[2])$, and it is effectivly computable. Also, unxer the assumption of finiteness of the the Tate-Shaferovitch group, we can compute $E(\mathbb{Q})/2E(\mathbb{Q})$ and so in particular we compute g with is the dimenison of $E_{\mathbb{Q}})$ and has another $\mathbb{Q}$ in there.

6.1. **To ℓ-descent.** Going from 2 to the power ℓ^k is hard. We have the same diagram.

Shall I recall the definition of the Selmer group? We have a diagram [Missed some]

Lemma 6.1. *$\mathbb{Q}_\ell/\mathbb{Z}_\ell = \bigcup \ell^{-n}\mathbb{Z}/\mathbb{Z}$.*

From the lemma we have

$$[0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to Sel(E[\ell^\infty]) \to =$$

In fact, this Selmer set is related directly to special values of L-functions. I want to add that L-functions can be computed very esaily. They're comuptationally of low cost.

7. Standard conjectures

We have the Hasse-Weil L-function associated to an elliptic curve. If E is the curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbb{Z}$. Assume E_i is minimal, so that the discriminant is the smallest with absolute value (or divisibility) among all discriminants of this equation under change of coordinates preserving this form. This is the Weierstrass minimal model. Over $\mathbb{Z}$ most minimal models coincide. In genus two curves, choosing a model at all isn't an easy problem. Elliptic curves over $\mathbb{Q}$, there is some ambiguity if you want something defined over $\mathbb{Z}$. If you want a mod p fiber you need something over $\mathbb{Z}$. You can't always choose a canonical model.

Define a_p to be p minus the number of points of some chosen minimal model $\tilde{E}_p$ modulo p over $\mathbb{F}_p$.

Define $L(E,s) = \prod_{p\nmid\Delta}(1 - a_p p^s + p^{-2s+1})^{-1} \times prod_{p\div\Delta}(\text{similar})$. You can define this for a complex number s whose real part is greater than $\frac{3}{2}$.

Theorem 7.1. *(Wiles, others) $L(E,s)$ has analytic continuation over the complex plane.*

So we identify $L(E,s)$ with an L-function associated to a *modular form*. This is a special type of automorphic form. By identifying this L-function in this way, we can use the theory of modular forms to analytically continue. This remark is the contents of the theorem, it's also essentially the Taniyama-Shimura-Weil theorem (which is necessary for the Birch and Swnnerton-Dyer conjecture or whatever).

For $y^2 = x^3 - x$, well, the Dedekind η function is $q^{\frac{1}{24}}\prod(1-q^n)$ where $q = e^{2\pi iz}$. Then the L-function of that elliptic curve is $\frac{\eta(11z)}{\eta(z)}$. This isn't quite right, there is a factor. It should be of weight two.

Define r_E to be the order at $s=1$ of $L(E,s)$. We had a geometric rank g_E, and the Birch and Swinnerton-Dyer conjecture is that $r_E = g_E$.

In order to find a modular form f we need to compute $S_2(\Gamma_0(N))$ which is a finite dimensional vector space over $\mathbb{C}$ and N is the conductor of E. This last was the Weil wight two 2-cusp modular forms for $\Gamma_0(N)$ which are two by two matrices of determinant one such that $c \equiv 0 \mod N$.

Suppose f is in this space, and is a Hecke eifenform. Then $T_pf = a_pf$. Your T_p operator is explicitly given and has an eigenvalue, and so you can do an explicit calculation. So $f = a_1q + a_2q^2$, et cetera.

The formula for the Hecke operator, which may not help, is

$$(T_pf)z = f(pz) + \sum_{i=1}^{p-1} f(\frac{z+i}{p})$$

[some discussion]

Let me tell you what the conductor is. The conductor $C(E)$ is

$$\prod p \div \Delta p^{f_p}$$

for $p > 3$ with f_p equal to 1 or two as p is a double point or cusp. For $p = 2, 3$ it's more difficult.

A stronger version of the Birch and Swinnerton Dyer conjecture, a more precise version, would be that $L(E, s) = \mathcal{L}(s-1)^{r_E} + \cdots$ with $\mathcal{L}$ over Ω, the period of

$$\frac{2x}{2y + a_1x + a_3}$$

is

$$\text{the regulator} \times \#\text{Ш}(E) \times \underbrace{\text{some fuzzy factors}}_{\text{Tamagawa numbers}}$$

where I haven't defined the regulator. I want to emphasize that this tells you the order of the Tate Shaferovich group.

