Arithmetic Field Theories and Arithmetic Invariants

Minhyong Kim
ICMS/Maxwell Institute
Edinburgh

Berkeley, November, 2021

1. Classification of arithmetic principal bundles

Classification of arithmetic principal bundles

Over a point?

The point is

$$\mathrm{Spec}(F),$$

where F is an algebraic number field, which has a complicated étale topology.

The data of the principal bundle is a topological group R and a space P with simply-transitive continuous right action of R. However, these are sheaves on $\mathrm{Spec}(F)$.

There is the inclusion $F \subset \bar{\mathbb{Q}} \subset \mathbb{C}$, where $\bar{\mathbb{Q}}$ is the field of all algebraic numbers and a natural topological group associated to it:

$$\pi_1(\mathrm{Spec}(F)) := \mathrm{Gal}(\bar{\mathbb{Q}}/F).$$

The sheaf structure is encoded in the fact that both R and P are equipped with compatible left actions of $\pi_1(\mathrm{Spec}(F))$.

Classification of arithmetic principal bundles

We denote by

$$\mathcal{M}(F,R) = H^1(F,R) = H^1(\pi_1(\mathrm{Spec}(F)),R),$$

the set of isomorphism classes of principal R-bundles on $\mathrm{Spec}(F)$, which can also be described as a set of R-valued cocycles on $\pi_1(\mathrm{Spec}(F))$ modulo an equivalence relation.

The group R is often a p-adic Lie group, e.g., $GL_n(\mathbb{Z}_p)$, or a finite group, the two cases being related by

$$GL_n(\mathbb{Z}_p) = \varprojlim GL_n(\mathbb{Z}/p^n).$$

But it might be a finite group like $A[p]$ for an abelian variety A or

$$T_pA = \varprojlim A[p^n] \simeq \mathbb{Z}_p^{2g},$$

which has a highly non-trivial action of $\pi_1(\mathrm{Spec}(F))$.

Classification of arithmetic principal bundles

The classification problem, i.e, understanding the structure of $H^1(F, R)$, is difficult mostly because of the complexities of $\pi_1(\mathrm{Spec}(F))$.

For example, when R has trivial action, then

$$H^1(F, R) = \mathrm{Hom}(\pi_1(\mathrm{Spec}(F)), R)/R,$$

a space of representations.

So a complete description would comprise the Langlands reciprocity conjecture.

Classification over arithmetic 3-folds

Let $\mathcal{O}_F$ be the ring of algebraic integers in F and let

$$X := \mathrm{Spec}(\mathcal{O}_F),$$

which is the set of prime ideals in $\mathcal{O}_F$, endowed with a complicated topology (étale). It has many properties of a compact closed three-manifold.

If v is a maximal ideal in $\mathcal{O}_F$, then $k_v = \mathcal{O}_F/v$ is a finite field and the inclusion

$$\mathrm{Spec}(k_v) \hookrightarrow X$$

is analogous to the inclusion of a knot.

The completion $\mathrm{Spec}(\mathcal{O}_{F,v})$ (e.g., $\mathbb{Z}_p$) is like the tubular neighbourhood of the knot.

Classification over arithmetic 3-folds

The completion F_v (e.g. $\mathbb{Q}_p$) of F is the fraction field of $\mathcal{O}_{F,v}$, so that

$$\mathrm{Spec}(F_v) = \mathrm{Spec}(\mathcal{O}_{F,v}) \setminus v$$

is like the tubular neighbourhood with the knot deleted, which should be homotopic to a torus.

