Survey of the Classification Theory of Semisimple Algebraic Groups Over Perfect Fields

by

Luke Jaskowiak
B.S., University of Illinois at Chicago, 2016

Thesis submitted in partial fulfillment of the requirements
for the degree of Master of Science in Mathematics
in the Graduate College of the
University of Illinois at Chicago, 2019

Chicago, Illinois

Defense Committee:
Ramin Takloo-Bighash, Chair and Advisor
Bhama Srinivasan
Kevin Tucker

ACKNOWLEDGMENTS

Dedicated to my wife for her patience and ability to suffer through my time in higher education as though she were a veritable saint. Thanks to all of my committee members for their time and patience. Thanks to my cohort for their support and many, many conversations about matters both related and unrelated to math.

TABLE OF CONTENTS

CHAPTER **PAGE**

SUMMARY

The focus of this work is to approach the question of the classification of semi-simple algebraic groups over perfect fields from the perspective of I. Satake's published lecture notes on the subject. This work will not cover every aspect of the classification, but will focus on groups with split tori. We will work through detailed examples of K/k-forms and the correspondence between the A_2 Dynkin diagram and the algebraic group $\mathrm{SL}(3, \mathbb{Q})$. If not specified, all definitions are from (1).

CHAPTER 1

INTRODUCTION

1.0.1 Notation

k denotes a field.

k_0 will denote the prime field of k, that is the subfield of k generated by the multiplicative identity 1. For example $\mathbb{Q}_0 = \mathbb{Q}$.

K/k denotes a field extension K over k.

Ω denotes a universal domain, that is a "sufficiently large" algebraically closed field with $k \subseteq K \subseteq \Omega$, for some given base field k and an extension K/k.

$\operatorname{char} k$ denotes the characteristic of a field k.

k^{sep} denotes the separable closure of k.

k^{insep} denotes the inseparable closure of k.

$\mathbb{A}_k^n$ denotes affine n-space over k, as a set $\mathbb{A}_k^n = \{(x_1, \cdots, x_n) | x_i \in k \text{ for } 1 \leq i \leq n\}$

The Galois group of K/k is denoted $\text{Gal}(K/k)$.

$k[x_1, \cdots, x_n]$ will denote the polynomial ring in n variables with coefficients in k.

$k(x_1, \cdots, x_n)$ denotes the field of fractions of $k[x_1, \cdots, x_n]$.

The characteristic exponent of a field k is defined to be 1 if $\operatorname{char} k = 0$ and p if $\operatorname{char} k = p > 0$.

If G is a group and H is a subgroup then $N_G(H)$ denotes the normalizer of H in G, i.e., $N_G(H) = \{g \in G \mid gH = Hg\}$.

If G is a group and H is a subgroup then $Z_G(H)$ denotes the centralizer of H in G, i.e., $Z_G(H) = \{g \in G \mid gh = hg, \forall h \in H\}$.

The group of non-singular linear transformations of a vector space V will be denoted by $\mathrm{GL}(V)$, this will be referred to as the *general linear group of* V.

The group of n by n invertable matrices with coefficients in k will be denoted by $\mathrm{GL}(n, k)$.

$TR(n)$ will denote the group of upper triangular matrices.

1.1 Algebraic Geometry/Groups

1.1.1 First Definitions

Definition 1. $A \subseteq \mathbb{A}_k^n$ is called a *closed algebraic set* if there is a subset $I \subseteq k[x_1, \cdots, x_n]$ so that

$$A = \mathbb{V}(I) = \{x \in \mathbb{A}_k^n | f(x) = 0, \forall f \in I\}.$$

This is also called the *vanishing set* of I, and we denote this as above by $\mathbb{V}(I)$. If A is an closed algebraic set then we denote the ideal generated by polynomials vanishing on A as

$$\mathbb{I}(A) = \{f \in k[x_1, \cdots, x_n] | f(x) = 0, \forall x \in A\}.$$

Hilbert's Basis Theorem implies that every ideal of $R[x]$ is finitely generated and hence the vanishing set of an infinite collection of polynomials can be defined instead by a finite collection of polynomials. More precisely,

Theorem 2. *(Hilbert's Basis Theorem)(2)*

If R is a commutative Noetherian ring, then the polynomial ring $R[x]$ is also Noetherian.

1.1.2 Topology

Definition 3. An algebraic set $A \subseteq \mathbb{A}^n_\Omega$ is *$k-$closed* if A is the set of zeros of some collection of polynomials with coefficients in k, i.e, $A = \mathbb{V}(\{f_1, \cdots, f_k\})$ such that $f_i \in k[x_1, \cdots, x_n]$ for $1 \leq i \leq k$.

An algebraic set A is *defined over* k if $\mathbb{I}(A)$ has a basis of polynomials with coefficients in k, that is $\mathbb{I}(A) = (f_1, \cdots, f_k)$ with $f_i \in k[x_1, \cdots, x_n]$ for $1 \leq i \leq k$. If A is defined over k, then we call k a *field of definition* for A.

Example 4. Consider $\mathbb{Q} \supset A = \{-1, 0, 1\}$. We have that $A = \mathbb{V}(x(x+1)(x-1))$ and $\mathbb{I}(A) = (x, x+1, x-1)$. Thus, A is $\mathbb{Q}-$closed and defined over $\mathbb{Q}$.

Let $A \subset \mathbb{A}^n_k$. Note that if $\mathbb{I}(A) = (f_1, \cdots, f_k)$ then $A \subseteq \mathbb{V}(f_1 f_2 \cdots f_k)$. However each $f_i \in k[x_1, \cdots, x_n]$ so the product is as well. This shows that if A is defined over k then A is $k-$closed. The converse is not true in general.

Example 5. Consider the field $\mathbb{F}_2(t)$, that is, the fraction field of the finite field with two elements adjoin a single transcendental element t. Note that $A := \left\{t^{1/2}\right\} = \mathbb{V}\left(x^2 - t\right)$ and is thus $\mathbb{F}_2(t)-$closed, however $\mathbb{I}(A) = (x - t^{1/2})$ which is not defined over $\mathbb{F}_2(t)$.

Proposition 6. *The $k-$closed algebraic sets induce a topology on $\mathbb{A}^n_\Omega$.*

Proof. Clearly, $\mathbb{V}(0) = \mathbb{A}^n_\Omega$ and $\mathbb{V}(1) = \varnothing$. Now, given $k-$closed algebraic sets $A, B \subseteq \mathbb{A}^n_\Omega$ so that

$$A = \mathbb{V}(\{f_1, \cdots, f_m\}) \text{ and } B = \mathbb{V}(\{g_1, \cdots, g_l\})$$

we have that

$$A \cup B = \mathbb{V}\left(\{f_i g_j | 1 \leq i \leq n, 1 \leq j \leq l\}\right),$$

and

$$A \cap B = \mathbb{V}\left(\{f_i | 1 \leq i \leq n\} \cup \{g_j | 1 \leq j \leq l\}\right).$$

□

We may easily construct am infinite union of closed sets which is not closed as follows.

Let $i \in \mathbb{N}, A_i = \{i\} \subseteq \mathbb{C}$. Then

$$\mathbb{N} = \bigcup_{\mathbb{N}} A_i = \mathbb{V}\left(\prod_{\mathbb{N}} (x - i)\right)$$

But $\prod_{\mathbb{N}}(x - i)$ does not have finite degree and is thus not a polynomial.

We call this topology the *Zariski k-topology*. In the case where $k = \Omega$ we will simply refer to it as the *Zariski topology*. Often we will call the open and closed sets in this topology as *k-open* and *k−closed*. Of particular importance are the k-closed algebraic sets which are irreducible.

Definition 7. Let A/k be a closed algebraic set. The set A is irreducible if $A = A_1 \cup A_2$ for non-empty algebraic sets A_1, A_2 implies that $A = A_1$ or $A = A_2$. We call A an *algebraic variety*.

We may also show that is A is irreducible if and only if $\mathbb{I}(A)$ is prime.

Remark. It is a general fact of point-set topology that an irreducible set is also connected.

It should be noted that these topologies are not Hausdorff. As an example, consider $\mathbb{C}$ with the Zariski topology. Every polynomial has a finite number of roots in $\mathbb{C}$, and in particular we

note that the closed sets in this case are $\varnothing, \mathbb{C}$, or finite sets in $\mathbb{C}$. In particular this is exactly the co-finite topology on $\mathbb{C}$ which is not Hausdorff.

The following example is a useful summary of the concepts discussed so far.

Example 8. Consider $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \overline{\mathbb{Q}}$. Let $i = \sqrt{-1}$, $A = \{1\}, B = \left\{1, \sqrt{2}\right\}$, and $C = \left\{1, \sqrt{2}, i\right\}$.

- Let $A = \mathbb{V}(x-1)$, then A is $\mathbb{Q}-$closed, $\mathbb{Q}[\sqrt{2}]-$closed, and trivially $\overline{\mathbb{Q}}-$closed. Since $\mathbb{Q}$ is perfect, A is defined over each of these fields as well. Furthermore, A is a closed set in each of the associated topologies.
- Let $B = \mathbb{V}\left((x-\sqrt{2})(x-1)\right)$. However, $(x-\sqrt{2})(x-1) = x^2 - (1+\sqrt{2})x + \sqrt{2} \notin \mathbb{Q}[x]$ and thus B is not $\mathbb{Q}-$closed. However, B is clearly closed over $\mathbb{Q}[\sqrt{2}]$ and $\overline{\mathbb{Q}}$.
- Let $C = \mathbb{V}\left((x-1)(x-\sqrt{2})(x-i)\right)$. $(x-1)(x-\sqrt{2})(x-i) \notin \mathbb{Q}[x]$ or $\mathbb{Q}[\sqrt{2}][x]$ so C is not closed in either of the associated topologies.

1.1.3 Maps

Definition 9. Let A be an algebraic set in $\mathbb{A}^n_\Omega$. A *polynomial function on A defined over Ω* is a polynomial in $\Omega[x]$ restricted to A. A *rational function on A defined over Ω* is the restriction to A of a function defined by a rational quotient f/g in $\Omega(x)$ with g not identically 0 on each irreducible component of A. Furthermore, we may define a *polynomial/rational function on A defined over* for any $k \subset \Omega$ in a similar manner, but with the extra condition that the polynomials have coefficients in k.

Definition 10. Let $A \subseteq \mathbb{A}^n_\Omega$ be algebraic. For any subfield $k \subseteq \Omega$ we denote the *ring of polynomial functions on A defined over k* by $k[A]$, and denote *the ring of rational functions on A defined over k* by $k(A)$. In the case where $k = \Omega$ we will simply drop "defined over k." In particular we have a canonical identification of $\Omega[A] \cong \Omega[X]/\mathbb{I}(A)$ we call this the *coordinate ring* of A.

As noted earlier, if A is irreducible then $\mathbb{I}(A)$ is prime so $\Omega[A]$ is an integral domain. In this case $\Omega(A)$ is the field of fractions of $\Omega[A]$.

Definition 11. Let A, B be closed sets in $\mathbb{A}^n_\Omega$ and $\mathbb{A}^m_\Omega$, respectively. A *polynomial map* $\phi : A \to B$ is a mapping defined by $\phi = (\phi_1, \cdots, \phi_m)$, $\phi_i \in \Omega[A]$ $1 \leq i \leq m$. We say that ϕ is *defined over k* if $\phi_i \in k[A]$ for $1 \leq i \leq m$ and we denote this by ϕ/k. Analogously, let A, B be closed sets in $\mathbb{A}^n_\Omega$ and $\mathbb{A}^m_\Omega$, respectively. A *rational map* $\phi : A \to B$ is a mapping defined by $\phi = (\phi_1, \cdots, \phi_m)$, $\phi_i \in \Omega(A)$ $1 \leq i \leq m$. If each ϕ_i is represented by $f_i/g_i \in \Omega(A)$ and $x \in A$ satisfies $g_i(x) \neq 0$ for $1 \leq i \leq m$ then we say that ϕ is *defined at x*, and

$$\phi(x) = (\phi_1(x), \cdots, \phi_m(x)) = \left(\frac{f_i(x)}{g_i(x)}, \cdots, \frac{f_m(x)}{g_m(x)}\right) \in B$$

We say that ϕ is *defined over k* if $\phi_i \in k(A)$ for $1 \leq i \leq m$ and we denote this by ϕ/k.

Definition 12. Let $A \subseteq \mathbb{A}^n_\Omega$ be an algebraic set. Define $A_k = A \cap \mathbb{A}^n_k$, which we call the *k-rational* points of A.

1.1.4 Affine algebraic groups

Definition 13. G is called an *affine algebraic group* if

- G supports a group structure.
- G is an algebraic set in $\mathbb{A}^n_\Omega$.
- The mapping $\phi : G \times G \to G$ defined by $(x, y) \mapsto x^{-1}y$ is a polynomial map.

  Remark. The previous bullet is equivalent to asking that the map which defines the group operation and the map $g \mapsto g^{-1}$ for $g \in G$ are both *polynomial maps.*

We say G is *defined over* k if G is defined over k as an algebraic set and ϕ/k. This will be denoted as as G/k.

Example 14. We will work through a more involved example momentarily, but for now we consider

1) $\mathbb{G}_a$, by which we denote the additive group of a field k. Note that $\mathbb{G}_a = \mathbb{V}(0)$.
2) $\mathbb{G}_m$; by which we denote the multiplicative group of a field k. The algebraic set structure is given by $\mathbb{V}(xy - 1)$ which identifies $\mathbb{G}_m$ as an algebraic set in $\mathbb{A}^2_k$.

1.1.5 Maps and subgroups

We now may define the algebraic group analogue of rational maps for algebraic sets. Unsurprisingly;

Definition 15. Let G, G' be algebraic groups. A map $\phi : G \to G'$ is called a *rational homomorphism* defined over k if ϕ is both a group homomorphism and a rational map defined over k. We may also use the term $k-$*homomorphism*. If ϕ is a bijective rational $k-$homomorphism

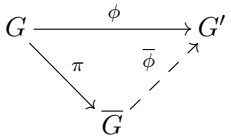
with a rational $k-$homomorphism as an inverse, then we call ϕ a *$k-$rational isomorphism*, and ϕ an automorphism if $G = G'$.

If G, G' are connected then a rational homomorphism $\phi : G \to G'$ which has a finite kernel is called an *isogeny*.

Note that since a rational homomorphism $\phi : G \to G'$ must be defined on all of G it is actually a polynomial map.