As a remark, $E(\mathbb{Q})$ has a positive definite quadratic form called the Neron Tate height function, and the regulator is the covolume of $E(\mathbb{Q})$.

[some discussion and a break]

Let's talk about Tate modules and Galois representations. I formulated $E[\ell^\infty]$-descent, which makes use of a discrete Galois module $E[\ell^\infty]$ which is isomorphic to $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\oplus 2}$. A Tate module is essentially the same data, and the data of the Galois action is everything you need to define descent. So

$$T_\ell E := Hom(E[\ell^\infty], \mathbb{Q}_\ell/\mathbb{Z}_\ell)$$

these are continuous homomorphisms of Abelian groups, not respecting any Galois action. Then

$$V_\ell E := T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

which is a two dimensional $\mathbb{Q}_\ell$ vector space with a continuous action of $G_{\mathbb{Q}}$. Both of these are called Tate modules. The V_ℓ is a vector space while the other is compact and discrete. Passing to V_ℓ you get something that is not dependent on isogeny class.

From $V_\ell E$ we can recover $L(E, s)$. That is, we can recover a_p for all p. So $G_{\mathbb{Q}}$ has a Frobenius element defined up to conjugacy; let ρ_ℓ be the homomorphism $G_{\mathbb{Q}} \to Aut_{\mathbb{Q}_\ell} V_\ell E$. Then the trace of ρ_ℓ is a_p for p not dividing $\ell \cdot N_E$. For these special bad primes you can do better and recover a_p but I won't go into that.

Let me make some remarks. The number a_p does not depend on ℓ because you do a construction on one side but on the other side there is no reliance. Also a_p is an integer. There is no a priori reason for this.

We also do not need all $\{V_\ell E\}_\ell$. That is,

$$Tr(\rho_\ell(Frob_p), V_\ell(E)) = Tr(\rho_{\ell'}(Frob_p), V_{\ell'}(E)$$

This is the end of section two.

7.1. **Motives and automorphic representations.** Some viewpoints on motives. I'm not competent to talk about every viewpoint, but let me point out what are there.

(1) A motive is a system of realizations. Given E you have families of realizations $\{V_\ell E\}$ for ℓ a prime, and $H^1_{dR}(E/\mathbb{Q})$ (algebraic de Rham cohomology), you also have $H^1_{Betti}(E(\mathbb{C}), \mathbb{Q})$. You have a comparison theory that gives you the Hodge structure, and you have compatible Galois representations. So a_p should be independent of ℓ. This is what I do in practice, e.g., a modular form gives all of them.

    Remark: There is no V over $\mathbb{Q}$ such that $V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = V_\ell$ for certain given triples $\{V_\ell\}, V_{Betti}, V_{dR}$.

(2) (numerical) You make the morphisms of motives $Hom(X, Y)$ to be the $\mathbb{Q}$-space generated by correspondences $X \leftarrow Z \rightarrow Y$ modulo (what is called numerical) equivalence. This gives rise to a mathematically well-defined category, but you can't prove that they satisfy certain axioms. The numerical equivalence, it's like the Hodge conjecture and Tate conjecture, it's kind of homological equivalence. We want to identify maps that are equivalent in any cohomology. Multiplication by n is not an isomorphism in varieties but it is in every cohomology theory.

(3) (simplicial schemes) This is Voevodsky, a triangulated category.

Similarly, we can define an L-function $L(M, s)$ to a motive M. We can define Ω as well, provided that M is critical, some technical condition, and if that's the case then $L(m, 0)/\Omega$ is rational, conjecturally. If M is the motive associated to the first cohomology $h^1(E)(-1)$ then $\frac{L(m,0)}{\Omega}$ is actually in $\mathbb{Q}$. This is Deligne's conjecture. The criticality is a condition that I won't define. By the motive associated to $h^1(E)$, well, let me explain. Varieties over $\mathbb{Q}$, motives, Hodge structures, and $\overline{\mathbb{Q}}_\ell$-representations have functors.

X gives $h^i(X)$, which gives the representation $H^i(X, \mathbb{Q}_\ell)$. This is a hypothetical motive, it should satisfy this. The functors from motives to representations and Hodge structures are faithful. The faithfulness is the Tate conjecture. It says a single piece of the Tate module will remember everything.

We can generalize Birch and Swinnerton-Dyer over other motives. Let's talk about analytic continuation. You can work with one motive even if the category hasn't been constructed. We want to analytically continue $L(M, s)$. So if you want to define the conjecture originally, 1 is outside the radius of convergence. We need (often we don't know how, we would like) to identify $L(M, s)$ with $L(\pi, s)$, where π is an automorphic representation and $L(\pi, s)$ is the automorphic L-function of π.