If B is a finite set of primes and $\mathcal{O}_{F,B}$ is the set of B-integers, then

$$X_B := \mathrm{Spec}(\mathcal{O}_{F,B}) = \mathrm{Spec}(\mathcal{O}_F) \setminus B$$

is like a three-manifold with boundary, the boundary having one torus component $\mathrm{Spec}(F_v)$ for each prime in B.

$$\partial X = \coprod_{v \in B} \mathrm{Spec}(F_v) \longrightarrow X_B \hookrightarrow X.$$

Classification over arithmetic 3-folds: Fundamental groups

Rather easy to describe:

$$\pi_1(\mathrm{Spec}(k_v)) = \mathrm{Gal}(\bar{k_v}/k_v) = \hat{\mathbb{Z}}$$

Somewhat harder, but still explicit and natural:

$$\pi_v = \pi_1(\mathrm{Spec}(F_v)) = \mathrm{Gal}(\bar{F_v}/F_v).$$

This leads to fairly accessible descriptions of

$$H^1(F_v, R) = H^1(\pi_v, R),$$

in many cases.

The global fundamental groups are much harder.

Classification over arithmetic 3-folds: Fundamental groups

A finite field extension K/F is unramified over $\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_F)$ if the decomposition

$$\mathcal{P}\mathcal{O}_K = \prod \mathcal{Q}_i$$

into prime ideals in $\mathcal{O}_K$ has no multiplicity.

F^{un}/F is the compositum of all finite field extensions that are unramified over all primes of F.

F^{un}_B/F is the compositum of all finite field extensions that are unramified over all primes not in B.

We have the following arithmetic fundamental groups:

$$\pi_1(X) = \mathrm{Gal}(F^{un}/F);$$

$$\pi_1(X_B) = \mathrm{Gal}(F^{un}_B/F).$$

Classification over arithmetic 3-folds: Fundamental groups

Very difficult to describe in general, even though $\pi_1(X)^{ab}$ is finite and isomorphic to $Pic(\mathcal{O}_F)$, the ideal class group of F.

Some triviality:

$$\pi_1(\mathrm{Spec}(\mathbb{Z})) = 0$$

More triviality

$$\pi_1(\mathrm{Spec}(\mathcal{O}_F) = 0$$

when F is an imaginary quadratic field of class number 1.

Some difficult examples:

$$\pi_1(\mathrm{Spec}(\mathcal{O}_{\mathbb{Q}\sqrt{653}})) = A_5.$$

(Kwang-Seob Kim, subject to RH)

$$\pi_1(\mathrm{Spec}(\mathcal{O}_{\mathbb{Q}\sqrt{-1567}})) = PSL_2(\mathbb{F}_8) \times C_{15}.$$

(Kwangseob Kim and Jochen König, subject to RH).

Classification over arithmetic 3-folds

The group

$$\pi_1(X_B) \twoheadrightarrow \pi_1(X)$$

is essentially inaccessible at present.

Nonetheless, we would like to understand

$$\mathcal{M}(X_B, R) = H^1(X_B, R) = H^1(\pi_1(X_B), R),$$

the isomorphism classes of principal R bundles over X_B.

Also

$$\mathcal{M}(X_B, R) = H^1(X_B, R) \xrightarrow{\mathrm{loc}_B} \prod_{v \in B} H^1(F_v, R) = \prod_{v \in B} \mathcal{M}(F_v, R)$$

whose image can sometimes be given a Lagrangian structure inside a non-Archimedean symplectic manifold.

When R has trivial action of $\pi_1(X_B)$, then this is a space of representations:

$$H^1(\pi_1(X_B), R) = \mathrm{Hom}(\pi_1(X_B), R)//R.$$

Classification over arithmetic 3-folds

Note that elements of $H^1(X, R)$ are like flat connections, while $H^1(X_B, R)$ are like flat connections with singularities? What are the 'off-shell fields'?

Some possible answers:

–Families

$$\{P_v\}_v$$

where P_v is a principal R bundle over $\mathrm{Spec}(F_v)$.

–For $R = GL_n(\mathbb{Z}_p)$, families $(M_v)_v$, where M_v is a $\mathbb{C}$-vector space with an action of the Weil-Deligne group of F_v.

–These are already off-shell, while the on-shell fields are the principal bundles of geometric origin.

II. Arithmetic actions

Arithmetic Actions

For technical reasons, we will assume throughout that F is complex, i.e., $F = \mathbb{Q}[x]/(f(x))$ where $f(x)$ has no real roots.

