### Lecture 10: lattices, encore et encore!

Gabriel Dospinescu

CNRS, ENS Lyon

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

# Goal

 In this lecture we will explain a series of deep relations between unimodular lattices in euclidean spaces, modular forms and adelic groups. Absolutely beautiful references are the book of Serre "A Course in Arithmetic", and (much more advanced) the book of Chenevier-Lannes "Automorphic forms and even unimodular lattices".

# Unimodular lattices

A unimodular quadratic lattice of rank n is a free Z-module L of rank n together with a symmetric bilinear pairing L<sup>2</sup> → Z, (x, y) → x•y which is perfect, i.e. the induced map

 $L \to \operatorname{Hom}(L, \mathbb{Z})$ 

is bijective. In terms of matrices, if

$$A = (e_i \bullet e_j)_{1 \le i,j \le n}$$

is the Gram matrix associated to a basis  $e_1, ..., e_n$  of L, then perfectness is equivalent to det  $A \in \{-1, 1\}$ .

# Unimodular lattices

A unimodular quadratic lattice of rank n is a free Z-module L of rank n together with a symmetric bilinear pairing L<sup>2</sup> → Z, (x, y) → x•y which is perfect, i.e. the induced map

 $L \to \operatorname{Hom}(L, \mathbb{Z})$ 

is bijective. In terms of matrices, if

$$A = (e_i \bullet e_j)_{1 \le i,j \le n}$$

is the Gram matrix associated to a basis  $e_1, ..., e_n$  of L, then perfectness is equivalent to det  $A \in \{-1, 1\}$ .

(II) There is an obvious notion of isomorphism between quadratic lattices. In terms of matrices this means replacing A by <sup>T</sup>BAB for some  $B \in \mathbb{GL}_n(\mathbb{Z})$ .

## Nice lattices

(1) Let  $\mathcal{L}_n$  be the set of **nice** lattices, i.e. unimodular quadratic lattices (L, q) of rank n (with  $q(x) = x \cdot x$ ) such that

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

- q is positive definite
- *L* is even, i.e.  $q(L) \subset 2\mathbb{Z}$ .

### Nice lattices

- (1) Let  $\mathscr{L}_n$  be the set of **nice** lattices, i.e. unimodular quadratic lattices (L, q) of rank n (with  $q(x) = x \cdot x$ ) such that
  - q is positive definite
  - *L* is even, i.e.  $q(L) \subset 2\mathbb{Z}$ .

(II) If 8 | *n* then one easily checks that  $E_n \in \mathscr{L}_n$ , where

$$E_n = \{x \in \mathbb{Z}^n | 2 | x_1 + ... + x_n\} + \mathbb{Z}_{\bullet}(\frac{1}{2}, \frac{1}{2}, ..., \frac{1}{2})$$

with the standard inner product.  $\mathbb{Z}^n$  is never nice (sic!).

(1) Let  $L \in \mathscr{L}_n$  and let  $r_L(m)$  be the number of  $x \in L$  for which  $q(x) = x \cdot x = 2m$ , a finite number since q is positive definite.

▲□▶ ▲圖▶ ▲圖▶ ▲圖▶ 二直 - のへで

(1) Let  $L \in \mathscr{L}_n$  and let  $r_L(m)$  be the number of  $x \in L$  for which  $q(x) = x \cdot x = 2m$ , a finite number since q is positive definite.

(II) The theta function of L (with  $q = e^{2i\pi z}$ ,  $z \in \mathscr{H}$ )

$$\Theta_L(z) = \sum_{x \in L} q^{x \cdot x/2} = \sum_{m \ge 0} r_L(m) q^m$$

is a 1-periodic holomorphic function on  $\mathcal{H}$ , since  $r_L(m) = O(m^{n/2})$ .

(I) Here is a key result:

Theorem Suppose that  $\mathscr{L}_n \neq \emptyset$  and let  $L \in \mathscr{L}_n$ . Then 8 | n and  $\Theta_L \in M_{n/2}(\mathbb{SL}_2(\mathbb{Z}))$ .

First, we prove that

$$\Theta_L(-1/z) = (-iz)^{n/2}\Theta_L(z).$$

It suffices to check it for z = it with t > 0, i.e. we want

$$\sum_{x \in t^{-1/2}L} f(x) = t^{n/2} \sum_{x \in t^{1/2}L} f(x),$$

with  $f(x) = e^{-\pi x \cdot x}$ . A standard computation (reduce to dimension 1 via a ON-basis of  $L \otimes \mathbb{R}$ ) shows that  $\hat{f} = f$ , where

$$\hat{f}(y) = \int_{L\otimes\mathbb{R}} e^{-2i\pi x \cdot y} f(x) dx.$$

(I) The trace formula (i.e. Poisson summation) applied to the compact quotient  $(L \otimes \mathbb{R})/(t^{1/2}L)$  easily yields the result:  $t^{-1/2}L$  is dual to  $t^{1/2}L$  and the co-volume of  $t^{1/2}L$  is  $t^{n/2}$ .

- (1) The trace formula (i.e. Poisson summation) applied to the compact quotient  $(L \otimes \mathbb{R})/(t^{1/2}L)$  easily yields the result:  $t^{-1/2}L$  is dual to  $t^{1/2}L$  and the co-volume of  $t^{1/2}L$  is  $t^{n/2}$ .
- (II) To finish the proof of the theorem, it suffices to check that  $8 \mid n$ . Replacing L by  $L \oplus L$  or  $L^{\oplus 4}$  we may assume that  $4 \mid n$  and 8 does not divide n. Then by what we've just proved

$$\omega(z) = \Theta_L(z) dz^{n/4}$$

satisfies  $S^*(\omega) = -\omega$  and  $T^*(\omega) = \omega$  (where  $S : z \to -1/z$ and  $T : z \to z + 1$ ), thus  $(ST)^*\omega = -\omega$ , impossible since  $(ST)^3 = 1$  and  $\omega \neq 0$ .

(1) Looking at constant terms we get, with k = n/4

$$\Theta_L - E_k \in S_{n/2} := S_{n/2}(\mathbb{SL}_2(\mathbb{Z})).$$

Hecke's trivial bound and the q-expansion of  $E_k$  give

$$r_L(m) = \frac{4k}{B_k}\sigma_{2k-1}(m) + O(m^k), \ k = n/4,$$

where the Bernoulli numbers are defined by

$$\frac{x}{e^{x}-1} = 1 - \frac{x}{2} + \sum_{k \ge 1} (-1)^{k+1} B_k \frac{x^{2k}}{(2k)!}.$$

▲□▶ ▲圖▶ ▲圖▶ ▲圖▶ 二直 - のへで

(I) Looking at constant terms we get, with k = n/4

$$\Theta_L - E_k \in S_{n/2} := S_{n/2}(\mathbb{SL}_2(\mathbb{Z})).$$

Hecke's trivial bound and the q-expansion of  $E_k$  give

$$r_L(m) = \frac{4k}{B_k}\sigma_{2k-1}(m) + O(m^k), \ k = n/4,$$

where the Bernoulli numbers are defined by

$$\frac{x}{e^{x}-1} = 1 - \frac{x}{2} + \sum_{k \ge 1} (-1)^{k+1} B_k \frac{x^{2k}}{(2k)!}.$$

(II) For n = 8 we have  $S_4 = 0$  so  $\Theta_L = E_2$  and  $r_{\Gamma}(m) = 240\sigma_3(m)$ . Mordell proved that any such L is isomorphic to  $E_8$ . For n = 16 we get  $\Theta_L = E_4$  and  $r_L(m) = 480\sigma_7(m)$ .