So GL_n is the linear group of rank n. Then $\mathbb{A}$ is the ring of adeles, so that's

$$\prod^{*} \mathbb{Q}_v = \{(x_v) \in \prod \mathbb{Q}_v | x_p \in \mathbb{Z}_p \text{ for all but finitely many } p\}.$$

Inside $GL_n(\mathbb{A})$ sits $GL_n(\mathbb{Q})$. We study the space $L^2(GL_n(\mathbb{Q})\backslash GL_n(\mathbb{A}))$. This is using the Haar measure.

Let $G = GL_n$. So $G(\mathbb{A})$ acts on $L^2(G(\mathbb{Q})\backslash G(\mathbb{A}))$. This decomposes into the direct sum of a discrete part and a direct integral. So the π giving rise to the analytic continuation for the L-function of a motive is in the discrete part. If the dimension of M is n then we hope to find π in $L^2(G(\mathbb{Q})\backslash G(\mathbb{A}))$. We let π go to $L(\pi, s)$ by Godemont-Jacquet. This isn't easy, but it's standard.

8. Kim Dohyeong, Introduction to descent

My plan is to start with a big picture summarizing what we had discussed, then discuss Iwasawa theory and the p-adic zeta function. I'll finish with some speculation.

Let me start with some examples. Take $y^2 = x^3 - x$. I could not recall the modular form associated to this. So the Dedekind eta function is $\eta(\tau) = q^{\frac{1}{24}} \prod(1 - q^n)$ where $\tau = x + iy$, with $y > 0$.

It turns out that E corresponds to $\eta^2(4\tau)\eta^2(8\tau)$.

We had looked at $E[\ell] = Ker(E \xrightarrow{\ell} E)$ and that led us into periods and motives.

We started with varieties over $\mathbb{Q}$ and that was our motivation. Then E our variety leads us to $h^1(E)$ in motives, and that leads us to ℓ-adic representations $V/\bar{\mathbb{Q}}_\ell$ with action of the absolute Galois group $G_\mathbb{Q}$. We have to consider de Rham and Betti cohomology, and comparison of these two gives you periods. So $\Omega = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}}$. For elliptic curves, the period is Ω.

From here, we were able to consider L-functions. Call a generic motive M. Then $L(M, s)$ for a sufficiently large real curve, well, we did not know whether this analytically continues or not. Here algebraic automorphic forms and representations contain modular forms as a small subset. This contains, for instance, the η function, call it f_E. Hypothetically, there is an arrow to automorphic forms and representations. This should share the L-function at least. This belongs to general automorphic forms and their representations, and this leads to an L-function, and those should agree.

Let me write just $\frac{L^{(r)}(E.1)}{\Omega}$, and this is related to $Ш(E)$. This is expected to compute descent for us.

8.1. Iwasawa theory.

So Iwasawa theory is p-adically deforming M_p, the p-adic representation arising from a motive. The number immediately above should vary p-adically as well. We want to match the deformed one with p-adic variation of $L(M, 1)/\Omega(M)$. So let's say M varies with a parameter t in a p-adic family, then we need to prove that this number varies p-adically. I'll give an example of the Riemann zeta function case.

This is simple because Ω is one if we consider some half-plane. In terms of Hodge structure, we are looking at the $(2\pi i)^{1-k}$ for k even and positive. This is defined as $\sum_{n=1}^\infty frac1n^s$. This should correspond to $M(1 - k)$. Then $\zeta(M(1 - k), s)/\zeta(s + (1 - k))$.

Theorem 8.1. *$\zeta(1 - k) = \frac{-B_k}{k}$ where B_k is the Bernoulli number.*

The parameter space for p-adic deformations is the ring of p-adic integers. This ring contains $\mathbb{Z}$ which contains points of the form $(1 - k)$ for k positive and even. These are called classial points. But we have $M_p(t)$ for all t in $\mathbb{Z}_p$, [missed] but for the others we have motives.

So the question is, how does $\zeta(1 - k)$ vary?

