Lecture 9: arithmetic of algebraic groups

Gabriel Dospinescu

CNRS, ENS Lyon

Goal

(I) In this lecture we will study rationality issues for algebraic groups, by focusing on a key example for the second semester, and then state the main (and deep) properties of arithmetic groups in algebraic groups. Finally, we introduce some key new players: adelic groups.

Rationality issues

(I) Let k be a field of characteristic 0 and let K be an algebraically closed extension of k (in practice $K = \mathbb{C}$ and $k \in \{\mathbb{Q}, \mathbb{R}\}$). All varieties are affine and over K.

Rationality issues

(I) Let k be a field of characteristic 0 and let K be an algebraically closed extension of k (in practice $K = \mathbb{C}$ and $k \in \{\mathbb{Q}, \mathbb{R}\}$). All varieties are affine and over K.

(II) For a variety $X \subset K^n$ with ideal $I_X \subset K[T_1, ..., T_n]$ the following statements are equivalent (this fails in positive characteristic), and if they are satisfied we say that X is **defined over k (or a k-variety)**

- X is the set of solutions in K^n of some polynomial equations with coefficients in k
- $\sigma(X) \subset X$ for all $\sigma \in \mathrm{Aut}(K/k)$
- I_X is generated by $I_X \cap k[T_1, ..., T_n]$.

Rationality issues

(I) If X is defined over k, then the k-algebra (of regular functions defined over k)

$$k[X] := k[T_1, ..., T_n]/(I_X \cap k[T_1, ..., T_n])$$

satisfies $k[X] \otimes_k K = K[X]$ and X gives rise to a **functor of points**

$$X : \{k - \text{algebras}\} \to \mathrm{Sets},\ X(A) := \mathrm{Hom}_{k-\mathrm{alg}}(k[X], A).$$

If G is a k-**group** (i.e. an algebraic group defined over k) the functor of points factors through Groups.

Rationality issues

(I) If X is defined over k, then the k-algebra (of regular functions defined over k)

$$k[X] := k[T_1, ..., T_n]/(I_X \cap k[T_1, ..., T_n])$$

satisfies $k[X] \otimes_k K = K[X]$ and X gives rise to a **functor of points**

$$X : \{k - \text{algebras}\} \to \mathrm{Sets},\ X(A) := \mathrm{Hom}_{k-\mathrm{alg}}(k[X], A).$$

If G is a k-**group** (i.e. an algebraic group defined over k) the functor of points factors through Groups.

(II) A morphism $f : X \to Y$ of affine k-varieties is said to be defined over k (or a k-morphism) if $\varphi \circ f \in k[X]$ for any $\varphi \in k[Y]$. The functor $X \to k[X]$ gives an anti-equivalence between k-varieties (with k-morphisms) and reduced k-algebras of finite type.

Rationality issues

(I) Algebraic groups interact well with rationality properties:

• if G is a k-group, then so are G^0, $Z(G)$, G_{der}, $R_u(G)$.

• If $G \subset \mathbb{GL}_n(K)$ is defined over k, then its Lie algebra $\mathfrak{g}$ is defined over k, i.e. $\mathfrak{g}_k \otimes_k K \simeq \mathfrak{g}$ with $\mathfrak{g}_k := \mathfrak{g} \cap M_n(k)$. If $K = \mathbb{C}$ and G is defined over $\mathbb{R}$ then $\mathfrak{g}_{\mathbb{R}} = \mathrm{Lie}(G(\mathbb{R}))$.

• if $f : G \to H$ is a k-morphism of k-groups, then $f(G)$ is defined over k. Thus if H is a normal k-subgroup of a k-group G then G/H is a k-group.

Rationality issues

(I) It's an excellent exercise to show that $\mathbb{SL}_n(\mathbb{Q})$ is Zariski dense in $\mathbb{SL}_n(\mathbb{C})$. Try to do it with $SO(n)$. A huge generalisation is:

Theorem (Rosenlicht) If G is a **connected** k-group, then $G(k)$ is Zariski dense in G.

Rationality issues

(I) It's an excellent exercise to show that $\mathbb{SL}_n(\mathbb{Q})$ is Zariski dense in $\mathbb{SL}_n(\mathbb{C})$. Try to do it with $SO(n)$. A huge generalisation is:

Theorem (Rosenlicht) If G is a **connected** k-group, then $G(k)$ is Zariski dense in G.

(II) Rosenlicht also proved that any connected k-group G has a maximal torus defined over k. Unfortunately, not any connected (even reductive) k-group has a Borel subgroup defined over k. Such groups are called **quasi-split** over k. Their class includes the important class of split groups, that we discuss next.

Split tori

(I) A k-torus T is called **split over** k if there is an isomorphism defined over k between T and the group of diagonal matrices in some $\mathbb{GL}_n(K)$. A k-group may not have a k-split maximal torus, but it always has a maximal k-split torus (sic!). The following theorem is very difficult:

Theorem (Borel, Tits)
In a connected reductive k-group G all maximal k-split tori are conjugate under $G(k)$.

Split groups

(I) The connected reductive group G is called **split over** k if G has a maximal torus that is split over k.

Split groups

(I) The connected reductive group G is called **split over** k if G has a maximal torus that is split over k.

(II) The Chevalley-Demazure theorem classifies split connected reductive k-groups in terms of reduced root data: all statements that we saw last time over K are valid over k if the surrounding group is split over k.

Split groups

(I) The connected reductive group G is called **split over** k if G has a maximal torus that is split over k.

(II) The Chevalley-Demazure theorem classifies split connected reductive k-groups in terms of reduced root data: all statements that we saw last time over K are valid over k if the surrounding group is split over k.

(III) In particular any connected reductive k-group G is isomorphic **over the algebraic closure** $\bar{k}$ **of** k **in** K to a split group over k, i.e. G is a k-**form** of a split group over k. Such forms are classified by $H^1(\mathrm{Gal}_k, \mathrm{Aut}(G))$, where $\mathrm{Gal}_k = \mathrm{Aut}(\bar{k}/k)$.

