Jacob Lurie, Arizona Winter School
Day 1, Lecture 1

Motivation

Consider classifying quadratic forms. We'd like to know when two are equal – i.e., when one can be obtained from the other by a linear change of variables.

Definition: Let R be a ring and q, q' be quadratic forms over R. We characterize their **equivalence** in the following way:

$$q \equiv q' \iff \forall R,\ \exists A \in \mathrm{GL}(n, R) \ \ni\ q = q' \circ A$$

Note that q, q' are positive definite, then they are automatically equivalent in $R = \mathbb{R}$.

Examples:

1. $x^2 + y^2$
2. $x^2 - y^2$
3. $-x^2 - y^2$

Note that these are all equivalent over $\mathbb{C}$, under the map $x \mapsto ix$ which sends $x^2 \to -x^2$. But these are not equivalent over $\mathbb{R}$, since (1) is positive-definite, (2) is indefinite, and (3) is negative definite.

We can similary have forms equivalent over $\mathbb{R}$ but not over $\mathbb{Z}$, e.g. by considering $x^2 + 3y^2$. This is equivalent to (1) over $\mathbb{R}$, since we have $\sqrt{3}$, but not over $\mathbb{Z}$ – this can be seen by reducing mod 3.

So we have two methods

- Look over $\mathbb{R}$, diagonalize, take signature
- Reduce mod p for various p.

Are these all you need?

Genus

Definition: The **genus** of a quadratic form is characterized by

$$q, q' \text{ are in the same genus } \iff \forall n \in \mathbb{N}, \quad q \equiv q' \mod n$$

Remark: there are only finitely many forms in each genus, and there is a formula to count them: the Smith-Minkowski-Segal formula.

Definition: For a commutative ring R, we define the **orthogonal group** over R to be

$$O_q(R) = \{A \in \mathrm{GL}(n, R) \ \ni \ q \circ A = q\},$$

i.e. the square matrices that preserve the quadratic form q.

Note that $O_q(\mathbb{R})$ is the usual orthogonal group, which is a compact Lie group.

Definition: Suppose q has genus g, then we define the **mass** of q as

$$\mathrm{Mass}(q) = \sum_{q' \ \ni \mathrm{genus}(q') = g} \frac{1}{O_{q'}(\mathbb{Z})}$$

which counts the number of forms of the same genus as q.

Definition: q is **unimodular** if q is nondegenerate nondegenerate mod n for all n.

For two forms in the same genus, q, q', then q is unimodular iff q' is, but the converse is actually true as well – for a fixed number of variables, any two unimodular forms are in the same genus.

Supposing q is unimodular, we can write the mass formula

$$\text{Mass}(q) = \sum_{q' \text{unimodular}} \frac{1}{O_{q'}(\mathbb{Z})} = \zeta(\frac{n}{2}) \frac{\zeta(2)\zeta(4)\cdots\zeta(n-2)}{\text{vol } S^1 \text{vol } S^2 \cdots \text{vol } S^n}$$

where the denominators are the volumes of spheres, and the numerator contains certain values of the Riemann-zeta function.

If, for example $n = 8$, we obtain

$$\frac{1}{2^{14}3^5 5^2 7}$$

This is actually the order of the Weil group of the exceptional Lie group E_8, i.e. $|W(E_8)|$. This appears as the symmetries of a certain quadratic over $\mathbb{Z}$ – namely the form associated to the root lattice of E_8. So we have one form that gives exactly the RHS of the mass formula, which tells us that there can only be one term on the LHS, and thus there is a unique unimodular form in 8 variables.

You can get other information from this formula – for example, if the RHS is large, note that the LHS contains summands all of which are less than 1, so there have to be many (many!) terms.

Counting Within a Genus

Let q, q' be in the same genus, so for each n there exists an A_n such that $q = q' \circ A_n$ for some $A_n \in \mathrm{GL}(n, \mathbb{Z}/n\mathbb{Z})$. By a compactness argument, we can make a choice that works for all n, so we consider the system $A := \{A_n\}$ which lives in $\mathrm{GL}(n, \hat{\mathbb{Z}})$.

> Recall that $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ is the ring of profinite integers, which can also be described as $\prod_{p \in \mathbb{P}} \mathbb{Z}_{(p)}$, the product of the p-adic integers over all primes.

We then get $q \equiv q'$ over $\hat{\mathbb{Z}}$, which means they are also equivalent over the p-adic integers $\mathbb{Z}_{(p)}$ for each p – but this means they are also equivalent over $\mathbb{Q}_{(p)} = \mathbb{Z}_{(p)}[\frac{1}{p}]$, i.e. the field of p-adic rational numbers obtained by adjoining an inverse of p.

Now invoke the Hasse-Minkowski theorem:

$$q \equiv q' \text{ over } \mathbb{Q} \iff q \equiv q' \text{ over every completion of } \mathbb{Q}.$$

Note that this includes $\mathbb{R}$ (the archimedean completion), as well as the p-adic completions $\mathbb{Q}_{(p)}$.