Theorem 8.2. *(Kuhota-LEopoldt, Kummer) There exists a p-adic analytic function $\zeta_p : \mathbb{Z}_p \to \mathbb{Z}_p$, $\zeta_p(s) = \sum a_r s^r, a_r \in \mathbb{Z}_p$, $|a_r|_p \to 0$, such that $\zeta_p(1 - k) = (1 - p^{k-1})(-\frac{B_k}{k})$ for all positive even k. The final quotient is equal to*

$\zeta(1-k)/\Omega(M(1-k))$ *and the other term in the product is the Euler factor at* p*.*

The goal of Iwasawa theory is to match the set of p-adic L-functions to the Selmer group for $M(t)$. The Selmer group appeared in descent. This is the main conjecture of Iwasawa theory.

How do you parameterize the Selmer group? Let Γ be a group isomorphic to $\mathbb{Z}_p$. Let Λ be $\mathbb{Z}_p[\Gamma]$. Take the usual group ring but then take the profinite completion. Then we view as $t \in \mathbb{Z}_p$ which is our parameter space can be identified with $\Lambda \to \mathbb{Q}_p$, the space of algebra homomorphisms. Here t is the character.

So $Sel(M_p)$ is defined as a certain subgroup of $H^1(G_{\mathbb{Q}}, M_p^*)$. Let me say a bit about parameterizing in families. Look at $Sel(M_p \otimes \Lambda)$ which is in $H^1(G_{\mathbb{Q}}, H_1 \otimes N^*)$. On the right hand side we get a Λ-action.

Now I will talk about the non-commutative generalization, which is just changing the parameter space to a non-commutative one. As in the lecture this afternoon, I have to say what I mean by non-commutative. I'll fix a non-commutative group G with a surjection onto it from $G_{\mathbb{Q}}$ and consider the space of all $\bar{\mathbb{Q}}_p$-representations of G.

Let's do a non-commutative example. Let $m \in \mathbb{Z}$, not 0 or ± 1. Let $F_n := \mathbb{Q}(\mu_{p^n}, m^{\frac{1}{p^n}})$. Let $F_\infty = \cup F_n$. Then F_∞ sits over $\mathbb{Q}(\mu_{p^\infty})$ which sits over $\mathbb{Q}$ with Galois groups respectively $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$, so that the total group is $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$. This is G and we look at the set of representations of G over $\bar{\mathbb{Q}}_p$.

Call this set X_G. Let $\Lambda = \Lambda(G) = \widehat{\mathbb{Z}_p[G]}$. Then the space of functions on X_G is $K_1(\Lambda(G)_S)$ for a suitable $S \subset \Lambda(G)$.

[A good amount of discussion that goes over my head.]

Let's talk about motivation. Why non-commutative geometry and why K_1? If E is an elliptic curve, we want to understand $E(F_\infty)$. This is the space of solutions over F_∞ and has an action of G. Suppose we have an irreducible representation ρ over $\bar{\mathbb{Q}}_p$. Then one can consider this space: $E(F_\infty) \otimes_{\mathbb{Z}} \bar{\mathbb{Q}}_p)^\rho$. If ρ is trivial, you get $E(\mathbb{Q})$. The main conjecture will imply, if we call this thing V^ρ, that the dimension of V^ρ is zero if $L(E, \rho, 1) \neq 0$. If we have the main conjecture, it will imply as an immediate corollary that if the L-function does not vanish, that this cohomology, space of solutions, is small or zero.

Secondly, let me explain why K_1. At least I do not know any better definition. The second reason is that it fits well with the formalism of Iwasawa theory.

There is a map $K_1(\Lambda_S) \to K_0(\Lambda; \Lambda_S)$ and $[Sel(M_p \otimes \Lambda)] \in K_0(\Lambda; \Lambda_S)$. Then conjecturally if $\mathcal{L}$ is the p-adic L-function then $\partial\mathcal{L}$ is the class of this Selmer group.

Assume that $1 \to H \to G \to \Gamma \to 1$ is a short exact sequence. Let the Galois group of F_∞ over $\mathbb{Q}^{cyc}$ be H and over $\mathbb{Q}$ be G. Then S is the set of $f \in \Lambda(G)$ such that $\Lambda(G)/\Lambda(G).f$ is finitely generated over $\Lambda(H)$. When $G = \Gamma$ then $\Lambda(G) \cong \mathbb{Z}_p[T]$ and S is f such that p does not divide f. I know this seems arbitrary.

