LECTURES ON SHIMURA CURVES 4.5: A CRASH COURSE ON LINEAR ALGEBRAIC GROUPS

PETE L. CLARK

It is an initially surprising fact how much of the geometry and arithmetic of Shimura varieties (e.g., moduli spaces of abelian varieties) is governed by the theory of *linear* algebraic groups. This is in some sense unfortunate, because the theory of algebraic groups (even over the complex numbers, and still more over a nonalgebraically closed field like $\mathbb{Q}$) is rich and complicated, containing for instance the entire theory of Lie groups, Lie algebras and representations.

To acquire a real mastery of this material requires substantial quiet time with a book such as [**?**]. The purpose of these notes is to acquaint the reader with the basic outlines of this theory. What we give is somewhere between a language lesson and a guided tour.

We will work over the context of a field K of characteristic zero. Some of the results would still be valid by requiring K to be merely perfect (or even an arbitrary field), but the theory in positive characteristic has some crucial differences that we do not want to discuss.

0.1. **Definition of algebraic group.** An algebraic group $G_{/K}$ is just an algebraic K-variety together with morphisms $m : G \times G \to G$ and $i : G \to G$ which satisfy the usual group axioms. (There is an interpretation of this in terms of commutativity of diagrams, corresponding to the notion of a "group object in a category." Or one can interpret this in terms of the functor of points: for any K-algebra A, the induced maps $m : G(A) \times G(A) \to G(A)$, $i : G(A) \to G(A)$ give a group law on $G(A)$, such that a homomorphism $A \to B$ of K-algebras induces a homomorphism of groups $G(A) \to G(B)$.)

0.2. **Weil restriction.** Let L/K be a finite field extension,[1] and suppose that $X_{/L}$ is an algebraic variety. There is a canonical way to get from X an algerbraic variety $R_{L/K}(X)$ defined over K, called the **Weil restriction** (or "restriction of scalars"). Moreover, if $X = G_{/L}$ is an algebraic group (by far the most useful special case), then it shall follow formally that $R_{L/K}(G)$ has the structure of an algebraic K-group. Before giving the abstract definitions / constructions, let us give a rough description of the process. Assume for simplicity that $X_{/L}$ is affine, so is embedded in some affine space $\mathbb{A}^N_{/L}$ as the zero locus of a collection of polynomials $P_i(X_1, \ldots, X_N) \in L[X_1, \ldots, X_N]$. Suppose $[L : K] = d$. We may view $\mathbb{A}^N(L) = L^N$ as an Nd-dimensional vector space over K. (In essence, then, the

[1]Note that, because of our running convention that K has characteristic 0, it goes without saying that L/K is separable. The definition that we are about to give uses the separability. On the other hand, it is possible to give a definition also in the purely inseparable case (which suffices for the general case, by "dévissage.") This is done in, e.g., Fried and Jarden's *Field Arithmetic*.

first step of the construction is to decree that $R_{L/K}(\mathbb{A}^N) \cong \mathbb{A}^{Nd}_{/K}$.) Choose a basis $\alpha_1, \ldots, \alpha_d$ of L/K. Using this basis and the "change of variables" $X_i = \sum_{i=1}^d \alpha_i Y_i$, we can regard each polynomial equation $P(X_i) = 0$ with L-coefficients as being d polynomial equations with K-coefficients. The resulting system of polynomials cuts out a closed subvariety of $\mathbb{A}^{Nd}_{/K}$, and that variety is $R_{L/K}(X)$.