(1) Witt proved that there are exactly two such L (up to isomorphism), namely  $E_8 \oplus E_8$  and  $E_{16}$ . These give rise to non-isomorphic iso-spectral tori (Milnor).

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

(1) Witt proved that there are exactly two such L (up to isomorphism), namely  $E_8 \oplus E_8$  and  $E_{16}$ . These give rise to non-isomorphic iso-spectral tori (Milnor).

(II) For 
$$n = 24$$
 letting  

$$\Delta = q \prod_{n} (1-q^{n})^{24} = \sum \tau(n)q^{n}, \quad E_{6} = 1 + \frac{65520}{691} \sum \sigma_{11}(n)q^{n},$$

$$M_{12}(\mathbb{SL}_{2}(\mathbb{Z})) = \mathbb{C}E_{6} \oplus \mathbb{C}\Delta, \text{ thus } \exists c_{L} \in \mathbb{Q} \text{ such that}$$

$$r_{L}(m) = \frac{65520}{691}\sigma_{11}(m) + c_{L}\tau(m).$$

Conway and Leech proved that there is a unique such L with  $r_L(1) = 0$ , the famous Leech lattice. Hence

 $r_{Leech}(m) = \frac{65520}{691}(\sigma_{11}(m) - \tau(m)), \quad \tau(m) \equiv \sigma_{11}(m) \pmod{691},$ 

a famous Ramanujan congruence.

・ロト・(型ト・(ヨト・(ヨト)) ヨージへ(?)

## Counting nice lattices

(I) Let

$$X_n = \mathscr{L}_n / \simeq .$$

We've just seen that  $X_n \neq \emptyset$  iff 8 | *n*, and  $|X_8| = 1$ ,  $|X_{16}| = 2$ . We'll see that  $X_n$  is finite. The next result is **much** deeper:

Theorem (Niemeier, King) We have  $|X_{24}| = 24$  and  $|X_{32}| > 10^9$ .

 $|X_n|$  has a very beautiful group-theoretic and adelic description, which requires some preliminary discussion.

### Brief recollections on adèles

Recall that the ring of adèles A is locally compact and Q is a co-compact lattice in it. An element of A is a family (a<sub>v</sub>)<sub>v</sub> indexed by places v of Q (i.e. primes or ∞) with a<sub>v</sub> ∈ Q<sub>v</sub> and a<sub>v</sub> ∈ Z<sub>v</sub> for almost all v. We have

$$\mathbb{A} = \mathbb{R} \times \mathbb{A}_f, \, \mathbb{A}_f = \mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}, \, \hat{\mathbb{Z}} = \prod_{p} \mathbb{Z}_{p}.$$

#### Brief recollections on adèles

Recall that the ring of adèles A is locally compact and Q is a co-compact lattice in it. An element of A is a family (a<sub>v</sub>)<sub>v</sub> indexed by places v of Q (i.e. primes or ∞) with a<sub>v</sub> ∈ Q<sub>v</sub> and a<sub>v</sub> ∈ Z<sub>v</sub> for almost all v. We have

$$\mathbb{A} = \mathbb{R} \times \mathbb{A}_f, \ \mathbb{A}_f = \mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}, \ \hat{\mathbb{Z}} = \prod_{p} \mathbb{Z}_{p}.$$

(II) For any Q-group G with a Z-model G, the topological group G(A) consists of (g<sub>v</sub>)<sub>v</sub> with g<sub>v</sub> ∈ G(Q<sub>v</sub>) and g<sub>v</sub> ∈ G(Z<sub>v</sub>) for almost all v. The group G(A) contains G(Q) as a discrete subgroup. If G is semi-simple over Q, then G(Q) is a lattice in G(A) (co-compact if and only if G is anisotropic over Q), by the Borel and Borel-Harish-Chandra theorem.

## Class numbers of algebraic groups

 Let G ⊂ GL<sub>n</sub>(C) be a connected Q-group. The next theorem is quite deep: applied to G = (F ⊗<sub>Q</sub> C)<sup>×</sup>, with F a number field, this gives the finiteness of the class number of F.

Theorem (Borel) The set  $G(\mathbb{Q}) \setminus G(\mathbb{A}_f) / G(\hat{\mathbb{Z}})$  is finite.

The class number of G is

$$\operatorname{cl}(G) = |G(\mathbb{Q}) \setminus G(\mathbb{A}_f) / G(\hat{\mathbb{Z}})|.$$

Be careful that it depends on the choice of the embedding  $G \subset \mathbb{GL}_n(\mathbb{C})$  since  $G(\hat{\mathbb{Z}})$  depends on that.

## Class number of $\mathbb{GL}_n$ and $\mathbb{SL}_n$

(I) As an amuse-bouche, let's prove in two ways the following:

Theorem We have  $cl(\mathbb{GL}_n) = 1$  and  $cl(\mathbb{SL}_n) = 1$ .

It suffices to check that cl(G) = 1, where  $G = \mathbb{SL}_n$ , and this would follow from the density of  $G(\mathbb{Q})$  in  $G(\mathbb{A}_f)$ : since  $G(\hat{\mathbb{Z}})$  is open in  $G(\mathbb{A}_f)$ , any  $G(\hat{\mathbb{Z}})$ -orbit will intersect  $G(\mathbb{Q})$  and thus  $G(\mathbb{A}_f) = G(\mathbb{Q})G(\hat{\mathbb{Z}})$ .

#### Class number of $\mathbb{GL}_n$ and $\mathbb{SL}_n$

(I) As an amuse-bouche, let's prove in two ways the following:

Theorem We have  $cl(\mathbb{GL}_n) = 1$  and  $cl(\mathbb{SL}_n) = 1$ .

It suffices to check that cl(G) = 1, where  $G = \mathbb{SL}_n$ , and this would follow from the density of  $G(\mathbb{Q})$  in  $G(\mathbb{A}_f)$ : since  $G(\hat{\mathbb{Z}})$  is open in  $G(\mathbb{A}_f)$ , any  $G(\hat{\mathbb{Z}})$ -orbit will intersect  $G(\mathbb{Q})$  and thus  $G(\mathbb{A}_f) = G(\mathbb{Q})G(\hat{\mathbb{Z}})$ .