[Missed some]

[Coates-Fukaya-Kato-Sujatha-Venjakob] $\rho : G \to GL_n(\bar{\mathbb{Q}}_p)$ leads to

$$\begin{tikzcd}
K_1(\Lambda(G)_S) \arrow[r, "\hat{\rho}"] \arrow[d, dotted, "\rho"] & \bar{\mathbb{Q}}_p \cup \{\infty\} \\
K_1(M_n(\bar{\mathbb{Q}}_p)) \arrow[r, "\cong"] & K_1(\bar{\mathbb{Q}}_p) = \bar{\mathbb{Q}}_p^\times \arrow[u, "\subset"']
\end{tikzcd}$$

Definition 8.1. *$\mathcal{L}$ is a p-adic L-function for E and G if $\hat{\rho}(\mathcal{L}) = (L(E,\rho,1)/\Omega(E,\rho))$ times Euler factors.*

[some discussion]

We look at the map

$$\Theta_G : K_1(\Lambda(G)) \to \prod_{P \leq G} K_1(\Lambda(P^{ab}))$$

Then you want to analyze the kernel and the image. The kernel is small, it's $SK_1(\Lambda(G)) = Ker(K_1(\Lambda(G))) \to K_1(\Lambda(G)[\frac{1}{p}])$.

This is pretty much what I wanted to say.

In the remaining ten minutes I'll talk about why this business is not sufficient and why we want to do some better theory. Let's say X has genus at least two and is smooth and projective. All of these conjectures won't tell you how to computer $X(\mathbb{Q})$. This is because all the theory factors through the Jacobian of X, for example. And $J_X(\mathbb{Q})$ may be infinite. We know $X(\mathbb{Q})$ is finite by the order conjecture proved by Haltings. With a basepoint there's a map to $J_X(\mathbb{Q})$ but no characterization of the subset coming from the image. That's why we need a better theory. I'll really briefly indicate the direction. So it's not my theory but Minhyong's program. If you look in terms of Galois theory, then everything comes from automorphisms of the fiber functor. If you think about these theories then the source of the fiber functor, you are thinking about constant sheaves.

His program is to consider unipotent sheaves instead of constant sheaves. This means it's a successive extension of constant sheaves, just moving one step further. I erased the Selmer group. So here the Galois group is acting on a unipotent group instead of an Abelian group. I think this is really, there are new difficulties arising from working with non-commutative coefficients. Still, one can compute $H^1(G_{\mathbb{Q}}R)$ where R is a unipotent group. This has an arithmetic origin, like as the torsion points of elliptic curves. This is a one-line summary. He's looking to compute the analog of the Selmer group in terms of p-adic L-functions.

9. December 9, 2013: Jae-Suk Park, What is homotopy probability space?

I will be quite brief today because I'm not in a good condition. We also have nothing to eat today because we'll eat that thing on Wednesday. I didn't drink coffee for three weeks now, I feel very stupid, maybe I'll recover. I have a very thick manuscript here but very disorganized. We'll have a party on Wednesday. Everyone is welcome. We'll do games. Darts. You know. Wine and darts. The regions will be marked, you hit that region, you get that wine. You can have four tries. You can have maximum four glasses. This is held by the donation of IBS members and staff. And yours, we'll have the bread for that on Wednesday.

The title is "what is homotopy probability theory" or something like that, "space" maybe. This is the title. You could say this is a strange combination of two words. Homotopy and probability in the same sentence. So probability theory was not regarded as mathematical for a long time. This became part of mathematics because of Kolmogorov, something like that. He defined this as measure theory plus a notion of independence. I will mainly focus on the notion of independence. The troublesome part for me is the measure theory. I hate measure theory because integration, that should be based on measure theory. We have something called Feynmann's path integral in quantum field theory. No one knows how to define the path integral measure. Maybe measure theory may be developed further, but so far there is no measure. So in measure theory, we want to some kind of integral without this measure theory. So for me the most important part is the notion of independence.

Let me recall the notion of an algebraic probability theory. This can be defined as an algebraic probability space plus independence. Let me explain what is an algebraic probability space. There may be a non-commutative version but I'll do the commutative version. The commutative version starts with A and a map c to the ground field $\mathbf{k}$, which is fixed. I'll assume the characteristic is zero. You can regard it as $\mathbb{C}$ or $\mathbb{R}$ or $\mathbb{Q}$, whatever. Then A is a commutative and associative unital $\mathbf{k}$-algebra and c is a $\mathbf{k}$-linear map so that $c(1) = 1$. This is an algebraic probability space.

There is some kind of dictionary, an element X in A is called a random variable. The value of $c(X)$ is called the expectation value of X. You can regard the map as an integral, the algebra of integrands. If you start with an ordinary probability space, so random variables and expectation value, it's the algebra of measurable functions with integration.