Proposition 16. *Assume that N is a normal subgroup of G/k, and N is a closed algebraic subset also defined over k. Then there exists an algebraic group $\overline{G}$ defined over k, and a surjective $k-$homomorphism $\pi : G \to \overline{G}$*

- $\ker \pi = N$
- *If $\phi : G \to G'$ is a $k-$rational homomorphism with $N \subset \ker \phi$, then there exists a unique $k-$homomorphism $\overline{\phi} : \overline{G} \to G'$ so that the following diagram commutes.*



We denote $\overline{G}$ by G/N and call it the quotient group of G by N.

The upshot is that we are justified in our use of "*the* quotient group" G/N since this group is unique up to $k-$isomorphism. Additionally, one can show that $k(G/N)$ is the subfield of $k(G)$ consisting of all $N-$invariant functions. That is to say, the subfield of functions $\psi \in k(G)$

so that $\psi(ax) = \psi(x)$ for all $a \in N$ and $x \in G$. Furthermore, G/N is entirely characterized by this property.

1.1.6 Linear algebraic groups

Assume that V is a vector space of dimension n defined over k. If we take a basis $\{e_1, \cdots, e_n\}$ of V, then there is an isomorphism $\rho : GL(V) \to GL(n, k)$, with respect to the basis, given by

$$\rho(T) = \begin{bmatrix} \vdots & | & \vdots & | & \vdots \\ T(e_1) & | & \cdots & | & T(e_n) \\ \vdots & | & \vdots & | & \vdots \end{bmatrix}.$$

Namely, we apply T to each basis element $\{e_1, \cdots, e_n\} \subset V$ and write the images as column vectors. The resulting matrix $\rho(T)$ then gives us an identification of T with an element of $\mathrm{GL}(n, k)$. Since we may take a different basis for V we note that this identification is only unique up to an inner automorphism given by the change of basis matrix.

Definition 17. A subgroup $G \subseteq GL(V)$ is a *linear algebraic group defined over* k if, under the isomorphism described above, we have that $\rho(G)$ is an affine algebraic group defined over k.

To clarify, this definition says if we have a subgroup $G \subseteq GL(V)$ which, after a choice of a basis for V, is isomorphic to an *affine* algebraic group in $\mathbb{A}^n_k$, then G is a *linear* algebraic group. That is, for some $n \in \mathbb{N}$ and some field k we can find some embedding for every linear algebraic group into $GL(n, k)$. The next theorem grants us that the two notions of *affine* and *linear* algebraic groups are essentially equivalent.

Theorem 18. *Any affine algebraic group may be realized as an algebraic subgroup of of some $GL(V)$, and as such it is a linear algebraic group.*

1.1.7 A Little Representation Theory

Definition 19. Let G be a group and V be a vector space. A *representation of* G in V is a map ϕ taking

$$G \ni g \mapsto \phi(g) : V \to V,$$

That is, $\phi : G \to \mathrm{GL}(V)$ so that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.

Alternatively, given a group G and a vector space V defined over k we may consider a representation of G to be a map $\rho : G \times V \to V$ so that:

- for all $g \in G$ the map $\rho(g) : V \to V$ defined by $v \mapsto \rho(g, v)$ is linear over k;
- $\rho(\mathrm{id}_G, v) = v$ for all $v \in V$; and,
- if $g_1, g_2 \in G$ then for any $v \in V$ we have $\rho(g_1, \rho(g_2, v)) = \rho(g_1 g_2, v)$

Definition 20. M be a commutative group and G be a group. Then M is a left $G-$module if there is a left group action $\rho : G \times M \to M$ so that if $a, b \in M, g \in G$ then

$$g \cdot (a + b) = \rho(g, a + b) = \rho(g, a) + \rho(g, b) = g \cdot a + g \cdot b$$

using the notational convention $\rho(g, x) = g \cdot x$.

Caution: The previous nomenclature unfortunately clashes with that of $R-$modules where R is a ring. In this paper, the only "modules" we are concerned with are 1) $\mathbb{Z}$ modules as ring-modules and 2) $\Gamma-$modules as defined above, where Γ is some Galois group.

1.1.8 Tori

Definition 21. An algebraic group G is called a *torus* if, for some n, there exists an isomorphism $\phi : G \to (\mathbb{G}_m)^n$. We call G either *$k-$trivial or split over k* if G is defined over k and ϕ is defined over k.

Definition 22. Let T be a torus defined over k. A *character of T* is a homomorphism $\chi : T \to \mathbb{G}_m$. Note that the set of characters forms a commutative group under pointwise multiplication.

Henceforth, T will denote a torus and $X(T)$ will be the group of characters of T if we wish to specify the torus. In practice we will abbreviate $X(T)$ to X if the context allows. In following with tradition we will use additive notation for the character group i.e. $(\chi_1+\chi_2)(t) = \chi_1(t)\chi_2(t)$ for $\chi_1, \chi_2 \in X(T), t \in T$. This makes it clear that $X(T)$ is a $\mathbb{Z}$-module, since $X(T)$ is a commutative group under this operation.

Example 23. The group of diagonal matrices $D(n) \subseteq GL(n,k)$ is a torus isomorphic to $\mathbb{G}_m^n$ in Ω^{n+1} with $D(n)$ an algebraic set defined by $\mathbb{V}((x_1 x_2 \cdots x_n y - 1))$. Thus $D(n)$ is defined over k_0 as an algebraic group and the isomorphism $\phi : D(n) \to (\mathbb{G}_m)^n$ which is given by

$$\phi \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & \vdots \\ \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix} = (a_1, a_2, \cdots, a_n)$$

If we consider $D(n)$ as a subset of $\mathbb{A}_k^{n^2}$ then the map ϕ is is also defined over k_0. Therefore, by definition $D(n)$ splits over the prime field k_0.

Now assume that $T \cong (\mathbb{G}_m)^n$. We have n canonical characters χ_i of T defined as "projections", that is if $x = (x_1, \cdots x_n) \in T$ then $\chi_i(x) = x_i$. Let $I = (x_1, \cdots, x_n, y)$. Under the identification $\Omega[T] = \Omega[x_1, \cdots, x_n, y]/I$, the character χ_i is identified with $x_i \pmod I$, and the function $(\prod_{i=1}^n \chi_i)^{-1}$ is identified with $y \pmod I$. These identifications give us the following three facts:

1) $\Omega[T] = \Omega[\chi_1^{\pm 1}, \cdots, \chi_n^{\pm 1}]$

2) $\Omega(T) = \Omega(\chi_1, \cdots, \chi_n)$ is a purely transcendental extension of Ω.

3) X is the subset of monomials $\chi_1^{m_1} \cdots \chi_n^{m_n}$ in $\Omega[T]$ with $m_i \in \mathbb{Z}$.

This last fact shows that as $\mathbb{Z}$-module, $X \cong \mathbb{Z}^n$.

From this proposition we see that if $\Gamma = \mathrm{Gal}(\Omega/k)$, then we have an action of Γ on X by applying $\sigma \in \Gamma$ to the coefficients of the elements of X. Since each $\sigma \in \Gamma$ is in particular

an isomorphism of Ω we have that $(a+b)^\sigma = (a)^\sigma + (b)^\sigma$. Therefore, X is a $\Gamma-$module by definition.

Example 24. Let

$$M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a, b \in \mathbb{R}, a^2 + b^2 \neq 0 \right\}.$$

It can easily be shown that M is a torus defined over $\mathbb{R}$ and there exist two maps $f_i : M \to \mathbb{C}^*, i \in \{1, 2\}$ defined by $f_1(m) = a + bi$, $f_2(m) = a - bi$ for $m \in M$. Clearly f_1, f_2 are elements of $X(T)$. Now let $\Gamma = \operatorname{Gal} \mathbb{C}/\mathbb{R}$. We know that $\Gamma \cong \mathbb{Z}/2\mathbb{Z}$ and the only non-trivial action is complex conjugation. Over $\mathbb{C}$ complex conjugation is not given by a polynomial, but over $\mathbb{R}$ we can realize it as a polynomial defined by $\sigma(a, b, -b, a) = (a, -b, ba)$. As such, σ takes $a + bi$ to $a - bi$.

Now assume that X is a $\Gamma-$module and the group of characters of T. Analogous to the correspondence between sets of points in affine space and ideal of polynomials vanishing on these sets there is a type of duality between certain submodules of X which are torsion-free and algebraic subgroups of T. Toward establishing this correspondence let $T_1 \subseteq T$ be a closed subgroup and define a submodule $T_1^\perp \subseteq X$ as

$$T_1^\perp = \{\chi \in X | \chi(t) = 1, \forall t \in T_1\}$$

For a submodule $X_1 \subseteq X$ define a closed subgroup $X_1^\perp \subseteq T$ as

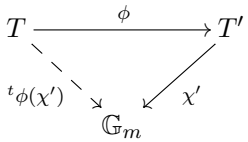
$$X_1^\perp = \{t \in T | \chi(t) = 1, \forall \chi \in X_1\}$$

We then have the following proposition.

Proposition 25.

- *The maps $T_1 \to T_1^\perp$ and $X_1 \to X_1^\perp$ define reciprocal bijections between the closed subgroups of T and the set of submodules of X satisfying the condition that X/X_1 has no p-torsion, where p is the characteristic of the prime field. However, if $p = 0$ there there is no condition on torsion.*
- *Let $T_1 \subseteq T$ be a closed subgroup. Then T_1 is connected if and only if X/X_1 has no torsion, where $X_1 = T_1^\perp$. Furthermore, T_1 is a torus if and only if it is connected.*
- *$X(T_1) = X/X_1, X(T/T_1) = X_1$ where $X_1 = T_1^\perp$ and $T_1 = x_1^\perp$.*

One may notice at this point that given tori T and T' with character modules X, X', $\chi' \in X'$ and a homomorphism $\phi : T \to T'$ we have the diagram



where we define ${}^t\phi : X' \to X$ by ${}^t\phi(\chi') = \chi' \circ \phi$. Note that for any $\chi_1', \chi_2' \in X'$ we have that

$${}^t\phi((\chi_1' + \chi_2')) = (\chi_1' + \chi_2') \circ \phi = \chi_1' \circ (\phi) + \chi_2' \circ (\phi) = {}^t\phi(\chi_1') + {}^t\phi(\chi_2')$$

Thus, ${}^t\phi$ is a $\Gamma-$module homomorphism

Conversely, if $\psi : X' \to X$ is a $\Gamma-$module homomorphism, then there exists a rational homomorphism $\phi : T \to T'$ so that $\psi = {}^t\phi$. Let $T = (\mathbb{G}_m)^n$ and $T' = (\mathbb{G}_m)^k$. Thus X has a basis $\{\chi_1, \cdots, \chi_n\}$ and X' has a basis $\{\chi_1, \cdots, \chi_k\}$, so there corresponds to ψ a matrix with integer coefficients m_{ij} where

$$\psi(\chi_i') = \sum_{j=1}^{n} m_{ij}\chi_j \text{ , where } 1 \leq i \leq k$$

ϕ is then defined as the mapping sending $(x_1, \cdots, x_n)$ to the element of in T' whose i^{th} coordinate is $\prod_{j=1}^{n} x_j^{m_{ij}}$. So $\phi : T \to T'$ is a rational homomorphism and $\psi = {}^t\phi$. We can see now that this gives us a one-to-one correspondence between homomorphisms of tori and homomorphisms of their character modules. What remains to be seen is whether or not this correspondence respects the field of definition of a homomorphism of tori.

Furthermore, one can show:

Proposition 26. *Let $\phi : T \to T'$ be a homomorphism, and p the characteristic of the prime field. Then*

- $(\operatorname{im}\phi)^\perp = \ker({}^t\phi)$ *so ϕ is surjective if and only if ${}^t\phi$ is injective.*
- $\ker\phi = (\operatorname{im}({}^t\phi))^\perp$*, so ϕ is injective if and only if $[X : {}^t\phi(X')]$ is a power of p.*

In particular, if $\dim T = \dim T'$ *then*

The following are equivalent .

- *ϕ is an isogeny.*

- ϕ *is surjective.*
- ${}^t\phi$ *is injective.*
- $|\ker\phi| < \infty$.
- $|\operatorname{coker}{}^t\phi| < \infty$.

Furthermore, if ϕ is an isogeny then $\deg\phi = [X : {}^t\phi(X')]$ so that ϕ is an isomorphism if and only if ${}^t\phi$ is an isomorphism.

Example 27. As an example let T be a torus defined over $\mathbb{F}_q$, and ϕ be the Frobenius endomorphism, $\phi : \mathbb{F}_q \to \mathbb{F}_q$ given by $\phi(x) = x^q$. New let $\chi \in X$. We use χ^ϕ to denote the character we get by taking q^{th} powers of the coefficients of χ. So then $(\chi(t))^{(q)} = \chi(t^{(q)})$ for $t \in T$. Now $\chi(t)$ is a scalar so then

$$(\chi(t))^{(q)} = (\chi(t))^q = q\chi(t)$$

Thus ${}^t\phi(\chi^{(q)}) = q\chi$. So if χ is defined over $\mathbb{F}_q$ then it follows that ${}^t\phi(\chi) = q\chi$.

Proposition 28. *Let $k \subseteq K$. If T is a torus defined over k, then T splits over k^{sep}.*

Let $k \subseteq \Omega$, and let k^{sep} be the separable closure of k in Ω. Let $\Gamma = \text{Gal}(k^{\text{sep}}/k)$, and T be a torus defined over k. Since there is an isomorphism (defined over k^{sep})) $\phi : T \to (\mathbb{G}_m)^n$, ${}^t\phi$ gives an isomorphism ${}^t\phi : X((\mathbb{G}_m)^n) \to X(T) = X$. Since the canonical characters χ_i are defined over the prime field, the characters ${}^t\phi(\chi_i)$ are defined over k^{sep}. Thus, X has the structure of a Γ module given by letting $\sigma \in \Gamma$ act on $\chi \in X$ by operating on the coefficients. A similar argument gives the following.

Proposition 29. *Let T be a torus defined over k. The following are equivalent..*

- *T is $k-$trivial.*
- *Every $\chi \in X$ is defined over k.*
- *Γ operates trivially on X.*

Furthermore T will split over any finite Galois extension $k \subseteq K$, and we can replace $\Gamma = \mathrm{Gal}_k(k^{\mathrm{sep}})$ by $\mathrm{Gal}_k(K)$ and the result still holds.

This result and the previously established correspondence between homomorphisms of tori and homomorphisms of their character modules can be repackaged nicely into the following proposition.

