SOME FINITENESS THEOREMS FOR ABELIAN VARIETIES

BRIAN CONRAD (NOTES BY SAM LICHTENSTEIN)

1. Introduction

Last time we saw (see Proposition 6.5 in those lecture notes) that an abelian variety A of dimension g over K, the fraction field of a henselian dvr R, acquires semistable reduction over $K(A[\ell])$ for ℓ equal to 4 or an odd prime, with ℓ not divisible by the residue characteristic. (The same circle of ideas yielded the non-obvious fact that over K^{un} the intersection of two "semistable field extensions for A" is another such, and that the minimal such extension has degree over K^{un} dividing an explicit constant N depending only on g, made explicit in Theorem 6.8 of those lecture notes.)

As a consequence, for an abelian variety A over a global field K, A acquires *everywhere* semistable reduction over $K(A[M])$ where $M \in \{12, 15, 20\}$ is chosen so that $\mathrm{char}(K)$ does not divide M, so for any finite place v of K there is a factor of M having the form ℓ as above relative to the valuation ring of v. (If $\mathrm{char}(K) = 0$ we can use $M = 12$, but in characteristics 2 and 3 we must use 15 and 20 respectively.) Moreover the Galois extension $K(A[M])/K$ is unramified at all $v \nmid M\infty$ that are good for A.

The conclusion is that for g-dimensional A over K, good outside a set of places S containing all $v|M\infty$, A becomes everywhere semistable over an extension K'/K that is unramified outside S and of degree bounded only in terms of g. By Hermite–Minkowski, there are finitely many such extensions K'. Thus, there is a single finite extension $K' = K'_{g,S}$ over which *all* such A become semistable with bad places contained in the preimage S' of S.

This reduces the problem of proving the Shafarevich conjecture for the triple (K, S, g) to the case of the triple (K', S', g) under the additional property of being everywhere semistable *provided* that an abelian variety A over K is determined up to finitely many possibilities (up to K-isomorphism) when its scalar extension $A_{K'}$ over K' is known up to K'-isomorphism. Thus, to justify the sufficiency of proving the Shafarevich conjecture in the more restrictive setting of everywhere semistable abelian varieties over number fields, it remains to prove:

Theorem 1.1. *Let k'/k be a finite Galois extension of fields. The base change functor*

$$\{\textit{abelian varieties over } k\}/\simeq_k \ \to \ \{\textit{abelian varieties over } k'\}/\simeq_{k'}$$

has finite fibers. Equivalently, for an abelian variety A' over k', there are at most finitely many k-isomorphism classes of abelian varieties A over k such that $A_{k'} \simeq A'$.

In this lecture we will address the proof of this result, which will complete the proof of Corollary 6.6 from the previous lecture (where we saw that to prove the Shafarevich conjecture, it suffices to restrict attention to everywhere semistable abelian varieties that admit a principal polarization).

Note that Theorem 1.1 is purely algebraic in the sense that it holds for any finite Galois extension k'/k of fields, without arithmetic hypotheses on k or k'. However, the proof of the theorem has tremendous arithmetic content, insofar as we will use the structure of endomorphism algebras of abelian varieties (as finite-dimensional semisimple $\mathbf{Q}$-algebras) to reduce Theorem 1.1 to a deep general finiteness theorem in the theory of arithmetic groups.

The reference for this lecture is §18 of Milne's article "Abelian varieties" in Cornell–Silverman.

2. A naïve attempt that works only for elliptic curves

We may assume a k-descent A of A' exists (as otherwise there is nothing to do). Fix an isomorphism $A_{k'} \simeq A'$. It is a general fact about Galois descent (see Serre's book "Galois Cohomology", §III.1) that the pointed set of k-isomorphism classes of abelian varieties B over k satisfying $B_{k'} \simeq A' = A_{k'}$ (called "twisted forms" of A relative to k'/k) injects into the pointed Galois cohomology set $\mathrm{H}^1(G, \mathrm{Aut}_{k'}(A_{k'}))$, where $G := \mathrm{Gal}(k'/k)$ acts on $\mathrm{Aut}_{k'}(A_{k'})$ in the evident manner through scalar extension by k-automorphisms of k' (so we are using the initial choice of k-structure A on A'). Here, the isomorphism class of $B = A$ is carried to the canonical base point of the cohomology set. This is all explained in Serre's book.