Tori over a field

(I) Say $K = \bar{k}$. Then $\mathrm{Aut}(\mathbb{G}_m^d) \simeq \mathbb{GL}_d(\mathbb{Z})$, with trivial Galois action, so k-tori of rank d are classified by homomorphisms $\mathrm{Gal}_k \to \mathbb{GL}_d(\mathbb{Z})$ with finite image. Where do these come from?

Tori over a field

(I) Say $K = \bar{k}$. Then $\mathrm{Aut}(\mathbb{G}_m^d) \simeq \mathbb{GL}_d(\mathbb{Z})$, with trivial Galois action, so k-tori of rank d are classified by homomorphisms $\mathrm{Gal}_k \to \mathbb{GL}_d(\mathbb{Z})$ with finite image. Where do these come from?

(II) Any k-torus T is defined over a finite extension of k, thus Gal_k acts on $X(T)$ by a finite quotient. This induces an anti-equivalence between k-tori and finite free $\mathbb{Z}$-modules together with an action of Gal_k factoring through a finite quotient.

Tori over a field

(I) Say $K = \bar{k}$. Then $\mathrm{Aut}(\mathbb{G}_m^d) \simeq \mathbb{GL}_d(\mathbb{Z})$, with trivial Galois action, so k-tori of rank d are classified by homomorphisms $\mathrm{Gal}_k \to \mathbb{GL}_d(\mathbb{Z})$ with finite image. Where do these come from?

(II) Any k-torus T is defined over a finite extension of k, thus Gal_k acts on $X(T)$ by a finite quotient. This induces an anti-equivalence between k-tori and finite free $\mathbb{Z}$-modules together with an action of Gal_k factoring through a finite quotient.

(III) The k-torus T is k-split if and only if Gal_k acts trivially on $X(T)$, i.e. all characters $T \to \mathbb{G}_m$ are defined over k,

Forms of $\mathbb{SL}_2$

(I) Keep $K = \bar{k}$. It's an excellent exercise to show that $\mathrm{Aut}(\mathbb{SL}_2(K)) = PSL_2(K) = PGL_2(K)$. The group $H^1(\mathrm{Gal}_k, PGL_2(K))$ is related to quaternion algebras. More generally $H^1(\mathrm{Gal}_k, PGL_n(K))$ is the set of isomorphism classes of central simple k-algebras of dimension n^2 (since $\mathrm{Aut}_{K-\mathrm{alg}}(M_n(K)) = PGL_n(K)$).

Forms of $\mathbb{SL}_2$

(I) Keep $K = \bar{k}$. It's an excellent exercise to show that $\mathrm{Aut}(\mathbb{SL}_2(K)) = PSL_2(K) = PGL_2(K)$. The group $H^1(\mathrm{Gal}_k, PGL_2(K))$ is related to quaternion algebras. More generally $H^1(\mathrm{Gal}_k, PGL_n(K))$ is the set of isomorphism classes of central simple k-algebras of dimension n^2 (since $\mathrm{Aut}_{K-\mathrm{alg}}(M_n(K)) = PGL_n(K)$).

Forms of $\mathbb{SL}_2$

(I) Keep $K = \bar{k}$. It's an excellent exercise to show that $\mathrm{Aut}(\mathbb{SL}_2(K)) = PSL_2(K) = PGL_2(K)$. The group $H^1(\mathrm{Gal}_k, PGL_2(K))$ is related to quaternion algebras. More generally $H^1(\mathrm{Gal}_k, PGL_n(K))$ is the set of isomorphism classes of central simple k-algebras of dimension n^2 (since $\mathrm{Aut}_{K-\mathrm{alg}}(M_n(K)) = PGL_n(K)$).

(II) A **quaternion algebra** over a field F (of characteristic 0, say) is a central simple algebra of dimension 4 over F. Concretely, all such algebras are of the form

$$D = F \oplus Fi \oplus Fj \oplus Fk$$

with $i^2 = a, j^2 = b, ij = -ji = k$, for some $a, b \in F^*$.

Forms of $\mathbb{SL}_2$

(I) If D is as above, its **reduced norm**

$$N : D \to F, \ N(x + yi + zj + tk) = x^2 - ay^2 - bz^2 + abt^2$$

is multiplicative.

Forms of $\mathbb{SL}_2$

(I) If D is as above, its **reduced norm**

$$N : D \to F, \ N(x + yi + zj + tk) = x^2 - ay^2 - bz^2 + abt^2$$

is multiplicative.

(II) Indeed, if $\alpha, \beta \in \bar{F}$ are such that $\alpha^2 = a, \beta^2 = b$, then we have an isomorphism of $\bar{F}$-algebras $\varphi : D \otimes_F \bar{F} \simeq M_2(\bar{F})$

$$\varphi(x_1 + x_2 i + x_3 j + x_4 k) = \begin{pmatrix} x_1 + x_2\alpha & x_3 + x_4\alpha \\ b(x_3 - x_4\alpha) & x_1 - x_2\alpha \end{pmatrix}$$

satisfying $\det(\varphi(x)) = N(x)$.

Forms of $\mathbb{SL}_2$

(I) The group $G = (D \otimes_F \bar{F})^*$ is thus isomorphic to $\mathbb{GL}_2(\bar{F})$. The left-regular representation of D realises G as an algebraic subgroup of $\mathbb{GL}_4(\bar{F}) = \mathbb{GL}(D \otimes_F \bar{F})$ defined over F. The subgroup $SL_1(D)$ of elements of reduced norm 1 in G becomes a connected reductive group defined over F, isomorphic to $\mathbb{SL}_2(\bar{F})$ over $\bar{F}$, but in general not over F (this happens if and only if $D \simeq M_2(F)$ as F-algebras, or equivalently D is not a division algebra over F).

Forms of $\mathbb{SL}_2$

(I) A good exercise: quaternion algebras over F, up to isomorphism, are in bijection with non-degenerate quadratic forms on F^3 with discriminant 1, up to equivalence, via $D \to N|_{D_0}$, where $D_0 = Fi \oplus Fj \oplus Fk$. The split quaternion algebra $M_2(F)$ corresponds to the unique (up to equivalence) such isotropic form, $x^2 - y^2 - z^2$.