Proposition 30.

- *Let T be defined over k. If $T_1 \subseteq T$ so that T_1 corresponds to $X_1 \subseteq X$, then T_1 is defined over k if and only if X_1 is a Γ-submodule of X.*
- *Let T, T' be tori defined over k, and $\phi : T \to T'$ be a homomorphism. Then ϕ is defined over k if and only if ${}^t\phi$ is a Γ-homomorphism; in particular, ϕ is a $k-$isomorphism if and only if ${}^t\phi$ is a Γ-isomorphism.*

At this point we have made significant progress to a major theorem, namely;

Theorem 31. *There is a one-to-one correspondence between the category of tori defined over k and the category of finitely generated torsion-free $\Gamma-$modules.*

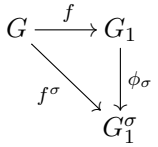
It remains to show that to each $\Gamma-$module X there corresponds a torus T which is unique up to $k-$isomorphism and has a character module $X(T)$ which is isomorphic to X as a Γ-module.

1.1.9 K/k-forms

It is helpful to keep in mind the goal of proving the previous theorem. Otherwise the concept of K/k-forms seems rather abrupt. In that sense, entirety of this section is essentially the remainder of the aforementioned proof.

Definition 32. Let k and K be subfields of Ω. and G_1 and algebraic group defined over K. A pair (G, f) is called a K/k *form of* G_1 if G is an algebraic group defined over k and $f : G \to G_1$ is an isomorphism defined over K. A pair (G, f) is called a k*-form of* G_1 if (G, f) is a K/k-form of G_1 for some extension $k \subseteq K$. We often use the latter terminology in order to suppress the notation and omit reference to the particular extension K/k.

From now on, we will only consider the case where k is perfect, and $k \subseteq K$ is a finite extension. In this case we note that $k^{\text{sep}} = \overline{k}$. Also, define $\Gamma = \text{Gal}_k(\overline{k})$. We begin by investigating how the elements of Γ act on K/k-forms. To this end let (G, f) be a K/k-form of G_1, which will be an algebraic group defined over K. So given $\sigma \in \Gamma$, we have an action of σ on the coefficients of the polynomial mapping f, we denote this map by f^σ. Since G is defined over k and σ is an element of $\text{Gal}_k(\overline{k})$, σ fixes G. Furthermore, $f^\sigma : G \to G_1^\sigma$ is a $\sigma(K)-$isomorphism. Therefore, σ takes a K/k-form (G, f) of G_1 to the $\sigma(K)/k$-form (G, f^σ) of G_1^σ. Now define $\phi_\sigma : G_1 \to G_1^\sigma$ by $\phi_\sigma = f^\sigma \circ f^{-1}$. Diagrammatically



Definition 33. We will call the set of maps ϕ_σ generated as σ varies in Γ a *system of isomorphisms* and denote it $(\phi_\sigma)_{\sigma\in\Gamma}$.

Note that from the definition we have that

1)

$$\phi_\sigma^\tau \circ \phi_\tau = (f^\sigma \circ f^{-1})^\tau \circ f^\tau \circ f^{-1} = f^{\sigma\tau} \circ f^{-\tau} \circ f^\tau \circ f^{-1} = f^{\sigma\tau} \circ f^{-1} = \phi_{\sigma\tau}$$

for $\sigma, \tau \in \Gamma$.

Additionally, f is defined over K, so even though Γ is infinite,

2) each ϕ_σ depends only on the restriction of σ to K.

Since there is a finite such number of such restrictions, we may consider $(\phi_\sigma)_{\sigma\in\Gamma}$ in a similar spirit as a finite system.

Conversely, the following result gives that for any system satisfying 1) and 2) there exists a K/k-form associated to it. We will notate this correspondence by dropping the subscript and calling (ϕ_σ) the system corresponding to a K/k form (G, f).

Theorem 34. *Let G_1 be an algebraic group defined over K and $\{\phi_\sigma\}_{\sigma\in\Gamma}$ be a system of isomorphisms satisfying* 1) *and* 2)*. There there exists a K/k-form (G, f) of G_1 so that $\phi_\sigma = f^\sigma \circ f^{-1}$ for all $\sigma \in \Gamma$.*

we will give a proof of Theorem 34 shortly. In the meantime we continue to investigate K/k-forms towards the goal of proving Theorem 31.

Definition 35. Let (G, f) and (G', f') be k-forms of G_1. We call (G, f) and (G', f') *isomorphic* if there exists an isomorphism $\rho : G \to G'$ which is defined over k.

Note that we have the diagram

$$\begin{array}{ccc} G & \xrightarrow{f} & G_1 \\ \downarrow{\scriptstyle \rho} & & \vdots{\scriptstyle \psi} \\ G' & \xrightarrow{f'} & G_1 \end{array}$$

Since all the maps are isomorphisms which are at worst defined over K we may define an isomorphism $\psi : G_1 \to G_1$ as $\psi = f' \circ \rho \circ f^{-1}$ which is defined over K. Now let (ϕ_σ) and (ϕ'_σ) be the systems respectively associated to (G, f) and (G', f'). Then letting σ act on the previous equation defining ψ and some small manipulations we have that

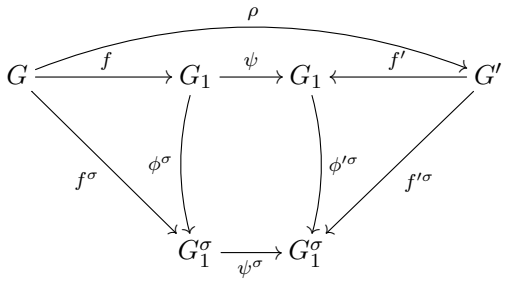
$$\psi^\sigma = f'^\sigma \circ \rho \circ f^{-\sigma} = f'^\sigma \circ f'^{-1} \circ f' \circ \rho \circ f^{-1} \circ f \circ f^{-\sigma} = \phi'_\sigma \circ f' \circ \rho \circ f^{-1} \circ \phi_\sigma^{-1} = \phi'_\sigma \circ \psi \circ \phi_\sigma^{-1}$$

Which implies that

3)

$$\phi'_\sigma = \psi^\sigma \circ \phi_\sigma \circ \psi^{-1}$$

This is to say that $\psi/K : G_1 \to G_1$ is such that the inner square of the diagram

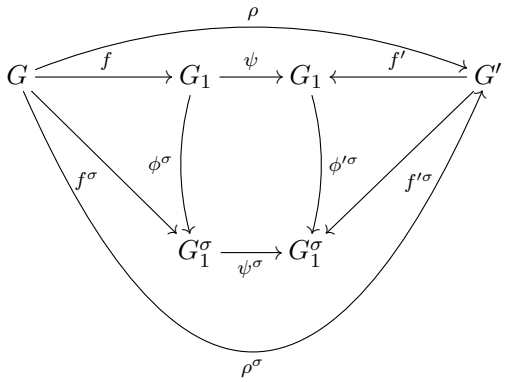


is commutative. Thus we define

Definition 36. Let G_1/K. Two systems of isomorphisms (ϕ_σ) and (ϕ'_σ) which satisfy condition 1) and 2) as above, are said to be $K-$equivalent (resp. equivalent) if there exists a $K-$automorphism (resp automorphism) ψ of G_1 satisfying condition 3) as described above.

Proposition 37. *Let G_1/K with K/k-forms (resp k-forms) (G, f) and (G', f'). (G, f) and (G', f') are isomorphic if and only if their corresponding systems are $K-$equivalent. (resp equivalent)*

Proof. The preceding paragraph proves isomorphic implies $K-$equivalence direction. So assume we have two such $K-$equivalent systems (ϕ_σ) and (ϕ'_σ) which are equivalent under some $\psi \in \mathrm{Aut}_K(G_1)$. Theorem 34 gives that there must exist K/k-forms (G, f) and (G', f') corresponding to these systems. Define $\rho = f'^{-1} \circ \psi \circ f$. Then $\rho^\sigma = f'^{-\sigma} \circ \psi^\sigma \circ f^\sigma$. We then have the diagram



which we use to note that

$$\rho^\sigma = f'^{-\sigma} \circ \psi^\sigma \circ f^\sigma = f'^{-1} \circ \phi'^{-1}_\sigma \circ \phi'_\sigma \circ \psi \circ \phi_\sigma^{-1} \circ \phi_\sigma \circ f = f'^{-1} \circ \psi \circ f = \rho$$

We conclude that ρ/k. Thus $G \cong G'$ via a $k-$isomorphism. □

The succinct statement of this result is the following.

Corollary 38. The $k-$isomorphism classes of K/k-forms of G_1/K are in a one to one correspondence with the $K-$equivalence classes of systems (ϕ_σ) satisfying 1) and 2).

Now for the remainder of the proof of Theorem 31.

Proof. Let $G_1 = (\mathbb{G}_m)^n$ be a torus defined over the prime field, and let (G, f) be a K/k-form of G_1. By definition G is isomorphic to G_1 by f/K and we have that $G_1 = (\mathbb{G}_m)^n$ so we have the G is a torus defined over k but split over K. Now let $\psi \in (\phi_\sigma)$ be the system corresponding to (G, f). By definition ψ/K. Furthermore, we have that G_1/k and thus $G^{\sigma_1} = G_1$. Therefore, $\psi \in \mathrm{Aut}_K(G_1)$, i.e., ψ is an isomorphism of the torus G_1. So let $X_1 = X(G_1)$. So by the duality

of Theorem 31 we have that ${}^t\psi : X_1 \to X_1$ is a $\Gamma-$isomorphism. So all elements ${}^t\phi_\sigma$ are in $\mathrm{Aut}_K(X_1)$. Now G_1 splits over the prime field, and so all elements of X_1 are also defined over the prime field. Thus Γ fixes X_1. Recall condition 1), that is, $\phi_\sigma^\tau \circ \phi_\tau = \phi_{\sigma\tau}$. Via this fact and the duality of Theorem 31 we have that

$$\begin{aligned}
{}^t\phi_{\sigma\tau} &= {}^t(\phi_\sigma^\tau \circ \phi_\tau) \\
&= \phi_\sigma^\tau \circ \phi_\tau \circ f \\
&= f^{\sigma\tau} \circ f^{-\tau} \circ f^\tau \circ f^{-1} \circ f \\
&= f^{\sigma\tau} \\
&= f^\tau \circ f^\sigma \\
&= f^\tau f^{-1} \circ f \circ f^\sigma \circ f^{-1} \circ f \\
&= \phi_\tau \circ f \circ \phi_\sigma \circ f \\
&= {}^t\phi_\tau \circ {}^t\phi_\sigma
\end{aligned}$$

Since the mapping $\alpha : \Gamma \to \mathrm{Aut}_K(X_1) \cong \mathrm{GL}(n,\mathbb{Z})$ defined by $\alpha(\sigma) = ({}^t\phi_\sigma)^{-1}$ gives a representation of Γ in $\mathrm{GL}(n,\mathbb{Z})$ we have that X_1 a $\Gamma-$module.

Now given any integral representation of Γ in $\mathrm{GL}(n,\mathbb{Z})$, one may show that there exists a K/k-form of G_1 which corresponds to this representation in the manner given above. This follows from the one-to-one correspondence between the automorphisms of X_1 and the automorphisms of G_1 (which is a torus) and Theorem 34.

We thus have a one-to-one correspondence between the category of tori defined over k of dimension n and the category of free Γ-modules of rank n, as claimed.

□

1.2 Proof details and some extras

1.2.1 Properties of $R_{K/k}(G_1)$

Let G_1 be an algebraic group defined over K, with $\dim G_1 = n$ and the degree of K/k equal to d. It is a natural question to ask if we can find some algebraic group defined over k which somehow corresponds to this information. We will prove the following shortly.

Proposition 39. *For any G_1 as described above, there exists an algebraic group $R_{K/k}(G_1)$ defined over k of dimension nd such that $R_{K/k} \cong (G_1)$.*

First we make the following observations.

Assume that $\{\sigma_1, \sigma_2, \cdots, \sigma_d\}$ is a maximal set of elements of Γ which have distinct restrictions to K, in particular assume σ_1 is the identity. Now define

$$\widetilde{G_1} = G_1^{\sigma_1} \times G_1^{\sigma_2} \times \cdots \times G_1^{\sigma_d}$$

$\widetilde{G_1}$ is defined over the field generated by $\cup_{i=1}^{d} K^{\sigma_i}$, which is the smallest Galois extension of k containing K and that if $\Gamma_1 := \mathrm{Gal}(\overline{k}/K)$ then $\Gamma = \cup_{i=1}^{d} \Gamma_1 \sigma_i$.

Now if $\sigma \in \Gamma$ then right multiplication of σ permutes the elements in set of cosets $\{\Gamma_1\sigma_1, \cdots, \Gamma_1\sigma_d\}$. For notational purposes we will denote the permutation of σ on $\Gamma_1\sigma_i$ by i^σ. As a quick example: $\Gamma_1\sigma_i\sigma = \Gamma_1\sigma_j \iff i^\sigma = j$. We may now define an isomorphism

$$\phi_\sigma : \widetilde{G_1} \to \widetilde{G_1}^\sigma = \prod_{i=1}^{d} \widetilde{G_1}^{\sigma_i\sigma}$$

defined by

$$\phi_\sigma(g_1, \cdots, g_d) = (g_{1^\sigma}, \cdots, g_{d^\sigma})$$

it can be shown that the system $\{\phi_\sigma\}$ satisfies the conditions of Theorem 34 and so there must exist a k-form $(\widetilde{G}, \widetilde{f})$ of $\widetilde{G_1}$ corresponding to this system. Furthermore $\widetilde{G}$ is an algebraic group defined over k of dimension nd. Now let $\pi_i : \widetilde{G_1} \to \widetilde{G_1^{\sigma_i}}$ be the standard projection to the i^{th} factor. We note that $\pi_i^\sigma \circ \phi_\sigma = \pi_{i^\sigma}$.

Define $p : \widetilde{G} \to G_1$ by $p = \pi_1 \circ \widetilde{f}$. Since we chose σ_1 as the identity, every $\sigma \in \Gamma$ fixes π_1, and furthermore $\pi_1 \circ \phi_\sigma = \pi_1$. This implies that $p^\sigma = p$, so p is defined over K. Finally noting that $\pi_i \circ \widetilde{f} = p^{\sigma_i}$ we get that

$$\widetilde{f} = p^{\sigma_1} \times \cdots p^{\sigma_d}$$

since $\widetilde{f}$ is determined by p. We now write the k-form $(\widetilde{G}, \widetilde{f})$ as $(\widetilde{G}, p)$ and define $R_{K/k}(G_1) := (\widetilde{G}, p)$. Via the definition, we see that $R_{K/k}(G_1)$ is a k-form of G_1. Furthermore, $R_{K/k}(G_1)$ is unique up to $k-$isomorphism.