Usually the probability theory is defined over $\mathbb{C}$. Then A has an involution related to complex conjugation. Then there is some condition related to that. You can associate a topology and place other conditions. So this is the bare minimum.

Let's record the notion of covariance. Random variables X and Y, you can look at $c(X)c(Y)$ and we can compare this to $c(XY)$, and call the difference

$$\kappa_2(X,Y) = c(XY) - c(X)c(Y).$$

This is the covariance.

Now in a certain sense, expectation value of each random variable itself may not be terribly important. Perhaps we are more interested in the interaction between them. Let me define the notion of joint moment. Consider a set of random variables $\{x_1, \dots, x_r\}$, and we'll define the joint moments of the set as the expectation of the product of the random variables:

$$\mu_n(x_{j_1}, \dots, k_{j_n}) := c(x_{j_1} \cdots x_{j_n}$$

as the j_i range. Then we can make a moment generating function

$$Z(t) = 1 + \sum_{n=1}^{\infty} \frac{1}{n!} \sum_{j_1,\dots,j_n} t_{j_1} \cdots t_{j_n} \mu_n(x_{j_1}, \dots, x_{j_n})$$

which is formally equal to $c(e^{\sum t_i x_i})$.

We just want to analyze this thing. We can introduce one more version called the cumulant generating function, which is the formal logarithm of that:

$$F(t) = \log Z(t)$$

This means that $Z(t) = e^{F(t)}$ where $F(t)$ can be written as

$$\sum \frac{1}{n!} \sum_{j_1,\dots,j_n} t_{j_1} \cdots t_{j_n} \kappa_n(x_{j_1}, \dots, x_{j_n})$$

If you look at what these are, you can see that $\kappa_1(x) = c(x) = \mu_1(x)$, the moment/expectation. Then $\kappa_2(x,y) = c(xy) - c(x)c(y)$. Let me write one more down:

$$\kappa_3(x,y,z) = c(xyz) - \kappa_1(x)\kappa_2(y,z) - \kappa_2(x,y)\kappa_1(z) - \kappa_1(y)\kappa_2(x,z) - \kappa_1(x)\kappa_1(y)\kappa_1(z).$$

These are higher cumulants. You can write these in the following way:

$$c(x_1, \dots, x_n) = \sum_{\pi \in P(n)} \kappa(x_{B_1}) \cdots \kappa(x_{B_{|\pi|}})$$

So here n is the set with n elements and π is a decomposition of n into $|\pi|$ disjoint blocks. There are many equivalent partitions. Each blocks are ordered by the induced order, and the set of blocks by the maximum in the block.

So the partitions of 1 are $\{1\}$. The partitions of 3 are $\{1,2,3\}$ and $\{1\} \sqcup \{2,3\}$ and $\{1,2\} \sqcup \{3\}$ and $\{2\} \sqcup \{1,3\}$ and $\{1\} \sqcup \{2\} \sqcup \{3\}$. I skipped 2 which has $\{1,2\}$ and $\{1\} \sqcup \{2\}$. Then $\kappa(X_B)$ is defined to be $\kappa_r(X_{j_1}, \dots, X_{j_r})$ where $B = \{j_1, \dots, j_r\}$.

So we define the joint cumulants of $\{X_1, \dots, X_r\}$ as the set of cumulants of all sets of elements (with repetition allowed) from the random variables.

The notion of classical independence is that two random variables X and Y are algebraically independent if $\kappa_n(X+Y, \dots, X+Y) = \kappa_n(X, \dots, X) + \kappa_n(Y, \dots, Y)$ for all $n \geq 1$.

So this notion is all from Voiculescu in the non-commutative case. First of all, ordinary probability theory starts from a measure space with a probability measure. Then independence is about the diagram. If I have two events together. If the measure is additive then that's independent. Instead of considering the space I consider the functions. Then measurable functions may form an algebra. In the nice cases some class of functions form an algebra. In the classical sense it's a commutative associative unital algebra. In that case we can translate the notion of independence to the notion I've given. Actual probability theorists don't really like this. They say that they don't form an algebra in general.

If you allow this version, we can just replace A with a non-commutative associative algebra. You can get a non-commutative theory this way. He was greatly inspired by Connes.

This is the end of my brief remark about probability theory, algebraic probability theory. You can google lectures on non-commutative probability theory or consult the book of Terence Tao. He has lecture notes on his homepage. It's beautifully written. I think the best source would be Terence Tao.