Remark 2.1. Since A' is quasi-projective (in fact projective), and Galois descent is effective for quasi-projective schemes, this injection of pointed sets is actually an equality (though we do not need this fact). See Chapter 6 of the book "Néron Models" for an elegant general discussion of effectivity in descent, including the Galois-descent case worked out in detail.

When $\mathrm{Aut}_{k'}(A_{k'})$ is finite we are done, because the cohomology set $\mathrm{H}^1(G, \Gamma)$ of a finite group G with coefficients in a finite group Γ equipped with an action by G is visibly finite. (Even the set $Z^1(G, \Gamma)$ of 1-cocycles on G with values in Γ is finite.) When A' is an elliptic curve, this automorphism group is always finite. Hence, we are done with Theorem 1.1 in the 1-dimensional case.

In general we need to use more properties of abelian varieties. Observe that the group $\mathrm{Aut}_{k'}(A') = \mathrm{End}_{k'}(A')^\times$ is the group of units in the $\mathbf{Z}$-order $\mathrm{End}_k(A)$ in a finite dimensional semisimple $\mathbf{Q}$-algebra $\mathrm{End}^0_{k'}(A')$. Thus it is an arithmetic group. But it's not clear – and probably not generally true – whether or not $\mathrm{H}^1(G, \Gamma)$ is finite for a finite group G equipped with an action on an arithmetic group Γ.

To force the cohomology to be finite, it is natural to try to convert our problem into proving the finiteness of the set of twisted forms of (A, ϕ) for a choice of polarization ϕ on A over k, since polarized abelian varieties have *finite* automorphism group. This runs into the difficulty that it seems as if we must polarize A' in a way which descends to *any* k-form of A'. One approach to doing so, using the "sum" of the Galois conjugates of $\phi_{k'}$ on $A_{k'}$, founders on a couple of questions, the most basic of which is: Galois conjugates for which k-structure? We will make this vague strategy succeed by using two key finiteness results for abelian varieties.

3. Two finiteness results imply the theorem

This section is a review of the main ingredients needed to complete the proof of Corollary 6.6 in the notes from my previous semistable lecture. We need two serious finiteness theorems

for abelian varieties over general fields, the proofs of which will turn out to hinge on a common finiteness theorem for arithmetic groups. First, we have 18.1 in Milne's "Abelian varieties" article:

Theorem 3.1. *For an abelian variety X over a field F, equip the set $\mathrm{Pol}_F^d(X)$ of F-rational polarizations $\phi : X \to X^\vee$ of degree d^2 with a right action by $\mathrm{Aut}_F(X)$ via $\phi.u = u^\vee \circ \phi \circ u$. (Note that when $\phi = \phi_{\mathcal{L}}$ is obtained from an ample line bundle via the Mumford construction, as occurs over $\overline{k}$, we have $\phi.u = \phi_{u^*\mathcal{L}}$.) Then the set $\mathrm{Pol}_F^d(X)/\mathrm{Aut}_F(X)$ is finite.*

Remark 3.2. Note that it isn't evident how to reduce this problem to the version over an extension field (such as $\overline{k}$), since both the collection of polarizations as well as the automorphism group may grow. In fact we will not change k at all in the proof of this theorem.

Next, we state 18.7 in Milne's article. This rests on the following notion: a *direct factor* of an abelian variety X over a field F is an abelian variety Y over F admitting a closed F-subgroup inclusion $j : Y \hookrightarrow X$ for which there exists a splitting $s : X \to Y$ (i.e., $s \circ j = \mathrm{id}_Y$), which is to say a j-compatible isomorphism $X \simeq Y \times Y'$ as abelian varieties over F. Note that this is a much *stronger* condition on Y than being an isogeny factor (over F).