$R_{K/k}(G_1)$ can be generalized to an algebraic set A_1/K as follows.

Definition 40. Let A_1 be an algebraic set defined over K. Then $R_{K/k}(A_1)$ is defined to be any pair $(\widetilde{A}, p)$ where $\widetilde{A}$ is an algebraic set defined over k, $p : \widetilde{A} \to A_1$ is defined over K and is a polynomial so that there is a $\overline{k}-$isomorphism

$$\widetilde{f} = p^{\sigma_1} \times \cdots p^{\sigma_d}$$

from $\widetilde{A}$ to $\widetilde{A_1} := A_1^{\sigma_1} \times \cdots A_1^{\sigma_d}$.

1.2.2 Proof of Theorem 34

Proof. This proof requires several steps. Step 1 is an explicit construction of $R_{K/k}(A_1)$ for a few special cases of algebraic groups which then give the result for any algebraic group. Step 2 explores the universal properties of $R_{K/k}(A_1)$, which are used in Step 3 to show that there exists a K/k-form of A_1. Step 4 is then the "actual" proof of the theorem.

Let K be a finite Galois extension of k with $K \subseteq \overline{k}$. Let $d = \deg K/k$ and $\{\sigma_1, \cdots, \sigma_d\}$ be the maximal set of elements in $\mathrm{Gal}(\overline{k}/k)$ with distinct restrictions to K with σ_1 as the identity.

Step 1) *The existence of $R_{K/k}(A_1)$, for any algebraic set A_1 defined over K.*

Case 1) Let $A_1 = \Omega$, $\widetilde{A} = \Omega^d$, and $\{w_1, \cdots, w_d\}$ be a vector space basis for K over k. Now define $f : \widetilde{A} \to A_1$ by

$$f(u_1, \cdots, u_d) = \sum_{i=1}^{d} u_i w_i$$

Clearly f is a polynomial defined over k. Additionally, we see that $f^{\sigma_j} = \sum_{i=1}^{d} u_i w_i^{\sigma_j}$. Now define $\tilde{f} : \Omega^d \to \Omega^d$ by

$$\tilde{f} = f^{\sigma_1} \times \cdots \times f^{\sigma_d}$$

This map may then be realized as multiplication by the matrix

$$F = \begin{pmatrix} w_1^{\sigma_1} & w_1^{\sigma_2} & \cdots & w_1^{\sigma_d} \\ w_2^{\sigma_1} & & & \vdots \\ \vdots & & \ddots & \\ w_d^{\sigma_1} & \cdots & & w_d^{\sigma_d} \end{pmatrix}$$

Thus, $\tilde{f}$ is also a polynomial. Furthermore $\det(F) \neq 0$ since K/k is separable, so $\tilde{f}$ is a $\overline{k}-$isomorphism of algebraic sets. By the previous definition $(\widetilde{A}, \tilde{f}) = R_{k/k}(A_1)$.

Case 2) Let A_1, B_1 be algebraic sets defined over K and assume that $R_{K/k}(A_1) = (\widetilde{A}, f_1)$ and $R_{K/k}(B_1) = (\widetilde{B}, f_2)$ exist. We run an argument similar to above to show that $R_{K/k}(A_1 \times B_1) = (\widetilde{A} \times \widetilde{B}, f_1 \times f_2)$. Thus $R_{K/k}(A_1 \times B_1)$ exists.

Case 3) Let A_1, B_1 be algebraic sets defined over K so that $B_1 \subseteq A_1$. Suppose that $R_{K/k}(A_1) = (\widetilde{A}, \tilde{f})$ exists. Since

$$\tilde{f} : \widetilde{A} \to \widetilde{A_1} = A_1^{\sigma_1} \times \cdots A_1^{\sigma_d}$$

is a $\overline{k}$-isomorphism and

$$\widetilde{B_1} := B_1^{\sigma_1} \times \cdots B_1^{\sigma_d} \subseteq A_1^{\sigma_1} \times \cdots A_1^{\sigma_d}$$

is algebraic subset we also have that $\widetilde{B} := \tilde{f}^{-1}(\widetilde{B_1})$ is an algebraic subset of $\widetilde{A}$. Note that $\widetilde{B_1}$ is defined over the field generated by $\cup_{i=1}^{d} K^{\sigma_i}$ and $\widetilde{f}^{-1}/\overline{k}$ so $\widetilde{B}$ is defined over $\overline{k}$. However, for $\sigma \in \Gamma$ we have that

$$\widetilde{B}^{\sigma} = \widetilde{f}^{-\sigma}(\widetilde{B_1}^{\sigma}) = \widetilde{f}^{-1} \circ \phi_{\sigma}^{-1}(\widetilde{B_1}^{\sigma}) = \widetilde{f}^{-1}\widetilde{B_1} = \widetilde{B}$$

so in fact $\widetilde{B}$ is defined over k. By definition $R_{K/k}(B_1) = (\widetilde{B}, \widetilde{f}|_{\widetilde{B}})$.

Now in particular, these three cases actually give the existence of $R_{K/k}(A_1)$ for any algebraic set A_1/K since every algebraic set may be viewed as a subset of Ω^n for some n.

Step 2) *Universal property of* $R_{K/k}(A_1)$. We noted already the uniqueness of $R_{K/k}(A_1)$ and we have the following universal property.

Let $R_{K/k}(A_1) = (\widetilde{A}, \widetilde{f})$, and $p = p_1 \circ \widetilde{f}$ where p_1 is defined above as a projection. Now if $\widetilde{B}/k$ is an algebraic set and $\phi : \widetilde{B} \to A_1$ is a polynomial defined over K, then there exists a polynomial map defined over k $\psi : \widetilde{B} \to \widetilde{A}$ so that the following diagram commutes:

$$\begin{array}{ccc} \widetilde{A} & \xrightarrow{p} & A_1 \\ \uparrow{\scriptstyle \psi} & \nearrow{\scriptstyle \phi} & \\ \widetilde{B} & & \end{array}$$

Furthermore, if B_1 is an algebraic set defined over K with $(\widetilde{B}, \widetilde{g}) = R_{K/k}(B_1)$, and $q = p_1 \circ g$ then there exists a unique polynomial map $\widetilde{\psi}$ defined over k so that the following diagram commutes:

$$\begin{array}{ccc} \widetilde{A} & \xrightarrow{p/K} & A_1/K \\ {\scriptstyle \widetilde{\psi}/k}\downarrow & & \downarrow{\scriptstyle \psi/K} \\ \widetilde{B}/k & \xrightarrow{q/K} & B_1/K \end{array}$$

Step 3) *For G_1 an algebraic group, we have $R_{K/k}(G_1)$ is a group.* Assume that $A_1 = G_1$ is an algebraic group defined over K. We want to show that $R_{K/k}(G_1)$ is a group, and p is a group homomorphism. Assume $R_{K/k}(G_1) = (\widetilde{G}, p)$, then $R_{K/k}(G_1 \times G_1) = (\widetilde{G} \times \widetilde{G}, p \times p)$. Now let

$$\phi : G_1 \times G_1 \to G_1$$

be the map defining multiplication in G_1. By the previous step, there exists $\widetilde{\phi}$ defined over k so that the following diagram commutes:

$$\begin{array}{ccc} \widetilde{G} \times \widetilde{G} & \xrightarrow{p \times p} & G_1 \times G_1 \\ {\scriptstyle \widetilde{\psi}}\downarrow & & \downarrow{\scriptstyle \psi} \\ \widetilde{G} & \xrightarrow{\quad p \quad} & G_1 \end{array}$$

In particular we have that $\widetilde{\psi}$ defines multiplication in $\widetilde{G}$. Similarly, if $\psi' : G_1 \to G_1$ defines the inverse operation in G_1, we have the existence of $\widetilde{\psi'}$ making the following diagram commute:

$$\begin{array}{ccc} \widetilde{G} & \xrightarrow{p} & G_1 \\ {\scriptstyle \widetilde{\psi'}}\downarrow & & \downarrow{\scriptstyle \psi'} \\ \widetilde{G} & \xrightarrow{p} & G_1 \end{array}$$

which defines the inverse operation in $\widetilde{G}$. Since these diagrams commute we have that p must also be a group homomorphism.

Step 4) *The proof of Theorem 34 for any algebraic set A_1 defined over K.* Recall that for A_1/K we have a system of rational isomorphisms (ϕ_σ) which map from A_1 to A_1^σ which satisfy

1)

$$\phi_\sigma^\tau \circ \phi_\tau = (f^\sigma \circ f^{-1})^\tau \circ f^\tau \circ f^{-1} = f^{\sigma\tau} \circ f^{-\tau} \circ f^\tau \circ f^{-1} = f^{\sigma\tau} \circ f^{-1} = \phi_{\sigma\tau}$$

for $\sigma, \tau \in \Gamma$;

2) each ϕ_σ depends only on the restriction of σ to K.

Now keeping the notation from Step 1) and Step 2) let $R_{K/k} = (\widetilde{A}, \widetilde{f})$ and define

$$A = \left\{ x \in \widetilde{A} \mid p^\sigma(x) = \phi_\sigma \circ p(x), \forall \sigma \in \Gamma \right\}$$

2) implies that $x \in A$ if and only if $P^{\sigma_i}(x) = \phi_{\sigma_i} \circ p(x)$ for $1 \leq i \leq d$ so the map $p|_A : A \to A_1$ is an injection. Now if $y \in A_1$ and we set

$$x = \widetilde{f}^{-1}(\phi_{\sigma_1}(y), \cdots, \phi_{\sigma_d}(y)$$

then $x \in A$ and $y = p(x)$ so $p|_A$ is surjective and thus an isomorphism. By definition we have that A is an algebraic subset of $\widetilde{A}$ defined over $\overline{k}$. However, 1) implies that $A^\sigma = A$ for all $\sigma \in \Gamma$ so A is in fact defined over k. So let $f = p|_A$, then (A, f) is a K/k-form of

A_1 with system (ϕ_σ). Furthermore, if $A_1 = G_1$ is a group, then one may verify that it is a subgroup of $R_{K/k}(G_1)$ and by step 3) f is an isomorphism of algebraic groups.

□

1.2.3 A side note on Galois cohomology

The results of corollary 38 require a few comments. First we give the definition of the first cohomology group of Galois cohomology.

Definition 41. (3) Let G be a group and A be an Abelian group. We will use additive notation for A. Assume that G acts on A by a homomorphism $\phi : G \to \mathrm{Aut}(A)$.

A *1-cocycle of G in A* is a family of elements $\{\alpha_\sigma\}_{\sigma\in G}$ with $\alpha_\sigma \in A$ satisfying

$$\alpha_\sigma + \sigma\alpha_\tau = \alpha_{\sigma\tau}$$

for all $\sigma, \tau \in G$. Note that the sum of $1-$cocycles must also be a cocycle. We denote the group of $1-$cocycles by $Z^1(G, A)$. A $1-$*coboundary of G in A* is a family $\{\alpha_\sigma\}_{\sigma\in G}$ so that there exists an element $\beta \in A$ which satisfies

$$\alpha_\sigma = \sigma\beta - \beta$$

Certainly any $1-$coboundary is a $1-$cocycle and we denote the group of coboundaries by $B^1(G, A)$. The *first cohomology group of G in A* is now defined as the factor group

$$H^1(G, A) := Z^1(G, A)/B^1(G, A)$$

Using Galois cohomology corollary 38 may be restated as

Corollary 42. The $k-$isomorphism classes of K/k forms of G_1/k are in one to one correspondence with the elements of $H^1(\mathrm{Gal}(K/k), \mathrm{Aut}_K(G_1))$.

In fact, we have the same correspondence for k-forms.

Corollary 43. The $k-$isomorphism classes of k-forms of G_1/k are in one to one correspondence with the elements of $H^1(k, \mathrm{Aut}_K(G_1))$, which is defined to be the direct limit $\cup_K H^1(\mathrm{Gal}(K/k), \mathrm{Aut}_K(G_1))$.

1.2.4 The structure of algebraic groups

We have proved some powerful and general results in the last few sections. In order to go further in the same spirit we will first need to dedicate time to certain substructures of algebraic groups. We will also see our first reduction of the classification of algebraic groups.

Definition 44. An element $M \in \mathrm{GL}(V)$ is called *semi-simple* if M is similar to a diagonal matrix D, that is, $P^{-1}MP = D$ for some non-singular P.

Definition 45. An element $M \in GL(V)$ is called *unipotent* there exists an $n \in \mathbb{N}$ so that $(M - I)^n = 0$.

Example 46. All matrices of the following form are semi-simple.

$$\begin{pmatrix} a & 0 & 0 \\ 0 & 1/a & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}(3, \mathbb{Q}) \text{ with } \mathbb{Q} \ni a \neq 0$$

All matrices of the following form are unipotent.

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}(3, \mathbb{Q}), a, b, c \in Q$$

Additionally, one may show that

Proposition 47. *Let G be an algebraic group. Then*

- *Every element in $g \in G$ is decomposable as $g = g_u \cdot g_s$ where g_s is semi-simple and g_u is unipotent. This is known as the* Jordan-Chevalley decomposition.
- *If $g \in G$ then $g_u, g_s \in G$ $g_s \cdot g_u = g_u \cdot g_s$ and g_s, g_u are independent of the representation in some $GL(V)$.*
- *If $\phi : G \to G'$ is a rational homomorphism from G to some other algebraic group G' then $\phi(g_s) = \phi(g)_s$ and $\phi(g_u) = \phi(g)_u$ for all $g \in G$.*

This proposition gives us license to write $G_u = \{g \in G | g = g_u\}$ and $G_s = \{g \in G | g = g_s\}$ without the usual ambiguity associated with bases.

Definition 48. If G is an algebraic group so that $G = G_u$ we call G a *unipotent* group.

Before proceeding we note a few more examples.

Example 49. Given any torus $T \cong D(n)$, we note that T is semi-simple via the identity I_n since any element in T is already diagonal. Furthermore, one may show that if $G = G_s$ and G is connected we have that G is a torus.