Forms of $\mathbb{SL}_2$

(I) A good exercise: quaternion algebras over F, up to isomorphism, are in bijection with non-degenerate quadratic forms on F^3 with discriminant 1, up to equivalence, via $D \to N|_{D_0}$, where $D_0 = Fi \oplus Fj \oplus Fk$. The split quaternion algebra $M_2(F)$ corresponds to the unique (up to equivalence) such isotropic form, $x^2 - y^2 - z^2$.

(II) Using this one proves that over $\mathbb{Q}_p$ or $\mathbb{R}$ there are exactly two quaternion algebras up to isomorphism, so up to isomorphism there is a unique quaternion division algebra over such a local field.

Forms of $\mathbb{SL}_2$

(I) It is much harder to classify quaternion algebras over $\mathbb{Q}$ (or any number field), but this can be done using the Hasse-Minkowski theorem. They are classified by finite sets of places of $\mathbb{Q}$ of even cardinality, by sending a quaternion algebra D to the set of places v of $\mathbb{Q}$ where D is ramified, i.e. such that the quaternion algebra $D \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is a division algebra over $\mathbb{Q}_v$.

Anisotropic groups

(I) Somewhat opposite to k-split groups are k-**anisotropic groups**, i.e. connected reductive k-groups G containing no nontrivial k-split torus.

Anisotropic groups

(I) Somewhat opposite to k-split groups are k-**anisotropic groups**, i.e. connected reductive k-groups G containing no nontrivial k-split torus.

(II) A k-torus T is k-anisotropic if and only if $X(T)^{\mathrm{Gal}_k} = 0$. Any k-torus is (uniquely) the almost direct product of a split k-torus and of an anisotropic k-torus. An important example of k-anisotropic torus is the set of elements of norm 1 in

$$(L \otimes_k \mathbb{C})^* \simeq \prod_{\sigma \in \mathrm{Gal}(L/k)} \mathbb{C}^*,$$

where L/k is a Galois extension of degree $d > 1$ (take $K = \mathbb{C}$ here).

Anisotropic groups

(I) The name comes from the following key result (excellent exercise!): if F is a non-degenerate quadratic form in n variables, with coefficients in k, the group $O(F)$ is anisotropic over k if and only if F is anisotropic, i.e. the equation $F(x) = 0$ has only the trivial solution in k^n. Also, if D is a quaternion division algebra over k, then $SL_1(D)$ is anisotropic over k.

(II) If G is a k-group, we let $X(G)_k \subset X(G)$ be the set of morphisms $G \to \mathbb{G}_m$ defined over k.

Theorem (Borel-Tits) A connected reductive k-group $G \subset \mathbb{GL}_n(K)$ is anisotropic over k if and only if $X(G)_k = \{1\}$ and the only unipotent matrix in $G(k)$ is I_n.

Anisotropic groups

(I) One implication in the next theorem is trivial, but the other one is quite hard. Gopal Prasad gave an amazing elementary (but still a bit long...) proof.

Theorem (Bruhat-Tits) Let $k = \mathbb{R}$ or $\mathbb{Q}_p$ for some prime p. A connected reductive k-group G is k-anisotropic if and only if $G(k)$ is compact (for its natural topology).

We will see a global version, i.e. for $\mathbb{Q}$-groups.

Arithmetic subgroups of algebraic groups

(I) If $G \subset \mathbb{GL}_n(\mathbb{C})$ is a $\mathbb{Q}$-group, we let

$$G(\mathbb{Z}) := G \cap \mathbb{GL}_n(\mathbb{Z}).$$

Contrary to $G(\mathbb{Q})$, this depends on the embedding of G in $\mathbb{GL}_n(\mathbb{C})$, but not that much: by the next theorem, it is well-defined up to commensurability. Two subgroups H_1, H_2 of a group H are **commensurable** if $H_1 \cap H_2$ has finite index in both H_1 and H_2.

Arithmetic subgroups of algebraic groups

(I) If $G \subset \mathbb{GL}_n(\mathbb{C})$ is a $\mathbb{Q}$-group, we let

$$G(\mathbb{Z}) := G \cap \mathbb{GL}_n(\mathbb{Z}).$$

Contrary to $G(\mathbb{Q})$, this depends on the embedding of G in $\mathbb{GL}_n(\mathbb{C})$, but not that much: by the next theorem, it is well-defined up to commensurability. Two subgroups H_1, H_2 of a group H are **commensurable** if $H_1 \cap H_2$ has finite index in both H_1 and H_2.

(II) If G is a $\mathbb{Q}$-group, a subgroup $\Gamma \subset G(\mathbb{Q})$ is called **arithmetic** if Γ is commensurable to $G(\mathbb{Z})$. This definition makes sense by the above discussion.

Arithmetic subgroups of algebraic groups

(I) Even the simplest structural properties of arithmetic groups are quite hard to prove, see Borel's book "Introduction aux groupes arithmétiques" or the (wonderful) book of Platonov and Rapinchuk "Algebraic groups and number theory" for the very involved proofs. One of the few easy things is:

Theorem If $\rho : G \to \mathbb{GL}_m(\mathbb{C})$ is a $\mathbb{Q}$-morphism of $\mathbb{Q}$-algebraic groups, then

a) $\rho^{-1}(\mathbb{GL}_m(\mathbb{Z}))$ contains a finite index subgroup of $G(\mathbb{Z})$.

b) If ρ is injective, then $\rho(G(\mathbb{Z}))$ is commensurable to $\rho(G)(\mathbb{Z})$.

Arithmetic subgroups of algebraic groups

(I) For a), note that

$$\Gamma(N) := \ker(\mathbb{GL}_n(\mathbb{Z}) \to \mathbb{GL}_n(\mathbb{Z}/N\mathbb{Z}))$$

has finite index in $\mathbb{GL}_n(\mathbb{Z})$, thus $\Gamma(N) \cap G$ has finite index in $G(\mathbb{Z})$. Using that the entries of $\rho(g)$ are polynomials in the entries of g and $\det(g)^{-1}$, and that $\rho(1) = 1$, one easily shows that for some sufficiently divisible N we have $\Gamma(N) \cap G \subset \rho^{-1}(\mathbb{GL}_m(\mathbb{Z}))$.