(II) Let *H* be the closure of  $G(\mathbb{Q})$  in  $G(\mathbb{A}_f)$ . Then *H* contains  $G(\mathbb{Q}_v)$  for any v: any  $g \in G(\mathbb{Q}_v)$  is a product of elementary matrices, and  $\mathbb{Q}$  is dense in  $\mathbb{Q}_v$ . Also *H* is closed in  $G(\mathbb{A}_f)$ , thus it contains  $\prod_{v \in S} G(\mathbb{Q}_v) \times \prod_{v \notin S} G(\mathbb{Z}_v)$  for any finite set *S*. But then *H* contains the union of these over all *S*, which is  $G(\mathbb{A}_f)$ .

The second proof is based on the next key result. Let V be a finite dimensional Q-vector space and let V<sub>p</sub> = V ⊗<sub>Q</sub> Q<sub>p</sub>. Let L(V) be the set of lattices in V. Define L(V<sub>p</sub>) similarly. There is a natural map

$$\mathscr{L}(V) \to \prod_{p} \mathscr{L}(V_{p}), \ L \to (L_{p} := L \otimes_{\mathbb{Z}} \mathbb{Z}_{p})_{p}.$$

Theorem (Eichler) Fix a lattice  $L_0 \subset V$ . The above map induces a bijection between

$$\mathscr{L}(V)\simeq\prod_p'\mathscr{L}(V_p):=$$

 $\{(L_p)_p \in \prod_p \mathscr{L}(V_p) | L_p = L_0 \otimes \mathbb{Z}_p \text{ for almost all } p\}.$ 

 Pick a basis of L<sub>0</sub> and identify it with Z<sup>n</sup>, and V with Q<sup>n</sup>. If L ∈ ℒ(V), there is an integer N ≥ 1 such that <sup>1</sup>/<sub>N</sub>Z<sup>n</sup> ⊂ L ⊂ NZ<sup>n</sup>. Thus L<sub>p</sub> = Z<sup>n</sup><sub>p</sub> inside V<sub>p</sub> = Q<sup>n</sup><sub>p</sub> for all p prime to N. Thus the map factors through ∏'<sub>p</sub>ℒ(V<sub>p</sub>).

- Pick a basis of L<sub>0</sub> and identify it with Z<sup>n</sup>, and V with Q<sup>n</sup>. If L ∈ ℒ(V), there is an integer N ≥ 1 such that <sup>1</sup>/<sub>N</sub>Z<sup>n</sup> ⊂ L ⊂ NZ<sup>n</sup>. Thus L<sub>p</sub> = Z<sup>n</sup><sub>p</sub> inside V<sub>p</sub> = Q<sup>n</sup><sub>p</sub> for all p prime to N. Thus the map factors through ∏'<sub>p</sub>ℒ(V<sub>p</sub>).
- (II) An easy exercise shows that for any lattice *L* we have  $L = \bigcap_p L_p$  (with  $L_p = L \otimes \mathbb{Z}_p$ ) inside  $V \otimes \mathbb{A}_f$ , giving injectivity. Using this recipe one also obtains an inverse of the map  $L \to (L_p)_p$ , namely  $(L_p)_p \to \bigcap_p (L_p \cap V)$ .

(1) Take  $V = \mathbb{Q}^n$  and  $L_0 = \mathbb{Z}^n$ . Then  $\mathbb{GL}_n(\mathbb{A}_f) \simeq \prod_p' \mathbb{GL}(V_p)$ acts transitively on  $\prod_p' \mathscr{L}(V_p)$ , by  $(g_p)_{p\bullet}(L_p)_p = (g_p(L_p))_p$ , the stabiliser of  $(\mathbb{Z}_p^n)_p$  being  $\mathbb{GL}_n(\hat{\mathbb{Z}})$ . Thus we obtain an identification

$$\mathbb{GL}_n(\mathbb{A}_f)/\mathbb{GL}_n(\hat{\mathbb{Z}}) \simeq \mathscr{L}(V) \simeq \mathbb{GL}_n(\mathbb{Q})/\mathbb{GL}_n(\mathbb{Z}),$$

giving  $\mathbb{GL}_n(\mathbb{A}_f) = \mathbb{GL}_n(\mathbb{Q})\mathbb{GL}_n(\hat{\mathbb{Z}})$  and  $\mathrm{cl}(\mathbb{GL}_n) = 1$ .

Fix n multiple of 8 and L<sub>0</sub> ∈ L<sub>n</sub>. Let G = O(L<sub>0</sub>) be the orthogonal group of L<sub>0</sub>, a group defined over Z, with G(A) the automorphism group of the quadratic A-module L<sub>0</sub> ⊗ A for any A.

Theorem There is a natural bijection

$$X_n \to G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / G(\hat{\mathbb{Z}}),$$

thus  $|X_n| = \operatorname{cl}(G)$ .

In particular  $X_n$  is finite by Borel's theorem (we will see a different argument later on).

 A key input in the proof of the previous theorem is the following nontrivial result, using the classification of quadratic forms over Z<sub>p</sub>:

Theorem Any two lattices in  $\mathscr{L}_n$  become isomorphic over  $\mathbb{Z}_p$  for any prime p and thus (by the Hasse-Minkowski theorem) also over  $\mathbb{Q}$ .

 A key input in the proof of the previous theorem is the following nontrivial result, using the classification of quadratic forms over Z<sub>p</sub>:

**Theorem** Any two lattices in  $\mathscr{L}_n$  become isomorphic over  $\mathbb{Z}_p$  for any prime p and thus (by the Hasse-Minkowski theorem) also over  $\mathbb{Q}$ .

(II) Now pick  $L \in \mathscr{L}_n$  and choose isomorphisms  $\gamma : L \otimes \mathbb{Q} \to L_0 \otimes \mathbb{Q}$  and  $\gamma_v : L \otimes \mathbb{Z}_v \to L_0 \otimes \mathbb{Z}_v$ . Then  $\gamma \circ \gamma_v^{-1} \in \operatorname{Aut}(L_0 \otimes \mathbb{Q}_v) = G(\mathbb{Q}_v)$  for all v, and they belong to  $G(\mathbb{Z}_v)$  for almost all v.