Would like to define

$$S : \mathcal{M}(X_B, R) = H^1(\pi_1(X_B), R) \longrightarrow K$$

as well as path integrals

$$\int_{\rho \in \mathcal{M}(X_B, R)} \exp\left(cS(\rho)\right) d\rho$$

possibly also on off-shell fields and/or related moduli spaces.

Motivating example: when $R = GL(V)$ with trivial action of $\pi_1(X_B)$, so that $\mathcal{M}(X_B, R)$ is a space of homomorphisms

$$\rho : \pi_1(X_B) \longrightarrow R.$$

Arithmetic actions: L-function

In that case, one has:

$$L : \mathcal{M}(X_B, GL(V)) \longrightarrow \mathbb{C} \quad (\text{or } \mathbb{C}_p).$$

To a representation $\rho : \pi_1(X_B) \longrightarrow GL(V)$, assign the value

$$L(\rho) = \prod_{v \text{ primes of } \mathcal{O}_F} \frac{1}{\det([I - Fr_v]|V^{I_v})}$$

$$= (\prod_{v \notin B} \frac{1}{\det([I - Fr_v]|V)})(\prod_{v \in B} \frac{1}{\det([I - Fr_v]|V^{I_v})}).$$

This is often infinite, so instead define

$$L(\rho(s)) = \prod_{v} \frac{1}{\det([I - |k_v|^{-s} Fr_v]|V^{I_v})}$$

for $Re(s) >> 0$ and try to compute $L(\rho)$ by analytic continuation.

Arithmetic actions: L-function

Even when the continuation can be carried out, we can have $L(\rho) = 0$.

In this case we focus on $L^{(r)}(0)/r!$, where $r = \mathrm{ord}_{s=0} L(\rho(s))$. Both the order and value have arithmetic interpretations.

For example, if $\rho = Triv$, then

$$r = \mathrm{rank}(\mathcal{O}_F^\times)$$

and we have

$$\frac{L^{(r)}(Triv, 0)}{r!} = -|Pic(\mathcal{O}_F)| \| \det(\mathcal{O}_F^\times) \|.$$

When ρ is $T_p E$, for $E/\mathbb{Q}$ an elliptic curve, then (BSD-conjecturally)

$$r = \mathrm{rank} E(\mathbb{Q}),$$

and

$$\frac{L^{(r)}(T_p E, 0)}{r!} = (\prod_v c_v) |\text{Ш}_E| \| \det(E(\mathbb{Q})) \|^2$$

Preliminary on arithmetic orientations

Orientation: Let μ_n be the n-th roots of 1. Then

$$H^3(X, \mu_n) = H^3(\mathrm{Spec}(\mathcal{O}_F), \mu_n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

This follows from

$$1 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{(\cdot)^n} \mathbb{G}_m \longrightarrow 1,$$

leading to

$$H^3(X, \mu_n) \simeq H^3(X, \mathbb{G}_m)[n].$$

Meanwhile

$$H^3(X, \mathbb{G}_m) \simeq \mathbb{Q}/\mathbb{Z}.$$

Arithmetic orientations

Local class field theory:

$$H^2(F_v, \mathbb{G}_m) \simeq \mathbb{Q}/\mathbb{Z}$$

Global class field theory:

$$0 \longrightarrow H^2(F, \mathbb{G}_m) \xrightarrow{\text{loc}} \oplus_v H^2(F_v, \mathbb{G}_m) \xrightarrow{\sum} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

$$0 \longrightarrow H^2(X_B, \mathbb{G}_m) \xrightarrow{\text{loc}_B} \oplus_{v \in B} H^2(F_v, \mathbb{G}_m) \xrightarrow{\sum} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

But

$$\oplus_{v \in B} H^2(F_v, \mathbb{G}_m) = H^2(\partial X_B, \mathbb{G}_m),$$

so that

$$coker(\text{loc}_B) \simeq H^3_c(X_B, \mathbb{G}_m) \simeq H^3(X, \mathbb{G}_m).$$

Arithmetic Chern-Simons Functionals (Finite Case)

Assume $\mu_n \subset F$. Then

$$H^3(X, \mathbb{Z}/n) \simeq H^3(X, \mu_n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

so we get a map

$$\text{inv} : H^3(\pi_1(X), \mathbb{Z}/n) \longrightarrow H^3(X, \mu_n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Let R have trivial $\pi_1(X)$-action. On the moduli space

$$\mathcal{M}(X, R) = \text{Hom}(\pi_1(X), R)//R,$$

of continuous representations of $\pi_1(X)$, a Chern-Simons functional is defined as follows.