Arithmetic subgroups of algebraic groups

(I) For a), note that

$$\Gamma(N) := \ker(\mathbb{GL}_n(\mathbb{Z}) \to \mathbb{GL}_n(\mathbb{Z}/N\mathbb{Z}))$$

has finite index in $\mathbb{GL}_n(\mathbb{Z})$, thus $\Gamma(N) \cap G$ has finite index in $G(\mathbb{Z})$. Using that the entries of $\rho(g)$ are polynomials in the entries of g and $\det(g)^{-1}$, and that $\rho(1) = 1$, one easily shows that for some sufficiently divisible N we have $\Gamma(N) \cap G \subset \rho^{-1}(\mathbb{GL}_m(\mathbb{Z}))$.

(II) For b), let $H = \rho(G)$, so that $\rho : G \to H$ is an isomorphism of $\mathbb{Q}$-groups (previous lecture). Now a) applied to both ρ and its inverse easily yield b).

Arithmetic subgroups of algebraic groups

(I) In particular if $f : G \to H$ is an isomorphism of $\mathbb{Q}$-groups, then the image of an arithmetic subgroup of G is an arithmetic subgroup of H. It is **much** harder to prove that the image of an arithmetic subgroup by a surjective $\mathbb{Q}$-morphism of $\mathbb{Q}$-algebraic groups is arithmetic (a theorem of Borel and Harish-Chandra).

Arithmetic subgroups of algebraic groups

(I) In particular if $f : G \to H$ is an isomorphism of $\mathbb{Q}$-groups, then the image of an arithmetic subgroup of G is an arithmetic subgroup of H. It is **much** harder to prove that the image of an arithmetic subgroup by a surjective $\mathbb{Q}$-morphism of $\mathbb{Q}$-algebraic groups is arithmetic (a theorem of Borel and Harish-Chandra).

(II) The next theorem is a huge generalisation of the fact that $\mathbb{GL}_n(\mathbb{Z})$ and $\mathbb{SL}_n(\mathbb{Z})$ are finitely presented groups.

Theorem (Borel, Harish-Chandra) An arithmetic subgroup of a $\mathbb{Q}$-group is finitely presented, in particular finitely generated.

Arithmetic subgroups of algebraic groups

(I) Note that if $G(\mathbb{R})$ is compact, then $G(\mathbb{Z})$ is finite (as it is discrete and closed in $G(\mathbb{R})$), so all arithmetic groups are finite and the previous theorem is trivial.

Arithmetic subgroups of algebraic groups

(I) Note that if $G(\mathbb{R})$ is compact, then $G(\mathbb{Z})$ is finite (as it is discrete and closed in $G(\mathbb{R})$), so all arithmetic groups are finite and the previous theorem is trivial.

(II) Take now D a quaternion division algebra over $\mathbb{Q}$, split at ∞, i.e. $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$. Then $G = SL_1(D)$ is anisotropic over $\mathbb{Q}$ and we will see later on that $G(\mathbb{Z})$ is a co-compact lattice in $G(\mathbb{R})$. Taking a suitable congruence subgroup, it is easy to see that $G(\mathbb{Z})$ has a finite index subgroup Γ that is torsion-free.

Arithmetic subgroups of algebraic groups

(I) Note that if $G(\mathbb{R})$ is compact, then $G(\mathbb{Z})$ is finite (as it is discrete and closed in $G(\mathbb{R})$), so all arithmetic groups are finite and the previous theorem is trivial.

(II) Take now D a quaternion division algebra over $\mathbb{Q}$, split at ∞, i.e. $D \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$. Then $G = SL_1(D)$ is anisotropic over $\mathbb{Q}$ and we will see later on that $G(\mathbb{Z})$ is a co-compact lattice in $G(\mathbb{R})$. Taking a suitable congruence subgroup, it is easy to see that $G(\mathbb{Z})$ has a finite index subgroup Γ that is torsion-free.

(III) Then Γ acts freely on $X = G(\mathbb{R})/K$ (K a maximal compact of $G(\mathbb{R})$): if $\gamma \in \Gamma$ fixes gK, then $\gamma \in gKg^{-1} \cap \Gamma$ and the latter group is trivial (it is finite a priori, but Γ is torsion-free). The quotient $\Gamma \backslash X$ is a compact manifold (by the above discussion) with fundamental group Γ and thus Γ is finitely presented, proving the theorem in this case.

Arithmetic subgroups of algebraic groups

(I) The following fundamental and difficult result is goes back to Hermite and Minkowski for $G = \mathbb{SL}_n$:

Theorem (Borel, Harish-Chandra) If G is a connected semi-simple $\mathbb{Q}$-group, then any arithmetic subgroup of $G(\mathbb{Q})$ is a lattice in $G(\mathbb{R})$.

In particular, if $G(\mathbb{R})$ is not compact then $G(\mathbb{Z})$ is infinite. This is a key ingredient in the proof of:

Theorem (Borel's density theorem) If G is a connected semi-simple $\mathbb{Q}$-group with $G(\mathbb{R})$ non compact, any arithmetic subgroup of G is Zariski dense in G.

Excellent exercise (do it by hand!): $\mathbb{SL}_n(\mathbb{Z})$ is Zariski dense in $\mathbb{SL}_n(\mathbb{C})$.

Arithmetic subgroups of algebraic groups

(I) One also deduces from the Borel-Harish-Chandra theorem that for any $\mathbb{Q}$-group G the subgroup $G(\mathbb{Z})$ (or any arithmetic subgroup) is a lattice in $G(\mathbb{R})$ if and only if $X(G^0)_{\mathbb{Q}} = 1$, i.e. there are no nontrivial morphisms $G^0 \to \mathbb{G}_m$ defined over $\mathbb{Q}$.

Godement's criterion

(I) For a $\mathbb{Q}$-group G set

$$R_G = G(\mathbb{Z})\backslash G(\mathbb{R}).$$

Note that $R_n := R_{\mathbb{GL}_n(\mathbb{C})}$ is the set of lattices in $\mathbb{R}^n$, via the map $\mathbb{GL}_n(\mathbb{Z})g \to g^{-1}(\mathbb{Z}^n)$. The following beautiful result is called **Godement's criterion**:

Theorem (Borel– Harish-Chandra, Mostow– Tamagawa)
A connected reductive $\mathbb{Q}$-group G is $\mathbb{Q}$-anisotropic if and only if $G(\mathbb{Z})\backslash G(\mathbb{R})$ is compact.