We obtain an element g = (γ ∘ γ<sub>ν</sub><sup>-1</sup>)<sub>ν</sub> ∈ G(A). Changing γ multiplies g on the left by an element of G(Q), and changing γ<sub>ν</sub> multiplies g on the right by an element of G(Ẑ<sub>ν</sub>) (resp. G(R)), thus the class of g in

$$G(\mathbb{Q}) \backslash G(\mathbb{A}) / G(\hat{\mathbb{Z}} \times \mathbb{R}) \simeq G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / G(\hat{\mathbb{Z}})$$

is well-defined, and only depends on the isomorphism class of  ${\it L},$  giving a map

$$X_n \to G(\mathbb{Q}) \setminus G(\mathbb{A}_f) / G(\hat{\mathbb{Z}}).$$

We obtain an element g = (γ ∘ γ<sub>ν</sub><sup>-1</sup>)<sub>ν</sub> ∈ G(A). Changing γ multiplies g on the left by an element of G(Q), and changing γ<sub>ν</sub> multiplies g on the right by an element of G(Ẑ<sub>ν</sub>) (resp. G(R)), thus the class of g in

$$G(\mathbb{Q}) \setminus G(\mathbb{A}) / G(\hat{\mathbb{Z}} \times \mathbb{R}) \simeq G(\mathbb{Q}) \setminus G(\mathbb{A}_f) / G(\hat{\mathbb{Z}})$$

is well-defined, and only depends on the isomorphism class of L, giving a map

$$X_n \to G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / G(\hat{\mathbb{Z}}).$$

(II) In the other direction, for any g ∈ G(A<sub>f</sub>) we can use the action of G(A<sub>f</sub>) ⊂ GL(L<sub>0</sub> ⊗ A<sub>f</sub>) on lattices in L<sub>0</sub> ⊗ Q to get a lattice L' = g(L<sub>0</sub>) ⊂ L<sub>0</sub> ⊗ Q. One easily checks that L' ∈ L<sub>n</sub> and its isomorphism class depends only on the class of g in G(Q)\G(A<sub>f</sub>)/G(Ẑ). An easy exercise shows that these constructions are inverse to each other.

(1) Here is one of the most amazing formulae in mathematics. It gives the cardinality of  $X_n$ , "if we count correctly". Let  $v(S^{d-1}) = 2\pi^{d/2}/\Gamma(d/2)$  (volume of the sphere).

Theorem (Smith-Minkowski-Siegel) For any  $n \in 8\mathbb{Z}_{>0}$ 

$$\sum_{L \in X_n} \frac{1}{|\operatorname{Aut}(L)|} = 2\zeta(n/2) \frac{\zeta(2)\zeta(4)...\zeta(n-2)}{v(S^0)v(S^1)...v(S^{n-1})}.$$

The theorem implies (exercise, using that  $|\operatorname{Aut}(L)| \ge 2$ ) the existence of c > 0 such that for 8 | n we have  $|X_n| > (cn)^{n^2}$ . One can also write (exercise!)

$$\sum_{L \in X_n} \frac{1}{|\operatorname{Aut}(L)|} = 2^{-n} \frac{B_{n/4}}{n/4} \prod_{j=1}^{n/2-1} \frac{B_j}{j}.$$

(I) This formula is deeply related to adelic harmonic analysis! Pick a decomposition

$$G(\mathbb{A}_f) = \prod_{i=1}^h G(\mathbb{Q})g_iG(\hat{\mathbb{Z}})$$

and let  $L_i \in X_n$  be the lattice corresponding to the class of  $g_i$ . We can compute the (finite) automorphism group of  $L_i$  by looking at those  $g \in G(\mathbb{Q}) = \operatorname{Aut}(L_0 \otimes \mathbb{Q})$  which stabilise  $L_i \otimes \mathbb{Z}_p$  for all p. We get

$$\operatorname{Aut}(L_i) = g_i K g_i^{-1} \cap G(\mathbb{Q}), \ K := G(\mathbb{R}) \times G(\hat{\mathbb{Z}}).$$

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

(I) This formula is deeply related to adelic harmonic analysis! Pick a decomposition

$$G(\mathbb{A}_f) = \prod_{i=1}^h G(\mathbb{Q})g_iG(\hat{\mathbb{Z}})$$

and let  $L_i \in X_n$  be the lattice corresponding to the class of  $g_i$ . We can compute the (finite) automorphism group of  $L_i$  by looking at those  $g \in G(\mathbb{Q}) = \operatorname{Aut}(L_0 \otimes \mathbb{Q})$  which stabilise  $L_i \otimes \mathbb{Z}_p$  for all p. We get

$$\operatorname{Aut}(L_i) = g_i K g_i^{-1} \cap G(\mathbb{Q}), \ K := G(\mathbb{R}) \times G(\hat{\mathbb{Z}}).$$

(II) We have a decomposition (send  $gAut(L_i)$  to the class of  $(g, g_i)$  for  $g \in G(\mathbb{R})$ )

$$G(\mathbb{Q})\backslash G(\mathbb{A})/G(\hat{\mathbb{Z}})\simeq \prod_{i=1}^{h} \operatorname{Aut}(L_{i})\backslash G(\mathbb{R}).$$

(I) Picking compatible Haar measures  $\mu$  on  $G(\mathbb{A}_f)$ ,  $G(\hat{\mathbb{Z}})$  and  $G(\mathbb{R})$  we have (note that  $G(\mathbb{R})$  is compact)

$$\frac{\mu(G(\mathbb{Q})\backslash G(\mathbb{A}))}{\mu(G(\hat{\mathbb{Z}}))} = \mu(G(\mathbb{R}))\sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(L_i)|},$$

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

thus

Theorem For any *n* multiple of 8 we have  

$$\sum_{L \in X_n} \frac{1}{|\operatorname{Aut}(L)|} = \frac{\mu(G(\mathbb{Q}) \setminus G(\mathbb{A}))}{\mu(G(\mathbb{R}) \times G(\hat{\mathbb{Z}}))}$$

for any Haar measure  $\mu$  on  $G(\mathbb{A})$ .

(I) Picking compatible Haar measures  $\mu$  on  $G(\mathbb{A}_f)$ ,  $G(\hat{\mathbb{Z}})$  and  $G(\mathbb{R})$  we have (note that  $G(\mathbb{R})$  is compact)

$$\frac{\mu(G(\mathbb{Q})\backslash G(\mathbb{A}))}{\mu(G(\hat{\mathbb{Z}}))} = \mu(G(\mathbb{R}))\sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(L_i)|},$$

thus

Theorem For any *n* multiple of 8 we have  $\sum_{L \in X_n} \frac{1}{|\operatorname{Aut}(L)|} = \frac{\mu(G(\mathbb{Q}) \setminus G(\mathbb{A}))}{\mu(G(\mathbb{R}) \times G(\hat{\mathbb{Z}}))}$ 

for any Haar measure  $\mu$  on  $G(\mathbb{A})$ .

(II) We next explain, following Tamagawa and Weil, how to construct canonical Haar measures on semisimple Q-groups (one can extend this to all Q-groups, with extra work).

## Measures and differential forms

Let v be a place of Q and let X be a smooth variety of dimension n over Q<sub>v</sub>. The smoothness of X implies (via the implicit function theorem) that X(Q<sub>v</sub>) has a natural structure of manifold, algebraic local coordinates at points of X(Q<sub>v</sub>) giving rise to analytic charts around that point. Any algebraic differential n-form ω on X (defined over Q<sub>v</sub>) gives rise to a measure on X(Q<sub>v</sub>), as follows.