Theorem 3.3. *Let X be an abelian variety over a field F. The set of direct factors of X over F, taken up to F-isomorphism as abelian varieties, is finite.*

Remark 3.4. Both of these theorems ultimately rest on a key fact about arithmetic groups with a "geometry of numbers" flavor, to be stated below.

Granting Theorems 3.1 and 3.3, we now prove Theorem 1.1. This completes the proof of Corollary 6.6 in my semistable lecture notes (and the arguments that follow also appear in the partial proof of Corollary 6.6 from last week's notes).

Proof. By Theorem 3.3, the map $A \mapsto (A \times A^\vee)^4$ from the set of k-isomorphism classes of abelian varieties of dimension $g > 0$ over k to the set of k-isomorphism classes of abelian varieties of dimension $8g$ over k has finite fibers. By Zarhin's trick (see Remark 16.12 in Milne's article "Abelian Varieties"), $(A \times A^\vee)^4$ admits a principal polarization ϕ. (This is built by choosing an initial polarization on A, of some unknown degree d^2, and then writing d as a sum of 4 squares and creating a clever 4×4 matrix out of that expression in order to create a principal polzation. The analogue in linear algebra is to begin with a non-degenerate alternating form on a $\mathbf{Z}$-lattice L in a $\mathbf{Q}$-vector space V and find a $\mathbf{Z}$-sublattice in $(V \oplus V^\vee)^4$ on which the alternating form is $\mathbf{Z}$-perfect. In the context of polarizations, Milne assumes that d is not divisible by $\mathrm{char}(F)$. For applications over number fields this is fine, but in positive characteristic it can really happen that *every* polarization on A has degree divisible by $\mathrm{char}(F)$. But the degree coprimality restriction that Milne imposes can be bypassed by using the scheme-theoretic approach to Weil pairings as on page 228 of the 1st edition of Mumford's book "Abelian Varieties" and Lemma 1.4 in the published version of Oda's thesis.)

Note that if $A' = A_{k'}$ then $(A \times A^\vee)^4_{k'} \simeq (A' \times A'^\vee)^4$. Thus, upon renaming $(A' \times A'^\vee)^4$ as A', we may assume that A' admits a principal polarization over k' and are reduced to showing that A' admits only finitely many k-descents that admit a principal polarization (over k).

Consider a pair (A, ϕ) consisting of an abelian variety A over k descending A' and a principal polarization ϕ of A over k. Upon choosing some k'-isomorphism $A_{k'} \simeq A'$, $\phi_{k'}$ is carried by this isomorphism to some principal polarization of A'. By Theorem 3.1, as we vary through all choices of the k'-isomorphism $A_{k'} \simeq A'$ (i.e., fix one such k'-isomorphism and then compose it with arbitrary elements of $\mathrm{Aut}_{k'}(A')$) we arrive at just finitely many possibilities for $\phi_{k'}$ up to the $\mathrm{Aut}_{k'}(A')$-action, say $\phi'_1, \ldots, \phi'_n$.

We now have a forgetful map from

$$(k\text{-descents of } A' \text{ equipped with a principal polarization } \phi)/\simeq_k$$

to

$$(k\text{-descents of } A' \text{ that admit a principal polarization})/\simeq_k,$$

as well as a map from

$$(k\text{-descents of } A' \text{ equipped with a principal polarization } \phi)/\simeq_k$$

to

$$\coprod_i (k\text{-descents of the pair } (A', \phi'_i))/\simeq_k .$$

(Here, by a "k-descent" of some structure over k' we mean a structure over k whose scalar extension to k' *admits* a k'-isomorphism to the chosen k'-structure. In particular, the isomorphism assumed to exist over k' is not specified!) By Theorem 3.1, the first map has finite fibers (since any A that admits a principal polarization ϕ admits only finitely many such ϕ up to the action of $\mathrm{Aut}_k(A)$) and the second map is injective.