Example: $R_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)$. The affine ring for $\mathbb{G}_{m/\mathbb{C}}$ is $\mathbb{C}[X_1, X_2]/(X_1X_2 - 1)$. Using the basis $\{1,\ i\}$ for $\mathbb{C}/\mathbb{R}$, we write $X_1 = Y_1 + iY_2$, $X_2 = Y_3 + iY_4$. Then our single relation $X_1X_2 - 1 = 0$ becomes

$$Y_1Y_3 - Y_2Y_4 - 1 = 0,$$

$$Y_1Y_4 + Y_2Y_3 = 0.$$

If we assume that $Y_1 \neq 0$, we can eliminate Y_3 and Y_4 and Y_2 can be arbitrary. If $Y_1 = 0$, then we get $1 + Y_2Y_4 = 0$, so again we can eliminate Y_4 as long as $Y_2 \neq 0$. In other words, the variety is isomorphic to the set of pairs of real numbers $(Y_1, Y_2) \neq (0, 0)$, or to $\mathbb{C}^\times$. (We will not carry out a similar discussion for the equations of the group law, since that would carry us into the realm of Hopf algebras: too far afield.)

Let us now give two abstract characterizations of $R_{L/K}(X)$.

(WR1): We will give the functor of points of $R_{L/K}(X)$ (which, by general nonsense – "Yoneda lemma" – characterizes the variety $R_{L/K}(X)$ up to isomorphism, but does not show that it exists): namely, for any K-algebra A, $R_{L/K}(X)(A) = X(A \otimes_K L)$. In particular, $R_{L/K}(X)(K) = X(L)$. Note that this is what we saw in the preceding example.

(WR2) We are defining a functor $R_{L/K}$ from the category of L-varieties to the category of K-varieties. There is a more evident functor going in the other direction, namely *extension* of scalars: it is the functor which takes $X_{/K}$ to X_L. Write $\mathrm{Mor}_K(X, Y)$ for the set of all K-morphisms from X to Y. Then the statement is that Weil restriction and scalar extension are adjoint functors: let Y be any K-variety. Then

$$\mathrm{Mor}_L(Y_{/L}, X) = \mathrm{Mor}_K(Y, R_{L/K}(X)).$$

Note that in the special case that $Y = \mathrm{Spec}\, K$ is a single point, this again says that the L-valued points of X are the K-valued points of the scalar restriction.

(WR3) This description is helpful for proving that a variety satisfying (WR1) and (WR2) exists, and is also enlightening about properties of the restriction over extension fields. Let M be the Galois closure of L/K, and $G = \mathrm{Gal}(M/K)$. For $\sigma \in G$, let $X^\sigma = X_M \otimes_\sigma M$. (In other words, regarding X as being defined by a set of polynomials with coefficients in M, X^σ is the variety obtained by applying the automorphism σ to all the coefficients of the equations.) Put $V = \prod_{\sigma \in G} X^\sigma$. Observe that by construction V has the agreeable property of being isomorphic to each of its Galois conjugates V^σ. In fact more is true: for each $\sigma \in G$, there is an automorphism $\psi^\sigma : V^\sigma \to V$ which satisfy the cocycle condition:

$$\psi^{\sigma\tau} = \psi^\sigma \circ \sigma(\psi^\tau).$$

This is precisely Weil's descent condition (which explains the name Weil restriction!), so that Galois descent gives V the structure of a variety over K.

Exercise 1: Show that $V = R_{L/K}(X)$, defined according to (WR1) or (WR2).

A useful special case: suppose L/K is a Galois extension and X is a variety defined over K. Then if we extend, restrict and extend again we

Exercise 2: Convince yourself that if $G_{/L}$ is an algebraic group, then it follows from (WR1) or (WR2) that $R_{L/K}(G)$ has the structure of an algebraic group. get $R_{L/K}(X_{/L})_{/L} \cong {X_{/L}}^{[L:K]}$.

(The following exercise belongs in a much later set of notes, but I put it here in case I forget to put it in later.)

Exercise 3: Let $K = \mathbb{Q}$ and L be a quadratic number field. Let $E_{/L}$ be an elliptic curve, and let $A = R_{L/K}(E)$, so $A_{/\mathbb{Q}}$ is an abelian surface, which over L is isomorphic to $E \times E^{\sigma}$, where σ is the nontrivial automorphism of $L/\mathbb{Q}$.
a) When is A $\mathbb{Q}$-simple?
b) When is A of GL_2-type?