Example 50. Let $G = \mathbb{G}_a$. First define the $\phi : G \to GL(2)$ by

$$\alpha \mapsto \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$$

Note that this is an isomorphism on its image. Also, note that the identity matrix is both semi-simple and unipotent. This is a triviality, but is important for this example.

Take any $g \in G$, then by definition

$$\phi(g) = \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}$$

However it is clear that $\phi(g) = \phi(g)_u$ since $\phi(g)$ is unipotent. Proposition 47 gives that both that $\phi(g)_u = \phi(g_u)$ (which implies that $g_u = g$) and that the representation of G into GL(2) is immaterial when considering the decomposition of g. Therefore, every $g \in G$ is in G_u so G is unipotent. The conclusion is that G is unipotent.

This last example provides a intuitive foothold into the example of $\mathrm{SL}(3, \mathbb{Q})$ (Proposition 67) worked out in the next section.

Proposition 51. *If G is a connected unipotent algebraic group then there exists a finite descending series of closed and connected normal subgroups of G*

$$G = G_0 \supset G_1 \supset \cdots \supset G_k = \{e\}$$

and the commutator subgroup $[G : G_i] \subseteq G_{i+1}$. *Furthermore, we may take this series so that* G_i/G_{i+1} *is rationally isomorphic to* $\mathbb{G}_a$ *for all* i *in the index.*

We now make the definition

Definition 52. An algebraic group G is called solvable if it is solvable with respect to its group structure.

In general, given an algebraic group G with two closed subgroups H_1, H_2 we have that the commutator subgroup $[H_1, H_2]$ is closed. So in our case we may take the composition series involved with the definition of solvability of an algebraic group to be closed. The following proposition collects a few significant results.

Proposition 53. *Let* G *be a connected solvable algebraic group defined over* k. *Then*

1) *There exists an isomorphism from* G *to the group of upper triangular matrices of degree* n.
2) G_u *is a* $k-$*closed connected normal subgroup of* G.
3) *The exists a maximal torus* T/k *of* G *so that* $G = G_u \rtimes T$. *This semidirect product is takes as a semidirect product of algebraic groups; that is a semidirect product of groups and a direct product of algebraic sets.*
4) *All such maximal tori are conjugate by inner automorphisms of* G.

Definition 54. Let G be a connected algebraic group. The *radical of* G, which we denote as $\mathcal{R}$, we define as a maximal element in the set of connected solvable normal subgroups of G. The *unipotent radical of* G is defines as the unipotent part of $\mathcal{R}$ and is denoted $\mathcal{R}_u$.

Definition 55. An algebraic group G is called *semi-simple* if $\mathcal{R} = \{1\}$, and *reductive* if $\mathcal{R}_u = \{1\}$.

We now come to our first major reduction in the problem of classifying semi-simple or reductive algebraic groups–the result is due to Chevalley.

Theorem 56. *Let G be a connected algebraic group.*

- *If G is semi-simple then G is isogeneous to a direct product of simple groups.*
- *If G is reductive then G is isogeneous to a direct product of a semi-simple group and a torus*

Example 57. Let $G = \{(g_1, g_2) \in GL(2,\mathbb{R}) \times GL(2,\mathbb{R}) | \det(g_1) = \det(g_2)\}$. We see that G has a subgroup $H = \{(tI_2, tI_2) \mid t \in \mathbb{G}_m\}$. Then G/H is isogeneous to $SL(2,\mathbb{R}) \times SL(2,\mathbb{R})$, but not isomorphic. Furthermore, the property of being reductive or semi-simple is invariant under isogeny, so even though these groups are not isomorphic, it may be shown that have the same classification as semi-simple affine algebraic groups.

Definition 58. A *Borel subgroup* is a maximal closed connected solvable subgroup of G. Any subgroup $H \subseteq G$ which contains a Borel subgroup is called *parabolic*.

It may be shown that

Proposition 59. *1) All Borel subgroups are conjugate by inner automorphisms of G.*

2) If $B \subseteq G$ is Borel, then the coset space G/B is a projective variety.

2)' In fact, if $H \subseteq G$ is closed and connected then G/H is a complete variety if and only if H is a parabolic subgroup of G.

3) Every Borel subgroup is its own normalizer in G. In particular this implies a parabolic subgroup is its own normalizer in G and is thus connected.

4) If $B \subseteq G$ is Borel then $G = \bigcup_{g \in G} gBg^{-1}$.

We must now momentarily define these objects with respect to fields of definition.

Proposition 60. *The following are equivalent.*

1) G is solvable, defined over k, and all rational characters of G are defined over k.

- *There exists an isomorphism $\phi : G \to Tr(n)$ which is defined over k.*
- *G is a semidirect product over k of a $k-$trivial torus and a unipotent subgroup of G which is defined over k.*

Definition 61. Any algebraic group satisfying one of the conditions of Proposition 60 is called *$k-$solvable.*

Definition 62. A *$k-$Borel subgroup of* G is a maximal connected $k-$solvable subgroup.

Proposition 63. *If G/k then all $k-$Borel subgroups of G are conjugate by inner automorphisms defined over k. As a corollary, all maximal $k-$trivial tori of G are conjugate with respect to $k-$rational inner automorphisms of G.*

Definition 64. The *$k-$rank of* an algebraic group G is the dimension of any maximal $k-$split torus. The *rank* of G is the $\Omega-$rank of G.

Definition 65. An algebraic group G/k is called *k-compact* if it has no non-trivial $k-$Borel subgroups.

As one might expect we do not have a perfect correspondence of results when we relativize the results for k, in particular item 2) from Proposition 59 fails. We have as an analogue that if G/k and $H \subset G$ is $k-$Borel then there exists a complete variety V defined over k on which G operates and an injective polynomial $f : G/H \to V$ which preserves multiplication by G in a way such that G_k acts transitively on V_k. In particular this gives us that

Corollary 66. Let G/k be an algebraic group and k a local field. G is k-compact if and only if G_k is compact.

We now discuss some examples.

1.3 Examples

1.3.1 $SL(3,\mathbb{Q})$

Let $\mathbb{Q} \subseteq \Omega$. As an example, we will consider $\mathrm{SL}(3,\mathbb{Q}) = \{M \in \mathrm{GL}(3,\mathbb{Q}) | \det(M) = 1\}$. First we will show the following.

Claim 67. *$SL(3,\mathbb{Q})$ is an affine algebraic group defined over $\mathbb{Q}$.*

Proof. Let

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{13} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = A, \text{ and } \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{13} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} = B$$

with both $A, B \in \mathrm{SL}(3,\mathbb{Q})$. First, we wish to show this is an abstract group. Matrix multiplication acts as an associative binary operation on $\mathrm{SL}(3,\mathbb{Q})$,

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is the identity. Inverses are given by

$$A^{-1} = \begin{pmatrix} M_{1,1} & -M_{2,1} & M_{3,1} \\ -M_{1,2} & M_{2,2} & -M_{3,2} \\ M_{1,3} & -M_{2,3} & M_{3,3} \end{pmatrix} = \begin{pmatrix} a_{22}a_{33} - a_{32}a_{23} & a_{13}a_{32} - a_{33}a_{12} & a_{12}a_{23} - a_{22}a_{13} \\ a_{23}a_{31} - a_{33}a_{21} & a_{11}a_{33} - a_{31}a_{13} & a_{13}a_{21} - a_{23}a_{11} \\ a_{21}a_{32} - a_{31}a_{22} & a_{12}a_{31} - a_{32}a_{11} & a_{11}a_{22} - a_{21}a_{12} \end{pmatrix},$$

that is, the usual matrix inverses—these are contained in $\mathrm{SL}(3,\mathbb{Q})$ since their determinant is equal to 1 and we can see that each entry is an element of $\mathbb{Q}$. Finally, closure under the binary operation is given by noting that $\det(A \cdot B) = \det(A) \cdot \det(B)$. Thus, $\mathrm{SL}(3,\mathbb{Q})$ is a group.

Continuing on, note that $\mathrm{SL}(3,\mathbb{Q}) \subseteq \mathbb{A}^9_{\mathbb{Q}} \subseteq \mathbb{A}^9_{\Omega}$ and can be defined as an algebraic set by

$$\mathbb{V}\left(\det\begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} - 1\right) = \mathbb{V}\left(x_1x_5x_9 + x_2x_6x_7 + x_3x_4x_8 - x_7x_5x_3 - x_8x_6x_1 - x_9x_4x_2 - 1\right)$$

Explicitly, define $f \in \mathbb{Q}[x_1, \cdots, x_9]$ by

$$f(x_1, \cdots, x_9) := x_1x_5x_9 + x_2x_6x_7 + x_3x_4x_8 - x_7x_5x_3 - x_8x_6x_1 - x_9x_4x_2 - 1$$

Thus, $\mathrm{SL}(3,\mathbb{Q})$ is $\mathbb{Q}-$closed as an algebraic set, and therefore defined over $\mathbb{Q}$ as an algebraic set since $\mathbb{Q}$ is perfect.

Let $M_{i,j}$ be the minor in the $i-$th row and $j-$th column of A. Note that

$$A^{-1}B = \begin{pmatrix} \sum_{i=1}^3 (-1)^{i-1} M_{i,1} b_{i,1} & \sum_{i=1}^3 (-1)^{i-1} M_{i,1} b_{i,2} & \sum_{i=1}^3 (-1)^{i-1} M_{i,1} b_{i,3} \\ \sum_{i=1}^3 (-1)^{i} M_{i,2} b_{i,1} & \sum_{i=1}^3 (-1)^{i} M_{i,2} b_{i,2} & \sum_{i=1}^3 (-1)^{i} M_{i,2} b_{i,3} \\ \sum_{i=1}^3 (-1)^{i-1} M_{i,3} b_{i,1} & \sum_{i=1}^3 (-1)^{i-1} M_{i,3} b_{i,2} & \sum_{i=1}^3 (-1)^{i-1} M_{i,3} b_{i,3} \end{pmatrix}$$

Let $\phi : \mathrm{SL}(3,\mathbb{Q}) \times \mathrm{SL}(3,\mathbb{Q}) \to \mathrm{SL}(3,\mathbb{Q})$ taking $(A, B) \mapsto A^{-1}B$. Recall that $M_{i,j}$ is a polynomial and note that we are considering $\mathrm{SL}(3,\mathbb{Q})$ as a subset of affine space, so we may

reinterpret this matrix multiplication as giving us the data of a map $\phi : \mathbb{A}^9_{\mathbb{Q}} \times \mathbb{A}^9_{\mathbb{Q}} \to \mathbb{A}^9_{\mathbb{Q}}$. Then ϕ can be seen as a polynomial map by definition, since in each coordinate ϕ is a polynomial function, and in particular is a polynomial with coefficients in $\mathbb{Q}$; ϕ is therefore defined over $\mathbb{Q}$.

Thus, by definition $\mathrm{SL}(3, \mathbb{Q})$ is an affine algebraic group. Furthermore, since $\mathrm{SL}(3, \mathbb{Q})$ is defined over $\mathbb{Q}$ as an algebraic set and the map ϕ is also defined over $\mathbb{Q}$, $\mathrm{SL}(3, \mathbb{Q})$ is defined over $\mathbb{Q}$ as an algebraic group. □

At this point we also find an example of a torus in $\mathrm{SL}(3, \mathbb{Q})$

Proposition 68. *The set of matrices $T \subset SL(3, \mathbb{Q})$ of the form*

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & \frac{1}{ab} \end{pmatrix}$$

is a torus in $SL(3, \mathbb{Q})$

Proof. First we show that T is an algebraic subgroup of $\mathrm{SL}(3, \mathbb{Q})$.

- Let
$$\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & \frac{1}{a_1 a_2} \end{pmatrix} = A, \text{ and } \begin{pmatrix} b_1 & 0 & 0 \\ 0 & b_2 & 0 \\ 0 & 0 & \frac{1}{b_1 b_2} \end{pmatrix} = B \in T$$

. By definition

$$AB = \begin{pmatrix} a_1b_1 & 0 & 0 \\ 0 & a_2b_2 & 0 \\ 0 & 0 & \frac{1}{a_1b_1a_2b_2} \end{pmatrix}$$

So T is closed under the binary operation. Also, note that T is Abelian.

- $I_3 \in T$
- $$A^{-1} = \begin{pmatrix} \frac{1}{a} & 0 & 0 \\ 0 & \frac{1}{b} & 0 \\ 0 & 0 & ab \end{pmatrix}$$

So T is a subgroup of G.

Additionally, $T \cong \mathbb{V}(x_1x_5x_9 - 1, x_2, x_3, x_4, x_6, x_7, x_8)$ (using the indexing from proposition 67) T is an algebraic subgroup of $\mathrm{SL}(3, \mathbb{Q})$. It is also easy to see that $T/\mathbb{Q}$. Now define $\phi : T \to \mathbb{A}^2_{\mathbb{Q}^\times} \subset \mathbb{A}^2_{\mathbb{C}^\times}$ by $\phi(A) = (a_1, a_2)$. Clearly, for all $A, B \in T$ we have that $\phi(AB) = (a_1b_1, a_2b_2)$, which is a polynomial in the coordinates. Furthermore, ϕ is a group isomorphism. So $T \cong \mathbb{A}^2_{\mathbb{Q}^\times}$ is a torus in $\mathrm{SL}(3, \mathbb{Q})$ defined over $\mathbb{Q}$.

□

Note that any permutation of the diagonal entries would also define a torus. As such we will consider T as the subgroup of matrices $T \subset \mathrm{SL}(3, \mathbb{Q})$ of the form

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \text{ so that } abc = 1$$

For the sake of clarity we note that we may consider this T as an algebraic group in $\mathbb{A}^3_\Omega$ defined by $\mathbb{V}(x_1 x_2 y - 1)$. In particular, we may consider T as only having two coordinates, since the third will depend on the first two.