More generally, for an algebraic group G over $\mathbb{Q}$ the quotient $G(\mathbb{Z})\backslash G(\mathbb{R})$ is compact if and only if the reductive part of G^0 is anisotropic over $\mathbb{Q}$.

Godement's criterion

(I) Applied to the torus $T = (F \otimes_{\mathbb{Q}} \mathbb{C})^*$, with F a number field, the next theorem (which is a consequence of the previous one) gives Dirichlet's unit theorem:

Theorem (Ono) Let T be a $\mathbb{Q}$-torus and let $d = \mathrm{rk}_{\mathbb{R}}(T) - \mathrm{rk}_{\mathbb{Q}}(T)$. There is a finite group μ such that

$$T(\mathbb{Z}) \simeq \mu \times \mathbb{Z}^d.$$

Here, for a k-group G we let $\mathrm{rk}_k(G)$ be the dimension of any k-split maximal torus in G, which is well-defined since they are all conjugate by the Borel-Tits theorem.

Godement's criterion

(I) The key input in the previous theorems is **reduction theory**, i.e. finding nice approximations to fundamental domains for $G(\mathbb{Z})\backslash G(\mathbb{R})$, cf. next lecture for the case of $\mathbb{SL}_n$ and chapter 4 of Platonov-Rapinchuk or Borel's book for the (very painful) general case. The case of $\mathbb{SL}_n$ gives the crucial:

Theorem (Mahler's compactness criterion) If $M \subset \mathbb{GL}_n(\mathbb{R})$ is such that for some $c > 0$

$$\det(g) \geq c \text{ and } \inf_{x \in \mathbb{Z}^n \setminus \{0\}} ||g^{-1}x|| \geq c, \ \forall g \in M,$$

then the image of M in R_n has compact closure.

In human language: a set of lattices in $\mathbb{R}^n$ is relatively compact if (and only if) their volumes are bounded and they avoid a small ball.

Godement's criterion

(I) The next result is at the heart of the proof of Godement's criterion:

Theorem Let $G \subset \mathbb{GL}_n(\mathbb{C})$ be a reductive $\mathbb{Q}$-group such that $|\det(g)| = 1$ for $g \in G(\mathbb{R})$. If there is a G-invariant polynomial $P \in \mathbb{Q}[\mathbb{C}^n]$ such that the equation $P(x) = 0$ has the only solution $x = 0$ in $\mathbb{Q}^n$, then $R_G = G(\mathbb{Z})\backslash G(\mathbb{R})$ is compact.

If D is a quaternion division algebra over $\mathbb{Q}$, then $G = SL_1(D)$ satisfies these conditions by taking the usual embedding in $\mathbb{GL}_4(\mathbb{C}) \simeq \mathbb{GL}(D \otimes \mathbb{C})$ (via the left-regular representation of D) and $P(d) = \det(m_d) = N(d)^2$.

Godement's criterion

(I) We conclude (a special case of Godement's criterion)

Theorem For a division quaternion algebra D over $\mathbb{Q}$ the group $SL_1(D)(\mathbb{Z})$ is a co-compact lattice in $SL_1(D)(\mathbb{R})$.

When D is split at ∞ we have $SL_1(D)(\mathbb{R}) \simeq \mathbb{SL}_2(\mathbb{R})$ and we get many examples of co-compact lattices. However, there are still **many** other (including continuous families!) co-compact lattices in $\mathbb{SL}_2(\mathbb{R})$. Amazingly, this breaks down for $\mathbb{SL}_n(\mathbb{R})$ with $n > 2$, by a very deep theorem of Margulis.

Godement's criterion

(I) The embedding $G \subset \mathbb{GL}_n(\mathbb{C})$ induces a continuous injection $i_G : R_G \to R_n$. A key nontrivial observation is:

Theorem The injection $i_G : R_G \to R_n$ is a homeomorphism onto its image, which is closed in R_n.

More generally, the same argument shows that if H is a reductive $\mathbb{Q}$-subgroup of a connected $\mathbb{Q}$-group G, then R_H is homeomorphic to a closed subset in R_G.

Godement's criterion

(I) Suppose that $i_G(G(\mathbb{Z})g_k)$ converges to $\mathbb{GL}_n(\mathbb{Z})g$, i.e. $\gamma_k g_k$ converges to g for some $\gamma_k \in \mathbb{GL}_n(\mathbb{Z})$. We need to show that there are $u_k \in G(\mathbb{Z})$ such that $u_k g_k$ converges in $G(\mathbb{R})$.

Godement's criterion

(I) Suppose that $i_G(G(\mathbb{Z})g_k)$ converges to $\mathbb{GL}_n(\mathbb{Z})g$, i.e. $\gamma_k g_k$ converges to g for some $\gamma_k \in \mathbb{GL}_n(\mathbb{Z})$. We need to show that there are $u_k \in G(\mathbb{Z})$ such that $u_k g_k$ converges in $G(\mathbb{R})$.

(II) By a theorem of Chevalley there is a representation $\rho : G \to \mathbb{GL}(V)$ defined over $\mathbb{Q}$ and a rational vector $v \in V$ such that $G = \{g \in \mathbb{GL}(V) | \, \rho(g)v = v\}$.

Godement's criterion

(I) Suppose that $i_G(G(\mathbb{Z})g_k)$ converges to $\mathbb{GL}_n(\mathbb{Z})g$, i.e. $\gamma_k g_k$ converges to g for some $\gamma_k \in \mathbb{GL}_n(\mathbb{Z})$. We need to show that there are $u_k \in G(\mathbb{Z})$ such that $u_k g_k$ converges in $G(\mathbb{R})$.

(II) By a theorem of Chevalley there is a representation $\rho : G \to \mathbb{GL}(V)$ defined over $\mathbb{Q}$ and a rational vector $v \in V$ such that $G = \{g \in \mathbb{GL}(V) | \, \rho(g)v = v\}$.