0.3. **Classification I: Chevalley decomposition.** First, an algebraic group need not be connected, but (as with any algebraic variety) it has only finitely many connected components. The connected component G^0 containing the identity element is a normal finite index subgroup of G. Conversely, G/G^0 can clearly be any finite group at all, so in classification results it makes sense to assume that G is connected.

One basic fact about group varieties is that they are quasi-projective. In particular, an algebraic group is complete if and only if it is projective. A projective algebraic group $G_{/K}$ is called an **abelian variety**. In some sense, these are the algebraic groups that we are "really interested in"; we will describe them later in more loving detail.

Example: For any positive integer N, the group GL_N of invertible $N \times N$ matrices with entries in K. This clearly makes GL_N into an algebraic variety, namely the quasi-affine variety given by the complement in $\mathbb{A}^{N^2}$ of the vanishing of the determinant map. In fact it is also an affine variety, and this is a standard trick (namely to show that subset of an affine variety defined by the *non*vanishing of a single function is again an affine variety; in general, open subsets of affine varieties need not be affine): by adding one more variable, we can realize the coordinate ring of GL_N as $K[\{X_{ij}\}_{i \leq i,\ j \leq N}, Y]/(\det X_{ij} \cdot Y - 1)$.

Theorem 1. *For an algebraic group $G_{/K}$, the following are equivalent:*
a) G is an affine K-variety.
b) There exists an embedding $\varphi_{/K} : G \hookrightarrow GL_N$.

That b) $\implies$ a) follows from the above discussion for GL_N. The converse implication is nontrivial; see e.g. [**?**]

Our first classification result says that linear algebraic groups and abelian varieties are the bulding blocks for all algebraic groups.

Theorem 2. *(Chevalley) Every algebraic group $X_{/K}$ admits a unique normal linear algebraic subgroup G such that X/G is an abelian variety.*

Remark: Chevalley's original proof was very difficult, and the more difficult for modern readers because it was couched in the language of algebraic geometry à la Weil (i.e., no schemes). Recently Brian Conrad gave a modern proof [**?**], which is still not easy.

We note (as does Conrad) that algebraic groups which are neither linear nor projective do arise naturally: as special fibers of Néron models of abelian varieties and as Jacobians of singular algebraic curves.

0.4. **Unipotent and solvable groups.** Jordan decomposition: If $g \in GL_N(K)$, then there exists a unique decomposition $g = g_s g_u$ such that g_s is semisimple (i.e., diagonalizable over $\overline{K}$), g_u is unipotent (every eigenvalue is 1), and $g_s g_u = g_u g_s$. Moreover, if $G \subset GL_N$, $H \subset GL_M$ and $f : G \to H$ is a homomorphism of algebraic groups, then $f(g)_s = f(g_s)$ and $f(g_u) = f(g)_u$. In particular, it makes sense to say that an element of an "abstract" affine algebraic group is unipotent or semisimple.

An algebraic group is **unipotent** if it consists entirely of unipotent elements. An example is the group H_N of $N \times N$ matices which are strictly upper triangular: $a_{ij} = 0$ if $i > j$ and $a_{ii} = 1$. Note that H_2 is isomorphic to the additive group $\mathbb{G}_a$ (i.e., the affine line endowed with its natural addition law) but H_N is noncommutative for any $N \geq 3$. In fact any connected unipotent group is isomorphic to a subgroup of H_N for some N. Moreover, a connected unipotent algebraic group admits a composition series each of whose composition factors is $\mathbb{G}_a$.[2]

Solvable groups: Let G' be the closure of the commutator subgroup $[G, G]$. By repeating this process, we get a sequence of groups G', G'', ... If for some n the nth iterated commutator subgroup of G is trivial, G is **solvable**. Over $\overline{K}$, a solvable group can be embedded into the group $T_N \subset GL_N$ of upper triangular matrices (this is the Lie-Kolchin theorem). Moreover, over $\overline{K}$, a connected solvable group is characterized by having a composition series whose factors are all $\mathbb{G}_a$ or $\mathbb{G}_m$.