#### Measures and differential forms

- Let v be a place of Q and let X be a smooth variety of dimension n over Q<sub>v</sub>. The smoothness of X implies (via the implicit function theorem) that X(Q<sub>v</sub>) has a natural structure of manifold, algebraic local coordinates at points of X(Q<sub>v</sub>) giving rise to analytic charts around that point. Any algebraic differential n-form ω on X (defined over Q<sub>v</sub>) gives rise to a measure on X(Q<sub>v</sub>), as follows.
- (II) Pick x ∈ X(Q<sub>v</sub>) and local coordinates t<sub>1</sub>,..., t<sub>n</sub> near x (i.e. t<sub>1</sub>,..., t<sub>n</sub> generate the maximal ideal of the local ring at x). The t<sub>i</sub> define a chart around x and we can express in this chart ω = g(t<sub>1</sub>,..., t<sub>n</sub>)dt<sub>1</sub> ∧ ... ∧ dt<sub>n</sub> for some power series g in t<sub>1</sub>,..., t<sub>n</sub>, convergent on some ball around 0.

#### Measures and differential forms

The measure |g(t<sub>1</sub>,...,t<sub>n</sub>)|<sub>v</sub>dt<sub>1</sub>...dt<sub>n</sub> (where dt<sub>1</sub>...dt<sub>n</sub> is the usual Haar measure on Q<sup>n</sup><sub>v</sub>, Lebesgue measure if v = ∞ and giving Z<sup>n</sup><sub>v</sub> mass 1 if v < ∞) is independent of the choice of local coordinates (exchange coordinates one at a time and use Fubini to reduce to the case n = 1, which is elementary) and compatible with restriction to smaller open subsets around x. These measures glue to a measure |ω| on X(Q<sub>v</sub>).

Theorem (Weil) If X has a smooth model  $\mathscr{X}$  over  $\mathbb{Z}_p$  and if  $\omega$  is the restriction of a nowhere vanishing *n*-form on  $\mathscr{X}$ , then

$$\int_{\mathscr{X}(\mathbb{Z}_p)} |\omega| = \frac{|\mathscr{X}(\mathbb{F}_p)|}{p^{\dim X}}.$$

### Measures and differential forms

(I) There is a natural surjective (by smoothness) reduction map

red : 
$$\mathscr{X}(\mathbb{Z}_p) \to \mathscr{X}(\mathbb{F}_p)$$

and one checks (using a suitable form of Hensel's lemma and local inversion theorem) that local coordinates around  $a \in \mathscr{X}(\mathbb{Z}_p)$  give rise to an analytic isomorphism

$$(p\mathbb{Z}_p)^{\dim X} \simeq \operatorname{red}^{-1}(\operatorname{red}(a)).$$

With respect to these local parameters  $\omega = f(t_1, ..., t_n)dt_1 \wedge ... \wedge dt_n$  and  $|f(t_1, ..., t_n)| = 1$  (since  $\omega$  is nowhere vanishing mod p), thus

$$\int_{\mathrm{red}^{-1}(\mathrm{red}(a))} |\omega| = \int_{(p\mathbb{Z}_p)^{\dim X}} dt_1 \dots dt_n = p^{-\dim X}.$$

Let now G be a semisimple Q-group of dimension n. The space Ω<sup>inv</sup><sub>G</sub> of left-invariant nowhere-vanishing n-forms on G (defined over Q) is one-dimensional over Q. Any nonzero ω ∈ Ω<sup>inv</sup><sub>G</sub> gives rise to measures |ω<sub>ν</sub>| on G(Q<sub>ν</sub>) for any place v of Q, by the above recipe applied to G as a smooth Q<sub>ν</sub>-variety. We want to define a measure on G(A) by

$$|\omega| := \otimes_{\mathbf{v}} |\omega_{\mathbf{v}}|,$$

but one needs serious care in implementing this.

Let now G be a semisimple Q-group of dimension n. The space Ω<sup>inv</sup><sub>G</sub> of left-invariant nowhere-vanishing n-forms on G (defined over Q) is one-dimensional over Q. Any nonzero ω ∈ Ω<sup>inv</sup><sub>G</sub> gives rise to measures |ω<sub>v</sub>| on G(Q<sub>v</sub>) for any place v of Q, by the above recipe applied to G as a smooth Q<sub>v</sub>-variety. We want to define a measure on G(A) by

$$|\omega| := \otimes_{\mathbf{v}} |\omega_{\mathbf{v}}|,$$

but one needs serious care in implementing this.

(II) For some  $N \ge 1$  G has a smooth model  $\mathscr{G}$  over  $\mathbb{Z}[1/N]$ , and  $\omega$  is induced by a nowhere-vanishing *n*-form on  $\mathscr{G}$ . By Weil's theorem we have

$$\prod_{\gcd(p,N)=1} |\omega_p|(\mathscr{G}(\mathbb{Z}_p)) = \prod_{\gcd(p,N)=1} \frac{|\mathscr{G}(\mathbb{F}_p)|}{p^n}.$$

 A deep theorem of Steinberg (crucially using that G is semisimple!) ensures that

$$\prod_{\gcd(\rho,N)=1}\frac{|\mathscr{G}(\mathbb{F}_{\rho})|}{\rho^n}<\infty.$$

For instance  $G = \mathbb{SL}_n$  we obtain

$$\prod_{p} \frac{\mathbb{SL}_{n}(\mathbb{F}_{p})}{p^{n^{2}-1}} = \prod_{p} (1-p^{-n})(1-p^{1-n})...(1-p^{-2})$$
$$= \zeta(2)^{-1}\zeta(3)^{-1}...\zeta(n)^{-1}.$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

 A deep theorem of Steinberg (crucially using that G is semisimple!) ensures that

$$\prod_{\gcd(\rho,N)=1}\frac{|\mathscr{G}(\mathbb{F}_{\rho})|}{\rho^n}<\infty.$$

For instance  $G = \mathbb{SL}_n$  we obtain

$$\prod_{p} \frac{\mathbb{SL}_{n}(\mathbb{F}_{p})}{p^{n^{2}-1}} = \prod_{p} (1-p^{-n})(1-p^{1-n})...(1-p^{-2})$$
$$= \zeta(2)^{-1}\zeta(3)^{-1}...\zeta(n)^{-1}.$$

(II) We can now define a measure on  $G(\mathbb{A})$  as follows: for any M multiple of N pick the measure on  $\prod_{\gcd(p,M)=1} \mathscr{G}(\mathbb{Z}_p)$  with total mass  $\prod_{\gcd(p,M)=1} |\omega_p|(\mathscr{G}(\mathbb{Z}_p))$  and use the product measure on  $\prod_{p|M} G(\mathbb{Q}_p) \times G(\mathbb{R})$ .

This gives us measures on
 G(ℝ) × Π<sub>p|M</sub> G(ℚ<sub>p</sub>) × Π<sub>gcd(p,M)=1</sub> G(ℤ<sub>p</sub>), which are
 compatible when increasing M, thus we get a measure on
 their union, which is G(A). The result, the Tamagawa
 measure μ<sub>G</sub><sup>Tam</sup>, is independent of any of the choices made,
 in particular of the choice of ω (since |λω<sub>ν</sub>| = |λ|<sub>ν</sub>|ω<sub>ν</sub>| and
 Π<sub>ν</sub> |λ|<sub>ν</sub> = 1 for λ ∈ ℚ\*).