Proposition 69. *The torus T as defined above is maximal with respect to inclusion in $SL(3, \mathbb{Q})$.*

Proof. We will argue by contradiction. Assume there is some larger torus T' containing T. By definition T' is a direct product of $(\mathbb{G}_m)^n$ for some $1 < n \leq 8$, therefore T' must be Abelian (Alternatively, we will soon see that $Z_G(T') = T'$). Now take the matrix

$$M := \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} \in T' \setminus T,$$

i.e., at least one of $\{x_2, x_3, x_4, x_6, x_7, x_8\}$ is not equal to zero. Since $T \subset T'$ we must have that

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1/2 \end{pmatrix} \in T'$$

However,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1/2 \end{pmatrix}^{-1} \cdot \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1/2 \end{pmatrix} = \begin{pmatrix} x_1 & 2x_2 & x_3/2 \\ x_4/2 & x_5 & x_6/4 \\ 2x_7 & 4x_8 & x_9 \end{pmatrix}$$

Since T' is Abelian it must be the case that M is equal to the matrix on the right. However, this cannot occur unless each of $\{x_2, x_3, x_4, x_6, x_7, x_8\}$ is equal to zero. This is a contradiction. Thus, T is maximal. $\square$

1.3.2 Example: $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$-form

Consider the sets $G_1 \subset GL(2,\mathbb{Q})$, $G_2 \subset GL(2,\mathbb{Q}[\sqrt{2}])$ given by

$$G_1 = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \right\},\ G_2 = \left\{ \begin{pmatrix} a+\sqrt{2}b & 0 \\ 0 & a-\sqrt{2}b \end{pmatrix} \right\}\ a,b \in \mathbb{Q}$$

After a routine definition check we find that both sets are in fact groups under matrix multiplication. The algebraic set structures are given by

$$\mathbb{V}\left((x_1^2 - 2x_2^2)x_5 - 1, x_1 - x_4, 2x_2 - x_3\right) = G_1 \text{ and } \mathbb{V}\left(x_1x_4x_5 - 1, x_2, x_3\right) = G_2$$

Where x_i denotes the standard coordinates in affine space. All that remains is to check that the maps $G_1 \times G_1 \to G_1$ and $G_2 \times G_2 \to G_2$ sending $(x,y) \mapsto x^{-1}y$ are polynomial maps, and to see what field they are defined over. We note that for $i \in \{1,2\}$ the map $G_i \times G_i \mapsto G_i$ defined by $(x,y) \mapsto x^{-1}y$ is given as

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\begin{pmatrix} c & d \\ 2d & c \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}^{-1}\begin{pmatrix} c & d \\ 2d & c \end{pmatrix}$$
$$= \begin{pmatrix} \frac{ac-2bd}{a^2-2b^2} & \frac{ad-bc}{a^2-2b^2} \\ \frac{2ad-2bc}{a^2-2b^2} & \frac{ac-2bd)d}{a^2-2b^2} \end{pmatrix}$$

and in G_2

$$\begin{pmatrix} a+b\sqrt{2} & 0 \\ 0 & a-b\sqrt{2} \end{pmatrix} \begin{pmatrix} c+d\sqrt{2} & 0 \\ 0 & c-d\sqrt{2} \end{pmatrix} \mapsto \begin{pmatrix} a+b\sqrt{2} & 0 \\ 0 & a-b\sqrt{2} \end{pmatrix}^{-1} \begin{pmatrix} c+d\sqrt{2} & 0 \\ 0 & c-d\sqrt{2} \end{pmatrix}$$
$$= \begin{pmatrix} \frac{(a-b\sqrt{2})(c+d\sqrt{2})}{a^2-2b^2} & 0 \\ 0 & \frac{(a+b\sqrt{2})(c-d\sqrt{2})}{a^2-2b^2} \end{pmatrix}$$

At first glance the maps defined by these matrices seem to look like rational functions rather than polynomial functions. However, we are considering polynomials in the coordinate ring, which is a quotient of $\mathbb{Q}[x_1, \cdots, x_n]$. For example, in the case of G_2 we have the relation $x_1x_4x_5 - 1 = 0 \iff x_5 = x_1^{-1}x_4^{-1}$. The previous map associated to G_2 is actually defined by $\phi((x_1, 0, 0, x_4) \times (x_1', 0, 0, x_4')) = (x_4x_1'x_5, 0, 0, x_1x_4'x_5)$, which is a polynomial. The argument for G_1 is similar.

Now consider the polynomial map $\phi : G_1 \to G_2$ defined by

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mapsto \begin{pmatrix} 1 & \frac{1}{\sqrt{2}} \\ 1 & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \begin{pmatrix} 1 & \frac{1}{\sqrt{2}} \\ 1 & \frac{-1}{\sqrt{2}} \end{pmatrix}^{-1}$$
$$= -\sqrt{2} \begin{pmatrix} 1 & \frac{1}{\sqrt{2}} \\ 1 & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ -1 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} a+b\sqrt{2} & 0 \\ 0 & a-b\sqrt{2} \end{pmatrix}$$

To justify the claim that this is a polynomial map, we may write this in a as

$$\phi(a, b, 2b, a) = (a + \sqrt{2}b, 0, 0, a - \sqrt{2}b)$$

or perhaps even more clearly as $\phi(x_1, x_2, x_3, x_4) = (x_1 + \sqrt{2}x_2, 0, 0, x_1 - \sqrt{2}x_2)$

Thus, ϕ is defined over $\mathbb{Q}[\sqrt{2}]$, is bijective, and is a group homomorphism. The map ϕ^{-1} is given as

$$\phi^{-1}(x_1, x_2, x_3, x_4) = \left(\frac{1}{2}(x_1 + x_4), \frac{1}{2\sqrt{2}}(x_1 - x_4), \frac{1}{\sqrt{2}}(x_1 - x_4), \frac{1}{2}(x_1 + x_4)\right)$$

Decoding this map in terms of matrices in G_1 and G_2 makes is clear that this is also a group homomorphism. So we see that $\phi/\mathbb{Q}[\sqrt{2}]$ is an isomorphism.

By definition we see that (G_1, ϕ) is a $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$-form of G_2, which makes it a $\mathbb{Q}$-form of G_2.

1.3.3 Computations with a torus

Let $k \subseteq K$ be a Galois extension and T be a torus defined over k and split over K. Let $\Gamma = \mathrm{Gal}_k(K)$. Our goal is to show that there exists subtori $A, T_0 \subseteq T$ so that:

- A is the largest $k-$trivial subtorus of T.
- T_0 is the largest k-compact subtorus of T.
- T is a semi-direct product of A and T_0.
- $T_0 \cap A$ is a finite set, and thus T is isogeneous to $A \times T_0$.

Let X be the character module of T and consider the following submodule of X:

$$X^{\Gamma} = \{\chi \in X | \chi^{\sigma} = \chi, \forall \sigma \in \Gamma\}$$

that is, X^{Γ} is the submodule of characters fixed by Γ. This is easy to see by recalling that $(\chi_1 + \chi_2)(t) := \chi_1(t)\chi_2(t)$ and X is a Γ-module so

$$(\chi_1 + \chi_2)(t)) = (\chi_1^{\sigma} + \chi_2^{\sigma})(t) = (\chi_1 + \chi_2)^{\sigma}(t)$$

thus X^{Γ} inherits all of its Γ-module structure from X and is closed under the $+$ operation. We also see the set

$$X_0 = \left\{ \chi \in X \Big| \sum_{\sigma \in \Gamma} \chi^{\sigma} = 0 \right\}$$

is a submodule of X by noting that

$$\sum_{\sigma \in \Gamma} \chi_1^{\sigma} + \sum_{\sigma \in \Gamma} \chi_2^{\sigma} = \left(\sum_{\sigma \in \Gamma} \chi_1^{\sigma} + \sum_{\sigma \in \Gamma} \chi_2^{\sigma} \right)(t) = \left(\sum_{\sigma \in \Gamma} \chi_1^{\sigma} \right)(t) \left(\sum_{\sigma \in \Gamma} \chi_2^{\sigma} \right)(t) = 0$$

so it is closed under the $+$ operation. Additionally, we note that each submodule X_0 and X^{Γ} are Γ-invariant since every element of X^{Γ} is fixed by Γ and every element of Γ fixes 0. Moreover, as discussed earlier, both submodules are cotorsion free. Now let $T_0 = (X^{\Gamma})^{\perp}$, $A = (X_0)^{\perp}$. Then both A and T_0 are subtori of T and defined over k. Now if $T' \subseteq T$ is a subtorus defined over k and $X_1 = (T')^{\perp}$, then T' is $k-$trivial if and only if Γ operates trivially on $X(T') = X/X_1$. However, this happens if and only if $X_0 \subseteq X_1$ if and only if $T' \subseteq A$. Thus, A is the maximal

subtorus of T which is $k-$trivial. It now follows that T is k-compact if and only if $A = \{1\}$, which is equivalent to $X_0 = X$. We may apply this idea $T' \subseteq T$, and we will find that t' is k-compact if and only if $X(T')_0 = (X(T')$, but this is equivalent to $X^\Gamma \subseteq X_1$ which is equivalent to $T' \subseteq T_0$. So T_0 is the largest k-compact subtorus of T. It follows that

$$X_{\mathbb{Q}} = (X_0)_{\mathbb{Q}} \oplus (X^\Gamma)_{\mathbb{Q}}$$

and so $[X : (X_0) \oplus (X^\Gamma)]$ is finite, $X_0 \cap X^\Gamma = \{0\}$. Thus $A \cap T_0$ is finite and T is a semi-direct product of A and T_0, and thus isogeneous to $A \times T_0$.

1.4 Representation theory/Geometry

1.4.1 Root systems,Weyl groups, fundamental systems, Weyl Chambers

Definition 70. Let G be an algebraic group and $T \leq G$ be a torus which is maximal with respect to inclusion. A character $X(T) \ni \chi : T \to \mathbb{G}_a$ is a *root* if there exists an isomorphism $f : \mathbb{G}_a \to P_a$, where P_α is some closed subgroup of G, so that

$$t \cdot f(\alpha) \cdot t^{-1} = f(\chi(t) \cdot \alpha)$$

for all $t \in T$ and $\alpha \in \mathbb{G}_m$.

The set of all roots of T will be denoted by $\surd$ and will be called the *root system* of G relative to T.

Furthermore:

Proposition 71.

- *The subgroup $P_\alpha \subseteq G$ is uniquely determined by α.*
- *The isomorphism $\chi_\alpha : \mathbb{G}_a \to P_\alpha$ is unique up to scalar multiplication in $\mathbb{G}_a$.*
- *$\surd$ is a finite set.*
- *$Z_G(T) = T$*
- *$N_G(T)/T$ is a finite group.*

Definition 72. The finite group $W = N_G(T)/T$ is called the *Weyl group* of G relative to T.

The Weyl group may be naturally interpreted as an automorphism group of T, X, or $\hat{X} := \mathrm{Hom}(X, \mathbb{Z})$. To see this, for each $s \in N_G(T)$ we may associate an automorphism $w_s : T \to T$ given by

$$w_s(t) = sts^{-1}$$

for $t \in T$.

similarly, denote the automorphism $w_s : X \to X$ given by

$$w_s(\chi)(w_s(t)) = \chi(t) \text{ that is}$$

for $t \in T$ and $\chi \in X$. The last isomorphism is the horrifically named contragredient of w_s when considered as an automorphism of X.

Proposition 73. *The triple $(X, \surd, W)$ has the following list of properties.*

- *X is a free $\mathbb{Z}-$module of rank $l = \dim T$*
- *$\surd$ is a finite subset of X.*
- *W is a finite automorphism group of X*

Additionally, we have that:

i) $0 \notin \surd$. *If* $\alpha \in \surd$ *then* $-\alpha \in \surd$

*i)** *if* $\alpha \in \surd$ *and* $c\alpha \in \surd$ *for* $c \in \mathbb{Q}$ *then* $c = \pm 1$.

ii) To each $\alpha \in \surd$ *there corresponds an element* $w_\alpha \in W$ *so that* $w_\alpha(\chi) = \chi - \alpha^*(\chi)\alpha$ *for* $\chi \in X$ *and where* $\alpha^* \in \hat{X}$. *Furthermore,* $w_\alpha(\surd) = \surd$.

iii) $X_{\mathbb{Q}} := X \otimes_{\mathbb{Z}} \mathbb{Q}$ *is generated by* $\surd$ *as a linear space over* $\mathbb{Q}$.

iv) W *is generated by* $\{w_\alpha | \alpha \in \surd\}$

Definition 74. We call $\surd$ an *abstract root system* if $\surd$ satisfies $i), i)*, ii)$ and $iii)$ and is a subset of any finite rank free module X. The group W generated by the set $\{w_\alpha | \alpha \in \surd\}$ is finite and is uniquely determined by the pair $(X, \surd)$. This group W is called the *Weyl group of* $\surd$.

Example 75. Given a root system $\surd$ in X the set $\surd^* := \{\alpha^* | \alpha \in \surd\}$ is a root system in $\hat{X}$.

Since W is finite, there must exist some positive definite symmetric bilinear form which is $W-$invariant. Take any symmetric bilinear form $<,>$ on the vector space $X_{\mathbb{Q}}$ and define $< \chi, \chi' >' = \sum_{w \in W} < w\chi, w\chi' >$. Since W is finite this is a finite sum and since W is closed under the group operation(composition) we have that acting by an element of W simply permutes the terms of this sum. So $<,>'$ is $W-$invariant.

The relations $< w_\alpha(\chi), w_\alpha(\chi) >=< \chi, \chi >$ and $w_\alpha(\chi) = \chi - \alpha^*(\chi)\alpha$ implies that

$$\alpha^*(\chi) = \frac{2 < \alpha, \chi >}{< \alpha, \alpha >}$$

And so α^* is identified with $\frac{2\alpha}{<\alpha,\alpha>}$. It then follows that $w_\alpha^2 = 1$. In line with geometric intuition, since $w_\alpha(\alpha) = -\alpha$ and the hyperplane $\{\chi | < \alpha, \chi >= 0\} \subset X_{\mathbb{R}}$ is fixed by w_α we call w_α a *reflection* or *symmetry* with respect to α.

Definition 76. The numbers $c_{\alpha,\beta} := \frac{2<\alpha,\beta>}{\alpha,\alpha}$ are called *Cartan integers*. Property ii) implies that $c_{\alpha,\beta} \in \mathbb{Z}$. This is called the *integrality condition* on a root system.

Assume $\surd$ is a root system of a free module X of rank l and W is the Weyl group of $\surd$. We fix a linear order compatible with addition in X and denote the set of positive roots by $\surd_+$. In practice this looks like taking a hyperplane containing none of the roots and declaring the set of roots contained in one of the connected components hyperplane to be positive. This depends on the fact that in affine space a hyperplane cuts the space into two connected components.

Definition 77. A positive root α is said to be *simple* if it cannot be expressed in the form $\beta + \gamma$ for $\beta, \gamma \in \surd_+$. Denote the set of simple roots of $\surd$ by Δ; we call this a *fundamental system* of $\surd$.

We then have the following.