0.5. **Tori.** Tori: An algebraic group $T_{/K}$ is a (linear!) **torus** if $T_{\overline{K}} \cong \mathbb{G}_m^n$ for some K. Such an isomorphism need not exist over K; if it does, T is said to be K-split.

For any algebraic group $G_{/\overline{K}}$, one defines the character group $X(G) = \mathrm{Hom}(G, \mathbb{G}_m)$. When K is not equal to its algebraic closure, $X(G)$ is endowed with a Galois module structure under the usual (adjoint) action: for any $\sigma \in \mathrm{Gal}_K$,

$$\sigma(\chi)(g) := \sigma(\chi(\sigma^{-1} g)).$$

This has the effect that the invariants $X(G)^{\mathrm{Gal}_K}$ are precisely those homomorphisms $G \to \mathbb{G}_m$ defined over K.

Tori are characterized among algebraic groups by the equality $X(T) \cong \mathbb{Z}^{\dim G}$.

[2]This is false over an algebraically closed field of characteristic p.

Thus the character of tori is (anti-)isomorphic to the category of Galois modules whose underlying abelian group is free of finite rank. Better yet, there is an **isogeny category** of tori where the objects are tori and the morphisms are the usual homomorphisms between tori (which form a free abelian group) tensored with $\mathbb{Q}$. Thus, the isogeny category of tori is anti-(isomorphic) to the category of finite-dimensional (continuous) representations of Gal_K on $\mathbb{Q}$-vector spaces. This is a semisimple category (this is essentially Maschke's theorem).

As an application of this: a torus T is **anisotropic** if $X(T)^{\mathrm{Gal}_K} = 1$, i.e., there are no nontrivial characters defined over K. By duality, $X(T)^{\mathrm{Gal}_K}$ defines a quotient T' of T on which Galois acts trivially (i.e., T' is split). The kernel of the map $T \to T'$ is an anisotropic torus, say T_a. Now the semisimplicity of the isogeny category implies that T is isogenous to $T_a \times T'$, the product of an anisotropic torus and a split torus.

Example: Let L/K be a finite field extension of degree n, and let $T = R_{L/K}(\mathbb{G}_{m/L})$. It follows from (WR3) that T is a torus which splits over M, the Galois closure of L/K. (In fact, since M is the minimal field extension of K for which $M \otimes_K L \cong L^n$), M is the minimal splitting field for T. Let $\mathfrak{g} = \mathrm{Gal}(M/K)$ and $\mathfrak{h} = \mathrm{Gal}(M/L)$. Then the character group $X(T)$ is, as a $\mathbb{Z}[\mathfrak{g}]$-module, isomorphic to $\mathbb{Z}[\mathfrak{g}/\mathfrak{h}]$. Note that the norm map $N : L^\times \to K^\times$ can be viewed as a K-rational character of T. Let $R^1_{L/K}(\mathbb{G}_m)$ be the kernel of this map. On characters, the norm map corresponds to the map $\mathbb{Z} \to \mathbb{Z}[\mathfrak{g}/\mathfrak{h}]$ given by $1 \mapsto \iota = \sum \sigma\mathfrak{h}$, the augmentation ideal. Because the $\mathfrak{g}$-action is the natural permutation action on the coset space, it is easy to see that this is in fact the largest submodule on which $\mathfrak{g}$ acts trivially. In other words, $R^1_{L/K}(\mathbb{G}_m)$ is the maximal anisotropic subtorus of T.

Exercise 4: Let $T_{/\mathbb{R}}$ be an algebraic torus. Show that T is **isogenous** to $R^1_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)^a \times \mathbb{G}_m^b$ for some non-negative integers a and b. What is the corresponding result for classification up to isomorphism?