Arithmetic Chern-Simons Functionals (Finite Case)

The functional will depend on the choice of a cohomology class (a level)

$$c \in H^3(R, \mathbb{Z}/n).$$

Then

$$\mathbb{CS} : \mathcal{M}(X, R) \longrightarrow \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is defined by

$$\rho \mapsto \rho^*(c) \in H^3(\pi_1(X), \mathbb{Z}/n) \mapsto \mathrm{inv}(\rho^*(c)).$$

Arithmetic Chern-Simons Functionals (Finite Case)

Example:

Let $R = \mathbb{Z}/n$. Then

$$\mathcal{M}_X = \text{Hom}(Pic(X), \mathbb{Z}/n),$$

where $Pic(X)$ is the group of invertible line bundles on $X = \text{Spec}(\mathcal{O}_F)$ (the ideal class group of F).

Take $c \in H^3(R, \mathbb{Z}/n)$ to be given as

$$a \cup \delta a,$$

where $a \in H^1(R, \mathbb{Z}/n) = \text{Hom}(\mathbb{Z}/n, \mathbb{Z}/n)$ is the class coming from the identity map, while

$$\delta : H^1(R, \mathbb{Z}/n) \longrightarrow H^2(R, \mathbb{Z}/n)$$

is the Bockstein map coming from the extension

$$0 \longrightarrow \mathbb{Z}/n \longrightarrow \mathbb{Z}/n^2 \longrightarrow \mathbb{Z}/n \longrightarrow 0.$$

Then

$$\mathbb{CS}_{a\cup\delta a}(\rho) = \text{inv}(\rho^*(a) \cup \rho^*(\delta a)).$$

Arithmetic Chern-Simons invariants

[Joint work with H. Chung, D. Kim, G. Pappas, J. Park, H. Yoo]

Let $n = p$, a prime and assume the Bockstein map

$$d : H^1(X, \mathbb{Z}/n) \longrightarrow H^2(X, \mathbb{Z}/n)$$

is an isomorphism. Let $a = \dim_{\mathbb{F}_p}(Pic(X)/p)$.

Then

$$\sum_{\rho \in (Pic(X)/p)^\vee} \exp[2\pi i \mathbb{CS}(\rho)]$$

$$= p^{a/2} \left(\frac{\det(d)}{p} \right) i^{\left[\frac{a(p-1)^2}{4}\right]}.$$

Arithmetic differentials

The Bockstein map

$$d : H^1(X, \mathbb{Z}/n) \longrightarrow H^2(X, \mathbb{Z}/n)$$

is very much like a differential. In crystalline cohomology of varieties over perfect fields of positive characteristic, Bockstein maps on crystalline cohomology sheaves are used to construct the De Rham-Witt complex.

In general, whenever you have an extension

$$0 \longrightarrow V \longrightarrow E \longrightarrow V \longrightarrow 0,$$

there is a differential

$$H^1(X, V) \longrightarrow H^2(X, V)$$

that can be used to construct arithmetic functionals.

Arithmetic BF-theory: [Joint work with Magnus Carlson]

There is also a bilinear map

$$BF : H^1(X, \mathbb{Z}/n) \times H^1(X, \mu_n) \longrightarrow \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

$$(a, b) \mapsto \mathrm{inv}(da \cup b).$$

Note that $da \cup b \in H^3(X, \mu_n)$ and μ_n doesn't need to be trivialised.