So I'm using this dictionary: independent meaning not correlated. If two random variables are not correlated, that means the expectation of the product is the product of their expectation. You can also check that if κ_n vanishes, then all the higher κ_{n+1} and so on vanish. If you change the sign, we have three people that interact with each other. $\kappa_2(X, Y)$ is the secret shared by X and Y. So κ_3 is regarded as like a totality.

Let me have a viewpoint for attacking the integral. Pick some good representatives of the variables, some X_1 through X_r. I don't know $c(X_j)$. I don't know it. But I want, I don't know $\mu_1(X_j)$. Maybe I'll never know this unless I define the measure and the integral. Let's assume though that if you could figure out all the joint moments from this value, then it's good enough. All those complicated correlations of these can be written in terms of the expectation of each random variable, that's good enough. That's a very practical goal, to understand these things.

I want to determine correlation up to finite ambiguity.

Note that c is not an algebra map. In that case there is no correlation. No one would be interested in this problem. The higher cumulant is a higher failure of the algebra homomorphism. You can say that $\kappa_{n+1}(x_1,\ldots,x_{n+1})$ can be written as

$$\kappa_n(X_1,\ldots,X_{n-1},X_nX_{n+1}) - \sum_{\pi\in P(n+1),|\pi|=2,n\nsim n+1} \kappa(X_{B_1})\kappa(X_{B_2}).$$

What you can do immediately is the following. A commutative probability space can be written down in a category. The objects are unital commutative and associative algebras over $\mathbf{k}$ and the morphisms are unit-preserving $\mathbf{k}$-linear maps. These form a category. Then we note that $\mathbf{k}$ is the initial object in the category.

The objects are algebras but the morphisms don't respect the structure. A homotopy probability space is just a diagram ending with the initial object. Let me introduce another category, the objects of $\mathcal{L}$ are $\mathbf{k}$-vector spaces with a distinguished element 1 and whose morphisms are $\phi_1,\ldots,\phi_n$ where $\phi_n : S^nV \to W$ for all n, $\mathbf{k}$-multilinear, such that $\phi_1(1) = 1$ and $\phi_n(X_1,\ldots,X_{n-1},1) = 0$ for $n \geq 2$.

Then we have V and W and U and we have two maps, we need to define composition. Then $\underline{\psi} \bullet \underline{\phi}(x_1,\ldots,x_n) = \sum_{\pi\in P(n)} \psi_{|\pi|}(\phi(X_{B_1}),\ldots,\phi(X_{B_{|\pi|}})$.

I'll define a functor from the first category to the second. You forget the product while $f(X_1,\ldots,X_n) = \sum_{\pi\in P(n)} \phi^f(X_{B_1})\cdots\phi^f(X_{B_n})$.

Call this descendent. Then you can prove that this is a functor. The descendent of composition is composition of descendents.

If you apply this to a diagram that stops at the initial object you get exactly the cumulants. So you can say that the classical algebraic probability space is the study of the stupid category with a functor to this other stupid category.

In algebraic homotopy theory, we have some algebra and there the algebra structure is enhanced by a structure of a cochain complex. The algebra map, it's only a map up to homotopy, and the failure of that homotopy induces another homotopy. If $f(xy)-f(x)f(y) \sim 0$, then $f(xyz)$, what's that? Then determining this has some ambiguity and induces higher homotopy.

Let me make a definition. A homotopy probability space is a tuple $(A,\cdot,1,K)$ with a map c to the ground field. This A is a unital $\mathbb{Z}$-graded supercommutative associative algebra over $\mathbf{k}$. What is $\mathbf{k}$? It's a differential that increases the degree by 1, it squares to zero, it annihilates the unit. Then c is a $\mathbf{k}$-linear map, unit preserving, and $cK = 0$. If A is concentrated in degree zero then this is nothing but a probability space.

We have to think categorically. The objects are now unital graded associative algebras with a differential. The morphisms are cochain maps, unit-preserving.

If I write the tuple A_c, then $A_c \to B_c$ is a degree zero $\mathbf{k}$-linear map f with $f(1) = 1$ and $fK = Kf$. One example for K is $\hbar\Delta + Q$. It's obvious that $\mathbf{k}$ is the initial object in this category. What is a homotopy probability space? It's a diagram which ends at the initial object.

So K is not a derivation of the product. We want to measure the failure. If you think just a little bit you can convince yourself that the morphism does not preserve algebra structure, the differential is not a derivation of product are closely related notions.