0.6. **Semisimple and reductive groups.** From now on, all our algebraic groups will be linear and connected.

Definition: The **radical** $R(G)$ of an algebraic group $G_{/K}$ is the maximal connected, solvable, normal subgroup of G.

Definition: The **unipotent radical** $R_u(G)$ of an algebraic group $G_{/K}$ is the maximal connected, solvable, normal subgroup of G.

Note that because unipotent groups are solvable, $R_u(G) \subset R(G)$.

We say that a group is **semisimple** if $R(G) = 0$ and **reductive** if $R_u(G) = 0$.

Remark: Because $R(G)$ and $R_u(G)$ are *unique*, an easy Galois descent implies that $R(G_{/K})_{/\overline{K}} = R(G_{\overline{K}})$ and similarly for the unipotent radical. In particular, an algebraic group over K is semisimple (resp. reductive) if and only if its extension to $\overline{K}$ is.

Theorem 3. *Let $G_{/K}$ be reductive.*
a) $R(G) = Z(G)^0$ is an algebraic torus.
b) $G' = [G, G]$ is semisimple.
c) $G = G'R(G)$ with $G' \cdot r(G)$ finite.

In other words, the only difference between a reductive group and a semisimple group is that a reductive group may have a nontrivial center, which must be an algebraic torus.

Theorem 4. *(Mostow) Let G be a linear algebraic group. Then there exists a reductive subgroup H of G, such that G is the semidirect product of $R_u(G)$ and H. The group H is unique up to conjugacy.*

Remark: The above semidirect product decomposition is referred to as the "Levi decomposition," and the group H is often referred to as "the Levi."

Example: If G is a commutative linear group, the Levi Decomposition gives $G = U \times T$, the direct product of a unipotent group and a torus.

0.7. **Maximal tori.** Any two maximal tori in a linear algebraic group G are conjugate. The **rank** of G is the dimension of a maximal torus. However, for arithmetic purposes, one also needs to consider the dimension of a maximal K-split torus of G, which is called the **K-rank** of G. (Moreover, G is said to be split if its rank equals its K-rank.) An algebraic group is said to be **anistropic** if it has K-rank 0.

Example: GL_N is a reductive but not semisimple, since its center is $\mathbb{G}_m$, the scalar matrices. A maximal torus is given by the diagonal matrices, which are isomorphic to $\mathbb{G}_m^N$. Thus GL_N is split, with rank equals K-rank equals N. Its derived subgroup is SL_N, which is semisimple, split and of rank equals K-rank equals $N-1$, as the restriction of a maximal torus of GL_N to SL_N gives a maximal torus of SL_N.

Example: Let B/K be a simple algebra, and let $G = B^\times$. It is not hard to see that G can be viewed as a linear algebraic group over K. By Wedderburn's theorem, we have $M \cong M_n(D)$ where D/K is a division algebra, so $G = GL_n(D)$.

Exercise 5: a) Show that $G_{/K}$ is a reductive group.

b) There exists a K-rational character $N : B^\times \to K^\times$, the "reduced norm." How is it defined? (Hint for both cases: Pass to the algebraic closure.)

We will write $SL_N(D)$ for the kernel of the character N of the preceding exercise.

Proposition 5. *The K-rank of $SL_N(D)$ is equal to $N-1$. In particular, $SL_1(D)$ is anisotropic over K.*

Exercise 6: Prove it.

Further examples (to be written later): SP_{2n}, GSp_{2n}, $O(n)$, $O(p,q)$, $U(p,q)$, ...

References

[1] A. Borel, *Linear Algebraic Groups*, Springer GTM 126.

[2] B. Conrad, *A modern proof of Chevalley's theorem on algebraic groups*, J. Ramanujan Math. Soc. 17 (2002), 1-18.
[3] J. Milne, *Algebraic and Arithmetic Groups*, lecture notes available at jmilne.org.