- This gives us measures on
   G(ℝ) × Π<sub>p|M</sub> G(ℚ<sub>p</sub>) × Π<sub>gcd(p,M)=1</sub> G(ℤ<sub>p</sub>), which are
   compatible when increasing M, thus we get a measure on
   their union, which is G(𝔅). The result, the Tamagawa
   measure μ<sub>G</sub><sup>Tam</sup>, is independent of any of the choices made,
   in particular of the choice of ω (since |λω<sub>ν</sub>| = |λ|<sub>ν</sub>|ω<sub>ν</sub>| and
   Π<sub>ν</sub> |λ|<sub>ν</sub> = 1 for λ ∈ ℚ\*).
- (II) What really matters in practice is that for any continuous integrable functions  $f_v$  on  $G(\mathbb{Q}_v)$  with  $f_v = 1_{\mathscr{G}(\mathbb{Z}_v)}$  (for some model  $\mathscr{G}$  over some  $\mathbb{Z}[1/N]$ ) for almost all v, setting  $f((g_v)_v) = \prod_v f_v(g_v)$  gives a continuous integrable function such that

$$\int_{\mathcal{G}(\mathbb{A})} f(g) \mu_{\mathcal{G}}^{\operatorname{Tam}}(g) = \prod_{\nu} \int_{\mathcal{G}(\mathbb{Q}_{\nu})} f_{\nu}(g_{\nu}) |\omega_{\nu}|(g_{\nu}).$$

Since G is semi-simple, G has no algebraic characters (it is perfect!). Thus the (algebraic) action (right translation) of G on Ω<sup>inv</sup>(G) must be trivial and all such forms are left and right invariant. Thus μ<sup>Tam</sup> is left and right invariant measure on G(A<sub>f</sub>), which is thus unimodular (and so are all G(Q<sub>ν</sub>)).

- Since G is semi-simple, G has no algebraic characters (it is perfect!). Thus the (algebraic) action (right translation) of G on Ω<sup>inv</sup>(G) must be trivial and all such forms are left and right invariant. Thus μ<sup>Tam</sup> is left and right invariant measure on G(A<sub>f</sub>), which is thus unimodular (and so are all G(Q<sub>ν</sub>)).
- (II) Since G is semi-simple, by the Borel-Harish-Chandra theorem we know that

$$\tau(G) := \int_{G(\mathbb{Q}) \setminus G(\mathbb{A})} \mu_G^{\mathsf{Tam}}(g)$$

is a real number (i.e.  $G(\mathbb{Q})$  is a lattice in  $G(\mathbb{A})$ ) called the **Tamagawa number of** G.

 The proof of the next theorem occupies a big chunk of Weil's book Adèles and algebraic groups:

Theorem (Tamagawa-Weil) We have  $\tau(\mathbb{SL}_n) = 1$ ,  $\tau(SO(q)) = 2$  for any non-degenerate quadratic form q over  $\mathbb{Q}$  and  $\tau(SL_1(D)) = 1$  for any division algebra D over  $\mathbb{Q}$ .

The equality  $\tau(SO(q)) = 2$  is equivalent to the mass formula of Smith-Minkowski-Siegel when q is attached to an element of  $\mathcal{L}_n$ . For this one needs to compute the volume of  $SO(q)(\hat{\mathbb{Z}} \times \mathbb{R})$ , which reduces to computing  $|SO(q)(\mathbb{F}_p)|$ and the volume of  $SO(n)(\mathbb{R})$  (easily expressed inductively in terms of volumes of spheres).

Kottwitz proved (using deep work of Langlands and Arthur and many others) Weil's conjecture:  $\tau(G) = 1$  for any connected, simply connected semi-simple group G over  $\mathbb{Q}$ .

・ロト・日本・モート モー うへぐ

(1) Let  $G = \mathbb{GL}_n(\mathbb{C})$ , K = O(n), A the subgroup of diagonal matrices with positive entries, N the group of upper triangular unipotent matrices in  $G(\mathbb{R})$ .

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

- Let G = GL<sub>n</sub>(C), K = O(n), A the subgroup of diagonal matrices with positive entries, N the group of upper triangular unipotent matrices in G(ℝ).
- (II) The Iwasawa decomposition (an easy exercise) says that multiplication gives a homeomorphism (even diffeo)

 $K \times A \times N \rightarrow G(\mathbb{R}).$ 

(III) For t > 0 let

 $A_t := \{ \text{diag}(a_1, ..., a_n) \in A | \max(a_1/a_2, a_2/a_3, ...) \le t \}$ 

and for u > 0 let  $N_u$  be the subset of matrices in N whose off-diagonal entries belong to [-u, u]

(I) Sets of the form

$$\Sigma_{t,u} = KA_t N_u$$

are called **Siegel sets** in  $G(\mathbb{R})$ .

Theorem (Hermite, Minkowski) We have

$$G(\mathbb{R}) = \Sigma_{2/\sqrt{3}, 1/2} G(\mathbb{Z}).$$

Using this, it is a simple (but excellent!) exercise to deduce the following basic result (already implicitly used...):

Theorem The set  $X_n$  is finite for all n.

Write G<sub>n</sub> = GL<sub>n</sub>(ℝ), Γ<sub>n</sub> = GL<sub>n</sub>(ℤ) and Σ<sub>n</sub> = Σ<sub>2/√3,1/2</sub>. Let ||•|| be the euclidean norm with respect to the canonical basis e<sub>1</sub>, ..., e<sub>n</sub> of ℝ<sup>n</sup>. We will prove by induction on n that min<sub>x∈gΓn</sub> ||xe<sub>1</sub>|| is reached in a point of Σ<sub>n</sub> for any g ∈ G<sub>n</sub> (the min is reached since gΓ<sub>n</sub>(e<sub>1</sub>) = g(ℤ<sup>n</sup>) is discrete), so that gΓ<sub>n</sub> intersects Σ<sub>n</sub>.