This lets us write $q = q' \circ B$ with $B \in \mathrm{GL}(n, \mathbb{Q})$, which lets us produce a new quadratic form that preserves q given by

$$q = q' \circ A = (q \circ B^{-1}) \circ A := q \circ M$$

and so $M \in O_q(R)$ for some ring R. To make sense of

multiplying A and B, since they are in different rings, we embed them both into the bigger ring

$$R = A^{\text{fin}} := \hat{\mathbb{Z}} \otimes \mathbb{Q} \subseteq \prod_{p \in \mathbb{P}}^{\text{restricted}} \mathbb{Q}_{(p)}$$

where the restricted product only allows finitely many primes in denominators.

Note that since $A \in \mathrm{GL}(n, \hat{\mathbb{Z}})$, M is only well-defined up to right-multiplication by elements in $O_q(\hat{\mathbb{Z}})$, and similarly it is only well-defined up to left-multiplication by elements in $O_q(\mathbb{Q}_p)$. If we take the double quotient out by these groups (forming a double coset), we get something unique.

If you land in the identity coset here, you have $B^{-1}A = I$, and so each entry of M would need to lie in $\mathbb{Q} \bigcap \hat{\mathbb{Z}} = \mathbb{Z}$. Moreover, this collection of cosets bijects with equivalence classes of quadratic forms in the genus of q.

This gives you a way to take a q' and produce a quotient, the size of which counts the isomorphism classes within a genus – going the other way is slightly easier.

Let $A = A^{\text{fin}} \times \mathbb{R}$; this is a locally compact ring containing $\mathbb{Q}$ as a discrete subring. We can then replace $O_q(A^{\text{fin}})$ with $O_q(A)$, which adds in a factor of $O_q(\mathbb{R})$, but this can be offset by replacing $O_q(\hat{\mathbb{Z}})$ with $O_q(\hat{\mathbb{Z}} \times \mathbb{R})$.

This makes each O_q in the equation a locally compact group, so we can take a Haar measure μ which is invariant under left-translation. This descends to a measure on $O_q(A)/O_q(\mathbb{Q})$, so

we'd like to understand the orbits under the action of $O_q(\hat{\mathbb{Z}} \times \mathbb{R})$.

If this was a free action, we would have

$$|\text{orbits}| = \frac{\mu(O_q(A)/O_q(\mathbb{Q}))}{\mu(O_q(\hat{\mathbb{Z}} \times \mathbb{R}))},$$

but since this is not a free action, orbits are counted with multiplicity.

For each orbit o, letting $G_o < O_q(\hat{\mathbb{Z}} \times \mathbb{R})$ being the subgroup that fixes some point in that orbit, i.e. the stabilizer subgroup. Then each multiplicity is equal to $\frac{1}{|\mathrm{G_o}|}$. Since each orbit o corresponds to a quadratic form q' in the genus of q and each stabilizer subgroup G_o corresponds to the symmetry group of q', the LHS is exactly $\mathrm{Mass}(q)$, and so we get

$$\mathrm{Mass}(q) = \frac{\mu(O_q(A)/O_q(\mathbb{Q}))}{\mu(O_q(\hat{\mathbb{Z}} \times \mathbb{R}))}.$$

Note that even though the Haar measure is only unique up to scalar multiplication, since a measure appears in the numerator and the denominator it will cancel. However, we can still apply a certain normalization that allows us to evaluate each independently.

Getting a Canonical Measure (The Tamagawa

Measure)

Definition: **the special orthogonal group** of R is defined as

$$SO_q(R) = \{A \in O_q(R) \ \ \text{э} \ \ \det A = 1\}.$$

This also has a Haar measure μ_S, and it turns out that for some $k \in \mathbb{N}$,

$$2^k \mathrm{Mass}(q) = \frac{\mu_S(SO_q(A)/SO_q(\mathbb{Q})}{\mu_S(SO_q(\hat{\mathbb{Z}} \times \mathbb{R}))}.$$

The real part

We can now use the fact that $SO_q(A)$ has a canonical measure called the Tamagawa measure.

We can factor

$$SO_q(A) = SO_q(\mathbb{R}) \times \prod_{p \in \mathbb{P}}^{\text{restricted}} SO_q(\mathbb{Q}_{(p)}).$$

We know that $SO_q(\mathbb{R}) = SO(\mathbb{R})$ is a compact Lie group, and in particular a smooth manifold of some dimension n, and so we can find a canonical measure by taking a differential form of degree n. In this case, just take any form of top degree, which will also be translation invariant.

We can define $V_{\mathbb{R}}$, the vector space of such forms, which is an $\mathbb{R}$-vector space of dimension 1. It unfortunately doesn't have a canonical measure, so we'd have to again make a real number

choice here – however, we can use the fact that this is a linear algebraic group, due to it being a subgroup of GL, which satisfies polynomial conditions. Moreover, the conditions only require $\mathbb{Q}$ coefficients, so we can find a $V_{\mathbb{Q}} \subseteq V_{\mathbb{R}}$ which is the space of algebraic top forms and a $\mathbb{Q}$- vector space.