Proposition 78. *1) The fundamental system Δ consists of l linearly independent roots $\alpha_1, \cdots, \alpha_l$. That is, every root $\alpha \in \surd$ can be expressed uniquely as a linear combination $\alpha = \pm \sum_{i=1}^{l} m_i \alpha_i$ where $m_i \in \mathbb{N} \cup \{0\}$.*

2) Every root $\alpha \in \surd$ can be written in the form $\alpha = w_{\alpha_{i_r}} \cdots w_{\alpha_{i_1}} \alpha_{i_0}$ for some $\alpha_{i_0} \in \Delta$ also with $\alpha_{i_1}, \cdots, \alpha_{i_r} \in \Delta$.

3) W is generated by $\{w_{\alpha_i} | \alpha_i \in \Delta\}$.

4) W acts simply transitively on the set of all fundamental systems of $\surd$.

An essential concept in the proof of this proposition is the concept of a Weyl chamber. This concept will be necessary for us later, so we introduce it here.

Given X, a root system $\surd$ of X, and a set of simple roots Δ, we define

$$H_\alpha = \{\chi \in X_{\mathbb{R}} := X \oplus_{\mathbb{Z}} \mathbb{R} \mid < \alpha, \chi >= 0\}$$

Clearly, this is vector subspace of X_R of codimension 1 which is cut out by a single polynomial equation. In other words, H_α is a hyperplane in $X_{\mathbb{R}}$.

Definition 79. The connected components of

$$X_{\mathbb{R}} \setminus \bigcup_{\alpha \in \surd} H_\alpha$$

are called *Weyl chambers*.

Assume $\Delta = \{\alpha_1, \cdots, \alpha_j\}$. We define

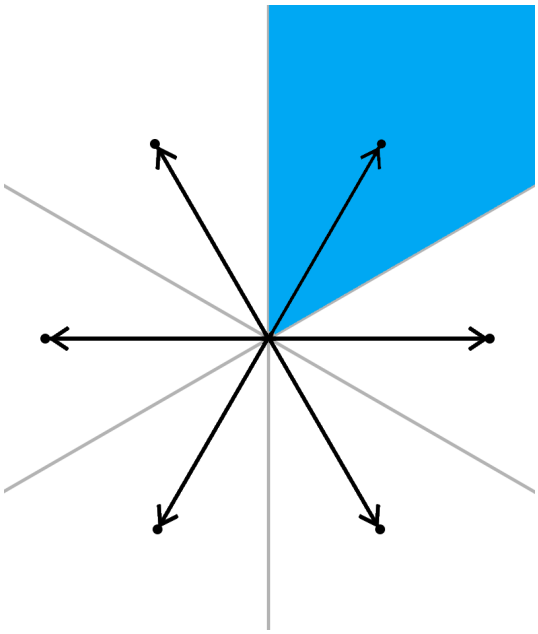
$$\Lambda_\Delta := \{\chi \in X_{\mathbb{R}} \mid \langle \alpha_i, \chi \rangle > 0, 1 \leq i \leq j\}.$$

This is a Weyl chamber. Note that

$$X_{\mathbb{R}} \setminus \bigcup_{\alpha \in \surd} H_\alpha = \bigcup_{\substack{\Delta | \Delta \text{ is a} \\ \text{fundamental} \\ \text{system}}} \Lambda_\Delta$$

Since we have a $W-$invariant metric $<,>$, we get that W fixes the set of hyperplanes H_α, and permutes the chambers by $w(\Lambda_\Delta) = \Lambda_{w(\Delta)}$ for $w \in W$.

Example 80. Weyl chambers are inherently geometric objects. As such, here is a pictorial representation of a Weyl chamber in $\mathbb{R}^2$. The following systems has 6 Weyl chambers, the roots are denoted by the vectors in black, the hyperplanes by the grey lines, and one of the 6 Weyl chambers is colored in blue.



Definition 81. A subset $\sqrt{}_1 \subseteq \sqrt{}$ is *closed* if $\sqrt{}_1 = (\{\sqrt{}_1\}_{\mathbb{Z}} \cap \sqrt{}$. A subset $\sqrt{}_1 \subseteq \sqrt{}$ is $\mathbb{Q}-$*closed* if $\sqrt{}_1 = (\{\sqrt{}_1\}_{\mathbb{Q}} \cap \sqrt{}$. $\sqrt{}$ is *reducible* if $\sqrt{} = \sqrt{}_1 \cup \sqrt{}_2$ where $\sqrt{}_1, \sqrt{}_2$ are nonempty subsystems of $\sqrt{}$ and $< \alpha, \beta >= 0$ for all $\alpha \in \sqrt{}_1, \beta \in \sqrt{}_2$ i.e. these subsystems are orthogonal. $\sqrt{}$ is called *irreducible* otherwise.

If $\sqrt{}$ is reducible, then we can decompose $X_{\mathbb{Q}} = \{\sqrt{}_1\}_{\mathbb{Q}} + \{\sqrt{}_2\}_{\mathbb{Q}}$ where the decomposition is comprised of orthogonal subsets with both $\sqrt{}_1$ and $\sqrt{}_2$ being $\mathbb{Q}$-closed. Since every root system

can be decomposed into a disjoint union of mutually orthogonal subsystems $\sqrt{} = \sqrt{}_1 \sqcup \cdots \sqcup \sqrt{}_s$, this induces a decomposition on the fundamental system Δ of $\sqrt{}$ as $\Delta = \Delta_1 \sqcup \cdots \sqcup \Delta_s$.

Definition 82. We call Δ *irreducible* if $\sqrt{}$ is irreducible.

So if $\Delta = \{\alpha_1, \cdots, \alpha_l\}$ is an irreducible fundamental system then

- $\alpha_1, \cdots, \alpha_l$ are linearly independent.
- $\frac{2<\alpha_i,\alpha_j>}{<\alpha_i,\alpha_i>}$ is non-positive if $i \neq j$.
- Δ is not decomposable as two mutually orthogonal subsets.

1.4.2 Dynkin Diagrams

Consider $\Delta = \{\alpha_1, \cdots, \alpha_l\}$ as a set of vectors in Euclidean space satisfying properties *i), ii),* and *iii).* We may classify such a set using the *Dynkin diagram of* Δ which we define as follows:

1) To each vector α_i associate a vertex;

2) Connect the two vertices associates with α_i and α_j with an edge if and only if $< \alpha_i, \alpha_j > \neq 0$;

3) The Schwarz inequality implies that

$$0 \leq \frac{2 < \alpha_i, \alpha_j >}{< \alpha_i, \alpha_i >} \frac{2 < \alpha_i, \alpha_j >}{< \alpha_j, \alpha_j >} \leq 4$$

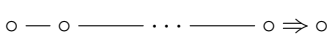
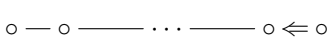
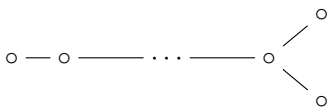
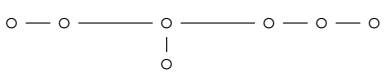
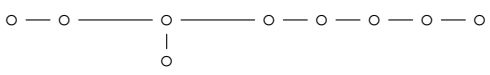
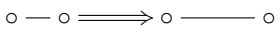
we have that

$$c_{\alpha_i,\alpha_j} := \frac{2 < \alpha_i, \alpha_j >}{< \alpha_i, \alpha_i >} \in \{0, -1, -2, -3\}$$

so connect vertices with single, double, or triple lines according to whether $c_{\alpha_i,\alpha_j} = 1, 2$, or 3;

4) Direct these edges with an arrow pointing from a longer vector to a shorter vector if the lengths are different.

Following this process, we classify all such Δ and, as we will find out shortly, the following Dynkin diagrams give the classification of simple algebraic groups defined over an algebraically closed field.

Classification	*Diagram*	*Group*
A_n :		$SL(n+1)$
B_n :		$SO(2n+1)$
C_n :		$S_p(n)\,\mathrm{char}(k) \neq 2$
D_n :		$SO(2n)$
E_6 :		
E_7 :		
E_8 :		
F_4 :		
G_2 :		

1.5 Example: $SL(3,\mathbb{Q})$: reprise

Recall that given a torus T defined over k, we defined the character group as the group of maps $\chi : T \to (\mathbb{G}_m)^n$ under the operation

$$(\chi + \chi')(t) = \chi(t) \cdot \chi'(t)$$

It's imperative to note the additive notation used in this definition. Also recall the canonical characters $\chi_i : T \to \mathbb{G}_m$ given as "projections", i.e., if $t = (t_1, \cdots t_n)$ then $\chi_i(t) = t_i$.

Define $E_{i,j}$ as a matrix which is 1 at the i-th row and j-th column and 0 elsewhere. We may note that we have a family of embeddings of $\mathbb{G}_a$ into $\mathrm{SL}(3,\mathbb{Q})$ given by $\alpha \mapsto I + \alpha \cdot E_{i,j}$ for $1 \leq i, j \leq 3, j \neq i$. This leads us to the following proposition.

Claim 83. *The set of matrices of the form*

$$\begin{pmatrix} 1 & m & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

form a closed subgroup of $SL(3,\mathbb{Q})$, which we will call $P_{1,2}$.

Proof.

- $$\begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- $I_3 \in P_{1,2}$
- Inverses are given by

$$\begin{pmatrix} 1 & -a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Thus, $P_{1,2}$ is a subgroup of $\mathrm{SL}(3,\mathbb{Q})$ obtained by additionally setting $x_3 = x_4 = x_6 = x_7 = x_8 = 0$. □

Define $f : \mathbb{G}_a \to \mathrm{SL}(3,\mathbb{Q})$ by $\alpha \mapsto I + \alpha \cdot E_{1,2}$. We will show f is a root. Let T be the maximal torus of $\mathrm{SL}(3,\mathbb{Q})$ defined previously. Let

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} = t \in T$$

Then,

$$
\begin{aligned}
t \cdot f(\alpha) \cdot t^{-1} &= \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \cdot \begin{pmatrix} 1 & \alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1/a & 0 & 0 \\ 0 & 1/b & 0 \\ 0 & 0 & 1/c \end{pmatrix} \\
&= \begin{pmatrix} 1 & \frac{a}{b}\alpha & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= f\left(\frac{a}{b} \cdot \alpha\right) \\
&= f\left(\frac{\chi_1}{\chi_2}(t) \cdot \alpha\right) \\
&= f((\chi_1 - \chi_2)(t) \cdot \alpha)
\end{aligned}
$$

Furthermore, we see that $f(\alpha)$ defines an isomorphism onto $P_{1,2}$. Note that we may let $f : \mathbb{G}_a \to \mathrm{SL}(3, \mathbb{Q})$ be given by $f(\alpha) = I + \alpha E_{2,3}$ and run a similar argument to show $(\chi_2 - \chi_3)(t)$ has a similar property. We may then choose there two roots to be positive. Now, there is a redundancy for $(\chi_1 - \chi_3)(t)$, since $(\chi_1 - \chi_3)(t) = ((\chi_1 - \chi_2) + (\chi_2 - \chi_3))(t)$. This root is also positive. Furthermore, we also will have similar results for $(\chi_3 - \chi_1)(t) = (-(\chi_1 - \chi_3))(t)$, $(\chi_2 - \chi_1)(t) = (-(\chi_1 - \chi_2))(t)$, and $(\chi_3 - \chi_2)(t) = (-(\chi_2 - \chi_3))(t)$, however, these roots are not positive. We can see that the only positive roots we need to generate other roots are $\chi_1 - \chi_2$ and $\chi_2 - \chi_3$. Assuming that these are the only roots in $\surd$, we will have that $\chi_1 - \chi_2$ and $\chi_2 - \chi_3$ are the simple roots of $\mathrm{SL}(3, \mathbb{Q})$.

Claim 84. *$SL(3,\mathbb{Q})$ is of type A_2. i.e. the Dynkin diagram of $SL(3,\mathbb{Q})$ is* $\circ$——$\circ$

Proof. We must first prove that

$$\{\chi_1-\chi_2,-(\chi_1-\chi_2),\chi_2-\chi_3,-(\chi_2-\chi_3),\chi_1-\chi_3,-(\chi_1-\chi_3)\}=\surd$$

and

$$\{\chi_1-\chi_2,\chi_2-\chi_3\}=\Delta$$

Then we must compute the value of the Cartan integers.

Observe that T is obviously normalized in G not only by itself, but also by matrices permuting the entries in the diagonal. One may show via some very tedious matrix computations that these are the only matrices normalizing T in G, so by definition $W=\mathbb{N}_G(T)/T\cong S_3$. The order of S_3 is 6, this implies that there are 6 Weyl chambers. Note the following lemma:

Lemma 85. Given an n-dimensional affine k-space $\mathbb{A}_k^n$ with $\operatorname{char} k=0$, a non-zero element $v\in\mathbb{A}_k^n$, and a hyperplane γ, we have that v is orthogonal to γ if and only if cv is orthogonal to γ for every $c\in k\setminus\{0\}$.

In particular, this lemma implies that the hyperplane $H_{e_i}=H_{-e_i}$ for $1\leq i\leq 3$. Furthermore, each of these hyperplanes must be distinct. Now since the dimension of T is 2, we know that X is a rank 2 $\mathbb{Z}-$module by proposition 73. By definition we are considering the Weyl chambers (and hence the roots as well) as vectors in the space $X_{\mathbb{R}}:=X\otimes_{\mathbb{Z}}\mathbb{R}$. Since X is a

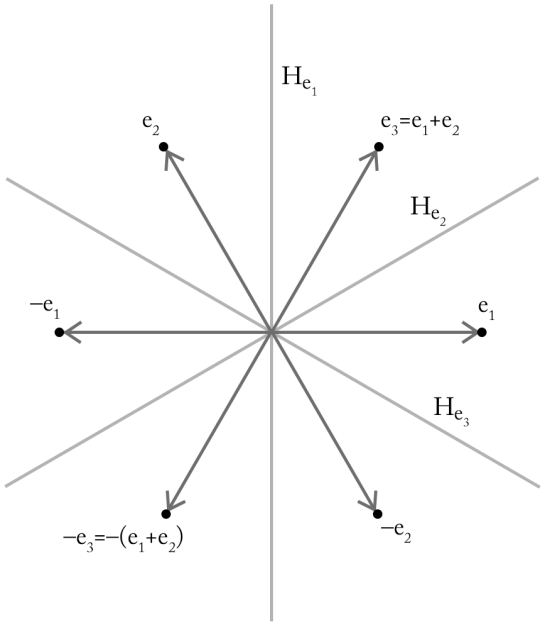
finitely generated rank 2 torsion free $\mathbb{Z}$-module and tensor commutes with direct products we have that

$$X_{\mathbb{R}} := X \otimes_{\mathbb{Z}} \mathbb{R} \cong (\mathbb{Z} \times \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{Z} \oplus_{\mathbb{Z}} \mathbb{R} \times \mathbb{Z} \oplus_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R} \times \mathbb{R}$$

In this particular case we can see that a hyperplane is just a linear subspace of $\mathbb{R}^2$, that is, a line. If we were to have an additional non-trivial element $e_4 \in \surd$, then we would have an additional distinct hyperplane H_{e_4} which would inevitably give us 8 Weyl chambers, rather than 6. So it must be the case that the roots are given as above and thus our choice of Δ is legitimate.