- Write G<sub>n</sub> = GL<sub>n</sub>(ℝ), Γ<sub>n</sub> = GL<sub>n</sub>(ℤ) and Σ<sub>n</sub> = Σ<sub>2/√3,1/2</sub>. Let ||•|| be the euclidean norm with respect to the canonical basis e<sub>1</sub>, ..., e<sub>n</sub> of ℝ<sup>n</sup>. We will prove by induction on n that min<sub>x∈gΓn</sub> ||xe<sub>1</sub>|| is reached in a point of Σ<sub>n</sub> for any g ∈ G<sub>n</sub> (the min is reached since gΓ<sub>n</sub>(e<sub>1</sub>) = g(ℤ<sup>n</sup>) is discrete), so that gΓ<sub>n</sub> intersects Σ<sub>n</sub>.
- (II) Say the claim is proved for n-1 and let g = kan such that  $||ge_1|| = \min_{x \in g\Gamma_n} ||xe_1||$ . First I claim that there is  $\tilde{c} \in \Gamma_n$  such that  $\tilde{c}e_1 = e_1$  and the Iwasawa decomposition of  $g\tilde{c}$  is

$$g\tilde{c} = \tilde{k} \begin{pmatrix} a_1 & 0 \\ 0 & a'' \end{pmatrix} \tilde{n}, \ \tilde{n} \in N_{1/2}$$

$$a'' = \operatorname{diag}(a''_1, ..., a''_{n-1}), \ a''_i / a''_{i+1} \le 2/\sqrt{3}.$$

◆□▶ ◆□▶ ◆ □▶ ◆ □▶ ○ □ ○ ○ ○

(1) Indeed, writing  $a = \begin{pmatrix} a_1 & 0 \\ 0 & a' \end{pmatrix}$ ,  $n = \begin{pmatrix} 1 & * \\ 0 & n' \end{pmatrix}$ , by induction we can find  $c' \in \Gamma_{n-1}$  such that  $a'n'c' = k''a''n'' \in \Sigma_{n-1}$ . A direct computation exhibits an identity of the form

$$g\begin{pmatrix}1&0\\0&c'\end{pmatrix} = \tilde{k}\begin{pmatrix}a_1&0\\0&a''\end{pmatrix}\begin{pmatrix}1&**\\0&n''\end{pmatrix}$$

But an easy induction shows that  $N = N_{1/2}(\Gamma_n \cap N)$ , so we can multiply  $\begin{pmatrix} 1 & **\\ 0 & n'' \end{pmatrix}$  by an element of  $\Gamma_n \cap N$  to make it land in  $N_{1/2}$ .

(1) Indeed, writing 
$$a = \begin{pmatrix} a_1 & 0 \\ 0 & a' \end{pmatrix}$$
,  $n = \begin{pmatrix} 1 & * \\ 0 & n' \end{pmatrix}$ , by induction we can find  $c' \in \Gamma_{n-1}$  such that  $a'n'c' = k''a''n'' \in \Sigma_{n-1}$ . A direct computation exhibits an identity of the form

$$g\begin{pmatrix}1&0\\0&c'\end{pmatrix} = \tilde{k}\begin{pmatrix}a_1&0\\0&a''\end{pmatrix}\begin{pmatrix}1&**\\0&n''\end{pmatrix}$$

But an easy induction shows that  $N = N_{1/2}(\Gamma_n \cap N)$ , so we can multiply  $\begin{pmatrix} 1 & **\\ 0 & n'' \end{pmatrix}$  by an element of  $\Gamma_n \cap N$  to make it land in  $N_{1/2}$ .

(II) Back to the main business: since  $\tilde{c}e_1 = e_1$ , we have  $||g\tilde{c}e_1|| = \min_{x \in g\tilde{c}\Gamma_n} ||xe_1||$ , so we win by the following key lemma applied to  $g\tilde{c}$ :

(I) Here's the key lemma:

Lemma Say g = kan is such that  $||ge_1|| = \min_{x \in g\Gamma_n} ||xe_1||$ . There is  $\bar{n} \in N_{1/2}$  such that  $h := ka\bar{n} \in g\Gamma_n$  and  $||ge_1|| = ||he_1||$ . Moreover,  $a_1/a_2 \le 2/\sqrt{3}$ .

The proof is simple. Pick  $\bar{n} \in N_{1/2}$  such that  $n \in \bar{n}(\Gamma_n \cap N)$ and set  $h = ka\bar{n}$ . Then  $||ge_1|| = ||ae_1|| = a_1 = ||he_1||$ . Next, if P is the matrix permuting  $e_1, e_2$  and fixing  $e_3, ...$ , we have

$$\begin{aligned} a_1 &= ||he_1|| \le ||hPe_1|| = ||he_2|| = ||k(a_1\bar{n}_{12}e_1 + a_2e_2)|| \\ &= \sqrt{a_1^2\bar{n}_{12}^2 + a_2^2} \le \sqrt{a_1^2/4 + a_2^2} \end{aligned}$$

and we are done.

## Proof of Mahler's compactness criterion

(I) Recall the statement:

Theorem (Mahler's compactness criterion) Let  $M \subset \mathbb{GL}_n(\mathbb{R})$  be a subset such that for some c > 0 we have  $\det(g) \ge c$  and  $\inf_{x \in \mathbb{Z}^n \setminus \{0\}} ||g^{-1}x|| \ge c$  for  $g \in M$ . Then the image of M in  $\mathbb{GL}_n(\mathbb{Z}) \setminus \mathbb{GL}_n(\mathbb{R})$  has compact closure.

Pick a sequence  $g_j \in M$  and write  $g_j^{-1} = k_j a_j n_j \gamma_j$  with  $\gamma_j \in \mathbb{GL}_n(\mathbb{Z})$  and  $k_j a_j n_j \in \sum_{2/\sqrt{3}, 1/2}$ . It suffices to check that the  $a_j$  stay in a compact set, as then  $\gamma_j g_j$  has a convergent sub-sequence. But if  $a_j = \text{diag}(a_j^1, a_j^2, ...)$  the condition on det g forces  $a_j^1 \cdot a_j^2 \cdot ...$  to be bounded from above, so it suffices to check that all  $a_j^k$  stay away from 0. This follows from  $a_j^1/a_j^2 \leq 2/\sqrt{3}, ...$  and

$$c \leq \inf_{x \in \mathbb{Z}^n \setminus \{0\}} ||g_j^{-1}x|| = \inf_x ||a_j n_j x|| \leq ||a_j n_j e_1|| = a_j^1.$$

# $\mathbb{SL}_n(\mathbb{Z})$ is a lattice in $\mathbb{SL}_n(\mathbb{R})$

 This also gives a simple proof that SL<sub>n</sub>(Z) is a lattice in SL<sub>n</sub>(R). Let Σ<sup>1</sup> = Σ<sub>2/√3,1/2</sub> ∩ SL<sub>n</sub>(R), then one easily gets SL<sub>n</sub>(R) = Σ<sup>1</sup>SL<sub>n</sub>(Z), so it suffices to show that Σ<sup>1</sup> has finite Haar measure.

# $\mathbb{SL}_n(\mathbb{Z})$ is a lattice in $\mathbb{SL}_n(\mathbb{R})$

- (1) This also gives a simple proof that  $\mathbb{SL}_n(\mathbb{Z})$  is a lattice in  $\mathbb{SL}_n(\mathbb{R})$ . Let  $\Sigma^1 = \Sigma_{2/\sqrt{3},1/2} \cap \mathbb{SL}_n(\mathbb{R})$ , then one easily gets  $\mathbb{SL}_n(\mathbb{R}) = \Sigma^1 \mathbb{SL}_n(\mathbb{Z})$ , so it suffices to show that  $\Sigma^1$  has finite Haar measure.
- (II) One has an Iwasawa decomposition SL<sub>n</sub>(ℝ) = SO<sub>n</sub>(ℝ)A<sub>0</sub>N with A<sub>0</sub> = A ∩ SL<sub>n</sub>(ℝ) relative to which the Haar measure on SL<sub>n</sub>(ℝ) decomposes

$$dg = \prod_{i < j} \frac{a_i}{a_j} dk \cdot da \cdot dn.$$

Using this it's a simple exercise to check that  $\Sigma^1$  has finite Haar measure.