Thus, we may now fix $\phi' = \phi'_i$ on A' and just have to show the set of k-descents of (A', ϕ') is finite. When this set is nonempty and contains some (A, ϕ), we can run through the same game with H^1's as in the previous section, but we now arrive at $\mathrm{H}^1(\Gamma, \mathrm{Aut}_{k'}(A', \phi'))$. This time we win, since the "coefficient group" $\mathrm{Aut}_{k'}(A', \phi')$ is finite. ■

Remark 3.5. In the elliptic curve case, the preceding argument essentially coincides with what was already done for elliptic curves (except that Zarhin's trick wasn't needed there). The point is that an elliptic curve admits a unique principal polarization, so the automorphism group of an elliptic curve coincides with its automorphism as a (uniquely) principally polarized abelian variety. This "explains" the finiteness of the automorphism group of an elliptic curve in terms of the generali finiteness of the automorphism group of a polarized abelian variety.

4. Reduction of Theorem 3.1 to a theorem of Borel and Harish-Chandra

Fix A over k and $d \geq 1$. We will show that the set $\mathrm{Pol}_k^{\leq N}(A) := \bigcup_{d^2 \leq N} \mathrm{Pol}_k^{d^2}(A)$ of polarizations of *bounded* degree consists of finitely many $\mathrm{Aut}_k(A)$-orbits. (Note that the action by this group does not affect the degree of a polarization.)

Fix an initial choice of k-polarization $\lambda_0 : A \to A^\vee$. This gives rise to a Rosati involution $(-)^\dagger$ on $\mathrm{End}_k^0(A)$ defined by $\alpha^\dagger = \lambda_0^{-1} \alpha^\vee \lambda_0$. The set $\mathrm{Pol}_k(A)$ of k-polarizations $\lambda : A \to A^\vee$ embeds into the $+1$-eigenspace $\mathrm{End}_k^0(A)^+$ for $(-)^\dagger$ via $\lambda \mapsto \lambda_0^{-1}\lambda$. (Indeed, $(\lambda_0^{-1}\lambda)^\dagger = \lambda_0^{-1}\lambda^\vee(\lambda_0^{-1})^\vee\lambda_0 = \lambda_0^{-1}\lambda\lambda_0^{-1}\lambda_0 = \lambda_0^{-1}\lambda$ since by definition polarizations are symmetric and hence self-dual with respect to the double duality of abelian varieties.)

The computation $\lambda_0^{-1}u^\vee\lambda u = \lambda_0^{-1}u^\vee\lambda_0\lambda_0^{-1}\lambda u = u^\dagger\lambda_0^{-1}\lambda u$ shows that this map $\mathrm{Pol}_k(A) \to \mathrm{End}_k^0(A)^+$ intertwines the right action of interest to us for $\mathrm{Aut}_k(A)$ on $\mathrm{Pol}_k(A)$ and the right action of $\mathrm{Aut}_k(A)$ on $\mathrm{End}_k^0(A)^+$ given by $\alpha.u = u^\dagger\alpha u$. (Observe that this action preserves $\mathrm{End}_k^0(A)^+ \subset \mathrm{End}_k^0(A)$ since $(u^\dagger\alpha u)^\dagger = u^\dagger\alpha^\dagger u$ by the anti-homomorphism property of the Rosati involution.)

The degree of $\lambda_0^{-1}\lambda$ is $\deg(\lambda)/\deg(\lambda_0) \leq N/\deg(\lambda_0)$ for $\lambda \in \mathrm{Pol}_k^{\leq N}(A)$. The degree map $\deg : \mathrm{End}_k^0(A) \to \mathbf{Q}$ is a power of the reduced norm on each simple factor of the endmorphism algebra, so bounding the degree bounds the absolute value of the reduced norm up to some constants depending only on A.