> Somehow this solves the scalar indeterminacy problem…?

The p–adic part

It's not the case that $SO_q(\mathbb{Q}_{(p)}$ are Lie groups, but there is a replacement notion of **p–adic analytic Lie groups**, which has an analog of differential forms, particularly in top degree and left-invariant, where any choice determines a Haar measure. We again look at the collection of such forms $V_{\mathbb{Q}_{(p)}}$, which is a 1-dimensional $\mathbb{Q}_{(p)}$-vector space. In a similar fashion, $O_q(\mathbb{Q}_{(p)}$ is an algebraic group, and we find that $V_{\mathbb{Q}} \subseteq V_{\mathbb{Q}_{(p)}}$.

So a choice of $\omega \in V_{\mathbb{Q}}$ determins measures on both factors, say $\mu_{\omega,\mathbb{R}}$ and $\mu_{\omega,\mathbb{Q}_{(p)}}$. So we can arrive at the Tamagawa measure:

$$\mu_{\mathrm{tam}} := \prod_{p \in \mathbb{P}} \mu_{\omega,\mathbb{Q}_{(p)}} \times \mu_{\omega,\mathbb{R}}.$$

Note that we need this product to converge – if we stick with the usual orthogonal group, it will not, but by choosing the special orthogonal group instead it will.

It also depended on a choice of $\omega \in V_{\mathbb{Q}}$, but we can show that this measure is independent of choice. If we let $\omega' = \lambda\omega$ for some scalar λ, we first note that multiplying a differential form by λ introduces a factor of $|\lambda|$, and so

$$\mu_{\omega',\mathbb{R}} = |\lambda|\mu_{\omega,\mathbb{R}}.$$

For the p-adic components, a similar story occurs but with the p-adic absolute value instead, which is zero for all but the $p = \lambda$ term in the product. For this remaining term, we have

$$\mu_{\omega',\mathbb{Q}_{(p)}} = |\lambda|_\lambda \mu_{\omega,\mathbb{Q}_{(p)}} = \frac{1}{\lambda}\mu_{\omega,\mathbb{Q}_{(p)}},$$

which exactly cancels the term coming from $\mu_{\omega,\mathbb{R}}$.

Since our mass formula didn't care about which Haar measure was chosen, we can use this one to write

$$\mathrm{Mass}(q) = 2^{-k}\frac{\mu_{\mathrm{Tam}}(SO_q(A)/SO_q(\mathbb{Q})}{\mu_{\mathrm{Tam}}(SO_q(\hat{\mathbb{Z}} \times \mathbb{R}))},$$

where we can now evaluate the numerator and denominator independently.

The latter can be evaluated explicitly, since there is a decomposition

$$SO_q(\hat{Z} \times \mathbb{R}) = SO_q(\mathbb{R}) \times \prod_{p\in\mathbb{P}} SO_q(\mathbb{Z}_{(p)})$$

and by the definition of the Tamagawa measure, we can write

$$\mu_{\mathrm{Tam}}(SO_q(\hat{Z} \times \mathbb{R})) = \mu_{\omega,\mathbb{R}}(SO_q(\mathbb{R})) \times \prod_{p\in\mathbb{P}} \mu_{\omega,\mathbb{Q}_{(p)}}(SO_q(\mathbb{Z}_{(p)})$$

for any compatible choice of form ω.

For the first term, the orthogonal group is some "twisted product of spheres", so terms involving their volumes will appear. The

other terms amount to solving counting problems at each prime p at taking their product, so you might expect something with an Euler product expansion (such as ζ) to appear here.

The numerator is just equal to 2! This holds not just in the unimodular case, but for any quadratic forms over $\mathbb{Z}$, as well as forms that aren't positive definite.

This 2 comes from the double cover

$$\mathrm{Spin}_q \twoheadrightarrow SO_q$$

and the fact that

$$\mu_{\mathrm{Tam}}\left(\frac{\mathrm{Spin}_q(A)}{\mathrm{Spin}_q(\mathbb{Q})}\right) = 1$$

Weil's Conjecture

Let G be a simply connected semisimple algebraic group over $\mathbb{Q}$. You can then take the adelic points of G, given by $G(A)$, and the conjecture states that

$$\mu_{\mathrm{Tam}}\left(\frac{G(A)}{G(\mathbb{Q})}\right) = 1$$

where $G(\mathbb{Q})$ is referred to as the Tamagawa number of G, τ_G, and so this conjecture also states that $\tau_G = 1$.

> This was proved by Langlands, Loi, Kottwitz.

We will now try to determine an analog in the case of function fields, i.e. finite extensions of $\mathbb{F}_p[t]$.