Proposition

For $n >> 0$,

$$\sum_{(a,b)\in H^1(X,\mathbb{Z}/n)\times H^1(X,\mu_n)} \exp(2\pi i BF(a, b))$$

$$= |Pix(X)[n]||\mathcal{O}_X^\times/(\mathcal{O}_X^\times)^n|.$$

Compare with

$$\frac{L^{(r)}(Triv, 0)}{r!} = -|Pic(X)|\|\det(\mathcal{O}_F^\times)\|$$

Arithmetic BF-theory

Similarly, if E is an elliptic curve with Neron model $\mathcal{E}$, then we have

$$0 \longrightarrow \mathcal{E}[n] \longrightarrow \mathcal{E}[n^2] \longrightarrow \mathcal{E}[n] \longrightarrow 0$$

for $n >> 0$. This gives us a map

$$H^1(X, \mathcal{E}[n]) \times H^1(X, \mathcal{E}[n]) \longrightarrow \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

as

$$(a, b) \longrightarrow \mathrm{inv}(da \cup b).$$

Proposition

For $n >> 0$,

$$\sum_{(a,b) \in H^1(X,\mathcal{E}[n]) \times H^1(X,\mathcal{E}[n])} \exp(2\pi i BF(a, b))$$

$$= |\text{Ш}(A)[n]||E(F)/n|^2.$$

Arithmetic BF-theory

Compare

$$\frac{L^{(r)}(T_pE,0)}{r!} = (\prod_v c_v)|Ш_E|\|\det(E(F))\|^2$$

III. Some Remarks on Function Fields

Fibered 3-manifolds

A curve $X/\mathbb{F}_q$ is viewed as analogous to a fibered three-manifold

$$M \xrightarrow{\pi} S^1.$$

Then

$$\bar{X} = X \otimes \bar{\mathbb{F}}_q$$

is the analogue of

$$\Sigma := \pi^{-1}(1),$$

and the Frobenius becomes analogous to the isotopy class of the monodromy transformation

$$f : \Sigma \simeq \Sigma.$$

Fibered 3-manifolds

A 3d TQFT will assign a vector space

$$H(\Sigma)$$

to the surface Σ.

In that case,

$$Z(M) = Tr(f|H(\Sigma)).$$

Can we assign

$$\bar{X} \mapsto H(\bar{X})$$

with Frobenius action?

Fibered 3-manifolds

[joint work in progress with David Ben-Zvi and Akshay Venkatesh]

Choose N such that $q \equiv 1 \mod N$. Let

$$H(\bar{X}) := \Gamma(J, \mathcal{L}^N),$$

where J is the Jacobian of a lift of $\bar{X}$ to characteristic zero.

Then $J[N]$ acts projectively on $H(\bar{X})$ and so does the symplectic group of $J[N]$ via the Weil representation.

The action of Fr_q on $J[N]$ puts it into the symplectic group.

Fibered 3-manifolds

Assume $J[N] = W \times W'$, where W, W' are Lagrangian, stabilised by Frobenius. Then

Theorem

$$Tr(Fr_q|H) = \sqrt{|Cl(X)[N]|}.$$

This is kind of a μ_N-CS-invariant of X.

Interesting to compare with the number field case, where

$$\mathbb{CS}(X, \mu_p) = \sqrt{|C_F[p]|} \left(\frac{\det(d)}{p} \right) i^{\left[\frac{dim(C_F[p])(p-1)^2}{4}\right]}$$

Fibered 3-manifolds

Gaitsgory, Rosenblyum, Raskin, ...study a $4d$ theory over finite fields.

Thus,

$$H(\bar{X})$$

is a dualisable category.

They then take a categorical trace

$$Tr(Fr_q|H(\bar{X}))$$

which is a vector space over $\bar{\mathbb{Q}}_\ell$. This is identified with a space of automorphic forms.

We are trying a $3d$ version of this.

IV. Chern-Simons with Boundaries

Finite Arithmetic Chern-Simons Functionals with Boundaries

$X_B = \text{Spec}(\mathcal{O}_F[1/B])$ for a finite set B of primes;

$\partial X_B = \coprod_{v\in B} \text{Spec}(F_v)$.

$$\pi_1(X_B) := \text{Gal}(F_B^{un}/F), \quad \pi_v := \text{Gal}(\bar{F}_v/F_v),$$

and fix a tuple of homomorphisms

$$i_S = (i_v : \pi_v \longrightarrow \pi_1(X_B))_{v\in B}$$

corresponding to embeddings $\bar{F} \hookrightarrow \bar{F}_v$.