Let $L = \mathbf{Z}[\mathrm{Pol}_k(A)] \subset \mathrm{End}_k^0(A)^+$ be the $\mathbf{Z}$-lattice spanned by the image of $\mathrm{Pol}_k(A)$ in the endomorphism algebra. This *is* a lattice – i.e. $L_{\mathbf{Q}}$ is all of $\mathrm{End}_k^0(A)^+$ – because *any endomorphism is a difference of images of polarizations*. Indeed, the map $\mathrm{Hom}_{k,\mathrm{sym}}^0(A, A^\vee) \to \mathrm{End}^0(A)^+$ given by $\lambda \mapsto \lambda_0^{-1}\lambda$ is an isomorphism (as one easily checks, since λ_0 is a symmetric isogeny). The italicized claim then amounts to the fact that any symmetric isogeny $\lambda : A \to A^\vee$ is a difference of polarizations. Choose your favorite polarization over k, say λ_0. Over $\bar{k}$, λ_0 is associated to an ample line bundle $\mathcal{L}_0$, while λ is associated to some random line bundle $\mathcal{L}$, both via the Mumford construction. For $n \gg 0$ the line bundle $\mathcal{L}_0^{\otimes n} \otimes \mathcal{L}$ on $A_{\bar{k}}$ is ample, from which it follows that the symmetric k-isogeny $\lambda + n\lambda_0$ is a polarization, proving the claim.

(Variant: avoid the above considerations by setting L to be the $\mathbf{Z}$-lattice in $\mathrm{End}_k^0(A)^+$ given by $L' + (L')^\dagger$ for $L' = (\frac{1}{\deg\lambda_0}\mathrm{End}_k(A)) \cap \mathrm{End}_k^0(A)^+$.)

Thus $L \subset \mathrm{End}_k^0(A)^+$ is an $\mathrm{Aut}_k(A) = \mathrm{End}_k(A)^\times$-stable $\mathbf{Z}$-lattice in $E := \mathrm{End}_k^0(A)$. It suffices to show that $\{\lambda \in L \cap \mathrm{End}_k(A)^\times : \mathrm{Nrd}(\lambda) \leq N\}/\mathrm{Aut}_k(A)$ is finite. This finiteness is a special case of the next proposition, applied to $E, (-)^\dagger$, L, and $R = \mathrm{End}_k(A)$.

Proposition 4.1. *Let E be a finite dimensional semisimple $\mathbf{Q}$-algebra with an involution $(-)^\dagger$. Let $R \subset E$ be a $\mathbf{Z}$-order and $L \subset E^+ := E^{\dagger=\mathbf{1}}$ a $\mathbf{Z}$-lattice stable under the action of $R^\times$ on E by $\alpha.u = u^\dagger\alpha u$. Then $\{\lambda \in L \cap E^\times : |\mathrm{Nrd}(\lambda)| \leq N\}/R^\times$ is finite.*

Remark 4.2. We remind the reader that an *involution* on a finite-dimensional semisimple algebra E over a field k is a k-linear automorphism $a \mapsto a^\dagger$ of E such that $(ab)^\dagger = b^\dagger a^\dagger$.

The proof of Proposition 4.1 will rest on a deep theorem from the theory of arithmetic groups. To make the link with arithmetic groups, observe that the reduced norm $\mathrm{Nrd} : E \to \mathbf{Q}$ is a polynomial map, and as such it naturally induces B-algebra maps $E_B = E \otimes_{\mathbf{Q}} B \to B$ for any $\mathbf{Q}$-algebra B. By expressing the $\mathbf{Q}$-algebra structure on E in terms of structure constants, and expressing the unit condition as the invertibility of the reduced norm, we get a natural linear algebraic group

$$\underline{E}^\times = \text{“}E^\times \text{ viewed as a } \mathbf{Q}\text{-group”}$$

as well as a $\mathbf{Q}$-homomorphism $\mathrm{Nrd} : \underline{E}^\times \to \mathbf{G}_m$ (which on B-points is the map $E_B^\times \to B^\times$ induced by the reduced norm). Moreover, consideration of structure constants relative to a $\mathbf{Z}$-basis of R shows that for varying $\lambda \in L$, the reduced norm $\mathrm{Nrd}(\lambda) \in \mathbf{Q}$ has *bounded* denominator. Thus, for the finiteness assertion in Proposition 4.1 we lose no generality by

replacing the condition "$|\mathrm{Nrd}(\lambda)| \leq N$" (for some integer $N > 0$) with "$\mathrm{Nrd}(\lambda) = q$" for a fixed $q \in \mathbf{Q}^\times$.