(III) Then $\rho(\gamma_k)\rho(g_k)v$ tends to $\rho(g)v$, thus $\rho(\gamma_k)v \to \rho(g)v$. But $\rho(\gamma_k)v$ stay in a lattice, thus $\rho(\gamma_k)v = \rho(g)v$ for k large enough and so $\gamma_k^{-1}g \in G(\mathbb{R})$ for k large enough, say $k \geq k_0$. Then $u_k := \gamma_{k_0}^{-1}\gamma_k \in \mathbb{GL}_n(\mathbb{Z}) \cap G(\mathbb{R}) = G(\mathbb{Z})$ and $u_k g_k$ tends to $\gamma_{k_0}^{-1}g$.

Godement's criterion

(I) Suppose now that there is $P \in \mathbb{Q}[\mathbb{C}^n]$ invariant under G and vanishing on $\mathbb{Q}^n$ only at 0. Let's prove that $R_G = G(\mathbb{Z})\backslash G(\mathbb{R})$ is compact. Since R_G is (via i_G) a closed subspace of R_n, it's enough to show that the image of $G(\mathbb{R})$ in R_n is relatively compact.

Godement's criterion

(I) Suppose now that there is $P \in \mathbb{Q}[\mathbb{C}^n]$ invariant under G and vanishing on $\mathbb{Q}^n$ only at 0. Let's prove that $R_G = G(\mathbb{Z})\backslash G(\mathbb{R})$ is compact. Since R_G is (via i_G) a closed subspace of R_n, it's enough to show that the image of $G(\mathbb{R})$ in R_n is relatively compact.

(II) If this is not the case, since $|\det(g)| = 1$ for $g \in G(\mathbb{R})$, Mahler's criterion gives the existence of sequences $g_j \in G(\mathbb{R})$ and $v_j \in \mathbb{Z}^n \setminus \{0\}$ with $g_j v_j \to 0$. But $P(g_j v_j)$ tends to $P(0) = 0$ and P is G-invariant, thus $P(v_j)$ tends to 0, but since $v_j \in \mathbb{Z}^n$ and $P \in \mathbb{Q}[\mathbb{C}^n]$, we must have $P(v_j) = 0$ for j large enough and, by hypothesis, $v_j = 0$ as well, a contradiction!

Godement's criterion

(I) We will prove now Godement's criterion when G has trivial centre (the general case reduces to this, but not after some delicate work!). The following amazing proof is due to Mostow and Tamagawa. Since G is anisotropic over $\mathbb{Q}$, we have $X(G)_{\mathbb{Q}} = 1$ and so $|\det(g)| = 1$ for $g \in G(\mathbb{R})$. The hypothesis on the centre (plus the connectedness of G) implies that $\mathrm{Ad} : G \to \mathbb{GL}(\mathfrak{g})$ is injective, where $\mathfrak{g} = \mathrm{Lie}(G)$.

Godement's criterion

(I) We will prove now Godement's criterion when G has trivial centre (the general case reduces to this, but not after some delicate work!). The following amazing proof is due to Mostow and Tamagawa. Since G is anisotropic over $\mathbb{Q}$, we have $X(G)_{\mathbb{Q}} = 1$ and so $|\det(g)| = 1$ for $g \in G(\mathbb{R})$. The hypothesis on the centre (plus the connectedness of G) implies that $\mathrm{Ad} : G \to \mathbb{GL}(\mathfrak{g})$ is injective, where $\mathfrak{g} = \mathrm{Lie}(G)$.

(II) We will construct $P \in \mathbb{Q}[\mathfrak{g}]^G$ such that $P(x) = 0$ has only the solution $X = 0$ in $\mathfrak{g}(\mathbb{Q})$. Write

$$\det(T \bullet 1 - X) = T^d + \sum_{i=0}^{d-1} p_i(X)\, T^i$$

and consider the polynomial

$$P = \sum_{i=0}^{d-1} P_i^2.$$

Godement's criterion

(I) Then clearly $P \in \mathbb{Q}[\mathfrak{g}]^G$. If $X \in \mathfrak{g}(\mathbb{Q})$ is a solution of $P(X) = 0$, then $P_i(X) = 0$ for all i, so X is nilpotent. But then $e^X \in G(\mathbb{Q})$ is unipotent, thus trivial (since G is $\mathbb{Q}$-anisotropic) and $X = 0$.

Adelic groups

(I) We will introduce now a new, but fundamental object. Let $G \subset \mathbb{GL}_n(\mathbb{C})$ be a $\mathbb{Q}$-group. A key source of arithmetic subgroups of $G(\mathbb{Q})$ is given by the congruence subgroups

$$G(\mathbb{Z})(N) = \ker(G(\mathbb{Z}) \to \mathbb{GL}_n(\mathbb{Z}) \to \mathbb{GL}_n(\mathbb{Z}/N\mathbb{Z})).$$

Adelic groups

(I) We will introduce now a new, but fundamental object. Let $G \subset \mathbb{GL}_n(\mathbb{C})$ be a $\mathbb{Q}$-group. A key source of arithmetic subgroups of $G(\mathbb{Q})$ is given by the congruence subgroups

$$G(\mathbb{Z})(N) = \ker(G(\mathbb{Z}) \to \mathbb{GL}_n(\mathbb{Z}) \to \mathbb{GL}_n(\mathbb{Z}/N\mathbb{Z})).$$

(II) Whenever $N \mid M$ there is a natural map $\mathbb{Z}/M\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, and we can take the inverse limit of the system $(\mathbb{Z}/N\mathbb{Z})_{N \in \mathbb{Z}_{>0}}$ to get a compact topological ring (the **profinite completion of** $\mathbb{Z}$)

$$\hat{\mathbb{Z}} = \varprojlim_N \mathbb{Z}/N\mathbb{Z}$$

of characteristic 0: the Chinese remainder theorem gives

$$\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p,$$

where $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is the ring of p-adic integers. Let $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, the field of p-adic numbers.