Assume B contains all places dividing n.

Now $c \in Z^3(R, \mathbb{Z}/n)$ will denote a 3-cocycle.

Finite Arithmetic Chern-Simons Functionals with Boundaries

In addition to the global moduli space

$$\mathcal{M}(X_B, R) = \mathrm{Hom}(\pi_1(X_B), R)//R$$

we have the local moduli space

$$\mathcal{M}(\partial X_B, R) := \{\phi_B = (\phi_v)_{v \in B} \mid \phi_v : \pi_v \longrightarrow R\}//R$$

Thus, we get a localisation map

$$\mathrm{loc}_B = i_B^* : \mathcal{M}(X_B, R) \longrightarrow \mathcal{M}(\partial X_B, R)$$

Finite Arithmetic Chern-Simons Functionals with Boundaries

Key cohomological facts:

$$H^2(\pi_v, \mathbb{Z}/n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

$H^i(\pi_v, \mathbb{Z}/n) = 0$ for $i > 2$.

There is a symplectic non-degenerate pairing

$$H^1(\pi_v, \mathbb{Z}/n) \times H^1(\pi_v, \mathbb{Z}/n) \longrightarrow H^2(\pi_v, \mathbb{Z}/n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

There is an exact sequence

$$0 \longrightarrow H^1(X_B, \mathbb{Z}/n) \longrightarrow \prod_{v \in B} H^1(\pi_v, \mathbb{Z}/n) \xrightarrow{\sum} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \longrightarrow 0.$$

Finite Arithmetic Chern-Simons Functionals with Boundaries

For any $\phi_B = (\phi_v)$, each $\phi_v^*(c) \in Z^3(\pi_v, \mathbb{Z}/n)$ is trivial. Thus,

$$\mathcal{T}_v := d^{-1}(\phi_v^*(c)) \in C^2(\pi_v, \mathbb{Z}/n)/B^2(\pi_v, \mathbb{Z}/n)$$

is a torsor for $H^2(\pi_v, \mathbb{Z}/n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Hence,

$$\prod_{v \in B} \mathcal{T}_v$$

is a torsor for

$$\prod_{v \in B} H^2(\pi_v, \mathbb{Z}/n) \simeq \prod_{v \in B} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

.

Finite Arithmetic Chern-Simons Functionals with Boundaries

We push this out using the sum map

$$\Sigma : \prod_{v \in B} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \longrightarrow \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

to get a $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsor

$$\mathcal{T}(\phi_B) := \Sigma_*(\prod_v d^{-1}(\phi_v)).$$

As ϕ_B varies, we get a $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$-torsor

$$\mathcal{T} \longrightarrow \mathcal{M}(\partial X_B, R)$$

over the local moduli space.

Finite Arithmetic Chern-Simons Functionals with Boundaries

If $\rho \in \mathcal{M}(X_B, R)$, because $H^3(\pi_1(X_B), \mathbb{Z}/n) = 0$, we can solve

$$d\beta = \rho^*(c) \in Z^3(\pi_1(X_B), \mathbb{Z}/n),$$

and put

$$\mathbb{CS}(\rho) = \Sigma_*(\mathrm{loc}_B(\beta)) \in \mathcal{T}(\mathrm{loc}_B(\rho)).$$

Lemma

$\mathbb{CS}(\rho)$ *is independent of the choice of* β*.*

This follows immediately from the reciprocity sequence

$$0 \longrightarrow H^2(\pi_1(X_B), \mathbb{Z}/n) \longrightarrow \prod_{v \in B} H^2(\pi_v, \mathbb{Z}/n) \xrightarrow{\Sigma} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \longrightarrow 0,$$

Thus, as ρ varies, we get a canonical section

$$\mathbb{CS} \in \Gamma(\mathcal{M}(X_B, R), (\mathrm{loc}_B)^*(\mathcal{T})).$$

Finite Arithmetic Chern-Simons Functionals with Boundaries

Can use the map

$$\exp 2\pi i : \frac{1}{n}\mathbb{Z}/\mathbb{Z} \longrightarrow S^1.$$

to push $\mathcal{T}$ out to a unitary line bundle $\mathcal{U}$ over $\mathcal{M}(\partial X_B, R)$.