 We will sketch a rather geometric proof of τ(G) = 1 for G := SL<sub>n</sub>. Let ω be the unique (up to a sign) invariant top-form on G, non-vanishing modulo any prime (exercise: write down one!). Since cl(G) = 1, we have

$$G(\mathbb{Q})\backslash G(\mathbb{A})/G(\hat{\mathbb{Z}})\simeq G(\mathbb{Z})\backslash G(\mathbb{R}).$$

Since

$$\operatorname{vol}(G(\hat{\mathbb{Z}})) = \prod_{p} |\omega_{p}|(G(\mathbb{Z}_{p})) = \prod_{p} \frac{G(\mathbb{F}_{p})}{p^{n^{2}-1}} = (\zeta(2)...\zeta(n))^{-1},$$

we are reduced to

$$\operatorname{vol}(D) := |\omega|_{\infty}(D) = \zeta(2)...\zeta(n)$$

for a fundamental domain D in  $G(\mathbb{R})$  with respect to the action of  $G(\mathbb{Z})$ .

## The Tamagawa number of $SL_n$

(1) Consider the standard invariant top-form on  $\mathbb{GL}_n$ 

$$\omega_{\rm can} = \frac{dx_{11} \wedge dx_{12} \wedge ... \wedge dx_{nn}}{\det(x_{ij})^n}$$

Its pullback by the product map  $m : \mathbb{SL}_n \times \mathbb{G}_m \to \mathbb{GL}_n$  is of the form  $\alpha \omega \wedge \frac{dt}{t}$  (*t* the coordinate on  $\mathbb{G}_m$ ) with  $\alpha$  a constant. One can find  $\alpha$  by looking at what's happening on tangent spaces at (1, 1) and obtains  $\alpha = \pm n$  and

$$m^*(dx_{11} \wedge dx_{12} \wedge ... \wedge dx_{nn}) = \pm n\omega \wedge t^{n^2-1}.$$

## The Tamagawa number of $SL_n$

(I) Consider the standard invariant top-form on  $\mathbb{GL}_n$ 

$$\omega_{\rm can} = \frac{dx_{11} \wedge dx_{12} \wedge ... \wedge dx_{nn}}{\det(x_{ij})^n}$$

Its pullback by the product map  $m : \mathbb{SL}_n \times \mathbb{G}_m \to \mathbb{GL}_n$  is of the form  $\alpha \omega \wedge \frac{dt}{t}$  (*t* the coordinate on  $\mathbb{G}_m$ ) with  $\alpha$  a constant. One can find  $\alpha$  by looking at what's happening on tangent spaces at (1, 1) and obtains  $\alpha = \pm n$  and

$$m^*(dx_{11} \wedge dx_{12} \wedge ... \wedge dx_{nn}) = \pm n\omega \wedge t^{n^2-1}$$

(II) Thus letting  $D_1 = m(D \times (0, 1]) = \{tx | t \in (0, 1], x \in D\}$  be the cone with section D, we have

$$\int_{D_1} |dx_{11} \wedge dx_{12} \wedge \ldots \wedge dx_{nn}| = \int_{D \times (0,1]} n |\omega| t^{n^2 - 1} dt = \frac{\operatorname{vol}(D)}{n}$$

and we need to show that

$$\operatorname{vol}(D_1) := \int_{D_1} |dx_{11} \wedge dx_{12} \wedge \ldots \wedge dx_{nn}| = \frac{\zeta(2) \ldots \zeta(n)}{\zeta(2) \ldots \zeta(n)}.$$

(1) For this we count lattice points in expanded versions of D, more precisely in  $D_T := \{td | t \in (0, T], d \in D\}$  for  $T \to \infty$ . Note that  $vol(D_T) = T^{n^2} vol(D_1)$ , so we need to estimate

$$\operatorname{vol}(D_1) = \lim_{T \to \infty} \frac{\operatorname{vol}(D_T)}{T^{n^2}} = \lim_{T \to \infty} \frac{|D_T \cap M_n(\mathbb{Z})|}{T^{n^2}}$$

(1) For this we count lattice points in expanded versions of D, more precisely in  $D_T := \{td | t \in (0, T], d \in D\}$  for  $T \to \infty$ . Note that  $vol(D_T) = T^{n^2} vol(D_1)$ , so we need to estimate

$$\operatorname{vol}(D_1) = \lim_{T \to \infty} \frac{\operatorname{vol}(D_T)}{T^{n^2}} = \lim_{T \to \infty} \frac{|D_T \cap M_n(\mathbb{Z})|}{T^{n^2}}$$

(II) Since  $D_T$  is a fundamental domain for  $\{X \in M_n(\mathbb{R}) | \ 0 < \det X \le T^n\}$  modulo  $G(\mathbb{Z})$ , we obtain

$$\operatorname{vol}(D_1) = \lim_{T \to \infty} \frac{1}{T^{n^2}} \sum_{k=1}^{T^n} a_k,$$

where  $a_k$  is the number of matrices  $X \in M_n(\mathbb{Z})$  with det X = k, modulo  $G(\mathbb{Z})$ .

However, a<sub>k</sub> is also the number of sub-lattices of Z<sup>n</sup> of index k and a nice inductive argument based on elementary divisors shows that

$$\sum_{k\geq 1}\frac{a_k}{k^s}=\zeta(s)\zeta(s-1)...\zeta(s-n+1),$$

thus as  $s \to 1$  $\sum_{k \ge 1} \frac{a_k}{k^{s+n-1}} = \zeta(s)\zeta(s+1)...\zeta(s+n-1) \approx \zeta(2)...\zeta(n)/(s-1).$ 

However, a<sub>k</sub> is also the number of sub-lattices of Z<sup>n</sup> of index k and a nice inductive argument based on elementary divisors shows that

$$\sum_{k\geq 1}\frac{a_k}{k^s}=\zeta(s)\zeta(s-1)...\zeta(s-n+1),$$

thus as s 
ightarrow 1

$$\sum_{k\geq 1} \frac{a_k}{k^{s+n-1}} = \zeta(s)\zeta(s+1)...\zeta(s+n-1) \approx \zeta(2)...\zeta(n)/(s-1).$$

(II) Suitable Tauberian theorems then yield

$$\lim_{x\to\infty}\frac{1}{x^n}\sum_{k\leq x}a_k=\frac{\zeta(2)...\zeta(n)}{n}$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

and this finishes the proof.