Since the Weyl group acts transitively by reflection on each Weyl chamber, each Weyl chamber must be symmetric with all the others, that is the angle between each hyperplane (line) is equal. Now, in order to satisfy that $< e_1, e_2 >=< e_2, e_1 > \leq 0$ we must have that the

angle between the vectors e_1 and e_2 is greater that $\pi/2$. So up to some rotation we have this figure,



Since the angle between e_1 and e_2 is $2\pi/3$ we have that

$$c_{e_1,e_2} = \frac{2 < e_1, e_2 >}{< e_1, e_1 >} = \frac{2|e_1||e_2|\frac{-1}{2}}{|e_1|^2} = \frac{-|e_2|}{|e_1|}$$

and also that

$$c_{e_2,e_1} = \frac{2 < e_2, e_1 >}{< e_2, e_2 >} = \frac{2|e_2||e_1|\frac{-1}{2}}{|e_2|^2} = \frac{-|e_1|}{|e_2|}$$

Note that $c_{e_2,e_1} = c_{e_1,e_2}$ are negative integers, and $|v| \geq 0$ for any $v \in \mathbb{R}^2$. Thus

$$\frac{-|e_1|}{|e_2|} = \frac{-|e_2|}{|e_1|} \iff |e_1|^2 = |e_2^2| \iff |e_1| = |e_2|$$

This implies that $c_{e_2,e_1} = c_{e_1,e_2} = -1$. Following our algorithm for generating the Dynkin diagram, we have that $\mathrm{SL}(3,\mathbb{Q})$ is described by an A_2 diagram. $\square$

1.6 Classification of Semi-simple groups

If G is an algebraic group and R its radical, then G/R is semi-simple. So to complete the classification of algebraic groups we need the following:

1. Classify all semi-simple groups.;
2. Classify all R, i.e., all solvable groups;
3. Determine how to "glue" a semi-simple group G and a solvable group R to construct all algebraic groups.

The first step is the classification of semi-simple groups—which is the focus of this section. We have introduced many if the ideas needed to consider the two other steps, but the details are beyond the scope of this work.

Unless indicated otherwise G and G' will be semi-simple algebraic groups with maximal tori T and T', character modules X and X' with root systems (with respect to T and T') $\surd$ and $\surd'$ and fundamental systems Δ and Δ'. We begin the reduced classification problem by noting the following.

If $\phi : G \to G'$ is an isogeny, then ϕ induces a one-to-correspondence between the sets of closed and connected subgroups of G and G' given by

$$H \mapsto \phi(H), \text{ and } H' \mapsto (\phi^{-1}(H))^0$$

where $(\phi^{-1}(H))^0$ denotes the connected component of the identity in $\phi^{-1}(H)$. In particular this induces a one-to-one correspondence between the sets of maximal tori in G and G'. So

let T be a maximal torus in G. The restriction of ϕ to T must then be an isogeny of T to T', and by Proposition 26 this induces an injection ${}^t\phi|_T : X' \to X$ which has finite cokernal. Denote ${}^t\phi|_T$ as ${}^t\phi$. For each $\alpha \in \surd, \alpha' \in \surd'$ let x_α and $x_{\alpha'}$ denote the isomorphisms of $\mathbb{G}_a$ to the subgroups P_α and $P_{\alpha'}$ defined in the definition of a root. Then

$$tx_\alpha(\eta)t^{-1} = x_\alpha(\alpha(t)\eta) \Rightarrow \phi(t)(\phi \circ x_\alpha)(\eta)\phi(t^{-1}) = (\phi \circ x_\alpha)(\alpha(t)\eta)$$

for $t \in T, \eta \in \mathbb{G}_a$. In particular $\phi(P_\alpha)$ is a one dimensional unipotent subgroup of G' which is invariant under T', so for some $\alpha' \in \surd'$ we have that $\phi(P_\alpha) = P'_{\alpha'}$. Furthermore, after observing the diagram

$$\begin{array}{ccc} \mathbb{G}_a & \xrightarrow{x_\alpha} & P_\alpha \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \phi} \\ \mathbb{G}_a & \xrightarrow{x'_{\alpha'}} & P'_{\alpha'} \end{array}$$

where ψ is the map making this diagram commute, we can see that ψ is an isogeny. It follows for any $\eta \in \mathbb{G}_1$ that $\psi(\eta) = \lambda\eta^{q_\alpha}$ where $\lambda \in \Omega$ and q_α is a power of the characteristic exponent. Via a diagram chase we can then prove that

$$x'_{\alpha'}(\alpha'(t')\lambda\eta^{q_\alpha}) = x'_{\alpha'}(\lambda\alpha(t)^{q_\alpha}\eta^{q_\alpha}$$

for all $t \in T, \eta \in \mathbb{G}_a$. We know that

$$\alpha'(t') = ({}^t\phi(\alpha'))(t)$$

and so in additive notation

$$^t\phi(\alpha') = q_\alpha \alpha$$

We may encode this data into the following definition

Definition 86. And injective homomorphism $\rho : X'_{\mathbb{Q}} \to X_{\mathbb{Q}}$ is called special if

- $\rho(X') \subseteq X$
- There exists a bijection $f : \surd \to \surd'$ so that $(\rho \circ f)(\alpha) = q_\alpha(\alpha)$ for every $\alpha \in \surd$ with q_α denoting a power of the characteristic exponent.

To summarize, we have proven that the injective homomorphism $^t\phi : X' \to X$ which is induced by an isogeny $\phi : G \to G'$ is special. In particular we note that ϕ is an isomorphism if and only if $^t\phi$ is surjective. The converse of this result is known as the fundamental theorem of Chevalley, which is true over an algebraically closed field.

Theorem 87. *(The Fundamental Theorem of Chevalley)*

Let G, G' be connected semi-simple algebraic groups with maximal tori T, T' and X, X' character modules of T, T'. If there exists a special injective homomorphism $\rho : X' \to X$ then there exists an isogeny $\phi/G \to G'$ so that $\phi/\overline{k}$ and $^t\phi = \rho$. Furthermore, ϕ is unique up to inner automorphism given by $T \in T$

Theorem 88. *(Existence Theorem of Chevalley)*

Let k_0 be any prime field. If X is a free module of finite rank, and $\surd$ a root system in X, then there exists a connected semi-simple algebraic group G, defined over k_0 having $(X, \surd)$ as

its root system with respect to some maximal torus T of G. Furthermore, we may take T to be k_0 trivial.

Definition 89. An algebraic group satifying the Existence Theorem of Chevalley is called a *Chevalley group*

In particular, Theorem 87 gives that any Chevalley group G is uniquely determined by only its character module X and its root system $\sqrt{}$. Thus we denote a Chevalley group by $G(X, \sqrt{})$.

Chevalley's theorems can also be used to further reduce our classification problem to the case where we only consider irreducible root systems in the following manner.

If we assume that $\sqrt{} = \sqrt{}_1 \cup \sqrt{}_2 \cup \cdots \cup \sqrt{}_n$ is a decomposition into mutually orthogonal irreducible subsets then the injection $(\oplus X_i, \cup \sqrt{}_i) \mapsto (X, \sqrt{})$ is special and thus $G(X, \sqrt{})$ is isogeneous to $\prod G(X_i, \sqrt{}_i)$. Now if $\sqrt{}_l \subseteq \sqrt{}$ is a closed subsystem, then denote by $G(\sqrt{}_l)$ the closed subgroup of $G(X, \sqrt{})$ generated by $\{P_\alpha | \alpha \in \sqrt{}_l\}$. It follows that $G(\sqrt{}_l)$ is a connected semi-simple algebraic subgroup, and restricting the previous isogeny to to $G(\sqrt{}_l)$ gives an isogeny from $G(\sqrt{}_l)$ to $G(X_l, \sqrt{}_l)$. Therefore, the classification reduces to the case where $\sqrt{}$ is irreducible.

Thus we give the following definitions:

Definition 90. An algebraic group G is called $k-$*simple* if G is defined over k, is semi-simple, and every connected normal subgroup is either trivial or the whole of G. Furthermore, G is called *absolutely simple* if G has an irreducible root system.

Concerning the field of definition, the following proposition modifies Theorem 88.

Proposition 91. *Let $G(X, \sqrt{})$ and $G(X', \sqrt{}')$ be Chevalley groups defined over the prime field k_0 with maximal tori T, T' which are split over k_0. If there exists a special injection $\rho : X' \to X$ then there exists an isogeny $\phi : G(X, \sqrt{}) \to G(X', \sqrt{}')$ so that ${}^t\phi = \rho$. Furthermore ϕ can be taken to be defined over k_0.*

We now can see an outline of how the classification of connected semi-simple algebraic groups over a perfect ground field k reduces to the problem of classifying absolutely simple algebraic groups defined over a finite extension K/k.

Assume G_k is a connected semi-simple algebraic group. Chevalleys theorems give that G is isomorphic to a Chevalley group $G(X, \sqrt{})$ by a isomorphism defined over k. We may reduce to the case where G is simply connected. So assume that G is $\overline{k}-$isomorphic to the product $\prod G(\sqrt{}_i)$ which are all connected, simple, and defined over $\overline{k}$. Note that taking $\Gamma^i = \{\sigma \in \Gamma | G(\sqrt{}_i)^\sigma = G_i\}$ defines an extension K_i/k which is the fixed field of Γ^i. Since $G(\sqrt{}_l)$ are defined over a finite extension of k we have that K_i/k is finite. Now set $d = [K_l : k]$ and let $\{\sigma_1, \cdots, \sigma_d\}$ be the set of coset representatives of $\frac{\Gamma}{\Gamma^l}$ be chosen with σ_1 as the identity. The set $\{G_1^{\sigma_1}, \cdots, G_1^{\sigma_n}\}$ is the set of Γ-conjugates of G_1, and each of these groups must be a factor of G_1 since Γ permutes direct factors of G_1. Thus we have that G must be isomorphic over $\overline{k}$ to $\prod_{i=1}^d G_1^{\sigma_i} \times G'$. Additionally the factor $\prod_{i=1}^d G_1^{\sigma_1}$ is invariant under Γ so it must be defined over k. In fact, G is $k-$isomorphic to $R_{K_1/k}(G_1) \times G'$. Repeating this argument with G' replacing G we will have that G is isomorphic to $R_{K_1/k}(G_1) \times R_{K_1/k}(G_1') \times \cdots$. This implies the following.

Proposition 92. *G is $k-$simple if and only if $G \cong R_{K_1/k}(G_1)$ where G_1/K_1 and G_1 is absolutely simple. Therefore, the classification of a connected algebraic groups G reduces to the*

classification of $k-$simple groups, but this reduces to the classification of absolutely simple groups defined over K, with K/k a finite extension. In other words—we have completed step 1. of our classification of algebraic groups and would need to look toward steps 2. and 3. to complete the classification of algebraic groups.

CITED LITERATURE

1. Satake, I. and Sugiura, M.: Classification theory of semi-simple algebraic groups. Number v. 3 in Lecture notes in pure and applied mathematics. M. Dekker, 1971.

2. Atiyah, M. and MacDonald, I.: Introduction To Commutative Algebra. Addison-Wesley series in mathematics. Avalon Publishing, 1994.

3. Lang, S.: Algebra. Graduate Texts in Mathematics. Springer New York, 2005.

Chicago, IL 60607

Luke Jaskowiak

Education

2016–present **M.S. in progress, Mathematics**, *University of Illinois at Chicago*, *Chicago, IL.*

2014–2016 **B.S., Mathematics with Honors**, *University of Illinois at Chicago*, *Chicago, IL.*

2013–2014 **Undergraduate Studies**, *Joliet Junior College*, *Joliet, IL.*

2009–2012 **AS**, *Monroe County Community College*, *Monroe, MI.*

Experience

Writings/publications

2018 **Masters Thesis: Survery on the Classification Theory of Semi-Simple Algebraic Groups Over Perfect Fields**, *My advisor for this project was Ramin Takloo-Bighash.*

2016 **Ulrich Partitions for Two-Step Flag Varieties**, *Joint with Izzet Coskun*, Involve, a Journal of Mathematics 10-3 (2017), 531–539. DOI 10.2140/involve.2017.10.531. Available at http://msp.org/involve/2017/10-3/p11.xhtml

Teaching

Summer 2017 and 2018 **Instructor for a Summer Enrichment Workshop in Mathematics**, *University of Illinois at Chicago*, Facilitated a summer workshop in mathematics designed to provide supplementary mathematical exposure for students.

Spring 2018 **Guest Graduate Mentor**, *2018 Meeting of MATh.en.JEANS in Chicago*, Facilitated the presentation and provided feedback for student projects. All presentations were conducted in French.

2017–present **Emerging Scholars Program Discussion Moderator**, University of Illinois at Chicago, Generated content for and guided learning sessions covering advanced material which utilize a cooperative learning methodology..

Department of Mathematics, Statistics, and Computer Science
University of Illinois at Chicago – 851 S. Morgan Street
815.685.0672 • *Ljasko2@uic.edu*

2016–present **Teaching Assistant**, University of Illinois at Chicago, Facilitated discussion sections for college math classes, including calculus, in addition to holding office hours in the mathematics department's tutoring center.

2015 **Undergraduate Math Tutor**, University of Illinois at Chicago.

Assisted undergraduate students at the tutoring center of the department of mathematics at University of Illinois at Chicago in a wide variety of topics, including geometry, statistics, probability, trigonometry, single and multi-variable calculus, differential equations, and linear algebra.

2013-2014 **Undergraduate Math Tutor**, Joliet Junior College.

Assisted students coming to the walk-in tutoring center at Joliet Junior College in a wide variety of topics, including geometry, trigonometry, single and multi-variable calculus, differential equations, and linear algebra.

Workshops and Conferences Attended

May 2016 **Undergraduate Algebraic Geometry**, *University of Utah.*