Adelic groups

(I) The group $G(\hat{\mathbb{Z}}) := G \cap \mathbb{GL}_n(\hat{\mathbb{Z}})$ depends on the embedding of G in $\mathbb{GL}_n(\mathbb{C})$. To get rid of the dependence on the embedding of G, we define the ring $\mathbb{A}_f$ of **finite adèles**

$$\mathbb{A}_f = \hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$$

and endow it with a locally compact topology having $N\hat{\mathbb{Z}}$ ($N \in \mathbb{Z}_{>0}$) as a basis of open neighborhoods of 0. Finally, we define the (locally compact) **ring of adèles**

$$\mathbb{A} = \mathbb{R} \times \mathbb{A}_f.$$

Adelic groups

(I) The group $G(\hat{\mathbb{Z}}) := G \cap \mathbb{GL}_n(\hat{\mathbb{Z}})$ depends on the embedding of G in $\mathbb{GL}_n(\mathbb{C})$. To get rid of the dependence on the embedding of G, we define the ring $\mathbb{A}_f$ of **finite adèles**

$$\mathbb{A}_f = \hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$$

and endow it with a locally compact topology having $N\hat{\mathbb{Z}}$ ($N \in \mathbb{Z}_{>0}$) as a basis of open neighborhoods of 0. Finally, we define the (locally compact) **ring of adèles**

$$\mathbb{A} = \mathbb{R} \times \mathbb{A}_f.$$

(II) More concretely, letting $\mathbb{Q}_\infty = \mathbb{R}$ and

$$\mathscr{P} = \{2, 3, 5, ...\} \cup \{\infty\}$$

be the set of places of $\mathbb{Q}$, the ring $\mathbb{A}$ is the subring of $\prod_{v \in \mathbb{P}} \mathbb{Q}_v$ consisting of sequences $(a_v)_v$ such that $a_v \in \mathbb{Z}_v$ for almost all (i.e. all but finitely many) v.

Adelic groups

(I) Let $G \subset \mathbb{GL}_n(\mathbb{C})$ be a $\mathbb{Q}$-group. Contrary to $G(\mathbb{Q}_v)$, the group $G(\mathbb{Z}_v) = G \cap \mathbb{GL}_n(\mathbb{Z}_v)$ depends on the embedding $G \subset \mathbb{GL}_n(\mathbb{C})$, but if we pick another embedding, the resulting groups are the same for almost all v and

$$G(\mathbb{A}) \simeq \{(g_v)_v \in \prod_{v \in \mathscr{P}} G(\mathbb{Q}_v) |\ g_v \in G(\mathbb{Z}_v) \text{ for almost all } v\}.$$

Adelic groups

(I) Let $G \subset \mathbb{GL}_n(\mathbb{C})$ be a $\mathbb{Q}$-group. Contrary to $G(\mathbb{Q}_v)$, the group $G(\mathbb{Z}_v) = G \cap \mathbb{GL}_n(\mathbb{Z}_v)$ depends on the embedding $G \subset \mathbb{GL}_n(\mathbb{C})$, but if we pick another embedding, the resulting groups are the same for almost all v and

$$G(\mathbb{A}) \simeq \{(g_v)_v \in \prod_{v \in \mathscr{P}} G(\mathbb{Q}_v) |\ g_v \in G(\mathbb{Z}_v) \text{ for almost all } v\}.$$

(II) The topology of $\mathbb{A}$ is **not** induced by that of $\prod_v \mathbb{Q}_v$. Rather, a basis of open neighborhoods of $a = (a_v) \in \mathbb{A}$ is given by sets of the form $\prod_{v \in S} U_v \times \prod_{v \notin S} \mathbb{Z}_v$, with $S \subset \mathscr{P}$ finite, containing ∞, and U_v open neighborhoods of a_v.

Adelic groups

(I) Let $G \subset \mathbb{GL}_n(\mathbb{C})$ be a $\mathbb{Q}$-group. Contrary to $G(\mathbb{Q}_v)$, the group $G(\mathbb{Z}_v) = G \cap \mathbb{GL}_n(\mathbb{Z}_v)$ depends on the embedding $G \subset \mathbb{GL}_n(\mathbb{C})$, but if we pick another embedding, the resulting groups are the same for almost all v and

$$G(\mathbb{A}) \simeq \{(g_v)_v \in \prod_{v \in \mathscr{P}} G(\mathbb{Q}_v) |\ g_v \in G(\mathbb{Z}_v) \text{ for almost all } v\}.$$

(II) The topology of $\mathbb{A}$ is **not** induced by that of $\prod_v \mathbb{Q}_v$. Rather, a basis of open neighborhoods of $a = (a_v) \in \mathbb{A}$ is given by sets of the form $\prod_{v \in S} U_v \times \prod_{v \notin S} \mathbb{Z}_v$, with $S \subset \mathscr{P}$ finite, containing ∞, and U_v open neighborhoods of a_v.

(III) The natural map $[0,1] \times \hat{\mathbb{Z}} \to \mathbb{A}/\mathbb{Q}$ is surjective and $\mathbb{Q} \cap (-1,1) \times \hat{\mathbb{Z}} = \{0\}$, thus $\mathbb{Q}$ is a co-compact lattice in $\mathbb{A}$ (while $\mathbb{Q}$ is dense in $\mathbb{A}_f$!). The inclusion $\mathbb{Q} \to \mathbb{A}$ is an analogue of the embedding $\mathbb{Z} \to \mathbb{R}$.

Adelic groups

(I) For any affine variety X over $\mathbb{Q}$ we can endow $X(\mathbb{A})$ with a canonical locally compact topology, the weakest one for which $f : X(\mathbb{A}) \to \mathbb{A}$ is continuous for any $f \in \mathbb{Q}[X]$. Concretely, if $X \subset \mathbb{C}^n$ is Zariski closed, then this topology is the one induced from the product topology on $\mathbb{A}^n$. **Caution**: the topology on $\mathbb{A}^* = \mathbb{GL}_1(\mathbb{A})$ is **not** the one induced by $\mathbb{A}$ (for which it is not even a topological group!), but from $\mathbb{A}^2$ via the embedding $x \to (x, x^{-1})$. So a basis of neighborhoods of 1 is given by $\prod_v U_v$ with U_v a neighborhood of 1 in $\mathbb{Q}_v^*$ and $U_v = \mathbb{Z}_v^*$ for almost all v.