Define the (disconnected) closed $\mathbf{Q}$-subgroup $G = \mathrm{Nrd}^{-1}(\mu_2)$, so $\Gamma := R^\times$ is a subgroup of $G(\mathbf{Q})$ (since the reduced norm carries $R^\times$ into $\mathbf{Z}^\times = \{\pm 1\}$). Since $\underline{E}^\times$ is reductive over $\mathbf{Q}$ (as we may check over $\overline{\mathbf{Q}}$, where every central simple algebra becomes a product of matrix algebras), clearly G is also reductive.

Let V be E^+ as a representation of G via the action $\alpha \mapsto u^\dagger \alpha u$ (which preserves Nrd for $u \in G$, precisely due to the definition of G).

Lemma 4.3. *The G-orbits X in $V \cap E^\times$ are precisely the level-sets for* Nrd *on V for invertible values of* Nrd*. In particular, these orbits are Zariski-closed in V.*

Proof. By computing on $\overline{\mathbf{Q}}$-points, it suffices to show that if $\alpha, \alpha' \in E_{\overline{\mathbf{Q}}}$ are fixed by the involution and have the same nonzero reduced norm $q \in \overline{\mathbf{Q}}$ then they lie in the same $G(\overline{\mathbf{Q}})$-orbit. By scaling α and α' by a common root extraction of q in $\overline{\mathbf{Q}}^\times$, we are reduced to checking that G acts transitively on the level set $\{\mathrm{Nrd} = 1\}$in $E^+_{\overline{\mathbf{Q}}}$. In fact, we claim that this level set consists of the elements $a^\dagger a$ where $\mathrm{Nrd}(a) = 1$. This is proved via an easy case-by-case consideration with the classification of semisimple algebras with involution over an algebraically closed field of characteristic 0. See 18.5 in Milne's "Abelian Varieties" article for this analysis (which rests on systematic applications of the Skolem–Noether theorem); there are only a few cases, so the case-wise analysis is rather straightforward. (Types B and C in Milne's list respectively correspond to the classification of non-degenerate quadratic forms and non-degenerate symplectic forms over an algebraically closed field of characteristic 0.) ■

Due to the closedness of orbits in Lemma 4.3, we see that Proposition 4.1 is a special case of the following deep result, for which we simply give a reference for a proof.

Theorem 4.4 (Borel, Harish–Chandra)**.** *Let G be a (possibly disconnected) reductive algebraic group over $\mathbf{Q}$, let $\Gamma \subset G(\mathbf{Q})$ be an arithmetic subgroup.*[1] *Let $\rho : G \to \mathrm{GL}(V)$ be a representation of G on a finite-dimensional $\mathbf{Q}$-vector space V, $L \subset V$ a Γ-stable $\mathbf{Z}$-lattice, and $X \subset V$ be a Zariski-closed G-orbit. Then $\Gamma\backslash(L \cap X(\mathbf{Q}))$ is finite.*

Proof. An elegant treatment is given in Borel's remarkable book "Introduction aux groupes arithmetiques", where this result appears as Theorem 9.11. It rests on nearly everything that comes before it in that book. ■

Remark 4.5. The proof of Theorem 4.4 given in Borel's book relies on a general result of Mostow concerning the behavior of Cartan involutions with respect to finite chains of inclusions among reductive $\mathbf{R}$-groups. Borel states the precise result at the start of §9.11 in his book, with references provided at the end of Chapter 9. I found that it requires a lot of effort to unravel the content of the proof of this result of Mostow, depending on one's background related to the Lie-theoretic and connectedness aspects of linear algebraic $\mathbf{R}$-groups,

[1]Recall that this means a subgroup commensurable with $G(\mathbf{Q}) \cap \mathrm{GL}_n(\mathbf{Z})$ for one, or equivalently any, faithful representation $G \hookrightarrow \mathrm{GL}_n$. "Commensurable" means that the intersection of the two groups in question has finite index in each of them. There are more intrinsic definitions of what it means for a subgroup to be arithmetic.

especially to make the inductions work without getting overwhelmed by complications arising from the distinction between reductive groups and semisimple groups. For instance, the theory of Cartan involutions in the semisimple case is intrinsic to the real-analytic theory, whereas in the reductive case it relies on the algebraic aspects of the situation.