Can also do this to the individual $\mathcal{T}_v$ to get a line bundle $\mathcal{U}_v$ over $\mathcal{M}(F_v, R)$.

Then

$$\mathcal{U} \simeq \boxtimes_{v\in B}\mathcal{U}_v$$

and

$$\mathcal{H}_B = \Gamma(\mathcal{M}(\partial X_B), R), \mathcal{U}) \simeq \otimes_{v\in B}\Gamma(\mathcal{M}(F_v, R), \mathcal{U}_v)$$

$$= \otimes_{v\in B}\mathcal{H}_v$$

Finite Arithmetic Chern-Simons Functionals with Boundaries

Thus, one has

$$\exp(2\pi i \mathbb{CS}(\rho)) \in \mathcal{U}_{\mathrm{loc}_B(\rho)}$$

and

$$\int_{\{\rho \mid \mathrm{loc}_B(\rho)=\rho_B\}} \exp(2\pi i \mathbb{CS}(\rho)) \in \mathcal{U}_{\rho_B}.$$

As ρ_B varies get an element of $\mathcal{H}$.

From the view of topological quantum field theory, this is the state

$$\Psi(X_B) \in \Gamma(\mathrm{loc}(\mathcal{M}(\partial X_B, R)), \mathcal{U})$$

on ∂X_B that the theory assigns to X_B.

V. Entanglement of primes

Entanglement entropy of primes

If we put

$$\mathcal{H}_v = \Gamma(\mathcal{M}(F_v, R), \mathcal{U}),$$

Then

$$\Gamma(\mathcal{M}(\partial X_B, R), \mathcal{U}) \simeq \otimes_{v \in B} \mathcal{H}_v.$$

Let $B := v_1, v_2$ be two primes in $\mathcal{O}_F$. For

$$\Psi(X_B) \in \mathcal{H}_{v_1} \otimes \mathcal{H}_{v_2},$$

let

$$\rho_{v_1} := \mathrm{Tr}_{v_2}(\Psi(X_B))$$

Define the *entanglement entropy* of v_1 and v_2 by

$$Ent(v_1, v_2) := -Tr(\rho_{v_1} \log \rho_{v_1}),$$

Arithmetic analogue of construction of V. Balasubramanian, J.R. Fliss, R.G. Leigh and O. Parrikar, 'Multi-boundary entanglement in Chern-Simons theory and link invariants'.

Entanglement entropy of primes

[Joint work with Hee-Joong Chung, Dohyeong Kim, Jeehoon Park, and Hwajong Yoo]

Take $n = p$ and $R = \mathbb{F}_p$. Let

$$\mathrm{loc}_v : \mathcal{M}(X_B, \mathbb{F}_p) \longrightarrow \mathcal{M}(\pi_v, \mathbb{F}_p)$$

be the localisation map to the moduli space over F_v.

Then

Theorem

Assume $Pic(X_B)[p] = 0$. Then

$$Ent(v_1, v_2)$$

$$= [dim\mathcal{M}(X_B, \mathbb{F}_p) - dimKer(loc_{v_1}) - dimKer(loc_{v_2}) + |A^S_{F,p}|] \log p.$$

Here, $A^S_{F,p}$ is the Galois group of the maximal unramified p-torsion extension of F that is split over the primes in S.

Entanglement entropy of primes

Explicit example:

$F = \mathbb{Q}(\zeta_{25}),\ R = \mathbb{F}_5,\ B = \{v = (1 - \zeta_{25}), w = (3)\}.$

Then

$$Ent(v, w) = 2 \log 5$$