[Some physics discussion about whether it is motivated to consider this with a commutative product]

We set up a category whose objects are unital L_∞ algebras over $\mathbf{k}$ and whose morphisms are unital L_∞ morphisms. Then we try to define the same descendent structure.

$$\begin{tikzcd}
A_c \arrow[r, "f"] \arrow[d] & B_c \arrow[d] \\
A_L \arrow[r, "\phi"] & B_L
\end{tikzcd}$$

One way to write down what ϕ^f should be is the following. Consider A_c. Define ℓ_n^K recursively as $[\cdots[K, L_{x_1}], L_{x_2}\cdots, L_{x_n}](1)$

Then $\ell_1^K(x) = K(x)$. We can check $\ell_2^X(x, y) = K(xy) - K(x)y - (-1)^{|x|}xK(y)$. You can write down a formula for ℓ_n^K. So ℓ_2 measures the failure of ℓ_1 being a derivation of the product. So A_L is nothing but A along with 1_A and the descendent structure ℓ^k. We use the same formula with the Koszul sign for ϕ^f.

Claim: this is a functor. If you measure the failure of being a derivation of the product, you get an L_∞ algebra and the failure of being a function is an L_∞ morphism.

If f and f' are homotopic, are these ϕ^f homotopic as L_∞ morphisms? Yes, so this is a homotopy functor.

What is the corresponding notion of random variable? Calin objected to the product, but here, the random variables are elements in A with $KX = 0$. Not everything is a random variable. If the degree is zero, then everything is a random variable. We say that X and X' are homologous if $X' = X + K\lambda$. It's obvious that $c(X) = c(X')$. Then c is defined up to homotopy. We say $c \sim c'$ if $c' = c + \gamma K$. Then $c(X) = c'(X)$. Expectation values should be the same whenever you have things in the same homotopy class, that's what we expect.

Now say we have x and y with $Kx = Ky = 0$. Then we have a well-defined expectation, but what about $c(xy)$? This isn't well-defined. $K(xy)$ is in general nonzero. A second problem is that even if $K(xy) = 0$, if I choose x' and y' which are homologous to x and y, then xy homologous to $x'y'$? The answer is generally no. If so, then the product of random variables would only depend on the homology classes. But this isn't guaranteed. Unfortunately, to understand correlations, we don't have $c(xy)$ that we can write in terms of cohomology. This is stupid. It's the wrong product.

In the end, let's return to the cumulant. The notions of the cumulant and moment were related to this world, and were defined up to homotopy. Anything meaningful we can observe must be homotopy invariant. We'll make something homotopy invariant. We now use the following thing. We need a "homotopical set of random variables."

We'll define this not as a subset of the vector space A but the image of some morphism. This is a finite dimensional graded vector space, which I regard as having zero L_∞ structure. Then we have A_c, and the descendent A_L which has ℓ^K, and we have c to the ground field, and κ_c which is a descendent. We consider an L_∞ morphism $\psi_1, \ldots, \psi_n$. This is an L_∞ morphism. What I'm trying to say is to define a homotopy set of random variables as an L_∞ map from a trivial L_∞ algebra to A_L.

Introduce a basis e_α of V and the dual basis t^α and consider θ^ψ which is defined to be

$$\sum \frac{1}{n!}\sum_\alpha t_{\alpha_1}\cdots t_{\alpha_n}\psi_n(e_{\alpha_1}, \ldots, e_{\alpha_n})$$

Remember that $\psi_1(e_\alpha) \in A$. Since this is an L_∞ morphism, we know that $K(\psi_1(e_\alpha)) = 0$. So this is our x_α. Then we consider $\Omega^\psi = e^{\theta^\psi}$ which lives in $(\mathbf{k}[[t_\alpha]] \otimes A)^0$.

Then Ω can be written as $\Omega_0 + \Omega_1 + \cdots$. Then $\Omega_0 = 1$ and $\Omega_1 = \sum t_\alpha \psi_1(e_\alpha)$. It's a little interesting, $\Omega_2 = t_\alpha t_\beta(\psi_1(e_\alpha)\psi_1(e_\beta) + \psi_2(e_\alpha, e_\beta))$.

Theorem 9.1. *We have $K\Omega^\psi) = 0$ and $\psi \sim \psi'$ implies $\Omega^{\psi'} - \Omega^\psi = K$ of something.*

So $Z = c(e^{\theta^\psi})$ is invariant of homotopy type. Of course, the corresponding moment generating function can be written. You can get cumulants by composing from $(V, 0)$ to $\mathbf{k}$ and the cumulants are well-defined.