Adelic groups

(I) There is a continuous norm character

$$|\bullet| : \mathbb{A}^* \to \mathbb{R}_{>0},\ |x := (x_v)_v| = \prod_v |x_v|_v$$

trivial on $\mathbb{Q}^*$ and $\mathbb{Q}^*\backslash\mathbb{A}^*$ surjects onto $\mathbb{R}_{>0}$, so $\mathbb{Q}^*$ is not co-compact in $\mathbb{A}^*$. However, letting $\mathbb{A}^1 = \ker(|\bullet|)$, the quotient $\mathbb{A}^1/\mathbb{Q}^*$ is compact (exercise!).

Adelic groups

(I) There is a continuous norm character

$$|\bullet| : \mathbb{A}^* \to \mathbb{R}_{>0},\ |x := (x_v)_v| = \prod_v |x_v|_v$$

trivial on $\mathbb{Q}^*$ and $\mathbb{Q}^*\backslash\mathbb{A}^*$ surjects onto $\mathbb{R}_{>0}$, so $\mathbb{Q}^*$ is not co-compact in $\mathbb{A}^*$. However, letting $\mathbb{A}^1 = \ker(|\bullet|)$, the quotient $\mathbb{A}^1/\mathbb{Q}^*$ is compact (exercise!).

(II) If G is a $\mathbb{Q}$-group, $G(\mathbb{A})$ becomes a locally compact group containing $G(\mathbb{Q})$ as a discrete subgroup. $G(\mathbb{Q})$ is to $G(\mathbb{A})$ what $G(\mathbb{Z})$ is to $G(\mathbb{R})$. For any rational character $\chi \in X(G)_{\mathbb{Q}}$ we get a continuous character $\chi : G(\mathbb{A}) \to \mathbb{A}^*$, which we can compose with $\mathbb{A}^* \to \mathbb{R}_{>0}$ to get a character $|\bullet| \circ \chi : G(\mathbb{A}) \to \mathbb{R}_{>0}$. Concretely

$$|\chi|((g_v)_v) = \prod_v |\chi(g_v)|_v.$$

Adelic groups

(I) We have the following fundamental theorem, in which

$$G(\mathbb{A})^1 = \bigcap_{\chi \in X(G)_{\mathbb{Q}}} \ker |\bullet| \circ \chi$$

Theorem (Borel) For a connected reductive $\mathbb{Q}$-group G

a) $G(\mathbb{Q})$ is a lattice in $G(\mathbb{A})^1$, so $G(\mathbb{A})^1$ is unimodular.

b) $G(\mathbb{Q})$ is a lattice in $G(\mathbb{A})$ if and only if $X(G)_{\mathbb{Q}} = 1$ (or equivalently $G(\mathbb{Z})$ is a lattice in $G(\mathbb{R})$).

c) $G(\mathbb{Q})$ is a co-compact lattice in $G(\mathbb{A})$ if and only if $G(\mathbb{Z})$ is a co-compact lattice in $G(\mathbb{R})$, thus if and only if G is anisotropic over $\mathbb{Q}$.

Adelic groups

(I) One can prove this (except for the unimodularity issues, discussed in the next lecture) using the following deep result, called the **finiteness of the class number**, and the case of arithmetic subgroups of $G(\mathbb{Q})$:

Theorem (Borel) For any compact open subgroup $K_f \subset G(\mathbb{A}_f)$ the set $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K_f$ is finite.

Taking a finite set of representatives $x_i \in G(\mathbb{A}_f)$, one obtains a homeomorphism (send $\Gamma_i g$ to the class of (g, x_i))

$$\coprod \Gamma_i \backslash G(\mathbb{R}) \simeq G(\mathbb{Q})\backslash G(\mathbb{A})/K_f$$

with $\Gamma_i = G(\mathbb{Q}) \cap x_i(G(\mathbb{R}) \times K_f)x_i^{-1}$ arithmetic (even congruence) subgroups of $G(\mathbb{Q})$.

Adelic groups

(I) Take for instance $G = \mathbb{SL}_2(\mathbb{C})$. We will see next time that for any compact open subgroup $K_f \subset G(\mathbb{A}_f)$

$$G(\mathbb{Q})\backslash G(\mathbb{A})/K_f \simeq (G(\mathbb{Q}) \cap K_f)\backslash G(\mathbb{R}).$$

For

$$K_f = K_0(N) := \prod_{p|N} K_p \times \prod_{\gcd(p,N)=1} G(\mathbb{Z}_p),$$

with K_p the matrices in $G(\mathbb{Z}_p)$ reducing mod p to an upper triangular matrix, we obtain $\Gamma_0(N) = G(\mathbb{Q}) \cap K_0(N)$ and

$$G(\mathbb{Q})\backslash G(\mathbb{A})/K_0(N) \simeq \Gamma_0(N)\backslash G(\mathbb{R}).$$

Adelic groups

(I) Take for instance $G = \mathbb{SL}_2(\mathbb{C})$. We will see next time that for any compact open subgroup $K_f \subset G(\mathbb{A}_f)$

$$G(\mathbb{Q})\backslash G(\mathbb{A})/K_f \simeq (G(\mathbb{Q}) \cap K_f)\backslash G(\mathbb{R}).$$

For

$$K_f = K_0(N) := \prod_{p|N} K_p \times \prod_{\gcd(p,N)=1} G(\mathbb{Z}_p),$$

with K_p the matrices in $G(\mathbb{Z}_p)$ reducing mod p to an upper triangular matrix, we obtain $\Gamma_0(N) = G(\mathbb{Q}) \cap K_0(N)$ and

$$G(\mathbb{Q})\backslash G(\mathbb{A})/K_0(N) \simeq \Gamma_0(N)\backslash G(\mathbb{R}).$$

(II) A similar argument gives the beautiful description

$$G(\mathbb{Q})\backslash G(\mathbb{A}) \simeq \varprojlim_N \Gamma(N)\backslash G(\mathbb{R}),$$

with $\Gamma(N) := \ker(G(\mathbb{Z}) \to G(\mathbb{Z}/N\mathbb{Z}))$.