The serious content of Mostow's proof lies in his article "Some new decomposition theorems for semisimple groups" in AMS Memoirs 14 (1955) that is hard to read (since it was written at a time when the algebraic aspects of the theory of linear algebraic groups over $\mathbf{R}$ was not yet fully developed, so most ideas are expressed in terms of semisimple Lie algebras over $\mathbf{R}$ and $\mathbf{C}$). I have hand-written notes which develop the entire topic from scratch, culminating in the result of Mostow that Borel states at the start of §9.11 in his book, but it is too onerous for me to type that up here.

5. Reduction of Theorem 3.3 to the theorem of Borel and Harish-Chandra

To conclude our discussion, we explain how to deduce Theorem 3.3 from Theorem 4.4. Letting A be an abelian variety over a field F, a direct factor of A as an abelian variety arises from a choice of idempotent $e \in R := \mathrm{End}_F(A)$, and if two idempotents $e, e' \in R$ satisfy $e' = u^{-1}eu$ for some $u \in R^\times$ then the corresponding direct factors are abstractly isomorphic as abelian varieties over F (with u providing the isomorphism). Thus, it suffices to prove:

Proposition 5.1. *For any order R in a finite-dimensional semisimple $\mathbf{Q}$-algebra E, the action of $R^\times$ on the set of idempotents in R via conjugation has only finitely many orbits.*

Proof. Let G be the reductive $\mathbf{Q}$ group $\underline{E}^\times$, so $\Gamma := R^\times$ is an arithmetic subgroup of $G(\mathbf{Q})$ and $V := E$ is a linear representation space for G via conjugation. The lattice $L = R$ in this representation space is stable under the action of Γ. By Theorem 4.4, it suffices to show that each idempotent in E has G-orbit in V that is Zariski-closed. Upon decomposing E into a direct product of simple $\mathbf{Q}$-algebras, G and V decompose correspondingly. Thus, we reduce to the case that E is simple, so it is a central simple K-algebra of some rank n^2 over a number field K.

First consider the situation over $\overline{\mathbf{Q}}$. Upon identifying $E_{\overline{\mathbf{Q}}}$ with a product $\prod \mathrm{M}_n(\overline{\mathbf{Q}})$ of matrix algebras, indexed by the embeddings σ of K into $\overline{\mathbf{Q}}$, G becomes the corresponding power of GL_n, and the G-orbits of idempotents are parameterized by collections of integers (r_σ) with $0 \leq r_\sigma \leq n$. Explicitly, r_σ is the rank of the σ-component e_σ of the idemponent $e = (e_\sigma)$, and this corresponds to the simultaneous collection of conditions $\mathrm{rank}(e_\sigma) \leq r_\sigma$ and $\mathrm{rank}(1 - e_\sigma) \leq n - r_\sigma$ for all σ (with e_σ conjugate to a diagonal matrix whose first r_σ entries are 1 and the rest are 0; combine a basis of $\ker e_\sigma$ and $\mathrm{im}(e_\sigma)$, and use that $e_\sigma^2 = e_\sigma$). These rank bounds amount to a Zariski-closed condition, namely the vanishing of many determinants. Thus, over $\overline{\mathbf{Q}}$ we have shown that there are finitely many G-orbits, with each orbit closed for the Zariski topology.

For an idempotent $e \in E$, the corresponding idempotent in $E_{\overline{\mathbf{Q}}}$ corresponds to parameters r_σ that all coincide with a common r. The G-orbit over $\overline{\mathbf{Q}}$ corresponding to the parameters $r_\sigma = r$ for all σ is Zariski-closed and descends to an orbit over $\mathbf{Q}$ (namely, the orbit of e). ∎